## \*\*1AC – CYBER AFF\*\*

### 1ac – Cyber Attacks Adv

**CONTENTION 1 IS CYBER ATTACKS**

**First Scenario is the Grid**

#### Most recent evidence says that cyber attacks on the power grid are coming now --- current security measures will fail

**Gjelten 8/15/13** [Tom, The Next Disaster Scenario Power Companies Are Preparing For, <http://www.npr.org/blogs/alltechconsidered/2013/08/15/212079908/the-next-disaster-scenario-power-companies-are-preparing-for>, nrb]

\*\*article cites Michael Assante – chief executive of the National Board of Information Security Examiners and an expert on grid security

In the 10 years since sagging power lines in Ohio sparked a blackout across much of the Northeastern United States and Canada, utility engineers say they have implemented measures to prevent another such event in the country's electric grid. But there is one disaster scenario for which the power companies are still unprepared: a massive attack on the computer networks that underlie the U.S. electric grid. Energy industry leaders believe **a cyberthreat could produce a blackout even bigger than the August 2003 outage**, which left an estimated 50 million people in the dark. "We have to treat the cyberthreat with the same respect that we give to forces of nature, [such as] hurricanes, floods, ice, storms," said Chris Peters, vice president for critical infrastructure at Entergy, a company that operates nuclear power plants. "We have to fund it, we have to staff it and we have to be ready to respond as necessary." Peters was among several power executives who gathered in Washington recently to discuss the need to better protect the electric grid against cyberattacks. Their consensus judgment was that such attacks are probably inevitable. "At some point in time, somebody is coming at me," said Scott Saunders, information security officer for the Municipal Utility District in Sacramento, Calif. "It's going to happen." The New Grid The concern that computer hackers could shut down the electric grid stems from technological changes in the power industry. Much of the equipment used in the grid, from the generators to the transformers, is now operated by computers. By disrupting computer network operations, hackers could shut down a key part of the grid. They would still need access to the computers, but this obstacle could be overcome because many of those computers are now connected to the Internet. "Now we can remotely manage devices via the Internet," notes Mark Weatherford, until recently a top cyberspecialist at the Department of Homeland Security. "So instead of putting someone in a truck and having them drive a hundred miles to a substation in the middle of the mountains somewhere, you remotely manage that." Weatherford, now consulting on cyber issues at the Chertoff Group, says power companies saw that managing grid operations via the Internet brought efficiencies and cut costs, so they jumped at the chance. Perhaps a bit recklessly. "To no one's fault at the time — we didn't realize it — [we] didn't think about the security and the insecurity [of Internet connections]," Weatherford said. When a computer is connected to the Internet, a skilled hacker can often find a way to break into it. This is the new disaster scenario for power companies. Security experts in the industry are aware of the challenge and moving quickly to meet it, but the **threats to their networks may be evolving even faster.** "Computers are tricky," says Michael Assante, chief executive of the National Board of Information Security Examiners and one of the country's top experts on the cyberthreat to the grid. "They just continue to become more complex, and the importance to how we operate the system continues to increase." The 2003 blackout was not caused by a cyberattack, but even then computers were part of the system, and Assante says one reason the blackout spread far and wide was that many operators didn't understand their own computer connections. "How do we teach power engineers and operators what they need to know about cyber and in particular about cybersecurity?" Assante asks. "These are tough questions. If you go to engineering school, you're not taught about cybersecurity as part of becoming a power engineer." Hurdles To A Solution The concern now is that a really sophisticated cyberattack could cause a blackout bigger than anything yet seen in North America. Congress has considered various bills that would require power companies to beef up their protection against cyberattack and impose mandatory security standards. A survey of electric utilities earlier this year, directed by Reps. Edward Markey (now a U.S. senator) and Henry Waxman, found that most of the companies had **failed to implement voluntary cybersecurity standards** recommended by the North American Electric Reliability Corp., an industry organization. Attempts to legislate mandatory cybersecurity standards have been rebuffed, however, in part because the power industry opposed them. "Our companies are in the business of selling electricity. They are fully motivated to do what they need to do to protect their systems against cyberattack and other problems," says James Fama, vice president for energy delivery at the Edison Electric Institute, which represents power companies. "We don't need to be penalized in order to be motivated to provide continuity of service. That's the business we're in." But computer hackers are becoming more sophisticated, and they increasingly see the power grid as a target. Redesigning the grid to make it less vulnerable to cyberattacks will be expensive. Some companies might calculate that the necessary investments to guarantee grid security might not be justified, given their assumptions that a major attack is still unlikely. "It's really hard to make the business case for this," said former CIA Director Michael Hayden, speaking at the recent Washington conference on grid security, organized by the Bipartisan Policy Center. Curt Hebert, the former chairman of the Federal Energy Regulatory Commission, asked power executives at the conference whether their industry was prepared to make the big investments necessary to secure the grid against a big cyberattack. "When it comes to cost cutting," Hebert suggested, "this may be one of the areas, quite frankly, that gets the knife." Consumers, after all, would eventually be stuck with the bill, paying for those investments through higher rates and being told it was necessary to secure the power grid against a threat they had not actually experienced. Yet.

#### Cyber attacks will devastate the grid --- new grid technology only increases the likelihood of catastrophic failure

**Krepinevich, PhD @ Harvard, 12** [Andrew, PhD & MPA at Harvard, West Point graduate, served 25 years in the Army, worked in the DOD Office of Net Assessment for 3 defense secretaries, president of the Center for Strategic and Budgetary Assessments, http://www.csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/, pp 53-58, nrb]

The Power Grid A WORLD OF POWER DISRUPTIONS? Most Americans are used to the occasional power outage that lasts a few moments or perhaps even a few hours. And many have endured the loss of electric power in their homes for several days following a rare natural disaster (e.g., hurricane, blizzard, ice storm); few have been subjected to power outages lasting more than two weeks, or frequent (i.e., six or more a year) outages that last longer than several days. Moreover, most of these outages are localized, with some communities losing power while others nearby maintain power. In the event of localized protracted outages, those affected can migrate fairly easily to areas with power to obtain food and shelter. In the event of a protracted and widespread outage, this would not be practical for many people. According to one survey, over half of the attacks being conducted against the energy/power and oil/gas sectors target these firms’ SCADA control systems.187 The Conficker worm raised eyebrows when it managed to work its way into some of these systems.188 Without electric power the United States would quickly find itself in many ways back in the 19th century, with the attendant consequences for its citizens’ well-being.189 At a more modest level, if the U.S. power grid were subject to frequent, extended disruptions it would likely result in major and enduring costs incurred to cope with the outages. For example, the loss of refrigeration could risk the large-scale loss of perishable foodstuffs. Pumps required for water and sanitation systems could be disabled. Depending upon the season, the loss of heating and cooling systems could cause significant health problems. The prospect of frequent power interruptions becoming a way of life could impose major, enduring costs on the United States. Assuming they can afford it, individuals may purchase backup generators to ensure the food in their refrigerators does not spoil, the pipes in their homes do not freeze, etc. Some firms in the food business ranging from food suppliers (e.g., supermarkets) to restaurants may require backup power on a far greater scale than is currently the case. Backup power systems would likely be needed to regulate traffic in the absence of traffic lights as would the ability to operate trains powered by electricity. Service stations would need to install backup systems to enable their gas pumps to function, lest automotive transportation break down. Businesses that rely on computers and the Internet might also install backup power systems to continue operating during periods of power outage. Water and sewage systems would need to install backup generators or, if they have them, replace them on a much more frequent basis than is now the case. Power companies would likely take their SCADA systems off the Internet; however, this would not solve the problems associated with insider threats or reliance on a global supply chain. A VULNERABLE GRID Could a cyber attack take the United States, or major parts of it, off the electric grid for significant periods of time? While it is not possible to provide a definitive answer, there is sufficient evidence to justify concern that such an event could occur. Initially U.S. power grid control systems (i.e., SCADA systems) were on closed networks that were not connected to the Internet. Over time, however, the electric industry began relying on SCADA systems to improve the efficiency and performance of their systems. As it is cheaper to maintain an open network than a closed one, firms opted to move to open networks. Access to the Internet, with its attendant benefits and vulnerabilities, became essential for operations.190 In addition to penetrating power companies via the Internet, hackers can compromise SCADA systems by exploiting outdated modems used for maintenance purposes, or by exploiting wireless access points—jumping the “air gap.” Again, irrespective of being on an open or closed network, the problems of supply chain security and insider threats remain. Finally, power companies may buy and trade power among one another, creating the prospect that hackers breaching the defenses of one firm will have effectively penetrated all its partners as well.191 The U.S. power grid’s vulnerability is heightened by two additional factors. First, most grid asset owners and operators have been historically resistant to report cyber attacks against their networks or to make the necessary investments to upgrade and secure their networks.192 Second, the U.S. power grid is highly centralized; the power grid serving the contiguous forty-eight states is composed of three distinct power grids, or “interconnections”—the Eastern Interconnection, the Western Interconnection, and the Electric Reliability Council of Texas Interconnection.193 These interconnections provide power to the continental United States, Canada, and a small part of Mexico. The combination of centralized grids and a lack of emphasis on defensive measures could make the power grid **more vulnerable to cascading failures**, as have been triggered by other events in the past. As roughly 90 percent of the Defense Department’s most critical assets are entirely dependent on the bulk power grid, **there is the potential for a “Cyber Pearl Harbor”** to result from a successful attack on the grid.194 A recent case points out just how vulnerable the grid may be. In 2008 a power company hired a cyber security firm to test the security of the network it employs to oversee its power grid. The cyber security team took only a day to organize its cyber tools before launching its attack. The penetration team monitored SCADA user groups, harvesting the email addresses of people working at the targeted power company. It then sent the workers an email describing the company’s intention to reduce their benefits along with a link to an Internet site where they could obtain more information. When the employees clicked on the link, they were directed to an Internet server set up by the penetration team. The employees’ machines displayed an error message; however, the Internet server down- loaded malware enabling the team to take command of the machines in less than one day.195 The situation may become worse before it gets better. In particular, the recent move by the United States to develop a **“smart grid” could increase the U**nited **S**tates’ **vulnerability to cyber attacks on its electric power infrastructure**.196 The U.S. Department of Energy (DoE) is working to build security into the smart grid, but the challenge is very complex.197 A GROWING CYBER THREAT? Reports in the open source literature indicate that the power grid has been targeted by cyber operations. In 2003 the Slammer worm temporarily took a U.S. nuclear power plant’s safety monitoring system offline.198 That same year the Blaster Worm allegedly was associated with a massive blackout that occurred in the eastern United States.199 More recently, in 2008 the CIA reported that multiple cities outside the United States had their electrical power shut off by hackers. The report was short on details, apparently owing to security concerns, but stated that the attacks came through the Internet.200 Such attacks may not be the sole province of nation-states. For example, computers and manuals **seized in al Qaeda training camps** contained large amounts of SCADA information related to dams and other critical infrastructure.201 One could imagine other non-state entities whose capabilities—both in terms of intellectual and financial resources—are likely to be far greater than those of al Qaeda. In October 2009 Project Grey Goose was established to determine whether there had been any successful hacker attacks against the power grid, both in the United States and in other countries. The project concluded that state and/or non-state actors from a number of countries, most likely China, Russia, and the Commonwealth of Independent States, are almost certainly targeting and penetrating energy provider networks as well as the networks of other critical infrastructures. Among their top priority targets are the United States, Brazil, Russia, and the European Union.202 The attacks have apparently been occurring at low levels for at least a decade. It has not been possible to provide definitive attribution as to who was behind the attacks. There is, however, considerable circumstantial evidence that the states cited above are behind a great many of them. For example, following the death of a People’s Liberation Army pilot in a collision with a U.S. military aircraft on April 1, 2001, thousands of Chinese hackers launched a series of concentrated attacks against U.S. websites in what the New York Times dubbed “The First World Hacker War.”203 The attacks peaked on May 7, coincidentally the two-year anniversary of the accidental U.S. bombing of the Chinese embassy in Belgrade during the 1999 Balkan War (also known as Operation Allied Force). That same day California experienced rolling blackouts over two days, affecting some 400,000 customers.204 An investigation by the California Independent System Operator (CAL ISO) revealed that hackers had gained access to two Solaris web servers that supported CAL ISO’s network and maintained access from April 25 until May 12, the last day of large-scale attacks. Nevertheless, CAL ISO claimed that this breach of its cyber defenses was not related to the blackout. Despite these claims, press reports from the Los Angeles Times claimed access to inside information from CAL ISO that concluded that the cyber penetration came close to producing a “catastrophic breach” of the system. The cyber attack on CAL ISO was traced to Guangdong province in China.205 Project Grey Goose also concluded that network attacks against the bulk power grid will almost certainly **escalate** steadily **in frequency and sophistication** over time due in part to international emphasis among the G20 nations on smart grid research, collaborative energy development projects, and the new opportunities these efforts are likely to create for acts of cyber espionage.206

#### DOD bases are highly vulnerable during grid failure --- vital military infrastructures will be destroyed --- communications breakdowns risk nuclear war

**Andres 11** [Richard B. – Professor of National Security Strategy at the National War College and a Senior Fellow and Energy and Environmental Security and Policy Chair in the Center for Strategic Research, Institute for National Strategic Studies, at the National Defense University, \*\*Hanna L. Breetz – Doctoral candidate in the Department of Political Science at The Massachusetts Institute of Technology, Small Nuclear Reactors for Military Installations: Capabilities, Costs, and Technological Implications, Strategic Forum, National Defense University, Institute for National Strategic Studies, February 2011, http://www.ndu.edu/press/lib/pdf/StrForum/SF-262.pdf]

Grid Vulnerability. DOD is unable to provide its bases with electricity when the civilian electrical grid is offline for an extended period of time. Currently, domestic military installations receive **99 percent** of their electricity from the civilian power grid. As explained in a recent study from the Defense Science Board: DOD’s key problem with electricity is that critical missions, such as national strategic awareness and national command authorities, are almost entirely dependent on the national transmission grid . . . [which] is fragile, vulnerable, near its capacity limit, and outside of DOD control. In most cases, neither the grid nor on-base backup power provides sufficient reliability to ensure continuity of critical national priority functions and oversight of strategic missions in the face of a long term (several months) outage.7 The grid’s fragility was demonstrated during the 2003 Northeast blackout in which 50 million people in the United States and Canada lost power, some for up to a week, when one Ohio utility failed to properly trim trees. The blackout created cascading disruptions in sewage systems, gas station pumping, cellular communications, border check systems, and so forth, and demonstrated the interdependence of modern infrastructural systems.8 More recently, awareness has been growing that the grid is also vulnerable to purposive attacks. A re- port sponsored by the Department of Homeland Secu- rity suggests that a coordinated cyber attack on the grid could result in a third of the country losing power for a period of weeks or months.9 Cyberattacks on critical infrastructure are not well understood. It is not clear, for instance, whether existing **terrorist groups** might be able to develop the capability to conduct this type of attack. It is likely, however, that some **nation-states** either have or are working on developing the ability to take down the U.S. grid. In the event of a war with one of these states, it is possible, if not likely, that parts of the civilian grid would cease to function, taking with them military bases located in affected regions. Government and private organizations are currently working to secure the grid against attacks; however, it is not clear that they will be successful. Most military bases currently have backup power that allows them to function for a period of hours or, at most, a few days on their own. If power were not restored after this amount of time, the results could be disastrous. First, military assets taken offline by the crisis would not be available to help with disaster relief. Second, during an extended blackout, global military operations could be seriously compromised; this disruption would be particularly serious if the blackout was induced during major combat operations. During the Cold War, this type of event was far less likely because the United States and Soviet Union shared the common understanding that blinding an opponent with a grid blackout could **escalate to nuclear war**. America’s current opponents, however, may not share this fear or be deterred by this possibility.

