# Aff Cards – Texas

# 1AC

### 1ac – Cyber Attacks Adv – UK

**Scenario 1 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%2BDai-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%2C%2BGeography/Towns%2C%2BCities%2C%2BCounties/New%2BYork%2BCity). 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.

**Nuclear power is sustainable in the long-term --- but, natural gas fills-in for any nuclear power decline**

David 8/4/13 [Javier E., US natgas boom sucks nuclear power into downdraft, http://www.cnbc.com/id/100935682, nrb]

Cheap and abundant natural gas is eating away at nuclear energy's traditional role in generating electricity in a way that has made the sector's prospects increasingly precarious, according to the institute and others. Even as the U.S. renews its push for climate change policies that could give nuclear a new lease on life, some observers are doubtful much can be done to arrest the sector's spiral.

Nobody 'foresaw what was going to happen'

"The shale industry in the U.S. and what's happening in terms of production and development…has taken the world by surprise," said Margaret Hill, co-chair of the environmental practice at law firm Blank Rome. "I don't think anybody foresaw what was going to happen."

Hill said the long-term prospects of the nuclear industry are uncertain at best, especially in a sector operating in the shadow of Japan's 2011 nuclear disaster. "The economics and the environment are driving development and the use of shale oll and gas to provide power," she said.

Furthermore, "the economics of nuclear plants are very difficult to maintain, and very costly to do so," she said. Hill pointed to issues that have for years dogged Yucca Mountain's nuclear facility in Las Vegas, Nevada, the site of vociferous environmental opposition.

For certain, some companies are pressing ahead with building a new plant: according to the Nuclear Energy Institute (NEI), companies have broken ground on five new plants since 2007, and 14 more are in the exploratory phases.

[Exelon](http://data.cnbc.com/quotes/EXC), the country's largest nuclear power operator, said this week that [it isn't planning to shutter any of its nuclear plants](http://www.reuters.com/article/2013/07/31/utilities-exelon-nuclear-idUSL1N0G11H220130731), even as the company acknowledged the competitive threat posed by natural gas. The fuel source has slowly eroded the dominance of nuclear power and coal as inputs for generating electricity.

One industry source who asked not to be identified said that as more companies move to use natgas, its price will shoot up. That could create an opening for nuclear plants to reassert their value, he said.

"Every time you're in a feast period, you think the feast is going to last forever," he said, warning that prices won't remain low forever, especially if the U.S. moves to export natural gas. "As consumption increases, prices will go up."

Meanwhile, there are still about 100 active nuclear plants in the U.S. that employ more than 100,000 workers, according to NEI data. Those plants generate "substantial domestic economic value in electricity sales and revenue—$40 billion to $50 billion each year," NEI said.

#### Natural gas displaces renewables and make runaway warming inevitable

Romm 11—Senior Fellow @ American Progress [Dr. Joe Romm (Ph.D. in physics from MIT), “IEA’s “Golden Age of Gas Scenario” Leads to More Than 6°F Warming and Out-of-Control Climate Change,” Think Progress, Jun 7, 2011 at 12:50 pm, pg. http://thinkprogress.org/climate/2011/06/07/238578/iea-golden-age-of-natural-gas-scenario-warming-climate-change/

The International Energy Agency has just issued a special report titled, “Are We Entering a Golden Age of Gas?”  The answer to that question is “yes” only if you are a natural gas producer who doesn’t care much about humanity.  For the rest of us, the report makes clear natural gas by itself does nothing to avert catastrophic climate change.  Quite the reverse.

The UK Guardian‘s story put it well:

Natural gas is not the “panacea” to solve climate change that fossil fuel industry lobbyists have been claiming, according to new research from the International Energy Agency.

Reliance on gas would lead the world to a 3.5C temperature rise, according to the IEA. At such a level, global warming could run out of control, deserts would take over in southern Africa, Australia and the western US, and sea level rises could engulf small island states.

Not exactly a champagne moment.

UPDATE:  I’ve added a featured comment (and link) by Tyler Hamilton, business columnist at The Toronto Star.

Ironically, the IEA report is built around what it calls “The Golden Age of Gas Scenario (GAS Scenario)” — except, of course,  the acronym for “Golden Age of Gas Scenario” should be GAG Scenario not GAS Scenario.  And GAG is exactly what the planet would do if the dash to gas becomes our primary energy policy, rather than a high and rising price for CO2.

The reason is clear.  Absent a high CO2 price, gas displaces as much low-carbon electricity as it does high-carbon coal.  That was precisely the point made by Nobuo Tanaka, executive director of the IEA, at a London press conference:

“While natural gas is the cleanest fossil fuel, it is still a fossil fuel. Its increased use could muscle out low-carbon fuels such as renewables and nuclear, particularly in the wake of Fukushima. An expansion of gas use alone is no panacea for climate change.”

The Guardian notes, “The IEA also warned that gas could push out renewables, if governments come under pressure to reduce renewables subsidies and opt for gas instead, as gas companies have been urging.

The report itself makes clear that in the GAG scenario:

Natural gas displaces coal and to a lesser extent oil, driving down emissions, but it also displaces some nuclear power, pushing up emissions…. This puts emissions on a long-term trajectory consistent with stabilising the concentration of greenhouse gases in the atmosphere at around 650 ppm, suggesting a long-term temperature rise of over 3.5°C.

Note that the GAG scenario assumes that not only does oil production peak in 2020 — but so does coal!

Yet we still get 650 ppm and more than 6°F warming even with that incredibly optimistic assumption — and with the additional optimistic assumption that industrial coal consumption (and CO2 emissions) only rises 22% from 2008 to 2020.  And assuming we don’t have a lot of that gas leaking into the air (see New study questions shale gas as a bridge fuel and Is natural gas cleaner than coal?).

Oh yes, and then we have the assumption that we can actually stabilize at 650 ppm.  In fact, once we go above 450 ppm, the carbon-cycle feedbacks are going to accelerate and shoot us to much higher levels of greenhouse gas concentrations  — see “NSIDC bombshell: Thawing permafrost feedback will turn Arctic from carbon sink to source in the 2020s, releasing 100 billion tons of carbon by 2100.”

In any case, 650 ppm is probably sufficient to lead to the ultimate disintegration of the Greenland ice sheet and many tens of feet of sea level rise — see New study of Greenland under “more realistic forcings” concludes “collapse of the ice-sheet was found to occur between 400 and 560 ppm” of CO2.  That SLR is likely to kick in sooner rather than later — see JPL bombshell: Polar ice sheet mass loss is speeding up, on pace for 1 foot sea level rise by 2050.

#### Fugitive methane emissions increases warming—the transition to renewables will be too late

Chameides 12—Professor of the Environment Earth & Ocean Sciences @ Duke University [Bill Chameides (Fellow of the American Geophysical Union and Chief scientist @ Environmental Defense), “Natural Gas: A Bridge to a Low-Carbon Future or Not?,” Huffington Post, 7/20/2012, http://www.huffingtonpost.com/bill-chameides/-natural-gas-a-bridge-to\_b\_1690857.html]

Chapter 2. Climate Threatened by Sinister Methane Leakage

Interestingly enough, with the advent of fracking for shale gas and the consequent jump in estimates of natural gas resources (see here and here), the use of natural gas as a transition fuel actually seems to be feasible. Good news for the climate, one might conclude.

Not really, scientists like Bob Howarth of Cornell University, protested. Why? Before answering that, you need to know a couple of background facts. First, methane, the major component of natural gas, is itself a very potent greenhouse gas -- some 21 times more effective a warmer than CO2 on a 100-year basis. And second, when we use natural gas, there are inevitably fugitive emissions, leaks during mining, transport, and consumption that allow methane to escape into the atmosphere where it can do its global warming thing. What Howarth argued in a much-debated paper published last year is that the leakage rates are so high that, contrary to conventional wisdom, transitioning from coal to natural gas would actually lead to more global warming than just sticking with coal, even though coal is the most carbon-intensive of the fossil fuels.

Since the paper's publication, other investigators and studies have weighed in on the matter, including RealClimate's Gavin Smith; the Council on Foreign Relations' Michael Levi; Ramón Alvarez of Environmental Defense Fund and co-authors; and another Cornell scientist, Lawrence Cathles. But a definitive conclusion has been elusive because the actual magnitude of these fugitive emissions remains very poorly defined.

Chapter 3. Methane Leakage Exonerated?

The upshot of the debate about the importance of fugitive emissions has led to a general consensus that we need a very thorough investigation into the leakage issue. In short we need to first pin down the magnitude of fugitive emissions and then cut them down by locking the methane up. (See here and here.)

But now Cornell's Cathles argues in a new paper published last week in the journal Geochemistry Geophysics Geosystems that fugitive emissions may not be that sinister after all. Or at least not if natural gas is indeed used as a bridge fuel that is first phased in as coal and some oil are phased out and then eventually is itself phased out in favor of carbon-free energy sources.

Assuming periods of 50, 100, and 200 years to make the transition from coal to natural gas to renewables, Cathles's model calculations indicate that the long-term (i.e., multiple decades to century timescales) climate impacts of the fugitive methane emissions are relatively small. The reason is that methane has a relatively short lifetime in the atmosphere -- about 12 years. And so once natural gas is no longer used as a fuel, the methane in the atmosphere from fugitive emissions will be removed from the atmosphere and so the warming from those emissions will be essentially gone. CO2 on the other hand is long-lived and so, Cathles argues, over the long term using natural gas instead of coal or oil is preferable because less CO2 will have been emitted in that scenario. Well, it is preferable provided we use natural gas as a transition fuel that eventually gives way to even cleaner renewables and/or nuclear. And then there's the issue of the short-term climate effects from fugitive emissions.

Chapter 4. The Question of the Short Term

Cathles's point about the transient effects of methane fugitive emissions is well taken. But there is a potential catch and it relates to short-term climate effects. During the transition period, when fugitive methane from using natural gas would build up in the atmosphere, there is a possibility, depending upon the magnitude of the methane emissions, that we would experience more short-term warming than if we were to have stuck with coal and oil. We might think of this as the transient version of the Howarth argument.

Now, as long as the fugitive emissions are small or the Earth system is "reversible," the transient Howarth scenario does not seem all that worrisome. But what if the emissions are large? And what if the disturbances from global warming are not reversible? Then we would have a problem. The transition to natural gas would lead to more warming for a period of time until natural gas is phased out and the excess methane is removed from the atmosphere. With the exit of the excess methane, the extra warming would also go away. Cathles seems to argue that all would be well:

"Even when methane leakage is so large (L = 10% of consumption) that substituting gas for coal and oil increases global warming in the short term, the benefit of gas substitution returns in the long term."

But it is not all that obvious that the impacts from global warming are reversible. If fragile ecosystems like coral reefs are decimated by a decade or two of extra methane-induced warming, can we be sure that they will recover once the methane is flushed from the atmosphere? Probably not.

Now for this to be a concern, fugitive emissions would need to be large -- about 10 percent or more. That's' a very remote possibility. Even so, Cathles's interesting results notwithstanding, I don't think we can ignore fugitive emissions and just assume they're too small to care about. And in any event from an economic and environmental point of view, the less of that stuff the better.

Epilogue

Cathles would agree. In fact he concludes his paper with the policy recommendation that leakage of methane related to natural gas production, transport, and use be reduced to about 1 percent. Let's call it the one-percent solution.

**US and global emissions are decreasing now --- shift to fossil fuels reverses the trend**

Willis 10/31/13 [Ben, Renewable energy transition behind ‘remarkable’ slowdown in CO2 emissions, http://www.pv-tech.org/news/renewable\_energy\_transition\_behind\_remarkable\_slowdown\_in\_co2\_emissions, nrb]

The increase in global carbon dioxide emissions slowed last year because of a shift towards renewable energy usage, a major new study claims.

A report by the Netherlands Environmental Assessment Agency and the European Commission's Joint Research Centre found that in 2012 the increase in global emissions slowed to 1.1%.

This was less than half the average annual increase over the past decade of 2.9% and, significantly, appeared to suggest a break in the link between global economic growth and increasing emissions. Global GDP grew by 2.5% last year.

The report said this “remarkable” trend was most pronounced in the world’s three worst emitting areas – China, the US and Europe. China’s emissions increased by 3% last year, compared to an average of 10% over the past decade, while the US and EU emissions decreased by 4% and 1.6% respectively.

The study ascribed this trend to a shift to less fossil fuel-intensive activities and a greater deployment of renewable energy, which accounted for 2.4% of the global energy mix in 2012.

The study said the trend could herald a “permanent” slowdown in CO2 emissions as long as these three countries and regions continue to cut total energy use and increase the amount of renewable energy they use.

**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

**Scenario 2 is the Economy**

**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

**Blackouts will destroy the US economy**

Jacobs 12 [Deborah L., India-Style Blackout Could Strike The U.S., http://www.forbes.com/sites/deborahljacobs/2012/08/06/india-style-blackout-could-strike-the-u-s/, nrb]

The U.S. is one of the most developed nations in the world. Our day-to-day interactions are guided by technologies and innovations that rely upon the power grid. But as we continue to develop technological mastery, our power grid is aging and fragile, and its susceptibility to outages means our way of life could break down in an instant.

Unlike generations past, our lives and businesses are now connected through a vast network of computers and data centers that consume enormous amounts of electricity. Our homes are bigger, with more luxuries and appliances than ever. We count on power in ways our parents couldn’t imagine.

Power quality is the measure of reliable power in our homes and businesses, and it has been declining steadily since 1990. During this time, demand for power has increased by 25%, but the infrastructure needed to transmit power to homes has increased by a mere 7%. We have become a digital society, but are burdened with an analog power grid—one that is inefficient and susceptible to weather, surging demand, and even terrorist attack.

Each outage comes at a cost; the average cost of a one-second outage among industrial and digital firms is about $1,477. That means the U.S. economy loses between $104 billion and $164 billion each year to power outages. Losses like that affect all of us. An outage lasting days, as in India, would represent hundreds of billions of dollars lost, taxing our already fragile economy.

Second internal link is public confidence --- cyber attacks will devastate the financial system

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 58-59, nrb]

The Financial System

Another key part of the U.S. critical infrastructure that is heavily dependent upon computer systems and networks is the financial system. Could the U.S. and (by extension) the global financial system be subjected to a catastrophic cyber attack? The stakes involved and the risks associated with the compromise of a financial computer system or network are potentially profound. Even more than other parts of the critical infrastructure, like the power grid and the transportation system (e.g., air traffic control systems and train routing systems), the financial system’s effective functioning depends upon the confidence of people. One Wall Street CEO summed it up well: “It is confidence in the data, not the gold bullion in the basement of the New York Fed, that makes the world financial markets work.”207

Were people to lose confidence in the financial system’s ability to keep accurate track of their funds, prevent their funds from being siphoned off, or engage in unauthorized transactions using their funds, the system could suffer a catastrophic failure even in the absence of any significant physical damage. Depending on the severity of the losses incurred, the loss of confidence in the system could be both widespread and enduring. Given the stakes involved and the risks of failure, it seems likely that the financial sector devotes a substantial amount of resources to defending its computer systems and networks from compromise or attack, to include maintaining entire backup systems on networks separate from those that are in active use. Whether these activities are sufficient to defend against or deter a determined attack is unclear, especially considering the challenge associated with the lack of security in global supply chains and the threat of an insider attack.

US key to the global economy

Caploe 9 [David Caploe is CEO of the Singapore-incorporated American Centre for Applied Liberal Arts and Humanities in Asia., “Focus still on America to lead global recovery”, April 7, The Strait Times, lexis]

IN THE aftermath of the G-20 summit, most observers seem to have missed perhaps the most crucial statement of the entire event, made by United States President Barack Obama at his pre-conference meeting with British Prime Minister Gordon Brown: 'The world has become accustomed to the US being a voracious consumer market, the engine that drives a lot of economic growth worldwide,' he said. 'If there is going to be renewed growth, it just can't be the US as the engine.' While superficially sensible, this view is deeply problematic. To begin with, it ignores the fact that the global economy has in fact been 'America-centred' for more than 60 years. Countries - China, Japan, Canada, Brazil, Korea, Mexico and so on - either sell to the US or they sell to countries that sell to the US. This system has generally been advantageous for all concerned. America gained certain historically unprecedented benefits, but the system also enabled participating countries - first in Western Europe and Japan, and later, many in the Third World - to achieve undreamt-of prosperity. At the same time, this deep inter-connection between the US and the rest of the world also explains how the collapse of a relatively small sector of the US economy - 'sub-prime' housing, logarithmically exponentialised by Wall Street's ingenious chicanery - has cascaded into the worst global economic crisis since the Great Depression. To put it simply, Mr Obama doesn't seem to understand that there is no other engine for the world economy - and hasn't been for the last six decades. If the US does not drive global economic growth, growth is not going to happen. Thus, US policies to deal with the current crisis are critical not just domestically, but also to the entire world. Consequently, it is a matter of global concern that the Obama administration seems to be following Japan's 'model' from the 1990s: allowing major banks to avoid declaring massive losses openly and transparently, and so perpetuating 'zombie' banks - technically alive but in reality dead. As analysts like Nobel laureates Joseph Stiglitz and Paul Krugman have pointed out, the administration's unwillingness to confront US banks is the main reason why they are continuing their increasingly inexplicable credit freeze, thus ravaging the American and global economies. Team Obama seems reluctant to acknowledge the extent to which its policies at home are failing not just there but around the world as well. Which raises the question: If the US can't or won't or doesn't want to be the global economic engine, which country will? The obvious answer is China. But that is unrealistic for three reasons. First, China's economic health is more tied to America's than practically any other country in the world. Indeed, the reason China has so many dollars to invest everywhere - whether in US Treasury bonds or in Africa - is precisely that it has structured its own economy to complement America's. The only way China can serve as the engine of the global economy is if the US starts pulling it first. Second, the US-centred system began at a time when its domestic demand far outstripped that of the rest of the world. The fundamental source of its economic power is its ability to act as the global consumer of last resort. China, however, is a poor country, with low per capita income, even though it will soon pass Japan as the world's second largest economy. There are real possibilities for growth in China's domestic demand. But given its structure as an export-oriented economy, it is doubtful if even a successful Chinese stimulus plan can pull the rest of the world along unless and until China can start selling again to the US on a massive scale. Finally, the key 'system' issue for China - or for the European Union - in thinking about becoming the engine of the world economy - is monetary: What are the implications of having your domestic currency become the global reserve currency? This is an extremely complex issue that the US has struggled with, not always successfully, from 1959 to the present. Without going into detail, it can safely be said that though having the US dollar as the world's medium of exchange has given the US some tremendous advantages, it has also created huge problems, both for America and the global economic system. The Chinese leadership is certainly familiar with this history. It will try to avoid the yuan becoming an international medium of exchange until it feels much more confident in its ability to handle the manifold currency problems that the US has grappled with for decades. Given all this, the US will remain the engine of global economic recovery for the foreseeable future, even though other countries must certainly help. This crisis began in the US - and it is going to have to be solved there too.

Economic collapse causes nuclear war

Kemp 10—Director of Regional Strategic Programs at The Nixon Center, served in the White House under Ronald Reagan, special assistant to the president for national security affairs and senior director for Near East and South Asian affairs on the National Security Council Staff, Former Director, Middle East Arms Control Project at the Carnegie Endowment for International Peace [Geoffrey Kemp, 2010, *The East Moves West: India, China, and Asia’s Growing Presence in the Middle East*, p. 233-4]

The second scenario, called Mayhem and Chaos, is the opposite of the first scenario; everything that can go wrong does go wrong. The world economic situation weakens rather than strengthens, and India, China, and Japan suffer a major reduction in their growth rates, further weakening the global economy. As a result, energy demand falls and the price of fossil fuels plummets, leading to a financial crisis for the energy-producing states, which are forced to cut back dramatically on expansion programs and social welfare. That in turn leads to political unrest: and nurtures different radical groups, including, but not limited to, Islamic extremists. The internal stability of some countries is challenged, and there are more “failed states.” Most serious is the collapse of the democratic government in Pakistan and its takeover by Muslim extremists, who then take possession of a large number of nuclear weapons. The danger of war between India and Pakistan increases significantly. Iran, always worried about an extremist Pakistan, expands and weaponizes its nuclear program. That further enhances nuclear proliferation in the Middle East, with Saudi Arabia, Turkey, and Egypt joining Israel and Iran as nuclear states. Under these circumstances, the potential for nuclear terrorism increases, and the possibility of a nuclear terrorist attack in either the Western world or in the oil-producing states may lead to a further devastating collapse of the world economic market, with a tsunami-like impact on stability. In this scenario, major disruptions can be expected, with dire consequences for two-thirds of the planet’s population.

Best studies prove economic collapse causes conflict

ROYAL 10Director of Cooperative Threat Reduction at the U.S. Department of Defense

 [Jedediah Royal, 2010, Economic Integration, Economic Signaling and the Problem of Economic Crises, in Economics of War and Peace: Economic, Legal and Political Perspectives, ed. Goldsmith and Brauer, p. 213-215]

**Less intuitive is how periods of economic decline may increase the likelihood of external conflict**. Political science literature has contributed a moderate degree of attention to the impact of economic decline and the security and defence behaviour of interdependent stales. Research in this vein has been considered at systemic, dyadic and national levels. Several notable contributions follow. First, on the systemic level. Pollins (20081 advances Modclski and Thompson's (1996) work on leadership cycle theory, finding that **rhythms in the global economy are associated with the rise and fall of a pre-eminent power and the often bloody transition from one pre-eminent leader to the next**. As such, **exogenous shocks such as economic crises could usher in a redistribution of relative power** (see also Gilpin. 19SJ) **that leads to uncertainty about power balances, increasing the risk of miscalculation** (Fcaron. 1995). Alternatively, **even a relatively certain redistribution of power could lead to a permissive environment for conflict as a rising power may seek to challenge a declining power** (Werner. 1999). Separately. Pollins (1996) also shows that global economic cycles combined with parallel leadership cycles impact the likelihood of conflict among major, medium and small powers, although he suggests that the causes and connections between global economic conditions and security conditions remain unknown. Second, on a dyadic level. Copeland's (1996. 2000) theory of trade expectations suggests that 'future expectation of trade' is a significant variable in understanding economic conditions and security behaviour of states. He argues that interdependent states arc likely to gain pacific benefits from trade so long as they have an optimistic view of future trade relations. However, **if the expectations of future trade decline**, **particularly for difficult to replace items such as energy resources**, **the likelihood for conflict increases**, **as states will be inclined to use force to gain access to those resources**. Crises could potentially be the trigger for decreased trade expectations either on its own or because it triggers protectionist moves by interdependent states.4 Third, **others** **have considered the link between economic decline and external armed conflict at a national level**. Mom berg and **Hess** (2002) **find a strong correlation between internal conflict and external conflict**, **particularly during periods of economic downturn**. They write. **The linkage, between internal and external conflict and prosperity are strong and mutually reinforcing**. **Economic conflict lends to spawn internal conflict, which in turn returns the favour**. Moreover, **the presence of a recession tends to amplify the extent to which international and external conflicts self-reinforce each other** (Hlomhen? & Hess. 2(102. p. X9> **Economic decline has also been linked with an increase in the likelihood of terrorism** (Blombcrg. Hess. & Wee ra pan a, 2004**). which has the capacity to spill across borders and lead to external tensions**. Furthermore, **crises generally reduce the popularity of a sitting government**. "**Diversionary theory" suggests that, when facing unpopularity arising from economic decline, sitting governments have increased incentives to fabricate external military conflicts to create a 'rally around the flag' effect**. Wang (1996), DcRoucn (1995), and Blombcrg. Hess, and Thacker (2006) find supporting evidence showing that economic decline and use of force arc at least indirecti) correlated. Gelpi (1997). Miller (1999). and Kisangani and Pickering (2009) suggest that Ihe tendency towards diversionary tactics arc greater for democratic states than autocratic states, due to the fact that democratic leaders are generally more susceptible to being removed from office due to lack of domestic support. DeRouen (2000) has provided evidence showing that periods of weak economic performance in the United States, and thus weak Presidential popularity, are statistically linked lo an increase in the use of force. In summary, **economic scholarship positively correlates economic integration with an increase in the frequency of economic crises**, **whereas political science scholarship links economic decline with external conflict** al systemic, dyadic and national levels.' This implied connection between integration, crises and armed conflict has not featured prominently in the economic-security debate and deserves more attention.

### 1ac – Plan Text

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

### 1ac – Solvency

Plan solves --- Congressional consultation decreases bureaucratic inertia and ensures more accurate counter-striking

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

III. ALEGISLATIVE HAND ON THE CYBER WAR MOUSE Cyber warfare, as that term is used here, refers to conflicts that utilize cyber or electronic weapons either offensively or defensively, or both.Cyber weapons are currently employed offensively in kinetic warfare, for example, to suppress an enemy’s air defenses or disrupt its communications, or defensively to track enemy troop movements. These weapons might also be used offensively to disable an enemy’s cyber weaponry or defensively in response to an enemy attack, to prevent further aggression. The term “cybersecurity” might be understood to refer to defense against cyber attacks. “Cyber attack” suggests offensive use, but the label is inexact and might be misleading. A preemptive strike to ward off an imminent enemy attack is considered defensive. Digital espionage might be part of the preparation for an attack, or it might be perceived that way by the target, which might then be provoked to defend itself by responding with a preemptive attack, either cyber or kinetic. The important point here is that any use of cyber weapons, offensive or defensive, could have enormous consequences for the security and other interests of the United States. The effect of such use, actual or potential, matters more than the labels. And if the effect – on human life or property, for example, or diplomatic relations or compliance with the law of armed conflict **–** is substantial, Congress has a role to play in adopting policy for that use. Congress has not thus far adopted measures suited to the regulation of cyber warfare**.** The War Powers Resolution, for example,is concerned with sending U.S. troops into harm’s way**,** rather than with clicking a computer mouse to launch a cyber attack, although the strategic consequences might be similar. And the WPR’s relatively relaxed timetable for executive notice and legislative response is unrealistic for war on a digital battlefield. Similarly, if cyber warfare is regarded as an intelligence activity, the intelligence oversight measures just described cannot, for reasons already indicated, ensure that Congress will be able to play a meaningful role. In the words of the National Research Council study cited above, “Today’s policy and legal framework for guiding and regulating the use of cyberattack is ill-formed, undeveloped, and highly uncertain.”45 Our experience with nuclear weapons may point to needed reforms. Since the beginning of the Cold War, the United States has had a fairly clear nuclear policy (albeit one that deliberately includes an element of ambiguity) – one known generally to Congress, the American public, and potential enemies.46 Congress has approved or disapproved the purchase of the weapons and delivery systems. It has been briefed on the policy, and it has debated that policy vigorously.47 While Congress has not articulated U.S. nuclear policy in any coherent form, it has collaborated closely with the executive branch in the development and execution of that policy. Cyber weapons bear a striking resemblance to nuclear weapons in some important ways. An enemy’s cyber attack would, like a nuclear strike, probably come without a clear warning. There are as yet no reliable defenses against either a cyber attack or a nuclear attack. Collateral damage from a nuclear attack would almost certainly be very extensive and would linger for an extended period.48 The direct and indirect effects of a cyber attack, while different in kind and degree, still could be widespread and indiscriminate.49 In other ways, cyber weapons are critically different from their nuclear counterparts. For one thing, the time frame for response to a cyber attack might be much narrower. A nuclear weapon delivered by a land-based ICBM could take 30 minutes to reach its target. An electronic attack would arrive instantaneously, and leave no time to consult with or even inform anyone outside the executive branch before launching a counterstrike, if that were U.S. policy. What most distinguishes digital warfare, however, is the potential difficulty in identifying the source of a cyber attack. It is always possible, of course, that an enemy might covertly deliver a nuclear device to the U.S. homeland in a shipping container or a Cessna. But the apparent ease with which a cyber attack may be carried out without attribution could make it impossible to fight back at all. If an attacker made it appear that the source was an innocent neutral state or perhaps another enemy of the attacker, a misdirected U.S. response might provoke a wider conflict. The potential difficulty in tracking the source also makes a policy of deterrence based on a threat of retaliation far less credible. Given these characteristics of cyber warfare, and the continuing refinement of cyber weaponry, we approach a state of extreme strategic instability, with each nation on hair-trigger alert. The execution of an illconceived cyber war policy calling for a prompt response – or any response – to an attack or threatened attack could have disastrous, unanticipated consequences. It also might, depending on the circumstances, violate the law of armed conflict. Congress accordingly needs to work closely with the executive branch in the development of a policy for this new kind of conflict. Such a policy ought to reflect the distinctive technology and strategy of digital warfare, and it should be reviewed constantly as the technology evolves. Like other regulations dealing with dynamic subjects, this policy should include general approaches that reflect this nation’s broad strategic concerns and fundamental values. But the policy must also be crafted with enough flexibility to allow those charged with its execution to deal with future developments that cannot now be predicted. And it should set out a procedure for such adaptive use by identifying, for example, who must be consulted under what circumstances, and who will make the final critical decisions. It is at least theoretically possible that Congress could play an active, real-time role in the implementation of whatever cyber warfare policy is adopted. The policy might, for example, like the War Powers Resolution, require consultation “in every possible circumstance.”50 But it seems more likely that a digital war would begin and end before any notice could ever reach Capitol Hill. Congress therefore needs to lay down clear guidelines, with as much flexibility as prudence requires, for executive branch officials to follow if consultation is not reasonably possible. And Congress should require a prompt and full account of every significant use of cyber weapons.