#### Regardless of retaliation, these attacks will collapse the militaries ability to function in critical theaters of combat

**Loudermilk 11** [Micah, Research Associate for the Energy & Environmental Security Policy program with the Institute for National Strategic Studies at National Defense University*, Small Nuclear Reactors: Enabling Energy Security for Warfighters*, Small Wars Journal, March 27th 2011, http://smallwarsjournal.com/blog/small-nuclear-reactors-enabling-energy-security-for-warfighters]

Especially on the domestic front, the need for energy security on military bases is often overlooked. There is no hostile territory in the United States, no need for fuel convoys to constantly supply bases with fuel, and no enemy combatants. However, while bases and energy supplies are not directly vulnerable, the civilian electrical grid on which they depend for 99% of their energy use is -- and that makes domestic installations highly insecure. The U.S. grid, though a technological marvel, is extremely old, brittle, and susceptible to a wide variety of problems that can result in power outages -- the 2003 blackout throughout the Northeast United States is a prime example of this. In the past, these issues were largely limited to accidents including natural disasters or malfunctions, however today, intentional threats such as cyber attacks represent a very real and growing threat to the grid. Advances in U.S. military technology have further increased the risk that a grid blackout poses to the nation's military assets. As pointed out by the Defense Science Board, **critical missions** including national strategic awareness and national command authorities depend on the national transmission grid. Additionally, capabilities vital to troops in the field -- including drones and satellite intelligence/reconnaissance -- are lodged at bases within the United States and their loss due to a blackout would **impair the ability** of troops to operate in forward operating areas.

#### US conventional war fighting is inevitable --- ineffectiveness leads to regional aggression and violent competition among major powers

**Horowitz 9** [Michael C. Horowitz and Dan A. Shalmon, Professor of Political Science @ University of Pennsylvania & Senior Analyst @ Lincoln Group, LLC. The Future of War and American Military Strategy, Orbis, Spring 2009]

It is important to recognize at the outset two key points about United States strategy and the potential costs and benefits for the United States in a changing security environment. First, the United States is very likely to remain fully engaged in global affairs. Advocates of restraint or global withdrawal, while popular in some segments of academia, remain on the **margins** of policy debates in Washington D.C. This could always change, of course. However, at present, **it is a given** that the United States will define its interests globally and pursue a strategy that requires capable military forces able to project power around the world. Because ‘‘indirect’’ counter-strategies are the rational choice for actors facing a strong state’s power projection, irregular/asymmetric threats are inevitable given America’s role in the global order.24 Second, the **worst-case scenario** is a loss of U.S. conventional superiority. Losing military control of the sea and the air, ‘‘the global commons,’’25 would render American global strategy **outmoded in an instant**. The idea that the United States must improve its capacity to fight counterinsurgency operations presumes a need to do so beyond defending the homeland and that the United States will have the capacity to intervene in future conflicts around the world. However, while it seems unlikely at present, what if developments in warfare cut down and then eliminated the conventional military superiority of the United States? The loss of conventional military superiority by the United States would probably make the current strategic environment **look like a picnic**.26 For example, currently a Marine unit deploying to Afghanistan or Iraq focuses most on the post-deployment battlefield tasks. However, imagine a world where commanders and soldiers, like their World War II forbears, must fear being sunk on a transport ship or shot out of the sky on the way over, or being targeted by electronic, nanotechnological, or directed energy or precision guided munitions when preparing to search a village for insurgents.27 In such a strategic environment, overseas deployments to win hearts and minds in a low intensity war or wipe out radical jihadi groups would likely—and logically— take a backseat to more ‘‘traditional’’ concerns: convoys, tank battles, air and coastal defenses, and crash programs to build a new generation of naval and air weapons to take back the seas and skies. Meanwhile, in the interim, the United States homeland would be more at risk than at any point since the World War II—arguably more threatened than in its entire history. What John Mearsheimer has called the ‘‘stopping power of water’’ previously functioned to shield the United States, with its oceanic buffers to the east and west, from existential threats. However, in the information age and if the United States no longer controls the waterways of the world, water may not be enough. A world without American conventional military superiority would also **encourage aggression** by regional actors eager to settle scores and take advantage of the fact that the United States could no longer destroy their military forces at a low cost, to say nothing of the global dangers inherent in the **competition among major powers** that could result. The latter scenario is the worst case and it bears mentioning only because it should inform the framework in which any debate about defense strategy occurs. Pg. 307-308

#### Numerous conflict flashpoints result in great power conflict

**Felzenberg 11** (\*Alvin S. Felzenberg, Professorial Lecturer at The Elliott School of International Affairs at George Washington University, Presidential Historian and Adjunct Faculty Member at the Annenberg School for Communication at the University of Pennsylvania, former Fellow at the Institute of Politics at the John F. Kennedy School of Government at Harvard University, served as Principal Spokesman for the 9/11 Commission, holds a Ph.D. in Politics from Princeton University, \*\*Alexander B. Gray, Student at the Elliott School of International Affairs at George Washington University and the War Studies Department of King’s College, London, *The New Isolationism*, *The National Review*, January 3rd 2011, http://www.nationalreview.com/articles/print/256150)

Anything Reps. Ron Paul (R., Tex.) and Barney Frank (D., Mass.) both support should give the rest of us pause. Their proposal to slash defense spending by $1 trillion over a decade — only the most recent joint effort by the new isolationists on the Left and Right to curtail American military strength around the world — is as foolhardy as it is unrealistic. Were such a policy enacted, the nation and the world would be set on a path not toward peace, but toward instability, conflict, and a lessening of freedom in many corners of the world. As the deteriorating situation on the Korean peninsula reminds us, the security concerns of the United States do not disappear in times of economic distress. America’s interests, whether economic, strategic, diplomatic, or moral, cannot be set aside when Congress tires of them. The United States and the world paid a severe price for the ostrich-like behavior too many democratic nations exhibited during the 1920s and 1930s. Reps. Paul and Frank appear determined to repeat this mistake. The United States continues to face an array of global challenges that require a modern, technologically superior military. It is very much in the interests of the United States to uphold the territorial integrity and economic independence of much of Asia, maintain the security of critical waterways such as the Strait of Hormuz, and protect American trade from pirates and terrorists worldwide. Rather than regard the nation’s defenses as a ready source of money available for diversion to domestic concerns, Congress and the president should identify the challenges America faces and assure that its military is able to meet them. At its core, the Frank-Paul effort appears to be an attempt to prevent repetitions of wars the two congressmen regard as either unnecessary or faultily executed. But the United States has broader and more important long-run national-security concerns than Iraq and Afghanistan. As the U.S. became bogged down in those two countries, it began feeling strains elsewhere, precipitated by China, Russia, and potentially toxic menaces such as Iran and Venezuela. Counterinsurgency warfare and Predator-drone strikes against transnational terrorists certainly defined much of the last decade. But the next decade will witness increasing competition among nation-states for control of valuable resources and the exertion of influence worldwide. Russia, through its control of vital energy pipelines, seeks to draw Western Europe more closely into its orbit, thereby weakening the latter’s historical ties to the United States. By taking a similar approach to Ukraine, Kyrgyzstan, Georgia, the Baltics, and Moldova, Russia is on the verge of re-colonizing economically many of its former satellites. China, while continuing to upgrade its naval capabilities, grows increasingly assertive. In pursuit of its own Monroe Doctrine for East Asia, Beijing has proclaimed its sovereignty over the entire South China Sea, menaced neighbors from India to Vietnam, used its economic muscle to intimidate Japan, and increased its threats against Taiwan. China’s leaders have been studying the writings of the 19th-century American naval theorist Alfred Thayer Mahan, who demonstrated the connection between sea power and economic strength. At the turn of the last century, Theodore Roosevelt found in Mahan the blueprint for achieving unprecedented American influence in world affairs. His efforts to build both a strong navy and a sound economy ushered in the “American century,” the period in which the United States became a force for good throughout the world and a beacon of hope for those yearning to breathe free. In pursuing a “blue-water” ocean-going navy capable of supporting their expanding global economic ambitions, the Chinese are acting from a desire to defend their nation’s trade and access to world markets, with a focus on energy supplies. It is critical that the Chinese — who are closely studying both Mahan’s writings and the history of the Monroe Doctrine — and Americans who see Chinese hegemony over Asia as either inevitable or a price they are willing to pay in exchange for slashing defense spending not draw the wrong lessons from history. Both sides should understand that it was not American might that gave the Monroe Doctrine force, but the then all-powerful British navy. For much of the 19th century, Great Britain had reasons of its own for keeping other nations out of the Western Hemisphere and for wanting to see the United States develop internally. If appropriately funded, the United States Navy has the capacity to play a similar role in China’s rise — perhaps, in the process, influencing how China develops. Should China conclude that the United States intends to remain a visible and active presence in the region, it will respond accordingly. Acting together, the two nations might embark on a series of cooperative ventures designed to help assure a steady flow of trade and an unimpeded exchange of people, goods, and ideas. They can also work together to combat a rise in piracy and terrorism in Asia and elsewhere and to respond to humanitarian crises, like the 2004 Indian Ocean tsunami. For its part, China, should it continue to hold North Korea in check, will achieve some of the status it seeks as a rising world power, with commensurate influence on the world stage. Should China conclude, on the other hand, that the United States intends to turn inward, it may grow even more ambitious and assertive in its region and beyond, potentially menacing world peace. Its smaller neighbors nervously wait to see how the United States will respond to China’s growing assertiveness. Should they come to believe that the U.S. is in retreat, they will make their own accommodations with Beijing. That result would wreak irreparable damage both to America’s economy and to its security. Messrs. Frank and Paul and their supporters have taken it into their minds that a reduced American presence in world affairs, particularly where the military is involved, would be a good thing. They had better think again: World politics, like nature, is hardly prone to respect vacuums. Iran and Venezuela remain as bellicose and destabilizing as ever, in spite of two years of Obama “engagement.” Iran squats beside the Strait of Hormuz, through which much of the world’s energy supply travels. Iran has also, the original Monroe Doctrine be damned, extended its military cooperation with Hugo Chávez’s authoritarian regime. Evidence is strong that Venezuela is providing sanctuary for Hezbollah terrorists in South America. The alliance of these two anti-American and increasingly menacing states could pose a threat to the United States of a kind that would make us nostalgic for the Cuban Missile Crisis. Faced with such challenges, the United States can ill afford military retrenchment as advocated by the new isolationists. While waste in the Pentagon’s budget can and should be cut, the new isolationists want to do it with a chainsaw when a scalpel is needed. In the last decade, the U.S. Navy’s fleet has shrunk to its smallest size since the 19th century, just as potential rivals such as China have not only expanded theirs but have begun to target perceived American maritime vulnerabilities. The U.S. Air Force is fielding an aging and shrinking force, while China is developing an advanced fighter for sale to adversaries of America, including Iran. A world in which the United States willingly ceded power and influence would both be more dangerous and prove less receptive to values that most Americans share, such as respect for human rights, the need to restrain governments through the rule of law, and the sanctity of contracts. By reducing its military strength to alarmingly low levels, the United States would create dangerous power vacuums around the world that other nations, with entirely different values, would be only too happy to fill. That, as history shows, would make war more, rather than less, likely. Congress and the president would do well to reflect on those lessons and remember their duty to provide a dominant American military presence on land, at sea, and in the air.

#### These wars cause extinction

**Chisholm 5** [Paul K. Chisholm, foreign policy and international relations scholar based in Kenya, holds a University Degree in Sociology and Diploma in Human Resources, *Terrorism, the Threat in Perspective and Great Power Conflict*, Free World Syndicate, April, 2005, http://www.synd.org/opinion-columns-chisholm/terrorism.html]

We've heard much about terrorism since the 9/11 attacks. It has become an issue at the forefront of foreign policy and the mainstream media. The danger is no doubt real, the threat to be taken seriously. However, looking at the big picture, we should keep terrorism in perspective and perhaps have a look at more traditional threats to world peace - namely conflict between the great powers. It is a matter of some speculation the damage terrorists could inflict on the western democracies. The worst case scenario being an attack with weapons of mass destruction on a major urban center. A reasonable estimate would place the death toll running from tens of thousands to perhaps a million with accompanying destruction/disruption of domestic infrastructure. The panic would no doubt exceed the actual damage. The ability of terrorist groups to effectively deliver weapons of mass destruction is open to debate. Chemical and biological weapons, while lethal and having great psychological impact may not be able to inflict the kind of mass damage many perceive. Nuclear weapons are the only available that can offer a guarantee of mass destruction. To obtain, deliver and detonate one is no easy task. As frightening as such scenarios are, actual damage would be limited to a city or relatively small geographic area. Simultaneous attacks on several cities with weapons of mass destruction are beyond the reach of international terrorist organizations, especially in the heightened security of the post 9/11 era. Terrorism is usually discussed as an unprecedented threat to western civilization. Those of us who grew up during the cold war were presented with a far more frightening threat to world civilization - the clash to two nuclear armed superpowers. Government officials, military leaders, foreign policy experts and journalists of the cold war era, right up until its end, presented the following scenario: A nuclear war would begin and end with a conventional attack on East Germany lasting approximately 30 minutes. This would be followed by nuclear strikes against major targets in both the United States and Soviet Union and other strategic locations. Accounting for delivery time the world, as we knew it, would **end in approximately 90 minutes**. To add insult to injury **nuclear winter would follow rendering the Earth uninhabitable**. This was made possible, as anti-nuclear protesters told us, by each superpower possessing enough nuclear weapons to destroy the world four times over. Coming back to the present, we are in a transitional stage brought about by 9/11. For the duration of the 1990s the potential for great power conflict was considerably less than during the cold war. Even the last few years have seen little real potential for a major war between superpowers. It was the 9/11 attacks that prompted a more aggressive foreign policy by the United States, soon to be imitated by other nations that have put us back on the path of the potential for major conflict. The immediate focus after the attacks was on international terrorist organizations. We then began to hear about rogue states for which the Bush Doctrine's most famous principle began to gain attention - pre-emptive strikes. The use of such strikes in the Bush Doctrine was originally reserved only for the United States. Many observers at the time warned that a foreign policy Pandora's box had been opened. The concept of pre-emptive strikes has now been adopted as a legitimate response by Russia. Putin has stated he would strike terrorist organizations anywhere in the world to protect the Russian homeland. Ask yourself what would happen should such a strike run counter to the interests of the United States or her allies? Another corner stone of the Bush Doctrine states that no foreign power should approach or equal the United States military capability. US military dominance is a concern of Russia and China. Both nations have been moving to establish closer ties and expand their military capability. Russia has announced they are developing a new generation of nuclear weapons. They are also negotiating increased arms sales to China and are cross training their military. The two countries have also signed agreements offering support for suppression of separatist movements within their borders. China has recently passed a law authorizing force against Taiwan should the island try for independence. With Europe considering lifting the ban of weapons sales to China there is potential for real trouble. We're not in another cold war yet, but we're moving back into the era of great power politics. Russia is the wild card, sitting on the fence between a western or eastern orientation. A look at the globe will tell you there is potential for major war, between India and Pakistan, whose relations always run tense; the growing prominence of Asian nations China and Korea could bring tension with Japan and finally in the next decade we'll see American interests threatened by great power alliance. Terrorism kills people and disrupts civilian life on a limited scale. It doesn't lead to the fall of nations and wide spread annihilation. **Only great power conflict can do that**. Should we not refocus our attention and foreign policy now? Diplomacy should be redirected to head off a full scale arms race and potential conflicts between nuclear parties.

### Scenario 2 is Nuclear Meltdowns

#### Cyber attacks on nuclear power plants are increasing

Goldman 1/9/13 [David, Hacker hits on U.S. power and nuclear targets spiked in 2012, http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/index.html, nrb]

America's power, water, and nuclear systems are increasingly being targeted by cybercriminals seeking to gain access to some of the nation's most critical infrastructure. The number of attacks reported to a U.S. Department of Homeland Security cybersecurity response team grew by 52% in 2012, according to a recent [report](http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf) from the team. There were 198 attacks brought to the agency's attention last year, several of which resulted in successful break-ins. An earlier report from DHS sketched in details on some of those successes. An unidentified group of hackers targeting natural gas pipeline companies gained access to the corporate systems of several of their targets and "exfiltrated" -- that's security-speak for "stole" -- data on how their control systems work. The information obtained "could facilitate remote unauthorized operations," DHS said. There's no evidence the hackers have actually broken into the control systems themselves, the agency added. The energy sector was the most-targeted field, with 82 attacks, and the water industry reported 29 attacks last year. Chemical plants faced seven cyber attacks, and nuclear companies reported six. **Hackers hit the bulls-eye on "several" of their nuclear targets**: "These organizations reported that their enterprise networks were compromised and in some cases, exfiltration of data occurred," the DHS team wrote. It said that it is not aware of any successful breaches of nuclear control networks. Those are only the attacks that we know about, though. Many companies choose not to report incidents, and the majority of cyberattacks go undiscovered, according to industry researchers. Of course, **it's not the quantity of attacks that matters. It's the small handful that succeed.**

#### That risks a nuclear meltdown

**Kesler 11** [Brent, managing editor of Strategic Insights at Naval Postgraduate School, MA Middlebury in international policy & terrorism studies, The Vulnerability of Nuclear Facilities to Cyber Attack, Strategy Insights, Spring 2011, http://edocs.nps.edu/npspubs/institutional/newsletters/strategic%20insight/2011/SI-v10-I1\_Kesler.pdf, nrb]

The United States has 104 nuclear power plants generating 98,000 megawatts of electricity, roughly 20% of the electricity generated within the US. These plants generally have process control systems, often designed by the same companies that provide these systems to non-nuclear power plants.14 However, the operators of non-nuclear plants usually have better hardware and cyber security experience than their colleagues at nuclear facilities. Since installation and upgrades of PCS are costly and time-consuming, most non-nuclear PCS operate for eight to fifteen years, the expected lifespan of the hardware used. However, nuclear plants face even higher costs and more stringent safety requirements for their PCS, so they often choose to continue using their original control systems rather than upgrade. A nuclear PCS can be in service for twenty to thirty years, well past the life expectancy of the hardware. Many plants are still using systems based on analog electronics rather than digital.15 This is confirmed by the experience of nuclear engineer Joe Weiss, now a managing partner of Applied Control Solutions, a consultancy specializing in control system cyber security. Mr. Weiss worked for five years managing a nuclear instrumentation program for the Electric Power Research Institute (EPRI). However, nuclear plants prefer to use tested technologies so Mr. Weiss did not get to do "bleeding edge" research until he managed EPRI's research program for fossil fuel plant instrumentation. This meant that nuclear plants had often adopted modern information technology for their process control systems, but had less experience implementing cyber security on those systems than their colleagues at other electric power plants. This experience gap often led nuclear operators to assume they were less exposed to cyber threats than non-nuclear power plants.16 In the past five years, US government-funded research into the cyber security of process control systems has focused mainly on oil and gas utilities and the electric grid. While nuclear power plants face many of the same issues in protecting their infrastructure, the key difference is the nuclear reactor. Non-nuclear generators can be completely shutdown, but nuclear reactors run for one to two years once the fuel is installed. Even when the reactor is "shutdown", the fuel still produces decay heat and must be cooled, or the reactor core may melt. The partial meltdown of Three-Mile Island Unit 2 occurred during a reactor shutdown due to operator errors and equipment malfunctions.17 If such errors and malfunctions can be replicated by a cyber attack, then **a reactor meltdown is possible**. To determine the danger of this threat, it is necessary to examine cyber incidents that have occurred at nuclear power plants. Davis-Besse worm infection On January 25, 2003, at 12:30 AM Eastern Standard Time, the Slammer worm began exploiting a vulnerability in Microsoft SQL Server. Within ten minutes, it had infected 75,000 servers worldwide—90% of vulnerable hosts. The design of Slammer was simple; it did not write itself to the hard drive, delete files, or obtain system control for its author. Instead, it settled in system memory and searched for other hosts to infect. Removing the worm was as simple as rebooting the server after closing network port 1434, Slammer's point of entry. Installing a patch Microsoft had released six months earlier would eliminate the vulnerability Slammer exploited and prevent another infection. Although Slammer carried no malicious payload, it still caused considerable disruption. It searched for new hosts by scanning random IP addresses. This generated a huge volume of spurious traffic, consuming bandwidth and clogging networks. Slammer’s random IP scans disabled data-entry terminals at a 911 call center in Bellevue, Washington (population 680,000), shutdown 13,000 Bank of America ATMs, and forced Continental Airlines to cancel several flights when their online ticketing system and kiosks could not process orders.18 South Korea suffered a nationwide internet outage lasting half a day.19 The Slammer worm also infected computer systems at the Davis-Besse nuclear power plant near Oak Harbor, Ohio. The worm traveled from a consultant's network, to the corporate network of First Energy Nuclear, the licensee for Davis-Besse, then to the process control network for the plant. The traffic generated by the worm clogged the corporate and control networks. For four hours and fifty minutes, plant personnel could not access the Safety Parameter Display System (SPDS), which shows sensitive data about the reactor core collected from coolant systems, temperature sensors, and radiation detectors—these components would be the first to indicate meltdown conditions. Power plants are required to notify the NRC if an SPDS outage lasts longer than eight hours. The reactor at Davis-Besse had been offline for nearly a year before its Slammer infection due to the discovery of a hole in the reactor head.20 Although Slammer's scanning traffic did block sensors from providing digital readouts to control systems, it did not affect analog readouts on the equipment itself; plant technicians could still get reliable data from sensors by physically walking up to them and looking at them, though this process is slower than retrieving data over a network. Davis-Besse had a firewall protecting its corporate network from the wider internet, and its configuration would have prevented a Slammer infection. However, a consultant had created a connection behind the firewall to the consultancy's office network. This allowed Slammer to bypass the firewall and infect First Energy's corporate network. From there, it faced no obstacle on its way to the plant control network. In response, First Energy set up a firewall between the corporate network and the plant control network. The Davis-Besse incident highlighted the fact that most nuclear power plants, by retrofitting their SCADA systems for remote monitoring from their corporate network, had unknowingly connected their control networks to the internet. At the time, the NRC did not permit remote operation of plant functions.21 That policy would change by 2008. Browns Ferry shutdown The August 19, 2006, shutdown of Unit 3 at the Browns Ferry nuclear plant near Athens, Alabama, demonstrates that not just computers, but even critical reactor components, could be disrupted and disabled by a cyber attack. Unit 3 was manually shutdown after the failure of both reactor recirculation pumps and the condensate demineralizer controller.22 Without the recirculation pumps, the power plant could not cool the reactor, making a shutdown necessary to avoid melting the reactor core. The condensate demineralizer is a kind of programmable logic controller (PLC); the recirculation pumps depend on variable frequency drives (VFD) to modulate motor speed. Both kinds of devices have embedded microprocessors that can communicate data over Ethernet, a popular standard for local access networks (LAN). However, both devices are prone to failure in high traffic environments. A device using Ethernet broadcasts data packets to every other device connected to the network. Receiving devices must examine each packet to determine which ones are addressed to them and to ignore those that are not. It appears the Browns Ferry control network produced more traffic than the PLC and VFD controllers could handle; it is also possible that the PLC malfunctioned and flooded the Ethernet with spurious traffic, disabling the VFD controllers; tests conducted after the incident were inconclusive. The failure of these controllers was not the result of a cyber attack. However, it demonstrates the effect that one component can have on an entire PCS network and every device on that network. Combined with the Davis-Besse worm infection, the Browns Ferry shutdown presents a possible attack scenario. If a worm like Slammer had infected the control network of an active plant and attempted to spread not only through UDP, but also through Ethernet, it could have disabled the recirculation pumps as well as the sensors that would alert plant personnel to the problem. Hatch automatic shutdown Due to the growing network connections between control systems and office computers, even seemingly simple actions can have unexpected results. On March 7, 2008, Unit 2 of the Hatch nuclear power plant near Baxley, Georgia, automatically shutdown after an engineer applied a software update to a single computer on the plant's business network. The computer was used to collect diagnostic data from the process control network; the update was designed to synchronize data on both networks. When the engineer rebooted the computer, the synchronization program reset the data on the control network. The control systems interpreted the reset as a sudden drop in the reactor's water reservoirs and initiated an automatic shutdown.23 This innocent mistake demonstrates how malicious hackers could make simple changes to a business network that end up affecting a nuclear reactor—even if they have no intent to interfere with critical systems. This incident is probably the least critical of those examined so far, since it activated safety systems rather than disrupting them. However, it also demonstrates that plant operators do not fully understand the dependencies between network devices. This would make it difficult to identify and protect all the vulnerabilities in a process control system. Stuxnet: a proof of concept The Stuxnet attack against the Iranian nuclear program demonstrates the impact that a sophisticated adversary with a detailed knowledge of process control systems can have on critical infrastructures. Stuxnet is believed to have destroyed 984 centrifuges at Iran’s uranium enrichment facility in Natanz.24 An analysis of the event by the Institute for Science and International Security (ISIS), based on open source technical data about the Stuxnet computer worm and the Iranian nuclear program, found that Stuxnet may have been designed specifically for that purpose. However, Stuxnet also demonstrates the limitations that even such a sophisticated adversary would face in launching an attack against process control systems. The ISIS report finds that the Stuxnet attack, though it successfully disrupted the Iranian centrifuge program, did not slow down Iran’s accumulation of low-enriched uranium.25 The attack is remarkable for its sophistication, but it did not pose an epic threat to Iran. However, that sophistication must be considered when assessing the vulnerability of nuclear facilities to cyber attack. The Stuxnet worm targeted specific PCS components used in the Iranian centrifuge cascades: a frequency converter manufactured by Iranian firm Fararo Paya, another frequency converter manufactured by Finland’s Vacon,26 and the S7-315 and S7-417 programmable logic controllers made by Siemens.27 The PLCs controlled the frequency converters to modulate the speed at which the centrifuges spun. Stuxnet commanded the PLCs to speed up and slow down the spinning centrifuges, destroying some of them, while sending false data to plant operators to make it appear the centrifuges were behaving normally. The New York Times report suggests that Stuxnet’s authors may have learned about vulnerabilities in the Siemens controllers thanks to a partnership between Siemens and the Idaho National Laboratory aimed at assessing vulnerabilities in such components. These products are general PCS components not unique to the Iranian nuclear program; Siemens reports that at least 24 of its customers were infected by Stuxnet, though they suffered no damage.28 The reason Stuxnet did not disrupt every vulnerable PCS it infected is that it was programmed to disrupt only systems that had the same configuration as the centrifuge cascade used at Natanz.29 Antivirus company Symantec began detecting Stuxnet traffic in June 2009, mostly in Iran, but also in neighboring countries. However, since it did not spread aggressively and did not damage the systems it had infected, it raised little alarm.30 Only at the Natanz enrichment facility did it have a major effect. Experts cited by the New York Times report suggest that Israeli intelligence provided the specific technical details necessary for Stuxnet to limit its damage to the Iranian nuclear program. While the New York Times article only presents a possible scenario, that scenario and the evidence reflect the challenges of executing a catastrophic cyber attack against a nuclear facility. Programming is a cyclical process of trial and error. For an amateur hacker working only with a computer, the costs of testing software are trivial. Testing software designed for process control systems, however, requires access to the system in question, which is usually expensive. Malicious hackers could run tests on a remote PCS they had compromised, but an unsuccessful test could raise alarms or damage the system before the hackers were ready for the next stage of an attack. The Stuxnet authors would need a dedicated testbed to refine their code. Stuxnet also incorporated technical information specific to the Iranian facility. These resources are out of the reach of amateurs and would require the kind of funding and actionable intelligence that comes from state sponsorship. The Stuxnet attack also incorporates elements of the other three incidents examined in this paper. First, it disrupted the systems that monitored physical components, like the Davis-Besse worm infection. Second, it interfered with programmable logic controllers, like the Browns Ferry data storm. Third, it relied on there being some path from ordinary office computer to process control systems, as in the Hatch automatic shutdown. At the same time, the Stuxnet authors innovated on these features: Stuxnet did not simply disrupt sensor output, it faked it; it did not simply interfere with PLCs, it gave them specific instructions; finally, it did not rely on an Internet connection to Natanz—it also traveled between computers on worker’s thumb drives31 and infected components destined for Natanz at their source in the Iranian chain of supply.32 Skeptics and alarmists can both use the Stuxnet attack to justify their positions. Alarmists can point to the vulnerability of PCS and its direct effect on Iranian national interests. However, skeptics can argue that the Stuxnet attack required specific knowledge of a particular facility and cannot be generalized to other systems, the same argument used by the Massachusetts Water Resource Authority. Further, the impact could hardly be described as catastrophic. However, it is important to look at the Stuxnet attack in the context of history. Cyber attacks have evolved from the work of amateurs and professional criminals into a serious endeavor for states engaged in international disputes. States have begun to use cyber attacks not just to gather intelligence or control information networks, but to damage physical infrastructures. While the damage is nowhere near a “digital Pearl Harbor”, the trend is clear: states are actively pursuing cyber attacks as an instrument of foreign policy while advancing the technical know-how such attacks require. Lessons These four incidents hold important lessons for the cybersecurity of nuclear facilities and critical infrastructures in general. First, skeptics claim that PCS are immune from attack since they are not connected to the internet. However, the Davis-Besse incident shows that this is a misconception; even operators who try to monitor and protect every connection cannot be sure they know about all of them. Stuxnet even traveled on portable thumb drives to infect computers that were not connected to the internet. Second, skeptics argue that PCS are immune from attack since they are different from ordinary computers. However, all four incidents demonstrate that PCS have become interoperable with ordinary computers, making them vulnerable. Third, vulnerabilities are more complicated than both skeptics and alarmists realize. Alarmists often invoke the danger of hackers taking control of a power plant, but these incidents show how unintelligent computer viruses and even malfunctions in small devices can have big unexpected effects. This suggests that even though nuclear facilities are vulnerable to attack, a malicious hacker would have difficulty making sure an attack works precisely as planned. Even so, states are working to make cyber attacks more precise, supplementing their methods with intelligence from other sources.