**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.)

**And, settling the legal framework around counterstrike operations bolsters 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.

**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

# 2ACs

### 2ac – T Restriction

**Restriction means a limit or qualification, and includes conditions on action**

CAA 8 [COURT OF APPEALS OF ARIZONA, DIVISION ONE, DEPARTMENT A, STATE OF ARIZONA, Appellee, v. JEREMY RAY WAGNER, Appellant., 2008 Ariz. App. Unpub. LEXIS 613]

P10 The term "restriction" is not defined by the Legislature for the purposes of the DUI statutes. See generally A.R.S. § 28-1301 (2004) (providing the "[d]efinitions" section of the DUI statutes). In the absence of a statutory definition of a term, we look to ordinary dictionary definitions and do not construe the word as being a term of art. Lee v. State, 215 Ariz. 540, 544, 15, 161 P.3d 583, 587 (App. 2007) ("When a statutory term is not explicitly defined, we assume, unless otherwise stated, that the Legislature intended to accord the word its natural and obvious meaning, which may be discerned from its dictionary definition.").

P11 The dictionary definition of "restriction" is "[a] limitation or qualification." Black's Law Dictionary 1341 (8th ed. 1999). In fact, "limited" and "restricted" are considered synonyms. See Webster's II New Collegiate Dictionary 946 (2001). Under these commonly accepted definitions, Wagner's driving privileges were "restrict[ed]" when they were "limited" by the ignition interlock requirement.Wagner was not only [\*7] statutorily required to install an ignitioninterlock device on all of the vehicles he operated, A.R.S. § 28-1461(A)(1)(b), but he was also prohibited from driving any vehicle that was not equipped with such a device, regardless whether he owned the vehicle or was under the influence of intoxicants, A.R.S. § 28-1464(H). These limitations constituted a restriction on Wagner's privilege to drive, for he was unable to drive in circumstances which were otherwise available to the general driving population. Thus, the rules of statutory construction dictate that the term "restriction" includes the ignition interlock device limitation.

**Statutory restrictions include 5 things**

Kaiser 80 [The Official Specialist in American National Government, Congressional Research Service, the Library of Congress, Congressional Action to Overturn Agency Rules: Alternatives to the Legislative Veto; Kaiser, Frederick M., 32 Admin. L. Rev. 667 (1980)]

In addition to direct statutory overrides, there are a variety of statutory and nonstatutory techniques that have the effect of overturning rules, that prevent their enforcement, or that seriously impede or even preempt the promulgation of projected rules. For instance, a statute may alter the jurisdiction of a regulatory agency or extend the exemptions to its authority, thereby affecting existing or anticipated rules. Legislation that affects an agency's funding may be used to prevent enforcement of particular rules or to revoke funding discretion for rulemaking activity or both. Still other actions, less direct but potentially significant, are mandating agency consultation with other federal or state authorities and requiring prior congressional review of proposed rules (separate from the legislative veto sanctions). These last two provisions may change or even halt proposed rules by interjecting novel procedural requirements along with different perspectives and influences into the process.

It is also valuable to examine nonstatutory controls available to the Congress:

1. legislative, oversight, investigative, and confirmation hearings;

2. establishment of select committees and specialized subcommittees to oversee agency rulemaking and enforcement; 3. directives in committee reports, especially those accompanying legislation, authorizations, and appropriations, regarding rules or their implementation; 4. House and Senate floor statements critical of proposed, projected, or ongoing administrative action; and 5. direct contact between a congressional office and the agency or office in question. Such mechanisms are all indirect influences; unlike statutory provisions**,** they are neither self-enforcing nor legally binding by themselves. Nonetheless, nonstatutory devices are more readily available and more easily effectuated than controls imposed by statute. And some observers have attributed substantial influence to nonstatutory controls in regulatory as well as other matters.3 It is impossible, in a limited space, to provide a comprehensive and exhaustive listing of congressional actions that override, have the effect of overturning, or prevent the promulgation of administrative rules. Consequently, this report concentrates upon the more direct statutory devices, although it also encompasses committee reports accompanying bills, the one nonstatutory instrument that is frequently most authoritatively connected with the final legislative product. The statutory mechanisms surveyed here cross a wide spectrum of possible congressional action: 1. single-purpose provisions to overturn or preempt a specific rule**;** 2. alterations in program authoritythat remove jurisdiction from an agency; 3. agency authorization and appropriation limitations**;** 4. inter-agency consultation requirements; and 5. congressional prior notification provisions

**Authority refers to granting permission**

**Taylor 96** [Ellen, 21 Del. J. Corp. L. 870 (1996), Hein Online]

The term authority is commonly thought of in the context of the law of agency, and the Restatement (Second) of Agency defines both power and authority.'89 Power refers to an agent's ability or capacity to produce a change in a legal relation (whether or not the principal approves of the change), and authority refers to the power given (permission granted) to the agent by the principal to affect the legal relations of the principal; the distinction is between what the agent can do and what the agent may do.

**C/I is superior --- it’s best for predictability --- our interpretation only allows for 5 mechanisms, which makes for a more manageable topic --- that’s best for limits and pre-round preparation --- and, it’s the best for real world education --- inter-branch consultation is the core of the literature and is how congress has restricted the president in the past**

**Prefer reasonability --- competing interpretations are arbitrary and makes aff prep impossible**

**Grid collapse causes 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.

### 2ac – OLC CP

**CP links --- CP uses Congress**

**Doesn’t make sense --- Congress doesn’t have the authority to use the OLC**

**No impact to SOP**

**Perm do both --- solves SOP**

**Plan solves SOP --- has congress establish a statutory f/w to check the prez**

**Perm do both --- solves the net benefit**

**Perm do the CP --- it’s an example of how the plan could be done because normal means is that Congress would have to enact legislation that establishes requirements for consultation**

OLC can’t solve and links to politics

Posner 11 Eric Posner is the Kirkland & Ellis Professor, University of Chicago Law School. “DEFERENCE TO THE EXECUTIVE IN THE UNITED STATES AFTER 9/11 CONGRESS, THE COURTS AND THE OFFICE OF LEGAL COUNSEL” available at http://www.law.uchicago.edu/academics/publiclaw/index.html.

These two events neatly encapsulate the dilemma for OLC, and indeed all the president’s legal advisers. If OLC tries to block the president from acting in the way he sees fit, it takes the risk that he will disregard its advice and marginalize the institution. If OLC gives the president the advice that he wants to hear, it takes the risk that it will mislead him and fail to prepare him for adverse reactions from the courts, Congress, and the public. Can OLC constrain the executive? That is the position taken by many scholars, most notably Jack Goldsmith. 18 The underlying idea here is that even if Congress and the courts cannot constrain the executive, perhaps offices within the executive can. The opposite view, advanced by Bruce Ackerman, is that OLC is a rubber stamp. 19 I advocate a third view: OLC does not constrain the executive but enables him to accomplish goals that he would not otherwise be able to accomplish. It is more accurate to say that OLC enables than constrains. B. OLC as a Constraint on the Executive A number of scholars have argued that OLC can serve as an important constraint on executive power. I will argue that OLC cannot act as a constraint on executive power. Indeed, its only function is the opposite—as an “enabler” (as I will put it) or extender of executive power. A president must choose a course of action. He goes to OLC for advice. Ideally, OLC will provide him good advice as to the legality of the course of action. It will not provide him political advice and other relevant types of advice. The president wants to maximize his political advantage, 21 and so he will follow OLC’s advice only if the legal costs that OLC identifies are greater than the political benefits. On this theory, OLC will properly always give the president neutral advice, and the president will gratefully accept it although not necessarily follow it. If the story ended here, then it would be hard to see what the controversy over OLC could be about. As an adviser, it possesses no ability to constrain the executive. It merely provides doctrinal analysis, in this way, if it does its job properly, merely supplying predictions as to how other legal actors will react to the president’s proposed action. The executive can choose to ignore OLC’s advice, and so OLC cannot serve as a “constraint” on executive power in any meaningful sense. Instead, it merely conveys to the president information about the constraints on executive power that are imposed from outside the executive branch. However, there is an important twist that complicates the analysis. The president may choose to publicize OLC’s opinions. Naturally, the president will be tempted to publicize only favorable opinions. When Congress 22 claims that a policy is illegal, the president can respond that his lawyers advised him that the policy is legal. This response at least partially deflects blame from the president. There are two reasons for this. First, the Senate consented to the appointment of these lawyers; thus, if the lawyers gave bad advice, the Senate is partly to blame, and so the blame must be shared. Second, OLC lawyers likely care about their future prospects in the legal profession, which will turn in part on their ability to avoid scandals and to render plausible legal advice; they may also seek to maintain the office’s reputation. When OLC’s opinions are not merely private advice, but are used to justify actions, then OLC takes on a quasi-judicial function. Presidents are not obliged to publicize OLC’s opinions, but clearly they see an advantage to doing so, and they have in this way given OLC quasi-judicial status. But if the president publicizes OLC opinions, he takes a risk. The risk is that OLC will publicly advise him that an action is illegal. If OLC approval helps deflect blame from the president, then OLC disapproval will tend to concentrate blame on the president who ignores its advice. Congress and the public will note that after all the president is ignoring the advice of lawyers that he appointed and thus presumably he trusts, and this can only make the president look bad. To avoid such blame, the president may refrain from engaging in a politically advantageous action. In this way, OLC may be able to prevent the president from taking an action that he would otherwise prefer. At a minimum, OLC raises the political cost of the action. I have simplified greatly, but I believe that this basic logic has led some scholars to believe that OLC serves as a constraint on the president. But this is a mistake. OLC strengthens the president’s hand in some cases and weakens them in others; but overall it extends his power—it serves as enabler, not constraint. To see why, consider an example in which a president must choose an action that lies on a continuum. One might consider electronic surveillance. At one extreme, the president can engage in actions that are clearly lawful—for example, spying on criminal suspects after obtaining warrants from judges. At the other extreme, the president can engage in actions that are clearly unlawful—for example, spying on political opponents. OLC opinions will not affect Congress’s or the public’s reaction to either the obviously lawful or the obviously unlawful actions. But then there are middle cases. Consider a policy L, which is just barely legal, and a policy I, which is just barely illegal. The president would like to pursue policy L but fears that Congress and others will mistakenly believe that L is illegal. As a result, political opposition to L will be greater than it would be otherwise. In such a case, a favorable advisory opinion from a neutral legal body that has credibility with Congress will help the president. OLC’s approval of L would cause political opposition (to the extent that it is based on the mistaken belief that L is unlawful) to melt away. Thus, OLC enables the president to engage in policy L, when without OLC’s participation that might be impossible. True, OLC will not enable the president to engage in I, assuming OLC is neutral. And, indeed, OLC’s negative reaction to I may stiffen Congress’ resistance. However, the president will use OLC only because he believes that OLC will strengthen his hand on net. It might be useful to make this point using a little jargon. In order for OLC to serve its ex ante function of enabling the president to avoid confrontations with Congress in difficult cases, it must be able to say “no” to him ex post for barely illegal actions as well as “yes” to him for barely legal actions. It is wrong to consider an ex post no as a form of constraint because, ex ante, it enables the president to act in half of the difficult cases. OLC does not impose any independent constraint on the president, that is, any constraint that is separate from the constraint imposed by Congress. An analogy to contract law might be useful. People enter contracts because they enable them to do things ex ante by imposing constraints on them ex post. For example, a debtor can borrow money from a creditor only because a court will force the debtor to repay the money ex post. It would be strange to say that contract law imposes “constraints” on people because of ex post enforcement. In fact, contract law enables people to do things that they could not otherwise do—it extends their power. If it did not,people would not enter contracts. A question naturally arises about OLC’s incentives. I have assumed that OLC provides neutral advice—in the sense of trying to make accurate predictions as to how other agents like Congress and the courts would reaction to proposed actions. It is possible that OLC could be biased—either in favor of the president or against him. However, if OLC were biased against the president, he would stop asking it for advice (or would ask for its advice in private and then ignore it). This danger surely accounts for the fact that OLC jurisprudence is pro-executive. 23 But it would be just as dangerous for OLC to be excessively biased in favor of the president. If it were, it would mislead the president and lose its credibility with Congress, with the result that it could not help the president engage in L policies. So OLC must be neither excessively pro-president nor anti-president. If it can avoid these extremes, it will be an “enabler”; if it cannot, it will be ignored. In no circumstance could it be a “constraint.” If the OLC cannot constrain the president on net, why have people claimed that OLC can constrain the president? What is the source of this mistake? One possibility, which I have already noted, is that commentators might look only at one side of the problem. Scholars note that OLC may “prevent” the president from engaging in barely illegal actions without also acknowledging that it can do so only if at the same time it enables the president to engage in barely legal actions. This is simply a failure to look at the full picture. For example, in The Terror Presidency, Goldsmith argues that President Bush abandoned a scheme of warrantless wiretapping without authorization from the FISA court because OLC declared the scheme illegal, and top Justice Department officials threatened to resign unless Bush heeded OLC’s advice. 25 This seems like a clear example of constraint. But it is important to look at the whole picture. If OLC had approved the scheme, and subsequently executive branch agents in the NSA had been prosecuted and punished by the courts, then OLC’s credibility as a supplier of legal advice would have been destroyed. For the president, this would have been a bad outcome. As I have argued, a credible OLC helps the president accomplish his agenda in “barely legal” cases. Without taking into account those cases where OLC advice helps the president’s agenda ex post as well as the cases where OLC advice hurts the president’s agenda ex post, one cannot make an overall judgment about OLC’s ex ante effect on executive power. Another possible source of error is that scholars imagine that “neutral” advice will almost always prevent the president from engaging in preferred actions, while rarely enabling the president to engage in preferred actions. The implicit picture here is that a president will normally want to break the law, that under the proper interpretation of the Constitution and relevant standards the president can accomplish very little. So if OLC is infact neutral and the president does obey its advice, then it must constrain the president. But this theory cannot be right, either. If OLC constantly told the president that he cannot do what he wants to do, when infact Congress and other agents would not object to the preferred actions, then the president would stop asking OLC for advice. As noted above, for OLC to maintain its relevance, it cannot offer an abstract interpretation of the Constitution that is divorced from political realities; it has to be able to make realistic predictions as to how other legal agents will react to the president’s actions. This has led OLC to develop a pro-executive jurisprudence in line with the long-term evolution of executive power. If OLC tried to impose constraints other than those imposed by Congress and other institutions with political power, then the president would ignore it.

**CP is a VI --- it’s object fiat --- they change the position of the thing we are trying to restrict --- that ruins aff ground --- and it abuses the literature which only exists because of an abusive executive --- they can have a CP that does a different restriction to solve --- that ensures clash**

**No solvency --- only plan gives the president political cover and legitimacy for launching more offensive cyber operations**

**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]

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 choicewhen 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 outagainst 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.

**Conditionality is a VI --- it skews 2AC strategy because the block can kick the least covered position --- and, it disadvantages the 1AR versus the block because of the neg’s time advantage --- kills fairness --- it also kills decision-making skills because it encourages the neg to go for the least covered position**

Doesn’t solve legal clarity OR president ignores

Posner 11 Eric Posner is the Kirkland & Ellis Professor, University of Chicago Law School. “DEFERENCE TO THE EXECUTIVE IN THE UNITED STATES AFTER 9/11 CONGRESS, THE COURTS AND THE OFFICE OF LEGAL COUNSEL” available at http://www.law.uchicago.edu/academics/publiclaw/index.html.

C. Evidence

1. Testing the Three Hypotheses

We have three hypotheses about OLC on the table. The first is that OLC is an ex ante constraint on presidential power, serving a role similar to thatof Congress and the courts. The second is that OLC is an ex ante enabler of presidential power. The third hypothesis is Ackerman’s rubber-stamp theory that OLC serves neither as a constraint nor as an enabler because it cannot say no ex post. In this section, I will briefly discuss the evidence. It is easy enough to distinguish Ackerman’s hypothesis from the other two: if OLC never or rarely says no, then Ackerman is right. In addition, Ackerman is right even if OLC sometimes says no but the president ignores OLC in those cases. Distinguishing the constraint and enabler hypotheses is more difficult. Both hypotheses predict some ex post no’s. To distinguish the hypotheses, one would need to look at the other side of the ledger: the cases where OLC has enabled the president to act where otherwise Congress would have opposed him. Unfortunately, it would be hard to identify such cases. 2. Statistical Evidence In a study of the written opinions of OLC, Trevor Morrison found that 79 percent approved the president’s position, 8 percent provided a mixed answer, and 13 percent disapproved the president’s position. 26 In several cases, OLC rejected the White House position on issues of significance. In addition, Morrison notes that since OLC usually provides negative advice orally, the written record reflects a selection bias in favor of approvals. 27 But there is less here than meets the eye. First, one must keep in mind that the executive is a “they,” not an “it.” When the president cannot resolve policy differences among his major advisers, he may well be indifferent about OLC’s reaction and indeed welcome a legal resolution (“sorry, my hands are tied”). Second, the relevant focus, for the purpose of my argument, is OLC advice on national security issues. On this topic, the consensus appears to be that OLC has said no to the executive in only four cases in its entire history aside from matters that remain classified: the rejection of the Bush administration’s argument that the Geneva Conventions do not apply to terrorists in Iraq in 2002; 28 the rejection of certain forms of coercive interrogation in 2003; rejection of electronic surveillance that circumvented the FISA court in 2003; and rejection of the Libya intervention in 2011. 2 Even these cases turn out to be ambiguous. It must be recalled that OLC first said “yes” on coercive interrogation and electronic surveillance, and then changed its mind a few years later. In addition, OLC’s “no” on coercive interrogation turned out to be less than absolute: it continued to authorize waterboarding even after the earlier memorandum was withdrawn. Unfortunately, evaluating the empirical evidence is even harder than Morrison indicates. The problem is not just that negative advice is confidential; the problem is that we do not know how the executive responded to this negative advice. Did it desist from its conduct? Modify it along the margins? Or ignore OLC? Maybe, maybe not. A further methodological problem concerns whether a “no” blocks an important policy or simply requires certain i’s to bedotted or t’s to be crossed. OLC officials often emphasize that their job is to help the White House find a legally acceptable method of accomplishing their aims. Even the early Bush administration OLC drew the line on certain forms of torture (such as mock executions, the use of insects to exploit fears, etc.) and established guidelines to ensure the safety of detainees. The problem with treating this advice as a “no” is that it is not clear that the executive cared about these details, as opposedto the broad agenda of using coercive interrogation practices. It no doubt wanted legal advice so as to minimize the risk of legal liability. Finally, as we have seen, President Obama ignored OLC’s position on the Libya intervention. So in that case, OLC took a brave stand and then discovered that it had been pushed to the sidelines. This major event offered unusuallyrapid confirmation of Ackerman’s claim that the executive can avoid negative advice from OLC by soliciting advice from the White House Counsel’s Office. (Obama also received favorable advice from the State Department legal counsel.) Morrison argued prior to this event that the president faces strong disincentives to end-running OLC. 30 Afterwards, he could only criticize the president, claim he suffered from negative political fallout, and hope that this sort of thing does not happen too often. 31 However, while the president was criticized, there is simply no evidence that his evasion of OLC has hurt him politically. As is so often case, the (apparent) success of the operation provides its own justification. The upshot is that there is some evidence that OLC serves as an ex post constraint, but it is fairly weak. Ackerman’s hypothesis seems too extreme, but it is hard to distinguish between the constraint and enabler hypothesis. It is possible that OLC serves as a weak constraint or a weak enabler. Why has it been so weak? First,it may turn out that the constellation of factors that drive decisionmaking in the executive branch prevents the president from solving a time-inconsistency problem by using OLC. The president benefits fromneutral advice, and frombeing able to cite OLC’s approval, but when OLC blocks the president, short-term political considerations trump the medium-term advantages of maintaining a neutral OLC. Meanwhile, OLC’s lawyers yield to political pressure either for careerist reasons or in order to prevent the president from cutting OLC out of the process. Private lawyers face similar pressures, but the market in legal services might provide some additional discipline. Second, the problem might lie in the nature offoreign relations and national security, an area of action that has been notoriously difficult to bring under legal control. Courts have frequently been asked to adjudicate disputes between Congress and the president inthe area of national security. Generally speaking, they have resisted these requests, treating these issues as political questions or nonjusticiable for other reasons. The usual explanation for this resistance is that courts are not experts on these issues; that the highly fluid, frequently changing nature of foreign relations and national security makes themunsuitable for judicial resolution, which is rule-bound, public, decentralized, and slow; and that, accordingly, courts fear that if they intervene, their rulings will be ignored by the executive branch, provoking a constitutional crisis. The supposed solution to this problem is to ask an advisory office in the executive branch to take over a function that the courts have repudiated. It is true that a small office in the executive branch can overcome certain problems that courts face relating to secrecy and speed. But the fundamental problem is that foreign relations are not susceptible to regulation by rules. 32

**Checks and balances are key to a credible deterrence strategy and prevents nuclear war**

Rothschild 13 [Matthew, Feb 4, "The Danger's of Obama's Cyber War Power Grab," www.progressive.org/dangers-of-obama-cyber-war-power-grab]

There are no checks or balances when the President, alone, decides when to engage in an act of war.

And this new aggressive stance will lead to a cyber arms race. TheUnited States hasevidently already used cyber weapons against Iran**,** and so many other countries will assume that cyber warfare is an acceptable tool and will try to use it themselves.

Most troubling, U.S. cybersupremacy—and that is Pentagon doctrine**—**will also raise fears among nuclear powers like Russia, China, and North Korea that theUnited States may use a cyberattack as the opening move in a nuclear attack.

Forif the United States can knock out the command and control structure of an enemy’s nuclear arsenal**,** it can then launch an all-out nuclear attack on that enemy with impunity**.** This would make such nuclear powers more ready to launch their nuclear weapons preemptively for fear that they would be rendered useless. So we’ve just moved a little closer to midnight.

Now, I don’t think Obama would use cyberwafare as a first strike in a nuclear war. But our adversaries may not be so sure, either about Obama or his successors. They, too, worry about the temptations of a President.

**Plan prevents cyber terrorists from hacking into nuclear command centers --- the impact is nuclear war**

**Fritz 9** [Jason, former captain in US Army, MA international relations (Bond), BS (St. Cloud), writer at Center for New American Security, paper written for International Commission on Nuclear Non-proliferation and Disarmament, http://www.icnnd.org/Documents/Jason\_Fritz\_Hacking\_NC2.pdf?noredirect=1, nrb]

This paper will analyse the threat of cyber terrorism in regard to nuclear weapons. Specifically, this research will use open source knowledge to identify the structure of nuclear command and control centres, how those structures might be compromised through computer network operations, and how doing so would fit within established cyber terrorists’ capabilities, strategies, and tactics. If access to command and control centres is obtained, terrorists could fake or actually cause one nuclear-armed state to attack another, thus provoking a nuclear response from another nuclear power. This may be an easier alternative for terrorist groups than building or acquiring a nuclear weapon or dirty bomb themselves. This would also act as a force equaliser, and provide terrorists with the asymmetric benefits of high speed, removal of geographical distance, and a relatively low cost. Continuing difficulties in developing computer tracking technologies which could trace the identity of intruders, and difficulties in establishing an internationally **agreed upon legal framework to guide responses** to computer network operations, point towards an inherent weakness in using computer networks to manage nuclear weaponry. This is particularly relevant to reducing the **hair trigger posture** of existing nuclear arsenals.

All computers which are connected to the internet are susceptible to infiltration and remote control. Computers which operate on a closed network may also be compromised by various hacker methods, such as privilege escalation, roaming notebooks, wireless access points, embedded exploits in software and hardware, and maintenance entry points. For example, e-mail spoofing targeted at individuals who have access to a closed network, could lead to the installation of a virus on an open network. This virus could then be carelessly transported on removable data storage between the open and closed network. Information found on the internet may also reveal how to access these closed networks directly. Efforts by militaries to place increasing reliance on computer networks, including experimental technology such as autonomous systems, and their desire to have multiple launch options, such as nuclear triad capability, enables multiple entry points for terrorists. For example, if a terrestrial command centre is impenetrable, perhaps isolating one nuclear armed submarine would prove an easier task. There is evidence to suggest multiple attempts have been made by hackers to compromise the extremely low radio frequency once used by the US Navy to send nuclear launch approval to submerged submarines. Additionally, the alleged Soviet system known as Perimetr was designed to automatically launch nuclear weapons if it was unable to establish communications with Soviet leadership. This was intended as a retaliatory response in the event that nuclear weapons had decapitated Soviet leadership; however it did not account for the possibility of cyber terrorists blocking communications through computer network operations in an attempt to engage the system.

Should a warhead be launched, damage could be further enhanced through additional computer network operations. By using proxies, multi-layered attacks could be engineered. Terrorists could remotely commandeer computers in China and use them to launch a **US nuclear attack against Russia**. Thus Russia would believe it was under attack from the US and the US would believe China was responsible. Further, emergency response communications could be disrupted, transportation could be shut down, and disinformation, such as misdirection, could be planted, thereby hindering the disaster relief effort and maximizing destruction. Disruptions in communication and the use of disinformation could also be used to provoke uninformed responses. For example, a **nuclear strike between India and Pakistan** could be coordinated with Distributed Denial of Service attacks against key networks, so they would have further difficulty in identifying what happened and be forced to respond quickly. Terrorists could also knock out communications between these states so they cannot discuss the situation. Alternatively, amidst the confusion of a traditional large-scale terrorist attack, claims of responsibility and declarations of war could be falsified in an attempt to instigate a hasty military response. These false claims could be posted directly on Presidential, military, and government websites. E-mails could also be sent to the media and foreign governments using the IP addresses and e-mail accounts of government officials. A sophisticated and all encompassing combination of traditional terrorism and cyber terrorism could be enough to launch nuclear weapons on its own, without the need for compromising command and control centres directly.

**CP links to politics**

Hallowell 13 [Billy Hallowell, writer for The Blaze, B.A. in journalism and broadcasting from the College of Mount Saint Vincent in Riverdale, New York and an M.S. in social research from Hunter College in Manhattan, “HERE’S HOW OBAMA IS USING EXECUTIVE POWER TO BYPASS LEGISLATIVE PROCESS” Feb. 11, 2013, http://www.theblaze.com/stories/2013/02/11/heres-how-obamas-using-executive-power-to-bylass-legislative-process-plus-a-brief-history-of-executive-orders/]

“In an era of polarized parties and a fragmented Congress, the opportunities to legislate are few and far between,” Howell said. “So presidents have powerful incentive to go it alone. And they do.”

And the political opposition howls. Sen. Marco Rubio, R-Fla., a possible contender for the Republican presidential nomination in 2016, said that on the gun-control front in particular, Obama is “abusing his power by imposing his policies via executive fiat instead of allowing them to be debated in Congress.”

 The Republican reaction is to be expected, said John Woolley, co-director of the American Presidency Project at the University of California in Santa Barbara.¶ “For years there has been a growing concern about unchecked executive power,” Woolley said. “It tends to have a partisan content, with contemporary complaints coming from the incumbent president’s opponents.”

**Unrestrained executive prevents faithful discussion --- that causes pre-emptive warfare**

Holmes 8 [Stephen, Walter E. Meyer Professor of Law at NYU School of Law, “Conclusion,” from Security v. Liberty: Conflicts Between Civil Liberties and National Security in American History, p. 219-220, ed by Daniel Farber]

RIGIDITIES OF THE INSULATED EXECUTIVE

Only an executive branch emancipated from legal and constitutional constraints, the administration's defenders argue, will have enough flexibility to defeat a diabolical enemy. This sounds theoretically plausible, but the facts tell a contrary story. Freedom from judicial and legislative oversight has produced not open-eyed flexibility but pathological rigidity. Instead of acknowledging the obvious, namely America's inability to democratize Iraq, the administration has lashed itself(and the country) to a failed policy. Indeed, it continues to act as if its misbegotten project is still on track, only somewhat delayed. Decision making in an echo chamber, refusing to pay any attention to dissident voices, means selecting evidence to corroborate preformed opinions, misunderstanding the challenges ahead, and refusing to ask what if and what then**.** Dispensing with uninhibited criticism and debate in the face of a threat intrinsically difficult to understand is to doom the country to wild goose chases and a reckless misallocation of scarce national security assets in an increasingly dangerous world. Surrounded by yes-men and sheltered from seriously informed criticism, a pampered and unchecked executive becomes catastrophically disconnectedfrom reality. Concentrating excessive authority in the executive does not increase effectiveness in time of multiple evolving dangers because, for one thing, an all-powerful president becomes unwilling to hear bad news. Thus, the advocates, not the opponents, of an imperial presidency are the ones who have spectacularly failed to understand the true seriousness of today's terrorist threat.

### 2ac – TPA DA

#### PC not key --- Kerry and others are pushing --- Obama doesn’t lose PC

#### Won’t pass and not key to trade

Watson 12/19 [Bill, Trade Policy Analyst at the Cato Institute’s Herbert A. Stiefel Center for Trade Policy Studies, 2013, “Stay Off the Fast Track: Why Trade Promotion Authority Is Wrong for the Trans-Pacific Partnership,” <http://www.cato.org/publications/free-trade-bulletin/stay-fast-track-why-trade-promotion-authority-wrong-trans-pacific>]

The benefits of trade promotion authority, however, come with a substantial cost. Congress generally sees trade promotion authority as a way not only to expedite the passage of trade agreements but also to influence their content.5 Any agreement that receives fast track treatment is expected to conform to demands imposed by Congress in the trade promotion authority statute.

The 2002 Trade Promotion Act, in particular, laid out extensive and detailed negotiating objectives. Topics covered in the objectives included investment protection, intellectual property laws, administrative law, labor law, and environmental protection.6 These objectives are mostly export-oriented and reflect the interests of certain U.S. business interests in foreign markets. Their inclusion may garner additional political support for the agreement, but they also attract opposition.

Most importantly, achieving these negotiating goals will not liberalize trade. Nevertheless, these non-trade issues are often the most politically contentious aspect of trade agreements. At the same time, they distract negotiators from the legitimate goal of lowering U.S. trade barriers and fighting protectionism. Trade Promotion Authority Is Unnecessary The conventional wisdom, among trade advocates and opponents alike, is that fast track is necessary to get agreements through Congress. But the most recent experiences with trade promotion authority following the Democratic takeover of the House of Representatives in 2007 aptly demonstrate how ineffective it can be. At the same time, trade policy has become increasingly partisan in recent decades so that trade promotion authority is now neither necessary nor sufficient to pass free trade agreements.

Partisan Congress

In theory, trade promotion authority works well to enable the president to pursue an ambitious trade policy despite a typically trade-skeptic Congress. The negotiating objectives Congress includes in trade promotion authority serve as politically necessary restrictions on the president’s power to open the U.S. market. According to conventional wisdom, accepting the need for a watered-down agreement in advance is the only way to avoid having an agreement rejected or delayed after years of difficult negotiations.

#### Globalization is inevitable

Brainard 8 Vice President and Director for Global Economy and Development

[Lael, Senate Committee on Finance, “America’s Trade Agenda: Examining the Trade Enforcment Act of 2007,” Senate testimony, 5/22/2008, brookings.edu/testimony/2008/0522\_trade\_brainard.aspx]

We are experiencing a period of breathtaking global integration that dwarfs previous episodes. Global trade has more than doubled in the last 7 years alone. The entry of India and China amounts to a 70 percent expansion of the global labor force—with wages less than a tenth of the level in wealthy economies. This expansion is more than three times bigger than the globalization challenge of the 1970s and 80s associated with the sequential advances of Japan, South Korea, and the other Asian tigers. It is also far larger than the more recent integration of the North American market. If, as is now widely expected, these trends in population and productivity growth continue, the time will soon approach where the balance of global economic heft flips. According to my colleague, Homi Kharas, the so-called emerging BRIC (Brazil, Russia, India and China) economies will account for over half of world income by 2050, up from 13 percent today, while the share of the G7 wealthiest economies will slip from 57 percent today to one quarter of world income in 2050. And by 2030, 83 percent of the world’s middle class consumers will reside in what are today considered emerging markets.

#### Healthcare thumps the DA

Finkel 1-15-- editor of Against the Current [David “Will the Iran deal hold?” <http://internationalviewpoint.org/spip.php?article3239>, DOA: 1-17-14]

A politically weakened U.S. president is pulled by a powerful domestic lobby and influential foreign governments toward launching a war that U.S. imperialism right now doesn’t want, that the world doesn’t want, and that the large majority of the American public doesn’t want — what will be the outcome? It’s an interesting, if dangerous and scary, test of how U.S. politics actually work. The initial results, at least, are in: The unleashed fury of the Israeli government and the “pro-Israel” lobby, the monarchy of Saudi Arabia, the neoconservative warmongers and the much-feared religious right weren’t able to block the Obama administration and European partners from reaching a six-month interim agreement with Iran over that country’s nuclear enrichment program. Any socialist, progressive or sane person must welcome this agreement. That’s not because it resolves the proliferation of nuclear weapons, or changes the hideous character of the Iranian regime in relation to its own population, or addresses the multiple underlying issues of the Middle East crisis — it does none of these things — but because it pushes back the imminent danger of a really catastrophic war. That’s one strike against the widely held theory that the toxic influence of the Israel Lobby can drag the United States into wars that this country‘s ruling class disapproves. The political fight, of course, is hardly over. We’ll explore the underlying reasons for the Israeli and Saudi sound and fury over the deal with Iran, which in fact have little to do with the rather distant specter of an Iranian atomic bomb. But we need to note the U.S. political context in which the fight will play out. If anything, this might have been expected to strengthen the hand of the “war party.” A Wounded Presidency The spectacular disaster of the Afford­able Care Act website is a self-inflicted wound from which the Obama administration will not easily, or perhaps ever, fully recover. Certainly all of us who support single-payer health insurance realized that the fantastically tangled system of “Obamacare” would ultimately fail, due to its scheme for subsidizing the parasitical private insurance industry, but no one could have expected such an immediate display of arrogant incompetence in the “rollout.” The Republican Party has regained big chunks of the ground lost during its own government shutdown fiasco. It’s true that Congress’s approval ratings remain even deeper in the toilet than the President’s, but that fact affects both capitalist parties — and now, Congressional Democrats who stood united against repealing “Obamacare,” because that would have represented the effective end of the Obama presidency and virtual suicide for the party, are angry, alienated and afraid to be near him. Whatever political capital the President had for immigration reform, seriously raising the minimum wage, protecting food stamps from savage cuts, or much of anything else including the climate change crisis, has been dissipated. The Democrats’ chances of regaining the House of Representatives in the November 2014 midterm election, marginal to begin with, are now much less than those of losing the Senate as well. In these circumstances, this might be considered a favorable moment for the power of the Israel Lobby, Saudi Arabia and rightwing militarists to derail the Obama administration’s deal with Iran. In fact, France made a last-minute move to block the first version of the interim agreement — right after Saudi Arabia signed off on a huge purchase of French weapons (a point worth noting in case anyone thought it’s only the USA that has a military-industrial complex). The President’s **loss of control over his own party** is such that many prominent Democratic Senators have taken to the airwaves loudly denouncing his “appeasement” of the Iranians and abandonment of Israel in its hour of existential peril.

#### TPA won’t pass now – Obama would need more capital

REUTERS 1 – 30 – 14 [Analysis: White House hopes for fast-track trade hit political tangle, <http://www.reuters.com/article/2014/01/31/us-usa-trade-analysis-idUSBREA0U05T20140131>]

President Barack Obama's push for authority to fast-track trade deals has hit a big setback in the form of opposition from his top fellow Democrat in Congress, but it is far from dead.

Senate Majority Leader Harry Reid's warning to policymakers on Wednesday "just to not push this right now" reflects concern about the domestic political agenda ahead of November's congressional elections, when free trade could be a damaging issue for many Democrats.

The unusually blunt public opposition came less than 24 hours after Obama noted the need for fast-track power in his State of the Union address, albeit less forcefully than business lobbyists and pro-trade Republicans would have liked.

The White House called Reid's office shortly after his comments to voice displeasure, a top Democratic party aide said.

"They were really upset," the aide said. But the aide said the White House did not try to get Reid to shift his position.

A bill before the House and Senate would grant the White House power to submit free trade deals to Congress for an up-or-down vote without amendments, something that would give trading partners peace of mind but that raises hackles among some lawmakers.

Add to that the genuine mistrust among some Democrats about the impact of trade deals on local jobs and industry and environmental standards, and it's a volatile mix.

With two major free trade deals hanging in the balance, the U.S. administration now faces even more pressure to win over skeptics on both sides of politics to pass trade promotion authority (TPA) as the electoral clock ticks down.

"Reid's put a strait-jacket on TPA for now," said Welles Orr, trade adviser for law firm Miller Chevalier and former congressional relations expert at the U.S. Trade Representative.

Aides insist that Reid, who controls what comes up on the Senate floor, has not decided to kill the bill but is not ready to embrace it either and has let the White House know he will not be an easy sell.

That leaves the White House with a tough decision on how much political capital to expend lining up support on a politically contentious measure ahead of the elections.

U.S. Trade Representative Michael Froman and his staff are lobbying lawmakers about the benefits of TPA and proposed trade pacts with Pacific Rim countries and the European Union, which would cover nearly two-thirds of global trade.

But he clearly has further to go.

**Congress is moving to restrict other areas of cyber operations**

**Fox News 12/30**, 2013 Cyberwar Takes Center Stage in Defense Budget http://www.military.com/daily-news/2013/12/30/cyberwar-takes-center-stage-in-defense-budget.html

The $552.1 billion defense budget **approved by Congress** calls for **new regulations on cyberweapons** -- an effort to prevent the pervasive digital bombs from further spreading throughout the world -- at the same time that it dramatically boosts spending on them.

Section 940 of the National Defense Authorization Act for Fiscal Year 2014, signed into law by President Obama Thursday night, calls for "Control of the Proliferation of Cyber Weapons" following increases in the clear and present danger from cyberbombs such as Stuxnet and growing teams of hackers in foreign countries.

"The President shall establish an interagency process to provide for the establishment of an integrated policy to control the proliferation of cyber weapons through unilateral and cooperative law enforcement activities, financial means, diplomatic engagement, and such other means as the President considers appropriate," the act declares. The goal of the $2 million Cyber Security Initiative: suppressing the trade in cyber tools and infrastructure that can be used for criminal, terrorist and military activities, while still allowing governments to use those tools in legitimate self-defense.

#### Logical policy maker could vote aff and pass the TPA. Disads must be an opportunity cost.

#### No fast track - Reid

NBC NEWS 1 – 30 – 14 <http://firstread.nbcnews.com/_news/2014/01/30/22507048-congress-health-care-debt-ceiling-immigration-on-gop-retreat-agenda?lite>

Harry Reid and Barack Obama are not on the same page on trade. Political Wire: “Senate Majority Leader Harry Reid (D-NV) ‘broke publicly with the White House Wednesday on trade policy, instantly imperiling two major international trade deals and punching a hole in one piece of the economic agenda the president outlined in his State of the Union address a day earlier,’ the Wall Street Journal reports. Said Reid: ‘I'm against fast track. I think everyone would be well-advised just not to push this right now.’”

#### NO TPA – lacks support – Reid won’t allow a vote

MARKETWATCH 1 – 22 – 14 [Congress won’t give Obama blank check on trade deals, <http://www.marketwatch.com/story/congress-wont-give-obama-blank-check-on-trade-deals-2014-01-22?link=MW_latest_news>]

Congress won’t give Obama blank check on trade deals

The proposed new trade agreement between the U.S. and several Pacific Rim countries may be the boon that advocates say it is, or it may be the corporate sellout described by its opponents.

One thing it should not be, however, is a fait accompli.

Supporters say the Trans-Pacific Partnership currently being negotiated among 12 countries will affirm or broaden existing agreements that will smooth the path of U.S. exports to this region while providing safeguards for intellectual property.

Detractors say the agreement has little to do with expanding trade and more with weakening labor and environmental standards through a back-door race to the bottom.

Both may be right, but the issues are certainly controversial enough to merit debate.

That is not what the administration is seeking, however, as it asks for fast-track authority to get the eventual agreement through Congress with a simple up-or-down vote — no debate, no amendments, no second thoughts.

The conventional wisdom is that trade agreements are so complex and delicately balanced after sensitive negotiations over months and years that letting Congress muck around with it would make it impossible to ever get a trade pact finished.

So instead Congress is invited, on behalf of the American people, to buy a pig in a poke.

The administration is saying, as have previous administrations that sought and won fast-track authority, “Trust me.”

The problem is that trust is not a very plentiful commodity in today’s Washington. President Barack Obama’s low approval ratings are evidence that, after his misfires on health care, budget, immigration and foreign policy, neither Democrats nor Republicans are eager to give him a blank check for trade or anything else.

While a bill introduced earlier this month to grant Obama trade promotion authority is labeled “bipartisan,” that fig leaf comes only from including Sen. Max Baucus as sponsor, though the Montana Democrat will be leaving the Senate soon to take up his appointment as ambassador to China.

No other Democrats in the House or Senate are lending their names to the bill, complaining that it does too little to keep lawmakers informed about negotiations or let them provide input.

The only other Senate sponsor so far is Orrin Hatch, R-Utah, ranking member of the Senate Finance Committee. The bill was introduced in the House by Rep. Dave Camp, R-Mich., chairman of the House Ways and Means Committee, and he has so far found only two other Republican congressmen to get on board.

It’s hard to square an agenda of boosting American wages, including the minimum wage, with introducing new competition with low-wage countries.

A dozen senators in the Democratic caucus wrote a letter to Senate Majority Leader Harry Reid of Nevada calling fast-track authority as described in the Camp-Baucus bill “outdated and inadequate,” and Reid indicated that no TPA bill would be coming to the Senate floor any time soon, given the controversy.

Obama is expected to bring up the trade pacts once again in his State of the Union address next week because he views both TPP and the Transatlantic Trade and Investment Partnership as potentially signature accomplishments for his legacy.

But it looks increasingly like he will be faced with a stark choice — he must abandon plans to get a classic fast-track approval and opt for a more consultative process, or forget about any wide-ranging trade agreements.

#### Fiat solves the link – plan passes immediately, means no backlash.

#### Obama’s capitals irrelevant

ECONOMIST 1 – 30 – 14 [Clowns to the left, jokers to the right, <http://www.economist.com/blogs/democracyinamerica/2014/01/barack-obama>]

It's obvious why Mr Obama's wry, pedagogical tone angers Republicans. Increasingly, though, it also angers Democrats, who are tired of having to throw their weight behind the president's call for reasonable compromise. Over the past three years, America's political system has descended into all-out partisan warfare. Democrats want a general in that fight; they are increasingly dissatisfied that their leader has to spend his rhetorical energy playing the role of the UN envoy calling on all sides to exercise restraint. Since the day after his re-election, pundits have been calling on Mr Obama to act more like LBJ: take strong ideological positions, propose major legislation, twist arms off and beat people's heads in with them (in Senator Russell's immortal words), and so forth. (Our Lexington argued that case a few months back.) Earlier this month Isaac Chotiner bemoaned the president's habit of forever presenting both sides of every argument, accusing him of "talk[ing] to us like we're children": "It's as if the reader can't be trusted to just hear one side from the president, because that might (heaven forbid) make him or her think Obama hasn't considered every angle."

I find this argument unpersuasive. Ed Luce made the key point a year and a half ago: LBJ had liberal Republicans and conservative Democrats to work with, whose decision about whether to vote with or against the president on different bills could be influenced by a variety of political considerations. Those legislative cross-loyalties don't exist anymore. Neither do earmarks, the budget goodies targeted to individual districts that were once a widespread currency of congressional dealmaking (something we lamented here). The parties today are ideologically sorted, and there is almost nothing Mr Obama can do to convince or compel Republicans to vote with him. Republicans are able to halt the president's agenda in its tracks, and they have every reason to do so. There simply isn't any reason to believe that more aggressive legislative arm-twisting would have generated more success for Mr Obama; it seems entirely possible that if he had aggressively tried to dictate the terms of health-care reform legislation rather than allowing various senators to rewrite (and weaken) the bill, he might have lost even that signature achievement. Last year, Mr Obama decided to throw his entire weight behind gun-control legislation, taking on just the sort of ambitious and improbable crusade Mr Ignatius had advised him to attempt. The result was that he lost, squandered political capital, and mired his party in the mud.

The fact is that, as unsatisfying as it may be for his partisans, Mr Obama's above-the-fray stance is his best political play. It taps into his natural character strengths and practiced rhetorical gestures. It safeguards him from being side-lined as a marginal, extremist figure by the media and commentariat—always a danger for black politicians who embrace strong ideological agendas. It allows him to take up themes like inequality and help bring them into the mainstream once they have been advanced by more ideological players.

Obama won’t fight the plan

Stirewalt 9/10/13 [Chris, digital politics editor for Fox News, Can Obama take credit for his own defeat?, http://www.foxnews.com/politics/2013/09/10/can-obama-take-credit-for-his-own-defeat/]

It was going to be big news because it was going to be just the sort of thing Obama almost never does. Risking his political capital on an unpopular policy hasn’t really been Obama’s bag since his health law creaked over the finish line in 2010. Once ObamaCare was on the books, the idea was to just survive past re-election. And then, once re-elected, to just get through midterms.

Obama’s hyper-reactive, base-nuzzling brand of politics forbids much risk taking.

On national security, Obama has been particularly unwilling to take ownership**.** He abandoned his goldilocks surge strategy for Afghanistan on the nation’s doorstep, waved away concerns about his huge expansions of domestic spying and mostly sidestepped his own intervention in Libya**,** particularly once American-backed Islamists there turned on their benefactors last year.

Ending unpopular wars or announcing the death of the world’s most hated man? Obama’s your man. Defending his own national security policies? Better call John McCain.

Capital theory is wrong

Hirsh 2/7/13 [Michael, Chief correspondent for National Journal, Previously served as the senior editor and national economics correspondent for Newsweek, Overseas Press Club award for best magazine reporting from abroad in 2001 and for Newsweek’s coverage of the war on terror which also won a National Magazine Award, There’s No Such Thing as Political Capital, http://www.nationaljournal.com/magazine/there-s-no-such-thing-as-political-capital-20130207]

But the abrupt emergence of the immigration and gun control issues illustrates how suddenly shifts in mood can occur and how political interests can align in new ways just as suddenly. Indeed, the pseudo-concept of political capital masks a larger truth about Washington that is kindergarten simple: You just don’t know what you can do until you try. Or as Ornstein himself once wrote years ago, “Winning wins.” In theory, and in practice, depending on Obama’s handling of any particular issue, even in a polarized time, he could still deliver on a lot of his second-term goals, depending on his skill and the breaks. Unforeseen catalysts can appear, like Newtown. Epiphanies can dawn, such as when many Republican Party leaders suddenly woke up in panic to the huge disparity in the Hispanic vote.

Some political scientists who study the elusive calculus of how to pass legislation and run successful presidencies say that political capital is, at best, an empty concept, and that almost nothing in the academic literature successfully quantifies or even defines it. “It can refer to a very abstract thing, like a president’s popularity, but there’s no mechanism there. That makes it kind of useless,” says Richard Bensel, a government professor at Cornell University. Even Ornstein concedes that the calculus is far more complex than the term suggests. Winning on one issue often changes the calculation for the next issue; there is never any known amount of capital. “The idea here is, if an issue comes up where the conventional wisdom is that president is not going to get what he wants, and he gets it, then each time that happens, it changes the calculus of the other actors” Ornstein says. “If they think he’s going to win, they may change positions to get on the winning side. It’s a bandwagon effect.”

**And, China will shut down the US grid and invade Taiwan**

Derene 9 [Glenn – Defense Analyst @ Popular Mechanics, “How Vulnerable is U.S. Infrastructure to a Major Cyber Attack?” October 1, 2009, http://www.popularmechanics.com/technology/military/4307521]

The next world war might not start with a bang, but with a blackout. An enemy could send a few lines of code to control computers at key power plants, causing equipment to overheat and melt down,plunging sectors of the U.S**.** and Canadian grid into darkness. Trains could roll to a stop on their tracks, while airport landing lights wink out and the few traffic lights that remain active blink at random. In the silence and darkness, citizens may panic, or they may just sit tight and wait for it all to reboot. Either way, much of the country would be blind and unresponsive to outside events. And that might be the enemy's objective: Divert America's attention while mounting an offensive against another country. Pentagon planners have long understood the danger of cyber attacks on U.S. military networks. Indeed, theDefense Department's Global Information Grid is one of the most frequently targeted computer networks on Earth. But the cat-and-mouse game of information espionage on military networks is not the only digital threat that keeps national-security experts up at night. There is a growing concern over the vulnerability of far more tangible assets essential to the economy and well-being of American citizens. Much of the critical infrastructure that keeps the country humming--water-treatment facilities, refineries, pipelines, dams, the electrical grid--is operated using a hodgepodge of technologies known as industrial control systems. Like banks and telecommunications networks, which are also generally considered critical infrastructure, these industrial facilities and utilities are owned by private companies that are responsible for maintaining their own security. But many of the control systems in the industrial world were installed years ago with few or no cyber-security features. That wasn't a big problem when these systems were self-contained. But in the past two decades, many of these controls have been patched into company computer networks, which are themselves linked to the Internet. And when it comes to computer security, a good rule of thumb is that any device that is computer-controlled and networked is vulnerable to hacking. Bad-guy hackers pulling the plug on public utilities is a common theme of Hollywood films, including 2007's Live Free or Die Hard, but such scenarios present more than a mere fictional scare to U.S. intelligence officials. According to Melissa Hathaway, cyber-coordination executive for the Office of the Director of National Intelligence, the list of potential adversaries in a cyber attack is long, ranging from disgruntled employees to criminals to hostile nations. Most experts agree that China and Russia routinely probe our industrial networks, looking for information and vulnerabilities to use as leverage in any potential dispute. James Lewis, a cyber-security expert for the policy think tank Center for Strategic and International Studies (CSIS), says that although cyberwarfare couldn't cripple the U.S., it could serve as an effective military tactic. "If I were China, and I were going to invade Taiwan," he says, "and I needed to complete the conquest in seven days, then it's an attractive option to turn off all the electricity, screw up the banks and so on." Could the entire U.S. grid be taken down in such an attack? "The honest answer is that we don't know," Lewis says. "And I don't like that answer."

**Annexation causes a South China Sea conflict**

**Tucker 2** [Nancy Bernkopf, The Washington Quarterly, If Taiwan Chooses Unification, Should the United States Care?, Summer 2002]

In practical terms, concern about a future threat from China encompasses the strategic advantages that unification with Taiwan would bring to Beijing. Probably more significant than any other factor, by eliminating China’s needs to build toward a hostile takeover of Taiwan, to protect itself from Taiwan, and to plan for a potential conflict with the United States over Taiwan, unification could release a significant percentage of China’s resources. The People’s Liberation Army (PLA) would be free to change its priorities, redeploy its forces, and reconceptualize its strategic objectives. For Washington, this change means a less predictable, more flexible, and potentially less-burdened opponent, though one still noted for its lack of transparency. Beijing’s recovery of Taiwan could in fact lead to a more significant projection of Chinese naval and air power beyond coastal waters. With the continuing need to manage a maritime frontier that includes disputed interests in the South China Sea, China might be tempted to contest the U.S. military presence in the region and strive for greater force-projection capabilities. Although China has pledged that Taiwan under “one country, two systems” will retain its own autonomous military and that the PLA will not station units on the island, no absolute guarantees are protecting crucial sea lanes carrying oil and other sensitive goods past Taiwan. Commercial channels from the South China Sea do not generally pass through the Taiwan Strait but do parallel the east coast of Taiwan, coming as close as 75 nautical miles, as ships travel north toward Japan, Korea, and Russia. These transportation routes would be more vulnerable to interruption by China if Taiwan were under Beijing’s control. Indeed, China has at times been less than scrupulous about respecting international waters. Angered by Canberra’s support for Washington in the EP-3 spy plane crisis in 2001, China harassed an Australian naval flotilla, claiming it had intruded into Chinese waters as it sailed through the Taiwan Strait, even though the strait is an international waterway under the United Nations Law of the Sea Convention.8 As former U.S. ambassador to China James R. Lilley has noted, Taiwan “is the cork in China’s bottle.” China’s reclamation of Taiwan would “end what China feels to be a blockade on its abilities to control its surrounding seas.” With Taiwan in mainland hands, Lilley observes, Beijing could diminish the potential vulnerability it feels because “as much as 50 percent of China’s economy depends on foreign trade, about 90 percent of which is transported by ship.”9 In addition, the enhancement of Beijing’s maritime security would almost certainly alarm Japanese military planners. A Chinese presence along Japan’s shipping routes and abutting its Ryukyu island chain would risk giving Beijing an opportunity to “strangle the world’s second-largest economy.” Further, China would gain greater proximity to disputed oil and natural gas fields in the Senkaku/Diaoyutai area. During the 1996 Taiwan Strait crisis, when Tokyo and Washington were revising their defense agreements to clarify mutual obligations, China’s aggressive use of missiles led the normally cautious Japanese to agree to a tougher set of commitments than first intended. Tokyo sought to make clear to Beijing that neither intimidating Taiwan nor disturbing the peace in areas around Japan was acceptable.

**The impact is nuclear war**

**Wittner 11** [Lawrence S. Wittner, Emeritus Professor of History at the State University of New York/Albany, Wittner is the author of eight books, the editor or co-editor of another four, and the author of over 250 published articles and book reviews, from 1984 to 1987, he edited Peace & Change, a journal of peace research., 11/28/2011, "Is a Nuclear War With China Possible?", [www.huntingtonnews.net/14446](http://www.huntingtonnews.net/14446)]

While nuclear weapons exist, there remains a danger that they will be used. After all,for centuries national conflicts have led to wars, with nations employing their deadliest weapons**.** The current deterioration of U.S. relations with China might end up providing us with yet another example of this phenomenon.The gathering tension between the United States and China is clear enough. Disturbed by China’s growing economic and military strength,the U.S. government recently challenged China’s claims in the South China Sea,increasedthe U.S.military presencein Australia,and deepened U.S. military ties with other nations in the Pacific region. According to Secretary of State Hillary Clinton, the United States was “asserting our own position as a Pacific power.” Butneed this lead to nuclear war?Not necessarily. Andyet**,** there are signs that it could.After all,both the United States and China possess large numbers of nuclear weapons.The U.S. government threatened to attack China with nuclear weapons during the Korean War and, later, during the conflict over the future of China’s offshore islands, Quemoy and Matsu. In the midst of the latter confrontation, President Dwight Eisenhower declared publicly, and chillingly, that U.S. nuclear weapons would “be used just exactly as you would use a bullet or anything else.” Of course, China didn’t have nuclear weapons then. Now that it does, perhaps the behavior of national leaders will be more temperate. But the loose nuclear threats of U.S. and Soviet government officials during the Cold War, when both nations had vast nuclear arsenals, should convince us that, even as the military ante is raised, nuclear saber-rattling persists.Some pundits argue that nuclear weapons prevent wars between nuclear-armed nations; and, admittedly, there haven’t been very many—at least not yet.But the Kargil Warof 1999,betweennuclear-armedIndia andnuclear-armedPakistan**,** should convince us that such wars can occur. Indeed,in that case, the conflict almost slipped into a nuclear war.Pakistan’s foreign secretary threatened that, if the war escalated, his country felt free to use “any weapon” in its arsenal. During the conflict, Pakistan did move nuclear weapons toward its border, while India, it is claimed, readied its own nuclear missiles for an attack on Pakistan. At the least, though,don’t nuclear weapons deter a nuclear attack? Do they?Obviously**,** NATO leaders didn’t feel deterred, for,throughout the Cold War, NATO’s strategy was to respond to a Soviet conventional military attack on Western Europe by launching a Western nuclear attack on the nuclear-armed Soviet Union. Furthermore,if U.S. government officials really believed that nuclear deterrence worked, they would not have resorted to championing “Star Wars” and its modern variant, national missile defense.Why are these vastly expensive—and probably unworkable—military defense systems needed if other nuclear powers are deterred from attacking by U.S. nuclear might? Of course,the bottom line for those Americans convinced that nuclear weapons safeguard them from a Chinese nuclear attack might be that the U.S. nuclear arsenal is far greater than its Chinese counterpart.Today, it is estimated that the U.S. government possesses over five thousand nuclear warheads, while the Chinese government has a total inventory of roughly three hundred. Moreover, only about forty of these Chinese nuclear weapons can reach the United States. Surely the United States would “win” any nuclear war with China. But what would that “victory” entail?A nuclear attack by China would immediately slaughter at least 10 million Americans in a great storm of blast and fire, while leaving many more dying horribly of sickness and radiation poisoning.The Chinese death toll in a nuclear war would be far higher**.** Both nations would be reduced to smoldering, radioactive wastelands. Also,radioactive debris sent aloft by the nuclear explosions would blot out the sun and bring on a “nuclear winter” around the globe—destroying agriculture, creating worldwide famine, and generating chaos and destruction.Moreover, in another decade the extent of this catastrophe would be far worse.The Chinese government is currently expanding its nuclear arsenal, and by the year 2020 it is expected to more than double its number of nuclear weapons that can hit the United States.The U.S. government, in turn,has plans to spend hundreds of billions of dollars “modernizing” its nuclear weaponsand nuclear production facilities over the next decade.To avert the enormous disaster of a U.S.-China nuclear war**,** there are two obvious actions that can be taken. The first is to get rid of nuclear weapons, as the nuclear powers have agreed to do but thus far have resisted doing. The second, conducted while the nuclear disarmament process is occurring, is toimprove U.S.-China relations**.** If the American and Chinese people are interested in ensuring their survival and that of the world, they should be working to encourage these policies**.**

### 2ac – T Restriction

**We meet the Taylor evidence --- it says “permission granted” is authority --- the aff gives permission to the DOD to conduct OCOs**

**We meet --- Obama can only conduct operations after he gets Congressional approval --- it’s binding consultation which means it’s prohibited in some cases**

**Restriction means a limit or qualification, and includes conditions on action**

CAA 8 [COURT OF APPEALS OF ARIZONA, DIVISION ONE, DEPARTMENT A, STATE OF ARIZONA, Appellee, v. JEREMY RAY WAGNER, Appellant., 2008 Ariz. App. Unpub. LEXIS 613]

P10 The term "restriction" is not defined by the Legislature for the purposes of the DUI statutes. See generally A.R.S. § 28-1301 (2004) (providing the "[d]efinitions" section of the DUI statutes). In the absence of a statutory definition of a term, we look to ordinary dictionary definitions and do not construe the word as being a term of art. Lee v. State, 215 Ariz. 540, 544, 15, 161 P.3d 583, 587 (App. 2007) ("When a statutory term is not explicitly defined, we assume, unless otherwise stated, that the Legislature intended to accord the word its natural and obvious meaning, which may be discerned from its dictionary definition.").