#### Meltdowns independently cause extinction

**Lendman 11** [Stephen, MBA @ Wharton, “Nuclear Meltdown in Japan,” 3-13, <http://www.thepeoplesvoice.org/TPV3/Voices.php/2011/03/13/nuclear-meltdown-in-japan>]

On March 12, Times writer Matthew Wald headlined, "Explosion Seen at Damaged Japan Nuclear Plant," saying: "Japanese officials (ordered evacuations) for people living near two nuclear power plants whose cooling systems broke down," releasing radioactive material, perhaps in far greater amounts than reported. NHK television and Jiji said the 40-year old Fukushima plant's outer structure housing the reactor "appeared to have blown off, which could suggest the containment building had already been breached." Japan's nuclear regulating agency said radioactive levels inside were 1,**000 times above normal**. Reuters said the 1995 Kobe quake caused $100 billion in damage, up to then the most costly ever natural disaster. This time, from quake and tsunami damage alone, that figure will be dwarfed. Moreover, under a worst case **core meltdown**, all bets are off as the entire region and beyond will be threatened with permanent contamination, making the most affected areas unsafe to live in. On March 12, Stratfor Global Intelligence issued a "Red Alert: Nuclear Meltdown at Quake-Damaged Japanese Plant," saying: Fukushima Daiichi "nuclear power plant in Okuma, Japan, appears to have caused a reactor meltdown." Stratfor downplayed its seriousness, adding that such an event "does not necessarily mean a nuclear disaster," that already may have happened - the ultimate nightmare short of nuclear winter. According to Stratfor, "(A)s long as the reactor core, which is specifically designed to contain high levels of heat, pressure and radiation, remains intact, the melted fuel can be dealt with. If the (core's) breached but the containment facility built around (it) remains intact, the melted fuel can be....entombed within specialized concrete" as at Chernobyl in 1986. In fact, that disaster **killed nearly one million people worldwide** from nuclear radiation exposure. In their book titled, "Chernobyl: Consequences of the Catastrophe for People and the Environment," Alexey Yablokov, Vassily Nesterenko and Alexey Nesterenko said: "For the past 23 years, it has been clear that **there is a danger greater than nuclear weapons concealed within nuclear power**. Emissions from this one reactor **exceeded a hundred-fold** the radioactive contamination of the **bombs dropped on Hiroshima and Nagasaki**." "No citizen of any country can be assured that he or she can be protected from radioactive contamination. One nuclear reactor can pollute half the globe. Chernobyl fallout covers the entire Northern Hemisphere." Stratfor explained that if Fukushima's floor cracked, "it is highly likely that the melting fuel will burn through (its) containment system and enter the ground. This has never happened before," at least not reported. If now occurring, "containment goes from being merely dangerous, time consuming and expensive to nearly impossible," making the quake, aftershocks, and tsunamis seem mild by comparison. Potentially, millions of lives will be jeopardized. Japanese officials said Fukushima's reactor container wasn't breached. Stratfor and others said it was, making the potential calamity far worse than reported. Japan's Nuclear and Industrial Safety Agency (NISA) said the explosion at Fukushima's Saiichi No. 1 facility could only have been caused by a core meltdown. In fact, 3 or more reactors are affected or at risk. Events are fluid and developing, but remain very serious. The possibility of an extreme catastrophe can't be discounted. Moreover, independent nuclear safety analyst John Large told Al Jazeera that by venting radioactive steam from the inner reactor to the outer dome, a reaction may have occurred, causing the explosion. "When I look at the size of the explosion," he said, "it is my opinion that there could be a very large leak (because) fuel continues to generate heat." Already, Fukushima way exceeds Three Mile Island that experienced a partial core meltdown in Unit 2. Finally it was brought under control, but coverup and denial concealed full details until much later. According to anti-nuclear activist Harvey Wasserman, Japan's quake fallout may cause nuclear disaster, saying: "This is a very serious situation. If the cooling system fails (apparently it has at two or more plants), the super-heated radioactive fuel rods will melt, and (if so) you could conceivably have an explosion," that, in fact, occurred. As a result, massive radiation releases may follow, impacting the entire region. "It could be, literally, an **apocalyptic event**. The reactor could blow." If so, Russia, China, Korea and most parts of Western Asia will be affected. Many thousands will die, potentially millions under a worse case scenario, including far outside East Asia. Moreover, at least five reactors are at risk. Already, a 20-mile wide radius was evacuated. What happened in Japan can occur anywhere. Yet Obama's proposed budget includes $36 billion for new reactors, a shocking disregard for global safety. Calling Fukushima an "apocalyptic event," Wasserman said "(t)hese nuclear plants have to be shut," let alone budget billions for new ones. It's unthinkable, he said. If a similar disaster struck California, **nuclear fallout** would affect all America, Canada, Mexico, Central America, and parts of South America.

#### Meltdowns also collapse the overall US nuclear industry by decimating public confidence

**USA TODAY 12/12/11** [Editorial: Japan's nuke meltdown shouldn't close U.S. plants, <http://usatoday30.usatoday.com/news/opinion/editorials/story/2011-12-12/Japan-Nuclear-Regulatory-Commission/51850082/1>, nrbontha]

There's never a shortage of things for Americans to worry about — housing foreclosures, the teetering European economy, even bedbugs — so it's no wonder the Japanese nuclear power plant catastrophe that transfixed the world in March has dropped down the list of things to lose sleep over. But new reports suggest that the meltdown at one of the ill-fated Japanese reactors was even worse than originally thought, and large areas around the plant could be [uninhabitable for decades](http://www.usatoday.com/USCP/PNI/NEWS/2011-11-13-APASJapanInsideFukushima_ST_U.htm). Germany, not known for the types of natural disasters that triggered Japan's crisis, responded to the [Fukushima Dai-ichi](http://content.usatoday.com/topics/topic/Fukushima+Dai-ichi) disaster by shutting down eight of its 17 reactors **and moving to phase out the rest by 2022**. Should the United States follow suit? In a word, no. For all its drawbacks, nuclear power remains an indispensable part of the [U.S.](http://content.usatoday.com/topics/topic/U.S) energy mix, reliably providing about [**20% of the nation's electricity**](http://www.eia.gov/energy_in_brief/nuclear_industry.cfm) with little to none of the greenhouse gas emissions generated by competitors such as coal, oil and natural gas. At a time when wind, solar and other renewable forms of energy are still a long way from being able to carry the 24/7 load for a nation increasingly reliant on computers and appliances, nuclear power makes sense — **as long as Americans are confident it's as safe as possible**, which is where the lessons from Japan come in. **The Japanese disaster showed that it's crucial to try to imagine the unimaginable** — Japanese regulators apparently never thought that a tsunami would knock out the plant's emergency electric supply. Here at home, designers of the North Anna nuclear power plant in central Virginia apparently never envisioned an earthquake as big as the one that struck the area in August and [exceeded the plant's supposed capacity](http://content.usatoday.com/communities/greenhouse/post/2011/08/nuclear-power-plant-inspected-quake-damage/1). Luckily, the plant rode it out with no serious damage. While earthquakes and floods are threats to nuclear plants, the worst threat of all is losing the backup electricity necessary to keep pumps running and water circulating to cool nuclear fuel rods. At first, the Japanese plants survived the earthquake and even the tsunami that followed, but when flooding knocked out the plant's badly located backup electricity supply, the reactors lost cooling water and **began to melt down**. Eventually, explosions released radioactive gas, forcing the evacuation of more than 80,000 people and heavily contaminating an area three times the size of [New York City](http://content.usatoday.com/topics/topic/Places,+Geography/Towns,+Cities,+Counties/New+York+City). Reassuringly, the Nuclear Regulatory Commission (NRC) has been focusing on the electricity problem. Plants now typically have just four hours of backup power (although some have ways to keep electricity going for 14 to 16 hours). The Fukushima plant was without power for several days. The commission is mulling new requirements, but it's anywhere from two to four years from implementing new rules for U.S. nuclear power plants to forestall a Fukushima-style disaster. That seems unnecessarily leisurely. Another troubling development: Members of the NRC are at each other's throats, with Chairman Gregory Jaczko and the other four commissioners trading charges of obstinacy. The five are set to [testify before Congress on Wednesday](http://www.usatoday.com/news/politics/story/2011-12-09/nuclear-regulatory-commission-gregory-jaczko/51772588/1). It can't be healthy that the people who are supposed to make sure the nation's nuclear plants operate securely disagree so sharply on regulating the industry. If history proves anything, it's that nuclear power is a reliable part of the U.S. energy mix only to the extent that **Americans are confident it's safe**. The last serious accident at a U.S. nuclear plant, at Pennsylvania's Three Mile Island in 1979, **set back the industry for decades**. No new plant has opened in the U.S. since 1996. The only plant under construction is [set to open in 2013](http://www.eia.gov/energy_in_brief/nuclear_industry.cfm). Another serious accident could **take the U.S. nuclear industry down** with it. The Fukushima disaster serves as a reminder that, [in nuclear power](http://www.usatoday.com/news/world/story/2011-09-21/us-learns-from-fukushima-nuclear-plant/50501582/1), there's **zero margin for major error**.

#### Collapse of the nuclear power industry causes a quick shift to coal --- the impact is warming

**Loudermilk 11** [Micah J., Research Associate for the Energy & Environmental Security Policy program with the Institute for National Strategic Studies at National Defense University, Contracted through ASE Inc, *Small Nuclear Reactors and US Energy Security: Concepts, Capabilities, and Costs*, May 31st, <http://www.ensec.org/index.php?option=com_content&view=article&id=314:small-nuclear-reactors-and-us-energy-security-concepts-capabilities-and-costs&catid=116:content0411&Itemid=375>]

Nuclear vs. Alternatives: a realistic picture When discussing the energy security contributions offered by small nuclear reactors, it is not enough to simply compare them with existing nuclear technology, but also to examine how they measure up against other electricity generation alternatives—renewable energy technologies and fossil fuels. Coal, natural gas, and oil currently account for 45%, 23% and 1% respectively of US electricity generation sources. Hydroelectric power accounts for 7%, and other renewable power sources for 4%. These ratios are critical to remember because idealistic visions of providing for US energy security are not as useful as realistic ones balancing the role played by fossil fuels, nuclear power, and renewable energy sources. Limitations of renewables Renewable energy technologies have made great strides forward during the last decade. In an increasingly carbon emissions and greenhouse gas (GHG) aware global commons, the appeal of solar, wind, and other alternative energy sources is strong, and many countries are moving to increase their renewable electricity generation. However, despite massive expansion on this front, renewable sources struggle to keep pace with increasing demand, to say nothing of decreasing the amount of energy obtained from other sources. The continual problem with solar and wind power is that, lacking efficient energy storage mechanisms, it is difficult to contribute to baseload power demands. Due to the intermittent nature of their energy production, which often does not line up with peak demand usage, electricity grids can only handle a limited amount of renewable energy sources—a situation which Germany is now encountering. Simply put, nuclear power provides virtually carbon-free baseload power generation, and renewable options are unable to replicate this, especially not on the scale required by expanding global energy demands. Small nuclear reactors, however, like renewable sources, can provide enhanced, distributed, and localized power generation. As the US moves towards embracing smart grid technologies, power production at this level becomes a critical piece of the puzzle. Especially since renewable sources, due to sprawl, are of limited utility near crowded population centers, small reactors may in fact prove instrumental to enabling the smart grid to become a reality. Pursuing a carbon-free world Realistically speaking, a world without nuclear power is not a world full of increased renewable usage, **but** rather, **of fossil fuels instead.** The 2007 Japanese Kashiwazaki-Kariwa nuclear outage is an excellent example of this, as is Germany’s post-Fukushima decision to shutter its nuclear plants, which, despite immense development of renewable options, will result in a heavier reliance on **coal-based power as** its **reactors are retired**, leading to a 4% increase in annual carbon emissions. On the global level, **without nuclear power, carbon dioxide emissions from electricity generation would rise nearly 20%** from nine to eleven billion tons per year. When examined in conjunction with the fact that an estimated 300,000 people per year die as a result of energy-based pollutants, the appeal of nuclear power expansion grows further. As the world copes simultaneously with burgeoning power demand and the need for clean energy, nuclear power remains **the one consistently viable option** on the table. With this in mind, it becomes even more imperative to make nuclear energy as safe as possible, as quickly as possible—a capacity which SMRs can fill with their high degree of safety and security. Additionally, due to their modular nature, SMRs can be quickly constructed and deployed widely. While this is not to say that small reactors should supplant large ones, the US would benefit from diversification and expansion of the nation’s nuclear energy portfolio.

#### Emissions are decreasing now --- best EPA data --- shift to coal reverses the trend

**Banerjee 4/15/13** [Neela, EPA: U.S. greenhouse gases drop 1.6% from 2010 to 2011, <http://articles.latimes.com/2013/apr/15/news/la-pn-us-greenhouse-gases-decrease-20130415>, nrb]

The Environmental Protection Agency says greenhouse gas emissions in the United States showed a 1.6% decline from 2010 to 2011. The decrease continued an **overall decline in U.S. greenhouse gas emissions, down 6.9%** since 2005. The EPA said the drop from 2010 to 2011 is driven mostly by power plants **switching from coal** to natural gas, which emits less carbon dioxide when burned. Additionally, a mild winter in the south Atlantic region of the U.S., where much of the heating is electric, resulted in lower electricity demand. Power plants are the single biggest source of greenhouse gases, with 33%. The transportation sector is second, with 28% of emissions. Increases in vehicle fuel economy through 2025 should reduce transportation emissions even further. Greater switching to natural gas from coal will cut power plant emissions. President Obama has pledged to reduce U.S. greenhouse gas emissions 17% below 2005 levels by 2020. Despite the general decline in greenhouse gas emissions, many experts contend that the administration would have to take further steps to meet the 2020 goal.