P11 The dictionary definition of "restriction" is "[a] limitation or qualification." Black's Law Dictionary 1341 (8th ed. 1999). In fact, "limited" and "restricted" are considered synonyms. See Webster's II New Collegiate Dictionary 946 (2001). Under these commonly accepted definitions, Wagner's driving privileges were "restrict[ed]" when they were "limited" by the ignition interlock requirement.Wagner was not only [\*7] statutorily required to install an ignitioninterlock device on all of the vehicles he operated, A.R.S. § 28-1461(A)(1)(b), but he was also prohibited from driving any vehicle that was not equipped with such a device, regardless whether he owned the vehicle or was under the influence of intoxicants, A.R.S. § 28-1464(H). These limitations constituted a restriction on Wagner's privilege to drive, for he was unable to drive in circumstances which were otherwise available to the general driving population. Thus, the rules of statutory construction dictate that the term "restriction" includes the ignition interlock device limitation.

**Statutory restrictions include 5 things**

Kaiser 80 [The Official Specialist in American National Government, Congressional Research Service, the Library of Congress, Congressional Action to Overturn Agency Rules: Alternatives to the Legislative Veto; Kaiser, Frederick M., 32 Admin. L. Rev. 667 (1980)]

In addition to direct statutory overrides, there are a variety of statutory and nonstatutory techniques that have the effect of overturning rules, that prevent their enforcement, or that seriously impede or even preempt the promulgation of projected rules. For instance, a statute may alter the jurisdiction of a regulatory agency or extend the exemptions to its authority, thereby affecting existing or anticipated rules. Legislation that affects an agency's funding may be used to prevent enforcement of particular rules or to revoke funding discretion for rulemaking activity or both. Still other actions, less direct but potentially significant, are mandating agency consultation with other federal or state authorities and requiring prior congressional review of proposed rules (separate from the legislative veto sanctions). These last two provisions may change or even halt proposed rules by interjecting novel procedural requirements along with different perspectives and influences into the process.

It is also valuable to examine nonstatutory controls available to the Congress:

1. legislative, oversight, investigative, and confirmation hearings;

2. establishment of select committees and specialized subcommittees to oversee agency rulemaking and enforcement; 3. directives in committee reports, especially those accompanying legislation, authorizations, and appropriations, regarding rules or their implementation; 4. House and Senate floor statements critical of proposed, projected, or ongoing administrative action; and 5. direct contact between a congressional office and the agency or office in question. Such mechanisms are all indirect influences; unlike statutory provisions**,** they are neither self-enforcing nor legally binding by themselves. Nonetheless, nonstatutory devices are more readily available and more easily effectuated than controls imposed by statute. And some observers have attributed substantial influence to nonstatutory controls in regulatory as well as other matters.3 It is impossible, in a limited space, to provide a comprehensive and exhaustive listing of congressional actions that override, have the effect of overturning, or prevent the promulgation of administrative rules. Consequently, this report concentrates upon the more direct statutory devices, although it also encompasses committee reports accompanying bills, the one nonstatutory instrument that is frequently most authoritatively connected with the final legislative product. The statutory mechanisms surveyed here cross a wide spectrum of possible congressional action: 1. single-purpose provisions to overturn or preempt a specific rule**;** 2. alterations in program authoritythat remove jurisdiction from an agency; 3. agency authorization and appropriation limitations**;** 4. inter-agency consultation requirements; and 5. congressional prior notification provisions

**C/I is superior --- it’s best for predictability --- our interpretation only allows for 5 mechanisms, which makes for a more manageable topic --- that’s best for limits and pre-round preparation --- and, it’s the best for real world education --- inter-branch consultation is the core of the literature and is how congress has restricted the president in the past**

**Prefer reasonability --- competing interpretations are arbitrary and makes aff prep impossible**

### 2ac – Impt: Warming (Inev)

Warming isn’t inevitable --- we must prevent increases in CO2 to prevent the worst impacts of warming --- that’s Gillis --- even if we have exceeded the tipping point, temporary overshoots are possible

Cook 11—\*an environmental scientist of 35 years’ experience. His PhD ‘The Wilderness Knot’ was in social ecology. \*\* the Climate Communication Fellow for the Global Change Institute at the University of Queensland. He studied physics at the University of Queensland, Australia. After the graduating, he majored in solar physics in his post-grad honors year and created the website skepticalscience.com (John and Haydn Washington, Climate Change Denial: Heads in the Sand, Published in 2011 by Earthscan, Page 30-31)

It has been suggested that warming the world by more than two degrees could push us into the area where we may cause runaway climate change. It may then take thousands of years to get back to current world temperatures. The world has already warmed by .7 degrees Celsius (Houghton, 2008; Pittock, 2009) and another .6 degrees is in the pipeline (Hansen, 2009). Runaway climate change means that human actions would then be unlikely to stop the temperature increase (short of massive government engineering). Hansen et al. (2008) define the ‘tipping point’ as the climate forcing threat that, if maintained for a long time, gives rise to a specific consequence. They define the ‘point of no return’ as a climate state beyond which the consequence is inevitable, even if climate forcings are reduced. A point of no return can be avoided, even if the tipping level is temporarily exceeded. This has been called an ‘overshoot’ scenario, where one exceeds the ‘safe’ CO2 level but then removes CO2 to return to that level (Pittock, 2009). Ocean and ice sheet inertia permit overshoot ‘provided the climate forcing is returned below the tipping level before initiating irreversible dynamic change’ (Hansen et al, 2008). Points of no return are difficult to define. We may be at a tipping level already at 387 ppm CO2, and it will require strong action to reduce CO2 levels so that we don’t pass the point of no return and can return CO2 levels below 350 ppm. Hansen et al (2008) note we may been to drop CO2 below 325 ppm to restore sea ice to the area it had 25 years ago (and so remove this positive feedback).

### 2ac – Grid Add-On

**Grid collapse causes 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.

### 2ac – OLC CP

**Perm do both --- solves the net benefit--- solves the separation of powers net benefit because the CP clarifies authority**

**No link to SOP --- there’s no statute that covers cyber security now**

**Perm do the CP --- the plan-text just says USFG --- the CP is an example of how the plan could be done**

OLC can’t solve and links to politics

Posner 11 Eric Posner is the Kirkland & Ellis Professor, University of Chicago Law School. “DEFERENCE TO THE EXECUTIVE IN THE UNITED STATES AFTER 9/11 CONGRESS, THE COURTS AND THE OFFICE OF LEGAL COUNSEL” available at http://www.law.uchicago.edu/academics/publiclaw/index.html.

These two events neatly encapsulate the dilemma for OLC, and indeed all the president’s legal advisers. If OLC tries to block the president from acting in the way he sees fit, it takes the risk that he will disregard its advice and marginalize the institution. If OLC gives the president the advice that he wants to hear, it takes the risk that it will mislead him and fail to prepare him for adverse reactions from the courts, Congress, and the public. Can OLC constrain the executive? That is the position taken by many scholars, most notably Jack Goldsmith. 18 The underlying idea here is that even if Congress and the courts cannot constrain the executive, perhaps offices within the executive can. The opposite view, advanced by Bruce Ackerman, is that OLC is a rubber stamp. 19 I advocate a third view: OLC does not constrain the executive but enables him to accomplish goals that he would not otherwise be able to accomplish. It is more accurate to say that OLC enables than constrains. B. OLC as a Constraint on the Executive A number of scholars have argued that OLC can serve as an important constraint on executive power. I will argue that OLC cannot act as a constraint on executive power. Indeed, its only function is the opposite—as an “enabler” (as I will put it) or extender of executive power. A president must choose a course of action. He goes to OLC for advice. Ideally, OLC will provide him good advice as to the legality of the course of action. It will not provide him political advice and other relevant types of advice. The president wants to maximize his political advantage, 21 and so he will follow OLC’s advice only if the legal costs that OLC identifies are greater than the political benefits. On this theory, OLC will properly always give the president neutral advice, and the president will gratefully accept it although not necessarily follow it. If the story ended here, then it would be hard to see what the controversy over OLC could be about. As an adviser, it possesses no ability to constrain the executive. It merely provides doctrinal analysis, in this way, if it does its job properly, merely supplying predictions as to how other legal actors will react to the president’s proposed action. The executive can choose to ignore OLC’s advice, and so OLC cannot serve as a “constraint” on executive power in any meaningful sense. Instead, it merely conveys to the president information about the constraints on executive power that are imposed from outside the executive branch. However, there is an important twist that complicates the analysis. The president may choose to publicize OLC’s opinions. Naturally, the president will be tempted to publicize only favorable opinions. When Congress 22 claims that a policy is illegal, the president can respond that his lawyers advised him that the policy is legal. This response at least partially deflects blame from the president. There are two reasons for this. First, the Senate consented to the appointment of these lawyers; thus, if the lawyers gave bad advice, the Senate is partly to blame, and so the blame must be shared. Second, OLC lawyers likely care about their future prospects in the legal profession, which will turn in part on their ability to avoid scandals and to render plausible legal advice; they may also seek to maintain the office’s reputation. When OLC’s opinions are not merely private advice, but are used to justify actions, then OLC takes on a quasi-judicial function. Presidents are not obliged to publicize OLC’s opinions, but clearly they see an advantage to doing so, and they have in this way given OLC quasi-judicial status. But if the president publicizes OLC opinions, he takes a risk. The risk is that OLC will publicly advise him that an action is illegal. If OLC approval helps deflect blame from the president, then OLC disapproval will tend to concentrate blame on the president who ignores its advice. Congress and the public will note that after all the president is ignoring the advice of lawyers that he appointed and thus presumably he trusts, and this can only make the president look bad. To avoid such blame, the president may refrain from engaging in a politically advantageous action. In this way, OLC may be able to prevent the president from taking an action that he would otherwise prefer. At a minimum, OLC raises the political cost of the action. I have simplified greatly, but I believe that this basic logic has led some scholars to believe that OLC serves as a constraint on the president. But this is a mistake. OLC strengthens the president’s hand in some cases and weakens them in others; but overall it extends his power—it serves as enabler, not constraint. To see why, consider an example in which a president must choose an action that lies on a continuum. One might consider electronic surveillance. At one extreme, the president can engage in actions that are clearly lawful—for example, spying on criminal suspects after obtaining warrants from judges. At the other extreme, the president can engage in actions that are clearly unlawful—for example, spying on political opponents. OLC opinions will not affect Congress’s or the public’s reaction to either the obviously lawful or the obviously unlawful actions. But then there are middle cases. Consider a policy L, which is just barely legal, and a policy I, which is just barely illegal. The president would like to pursue policy L but fears that Congress and others will mistakenly believe that L is illegal. As a result, political opposition to L will be greater than it would be otherwise. In such a case, a favorable advisory opinion from a neutral legal body that has credibility with Congress will help the president. OLC’s approval of L would cause political opposition (to the extent that it is based on the mistaken belief that L is unlawful) to melt away. Thus, OLC enables the president to engage in policy L, when without OLC’s participation that might be impossible. True, OLC will not enable the president to engage in I, assuming OLC is neutral. And, indeed, OLC’s negative reaction to I may stiffen Congress’ resistance. However, the president will use OLC only because he believes that OLC will strengthen his hand on net. It might be useful to make this point using a little jargon. In order for OLC to serve its ex ante function of enabling the president to avoid confrontations with Congress in difficult cases, it must be able to say “no” to him ex post for barely illegal actions as well as “yes” to him for barely legal actions. It is wrong to consider an ex post no as a form of constraint because, ex ante, it enables the president to act in half of the difficult cases. OLC does not impose any independent constraint on the president, that is, any constraint that is separate from the constraint imposed by Congress. An analogy to contract law might be useful. People enter contracts because they enable them to do things ex ante by imposing constraints on them ex post. For example, a debtor can borrow money from a creditor only because a court will force the debtor to repay the money ex post. It would be strange to say that contract law imposes “constraints” on people because of ex post enforcement. In fact, contract law enables people to do things that they could not otherwise do—it extends their power. If it did not,people would not enter contracts. A question naturally arises about OLC’s incentives. I have assumed that OLC provides neutral advice—in the sense of trying to make accurate predictions as to how other agents like Congress and the courts would reaction to proposed actions. It is possible that OLC could be biased—either in favor of the president or against him. However, if OLC were biased against the president, he would stop asking it for advice (or would ask for its advice in private and then ignore it). This danger surely accounts for the fact that OLC jurisprudence is pro-executive. 23 But it would be just as dangerous for OLC to be excessively biased in favor of the president. If it were, it would mislead the president and lose its credibility with Congress, with the result that it could not help the president engage in L policies. So OLC must be neither excessively pro-president nor anti-president. If it can avoid these extremes, it will be an “enabler”; if it cannot, it will be ignored. In no circumstance could it be a “constraint.” If the OLC cannot constrain the president on net, why have people claimed that OLC can constrain the president? What is the source of this mistake? One possibility, which I have already noted, is that commentators might look only at one side of the problem. Scholars note that OLC may “prevent” the president from engaging in barely illegal actions without also acknowledging that it can do so only if at the same time it enables the president to engage in barely legal actions. This is simply a failure to look at the full picture. For example, in The Terror Presidency, Goldsmith argues that President Bush abandoned a scheme of warrantless wiretapping without authorization from the FISA court because OLC declared the scheme illegal, and top Justice Department officials threatened to resign unless Bush heeded OLC’s advice. 25 This seems like a clear example of constraint. But it is important to look at the whole picture. If OLC had approved the scheme, and subsequently executive branch agents in the NSA had been prosecuted and punished by the courts, then OLC’s credibility as a supplier of legal advice would have been destroyed. For the president, this would have been a bad outcome. As I have argued, a credible OLC helps the president accomplish his agenda in “barely legal” cases. Without taking into account those cases where OLC advice helps the president’s agenda ex post as well as the cases where OLC advice hurts the president’s agenda ex post, one cannot make an overall judgment about OLC’s ex ante effect on executive power. Another possible source of error is that scholars imagine that “neutral” advice will almost always prevent the president from engaging in preferred actions, while rarely enabling the president to engage in preferred actions. The implicit picture here is that a president will normally want to break the law, that under the proper interpretation of the Constitution and relevant standards the president can accomplish very little. So if OLC is infact neutral and the president does obey its advice, then it must constrain the president. But this theory cannot be right, either. If OLC constantly told the president that he cannot do what he wants to do, when infact Congress and other agents would not object to the preferred actions, then the president would stop asking OLC for advice. As noted above, for OLC to maintain its relevance, it cannot offer an abstract interpretation of the Constitution that is divorced from political realities; it has to be able to make realistic predictions as to how other legal agents will react to the president’s actions. This has led OLC to develop a pro-executive jurisprudence in line with the long-term evolution of executive power. If OLC tried to impose constraints other than those imposed by Congress and other institutions with political power, then the president would ignore it.

Only statutory clarification sends a signal of deterrence

Waxman 10/1/13 (Matthew Waxman is a law professor at Columbia Law School, where he co-chairs the Roger Hertog Program on Law and National Security. He is also Adjunct Senior Fellow for Law and Foreign Policy at the Council on Foreign Relations and a member of the Hoover Institution Task Force on National Security and Law. He previously served in senior policy positions at the State Department, Defense Department, and National Security Council. After graduating from Yale Law School, he clerked for Judge Joel M. Flaum of the U.S. Court of Appeals and Supreme Court Justice David H. Souter, “The Constitutional Power to Threaten War” Forthcoming in YALE LAW JOURNAL, vol. 123, 2014, October 1st DRAFT) **\*\*Footnote 213 included**

A second argument, this one advanced by some congressionalists, is that stronger legislative checks on presidential uses of force would **improve deterrent and coercive strategies** by making them more selective and credible. The most credible U.S. threats, this argument holds, are those that carry **formal approval by Congress**, which reflects strong public support and willingness to bear the costs of war; requiring express legislative backing to make good on threats might therefore be thought to enhance the potency of threats by encouraging the President to seek congressional authorization before acting. 181 A frequently cited instance is President Eisenhower’s request (soon granted) for standing congressional authorization to use force in the Taiwan Straits crises of the mid- and late-1950s – an authorization he claimed at the time was important to bolstering the credibility of U.S. threats to protect Formosa from Chinese aggression. 182 (Eisenhower did not go so far as to suggest that congressional authorization ought to be legally required, however.) “It was [Eisenhower’s] seasoned judgment … that a commitment the United States would have much greater impact on allies and enemies alike because it would represent the collective judgment of the President and Congress,” concludes Louis Fisher. “Single-handed actions taken by a President, without the support of Congress and the people, can threaten national prestige and undermine the presidency. Eisenhower’s position was sound then. It is sound now.” 183 A critical assumption here is that legal requirements of congressional participation in decisions to use force filters out unpopular uses of force, the threats of which are unlikely to be credible and which, if unsuccessful, undermine the credibility of future U.S. threats.

A third view is that legal clarity is important to U.S. coercive and deterrent strategies; that ambiguity as to the President’s powers to use force undermines the credibility of threats. Michael Reisman observed, for example, in 1989: “Lack of clarity in the allocation of competence and the uncertain **congressional role** will sow uncertainty among those who depend on U.S**. effectiveness** for security **and the maintenance of world order**. Some reduction in U.S. credibility and diplomatic effectiveness may result.” 184 Such stress on legal clarity is common among lawyers, who usually regard it as important to planning, whereas strategists tend to see possible value in “constructive ambiguity”, or deliberate fudging of drawn lines as a negotiating tactic or for domestic political purposes. 185 A critical assumption here is that clarity of constitutional or statutory design **with respect to decisions about force exerts significant effects on** foreign perceptions of U.S. resolve **to make good on threats, if not by** affecting the substance of U.S. policy **commitments with regard to force then by pointing foreign actors to the appropriate institution or process for reading them.**

Political scientists almost never engage directly on these questions of constitutional design and reform (it is difficult, in fact, to find even passing references to questions of legal doctrine or reform in political science scholarship on threats of force). Partly this may reflect a general scholarly disposition favoring descriptive over normative or prescriptive analysis - the opposite of most American legal scholarship. Partly, though, it also reflects a difference in emphasis between legal scholars and political scientists with respect to democratic institutions. Whereas legal scholars tend to focus on formal legal powers and checks - such as binding legislative control and judicial review -political scientists focus on the political interactions that these institutions facilitate rather than the specific allocations of power among different institutions themselves.186 In other words, they tend to concentrate on the allocation of powers between branches of government only to the extent that such arrangements formalize or provide a forum for political contestation and competition among domestic political opponents. As a result, political scientists rarely examine how the sorts of constitutional and legislative reforms so often put forward by legal thinkers would affect the credibility of threats.

That said, political science contributions in this area suggest that all three views that have appeared in legal debates probably have some truth in some cases, but all three are also exaggerated. They are exaggerated to the extent that they fail to account for the political checks imposed by Congress that presidents already internalize and that foreign actors already perceive; they tend to consider formal legal checks in absolute terms rather than their marginal effects relative to baseline politics, which operate quite robustly as constraints.

Furthermore, anv reading of signals b> foreign audiences would have to take account of the possibility that a President might act outside the law. especially in a grave national security crisis. On balance and in general, though, the political science scholarship surveyed above suggests that a result of stronger formal congressional cheeks on force would probably be restricted reliance on threatened force, but the ensuing would in turn be more credible.

Even if Congress already wields informal political influence over threatened force, more potent and formal requirements of legislative force authorization or stricter enforcement of existing ones would still probably push U.S. policy a narrower set of commitments and more reserved use of threats - a more selective coercive and deterrent strategy - in several ways. For a President, knowing that he requires legally authorization from Congress to carry through on threats raises the expected political costs of making them (even very popular ones would require spending some political capital to obtain formal legislative backing). A more formal and substantial role for Congress in authorizing the carrying out of threats would also probably amplify some of the informational effects of executive-legislative dialogue and congressional debate described in the previous section: these processes - which could become more robust and attract greater attention - make it difficult to conceal or misrepresent preferences about war and peace, and therefore reduce opportunities for bluffing. If stronger legislative checks on war and force likely mean a more narrowly selective policy of threatened force, then the previous sections' analysis also suggests that the credibility of those select threats will probably be enhanced Returning to the Iran example with which this Article began, for example, a Presidents decision to draw a red-line threat would likely send an even more potent signal of resolve if legislation were required ultimately required to carry it out. because it would more clearly communicate likely inter-branch unity behind the threat. As the next Part will explain, whether more narrowly selective - but perhaps more credible - threats would result in an overall improvement from a policy standpoint depends on shifting geopolitical context and other balances in U.S. strategy.

The general point here is that the ultimate effects of any legal reform on war and peace will depend not just on the internal effects on U.S. government decision-making but the external perceptions of actors reading U.S. signals. An agenda for constitutional scholars and political scientists alike would more thoroughly link different internal legal arrangements within democracies to different strategies for using military power, some aspects of which arc outlined in the next Part. One question for future study of interest to both political scientists and legal scholars, for example, is whether Congress is as institutionally suited or inclined as the executive branch to consider the credibility effects of threatened or actual military actions in one case on other or future cases - that is. To take account of and give substantial weight to the signals it sends to other international actors with grants or denials of authorization to use force. A related question critical to considering possible legal reform is whether Congress's inclinations in that regard would shift were it to assume a more significant and sustained formal role in decision-making about war and force - that is. whether any such congressional policy biases are structurally inherent or a function of reigning legal doctrine

III. Constitutional War Powers and American Grand Strategy

One broad implication of this analysis is that the true allocation of constitutional war powers is - in anything but a formalistic sense - geopolitically and strategically contingent. It is often believed that the power to go to war is one of the most important constitutional powers because wars put American blood and treasure at risk.187 But even assuming as a normative matter that this means that our Constitution should be structured to be war-averse, as some constitutional scholars have argued,188 this principle does not provide as much guidance about legal doctrine as often supposed unless integrated with ideas about how the United States can and should pursue that agenda in relation to other actors pursuing theirs and amid a changing international context.

A. Threats of War and Presidential Powers in Historical and Strategic Context

Thinking generally about the "powers of war and peace/" the power to decide to go to war was a much more significant one relative to the power to threaten war - as well as other foreign relations powers - when the United States was a small, militarily-weak power and when our strategy was avowedly to stay out of foreign disputes, or when coercive diplomacy and deterrence that extended to protecting distant allies abroad was not a serious strategic option.189 If a major component of grand strategy is hiding behind geographical barriers and avoiding conflict by not taking sides in disputes among other powers - as it was during the infancy of the Republic and as it was again in the interwar years - then the power to threaten war is not often very consequential and an allocation of powers that makes it difficult to engage in military conflicts or even threaten to do so is consistent with that strategic vision.' Note. too. that the lack of a very potent standing military force during these periods limited options for coercive and deterrent strategies and made the President heavily dependent on Congress to furnish the means to initiate

Because the importance for the United States of threatened force - to coerce or deter adversaries, and to reassure allies - in affecting war and peace grew so substantially after World War II. the constitutional decision-making about using force has been relegated in large degree to a mechanism for implementing grand strategy rather than setting it.192 As a superpower that plays a major role in sustaining global security, threatening war is in some respects a much more policy-significant constitutional power than the power to actually make war.

Moreover, assessing the functional benefits or dangers attendant to unilateral presidential discretion to use force or to formulas for ensuring congressional involvement cannot be separated from the means by which the United States pursues its desired geopolitical ends. Of course those merits are inextricably linked to substantive policy ends associated with its military capacity, such as whether the United States is pursuing an aggressively expansionist agenda, a territorially-defensive one. or something else But it also depends on how it seeks to wield its military power - as much its potential for armed force as its engagement of the enemy with it - toward those ends.

B. Re framing "War Powers" Scholarship

One might object to the main point of this Article - that constitutional allocations of power to use force cannot meaningfully be assessed either descriptively or normatively in other than very formalistic ways without accounting for the way U.S. military power is used - that it falls victim to its own critique: if the American condition of war and peace is determined by more than just decisions to commence hostilities or resist actual force with force, why stop at threats of war and force'' Why not extend the analysis even further, to include the many other presidential powers - like diplomatic communication and recognition, intelligence activities, negotiation, and so on - that could lead also to or affect the course of events in crises?193

This Article has focused on the way presidents wield U.S. military might not because analysis of those powers can be neatly separated from other ones but to show how even widening the lens a little bit reveals a much more complex interaction of law and strategy then often assumed and opens up new avenues for analysis and possible reform Military force is also an important place to start because it has always carried special political and diplomatic salience.194 Moreover, many types of non-military moves a President might take to communicate threats, such as imposing economic sanctions or freezing financial assets.195 rest on express statutory delegations from Congress.196 Military threats, by contrast, often rest primarily on the President's independent constitutional powers, perhaps buttressed by implicit congressional assent, and therefore pose the most fundamental questions of constitutional structure and power allocation in relation to strategy

A next step, though, would incorporate into this analysis other instruments of statecraft, such as covert intervention or economic and financial actions, recognizing that their legal regulation could similarly affect perceptions about U.S. power abroad as well as the political and institutional incentives a President has to rely on one tool versus another. Moreover, sometimes coercive strategies involve both carrots and sticks -threats as well as positive inducements197 - and Congress's powers may be dominant with regard to the latter elements of that formula, perhaps in the form of spending on offered benefits or lifting of economic sanctions.198 Further study might focus on such strategies and the way they necessarily require inter-branch coordination, not only in carrying out those elements but in signaling credibly an intention to do so.

At this point, many legal scholars reading this (yet another) Article on constitutional war powers are bound to be disappointed that it proposes neither a specific doctrinal reformulation nor offers an account of optimal legal-power allocation to achieve desired results One reason for that is that evidence surveyed in Part II is inconclusive with respect to some key questions. Another, however, is that the very quest for optimal allocation of these powers is generally mis-framed, because "optimal" only makes sense in reference to some assumptions about strategy, which are not themselves fixed By tying notions of optimal legal allocations to strategy I do not simply mean the basic point that we need prior agreement on desired ends (in the same sense that economists talk about optimality by assuming goals of maximizing social welfare), but the linking of means to ends. As the Article tries to show throughout, even if one agrees that the desired ends are peace and security. there are many strategies to achieve it - isolation, preventive war. deterrence, and others - and variations among them, depending on prevailing geopolitical conditions.

A more productive mode of study, then, recognizes the interdependence of the allocation of war-related powers and the setting of grand strategy. Legal powers and institutions enable or constrain strategies, and they also provide the various actors in our constitutional system w ith levers for shaping those strategies. At the same time, some strategies either reinforce or destabilize legal designs.

C. Threats, Grand Strategy, and Future Executive-Congressional Balances

Having homed in here on threatened war or force, one might take from this analysis yet another observation about the expanding or constitutionally "imperial" power of the U.S. President. That is, beyond the President's wide latitude to use military force abroad, he can take threatening steps that could provoke or prevent war and even alter unilateral the national interests at stake in a crisis by placing U.S. credibility on the line -the President's powers of war and peace are therefore even more expansive than generally supposed

It is also important to see this analysis, however, as showing more complex dependency of presidential powers on Congress with respect to setting and sustaining American grand strategy. In that respect, Philip Bobbitt was quite correct when he decried lawyers' undue emphasis on the Declare War clause and the commencement of armed hostilities as the critical legal events in thinking about constitutional allocations and U.S. security policy:

Wars rarely start as unexpected ambushes; they are usually the culmination of a long period of policy decisions. & If we think of the declaration of war as a commencing act - which it almost never is and which the Framers did not expect it to be - we will not scrutinize those steps that bring us to war, steps that are in the main statutory in nature. Moreover, we will be inclined to pretend & that Congress really has played no role in formulating and funding very specific foreign and security policies.199

Those foreign and security policies to which Bobbitt refers include coercive and deterrent strategies.

Indeed- it is important to remember that the heavy reliance on threatened force especially after World War II has itself been a strategic choice by the United States - not a predestined one - and one that could only be made and continued with sustained congressional support. Since the beginning of the Cold War period, the reliance on deterrence and coercive diplomacy became so deeply engrained in U.S. foreign policy that it is easy to forget that the United States had other strategic options open to it. One option was war: some senior policy-makers during the early phases of the Cold War believed that conflict with the Soviet Union was inevitable, so better to seize the initiative and strike while the United States held some advantages in the balance of strength. Another option was isolation: the United States could have retracted it security commitments to its own borders or hemisphere, as it did after World War I, ceding influence to the Soviet bloc or other political forces/01 These may have been very bad alternatives, but they were real ones and they were rejected in favor of a combination of standing threats of force and discrete threats of force - sometimes followed up with demonstrative uses of force - that was only possible with congressional buy-in. That buy-in came in the form of military funding for the standing forces and foreign deployments needed to maintain the credibility of U.S. threats, as well as in Senate support for defense pacts with allies. While a strategy of deterrent and coercive force has involved significant unilateral discretion as to how and when specifically to threaten military action in specific crises and incidents, the overall strategy rested on a foundation of executive-congressional collaboration and dialogue that played out over decades.

Looking to the future, the importance of threatened force relative to other foreign policy instruments will shift - and so, therefore, will the balance of powers between the President and Congress. United States grand strategy for the coming decades will be shaped by conditions of fiscal austerity, for example, which may mean cutting back on some security commitments or reorienting doctrine for defending them toward greater reliance on less-expensive means (perhaps such as a shift from large-scale military forces to smaller ones, or **greater reliance on high-technology**, or even revised doctrines of nuclear deterrence).

One possible geostrategic outlook is that the United States will retain its singular military dominance, and that it will continue to play a global policing role. Another outlook, though, is that U.S. military dominance will be eclipsed by other rising powers and diminished U.S. resources and influence." The latter scenario might mean that international relations will be less influenced by credible threats of U.S. intervention, and perhaps more so by the actions of regional powers and political bodies, or by institutions of global governance like the UN Security Council." These possibilities could entail a practical rebalancing of powers wielded by each branch, including the pow er to threaten force and other foreign policy tools.

Were the United States to retreat from underw riting its allies' security and some elements of global order with strong coercive and deterrent threats, one should expect different patterns of executive-congressional behavior with respect to threatening and using force, because wars and threats of wars will come about in different ways: less often as a breakdown of U.S. hegemonic commitments, for example. Reduced requirements of maintaining credible U.S. threats, and therefore reduced linkage between U.S. actions in one crisis and others, would also likely reduce pressure on the President to protect prerogatives to threaten force and to make good on those threats. A foreign policy strategy of more selective and reserved military engagement would likely be one more accommodating to case-by-case, joint executive-legislative deliberation as to the threat or use of U.S. military might, insofar as U.S. strategy would self-consciously avoid cultivating foreign reliance on U.S. power.

Besides shifting geostrategic visions, ranging from a global policing role to receding commitments, the set of tools available to Presidents for projecting power will evolve, too, as will the nature of security threats, and this will produce readjustments among the relative importance of constitutional powers and inter-branch relations.

Transnational terrorist threats, for example, are sometimes thought to be impervious to deterrent threats, whether because they may hold nihilistic agendas or lack tangible assets that can be held at risk. 06 Technologies like unmanned drones may make possible the application of military violence with fewer risks and less public visibility than in the past/ While discussion of these developments as revolutionary is in vogue, they are more evolutionary and incremental; their purported effects are matters of degree. Such developments will, however, retune strategies for brandishing and exercising military capabilities and the politics of using them.

Whatever the future of U.S. power and strategies for wielding it, the analysis above points toward **a revised war powers reform agenda**. If legal discourse of war powers is too narrowly focused on actual wars and forceful military engagements to the exclusion of threats of them, then so too is discussion of reforms too narrowly focused on congressional involvement at the end stages of coercive diplomacy - often long after threats have been issued and responded to, positively or negatively - rather than at earlier ones.

A more productive agenda (and by no means a mutually exclusive one) would focus on strengthening Congress's role in the shaping of U.S. grand strategy more broadly - that rather than devoting its institutional energy to reasserting it control over decisions to engage the enemy with military force in particular circumstances, it would work to engage the executive branch more seriously and continually on the general policy circumstances under which force might be contemplated. This would mean Congress doing something it is not disposed toward, which is using its other powers - such as hearings, control of funds,statutory delegations of bounded policy discretion - to engage the executive branch on strategic questions inadvance of or at the earliest stages of crises about the way force may be wielded**. Proposals to restructure congressional national security committees - such as creating more** consolidated, joint House-Senate national security committee, to give them more leverage, expertise, and oversight responsibility that ties together the elements of U.S. power **213 213 See KOH, supra note , at 167-68; NATIONAL WAR POWERS COMMISSION REPORT 36-37 (2008). -** should be viewed not simply as a means for consulting with the Executive once large-scale military intervention is imminent, but for consulting on the matching of foreign policy means and ends well in advance of crises.

**CP is a VI --- it’s object fiat --- they change the position of the thing we are trying to restrict --- that ruins aff ground --- and it abuses the literature which only exists because of an abusive executive --- they can have a CP that does a different restriction to solve --- that ensures clash**

**No solvency --- only plan gives the president political cover and legitimacy for launching more offensive cyber operations**

**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]

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 choicewhen 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 outagainst 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.

**Conditionality is a VI --- it skews 2AC strategy because the block can kick the least covered position --- and, it disadvantages the 1AR versus the block because of the neg’s time advantage --- kills fairness --- it also kills decision-making skills because it encourages the neg to go for the least covered position**

Doesn’t solve legal clarity OR president ignores

Posner 11 Eric Posner is the Kirkland & Ellis Professor, University of Chicago Law School. “DEFERENCE TO THE EXECUTIVE IN THE UNITED STATES AFTER 9/11 CONGRESS, THE COURTS AND THE OFFICE OF LEGAL COUNSEL” available at http://www.law.uchicago.edu/academics/publiclaw/index.html.

C. Evidence

1. Testing the Three Hypotheses

We have three hypotheses about OLC on the table. The first is that OLC is an ex ante constraint on presidential power, serving a role similar to thatof Congress and the courts. The second is that OLC is an ex ante enabler of presidential power. The third hypothesis is Ackerman’s rubber-stamp theory that OLC serves neither as a constraint nor as an enabler because it cannot say no ex post. In this section, I will briefly discuss the evidence. It is easy enough to distinguish Ackerman’s hypothesis from the other two: if OLC never or rarely says no, then Ackerman is right. In addition, Ackerman is right even if OLC sometimes says no but the president ignores OLC in those cases. Distinguishing the constraint and enabler hypotheses is more difficult. Both hypotheses predict some ex post no’s. To distinguish the hypotheses, one would need to look at the other side of the ledger: the cases where OLC has enabled the president to act where otherwise Congress would have opposed him. Unfortunately, it would be hard to identify such cases. 2. Statistical Evidence In a study of the written opinions of OLC, Trevor Morrison found that 79 percent approved the president’s position, 8 percent provided a mixed answer, and 13 percent disapproved the president’s position. 26 In several cases, OLC rejected the White House position on issues of significance. In addition, Morrison notes that since OLC usually provides negative advice orally, the written record reflects a selection bias in favor of approvals. 27 But there is less here than meets the eye. First, one must keep in mind that the executive is a “they,” not an “it.” When the president cannot resolve policy differences among his major advisers, he may well be indifferent about OLC’s reaction and indeed welcome a legal resolution (“sorry, my hands are tied”). Second, the relevant focus, for the purpose of my argument, is OLC advice on national security issues. On this topic, the consensus appears to be that OLC has said no to the executive in only four cases in its entire history aside from matters that remain classified: the rejection of the Bush administration’s argument that the Geneva Conventions do not apply to terrorists in Iraq in 2002; 28 the rejection of certain forms of coercive interrogation in 2003; rejection of electronic surveillance that circumvented the FISA court in 2003; and rejection of the Libya intervention in 2011. 2 Even these cases turn out to be ambiguous. It must be recalled that OLC first said “yes” on coercive interrogation and electronic surveillance, and then changed its mind a few years later. In addition, OLC’s “no” on coercive interrogation turned out to be less than absolute: it continued to authorize waterboarding even after the earlier memorandum was withdrawn. Unfortunately, evaluating the empirical evidence is even harder than Morrison indicates. The problem is not just that negative advice is confidential; the problem is that we do not know how the executive responded to this negative advice. Did it desist from its conduct? Modify it along the margins? Or ignore OLC? Maybe, maybe not. A further methodological problem concerns whether a “no” blocks an important policy or simply requires certain i’s to bedotted or t’s to be crossed. OLC officials often emphasize that their job is to help the White House find a legally acceptable method of accomplishing their aims. Even the early Bush administration OLC drew the line on certain forms of torture (such as mock executions, the use of insects to exploit fears, etc.) and established guidelines to ensure the safety of detainees. The problem with treating this advice as a “no” is that it is not clear that the executive cared about these details, as opposedto the broad agenda of using coercive interrogation practices. It no doubt wanted legal advice so as to minimize the risk of legal liability. Finally, as we have seen, President Obama ignored OLC’s position on the Libya intervention. So in that case, OLC took a brave stand and then discovered that it had been pushed to the sidelines. This major event offered unusuallyrapid confirmation of Ackerman’s claim that the executive can avoid negative advice from OLC by soliciting advice from the White House Counsel’s Office. (Obama also received favorable advice from the State Department legal counsel.) Morrison argued prior to this event that the president faces strong disincentives to end-running OLC. 30 Afterwards, he could only criticize the president, claim he suffered from negative political fallout, and hope that this sort of thing does not happen too often. 31 However, while the president was criticized, there is simply no evidence that his evasion of OLC has hurt him politically. As is so often case, the (apparent) success of the operation provides its own justification. The upshot is that there is some evidence that OLC serves as an ex post constraint, but it is fairly weak. Ackerman’s hypothesis seems too extreme, but it is hard to distinguish between the constraint and enabler hypothesis. It is possible that OLC serves as a weak constraint or a weak enabler. Why has it been so weak? First,it may turn out that the constellation of factors that drive decisionmaking in the executive branch prevents the president from solving a time-inconsistency problem by using OLC. The president benefits fromneutral advice, and frombeing able to cite OLC’s approval, but when OLC blocks the president, short-term political considerations trump the medium-term advantages of maintaining a neutral OLC. Meanwhile, OLC’s lawyers yield to political pressure either for careerist reasons or in order to prevent the president from cutting OLC out of the process. Private lawyers face similar pressures, but the market in legal services might provide some additional discipline. Second, the problem might lie in the nature offoreign relations and national security, an area of action that has been notoriously difficult to bring under legal control. Courts have frequently been asked to adjudicate disputes between Congress and the president inthe area of national security. Generally speaking, they have resisted these requests, treating these issues as political questions or nonjusticiable for other reasons. The usual explanation for this resistance is that courts are not experts on these issues; that the highly fluid, frequently changing nature of foreign relations and national security makes themunsuitable for judicial resolution, which is rule-bound, public, decentralized, and slow; and that, accordingly, courts fear that if they intervene, their rulings will be ignored by the executive branch, provoking a constitutional crisis. The supposed solution to this problem is to ask an advisory office in the executive branch to take over a function that the courts have repudiated. It is true that a small office in the executive branch can overcome certain problems that courts face relating to secrecy and speed. But the fundamental problem is that foreign relations are not susceptible to regulation by rules. 32

**Checks and balances are key to a credible deterrence strategy and prevents nuclear war**

Rothschild 13 [Matthew, Feb 4, "The Danger's of Obama's Cyber War Power Grab," www.progressive.org/dangers-of-obama-cyber-war-power-grab]

There are no checks or balances when the President, alone, decides when to engage in an act of war.

And this new aggressive stance will lead to a cyber arms race. TheUnited States hasevidently already used cyber weapons against Iran**,** and so many other countries will assume that cyber warfare is an acceptable tool and will try to use it themselves.

Most troubling, U.S. cybersupremacy—and that is Pentagon doctrine**—**will also raise fears among nuclear powers like Russia, China, and North Korea that theUnited States may use a cyberattack as the opening move in a nuclear attack.

Forif the United States can knock out the command and control structure of an enemy’s nuclear arsenal**,** it can then launch an all-out nuclear attack on that enemy with impunity**.** This would make such nuclear powers more ready to launch their nuclear weapons preemptively for fear that they would be rendered useless. So we’ve just moved a little closer to midnight.

Now, I don’t think Obama would use cyberwafare as a first strike in a nuclear war. But our adversaries may not be so sure, either about Obama or his successors. They, too, worry about the temptations of a President.

**Presidents will circumvent the CP**

Harvard Law Review 12 ["Developments in the Law: Presidential Authority," Vol. 125:2057, www.harvardlawreview.org/media/pdf/vol125\_devo.pdf]

The recent history of signing statements demonstrates how public opinion can effectively check presidential expansions of power by inducing executive self-binding. It remains to be seen, however, if this more restrained view of signing statements can remain intact, for it relies on the promises of one branch — indeed of one person — to enforce and maintain the separation of powers. To be sure, President Obama’s guidelines for the use of signing statements contain all the hallmarks of good executive branch policy: transparency, accountability, and fidelity to constitutional limitations.Yet, in practice, this apparent constraint (however well intentioned) may amount tolittle more than voluntary self-restraint. 146 Without a formal institutional check, it is unclear what mechanism will prevent the next President (or President Obama himself) from reverting to the allegedly abusive Bush-era practices. 147 Only time, and perhaps public opinion, will tell.

**CP links to politics**

Hallowell 13 [Billy Hallowell, writer for The Blaze, B.A. in journalism and broadcasting from the College of Mount Saint Vincent in Riverdale, New York and an M.S. in social research from Hunter College in Manhattan, “HERE’S HOW OBAMA IS USING EXECUTIVE POWER TO BYPASS LEGISLATIVE PROCESS” Feb. 11, 2013, http://www.theblaze.com/stories/2013/02/11/heres-how-obamas-using-executive-power-to-bylass-legislative-process-plus-a-brief-history-of-executive-orders/]

“In an era of polarized parties and a fragmented Congress, the opportunities to legislate are few and far between,” Howell said. “So presidents have powerful incentive to go it alone. And they do.”

And the political opposition howls. Sen. Marco Rubio, R-Fla., a possible contender for the Republican presidential nomination in 2016, said that on the gun-control front in particular, Obama is “abusing his power by imposing his policies via executive fiat instead of allowing them to be debated in Congress.”

 The Republican reaction is to be expected, said John Woolley, co-director of the American Presidency Project at the University of California in Santa Barbara.¶ “For years there has been a growing concern about unchecked executive power,” Woolley said. “It tends to have a partisan content, with contemporary complaints coming from the incumbent president’s opponents.”

**Unrestrained executive prevents faithful discussion --- that causes pre-emptive warfare**

Holmes 8 [Stephen, Walter E. Meyer Professor of Law at NYU School of Law, “Conclusion,” from Security v. Liberty: Conflicts Between Civil Liberties and National Security in American History, p. 219-220, ed by Daniel Farber]

RIGIDITIES OF THE INSULATED EXECUTIVE

Only an executive branch emancipated from legal and constitutional constraints, the administration's defenders argue, will have enough flexibility to defeat a diabolical enemy. This sounds theoretically plausible, but the facts tell a contrary story. Freedom from judicial and legislative oversight has produced not open-eyed flexibility but pathological rigidity. Instead of acknowledging the obvious, namely America's inability to democratize Iraq, the administration has lashed itself(and the country) to a failed policy. Indeed, it continues to act as if its misbegotten project is still on track, only somewhat delayed. Decision making in an echo chamber, refusing to pay any attention to dissident voices, means selecting evidence to corroborate preformed opinions, misunderstanding the challenges ahead, and refusing to ask what if and what then**.** Dispensing with uninhibited criticism and debate in the face of a threat intrinsically difficult to understand is to doom the country to wild goose chases and a reckless misallocation of scarce national security assets in an increasingly dangerous world. Surrounded by yes-men and sheltered from seriously informed criticism, a pampered and unchecked executive becomes catastrophically disconnectedfrom reality. Concentrating excessive authority in the executive does not increase effectiveness in time of multiple evolving dangers because, for one thing, an all-powerful president becomes unwilling to hear bad news. Thus, the advocates, not the opponents, of an imperial presidency are the ones who have spectacularly failed to understand the true seriousness of today's terrorist threat.

### 2ac – Iran DA

#### Reid outweighs the link

TOBIN 2 – 4 – 14 Commentary Magazine [Jonathan S. Tobin, Sanctions Stall Doesn’t Signal AIPAC’s Fall, <http://www.commentarymagazine.com/2014/02/04/iran-sanctions-stall-doesnt-signal-aipacs-decline-nuclear/>]

After amassing an impressive 58 senators from both parties to co-sponsor a bill calling for new sanctions on Iran in case the current negotiations end in failure, the legislation has stalled in the Senate. Alarmed by what it felt was a threat to its diplomacy with Iran, the administration and its backers launched an all-out attack on the measure, claiming its passage would so offend Tehran that it would end nuclear talks with the West and leave the United States no alternative but to go to war. Even worse, some of the president’s supporters claimed that the only reason so many legislators, including 16 Democrats, would back the bill was that they were acting, in the words of influential television comedian Jon Stewart, as senators “from the great state of Israel.” This not-so-subtle invocation of the Walt-Mearsheimer canard in which a vast pro-Israel conspiracy manipulates a helpless Congress paid off by wealthy Jews to the detriment of American interests has become a chestnut of Washington policy debates, but one the administration’s cheerleaders haven’t hesitated to invoke.

All this has chilled a debate about passing more Iran sanctions that might be considered moot in any case since as long as Majority Leader Harry Reid is determined to keep the bill from coming to a vote, it has little chance of passage. But rather than discuss the administration’s scorched-earth campaign on the issue, the New York Times prefers to join with the administration in taking another shot at the arch-villain of the supporters of the conspiratorial view of U.S. foreign policy put forward in the infamous “Israel Lobby” thesis: the American Israel Public Affairs Committee (AIPAC). According to the Times, the lull in the battle over sanctions is a sign that AIPAC is losing its touch on Capitol Hill. This is considered good news for the administration and critics of the pro-Israel lobby and the bipartisan community for which it speaks. But while AIPAC can’t be happy with the way it and other advocates of sanctions have been brushed back in this debate, reports of its decline are highly exaggerated. While the administration has won its point for the moment in stalling the bill, the idea that it has won the political war over Iran is, at best, premature.

#### Waivers solve the impact

Adam Kredo, 1/21/14, White House Seeks to Bypass Congress on Iran Deal, freebeacon.com/white-house-seeks-to-bypass-congress-on-iran-deal/

The White House has been exploring ways to circumvent Congress and unilaterally lift sanctions on Iran once a final nuclear agreement is reached, according to sources with knowledge of White House conversations and congressional insiders familiar with its strategy.

The issue of sanctions relief has become one of the key sticking points in the Iran debate, with lawmakers pushing for increased economic penalties and the White House fighting to roll back regulations.

While many in Congress insist that only the legislative branch can legally repeal sanctions, senior White House officials have been examining strategies to skirt Congress, according to those familiar with internal conversations.

Sen. Mark Kirk (R., Ill.), who is leading the charge on new sanctions legislation, said that it is unacceptable for the White House to try to bypass Congress on such a critical global issue.

“The American people must get a say in any final nuclear agreement with Iran to ensure the mullahs never get the bomb,” Kirk told the Washington Free Beacon. “The administration cannot just ignore U.S. law and lift sanctions unilaterally.”

Congressional insiders say that the White House is worried Congress will exert oversight of the deal and demand tougher nuclear restrictions on Tehran in exchange for sanctions relief.

Top White House aides have been “talking about ways to do that [lift sanctions] without Congress and we have no idea yet what that means,” said one senior congressional aide who works on sanctions. “They’re looking for a way to lift them by fiat, overrule U.S. law, drive over the sanctions, and declare that they are lifted.”

Under the interim nuclear deal with Iran that began on Monday, Tehran will receive more than $4 billion in cash, according to the White House.

President Barack Obama could unilaterally unravel sanctions through several executive channels, according to former government officials and legal experts.

Executive orders grant the president significant leverage in the how sanctions are implemented, meaning that Obama could choose to stop enforcing many of the laws on the books, according to government insiders.

Those familiar with the ins and outs of sanctions enforcement say that the White House has long been lax with its enforcement of sanctions regulations already on the books.

“It’s no secret that the president, with executive power, can determine sanctions implementation, particularly with waivers and the decision not to sanction certain entities,” said Jonathan Schanzer, a former terrorism finance analyst at the Treasury Department, which is responsible for enforcing sanctions.

“The financial pressure has always been about closing loopholes and identifying new ones to close,” Schanzer added. “If you stop that process of constant gardening, you leave a backdoor open.”

Obama could also use executive waivers to “bypass restrictions imposed by the law,” according to a report by Patrick Clawson, director of research at the Washington Institute for Near East Policy (WINEP).

The president has a lot of leverage when it comes to sanctions and could effectively “turn a blind eye” to Iranian infractions.

“In the case of Iran, such an approach could allow Washington to reach a nuclear accord without Congress having to vote on rescinding, even temporarily or conditionally, certain sanctions,” Clawson wrote. “No matter how stiff and far-reaching sanctions may be as embodied in U.S. law, they would have less bite if the administration stopped enforcing them.”

One former senior government official said that President Obama’s legal team has likely been investigating the issue for quite some time.

“I’d be shocked if they weren’t putting the various sanctions laws under a microscope to see how they can waive them or work around them in order to deliver to Iran sanctions relief without having to worry about Congress standing in their way,” said Stephen Rademaker, who served as deputy legal adviser to former President George H.W. Bush’s National Security Council (NSC).

Executive branch lawyers are often tasked with finding ways to get around existing legislation, Rademaker said.

“I’m sure pretty early in the negotiating process they developed a roadmap” to ensure the president has the authority to promise Iran significant relief from sanctions, said Rademaker, who also served as chief council for the House Committee on International Relations. “I’m sure they’ve come up with an in depth analysis of what they can do relying exclusively on the president’s legal authority.”

The White House has been known to disregard portions of the sanctions laws that it disagrees with, according to Schanzer.

#### Logical policy maker could vote aff and maintain their votes in the status quo. Disads must be an opportunity cost.

#### Deal collapse doesn’t cause a strike

Yousaf Butt, a nuclear physicist, is director of the Emerging Technologies Program at the Cultural Intelligence Institute, 1/17/14, Eight Ways You're Wrong About Iran's Nuclear Program, nationalinterest.org/print/commentary/eight-ways-youre-wrong-about-irans-nuclear-program-9723

Meme 1: “If the world powers fail to reach a deal with Tehran the alternative is bombing.”

An incarnation of this shopworn meme appears in [4]Matthew Kroenig's recent piece in Foreign Affairs [4]. He states “A truly comprehensive diplomatic settlement between Iran and the West is still the best possible outcome, but there is little reason to believe that one can be achieved. And that means the United States may still have to choose between bombing Iran and allowing it to acquire a nuclear bomb.” Er, no. That's a false choice. Iran is not acquiring a nuclear bomb—the [6]US Director of National Intelligence (DNI) has a “high level of confidence” [6] that no decision to weaponize has yet been taken in Tehran. This conclusion of the DNI is not based on an absence of evidence but on actual information [7] that whatever weaponization research Iran may have been doing up to about 2003 has been wrapped up a decade ago.

The P5+1 nations—the five permanent members of the Security Council: the US, UK, France, Russia and China, plus Germany—are not negotiating with Iran to stop it from making a nuclear bomb. They are negotiating with Iran on how to continue to keep its nuclear program peaceful. The discussion is about the methods used to verify that Iran continues its peaceful nuclear program. Even if the nuclear talks fall apart the IAEA inspectors would still continue to inspect Iranian nuclear facilities.

If we—or our allies—bomb Iran the IAEA inspectors would most certainly be expelled, Iran would likely leave the NPT, and Tehran would likely kick off a full-blown nuclear weapons development project. Iraq's nuclear weapons project also started in earnest after Israel bombed [8] Iraq's Osirak reactor in 1981.

To sum up: The negotiations with Iran are about the methods to use to continue to make sure Iran's nuclear program is peaceful. Not reaching a deal is not the end of the world. And if we do bomb Iran, it is likely to bring about the very thing the bombs were trying to prevent: a full-blown nuclear weapons program.

#### Turn—sanctions prevent Israel strikes

PHILLIPS 11 – 24 – 13 Senior Research Fellow for Middle Eastern Affairs [James Phillips, A Bad Nuclear Deal with Iran Could Lead to War, <http://blog.heritage.org/2013/11/24/bad-nuclear-deal-iran-lead-war/>]

The deal that the Obama Administration struck at the Geneva talks yesterday amounts to a flawed agreement that risks reducing sanctions pressure on Iran over next six months in return for easily reversible Iranian pledges, some of which Iran has given before but subsequently reneged on. The deal requires Iran to curb some, but not all, of its nuclear activities over the next six months in return for about $7 billion in sanctions relief.

Significantly, Iran is not required to comply with U.N. Security Council sanctions that require a total suspension of uranium enrichment. Instead, Iran is allowed to continue enriching uranium to 3.5 percent levels, ostensibly for its nuclear power reactor at Bushehr, despite the fact that Russia already has committed to fuel that facility.

Another problem is that the interim deal, which creates a six-month window for further negotiations, may hinder Washington’s ability to reach an acceptable final deal. The Obama Administration has been stung by strong criticism from Congress and from U.S. allies who fear that it has squandered its bargaining leverage by easing sanctions in return for marginal concessions from Iran that will not reduce the long-term threat of an Iranian nuclear breakout.

To force Tehran to make the necessary deeper concessions in a final deal, more—not fewer—sanctions are required. But Iran has warned that any further sanctions will prompt it to abandon the agreement. Despite that warning, a bipartisan coalition in Congress has announced that it will impose more sanctions.

The Administration claims that the easing of sanctions will be reversible if Iran defaults on its obligations, but as long as Iran keeps the talks alive, it will be difficult to re-impose the sanctions without being accused of sabotaging negotiations.

As columnist Charles Krauthammer has warned, there is concern that “A President desperate to change the subject and a Secretary of State desperate to make a name for himself” will succumb to “a sucker’s deal” with Iran.

The Administration has resisted bipartisan congressional efforts to impose new sanctions on Iran. White House spokesman Jay Carney has warned that additional pressure on Iran could derail diplomatic negotiations and put the U.S. on a “march to war.”

But as Heritage Foundation Senior Fellow Peter Brookes has noted: “On the contrary, not being tough enough on Iran—whether with new sanctions or at the Geneva talks—may actually propel the simmering crisis toward armed conflict despite intentions to do otherwise.”