#### Warming is real and anthropogenic

**Prothero, prof of Geology, 12** [Donald R. Prothero, Professor of Geology at Occidental College and Lecturer in Geobiology at the California Institute of Technology, 3-1-2012, "How We Know Global Warming is Real and Human Caused," Skeptic, 17.2, EBSCO]

How do we know that global warming is real and primarily human caused? There are numerous lines of evidence that converge toward this conclusion. 1. Carbon Dioxide Increase Carbon dioxide in our atmosphere has increased at an unprecedented rate in the past 200 years. Not one data set collected over a long enough span of time shows otherwise. Mann et al. (1999) compiled the past 900 years' worth of temperature data from tree rings, ice cores, corals, and direct measurements in the past few centuries, and the sudden increase of temperature of the past century stands out like a sore thumb. This famous graph is now known as the "hockey stick" because it is long and straight through most of its length, then bends sharply upward at the end like the blade of a hockey stick. Other graphs show that climate was very stable within a narrow range of variation through the past 1000, 2000, or even 10,000 years since the end of the last Ice Age. There were minor warming events during the Climatic Optimum about 7000 years ago, the Medieval Warm Period, and the slight cooling of the Litde Ice Age in the 1700s and 1800s. But the magnitude and rapidity of the warming represented by the last 200 years is simply unmatched in all of human history. More revealing, the timing of this warming coincides with the Industrial Revolution, when humans first began massive deforestation and released carbon dioxide into the atmosphere by burning an unprecedented amount of coal, gas, and oil. 2. Melting Polar Ice Caps The polar icecaps are thinning and breaking up at an alarming rate. In 2000, my former graduate advisor Malcolm McKenna was one of the first humans to fly over the North Pole in summer time and see no ice, just open water. The Arctic ice cap has been frozen solid for at least the past 3 million years (and maybe longer),[ 4] but now the entire ice sheet is breaking up so fast that by 2030 (and possibly sooner) less than half of the Arctic will be ice covered in the summer.[ 5] As one can see from watching the news, this is an ecological disaster for everything that lives up there, from the polar bears to the seals and walruses to the animals they feed upon, to the 4 million people whose world is melting beneath their feet. The Antarctic is thawing even faster. In February-March 2002, the Larsen B ice shelf -- over 3000 square km (the size of Rhode Island) and 220 m (700 feet) thick -- broke up in just a few months, a story -typical of nearly all the ice shelves in Antarctica. The Larsen B shelf had survived all the previous ice ages and interglacial warming episodes over the past 3 million years, and even the warmest periods of the last 10,000 years -- yet it and nearly all the other thick ice sheets on the Arctic, Greenland, and Antarctic are vanishing at a rate never before seen in geologic history. 3. Melting Glaciers Glaciers are all retreating at the highest rates ever documented. Many of those glaciers, along with snow melt, especially in the Himalayas, Andes, Alps, and Sierras, provide most of the freshwater that the populations below the mountains depend upon -- yet this fresh water supply is vanishing. Just think about the percentage of world's population in southern Asia (especially India) that depend on Himalayan snowmelt for their fresh water. The implications are staggering. The permafrost that once remained solidly frozen even in the summer has now thawed, damaging the Inuit villages on the Arctic coast and threatening all our pipelines to the North Slope of Alaska. This is catastrophic not only for life on the permafrost, but as it thaws, the permafrost releases huge amounts of greenhouse gases which are one of the major contributors to global warming. Not only is the ice vanishing, but we have seen record heat waves over and over again, killing thousands of people, as each year joins the list of the hottest years on record. (2010 just topped that list as the hottest year, surpassing the previous record in 2009, and we shall know about 2011 soon enough). Natural animal and plant populations are being devastated all over the globe as their environments change.[ 6] Many animals respond by moving their ranges to formerly cold climates, so now places that once did not have to worry about disease-bearing mosquitoes are infested as the climate warms and allows them to breed further north. 4. Sea Level Rise All that melted ice eventually ends up in the ocean, causing sea levels to rise, as it has many times in the geologic past. At present, the sea level is rising about 3-4 mm per year, more than ten times the rate of 0.1-0.2 mm/year that has occurred over the past 3000 years. Geological data show that the sea level was virtually unchanged over the past 10,000 years since the present interglacial began. A few mm here or there doesn't impress people, until you consider that the rate is accelerating and that most scientists predict sea levels will rise 80-130 cm in just the next century. A sea level rise of 1.3 m (almost 4 feet) would drown many of the world's low-elevation cities, such as Venice and New Orleans, and low-lying countries such as the Netherlands or Bangladesh. A number of tiny island nations such as Vanuatu and the Maldives, which barely poke out above the ocean now, are already vanishing beneath the waves. Eventually their entire population will have to move someplace else.[ 7] Even a small sea level rise might not drown all these areas, but they are much more vulnerable to the large waves of a storm surge (as happened with Hurricane Katrina), which could do much more damage than sea level rise alone. If sea level rose by 6 m (20 feet), most of the world's coastal plains and low-lying areas (such as the Louisiana bayous, Florida, and most of the world's river deltas) would be drowned. Most of the world's population lives in low-elevation coastal cities such as New York, Boston, Philadelphia, Baltimore, Washington, D.C., Miami, and Shanghai. All of those cities would be partially or completely under water with such a sea level rise. If all the glacial ice caps melted completely (as they have several times before during past greenhouse episodes in the geologic past), sea level would rise by 65 m (215 feet)! The entire Mississippi Valley would flood, so you could dock an ocean liner in Cairo, Illinois. Such a sea level rise would drown nearly every coastal region under hundreds of feet of water, and inundate New York City, London and Paris. All that would remain would be the tall landmarks such as the Empire State Building, Big Ben, and the Eiffel Tower. You could tie your boats to these pinnacles, but the rest of these drowned cities would lie deep underwater. Climate Change Critic's Arguments and Scientists' Rebuttals Despite the overwhelming evidence there are many people who remain skeptical. One reason is that they have been fed distortions and misstatements by the global warming denialists who cloud or confuse the issue. Let's examine some of these claims in detail: \* "It's just natural climatic variability." No, it is not. As I detailed in my 2009 book, Greenhouse of the Dinosaurs, geologists and paleoclimatologists know a lot about past greenhouse worlds, and the icehouse planet that has existed for the past 33 million years. We have a good understanding of how and why the Antarctic ice sheet first appeared at that time, and how the Arctic froze over about 3.5 million years ago, beginning the 24 glacial and interglacial episodes of the "Ice Ages" that have occurred since then. We know how variations in the earth's orbit (the Milankovitch cycles) controls the amount of solar radiation the earth receives, triggering the shifts between glacial and interglacial periods. Our current warm interglacial has already lasted 10,000 years, the duration of most previous interglacials, so if it were not for global warming, we would be headed into the next glacial in the next 1000 years or so. Instead, our pumping greenhouse gases into our atmosphere after they were long trapped in the earth's crust has pushed the planet into a "super-interglacial," already warmer than any previous warming period. We can see the "big picture" of climate variability most clearly in ice cores from the EPICA (European Project for Ice Coring in Antarctica), which show the details of the last 650,000 years of glacial-inters glacial cycles (Fig. 2). At no time during any previous interglacial did the carbon dioxide levels exceed 300 ppm, even at their very warmest. Our atmospheric carbon dioxide levels are already close to 400 ppm today. The atmosphere is headed to 600 ppm within a few decades, even if we stopped releasing greenhouse gases immediately. This is decidedly not within the normal range of "climatic variability," but clearly unprecedented in human history. Anyone who says this is "normal variability" has never seen the huge amount of paleoclimatic data that show otherwise. \* "It's just another warming episode, like the Medieval Warm Period, or the Holocene Climatic Optimum or the end of the Little Ice Age." Untrue. There were numerous small fluctuations of warming and cooling over the last 10,000 years of the Holocene. But in the case of the Medieval Warm Period (about 950-1250 A.D.), the temperatures increased only 1°C, much less than we have seen in the current episode of global warming (Fig. 1). This episode was also only a local warming in the North Atlantic and northern Europe. Global temperatures over this interval did not warm at all, and actually cooled by more than 1°C. Likewise, the warmest period of the last 10,000 years was the Holocene Climatic Optimum ( 5,000-9,000 B.C.E.) when warmer and wetter conditions in Eurasia contributed to the rise of the first great civilizations in Egypt, Mesopotamia, the Indus Valley, and China. This was largely a Northern Hemisphere-Eurasian phenomenon, with 2-3°C warming in the Arctic and northern Europe. But there was almost no warming in the tropics, and cooling or no change in the Southern Hemisphere.[ 8] From a Eurocentric viewpoint, these warming events seemed important, but on a global scale the effect was negligible. In addition, neither of these warming episodes is related to increasing greenhouse gases. The Holocene Climatic Optimum, in fact, is predicted by the Milankovitch cycles, since at that time the axial tilt of the earth was 24°, its steepest value, meaning the Northern Hemisphere got more solar radiation than normal -- but the Southern Hemisphere less, so the two balanced. By contrast, not only is the warming observed in the last 200 years much greater than during these previous episodes, but it is also global and bipolar, so it is not a purely local effect. The warming that ended the Little Ice Age (from the mid-1700s to the late 1800s) was due to increased solar radiation prior to 1940. Since 1940, however, the amount of solar radiation has been dropping, so the only candidate remaining for the post-1940 warming is carbon dioxide.[ 9] "It's just the sun, or cosmic rays, or volcanic activity or methane." Nope, sorry. The amount of heat that the sun provides has been decreasing since 1940,[ 10] just the opposite of the critics' claims (Fig. 3). There is no evidence of an increase in cosmic ray particles during the past century.[ 11] Nor is there any clear evidence that large-scale volcanic events (such as the 1815 eruption of Tambora in Indonesia, which changed global climate for about a year) have any long-term effects that would explain 200 years of warming and carbon dioxide increase. Volcanoes erupt only 0.3 billion tonnes of carbon dioxide each year, but humans emit over 29 billion tonnes a year,[ 12] roughly 100 times as much. Clearly, we have a bigger effect. Methane is a more powerful greenhouse gas, but there is 200 times more carbon dioxide than methane, so carbon dioxide is still the most important agent.[ 13] Every other alternative has been looked at and can be ruled out. The only clear-cut relationship is between human-caused carbon dioxide increase and global warming. \* "The climate records since 1995 (or 1998) show cooling." That's simply untrue. The only way to support this argument is to cherry-pick the data.[ 14] Over the short term, there was a slight cooling trend from 1998-2000, but only because 1998 was a record-breaking El Nino year, so the next few years look cooler by comparison (Fig. 4). But since 2002, the overall long-term trend of warming is unequivocal. All of the 16 hottest years ever recorded on a global scale have occurred in the last 20 years. They are (in order of hottest first): 2010, 2009, 1998, 2005, 2003, 2002, 2004, 2006, 2007, 2001, 1997, 2008, 1995, 1999, 1990, and 2000.[ 15] In other words, every year since 2000 has been on the Top Ten hottest years list. The rest of the top 16 include 1995, 1997, 1998, 1999, and 2000. Only 1996 failed to make the list (because of the short-term cooling mentioned already). \* "We had record snows in the winter of 2009-2010, and also in 2010-2011." So what? This is nothing more than the difference between weather (short-term seasonal changes) and climate (the long-term average of weather over decades and centuries and longer). Our local weather tells us nothing about another continent, or the global average; it is only a local effect, determined by short-term atmospheric and oceano-graphic conditions.[ 16] In fact, warmer global temperatures mean more moisture in the atmosphere, which increases the intensity of normal winter snowstorms. In this particular case, the climate change critics forget that the early winter of November-December 2009 was actually very mild and warm, and then only later in January and February did it get cold and snow heavily. That warm spell in early winter helped bring more moisture into the system, so that when cold weather occurred, the snows were worse. In addition, the snows were unusually heavy only in North America; the rest of the world had different weather, and the global climate was warmer than average. Also, the summer of 2010 was the hottest on record, breaking the previous record set in 2009. \* "Carbon dioxide is good for plants, so the world will be better off." Who do they think they're kidding? The Competitive Enterprise Institute (funded by oil and coal companies and conservative foundations[ 17]) has run a series of shockingly stupid ads concluding with the tag line "Carbon dioxide: they call it pollution, we call it life." Anyone who knows the basic science of earth's atmosphere can spot the gross inaccuracies in this ad.[ 18] True, plants take in carbon dioxide that animals exhale, as they have for millions of years. But the whole point of the global warming evidence (as shown from ice cores) is that the delicate natural balance of carbon dioxide has been thrown off balance by our production of too much of it, way in excess of what plants or the oceans can handle. As a consequence, the oceans are warming[ 19, 20] and absorbing excess carbon dioxide making them more acidic. Already we are seeing a shocking decline in coral reefs ("bleaching") and extinctions in many marine ecosystems that can't handle too much of a good thing. Meanwhile, humans are busy cutting down huge areas of temperate and tropical forests, which not only means there are fewer plants to absorb the gas, but the slash and burn practices are releasing more carbon dioxide than plants can keep up with. There is much debate as to whether increased carbon dioxide might help agriculture in some parts of the world, but that has to be measured against the fact that other traditional "breadbasket" regions (such as the American Great Plains) are expected to get too hot to be as productive as they are today. The latest research[ 21] actually shows that increased carbon dioxide inhibits the absorption of nitrogen into plants, so plants (at least those that we depend upon today) are not going to flourish in a greenhouse world. It is difficult to know if those who tell the public otherwise are ignorant of basic atmospheric science and global geochemistry, or if they are being cynically disingenuous. \* "I agree that climate is changing, but I'm skeptical that humans are the main cause, so we shouldn't do anything." This is just fence sitting. A lot of reasonable skeptics deplore the right wing's rejection of the reality of climate change, but still want to be skeptical about the cause. If they want proof, they can examine the huge array of data that points directly to human caused global warming.[ 22] We can directly measure the amount of carbon dioxide humans are producing, and it tracks exactly with the amount of increase in atmospheric carbon dioxide. Through carbon isotope analysis, we can show that this carbon dioxide in the atmosphere is coming directly from our burning of fossil fuels, not from natural sources. We can also measure the drop in oxygen as it combines with the increased carbon levels to produce carbon dioxide. We have satellites in space that are measuring the heat released from the planet and can actually see the atmosphere getting warmer. The most crucial evidence emerged only within the past few years: climate models of the greenhouse effect predict that there should be cooling in the stratosphere (the upper layer of the atmosphere above 10 km or 6 miles in elevation), but warming in the troposphere (the bottom layer below 10 km or 6 miles), and that's exactly what our space probes have measured. Finally, we can rule out any other suspects (see above): solar heat is decreasing since 1940, not increasing, and there are no measurable increases in cosmic rays, methane, volcanic gases, or any other potential cause. Face it -- it's our problem. Why Do People Continue to Question the Reality of Climate Change? Thanks to all the noise and confusion over climate change, the general public has only a vague idea of what the debate is really about, and only about half of Americans think global warming is real or that we are to blame.[ 23] As in the evolution/creationism debate, the scientific community is virtually unanimous on what the data demonstrate about anthropogenic global warming. This has been true for over a decade. When science historian Naomi Oreskes[ 24] surveyed all peer-reviewed papers on climate change published between 1993 and 2003 in the world's leading scientific journal, Science, she found that there were 980 supporting the idea of human-induced global warming and none opposing it. In 2009, Doran and Kendall Zimmerman[ 25] surveyed all the climate scientists who were familiar with the data. They found that 95-99% agreed that global warming is real and human caused. In 2010, the prestigious Proceedings of the National Academy of Sciences published a study that showed that 98% of the scientists who actually do research in climate change are in agreement over anthropogenic global warming.[ 26] Every major scientific organization in the world has endorsed the conclusion of anthropogenic climate change as well. This is a rare degree of agreement within such an independent and cantankerous group as the world's top scientists. This is the same degree of scientific consensus that scientists have achieved over most major ideas, including gravity, evolution, and relativity. These and only a few other topics in science can claim this degree of agreement among nearly all the world's leading scientists, especially among everyone who is close to the scientific data and knows the problem intimately. If it were not such a controversial topic politically, there would be almost no interest in debating it since the evidence is so clear-cut. If the climate science community speaks with one voice (as in the 2007 IPCC report, and every report since then), why is there still any debate at all? The answer has been revealed by a number of investigations by diligent reporters who got past the PR machinery denying global warming, and uncovered the money trail. Originally, there were no real "dissenters" to the idea of global warming by scientists who are actually involved with climate research. Instead, the forces with vested interests in denying global climate change (the energy companies, and the "free-market" advocates) followed the strategy of tobacco companies: create a smokescreen of confusion and prevent the American public from recognizing scientific consensus. As the famous memo[ 27] from the tobacco lobbyists said "Doubt is our product." The denialists generated an anti-science movement entirely out of thin air and PR. The evidence for this PR conspiracy has been well documented in numerous sources. For example, Oreskes and Conway revealed from memos leaked to the press that in April 1998 the right-wing Marshall Institute, SEPP (Fred Seitz's lobby that aids tobacco companies and polluters), and ExxonMobil, met in secret at the American Petroleum Institute's headquarters in Washington, D.C. There they planned a $20 million campaign to get "respected scientists" to cast doubt on climate change, get major PR efforts going, and lobby Congress that global warming isn't real and is not a threat. The right-wing institutes and the energy lobby beat the bushes to find scientists -- any scientists -- who might disagree with the scientific consensus. As investigative journalists and scientists have documented over and over again,[ 28] the denialist conspiracy essentially paid for the testimony of anyone who could be useful to them. The day that the 2007 IPCC report was released (Feb. 2, 2007), the British newspaper The Guardian reported that the conservative American Enterprise Institute (funded largely by oil companies and conservative think tanks) had offered $10,000 plus travel expenses to scientists who would write negatively about the IPCC report.[ 29] In February 2012, leaks of documents from the denialist Heartland Institute revealed that they were trying to influence science education, suppress the work of scientists, and had paid off many prominent climate deniers, such as Anthony Watts, all in an effort to circumvent the scientific consensus by doing an "end run" of PR and political pressure. Other leaks have shown 9 out of 10 major climate deniers are paid by ExxonMobil.[ 30] We are accustomed to hired-gun "experts" paid by lawyers to muddy up the evidence in the case they are fighting, but this is extraordinary -- buying scientists outright to act as shills for organizations trying to deny scientific reality. With this kind of money, however, you can always find a fringe scientist or crank or someone with no relevant credentials who will do what they're paid to do. Fishing around to find anyone with some science background who will agree with you and dispute a scientific consensus is a tactic employed by the creationists to sound "scientific". The NCSE created a satirical "Project Steve,"[ 31] which demonstrated that there were more scientists who accept evolution named "Steve" than the total number of "scientists who dispute evolution". It may generate lots of PR and a smokescreen to confuse the public, but it doesn't change the fact that scientists who actually do research in climate change are unanimous in their insistence that anthropogenic global warming is a real threat. Most scientists I know and respect work very hard for little pay, yet they still cannot be paid to endorse some scientific idea they know to be false. The climate deniers have a lot of other things in common with creationists and other anti-science movements. They too like to quote someone out of context ("quote mining"), finding a short phrase in the work of legitimate scientists that seems to support their position. But when you read the full quote in context, it is obvious that they have used the quote inappropriately. The original author meant something that does not support their goals. The "Climategate scandal" is a classic case of this. It started with a few stolen emails from the Climate Research Unit of the University of East Anglia. If you read the complete text of the actual emails[ 32] and comprehend the scientific shorthand of climate scientists who are talking casually to each other, it is clear that there was no great "conspiracy" or that they were faking data. All six subsequent investigations have cleared Philip Jones and the other scientists of the University of East Anglia of any wrongdoing or conspiracy.[ 33] Even if there had been some conspiracy on the part of these few scientists, there is no reason to believe that the entire climate science community is secretly working together to generate false information and mislead the public. If there's one thing that is clear about science, it's about competition and criticism, not conspiracy and collusion. Most labs are competing with each other, not conspiring together. If one lab publishes a result that is not clearly defensible, other labs will quickly correct it. As James Lawrence Powell wrote: Scientists…show no evidence of being more interested in politics or ideology than the average American. Does it make sense to believe that tens of thousands of scientists would be so deeply and secretly committed to bringing down capitalism and the American way of life that they would spend years beyond their undergraduate degrees working to receive master's and Ph.D. degrees, then go to work in a government laboratory or university, plying the deep oceans, forbidding deserts, icy poles, and torrid jungles, all for far less money than they could have made in industry, all the while biding their time like a Russian sleeper agent in an old spy novel? Scientists tend to be independent and resist authority. That is why you are apt to find them in the laboratory or in the field, as far as possible from the prying eyes of a supervisor. Anyone who believes he could organize thousands of scientists into a conspiracy has never attended a single faculty meeting.[ 34] There are many more traits that the climate deniers share with the creationists and Holocaust deniers and others who distort the truth. They pick on small disagreements between different labs as if scientists can't get their story straight, when in reality there is always a fair amount of give and take between competing labs as they try to get the answer right before the other lab can do so. The key point here is that when all these competing labs around the world have reached a consensus and get the same answer, there is no longer any reason to doubt their common conclusion. The anti-scientists of climate denialism will also point to small errors by individuals in an effort to argue that the entire enterprise cannot be trusted. It is true that scientists are human, and do make mistakes, but the great power of the scientific method is that peer review weeds these out, so that when scientists speak with consensus, there is no doubt that their data are checked carefully Finally, a powerful line of evidence that this is a purely political controversy, rather than a scientific debate, is that the membership lists of the creationists and the climate deniers are highly overlapping. Both anti-scientific dogmas are fed to their overlapping audiences through right-wing media such as Fox News, Glenn Beck, and Rush Limbaugh. Just take a look at the "intelligent-design" cre-ationism website for the Discovery Institute. Most of the daily news items lately have nothing to do with creationism at all, but are focused on climate denial and other right-wing causes.[ 35] If the data about global climate change are indeed valid and robust, any qualified scientist should be able to look at them and see if the prevailing scientific interpretation holds up. Indeed, such a test took place. Starting in 2010, a group led by U.C. Berkeley physicist Richard Muller re-examined all the temperature data from the NOAA, East Anglia Hadley Climate Research Unit, and the Goddard Institute of Space Science sources. Even though Muller started out as a skeptic of the temperature data, and was funded by the Koch brothers and other oil company sources, he carefully checked and re-checked the research himself. When the GOP leaders called him to testify before the House Science and Technology Committee in spring 2011, they were expecting him to discredit the temperature data. Instead, Muller shocked his GOP sponsors by demonstrating his scientific integrity and telling the truth: the temperature increase is real, and the scientists who have demonstrated that the climate is changing are right (Fig. 5). In the fall of 2011, his study was published, and the conclusions were clear: global warming is real, even to a right-wing skeptical scientist. Unlike the hired-gun scientists who play political games, Muller did what a true scientist should do: if the data go against your biases and preconceptions, then do the right thing and admit it -- even if you've been paid by sponsors who want to discredit global warming. Muller is a shining example of a scientist whose integrity and honesty came first, and did not sell out to the highest bidder.[ 36] \* Science and Anti-Science The conclusion is clear: there's science, and then there's the anti-science of global warming denial. As we have seen, there is a nearly unanimous consensus among climate scientists that anthropogenic global warming is real and that we must do something about it. Yet the smokescreen, bluster and lies of the deniers has created enough doubt so that only half of the American public is convinced the problem requires action. Ironically, the U.S. is almost alone in questioning its scientific reality. International polls taken of 33,000 people in 33 nations in 2006 and 2007 show that 90% of their citizens regard climate change as a serious problem[ 37] and 80% realize that humans are the cause of it.[ 38] Just as in the case of creationism, the U.S. is out of step with much of the rest of the world in accepting scientific reality. It is not just the liberals and environmentalists who are taking climate change seriously. Historically conservative institutions (big corporations such as General Electric and many others such as insurance companies and the military) are already planning on how to deal with global warming. Many of my friends high in the oil companies tell me of the efforts by those companies to get into other forms of energy, because they know that cheap oil will be running out soon and that the effects of burning oil will make their business less popular. BP officially stands for "British Petroleum," but in one of their ad campaigns about 5 years ago, it stood for "Beyond Petroleum."[ 39] Although they still spend relatively little of their total budgets on alternative forms of energy, the oil companies still see the handwriting on the wall about the eventual exhaustion of oil -- and they are acting like any company that wants to survive by getting into a new business when the old one is dying. The Pentagon (normally not a left-wing institution) is also making contingency plans for how to fight wars in an era of global climate change, and analyzing what kinds of strategic threats might occur when climate change alters the kinds of enemies we might be fighting, and water becomes a scarce commodity. The New York Times reported[ 40] that in December 2008, the National Defense University outlined plans for military strategy in a greenhouse world. To the Pentagon, the big issue is global chaos and the potential of even nuclear conflict. The world must "prepare for the inevitable effects of abrupt climate change -- which will likely come [the only question is when] regardless of human activity." Insurance companies have no political axe to grind. If anything, they tend to be on the conservative side. They are simply in the business of assessing risk in a realistic fashion so they can accurately gauge their future insurance policies and what to charge for them. Yet they are all investing heavily in research on the disasters and risks posed by climatic change. In 2005, a study commissioned by the re-insurer Swiss Re said, "Climate change will significantly affect the health of humans and ecosystems and these impacts will have economic consequences."[ 41] Some people may still try to deny scientific reality, but big businesses like oil and insurance and conservative institutions like the military cannot afford to be blinded or deluded by ideology. They must plan for the real world that we will be seeing in the next few decades. They do not want to be caught unprepared and harmed by global climatic change when it threatens their survival. Neither can we as a society.

#### Warming causes extinction

**Bushnell 10** [Dennis, chief scientist at the NASA Langley Research Center, MS in mechanical engineering, recipient of the Lawrence A. Sperry Award, AIAA Fluid and Plasma Dynamics Award, the AIAA Dryden Lectureship, and is the recipient of many NASA Medals for outstanding Scientific Achievement and Leadership.) “Conquering Climate Change,” The Futurist, May-June, 2010]

During the Permian extinction, a number of chain reaction events, or “positive feedbacks,” resulted in oxygen-depleted oceans, enabling overgrowth of certain bacteria, producing copious amounts of hydrogen sulfide, making the atmosphere toxic, and decimating the ozone layer, all producing species die-off. The positive feedbacks not yet fully included in the IPCC projections include the release of the massive amounts of fossil methane, some 20 times worse than CO2 as an accelerator of warming, fossil CO2 from the tundra and oceans, reduced oceanic CO2 uptake due to higher temperatures, acidification and algae changes, changes in the earth’s ability to reflect the sun’s light back into space due to loss of glacier ice, changes in land use, and extensive water evaporation (a greenhouse gas) from temperature increases. The additional effects of these feedbacks increase the projections from a 4°C–6°C temperature rise by 2100 to a 10°C–12°C rise, according to some estimates. At those temperatures, beyond 2100, essentially **all the ice would melt and the ocean would rise** by as much as 75 meters, flooding the homes of one-third of the global population. Between now and then, ocean methane hydrate release could cause major tidal waves, and glacier melting could affect major rivers upon which a large percentage of the population depends. We’ll see increases in flooding, storms, **disease, droughts, species extinctions, ocean acidification**, and a litany of other impacts, all as a consequence of man-made climate change. Arctic ice melting, CO2 increases, and ocean warming are all occurring much faster than previous IPCC forecasts, so, as dire as the forecasts sound, they’re actually conservative. Pg. 7-8

### 1ac – Plan Text

#### The United States Federal Government should prohibit the use of offensive cyber operations absent prior Congressional notification

### 1ac – Solvency

#### Plan solves --- establishing prior notifications requirements gives the president political cover and legitimacy for launching more offensive cyber operations --- statutory restrictions are key

**Brecher 12** [Aaron P, J.D. Candidate (May 2013), recipient of Howard B. Coblentz award for outstanding contributions to the Michigan Law Review, University of Michigan Law School, Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations, December, 2012, Michigan Law Review, 111 Mich. L. Rev. 423]