Iranian President Hassan Rouhani has claimed that the deal has recognized Iran’s “right” to uranium enrichment, although that language did not appear in the agreement. This sets the stage for Iran to back out of the deal in the future, claiming that the West reneged on its commitments.

Israeli Prime Minister Benjamin Netanyahu denounced the deal as a “historic mistake” and warned that Israel “has the right and duty to defend itself by itself.” This is a signal that Israel could take preventive action to protect itself against Iran’s nuclear threat in the future.

Britain’s Sunday Times reported that Israeli and Saudi officials secretly have met to discuss cooperation against Iran, with Saudi Arabia agreeing to allow Israeli warplanes to cross Saudi airspace to attack Iran’s nuclear sites.

Recently, one of Netanyahu’s closest associates, former national security adviser Yaakov Amidror, told the Financial Times that Israel had the military capability to set back Iran’s nuclear program “for a very long time” and that there was “no question” that Netanyahu would act unilaterally if necessary.

If such a preventive strike occurs, Iran likely would strike back against both Israel and the U.S. In plain English, this means war.

#### Obama’s nuclear deal with Iran sucks now

KESLO 12 – 15 – 13 Heritage Round Up [Maria Keslo, Iran Now Unhindered in Obtaining Nuclear Weapons, Experts Warn, http://blog.heritage.org/2013/12/15/iran-now-unhindered-obtaining-nuclear-weapons-experts-warn/]

The nuclear deal the Obama Administration negotiated with Iran is flawed by the premature easing of sanctions in return for easily reversed Iranian pledges that do not substantially set back Iran’s nuclear weapons program, according to a panel of experts who spoke at a recent Heritage event. The deal also implicitly recognizes Iran’s claim that it has a fundamental right to enrich uranium, the experts warned.

Heritage’s James Phillips, an expert on the Middle East, spoke at the event along with Patrick Clawson, director of research at The Washington Institute for Near East Policy, and Fred Fleitz, a chief analyst of the Langley Intelligence Group Network.

They explained why the flawed agreement will make it more likely that Iran will obtain nuclear weapons.

According to Fleitz, “A deal like this is based on many questionable assumptions. It assumes Rouhani is a relative moderate. It also assumes Iran has a legitimate right to uranium enrichment.”

Phillips said the Obama Administration worked to block new sanctions being imposed on Iran, and he now worries about the consequences.

“I would argue,” Phillips said, “that not being tough enough on Iran, either with the sanctions or further talks at Geneva, could actually increase the chances of war, increase the chances that Israel will go it alone and launch a preventive strike at Iran’s nuclear infrastructure.”

Clawson explained that while the deal is initially set for a six-month period, it can be renewed indefinitely, effectively allowing Iran to go on for years without the world stopping them from obtaining nuclear weapons.

“That, indeed, is the greatest fear of many of the critiques around the country and around the world,” Clawson said. “This agreement is likely not to be the elements of a ‘first step,’ but instead the details of a last step.”

#### Fiat solves the link – plan passes immediately, means no backlash.

**Congress is moving to restrict other areas of cyber operations**

**Fox News 12/30**, 2013 Cyberwar Takes Center Stage in Defense Budget http://www.military.com/daily-news/2013/12/30/cyberwar-takes-center-stage-in-defense-budget.html

The $552.1 billion defense budget **approved by Congress** calls for **new regulations on cyberweapons** -- an effort to prevent the pervasive digital bombs from further spreading throughout the world -- at the same time that it dramatically boosts spending on them.

Section 940 of the National Defense Authorization Act for Fiscal Year 2014, signed into law by President Obama Thursday night, calls for "Control of the Proliferation of Cyber Weapons" following increases in the clear and present danger from cyberbombs such as Stuxnet and growing teams of hackers in foreign countries.

"The President shall establish an interagency process to provide for the establishment of an integrated policy to control the proliferation of cyber weapons through unilateral and cooperative law enforcement activities, financial means, diplomatic engagement, and such other means as the President considers appropriate," the act declares. The goal of the $2 million Cyber Security Initiative: suppressing the trade in cyber tools and infrastructure that can be used for criminal, terrorist and military activities, while still allowing governments to use those tools in legitimate self-defense.

#### Obama’s capitals irrelevant

ECONOMIST 1 – 30 – 14 [Clowns to the left, jokers to the right, <http://www.economist.com/blogs/democracyinamerica/2014/01/barack-obama>]

It's obvious why Mr Obama's wry, pedagogical tone angers Republicans. Increasingly, though, it also angers Democrats, who are tired of having to throw their weight behind the president's call for reasonable compromise. Over the past three years, America's political system has descended into all-out partisan warfare. Democrats want a general in that fight; they are increasingly dissatisfied that their leader has to spend his rhetorical energy playing the role of the UN envoy calling on all sides to exercise restraint. Since the day after his re-election, pundits have been calling on Mr Obama to act more like LBJ: take strong ideological positions, propose major legislation, twist arms off and beat people's heads in with them (in Senator Russell's immortal words), and so forth. (Our Lexington argued that case a few months back.) Earlier this month Isaac Chotiner bemoaned the president's habit of forever presenting both sides of every argument, accusing him of "talk[ing] to us like we're children": "It's as if the reader can't be trusted to just hear one side from the president, because that might (heaven forbid) make him or her think Obama hasn't considered every angle."

I find this argument unpersuasive. Ed Luce made the key point a year and a half ago: LBJ had liberal Republicans and conservative Democrats to work with, whose decision about whether to vote with or against the president on different bills could be influenced by a variety of political considerations. Those legislative cross-loyalties don't exist anymore. Neither do earmarks, the budget goodies targeted to individual districts that were once a widespread currency of congressional dealmaking (something we lamented here). The parties today are ideologically sorted, and there is almost nothing Mr Obama can do to convince or compel Republicans to vote with him. Republicans are able to halt the president's agenda in its tracks, and they have every reason to do so. There simply isn't any reason to believe that more aggressive legislative arm-twisting would have generated more success for Mr Obama; it seems entirely possible that if he had aggressively tried to dictate the terms of health-care reform legislation rather than allowing various senators to rewrite (and weaken) the bill, he might have lost even that signature achievement. Last year, Mr Obama decided to throw his entire weight behind gun-control legislation, taking on just the sort of ambitious and improbable crusade Mr Ignatius had advised him to attempt. The result was that he lost, squandered political capital, and mired his party in the mud.

The fact is that, as unsatisfying as it may be for his partisans, Mr Obama's above-the-fray stance is his best political play. It taps into his natural character strengths and practiced rhetorical gestures. It safeguards him from being side-lined as a marginal, extremist figure by the media and commentariat—always a danger for black politicians who embrace strong ideological agendas. It allows him to take up themes like inequality and help bring them into the mainstream once they have been advanced by more ideological players.

#### No Israeli strikes. Strategic incentives and institutional checks.

Zachary Keck, 11/28/13. Associate editor of The Diplomat. “Five Reasons Israel Won't Attack Iran,” The National Interest, http://server1.nationalinterest.org/commentary/five-reasons-israel-wont-attack-iran-9469?page=2.

Although not a member of the P5+1 itself, Israel has always loomed large over the negotiations concerning Iran’s nuclear program. For example, in explaining French opposition to a possible nuclear deal earlier this month, French Foreign Minister Laurent Fabius stated: “The security concerns of Israel and all the countries of the region have to be taken into account.”

Part of Fabius’ concern derives from the long-held fear that Israel will launch a preventive strike against Iran to prevent it from obtaining nuclear weapons. For some, this possibility remains all too real despite the important interim agreement the P5+1 and Iran reached this weekend. For example, when asked on ABC’s This Week whether Israel would attack Iran while the interim deal is in place,William Kristol responded: “I don't think the prime minister will think he is constrained by the U.S. deciding to have a six-month deal. […] six months, one year, I mean, if they're going to break out, they're going to break out.”

Israeli prime minister Benjamin Netanyahu has done little to dispel this notion. Besides blasting the deal as a “historic mistake,” Netanyahu said Israel “is not obliged to the agreement” and warned “the regime in Iran is dedicated to destroying Israel and Israel has the right and obligation to defend itself with its own forces against every threat.”

Many dismiss this talk as bluster, however. Over at Bloomberg View, for instance, Jeffrey Goldberg argues that the nuclear deal has “boxed-in Israeli Prime Minister Benjamin Netanyahu so comprehensively that it's unimaginable Israel will strike Iran in the foreseeable future.” Eurasia Group's Cliff Kupchan similarly argued: “The chance of Israeli strikes during the period of the interim agreement drops to virtually zero.”

Although the interim deal does further reduce Israel’s propensity to attack, the truth is that the likelihood of an Israeli strike on Iran’s nuclear facilities has always been greatly exaggerated. There are at least five reasons why Israel isn’t likely to attack Iran.

1. You Snooze, You Lose

First, if Israel was going to strike Iran’s nuclear facilities, it would have done so a long time ago. Since getting caught off-guard at the beginning of the Yom Kippur War in 1973, Israel has generally acted proactively to thwart security threats. On no issue has this been truer than with nuclear-weapon programs. For example, Israel bombed Saddam Hussein’s program when it consisted of just a single nuclear reactor. According to ABC News, Israel struck Syria’s lone nuclear reactor just months after discovering it. The IAEA had been completely in the dark about the reactor, and took years to confirm the building was in fact housing one.

Contrast this with Israel’s policy toward Iran’s nuclear program. The uranium-enrichment facility in Natanz and the heavy-water reactor at Arak first became public knowledge in 2002. For more than a decade now, Tel Aviv has watched as the program has expanded into two fully operational nuclear facilities, a budding nuclear-research reactor, and countless other well-protected and -dispersed sites. Furthermore, America’s extreme reluctance to initiate strikes on Iran was made clear to Israel at least as far back as 2008. It would be completely at odds with how Israel operates for it to standby until the last minute when faced with what it views as an existential threat.

2. Bombing Iran Makes an Iranian Bomb More Likely

Much like a U.S. strike, only with much less tactical impact, an Israeli air strike against Iran’s nuclear facilities would only increase the likelihood that Iran would build the bomb. At home, Supreme Leader Ali Khamenei could use the attack to justify rescinding his fatwa against possessing a nuclear-weapons program, while using the greater domestic support for the regime and the nuclear program to mobilize greater resources for the country’s nuclear efforts.

Israel’s attack would also give the Iranian regime a legitimate (in much of the world’s eyes) reason to withdraw from the Nuclear Non-Proliferation Treaty (NPT) and kick out international inspectors. If Tehran’s membership didn’t even prevent it from being attacked, how could it justify staying in the regime? Finally, support for international sanctions will crumble in the aftermath of an Israeli attack, giving Iran more resources with which to rebuild its nuclear facilities.

3. Helps Iran, Hurts Israel

Relatedly, an Israeli strike on Iran’s nuclear program would be a net gain for Iran and a huge loss for Tel Aviv. Iran could use the strike to regain its popularity with the Arab street and increase the pressure against Arab rulers. As noted above, it would also lead to international sanctions collapsing, and an outpouring of sympathy for Iran in many countries around the world.

Meanwhile, a strike on Iran’s nuclear facilities would leave Israel in a far worse-off position. Were Iran to respond by attacking U.S. regional assets, this could greatly hurt Israel’s ties with the United States at both the elite and mass levels. Indeed, a war-weary American public is adamantly opposed to its own leaders dragging it into another conflict in the Middle East. Americans would be even more hostile to an ally taking actions that they fully understood would put the U.S. in danger.

Furthermore, the quiet but growing cooperation Israel is enjoying with Sunni Arab nations against Iran would evaporate overnight. Even though many of the political elites in these countries would secretly support Israel’s action, their explosive domestic situations would force them to distance themselves from Tel Aviv for an extended period of time. Israel’s reputation would also take a further blow in Europe and Asia, neither of which would soon forgive Tel Aviv.

4. Israel’s Veto Players

Although Netanyahu may be ready to attack Iran’s nuclear facilities, he operates within a democracy with a strong elite structure, particularly in the field of national security. It seems unlikely that he would have enough elite support for him to seriously consider such a daring and risky operation.

For one thing, Israel has strong institutional checks on using military force. As then vice prime minister and current defense minister Moshe Yaalon explained last year: “In the State of Israel, any process of a military operation, and any military move, undergoes the approval of the security cabinet and in certain cases, the full cabinet… the decision is not made by two people, nor three, nor eight.” It’s far from clear Netanyahu, a fairly divisive figure in Israeli politics, could gain this support. In fact, Menachem Begin struggled to gain sufficient support for the 1981 attack on Iraq even though Baghdad presented a more clear and present danger to Israel than Iran does today.

What is clearer is that Netanyahu lacks the support of much of Israel’s highly respected national security establishment. Many former top intelligence and military officials have spoken out publicly against Netanyahu’s hardline Iran policy, with at least one of them questioning whether Iran is actually seeking a nuclear weapon. Another former chief of staff of the Israeli Defense Forces told The Independent that, “It is quite clear that much if not all of the IDF [Israeli Defence Forces] leadership do not support military action at this point…. In the past the advice of the head of the IDF and the head of Mossad had led to military action being stopped.”

5. A Deal is Better Than No Deal

Finally, Israel won’t attack Iran because it is ultimately in its interests for the US and Iran to reach an agreement, even if it is a less than an ideal one. To begin with, an agreement is the only way to prevent Iran from acquiring nuclear weapons short of an invasion and occupation of the country. Moreover, Israel would benefit both directly and indirectly from a U.S.-Iranian nuclear deal and especially larger rapprochement. Israel would gain a number of direct benefits from a larger warming of U.S.-Iranian relations, which a nuclear deal could help facilitate. Iran currently pays no costs while benefiting significantly from its anti-Israeli tirades and actions. A rapprochement with the U.S. would force Iranian leaders to constrain their anti-Israeli rhetoric and actions, or risk losing their new partner. While Israel and Iran might not enjoy the same relationship they did under the Shah or the first decade of the Islamic Republic, a U.S.-allied Iran would be much less of a burden for Israel. History is quite clear on this point: U.S. Middle Eastern allies—notable Egypt under Sadat—have been much less hostile to the Jewish state than countries that have been U.S. adversaries.

Tel Aviv would also benefit indirectly from a U.S.-Iran nuclear deal and possible rapprochement. That’s because either of these agreements would spark panic in Sunni Arab capitals. For the foreseeable future, then, Israel would enjoy some breathing room, which would obtain as these governments would be preoccupied with Iran for the foreseeable future. Indeed, just the possibility of an interim nuclear deal between the U.S. and Iran has created rumors of Saudi Arabia seeking tighter cooperation with Israel.

For these reasons, the interim nuclear deal has made it less likely that Israel will attack Iran. That being said, the possibility of an Israeli attack on Iran was already remote long before Iran and the P5+1 held their talks in Geneva last month.

#### No strike – no escalation anyway

Elhusseini 13 (Fadi, Palestinian Diplomat and Journalist, 3/12/2013, "Will Israel attack Iran?", jordantimes.com/will-israel-attack-iran)

That red line is fast approaching, but is Israel going to really attack Iran?

Many observers say this is sheer fantasy, especially in view of the new Israeli government coalition and the current developments in the Middle East.

Iran insists its nuclear programme is peaceful and a national right, yet the fiery speeches and comments delivered by its officials proffer neither good gestures nor convincing assurances to the international community or its sympathisers.

The prospect of war terrifies not only Israelis, but also people across the Middle East and the rest of the world. Surveys in Israel show that most Israelis oppose launching a unilateral attack on Iranian nuclear facilities.

Experts believe that no Israeli attack would deter the Iranian nuclear programme and its ambition would not be ended, but simply delayed. Israeli military and intelligence chiefs believe that a strike on Iran is a bad idea, while the Obama administration has told Israel to back off and wait for sanctions to work.

While it is likely that Iran would retaliate against Israel and possibly the US in response to any attack, it is unlikely that Iran will instigate a major war. Albeit for different reasons, Iran, Israel and the US understand that a war would not serve their interests.

Israeli decision makers are confident that if things go bad, the US will not leave Israel at peril.

Neither the US, whose most difficult decisions are usually taken in the second presidential term, nor other international powers would leave Israel unaided or accept an Israeli defeat.

Iranian decision makers are also aware of the fact that initiating a major war would lead to an eventual American intervention and an inevitable confrontation with the world’s biggest military might.

#### Obama won’t push the plan – he’d just sign on at the end.

#### Healthcare thumps the DA

Finkel 1-15-- editor of Against the Current [David “Will the Iran deal hold?” <http://internationalviewpoint.org/spip.php?article3239>, DOA: 1-17-14]

A politically weakened U.S. president is pulled by a powerful domestic lobby and influential foreign governments toward launching a war that U.S. imperialism right now doesn’t want, that the world doesn’t want, and that the large majority of the American public doesn’t want — what will be the outcome? It’s an interesting, if dangerous and scary, test of how U.S. politics actually work. The initial results, at least, are in: The unleashed fury of the Israeli government and the “pro-Israel” lobby, the monarchy of Saudi Arabia, the neoconservative warmongers and the much-feared religious right weren’t able to block the Obama administration and European partners from reaching a six-month interim agreement with Iran over that country’s nuclear enrichment program. Any socialist, progressive or sane person must welcome this agreement. That’s not because it resolves the proliferation of nuclear weapons, or changes the hideous character of the Iranian regime in relation to its own population, or addresses the multiple underlying issues of the Middle East crisis — it does none of these things — but because it pushes back the imminent danger of a really catastrophic war. That’s one strike against the widely held theory that the toxic influence of the Israel Lobby can drag the United States into wars that this country‘s ruling class disapproves. The political fight, of course, is hardly over. We’ll explore the underlying reasons for the Israeli and Saudi sound and fury over the deal with Iran, which in fact have little to do with the rather distant specter of an Iranian atomic bomb. But we need to note the U.S. political context in which the fight will play out. If anything, this might have been expected to strengthen the hand of the “war party.” A Wounded Presidency The spectacular disaster of the Afford­able Care Act website is a self-inflicted wound from which the Obama administration will not easily, or perhaps ever, fully recover. Certainly all of us who support single-payer health insurance realized that the fantastically tangled system of “Obamacare” would ultimately fail, due to its scheme for subsidizing the parasitical private insurance industry, but no one could have expected such an immediate display of arrogant incompetence in the “rollout.” The Republican Party has regained big chunks of the ground lost during its own government shutdown fiasco. It’s true that Congress’s approval ratings remain even deeper in the toilet than the President’s, but that fact affects both capitalist parties — and now, Congressional Democrats who stood united against repealing “Obamacare,” because that would have represented the effective end of the Obama presidency and virtual suicide for the party, are angry, alienated and afraid to be near him. Whatever political capital the President had for immigration reform, seriously raising the minimum wage, protecting food stamps from savage cuts, or much of anything else including the climate change crisis, has been dissipated. The Democrats’ chances of regaining the House of Representatives in the November 2014 midterm election, marginal to begin with, are now much less than those of losing the Senate as well. In these circumstances, this might be considered a favorable moment for the power of the Israel Lobby, Saudi Arabia and rightwing militarists to derail the Obama administration’s deal with Iran. In fact, France made a last-minute move to block the first version of the interim agreement — right after Saudi Arabia signed off on a huge purchase of French weapons (a point worth noting in case anyone thought it’s only the USA that has a military-industrial complex). The President’s **loss of control over his own party** is such that many prominent Democratic Senators have taken to the airwaves loudly denouncing his “appeasement” of the Iranians and abandonment of Israel in its hour of existential peril.



No spillover link --- losing capital on one issue won’t hurt votes in others --- they don’t have a vote switch card

Obama won’t fight the plan

Stirewalt 9/10/13 [Chris, digital politics editor for Fox News, Can Obama take credit for his own defeat?, http://www.foxnews.com/politics/2013/09/10/can-obama-take-credit-for-his-own-defeat/]

It was going to be big news because it was going to be just the sort of thing Obama almost never does. Risking his political capital on an unpopular policy hasn’t really been Obama’s bag since his health law creaked over the finish line in 2010. Once ObamaCare was on the books, the idea was to just survive past re-election. And then, once re-elected, to just get through midterms.

Obama’s hyper-reactive, base-nuzzling brand of politics forbids much risk taking.

On national security, Obama has been particularly unwilling to take ownership**.** He abandoned his goldilocks surge strategy for Afghanistan on the nation’s doorstep, waved away concerns about his huge expansions of domestic spying and mostly sidestepped his own intervention in Libya**,** particularly once American-backed Islamists there turned on their benefactors last year.

Ending unpopular wars or announcing the death of the world’s most hated man? Obama’s your man. Defending his own national security policies? Better call John McCain.

Capital theory is wrong

Hirsh 2/7/13 [Michael, Chief correspondent for National Journal, Previously served as the senior editor and national economics correspondent for Newsweek, Overseas Press Club award for best magazine reporting from abroad in 2001 and for Newsweek’s coverage of the war on terror which also won a National Magazine Award, There’s No Such Thing as Political Capital, http://www.nationaljournal.com/magazine/there-s-no-such-thing-as-political-capital-20130207]

But the abrupt emergence of the immigration and gun control issues illustrates how suddenly shifts in mood can occur and how political interests can align in new ways just as suddenly. Indeed, the pseudo-concept of political capital masks a larger truth about Washington that is kindergarten simple: You just don’t know what you can do until you try. Or as Ornstein himself once wrote years ago, “Winning wins.” In theory, and in practice, depending on Obama’s handling of any particular issue, even in a polarized time, he could still deliver on a lot of his second-term goals, depending on his skill and the breaks. Unforeseen catalysts can appear, like Newtown. Epiphanies can dawn, such as when many Republican Party leaders suddenly woke up in panic to the huge disparity in the Hispanic vote.

Some political scientists who study the elusive calculus of how to pass legislation and run successful presidencies say that political capital is, at best, an empty concept, and that almost nothing in the academic literature successfully quantifies or even defines it. “It can refer to a very abstract thing, like a president’s popularity, but there’s no mechanism there. That makes it kind of useless,” says Richard Bensel, a government professor at Cornell University. Even Ornstein concedes that the calculus is far more complex than the term suggests. Winning on one issue often changes the calculation for the next issue; there is never any known amount of capital. “The idea here is, if an issue comes up where the conventional wisdom is that president is not going to get what he wants, and he gets it, then each time that happens, it changes the calculus of the other actors” Ornstein says. “If they think he’s going to win, they may change positions to get on the winning side. It’s a bandwagon effect.”

### 2ac – Terrorism Add-On

**Plan prevents cyber terrorists from hacking into nuclear command centers --- the impact is nuclear war**

**Fritz 9** [Jason, former captain in US Army, MA international relations (Bond), BS (St. Cloud), writer at Center for New American Security, paper written for International Commission on Nuclear Non-proliferation and Disarmament, http://www.icnnd.org/Documents/Jason\_Fritz\_Hacking\_NC2.pdf?noredirect=1, nrb]

This paper will analyse the threat of cyber terrorism in regard to nuclear weapons. Specifically, this research will use open source knowledge to identify the structure of nuclear command and control centres, how those structures might be compromised through computer network operations, and how doing so would fit within established cyber terrorists’ capabilities, strategies, and tactics. If access to command and control centres is obtained, terrorists could fake or actually cause one nuclear-armed state to attack another, thus provoking a nuclear response from another nuclear power. This may be an easier alternative for terrorist groups than building or acquiring a nuclear weapon or dirty bomb themselves. This would also act as a force equaliser, and provide terrorists with the asymmetric benefits of high speed, removal of geographical distance, and a relatively low cost. Continuing difficulties in developing computer tracking technologies which could trace the identity of intruders, and difficulties in establishing an internationally **agreed upon legal framework to guide responses** to computer network operations, point towards an inherent weakness in using computer networks to manage nuclear weaponry. This is particularly relevant to reducing the **hair trigger posture** of existing nuclear arsenals.

All computers which are connected to the internet are susceptible to infiltration and remote control. Computers which operate on a closed network may also be compromised by various hacker methods, such as privilege escalation, roaming notebooks, wireless access points, embedded exploits in software and hardware, and maintenance entry points. For example, e-mail spoofing targeted at individuals who have access to a closed network, could lead to the installation of a virus on an open network. This virus could then be carelessly transported on removable data storage between the open and closed network. Information found on the internet may also reveal how to access these closed networks directly. Efforts by militaries to place increasing reliance on computer networks, including experimental technology such as autonomous systems, and their desire to have multiple launch options, such as nuclear triad capability, enables multiple entry points for terrorists. For example, if a terrestrial command centre is impenetrable, perhaps isolating one nuclear armed submarine would prove an easier task. There is evidence to suggest multiple attempts have been made by hackers to compromise the extremely low radio frequency once used by the US Navy to send nuclear launch approval to submerged submarines. Additionally, the alleged Soviet system known as Perimetr was designed to automatically launch nuclear weapons if it was unable to establish communications with Soviet leadership. This was intended as a retaliatory response in the event that nuclear weapons had decapitated Soviet leadership; however it did not account for the possibility of cyber terrorists blocking communications through computer network operations in an attempt to engage the system.

Should a warhead be launched, damage could be further enhanced through additional computer network operations. By using proxies, multi-layered attacks could be engineered. Terrorists could remotely commandeer computers in China and use them to launch a **US nuclear attack against Russia**. Thus Russia would believe it was under attack from the US and the US would believe China was responsible. Further, emergency response communications could be disrupted, transportation could be shut down, and disinformation, such as misdirection, could be planted, thereby hindering the disaster relief effort and maximizing destruction. Disruptions in communication and the use of disinformation could also be used to provoke uninformed responses. For example, a **nuclear strike between India and Pakistan** could be coordinated with Distributed Denial of Service attacks against key networks, so they would have further difficulty in identifying what happened and be forced to respond quickly. Terrorists could also knock out communications between these states so they cannot discuss the situation. Alternatively, amidst the confusion of a traditional large-scale terrorist attack, claims of responsibility and declarations of war could be falsified in an attempt to instigate a hasty military response. These false claims could be posted directly on Presidential, military, and government websites. E-mails could also be sent to the media and foreign governments using the IP addresses and e-mail accounts of government officials. A sophisticated and all encompassing combination of traditional terrorism and cyber terrorism could be enough to launch nuclear weapons on its own, without the need for compromising command and control centres directly.

# 1ARs

## QDR CP

### 1AR Perm Do the CP

#### Recommend CPs don’t compete textually – they add the entire aff – CP has to be functionally and textually competitive.

#### Their external committee is established by congress which means that could be a result of the aff.

#### Changing the agent in order for the CP to be competitive links to our offense- - plan says USFG means anything NON executive is part of the function of the plan.

US institute of peace 13 (August 12, 2013, “USIP Tapped to Facilitate Congressionally-Mandated National Defense Panel”

 <http://www.usip.org/publications/usip-tapped-facilitate-congressionally-mandated-national-defense-panel>)

Required by Congress, the QDR is a review of Department of Defense (DoD) strategy and priorities and sets a long-term course for DoD as it assesses the threats and challenges faced by the U.S. In turn, Congress directed that members of the National Defense Panel review the QDR, assess the assumptions, strategy, findings, and risks in the report, conduct an independent assessment of a variety of possible force structures, review the resource requirements, and provide recommendations to Congress and the secretary of Defense.

#### Statutory isn’t exclusively legislative

CASSIN 47 Justice of the Municipal Court of the City of New York [Edward Cassin, Constitutional Versus Legislative Courts, 16 Fordham L. Rev. 87 (1947).]