I. The Covert Action and Military Regimes Explored

It is first useful to delineate the detailed statutory requirements for carrying out covert actions, as well as the circumstances under which the military may engage in cyberattacks. To that end, Section I.A briefly summarizes the covert action and military regime procedures. Section I.B then argues that the unique features of cyberspace make applying the law of armed conflict very difficult. Specifically, uncertainty over which cyberattacks constitute a use of force under international law could hamper the military's legal ability to launch cyberattacks under the military authority regime. Section I.C argues that while the covert action framework is not a catchall for every cyberattack that the government may wish to initiate, it does provide a legal basis for a considerable range of offensive actions in cyberspace. Examining the definition of covert action and an important exception to this definition, Section I.C shows that the covert action framework can be used by any number of agencies operating under a single framework, and it adapts well to the increasing blending of military and intelligence functions in the American national security apparatus. A. Comparing the Covert Action and Military Regimes Both military and intelligence activities are subject to complex internal planning and approval procedures. The most relevant difference between the respective legal regimes for purposes of this Note is that covert actions require the president to submit written "findings" to Congress whereas "execute orders" lack similarly rigorous reporting requirements. A "finding" is a written report authorizing a covert action that the president must submit [\*428] to the relevant congressional committees in advance of the operation. n21 An "execute order" is the analogous source of authority for military operations, and can be issued by the president or other high-ranking military officials. n22 1. The Covert Action Regime: Written Findings and Advance Reports to Congressional Intelligence Committees The covert action statute establishes a norm of submitting ex ante written reports to congressional intelligence committees that describe an impending operation, as well as the national security interest that it will serve. The statute dates back to 1991 n23 and was first enacted in response to the Iran-Contra affair. n24 A covert action is an activity designed to influence conditions abroad in situations where the U.S. role is not meant to be publicly acknowledged. n25 Importantly, the definition of covert action excludes, among other things, "traditional diplomatic or military activities or routine support to such activities." n26 It follows from this exclusion that even activities meant to be unacknowledged or potentially unacknowledged are not covert actions if they are traditional military activities. Before initiating a covert action, the president must make a written finding that the action supports an identifiable foreign policy objective and is important to national security. n27 The finding must also specify each U.S. government "department, agency, or entity ... authorized to fund or otherwise participate in any significant way" in the action. n28 "A finding may not authorize any action that would violate the Constitution or any statute ... ." n29 Normally, the finding must be submitted to the members of the congressional intelligence committees soon after the decision is made and before the action is initiated. n30 When the need for secrecy is very great, however, the president has the option of initially submitting the finding only to the Speaker and minority leader of the House, the majority and minority leaders of the Senate, and the chairmen and ranking members of the two intelligence committees. n31 If neither of these reporting procedures is followed, the [\*429] president must make a timely report to the committees, as well as give reasons for the delay. n32 2. The Military Regime: Execute Orders and Limited Congressional Notification Unlike covert actions, military operations do not require written findings. Instead, "execute orders" are the source of authority for initiating such actions. n33 These orders may state an obligation to seek approval from certain officials, even the president or secretary of defense, to conduct certain types of operations. n34 In addition, an execute order, unlike a finding, can function as an ex ante authorization to act if particular circumstances arise. n35 Thus, the orders can, but need not, substantially replicate an internal process similar to that for covert action. n36 As for reporting to Congress, the president has an obligation under the War Powers Resolution to make a written report to the entire Congress within forty-eight hours of introducing U.S. military forces into active hostilities. n37 Notably, though, the Obama Administration has taken an extremely narrow view of what constitutes "hostilities," so that many military activities will likely not be reported under the War Powers Resolution. n38 While there are other statutes in place that require reports of certain military activities to the congressional armed services committees, there is nothing analogous to the covert action requirements, and many activities are exempt from any reporting requirements. n39 In the case of cyberattacks in particular, a recently enacted statute seems to require additional procedures. The National Defense Authorization Act for Fiscal Year 2012, an annual appropriations bill that funds and governs the military, provides that the military may conduct offensive operations in [\*430] cyberspace, subject to presidential approval. n40 It does not appear that presidential approval is required for other cyberoperations that are not cyberattacks, such as cyberexploitations. Moreover, it is unclear whether the presidential-approval requirement means that each specific cyberattack must be approved, as is the case with covert action, or whether there can be an advance presidential authorization to conduct a cyberattack under certain conditions, like with other execute orders. B. The Military and Cyberattacks: An Uncomfortable Fit This Section argues that the legal regime generally governing military action is not always well suited to governing cyberattacks. Cyberattacks' key attributes - remote access, unpredictable effects, and difficulty of attribution - can result in fundamentally different legal problems than conventional weapons attacks. This is because many cyberattacks bear no similarity to military attacks at all. Those that arguably constitute a use of force under international law are even more problematic. A military's essential purpose is national defense. When many think of military operations, they first imagine kinetic strikes: the use of bombs, guns, and other conventional weapons. The emergence of the cyberattack as a viable tool of warfare enables a military with sufficient technological capacity to disable an enemy's communication network, issue false orders, and even impair critical infrastructure, such as by shutting down a power grid, all without firing a shot or even entering the enemy's territory. n41 Although the United States has taken advantage of earlier advances in technology for strategic gain n42 without sustained confusion over the law that governs the use of those tools, activity in the digital world cannot always be neatly analogized to activity in the physical world. Given that the term cyberattack denotes any action to alter, degrade, or destroy data on computer programs or networks, n43 it should be obvious that many cyberattacks bear no resemblance to warlike actions in their effects. For example, almost no one would label an attack that temporarily shuts down service on a private commercial website an act of war. In situations in which the United States has a legitimate national security interest in carrying out such an attack, it is unlikely that the military would play a helpful [\*431] role. n44 The more difficult analytical issues arise when the physical effects of a cyberattack are substantially similar to those of an armed attack under the terms of article 51 of the United Nations ("UN") Charter, which recognizes an inherent right of self-defense in the event of an armed attack on a UN member state. n45 One test to determine whether cyberattacks constitute an armed attack or use of force depends on whether the real-world effects of the operations are equivalent to those of a traditional physical attack, n46 but this effects-based approach can be difficult to apply. n47 Once one shifts to the digital realm, with its features of remote access and relative anonymity, analogizing activities to those that take place in the physical world can be a frustrating exercise. One prominent analogy discussed in the cyberattack literature is the distinction between economic sanctions and a blockade. n48 Economic sanctions are not a use of force under international law. n49 But a blockade, which may have the same effect, is. n50 Unlike sanctions, a blockade involves physically stopping or threatening to physically stop shipments. Applying this analogy to cyberattacks, the debate centers on what type of economic impact might justify either a warlike cyberattack in response or an attack in the physical world. For example, it is unclear whether an attack that manipulates data on a stock exchange, causing a devastating economic impact, constitutes a use of force. n51 Similarly, is a cyberattack that targets a specific industry, in a similar manner to illegal blockades and legal sanctions, a use of force? n52 [\*432] If the issue is whether the military can carry out cyberattacks as a general matter, these line-drawing difficulties are far from merely academic; the United States might wish to carry out a cyberattack without triggering a right for the target to respond with traditional force under international law. Alternatively, the United States may choose to respond to a cyberattack with one of its own. If the initial attack is not an armed attack but the response is a use of force, n53 the American attack could create profound diplomatic and security troubles for the United States. Whichever legal regime is chosen, it should give a policymaker pause to think that a cyberattack, if undertaken by military authorities, could be done with significantly less congressional oversight than a covert action would require. n54 This in turn means less opportunity for persons outside the executive branch to weigh in on the wisdom of the proposed action. The difficulties only increase when the question of whom to target arises. Not only are cyberattacks extremely difficult to trace definitively to their origins, but the wide availability of information technology and the ability to operate from virtually anywhere means that the target (or perpetrator) of a cyberattack could be a state or more problematically, a terrorist organization, criminal group, or an individual. n55 Obviously, these nonstate actors can all operate within the territory of a state. The attribution difficulty means that nonstate actors may be able to operate on a digital plane without detection by either the state in which they operate or a state (like the United States) that wishes to target them. Two important consequences flow from the attribution difficulty in a scenario where the United States carries out a cyberattack in response to a cyberattack by a nonstate actor. First, the United States may be attacking the wrong people. Almost as importantly, even if the original attack can be definitively traced to its source, the state from which the group operated may have nothing to do with the conflict. n56 For example, suppose the United States sustained a cyberattack on its critical infrastructure and wished to [\*433] respond with its own cyberattack, only to discover that the attack originated from a small group of terrorists using computers in an allied country (and that the attack probably passed through computer networks in many allies' territories). n57 If a responsive cyberattack were to affect, for example, access to the internet in those allied countries, n58 the attack may be inappropriate or, in extreme circumstances, may be best done covertly, which would allow the United States to disavow its actions. n59 C. The Covert Action Regime: Some Advantages and a Limitation This Section explains that the covert action framework provides a source of authority for a broader range of cyberattacks than military authorities do, and addresses the advantages of the covert action framework over those of the military regime, as well as an important limitation on covert action. This Section first discusses the advantages of the covert action framework, such as a wider range of covered activities and the ability to avoid the boundary problems arising from the similarity between cyberattacks and cyberexploitations. This Section next argues that the covert action framework provides a single regime under which any appropriate U.S. agency or department could conduct cyberattacks under one set of legal rules. The covert action regime's considerable flexibility also tracks the emerging convergence of military and intelligence functions in twenty-first-century warfare. Finally, this Section addresses the important "traditional military activities" exception to the covert action requirements and the analytical challenge it poses in the case of cyberattacks. The covert action framework offers advantages over those of the military framework when it comes to cyberattacks. At the most basic level, covert action captures a range of activities that the military framework does not. For example, suppose that the government thought it was necessary to alter data in a foreign bank that it believed was being used by a terrorist group. The military could not plausibly construe this action as preparation of any battlefield, and (depending on the bank's location) the bank would be unlikely to be the target of future armed conflict. n60 Indeed, even when there is potential for a future armed conflict, some activities not targeted directly at the state's apparatus may be initiated as covert actions even if the target could be legitimately struck by the military in wartime. For example, some have alleged that in 1982, the United States doctored software that controlled the pumps and valves of a Soviet natural gas pipeline, causing an [\*434] explosion. n61 Aside from these more sensational possibilities, there are many gradations of alteration or disruption of computer programs or networks abroad. Very few of these would involve military purposes, but all would be cyberattacks, and their indirect effects would be difficult to predict. n62 There are reasons beyond the statute's broader range of covered activities to prefer the covert action statute to military legal authority. One significant consideration is the technical similarity between cyberattacks and cyberexploitations. Because these two types of cyberoperations are distinguished primarily by the intent of the actor, n63 prudence might suggest that the covert action statute is a stronger basis on which to initiate cyberexploitations, which could evolve rapidly into cyberattacks. The unpredictable effects of operations over a computer network mean that what starts as espionage conducted by the intelligence apparatus can transform into an activity that changes the targeted program or network. n64 Therefore, the agencies that conduct cyberexploitations would benefit from the greater latitude to conduct cyberattacks that comes with the covert action regime, and use of the covert action regime would also cause agency personnel to err on the side of reporting their activities to the congressional committees. The covert action statute is a flexible regime for operations that lie at the border separating military from intelligence activities. This is so because it provides a single framework that can be used by any agency, n65 and such broad use is well suited to the emerging reality of increased convergence of military and intelligence functions. The definition of covert action is "act-based, not actor-based." n66 Indeed, the covert action framework can be employed even [\*435] when military authority is equally available. For example, even though Osama bin Laden was clearly within the scope of a congressional authorization to use force, n67 U.S. policymakers decided to carry out a kill mission under the covert action framework. n68 Moreover, after the success of the mission, the United States clearly made no effort to conceal its own role. Had the operation failed though, the covert action framework would have offered deniability, as opposed to merely secrecy. Thus, an operation under military legal authority can also be conducted in secret under the covert action framework. Also, by ensuring prior notification to members of Congress, the covert action framework means members would know of a high-risk decision and could express a (nonbinding) view that might inform the decisionmaking. n69 In the case of the bin Laden mission, congressional notification was a politically astute move, regardless of whether the committee members actually expressed substantive thoughts on the operation; the notification gave President Obama a means to try to diffuse blame for a failed mission by noting knowledge (and perhaps tacit approval) of the plan on the part of members of Congress. It also allowed the Central Intelligence Agency ("CIA"), an agency with a great deal of covert action experience, to take the operational lead. n70 The covert action framework is not a panacea for all of the difficulties of applying military authorities to cyberattacks, however. For one thing, a covert action that constitutes a use of force must comply with the law of armed conflict, regardless of whether U.S. military or civilian personnel carry it out. n71 Indeed, the covert action statute itself lays out some important limitations. Most broadly, no covert action can be conducted that "would violate the Constitution or laws of the United States." n72 There is a view that a broad range of deniable cyberattacks may be carried out by the military under the covert action statute's exception for "traditional ... military activities or routine support to such activities[,]" n73 [\*436] thus evading the finding and reporting requirements. n74 But taken to extremes, this perspective would render the covert action statute meaningless. Admittedly, the National Defense Authorization Act for Fiscal Year 2012 does recognize military authority to conduct cyberattacks n75 and the Act's legislative history reveals that Congress meant to affirm that some cyberattacks can be traditional military activities carried out under the same regime that governs kinetic capabilities. n76 Further, the covert action statute's own legislative history suggests that Congress meant to exclude from the reporting requirement activities that were carried out under a military commander or that constituted routine support for a military operation, even if carried out well in advance of anticipated hostilities. n77 However, the argument taken too far recognizes almost no limits on the military's ability to conduct cyberattacks (or many other military operations) free of legislative oversight. In the case of an acknowledged conflict, even if the operation itself is secret, there is indeed a strong basis for claiming the exception. Presumably, in that scenario, either Congress has authorized the hostilities in general, or the president is exercising his constitutional power to defend the nation from attack. n78 But it is not plausible to suggest that routine support for anticipated hostilities (which would fall into the exception) includes penetration of foreign networks that begins years, if not decades, before hostilities. n79 That interpretation is undesirable because it could entirely prevent members of Congress from being informed of ongoing cyberattacks by the United States. n80 Cyberattacks' potential for massive indirect effects that cannot be reliably estimated ex ante makes this a more serious problem than many other secret military operations might pose. The perspective of even a few members of Congress might go far in increasing [\*437] the amount of consideration that would precede such operations. n81 More importantly, as a matter of statutory interpretation, reading the finding and reporting requirements into oblivion in cases of preparation far in advance of conflict seems to fly in the face of the animating purpose of a statute enacted in the wake of executive excess. n82 The covert action statute enables the military, the CIA, the National Security Agency ("NSA"), and any other entity that may plausibly conduct cyberattacks targeted abroad to do so pursuant to the same legal framework of findings and reporting requirements. This unity of legal authority will be useful as the lines between intelligence and military functions continue to blur. n83 The covert action statute serves as a cautious choice when it is difficult to ascertain whether a cyberattack is a use of force or not, or a traditional military activity or not. If a particular cyberattack that was meant to be deniable is not considered a traditional military activity or within the scope of the military's mission, failing to comply with the title 50 requirements would be a statutory violation by the executive. Meeting the threat of terrorist organizations, individuals, or other targets (whether in the physical world or cyberspace) whose locations may prevent traditional kinetic strikes may call for more than can be delivered with cyberexploitations, and less than what the military could do in a recognized conflict. II. The Covert Action Statute as an Independent Domestic Legal Basis for Use of Force If a cyberattack rising to the level of a use of force is carried out against a target not covered by a congressional authorization to use force, the covert action statute would endow the president with greater constitutional legitimacy in ordering the attack than would independent presidential authority alone. To support this claim, Section II.A provides an overview of separation of powers doctrine generally and constitutional [\*438] war powers in particular. Next, Section II.B argues that the covert action statute can plausibly be read to provide congressional support for certain uses of force, based on its text and the executive's history of interpreting statutes originally meant to limit executive authority as affirmations of presidential power. In addition, the textual limits in the covert action statute are consistent with those necessary for Congress to delegate to the president certain powers. A. Separation of Powers and Constitutional War Powers It has become axiomatic of American constitutional doctrine that presidential decisions gain greater constitutional legitimacy when they are carried out with Congress's approval. Though the president has tremendous freedom to act autonomously when conducting foreign affairs, the concerted action of both elected branches strengthens the presumption that the presidential policy is lawful. It is unclear, however, what the respective powers of either branch are when the president and Congress actively oppose one another, or when the president acts in the face of congressional silence. n84 In the exercise of constitutional war powers, it seems clear that the president can order the responsive use of force, but becomes less so when faced with the question of whether the president may initiate an armed conflict. Congress is probably empowered to place substantive limits on the scope of hostilities and the initiation of conflicts.

#### And, the plan facilitates counterstrike operations and attacks that would bolster cyber deterrence

**Kesan, prof of law, 12** [Jay P. & Carol M., \*Professor, H. Ross & Helen Workman Research Scholar, and Director of the Program in Intellectual Property & Technology Law, University of Illinois College of Law, \*\* Research Fellow, University of Illinois College of Law, Mitigative Counterstriking: Self-defense and deterrence in cyberspace, Spring, 2012, Harvard Journal of Law & Technology, 25 Harv. J. Law & Tec 415]

Ideas, computers, and intellectual property have become extremely important in the modern Information Age. The Internet has become so essential to modern life that several countries have declared Internet access to be a fundamental right. n4 But the importance of technology in the Information Age comes with a downside: the vulnerability of modern society and the global economy to minimally funded cyberat-tacks from remote corners of the world. In the 1950s, American school children were taught to "duck and cover" in the event of an atomic bomb explosion. n5 A popular cautionary film from 1951 warns that a flash of light brighter than the sun accompanies such an explosion and that the flash could cause an injury [\*418] more painful than a terrible sunburn. n6 The film, however, asserts that a child who "ducks and covers" will be more protected from the aftermath of nuclear detonation than otherwise. n7 Fortunately, no American city has ever experienced a nuclear attack, so no child has ever learned the hard way that a newspaper or a coat affords little protection against the heat from the detonation of an atomic bomb. The nuclear capabilities on both sides of the Cold War served as a deterrent against nuclear strikes and helped avoid an all-out nuclear conflict. n8 "Duck and cover," however, had no deterrent effect. The Cold War ended about two decades ago, but new threats have emerged. The conflicts have shifted, the battlefields have morphed, and technologies that were not even dreamed of in 1951 now form the foundations for our everyday lives. The Internet, a technology partially developed to facilitate communication in the event of a nuclear attack, n9 changed the world forever. It is quite possible that future wars will be fought primarily in cyberspace, with the lines between civilian and military becoming increasingly blurred. n10 Instead of "duck and cover," computer users must now "scan, firewall, and patch." n11 However, like "duck and cover," purely passive defenses have questionable utility in the face of zero-day vulnerabilities n12 and sophisticated cyberweapons like the Stuxnet worm. n13 Likewise, law enforcement [\*419] and judicial action against malicious cyber intrusions currently do not present enough of a practical threat to deter potential attackers. n14 The weaknesses of the current reliance on employing passive defense methods and seeking help from the authorities -- who are both technologically and legally ill-equipped to seek justice for victims -- present a difficult situation. Considering how modern society relies on the Internet and networked services, there is an urgent need for proactive policy to help insulate critical services from damage as well as mitigate harm from potential attacks. For a number of reasons explored below, we argue that, in some circumstances, permitting mitigative counterstrikes in response to cyberattacks would be more optimal. There is an urgent need for dialog on this topic as the development of technology has outpaced the law in this area. n15 While progress has been made in the form of executive orders addressing cybersecurity, n16 the proposed Cyber Intelligence Sharing and Protection Act ("CISPA"), n17 and cybersecurity provisions of the National Defense Authorization Act ("NDAA"), n18 these measures do not go far enough. New discussions and analyses are needed to ensure that responsive actions can be grounded in sound policy. Because of the inadequacy in current means to address cyber threats, this Article examines other possible methods to deter cyberattacks, specifically the use of cyber counterstrikes as part of a model of active defense. Active defense involves (1) detecting an intrusion, (2) tracing the intruder, and (3) some form of cyber counterstrike. n19 [\*420] Though intrusion detection and tracing are essential, counterstriking is key to enhancing the deterrent effects of active defense. At its core, cyber counterstriking is about two things: (1) deterring attackers and (2) ensuring that attacked parties are not deprived of the inherent right to defend themselves and their property. There are many views of deterrence, but deterrence is generally accomplished by the threat of some combination of the following elements: (1) punishing attackers by inflicting unacceptable costs, or (2) preventing attackers from succeeding in their attacks. n20 These two elements of deterrence have led us to apply the terms "retributive counterstriking" and "mitigative counterstriking," respectively, to the counterstriking component of active defense. In the cyber context, a "counterstrike" can involve any number of actions. As discussed in Part III.B, a counterstrike can involve the target executing its own Denial of Service ("DoS") attack against the attacker (for example, by redirecting the attacker's packets back at the attacker to knock the attacker's systems offline), n21 infecting the attacker's system with a virus or worm to permit the victim to take control, or a number of other options. The technologies available to execute counterstrikes are generally the same ones used in initial attacks; as we examine in more detail below, some of these currently available technologies permit an attack to be traced back to its origin -- with varying degrees of accuracy. Furthermore, there is now evidence that "cyber contractors" exist as part of what some have termed the new "military digital complex," whose work involves creating offensive cyber technologies that can have applications in the context of counterstriking. n22 The goal of a counterstrike can vary, from punishing the attacker to simply mitigating the harm to the target. We call the former "retributive counterstriking"; this type should remain under the sole control [\*421] of the military, as a national security matter relating to sensitive domestic and international legal issues. We define "mitigative counterstriking" as taking active efforts to mitigate harm to a targeted system, in a manner strictly limited to the amount of force necessary to protect the victim from further damage. We recognize there may be overlap between retributive and mitigative counterstriking, as the latter could potentially result in damage to the attacker's system. How-ever, the goal of mitigative counterstriking must be to mitigate damage from a current and immediate threat. We argue that whatever measures are deployed must be justifiable under a mitigation frame-work. Cyber counterstrikes, however, are currently controversial, and it can be difficult under the current framework to differentiate between "hack back" vigilantism and legitimate exercises of a right to self-help. n23 Our proposal in this area is both modest and bold. Modest, because while we also discuss active defense as a broad topic, our primary focus is on mitigative counterstriking as a discrete subcategory of active defense activities. Bold, because we advocate for a significant shift from the prevailing approach to cyber intrusions. In recommending a new regime, we have chosen to focus on mitigative counterstriking as a starting point for two reasons. First, it is likely to be more effective than passive defense at accomplishing the goal of deterrence by denial. Second, a mitigative counterstriking regime would endow network administrators with the right to actively defend their property, thereby legitimizing the right to self-defense in the cyber realm. The current regime creates an unconscionable situation where parties are expected to give up the right to actively defend themselves against threats and instead rely on passive defense measures that may prove ineffective. Parties are left with no practical recourse through criminal enforcement or civil litigation for a number of reasons we discuss below. Currently, the biggest barrier to defending against cyberattacks is the lack of a legal method to respond to cyberattacks that also has a credible deterrent effect on potential attackers. We posit that accurate and consistent use of mitigative counterstrikes could serve to deter cyberattacks against sensitive systems such as hospitals, **government defense systems, and** critical national infrastructure ("CNI"), and argue that implementing a regime to permit these sorts of counterattacks should be a priority. There is some evidence that the private sector has [\*422] been tacitly utilizing this sort of technology to protect their systems, n24 effectively acting as cyber vigilantes under the current regime. Such behavior is at best legally ambiguous, and at worst illegal. Currently, the idea of mitigative counterstriking is treated like the proverbial elephant in the room, with legal commentators largely ignoring it. n25 After careful analysis, we conclude that this neglect is due to the lack of an analytical framework distinguishing between the perceived vigilantism of retributive counterstriking and the employment of self-help through mitigative counterstriking. We thus propose a new policy and legal regime to address the threat of cyberattacks using active defense and mitigative counterstriking. There is a grave need to standardize approaches to mitigative counterstrikes, n26 and we must determine when the use of mitigative counterstrikes is appropriate, as well as who should be permitted to conduct mitigative counterstrikes. We recognize that counterstrikes of any variety can raise a number of legal and diplomatic concerns. While additional analysis and technological development may be desirable before implementing a broad self-defense regime, we argue that implementing mitigative counterstriking capabilities to protect CNI should be the first priority. Cyberattacks significantly affect private parties, including owners of CNI, n27 so it is important to legitimize active defense and mitigative counterstriking approaches in order to afford these private parties more protection against these threats.

#### Clarifying the legal framework on cyber operations is key to a credible cyber deterrence strategy

**Goldsmith, prof of law @ Harvard, 12** [Jack, Henry L. Shattuck Professor @ Harvard Law School, where he teaches and writes about national security law, presidential power, cybersecurity, international law, internet law, foreign relations law, and conflict of laws, served as Assistant Attorney General, Office of Legal Counsel from 2003–2004, and Special Counsel to the Department of Defense from 2002–2003, member of the Hoover Institution Task Force on National Security and Law, 10/15, “The Significance of Panetta’s Cyber Speech and the Persistent Difficulty of Deterring Cyberattacks,” Lawfare, <http://www.lawfareblog.com/2012/10/the-significance-of-panettas-cyber-speech-and-the-persistent-difficulty-of-deterring-cyberattacks/>]

Secretary of Defense Leon Panetta’s speech last week on cyber is more significant than has been reported. Most of the coverage focused on Panetta’s grave warnings about cyber threats facing the nation, but the speech’s real significance, I think, concerns DOD’s evolving deterrence posture. (The speech has other significant elements, but I focus here on deterrence.) Panetta had two main messages related to deterrence. First, because the USG’s attribution skills have improved, “[p]otential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America.” Second, “If we detect an imminent threat of attack that will cause significant, physical destruction in the United States or kill American citizens,” then on the orders of the President, DOD can “conduct effective operations to counter threats to our national interests in cyberspace.” (This second point echoes earlier USG statements, including one made earlier this month by DRNSA Keith Alexander, who said, somewhat less cautiously than Panetta, that DOD must be able to “stop [an attack] before it happens. . . . Part of our defense has to consider offensive measures like that to stop it from happening.”) Here is what I think is significant about Panetta’s speech.¶ First, DOD has previously said that it is trying to improve is attribution capabilities, and in conversation officials have noted some success. Panetta goes further, saying concretely and definitively that DOD has “made significant advances in solving” the attribution problem, presumably through a combination of tracing back the source of a cyber attack and identifying the attacker through “behavior-based algorithms” and human and electronic intelligence. Panetta does not tell us how good or fast DOD is at attribution, and he may to some unknown degree be puffing. Nonetheless, this is a potentially big deal for cyber deterrence. Second, Panetta was more aggressive than DOD has been in the past about the trigger for a self-defensive cyberattack by the United States. Previously, DOD has stated that adversaries would face a “grave risk” if they launched a “crippling” or “significant” cyberattack on the homeland. Panetta’s speech changes this posture in two ways. He is less definitive about the high threshold of a “significant” or “crippling” attack as a trigger for a USG response, and indeed implies that the threshold is (or can be) lower. And more importantly, he makes plain that the DOD has the capabilities and desire to engage in a preemptive attacks against imminent cyber threats. This possibility has been hinted at before (most recently, in Alexander’s comment above and in Harold Koh’s NSA Cyber Command legal conference speech last month). But Panetta was more definitive about DOD’s capacity and desire to engage in such attacks. (Herb Lin, chief scientist at the National Research Council’s Computer Science and Telecommunications Board, noted to me that Panetta referred to the need to “take action” with “effective operations” against imminent cyberthreats, and pointedly did not state that such actions or operations would necessarily involve cyber means or cyber targets. This is consistent with DOD’s prior claims that it would use “cyber and/or kinetic capabilities” to redress large-scale cyberattacks.) Panetta was ambiguous, however, about whether DOD currently has the authorities to engage in such preemptive attacks (by cyber means or other means) in the face of cyber threats. He said that “we need to have the option to take action against those who would attack us to defend this nation when directed by the president” (emphasis added), and he emphasized DOD capabilities while several times calling for more DOD authorities. I have previously criticized DOD’s announced deterrence policy, so I should say that Panetta’s speech takes steps in the right direction. Panetta noted improvement in attribution (which is potentially huge), he warned that the USG would hold attackers responsible, he appeared to eliminate unjustifiably super-high thresholds for a self-defensive responses to cyberattacks, and he noted DOD’s capacity and need for preemptive attacks in the face of imminent cyberattacks. That said, Panetta made these points in an after-dinner speech, not an official declaratory policy. And many questions remain, such as: How much better (in terms of speed and accuracy) is our attribution capacity? How do adversaries know whether the USG’s supposed attribution advances are not a bluff? What exactly is the threshold for a self-defensive offensive operation in response to a cyber attack? What counts as an imminent threat of cyberattack that would warrant a preemptive attack by the USG? The effectiveness of any deterrence posture depends on the answers to these (and related) questions, and (very importantly) on our adversaries’ beliefs about the answers to these questions. Ambiguity about the answers might over-deter (as vague criminal law often does), but it might also under-deter (because the adversary misperceives where the red lines are). The effectiveness of deterrencealsodepends, crucially, on the credibility of our threat to attack in the face of actual or imminent attacks. Several obstacles prevent our threats from being entirely credible. Panetta’s speech and other DODpronouncements, as well as news reports, indicate that DOD does not think it has adequate legal authorities to engage in offensive operations related to defense, and that USG lawyers are currently putting up affirmative obstacles to such operations. To the extent that the USG is and appears to be legally constrained from acting as it says it needs to, its threats to act are not credible. In addition, even if our attribution skills are fast and accurate (which they won’t always be), any responsive cyberattack that has public effects must be accompanied by public evidence that the attack was warranted – something very hard to do when attribution is based on sophisticated and fragile intelligence tools. To the extent the USG cannot prove attribution publicly, its threats of a cyberattack are diminished. This point implies that self-defensive cyberattacks are (all things equal) more likely to be unattributable than attributable. But that conclusion in turn presents two problems. First, how to convince the adversary that we have hit it in response to a cyberattack when we cannot take public credit for the attack? (This is potentially difficult, not impossible; Iran certainly suspected the USG even before the public revelations about Stuxnet/Olympic Games.)\* Second, an unattributable self-defensive cyberattack is more likely in response to a relative small actual or threatened cyberattack on the nation. If we suffer a crippling blow, we will need to respond with large public fire, in cyber or kinetic space, or both. The worry is that the difficulties of public proof of attribution will slow the needed public response, or weaken it, or make it seem less legitimate ex post – all of which weakens the credibility of a responsive attack ex ante, and thus weakens deterrence. Finally, some thoughts about Stuxnet/Olympic Games, the cyber operation(s) against the Iranian nuclear facilities. While many in the USG are no doubt genuinely angry that the USG hand in Stuxnet was revealed, this revelation probably has the happy effect of **enhancing U.S. cyber deterrence**. For it demonstrates that the USG has sophisticated cyberweapons that – despite legal and other obstacles – it is willing to deploy, even in a preemptive fashion. For many reasons that I lack time explain (having to do with the nature of the Iranian threat, which did not present an attribution problem, and the nature of the cyber attack on the Iranian facilities), I think the legal and policy hurdles to the Iranian operation **were less significant than ones that would arise with a self-defensive USG attack** in response to an actual or threatened cyberattack.  Nonetheless, the Stuxnet/Olympic Games revelations probably **enhance U.S. cyber deterrence overall**.  (And no, the Iranian cyberattacks [in the news yesterday](http://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html), which reportedly inflicted “modest damage,” do not by themselves belie this claim.)

#### Only deterrence can solve future cyber attacks

**Kramer 12** [Franklin D. Kramer is a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He served as the assistant secretary of defense for international security affairs from 1996 to 2001. Stuart H. Starr is also a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He concurrently serves as the president of the Barcroft Research Institute. Larry Wentz is a senior research fellow in the Center for Technology and National Security Policy at the National Defense University., “Cyberpower and National Security”, p. 318]

No cyber deterrence strategy can hope to be airtight to prevent all minor attacks.However, a strategy can increase the chances that major cyber attacks can be prevented;this could protect the UnitedStates and its allies not only from a single major attack but also from serial cyber aggressions and resulting damage**.** A worthwhile goal of a cyber deterrence strategy would be to transform medium-sized attacks into low-probability eventsand to provide practically 100 percent deterrence of major attacks. A cyber deterrence strategycould contribute to other key defense activities and goals, includingassurance of allies, dissuasion, and readiness to defeat adversaries in the event of actual combat. The goal of dissuading adversaries is crucially important. Thus far, theUnited Stateshas not been noticeably forceful in stating its intentions to deter major cyber attacksand, if necessary, to respond to them with decisive force employing multiple instruments of power. Meanwhile,several countries and terrorist groups are reportedly developing cyber attack capabilities.Dissuasion of such activities is not an easy task:it requires investment in technical capabilities as well as building an internal consensus to employ these capabilities.If some of these actors can be dissuaded from entering into cyber competition with the United States and its allies, the dangers of actual cyber aggression will diminish. How would a cyber deterrence strategy operate,and how can its potential effectiveness be judged?Deterrence depends on the capacity of the UnitedStatesto project an image of resolve, willpower, and capability in sufficient strengthto convince a potential adversary to refrain from activities that threaten U.S. and allied interests. As recent experience shows,deterrence can be especially difficult in the face of adversaries who are inclined to challenge the United States and otherwise take dangerous risks. In cases of failure, deterrence might well have been sound in theory but not carried out effectively enough to work.The aggressions ofSaddamHussein, SlobodanMilosevic,and al Qaeda might not have been carried out had these actors been convinced thatthe United States would respond with massive military force**.** These aggressions resulted because of a failure to communicate U.S. willpower and resolve, not because the attackers were wholly oblivious to any sense of restraint or self-preservation, nor because the logic of deterrence had lost its relevance.

#### Defensive measures against cyber attacks are ineffective and can’t solve

**Krepinevich, PhD @ Harvard, 12** [Andrew, PhD & MPA at Harvard, West Point graduate, served 25 years in the Army, worked in the DOD Office of Net Assessment for 3 defense secretaries, president of the Center for Strategic and Budgetary Assessments, http://www.csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/, pp 45-47, nrb]

As the **cyber competition appears to favor the offense**, and potentially by a considerable margin, even a cyber defense **with access to an unlimited budget** could not eliminate the possibility of intrusions, as new vulnerabilities are constantly being identified. General Alexander summed up the competition well when he stated “In cyberspace the only ‘perfect’ defense is the static one: to disconnect [from networks] and thereby forfeit the cyber realm and its economic and social benefits to one’s adversaries.”158 Mounting a serious defense against a major cyber attack would likely require, at a minimum, intrusion detection and intrusion prevention on a nationwide scale. This seems unfeasible, however, as the networks that comprise the Internet are typically not segmented along national boundaries. Put another way, there are no national borders when it comes to the cyber world. Even if there were and the United States could close its virtual cyber borders to traffic coming in from the outside, the attack could be generated from within its borders (i.e., originate within the United States using the Internet or insider access), and there is as of yet **no effective means to prevent such an attack from occurring**.159