There is something else that should be discussed at this point. I refer to the inexact use of the word "statutory" as being synonymous with "legislative." 28 It is correct to say that all legislative courts are statutory courts but all statutory courts are not legislative courts. Nowhere has this been clearer put than in the minority opinion in the Rhode Island case:

"It is true that they are brought into existence by legislative enactment, and that, because of this fact, they may be loosely termed statutory courts, but when they are so instituted the judicial power of the state is vested in them by the Constitution, which makes them constitutional courts in the strict sense of the term." 29

## Ice Age

### Ice Age

#### Zero cooling – arguments use bad data, poor methodology, aren’t peer reviewed

Borenstein 09 [Seth, writer for the Associated Press, “Is the Earth cooling instead of warming? No way, statisticians say,” 10-31, houmatoday.com/apps/pbcs.dll/article?AID=/20091031/articles/910319962&template=printart]

Have you heard that the world is now cooling instead of warming? You may have seen some news reports on the Internet or heard about it from a provocative new book. Only one problem: It's not true, according to an analysis of the numbers done by several independent statisticians for The Associated Press. The case that the Earth might be cooling partly stems from recent weather. Last year was cooler than previous years. It's been a while since the super-hot years of 1998 and 2005. So is this a longer climate trend or just weather's normal ups and downs? In a blind test, the AP gave temperature data to four independent statisticians and asked them to look for trends, without telling them what the numbers represented. The experts found no true temperature declines over time. "If you look at the data and sort of cherry-pick a micro-trend within a bigger trend, that technique is particularly suspect," said John Grego, a professor of statistics at the University of South Carolina. Yet the idea that things are cooling has been repeated in opinion columns, a BBC news story posted on the Drudge Report and in a new book by the authors of the best-seller "Freakonomics." Last week, a poll by the Pew Research Center found that only 57 percent of Americans now believe there is strong scientific evidence for global warming, down from 77 percent in 2006. Global warming skeptics base their claims on an unusually hot year in 1998. Since then, they say, temperatures have dropped — thus, a cooling trend. But it's not that simple. Since 1998, temperatures have dipped, soared, fallen again and are now rising once more. Records kept by the British meteorological office and satellite data used by climate skeptics still show 1998 as the hottest year. However, data from the National Oceanic and Atmospheric Administration and NASA show 2005 has topped 1998. Published peer-reviewed scientific research generally cites temperatures measured by ground sensors, which are from NOAA, NASA and the British, more than the satellite data. The recent Internet chatter about cooling led NOAA's climate data center to re-examine its temperature data. It found no cooling trend. "The last 10 years are the warmest 10-year period of the modern record," said NOAA climate monitoring chief Deke Arndt. "Even if you analyze the trend during that 10 years, the trend is actually positive, which means warming." The AP sent expert statisticians NOAA's year-to-year ground temperature changes over 130 years and the 30 years of satellite-measured temperatures preferred by skeptics and gathered by scientists at the University of Alabama in Huntsville. Statisticians who analyzed the data found a distinct decades-long upward trend in the numbers, but could not find a significant drop in the past 10 years in either data set. The ups and downs during the last decade repeat random variability in data as far back as 1880. Saying there's a downward trend since 1998 is not scientifically legitimate, said David Peterson, a retired Duke University statistics professor and one of those analyzing the numbers. Identifying a downward trend is a case of "people coming at the data with preconceived notions," said Peterson, author of the book "Why Did They Do That? An Introduction to Forensic Decision Analysis." One prominent skeptic said that to find the cooling trend, the 30 years of satellite temperatures must be used. The satellite data tends to be cooler than the ground data. And key is making sure 1998 is part of the trend, he added. It's what happens within the past 10 years or so, not the overall average, that counts, contends Don Easterbrook, a Western Washington University geology professor and global warming skeptic. "I don't argue with you that the 10-year average for the past 10 years is higher than the previous 10 years," said Easterbrook, who has self-published some of his research. "We started the cooling trend after 1998. You're going to get a different line depending on which year you choose. "Should not the actual temperature be higher now than it was in 1998?" Easterbrook asked. "We can play the numbers games." That's the problem, some of the statisticians said. Grego produced three charts to show how choosing a starting date can alter perceptions. Using the skeptics' satellite data beginning in 1998, there is a "mild downward trend," he said. But doing that is "deceptive." The trend disappears if the analysis starts in 1997. And it trends upward if you begin in 1999, he said. Apart from the conflicting data analyses is the eyebrow-raising new book title from Steven D. Levitt and Stephen J. Dubner, "Super Freakonomics: Global Cooling, Patriotic Prostitutes and Why Suicide Bombers Should Buy Life Insurance." A line in the book says: "Then there's this little-discussed fact about global warming: While the drumbeat of doom has grown louder over the past several years, the average global temperature during that time has in fact decreased." That led to a sharp rebuke from the Union of Concerned Scientists, which said the book mischaracterizes climate science with "distorted statistics." Levitt, a University of Chicago economist, said he does not believe there is a cooling trend. He said the line was just an attempt to note the irony of a cool couple of years at a time of intense discussion of global warming. Levitt said he did not do any statistical analysis of temperatures, but "eyeballed" the numbers and noticed 2005 was hotter than the last couple of years. Levitt said the "cooling" reference in the book title refers more to ideas about trying to cool the Earth artificially. Statisticians say that in sizing up climate change, it's important to look at moving averages of about 10 years. They compare the average of 1999-2008 to the average of 2000-2009. In all data sets, 10-year moving averages have been higher in the last five years than in any previous years. "To talk about global cooling at the end of the hottest decade the planet has experienced in many thousands of years is ridiculous," said Ken Caldeira, a climate scientist at the Carnegie Institution at Stanford. Ben Santer, a climate scientist at the Department of Energy's Lawrence Livermore National Lab, called it "a concerted strategy to obfuscate and generate confusion in the minds of the public and policymakers" ahead of international climate talks in December in Copenhagen. President Barack Obama weighed in on the topic Friday at MIT. He said some opponents "make cynical claims that contradict the overwhelming scientific evidence when it comes to climate change — claims whose only purpose is to defeat or delay the change that we know is necessary." Earlier this year, climate scientists in two peer-reviewed publications statistically analyzed recent years' temperatures against claims of cooling and found them not valid. Not all skeptical scientists make the flat-out cooling argument. "It pretty much depends on when you start," wrote John Christy, the Alabama atmospheric scientist who collects the satellite data that skeptics use. He said in an e-mail that looking back 31 years, temperatures have gone up nearly three-quarters of a degree Fahrenheit (four-tenths of a degree Celsius). The last dozen years have been flat, and temperatures over the last eight years have declined a bit, he wrote. Oceans, which take longer to heat up and longer to cool, greatly influence short-term weather, causing temperatures to rise and fall temporarily on top of the overall steady warming trend, scientists say. The biggest example of that is El Nino. El Nino, a temporary warming of part of the Pacific Ocean, usually spikes global temperatures, scientists say. The two recent warm years, both 1998 and 2005, were El Nino years. The flip side of El Nino is La Nina, which lowers temperatures. A La Nina bloomed last year and temperatures slipped a bit, but 2008 was still the ninth hottest in 130 years of NOAA records. Of the 10 hottest years recorded by NOAA, eight have occurred since 2000, and after this year it will be nine because this year is on track to be the sixth-warmest on record. The current El Nino is forecast to get stronger, probably pushing global temperatures even higher next year, scientists say. NASA climate scientist Gavin Schmidt predicts 2010 may break a record, so a cooling trend "will be never talked about again."

#### 2. Warming causes saline shocks- Turns ice age.

Ecological Society of America 2008 (nonpartisan, nonprofit organization of over 10,000 scientists founded in 1915, Targeted News Service, “HEADLINE: Ecologists Use Oceanographic Data to Predict Future climate Change,” 11/6/2008, p. lexis)

The Ecological Society of America issued the following news release: Earth scientists are attempting to predict the future impacts of climate change by reconstructing the past behavior of Arctic climate and ocean circulation. In a November special issue of the journal Ecology, a group of scientists report that if current patterns of change in the Arctic and North Atlantic Oceans continue, alterations of ocean circulation could occur on a global scale, with potentially dramatic implications for the world's climate and biosphere. Charles Greene of Cornell University and his colleagues reconstructed the patterns of climate change in the Arctic from the Paleocene epoch to the present. Over these 65 million years, the Earth has undergone several major warming and cooling episodes, which were largely mitigated by the expansion and contraction of sea ice in the Arctic. "When the Arctic cools and ice sheets and sea ice expand, the increased ice cover increases albedo, or reflectance of the sun's rays by the ice," says Greene, the lead author on the paper. "When more of the sun is reflected rather than absorbed, this leads to global cooling." Likewise, when ice sheets and sea ice contract and expose the darker-colored land or ocean underneath, heat is absorbed, accelerating climate warming. Currently, the Earth is in the midst of an interglacial period, characterized by retracted ice sheets and warmer temperatures. In the past three decades, changes in Arctic climate and ice cover have led to several reorganizations of northern ocean circulation patterns. Since 1989, a species of plankton native to the Pacific Ocean has been colonizing the North Atlantic Ocean, a feat that hasn't occurred in more than 800 thousand years. These plankton were carried across the Arctic Ocean by Pacific waters that made their way to the North Atlantic. "When Arctic climate changes, waters in the Arctic can go from storing large quantities of freshwater to exporting that freshwater to the North Atlantic in large pulses, referred to as great salinity anomalies," Greene explains. "These GSAs flow southward, disrupting the ocean's circulation patterns and altering the temperature stratification observed in marine ecosystems." In the continental shelf waters of the Northwest Atlantic, the arrival of a GSA during the early 1990s led to a major ecosystem reorganization, or regime shift. Some ocean ecosystems in the Northwest Atlantic saw major drops in salinity, increased stratification, an explosion of some marine invertebrate populations and a collapse of cod stocks. "The changes in shelf ecosystems between the 1980s and 1990s were remarkable," says Greene. "Now we have a much better idea about the role climate had in this regime shift." The changes observed in recent decades are only the tip of the iceberg. Previous interglacial periods have ended when the global ocean's deep circulation slowed in response to reductions in the formation of North Atlantic Deep Water, or NADW, a large, deep mass of highly saline water in the North Atlantic. At these tipping points in the Earth's history, NADW formation was disrupted by pulses of freshwater entering the North Atlantic. The slowing of the global ocean's deep circulation results in less heat being transported to higher latitudes, accelerating ice formation and advancing the Earth into glacial conditions. Recent modeling studies show that NADW formation will likely be resilient to freshwater pulses from the Arctic during the 21st century, according to the authors. Continued exposure to such freshwater forcing, however, could **disrupt global ocean circulation** **during the next century** and lead **to very abrupt changes** in climate, similar to those that occurred at the onset of **the last ice age**. "If the Earth's deep ocean circulation were to be shut down, many of the atmospheric, glacial and oceanic processes that have been stable in recent times would change, and the change would likely be abrupt," says Greene. "While the ecosystem consequences of gradual changes in the ocean are somewhat predictable, all bets are off after such abrupt changes occur."

#### 3. Warming causes a climate flip.

Space Daily 2008 (“HEADLINE: On the Threshold of Abrupt Climate Change,” 9/23/2008, lexis)

But climate change has occurred with frightening rapidity in the past and will almost certainly do so again. Perhaps the most famous example is the reverse hiccup in a warming trend that began 15,000 years ago and eventually ended the last ice age. Roughly 2,000 years after it started, the warming trend **suddenly reversed**, **and temperatures fell back to near-glacial conditions**; Earth stayed cold for over a thousand years, a period called the Younger Dryas (named for an alpine wildflower). Then warming resumed so abruptly that global temperatures shot up 10 degreesC in just 10 years. Because civilizations hadn't yet emerged, complex human societies escaped this particular roller-coaster ride. Nevertheless, some form of abrupt climate change **is highly likely in the future**, with wide-ranging economic and social effects.

#### 4. No Ice age now

Nielsen 2004 (Rolf Haugaard, journalist, “Not Quite the Day After Tomorrow,” NEW SCIENTIST, 9—11—04, p. 6.)

Testing and verifying climate models is essential for understanding how long our interglacial period will last. The main trigger for a new ice age is a shift in the Earth's orbit from being more elliptical to being more circular, which happens in cycles lasting roughly 100,000 years**. Ignoring the effect of human activity,** the next ice age is at least 10,000 **to 20,000** years away**.** However, "the anthropogenic greenhouse effect is a joker in the pack", Steffensen says.

## Politics TPA

### AT: Trade Impact

#### Globalization is somewhat inevitable

BRAINARD 08 Vice President and Director for Global Economy and Development

[Lael, Senate Committee on Finance, “America’s Trade Agenda: Examining the Trade Enforcment Act of 2007,” Senate testimony, 5/22/2008, brookings.edu/testimony/2008/0522\_trade\_brainard.aspx]

We are experiencing a period of breathtaking global integration that dwarfs previous episodes. Global trade has more than doubled in the last 7 years alone. The entry of India and China amounts to a 70 percent expansion of the global labor force—with wages less than a tenth of the level in wealthy economies. This expansion is more than three times bigger than the globalization challenge of the 1970s and 80s associated with the sequential advances of Japan, South Korea, and the other Asian tigers. It is also far larger than the more recent integration of the North American market. If, as is now widely expected, these trends in population and productivity growth continue, the time will soon approach where the balance of global economic heft flips. According to my colleague, Homi Kharas, the so-called emerging BRIC (Brazil, Russia, India and China) economies will account for over half of world income by 2050, up from 13 percent today, while the share of the G7 wealthiest economies will slip from 57 percent today to one quarter of world income in 2050. And by 2030, 83 percent of the world’s middle class consumers will reside in what are today considered emerging markets.

### Won’t Pass

#### NO TPA – lacks support – Reid won’t allow a vote

MARKETWATCH 1 – 22 – 14 [Congress won’t give Obama blank check on trade deals, <http://www.marketwatch.com/story/congress-wont-give-obama-blank-check-on-trade-deals-2014-01-22?link=MW_latest_news>]

Congress won’t give Obama blank check on trade deals

The proposed new trade agreement between the U.S. and several Pacific Rim countries may be the boon that advocates say it is, or it may be the corporate sellout described by its opponents.

One thing it should not be, however, is a fait accompli.

Supporters say the Trans-Pacific Partnership currently being negotiated among 12 countries will affirm or broaden existing agreements that will smooth the path of U.S. exports to this region while providing safeguards for intellectual property.

Detractors say the agreement has little to do with expanding trade and more with weakening labor and environmental standards through a back-door race to the bottom.

Both may be right, but the issues are certainly controversial enough to merit debate.

That is not what the administration is seeking, however, as it asks for fast-track authority to get the eventual agreement through Congress with a simple up-or-down vote — no debate, no amendments, no second thoughts.

The conventional wisdom is that trade agreements are so complex and delicately balanced after sensitive negotiations over months and years that letting Congress muck around with it would make it impossible to ever get a trade pact finished.

So instead Congress is invited, on behalf of the American people, to buy a pig in a poke.

The administration is saying, as have previous administrations that sought and won fast-track authority, “Trust me.”

The problem is that trust is not a very plentiful commodity in today’s Washington. President Barack Obama’s low approval ratings are evidence that, after his misfires on health care, budget, immigration and foreign policy, neither Democrats nor Republicans are eager to give him a blank check for trade or anything else.

While a bill introduced earlier this month to grant Obama trade promotion authority is labeled “bipartisan,” that fig leaf comes only from including Sen. Max Baucus as sponsor, though the Montana Democrat will be leaving the Senate soon to take up his appointment as ambassador to China.

No other Democrats in the House or Senate are lending their names to the bill, complaining that it does too little to keep lawmakers informed about negotiations or let them provide input.

The only other Senate sponsor so far is Orrin Hatch, R-Utah, ranking member of the Senate Finance Committee. The bill was introduced in the House by Rep. Dave Camp, R-Mich., chairman of the House Ways and Means Committee, and he has so far found only two other Republican congressmen to get on board.

It’s hard to square an agenda of boosting American wages, including the minimum wage, with introducing new competition with low-wage countries.

A dozen senators in the Democratic caucus wrote a letter to Senate Majority Leader Harry Reid of Nevada calling fast-track authority as described in the Camp-Baucus bill “outdated and inadequate,” and Reid indicated that no TPA bill would be coming to the Senate floor any time soon, given the controversy.

Obama is expected to bring up the trade pacts once again in his State of the Union address next week because he views both TPP and the Transatlantic Trade and Investment Partnership as potentially signature accomplishments for his legacy.

But it looks increasingly like he will be faced with a stark choice — he must abandon plans to get a classic fast-track approval and opt for a more consultative process, or forget about any wide-ranging trade agreements.

### Obama No Push the Plan

Obama won’t fight the plan

Stirewalt 9/10/13 [Chris, digital politics editor for Fox News, Can Obama take credit for his own defeat?, http://www.foxnews.com/politics/2013/09/10/can-obama-take-credit-for-his-own-defeat/]

It was going to be big news because it was going to be just the sort of thing Obama almost never does. Risking his political capital on an unpopular policy hasn’t really been Obama’s bag since his health law creaked over the finish line in 2010. Once ObamaCare was on the books, the idea was to just survive past re-election. And then, once re-elected, to just get through midterms.

Obama’s hyper-reactive, base-nuzzling brand of politics forbids much risk taking.

On national security, Obama has been particularly unwilling to take ownership**.** He abandoned his goldilocks surge strategy for Afghanistan on the nation’s doorstep, waved away concerns about his huge expansions of domestic spying and mostly sidestepped his own intervention in Libya**,** particularly once American-backed Islamists there turned on their benefactors last year.

Ending unpopular wars or announcing the death of the world’s most hated man? Obama’s your man. Defending his own national security policies? Better call John McCain.

#### Obama won’t push the plan

Jack Goldsmith 13, Henry L. Shattuck Professor at Harvard Law School, Feb 13 2013, “The President’s SOTU Pledge to Work With Congress and Be Transparent on National Security Issues,” www.lawfareblog.com/2013/02/the-presidents-sotu-pledge-to-work-with-congress-and-be-transparent-on-national-security-issues/

As for a broader and sturdier congressional framework for the administration’s growing forms of secret war (not just targeted killing, but special forces activities around the globe, cyber attacks, modern forms of covert action, etc.) along the lines that I proposed last week, I also don’t think much will happen. Friends and acquaintances in and around the Obama administration told me they would cherish such a new statutory framework, but argued that Congress is too political, and executive-congressional relations too poisonous, for anything like this to happen. There is some truth in this charge, although I sense that Congress is preparing to work more constructively on these issues. But even in the face of a very political and generally unsupportive Congress, Presidents tend to get what they want in national security when they make the case publicly and relentlessly. (Compare the Bush administration’s successful push for FISA reform in the summer of 2008, when the President’s approval ratings were below 30%, and Democrats controlled both houses of Congress; or FDR’s push in late 1940 and early 1941 – against popular and congressional opposition – to secure enactment of Lend-Lease legislation to help to British fend off the Nazis; or the recent FISA renewal legislation.) And of course the administration can never succeed if it doesn’t try hard. Not fighting the fight for national security legal reform is just another way of saying that the matter is not important enough to the administration to warrant a fight. The administration’s failure to date to make a sustained push before Congress on these issues reveals a preference for reliance on ever-more-tenuous old authorities and secret executive branch interpretations in areas ranging from drones to cyber, and an implicit judgment that the political and legal advantages that would flow from a national debate and refreshed and clarified authorities are simply not worth the effort. The administration might be right in this judgment, at least for itself in the short run. But the President has now pledged something different in his SOTU address. We will see if he follows through this time. Count me as skeptical, but hopeful that I am wrong.

### 1ar—Iran Thumps

#### Momentum preventing sanctions – Obama’s capital is key – bill would start a war with Iran

WEBER 1 – 30 – 14 senior editor at TheWeek.com [Peter Weber, What sank the Senate's Iran sanctions bill? After Obama's State of the Union speech, it looks like Democrats are going to give peace a chance, after all, <http://theweek.com/article/index/255771/what-sank-the-senates-iran-sanctions-bill>]

In mid-January it appeared that a bipartisan Senate bill threatening Iran with new sanctions was a foregone conclusion. Yes, President Obama opposed the legislation and promised to veto it, but supporters of the Nuclear Weapon Free Iran Act strongly hinted that they had a veto-proof majority — and with 59 senators (43 Republicans and 16 Democrats) co-sponsoring the bill, that seemed eminently plausible.

They would only need eight more votes (and action in the House) to thwart Obama's veto pen, and momentum appeared to be on their side.

If there is any momentum on the bill now, it's on the other side. Obama reiterated his veto threat in the very public setting of his State of the Union address on Tuesday night, saying that "for the sake of our national security, we must give diplomacy a chance to succeed." Jan. 20 marked the beginning of a six-month period of negotiations between the U.S., Iran, and five other world powers aimed at preventing Iran from developing a nuclear bomb.

The negotiations won't be easy, and "any long-term deal we agree to must be based on verifiable action," not trust, Obama said. But "if John F. Kennedy and Ronald Reagan could negotiate with the Soviet Union, then surely a strong and confident America can negotiate with less powerful adversaries today."

After the speech, at least four Democratic cosponsors — Sens. Chris Coons (Del.), Kirsten Gillibrand (N.Y.), Joe Manchin (W.Va.), and Ben Cardin (Md.) — said they didn't want to vote on the bill while negotiations are ongoing. Sen. Richard Blumenthal (D-Conn.) had already adopted that position earlier in the month.

The distance these cosponsors put between themselves and the bill wasn't uniform. Cardin punted to Sen. Harry Reid (D-Nev.), who is opposed to bringing the bill to the floor for a vote. (Cardin "wants to see negotiations with Iran succeed," a spokeswoman's said. "As for timing of the bill, it is and has always been up to the Majority Leader.")

Manchin, on the other hand, told MSNBC that he didn't sign on to the bill "with the intention that it would ever be voted upon or used upon while we were negotiating," but rather "to make sure the president had a hammer if he needed it." He added: "We've got to give peace a chance here."

With the list of Democratic cosponsors willing to vote for the bill shrinking by five, the dream of a veto-proof majority in the next six months appears to be dead. Even Republican supporters of the legislation are pessimistic of its chances: "Is there support to override a veto?" Sen. Jim Inhofe (R-Okla.), the top Republican on the Senate Armed Services Committee, told National Journal on Wednesday. "I say, 'No.'"

So, what happened to the Iran sanctions bill? The short version: Time, pressure, and journalism.

The journalism category encompasses two points: First, reporters actually read the legislation, and it doesn't quite match up with the claims of lead sponsors Sen. Robert Menendez (D-N.J.) and Sen. Mark Kirk (R-Ill.), who say the sanctions would only take effect if Iran was found to be negotiating in bad faith. A much-cited analysis by Edward Levine at the Center for Arms Control and Non-Proliferation showed that the Iran sanctions would kick in unless Obama certified a list of impossible or deal-breaking conditions.

Journalists also started asking the cosponsors about their intentions. It's possible there were never 59 votes for the bill, but the legislation was filed right before Christmas and many reporters (not unreasonably) conflated cosponsorship with support for the bill, regardless of what was happening with the negotiations. They only asked on Tuesday night and Wednesday because Obama brought up the issue in his State of the Union speech.

Time without action always saps momentum, but with the Iran sanctions bill it also allowed events to catch up with the proponents of new sanctions. When they filed the bill Dec. 20, the interim Iran deal was just a talking point; a month later it was reality. The Obama administration, U.S. intelligence community, and outside analysts agree that new sanctions would scuttle the deal, and its harder to take that risk when that deal is in effect.

Finally, critics of the bill — including the White House and J Street, the liberal pro-Israel lobbying group — had time to mount a counterattack. Starting Jan. 6, J Street and other groups opposed to the legislation "reached out to senators who were on the fence and senators who'd cosponsored on day one," says Slate's David Weigel. "The message was the same: Have you guys read this thing?" Dylan William, J Street's director of government relations, describes the strategy in more depth:

We made especially prodigious use of our grass tops activists. These are people who have longstanding relationships with members of Congress to express two things. One: The bill is bad policy. Two: There was no political reason that these senators should feel they need to support the bill. There is deep political support in communities for members of Congress and senators who want to reserve this peaceably. [Slate]

So take a bow, J Street — for now, the David of the Israel lobby has slain its Goliath, the American Israel Public Affairs Committee (AIPAC), which is pushing for the legislation. That could all change if the interim Iran deal falls apart or some other event intercedes to change the equation for lawmakers. But momentum is hard to un-stall, and lawmakers are now considering changing the bill into a non-binding resolution.

John Judis at The New Republic is relieved, and counts Obama's veto threat Tuesday night as the boldest part of his speech. "If these negotiations with Iran fail, the United States will be left with very unsatisfactory alternatives," he writes:

Use military force to stop Iran, which might only delay Iran's acquisition of nuclear weapons, and will potentially inflame the region in a new war, or allow Iran to go ahead and hope to contain Iran as we have contained other potentially hostile nuclear powers. Obama may not be able to secure authorization for the first alternative... and if he opts for the second, he will leave open the possibility of regional proliferation or of Israel going to war against Iran. It's in America's interest — and, incidentally, Israel's as well — to allow the current negotiations to take their course — without malignant interference from Congress and AIPAC. [New Republic]

### Attacks Now

#### **Real and coming now**

Daheem 1/5 -- writer for the Frontier Post, a leading Pakistani journal (Muhammad, "Cyber Warfare," The Fronteir Post, January 5, 2014, http://www.thefrontierpost.com/article/66472/Cyber-warfare/)

Cyber war is a new domain in warfare. It is now acknowledged as “the fifth domain of warfare.” Its target and objective is cyberspace. Professor Alexander Merezhko defines cyber war “as the use of Internet and related technological means by one state against political, economic, technological and information sovereignty and independence of any other state.” Richard A. Clarke, in his book Cyber War, defines “Cyber-warfare” as “actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.”
Pakistan, just like several other countries, will have to face the challenge of Cyber war in the near future. The question is: does Pakistan have the ability to counter sophisticated cyber-attacks? In case of cyber-attacks Pakistan will have to fight back in self-defense. It should have a concrete counterattack strategy and capability to trace attacks to their origin and fight back against enemies. The Defense Ministry and other government agencies should take concrete measures for this purpose. Cyber-attack demands sophisticated and complex technology. Computers and satellite play an important role in cyber warfare. It is just possible that a foreign enemy may try to intrude into the computer system of a government agency or military installation to steal secret information. The intruder may try to disrupt the system or temper with the data to harm the national integrity. The enemy may try to create national security breaches. Sometimes cutting undersea communication cables is also part of the cyber-attack.
The typical target sites or services can be banks and credit card services. These attacks can be devastating and may disrupt the economy of the country. The enemy can also target industry, academia, military, navy and air force and space domains.
Potential targets in internet sabotage may include: web, the Internet Service Providers, various types of data communication mediums and network equipment etc. Then there are certain criminal activities such as commercial espionage or theft of intellectual property. These pieces of information can be used for sabotage purposes. Several specific attacks like Titan Rain and Moonlight Maze have already occurred in the United States of America. In Cyber war secret information can be obtained for military, political and financial purposes from individuals, competitors, rivals, and governments. It has a vast battlefield and command-and-control system. All the services depending on computers such as banking and finance, transportation, manufacturing and medical education are under cyber threat. The cyber war may also involve electrical grids. America had blamed China and Russia for infiltration in the U.S. electrical grid system in 2009. The North American Electric Reliability Corporation (NERC) has warned that that the electrical grid is not adequately protected from cyber-attack. China has denied any intruding into the US electrical grid system.
Indian government is also under cyber-attack. There are at least 23 reports of Indian cyber security breaches. Nonetheless, it is thwarting attacks against heavy odds in the field of energy, transport, banking, telecom, defense, space and other sensitive areas. It is reported that Chinese ‘nationalist hackers’ attacked CNN in 2008. Russia started a cyber-attack on the Georgian government in 2008. These examples simply show cyber-attacks can be politically motivated worldwide. Sometimes cyber-attacks are as dangerous as biological attacks. The cruel attacks are made time and again without any particular information about the attackers.
It is reported that more than 120 countries are making efforts to develop ways to use internet as a weapon. Some are already using it as a weapon. George W. Bush, the former American President, once informed the Reuters news agency that “the U.S. has already launched attacks on computer networks in other countries.” In June 2012 the New York Times reported that “President Obama had ordered the cyber-attack on Iranian nuclear enrichment facilities.” The major targets, in general, are financial markets, government computer networks and utilities.
Several countries including Russia, Iran, Israel and North Korea have already organized themselves in this field. Iran claims that it has second-largest cyber-army in the world. It is just possible that wars may have a different style by the mid-21st century.
America has a severe shortage of computer security specialists. It has about 1000 qualified persons in this field while it needs 20,000 to 30,000 skilled experts. On the other hand North Korea has more than 3,000 highly trained hackers. It is reported that several organizations are using “information warfare units” to develop viruses to attack enemy computer systems and networks, and those units include civilian computer professionals. These organizations are constantly developing their programs and capabilities to counter any potential cyber threat.
The use of computers and the Internet to conduct warfare in cyberspace can be a threat to national security. It can be used to “attack, degrade, and disrupt communications and the flow of information.” Internet has posed certain threats to the Armed Forces of powerful countries. Potential targets in internet sabotage may include: web, the Internet Service Providers, various types of data communication mediums and network equipment etc.
Several countries including the United States, India, Russia, Canada, China and France deny any involvement in cyber-spying and unorthodox attacks. Several countries have expanded and developed their cyber capabilities. The advanced countries are now using “new space-based surveillance and intelligence gathering systems, anti-satellite weapon, anti-radar, infrared decoys, and false target generators” to obtain the required results.
A cyber-worm, named Stuxnet, was infiltrated in the Iranian computers by the joint efforts of the United States of America and Israel to destroy perhaps more than 1000 nuclear centrifuges in Iran. It reduced the efficiency of Tehran’s nuclear program for a limited period and possibly put it two years back. Iran, on the other hand, has been accused by western analysts of its own cyber-attacks against the United States, Israel and Gulf Arabs. Iran has denied all these charges. The conflict between Iran and the United States of America is the beginning of the first ever cyber-war between the two countries. Cyber-attacks can cripple the economy of the nation, change its political scenario and reduce its military strength.
The Indian Cyber Army, a group of cyber organization, hacked the website belonging to Pakistan Army on 26 November 2010. It also hacked websites belonging to different ministries, including the Ministry of Foreign Affairs, Ministry of Education, Ministry of Finance, Pakistan Computer Bureau, Council of Islamic Ideology, etc. The website of India’s investigating agency, the Central Bureau of Investigation (CBI) was hacked by a group calling itself the Pakistan Cyber Army. The event happened on 4 December, 2010.
South Korea’s major banks Shinhan Bank, Woori Bank, Nong Hyup Bank and several broadcasting stations were hacked In March 2013. These events affected more than 30,000 computers. To avoid military attacks in cyberspace Obama and Vladimir Putin agreed to install a “secure voice communications line” between the US and Russia in June 2013.The world faces a real and credible threat from hostile states and governments. These attacks can ruin the economy of the world.

### No PC TPA

#### Baucus leaving ensures a push for passage

#### No PC on TPA

Foreign Policy 1 – 29 – 14 [Is Obama Even Trying on Trade?, <http://shadow.foreignpolicy.com/posts/2014/01/29/is_obama_even_trying_on_trade>]

The president faces an enormous challenge on trade. He has built much of his Asian foreign policy around the Trans-Pacific Partnership (TPP) and much of his European foreign policy around the Transatlantic Trade and Investment Partnership (TTIP). In each case, he did so on the promise to our international partners -- explicit or implicit -- that he would sooner or later bring Congress around.

It is now later. The TPP was nominally to conclude last year. Other countries' trade ministers have stated their desire to see it wrap up as soon as possible. They are waiting on White House efforts to win a negotiating mandate from Congress (known as TPA). While such a measure has met some Republican opposition, the most serious challenge has come from Democrats, particularly in the House. The Senate looked safer, at least before the president sent the bill's key Democratic backer, Finance Committee Chairman Max Baucus (D-MT), off to Beijing.

In the House, members of the president's party have voiced skepticism about what trade deals do. They believe those deals cost jobs, damage the environment, and harm workers. A key part of the president's task in his State of the Union address was to speak to these members of his party and their constituents watching at home. He had to persuade them that, while he had once espoused such positions and empathized, the critics were mistaken. Instead, here was the sum total of the president's pitch:

"...when 98 percent of our exporters are small businesses, new trade partnerships with Europe and the Asia-Pacific will help them create even more jobs. We need to work together on tools like bipartisan trade promotion authority to protect our workers, protect our environment and open new markets to new goods stamped 'Made in the USA.'"

Even had the president made this statement at the beginning of last summer, when discussions were just starting up on the TPA, it would have been cursory. Few people are persuaded by the bare assertion that their strong beliefs are false and the opposite is true

. Usually, to change minds, some supporting detail is required, some evidence, or a carefully structured argument. Weak mercantilist claims are easily rejected by skeptics (e.g. if trade is good because exports bring jobs, what does it mean when we run a trade deficit and imports exceed exports?).

Not only did the president fail to make much of a sales pitch, but his vague call to ‘work together' comes at a time when a bipartisan bill has been crafted and the battle lines are drawn. By not mentioning the bill, nor taking a stance on the controversial facets under debate -- currency provisions, intellectual property protection clauses, trade adjustment assistance -- the White House remains on the sidelines, hoping that TPA will simply fall into its lap without much expenditure of effort or political capital.

Success on the trade front was going to require experienced leadership in the Congress and a concerted public and private persuasion campaign from the President. Instead, the last month has brought the removal of an irreplaceable Capitol Hill proponent and noncommittal nods from the White House. This does not bode well.

## OLC CP

### 1AR Solvency Defecit

#### OLC lawyers are political appointees and will bend to presidential pressure --- no effective internal oversight to ensure independence.

Ross L. Weiner, February 2009. JD May 2009 @ George Washington University Law School. “THE OFFICE OF LEGAL COUNSEL AND TORTURE: THE LAW AS BOTH A SWORD AND SHIELD,” THE GEORGE WASHINGTON LAW REVIEW, 77 Geo. Wash. L. Rev. 524, Lexis.

The OLC, located in the Department of Justice in the executive branch, is often referred to as the "Attorney General's lawyer." [n18](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n18) The OLC is tasked with writing legal opinions on behalf of the Attorney General, and it provides its own written opinions in response to requests from the White House Counsel, various agencies of the executive branch, and offices within the Department of Justice. [n19](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n19) The OLC also provides legal advice to the executive branch "on all constitutional questions and [assists in] reviewing pending legislation for constitutionality." [n20](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n20)

The OLC derives its authority from both Congress and the Attorney General. The Attorney General has delegated to the OLC responsibility for preparing the formal opinions of the Attorney General, rendering opinions to the various federal agencies, and assisting  [\*528]  the Attorney General in the performance of his function as legal adviser to the President. [n21](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n21)

The importance of the OLC cannot be overstated; it has been called "the most important legal office in the federal government." [n22](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n22) When the OLC issues an opinion, it is the binding interpretation for the entire executive branch. [n23](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n23) This signifies that everyone in the executive branch, including the legal staffs of other offices (e.g., the Department of Defense), must abide by the OLC's rulings. Thus, the OLC is the definitive arbiter on critical legal issues. [n24](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n24)

According to Theodore Olson, a former Assistant Attorney General and head of the OLC, the role of the OLC is to determine for the Attorney General and the President how the courts will rule on a given matter:
It is not our function to prepare an advocate's brief or simply to find support for what we or our clients might like the law to be; rather, OLC seeks to make the clearest statement of what we believe the law provides and how the courts would resolve the matter... . The Attorney General is interested in having us provide as objective a view as possible. [n25](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n25)
[\*529]  William Barr, a former head of the OLC and a former Attorney General under the first President Bush, concurred in this assessment. [n26](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n26) He stated that the OLC must "reach sound legal conclusions, even if sometimes they are not the conclusions that some may deem to be politically preferable [to the administration]." [n27](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n27)

Although this proposition sounds simple in concept, in reality it is laden with problems. The OLC consists of lawyers who are appointed by the President, in part because of a shared ideology. [n28](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n28) Thus, when a President seeks legal advice with a certain result in mind, an OLC attorney must deal with competing loyalties: his ethical obligation to discern the law, and his desire to serve the President who appointed him in the first place.

B. The OLC's Ethical Considerations [n29](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n29)
Government lawyers have always faced the issue of competing loyalties: are they appointed to uphold the Constitution for the populace, or to serve the current administration by helping it accomplish its objectives? This issue is even more pronounced for lawyers in the OLC. Robert Jackson, who served as Attorney General under President Franklin Delano Roosevelt, believed that a government lawyer's responsibility is different from that of a private defense attorney in a criminal trial. [n30](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n30) Specifically, a government attorney is not "quite as free to advocate an untenable position," even if his client desires it, because he "is the legal officer of the United States" and has "a responsibility to others than the President." [n31](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n31) The Torture Memo presents this issue clearly: the OLC had to choose between determining  [\*530]  what the law on torture and interrogation was, and advocating a position that the White House sought. [n32](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n32)

According to one scholar, the OLC's Torture Memo (along with others) crossed the line demarcating ethical advice from pure advocacy. [n33](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n33) "[The OLC attorneys] did not enable the client to make an intelligent and informed decision on the basis of real, not fanciful, law. To this extent, the [Torture Memo] writers failed their clients by not fully and frankly explicating the law." [n34](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n34) Furthermore, he believes that the OLC violated the rules of professional responsibility in drafting the Torture Memo. [n35](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n35)

C. The OLC's Oversight Mechanisms
Currently, the OLC is subject to oversight within the executive branch by the Department of Justice's Office of Professional Responsibility ("OPR"). [n36](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n36) The OPR reports directly to the Attorney General and Deputy Attorney General. [n37](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n37) The OPR "has jurisdiction to investigate allegations of misconduct involving Department attorneys that relate to the exercise of their authority to ... provide legal advice." [n38](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n38)

Theoretically, the OPR would provide a sufficient check on lawyers in the OLC to ensure that they would abide by the OLC's best practices. [n39](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n39) In reality, the OPR has been described as a "paper tiger, which is most often used to create the appearance of investigation to clear its own attorneys." [n40](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n40) Critics argue that OPR investigations are merely for show, and are used "to give the appearance of investigation without any substantive action." [n41](http://www.lexisnexis.com.proxy.library.emory.edu/lnacui2api/frame.do?tokenKey=rsh-20.578738.7381538657&target=results_DocumentContent&returnToKey=20_T18153792478&parent=docview&rand=1379283218067&reloadEntirePage=true#n41)

#### **Lack of statutory clarification means we have NO DETERRENCE POSTURE the exec is in a zone of twilight – only stator clarification solves.**

Huston 11 (Warner Todd Huston Political analyst, and freelance writer, <http://www.conservativecrusader.com/articles/we-need-rules-for-cyberwarfare-before-a-president-steals-that-power-too>)

**Presidents** have had certain restrictions for war-making ever since because the founders wanted to make sure that war was something duly considered not easily engaged.

 **This should** hold as much for use of computer-based warfare as it does for any other type of military attack. **Currently** computer-based war, or cyberwarfare, presents a new field of military application and we have no legal precedent to govern its use.

**Despite the last 200 years of presidents slowly stealing away power from Congress to initiate military actions, we should really think long and hard about allowing any president to unleash cyberwarfare at his discretion**. In fact, we should set a precedent immediately to prevent any president from using cyberwarfare without the consent of Congress**.**

Why? Because cyberwarfare is a far, far different animal than use of conventional military forces and indiscriminate use of it **would endanger** our way of **life** in harsh and immediate terms if used against us. For that reason, **we should be very careful when we use it against others**. We should have solid legal definitions behind its use so as not to give enemies the excuse to resort to it quickly themselves.

You see, cyberwarfare is a relatively cheap war power, easier to implement, and requires far fewer in personnel and facilities than launching an invasion using conventional military forces. This is not to say that cyberwarfare is easy -- far from it. But it is cheaper and easier than deploying regular military forces.

So, we should casually resort to cyberwarfare no more easily than we would to using conventional forces. But **if we do not set down** specific and binding rules for its use we risk giving this power over to a president which could cause less considered use of this sort of warfare. **That** in turn, would give enemies an excuse to do the same. Further, remember that setting legally binding reasons for warfare is a long and proud American tradition, one that legitimizes our nation and one we should not casually toss aside simply under the assumption that enemies will not be as thoughtful as we.

**We should lead the world in** **considered** **use of cyberwarfare** **and we should do so now**. Any of those that felt we illicitly launched into the war on terror should no less worry about indiscriminate use of cyberwarfare. But illicit use or no, **we should be** deadly certain of what powers our president can have**,** **when and how he can use them, and where the line should be drawn, even in cyberspace.**

### CP Links

#### Executive orders link – high scrutiny now

NYT 1 – 29 – 14 http://www.nytimes.com/2014/01/29/us/politics/executive-order-may-be-only-option-but-it-comes-with-limits.html

If Congress cannot move on economic and social policy that Democrats and Republicans essentially embrace and that would be a political victory for both parties, how can real disagreement be bridged?

Finding consensus only gets harder from here. The midterms are already taking over the conversation on Capitol Hill, intensifying scrutiny on every vote and making lawmakers even more reluctant to take chances. The growing sense that Republicans have a chance to win the Senate in November raises the prospect that the president’s final two years could be consumed by veto fights with opposition majorities in the House and Senate.

Republicans criticized the president’s focus on executive action as counterproductive. “Circumventing Congress won’t foster job creation and won’t result in economic growth,” said Senator Jeff Flake of Arizona.

The approach will also feed the conservative narrative that Mr. Obama is engaged in a power grab and is ignoring constitutional limits. They point for validation to the so-far-successful legal challenge to his use of recess appointments in a case now before the Supreme Court.

“We’re going to watch very closely because there’s a Constitution that we all take an oath to, including him, and following that Constitution is the basis for our republic and we shouldn’t put that in jeopardy,” Speaker John A. Boehner said hours before the president’s address on Tuesday.

Mr. Boehner said House Republicans would use a retreat that starts Wednesday to examine their options when it comes to the president’s use of executive authority. They could conceivably file suit or employ legislative tools to seek disapproval of disputed executive orders. Even if they cannot get the disapprovals through Congress, they can use the fight to highlight the president’s actions to motivate Republican voters in November.

Mr. Obama’s allies say he cannot stand idle while Republicans, driven by political calculations, block worthwhile legislation that has widespread popular support. They say executive orders can create momentum and note that some — like the Emancipation Proclamation, the order by President Harry S. Truman to desegregate the military and President Bill Clinton’s expansion of public lands through the declaration of national monuments — have been transformative.

And they say Congressional Republicans have driven Mr. Obama into finding a way to get something done.

“Should he have to wait because of the intransigence, the obstacles that are placed by Republicans or because the Republicans would prefer to shut down our government?” asked Representative Xavier Becerra, Democrat of California.

Representative Joseph Crowley, Democrat of New York, conceded that governance by executive order is not ideal but was justifiable given the depth of Republican opposition.

“This is not a panacea, this is not the fix we are looking for,” he said of the president’s action on wages. “But he is leading by example, sending a message to Congress that we need to raise the minimum wage for all Americans.”

But for Mr. Obama, who began his presidency with a gauzy vision of a post-partisan brand of politics that proved to be unrealistic, leading through executive order is not what he had in mind.

## Iran Politics

### Deal Fails

#### Kessler is from a retired general and a huff post blog Dialogue risks Israeli strikes – and won’t stop prolif – dialogue failure is better. Friedman ev has NO qualifications literally businessinsider.

CARAFANO 10 – 17 – 13 vice president for defense and foreign-policy studies at Heritage [James Jay Carafano, President Barack Obama, Iran and Israel, <http://www.heritage.org/research/commentary/2013/10/negotiations-with-iran-could-start-a-war>]

War is a great leap into the dark. It is a chancy affair to predict when a particular act will end with the troops going over the top.

Still, one can't help but worry that President Obama's plan to negotiate with Tehran one more time might bring Israel one step closer to a direct military confrontation with Iran. Here is why.

It doesn't take a crystal ball to guess how the latest diplomatic minuet between the Iranian regime and the Obama administration will end. There will be no halt in Iran's nuclear weapons program.

The Iranian regime sees three key strategic purposes for having the bomb: -One is so the mullahs can continue to oppress their own people without fear of intervention from the outside.

When you have a nuclear weapon, no one seriously attempts to meddle in your internal affairs. That was a lesson President Dwight Eisenhower learned during the Cold War, when he had to hastily abandon his "rollback" strategy. Regime change by force is just too risky when the regime has nukes.

-The second reason Iran wants to go nuclear is that it believes such weaponry will allow it to pursue a much more muscular policy in establishing dominance in the region. Tehran rightly figures that few nations will want to risk resistance that might escalate to nuclear conflict. With a nuke in its hip pocket, it will be much easier for the regime to push its neighbors around.

-It will also allow Iran to hold the "great powers" hostage. True, Tehran would lose a nuclear war with any major power. But what major power would be willing to risk losing even a single city to keep Iran's regional ambitions in line? Together, Tehran sees nukes as a golden ticket, guaranteed to perpetuate the revolution. No matter what Iran's leaders might say for public consumption, they will never agree to anything that would keep them from getting the bomb.

Iran has a new president, Hassan Rouhani, but the same old overlord. And that overlord's views haven't changed: Negotiations are fine if they help the regime crack the sanctions that are strangling the economy, but that is their only purpose. For Tehran, negotiations remain a short-term ploy for winning economic relief, not a game-changer in U.S.-Iranian relations.

The Israelis know the current Obama-Rouhani waltz is a dead end. And they know that if Iran dupes the West into easing sanctions, the prospects of the mullahs going nuclear become more - not less - likely. And that is something Israel cannot let happen.

The more Tel Aviv sees developments trending that way, the more pressure its leaders will feel to take matters into its own hands. And that makes dropping bombs more, not less, likely.

Israel-Iran is not like North Korea-South Korea. South Korea could be less apoplectic about the north going nuclear because they have American troops sitting on the DMZ. South Korea also rests much more comfortably under the American nuclear umbrella. Not so for Israel.

Plus the Israelis are not just worried about Iran. They are worried about the whole neighborhood. It is widely believed that, if Iran gets the bomb, many of its neighbors - including Saudi Arabia, Turkey and Egypt - will feel compelled to get nuclear arsenals of their own.

After all, they don't want to be bullied by Iran. A neighborhood bristling with nukes scattered among mutually distrustful nations is a neighborhood that few will feel safe in.

In reality, it is improbable that Israel could eliminate an Iranian weapons program with one swift, decisive military strike. Thus, if Israel were to attack, it would only be the opening gambit in a long and dangerous confrontation.

That is not a happy prospect. Sadly, Obama's faux dialogue with Rouhani increase the chances that Israel will feel compelled to run that course.

#### Delaying the deal is the only way to stop Iranian nuclearization which turns their impact

BOLTON 11 – 19 – 13 Former US ambassador to the UN, Former Under Secretary of State for Arms Control and International Security [John R. Bolton, Desperate for a deal - even if it helps Iran get a bomb, <http://www.aei.org/article/foreign-and-defense-policy/regional/middle-east-and-north-africa/desperate-for-a-deal-even-if-it-helps-iran-get-a-bomb/>]

Barack Obama seems poised this week to reach an agreement with Iran on its nuclear-weapons program in talks that resume Wednesday. Negotiations came unstuck this month in Geneva either because France felt the terms too favorable to Iran, because Iran refused to compromise its “right” to enrich uranium, or both. The outcome embarrassed President Obama and fortified Tehran’s view that he is desperate for a deal on almost any basis.

Secretary of State John Kerry has spared no effort to avoid another Geneva debacle, almost certainly making more concessions to Iran to secure agreement. The failed deal was certainly wretched from America’s perspective, involving countless problems and deficiencies. This week’s deal will be worse.

It is no answer that Obama is seeking merely an “interim” understanding with Iran. “Interim” concessions have a way of getting locked-in, as seemingly ad hoc trade-offs freeze into permanence. Indeed, Obama’s “step-by-step” approach itself tells Tehran’s mullahs how desperately Obama wants a deal, and how willingly he ignores the reality that Iran’s nuclear program has never been peaceful.

But there is a larger point here, beyond whatever specific terms emerge this week in Geneva. The West’s efforts to negotiate with Iran are doomed to failure because the parties’ objectives are utterly incompatible. A decade of abortive negotiations alone demonstrates this basic truth, which Iran’s ongoing diplomatic “charm offensive” cannot obscure.

Obama sees negotiations as deflecting the threat of Iranian nuclear weapons. Iran sees them, by contrast, as helping ensure success for that very weapons program. There is simply no compromise between these objectives. There are no “bridging proposals” that can overcome irreconcilable differences.

Tehran’s primary negotiation objective is to eliminate the threat of military strikes against its nuclear program. Despite Obama’s rhetoric that “all options are on the table,” no one believes he will use force. And who knows what private assurances Obama or Kerry have already given the ayatollahs (a fruitful area for congressional inquiry)? That leaves Israel, which the Obama administration is pressuring unmercifully, not just on Iran but also on the Palestinians. In Israel before his Geneva embarrassment, Kerry squeezed Prime Minister Benjamin Netanyahu to make more concessions to the Palestinians, implicitly green-lighting both a third intifada and continuing European efforts to delegitimize Israel in their absence. This pressure on Netanyahu, already back-breaking in Obama’s first term, is now at unprecedented levels. That means Iran is very close to its goal of neutralizing Israel.

Iran also wants relief from economic sanctions. And why not, given the economic harm they are causing? Remember, however, the mullahs are not US consumers. Threatened with a diminished lifestyle, too many Americans would concede almost anything. Not so the Islamic revolution. Tehran understands that securing even modest sanctions relief in Geneva will carry it over a critical inflection point. Instead of slowly increasing in severity, the sanctions will have decreased. To exploit Obama’s (and Europe’s) palpable diplomatic weakness, Iran will make superficial concessions, like those reported in leaks about this month’s aborted deal. President Hassan Rouhani employed precisely this strategy 10 years ago as Iran’s chief nuclear negotiator, making purely cosmetic, tactical concessions. He is using the same playbook today.

Iran knows that under existing US law, India, China and others themselves face sanctions unless they continue to reduce their imports of Iranian oil. Obama fears either having to sanction such important countries or granting them further waivers, thus undoubtedly triggering vociferous domestic political criticism that he can hardly now afford. Moreover, Iran will have won an enormous psychological victory in Beijing, New Delhi and other important capitals, which will realize that the diaphanous sanctions regime is near total collapse.

US sanctions advocates also need to acknowledge reality. Even if their policy could work to stop Iran’s nuclear efforts (which it can’t), hard-headed strategists are not administering America’s sanctions. Barack Obama is. Any policy that rests on Obama taking a tough negotiating position with Iran is doomed to failure, given his desperation for a deal, his naïveté and incompetence and his basic operating premise: He fears an Israeli military strike more than an Iran with nuclear weapons.

That is why evaluating the terms of the upcoming interim deal — who scored on this issue, who scored on that — is beside the point. The negotiation process itself buys Iran both time to continue its nuclear-weapons activities and international legitimacy. Kerry and others, even at this supposedly interim stage, are already speculating openly about ultimately normalizing relations between Washington and Tehran. This tells the ayatollahs everything they need to know.

Consider one historical analogy. In 1938, Germany wanted the Sudetenland from Czechoslovakia. It would either get the territory or not. There was no compromise position. Ask Neville Chamberlain how that worked out.

#### Deal fails – no risk of war – just delays the ability to prevent Iranian prolif.

CARAFANO 1 – 18 – 14 vice president for defense and foreign-policy studies at Heritage [James Jay Carafano, Iran Nuclear Deal Isn't an Episode of "24", <http://blog.heritage.org/2014/01/18/iran-nuclear-deal-isnt-episode-24/>]

Too many in Washington seem to regard the P5+1 nuclear deal with Iran as an episode of the once-popular TV show 24. They think the clock starts counting down on January 20, and then we’ll wait breathlessly for six months to find out whether the West has successfully sidetracked Iran’s nuclear-weapons program.

That might happen in Hollywood. But in the real world, six months from now no one will be the slightest bit more confident that Iran’s nuclear ambitions have been jettisoned.

If pressed, the White House might even admit that is true. But they will maintain that the temporizing P5+1 deal is intended mainly as a trust- and confidence-building measure. If Tehran lives up to its commitment, it will demonstrate that the regime is ready to take the next step back from nukes. If the Iranians fail to deliver, the West will go back to tightening the economic screws.

But that answer can be nothing but cold comfort to those who believe a nuclear-armed Iran really is unacceptable.

First, in the P5+1, the U.S. has already negotiated away its strongest leverage on the regime (the economic sanctions). The preemptive giveaway makes it less — not more — likely that the West will get an ironclad deal in six months. What is more likely is that Tehran will have set us up for another round of “rope-a-dope” bargaining — either stringing out negotiations even longer, or walking away as they blame the U.S. for being unreasonable.

Second, the White House knows that cracks in the sanctions regime might prove to be irreparable. Tehran will continue to find ways to bring in enough hard currency to keep the regime in comfort, even if it is not enough dough to revive Iran’s anemic economy.

It is understandable why the administration leapt at this deal. The president’s foreign policy is in tatters on every front. Nowhere does it look like more of a disaster than in the Middle East. Desperate to latch onto something that might suggest it has not lost completely its capacity to influence affairs, the Oval Office grabbed this deal, which offers a six-month reprieve from having to deal foursquare with the problem of Iran’s nuclear program.

There may even be delusional forces in the administration that believe a rapprochement with Iran is possible. Accept this magical thought, and it’s possible to dream of a friendly Iran helping to cure any number of difficult problems, from the meltdown in Iraq, to the civil war in Syria, to extricating the U.S. from Afghanistan without having that country fall into the hands of Islamists.

Indeed, some individuals in the administration may see the deal as their shot at a Nobel Peace Prize of their own.

But it’s all just fairy-dust foreign policy if Tehran is committed to having anything more than ‘just” a civil nuclear program. And the regime has given no indication that it would limit itself to such a program.

Worse, the White House seems to have no real plan B. It has already called congressional efforts to draft even tougher sanctions “warmongering.” Now, the president well knows there is virtually no chance that a tough sanctions bill will get out of Congress; Senate majority leader Harry Reid will make sure of that. And, even if a bill somehow snuck through, the president could simply veto it. So why has the White House cranked up the rhetoric? It seems desperate to rule out of bounds any suggestion that its Iran policy might fail.

Unfortunately, failure is the most likely outcome of the P5+1 charade. It might not be dramatically apparent when the clock runs out in six months. But those monitoring the nuclear clock in the Middle East know that the real issue is whether or not Iran can be dissuaded from becoming a nuclear power. And six months from now, P5+1 will have brought us no closer to answering that question.

#### Talks will fail – Iran subverts diplomatic efforts

Abrams 1/3/14( Elliot, Senior Fellow for Middle Eastern Studies at the Council on Foreign Relations, “Iran Continues Subversion Despite the Nuclear Negotiations,” 1-3-14, ¶ <http://blogs.cfr.org/abrams/2014/01/03/iran-continues-subversion-despite-the-nuclear-negotiations/>)

The Obama administration is fighting strongly to prevent Congress from adopting new sanctions legislation that would go into effect one year from now if, and only if, the nuclear negotiations fail or Iran cheats on its commitments. It seems that adopting such legislation would anger the Iranian regime, and would be contrary to the spirit of the talks. Or something like that. But while we are told to walk on eggshells lest we offend the delicate Iranians, they continue to subvert their neighbors. Not for them this idea that, because there are talks, they should stop shipping arms. Syria is the obvious case, but now we have a new one: Bahrain. This week Bahraini authorities discovered “plastic explosives, detonators, bombs, automatic rifles and ammunition” which “were found in a warehouse and onboard a boat intercepted as it was heading to the country.” To be more precise, Gulf News reported that Iranian-made explosives, Syrian bomb detonators, Kalashnikovs, C-4 explosives, Claymores, hand grenades, a PK machine gun, circuit boards for use in bomb making, armour-piercing explosives, TNT and a raft of other materials used to manufacture bombs were discovered. Is this just propaganda from the Government of Bahrain? No; I’ve checked with US authorities and these reports are accurate. This is of course very worrying for Bahrain; an Iranian campaign of subversion and terrorism could turn the tiny country into a war zone. I’ve written on this site many times about the need for progress in negotiations between the royal family and the majority-Shia population (most recently here), but obviously the Iranian subversion is not an effort to promote peace and democracy in Bahrain. It is among other things an effort to tell the Gulf Arab states that Iran can make their lives miserable if they continue to oppose its policies. It is striking that at the very moment when the Obama administration is pleading with Congress to be very careful in its behavior, the Iranian regime has no fears and no hesitation to engage in this subversion. They must have calculated that the Obama administration is so committed to these nuclear talks, and so committed to the “Rouhani narrative” –that Rouhani is a moderate and we must help him succeed– that nothing they do will affect administration policy. Sadly, and dangerously, they appear to be right. Not these arms shipments to Bahrain, nor shipments early last year to Yemen, nor the famous plot to blow up the Saudi ambassador in a restaurant in Washington, D.C. have had the slightest impact on administration policy. This helps explain why the Arabs are so nervous: they see the United States hell-bent on a nuclear deal and willing to ignore everything else the Iranian regime is doing. It’s an analogue to Obama policy in Syria, where we have embraced a deal on chemical weapons that leaves Assad free to murder as many people as he likes as long as he does not use that one method. For a couple of years after the protests began in Bahrain, Iran limited itself to broadcasting nasty material in Arabic, and did not try to subvert the country. U.S. officials repeatedly told me we simply had no evidence of armed subversion. Well, now we do. What will the American reaction be? Nothing– you see, this is a delicate moment and we don’t want to upset the nuclear talks. One can only imagine the satisfied laughter such a position causes in Tehran. And the fear it engenders in capitals like Manama, Riyadh, and Abu Dhabi.

#### Zero chance of an effective iran deal – they won’t give up their nukes

Jpost 1/21/14 (Jereusalem Post, “Iranian nukes”, http://www.jpost.com/Opinion/Editorials/Iranian-nukes-338944)

While Iran’s gestures are a positive development, there is a long way to go before its nuclear weapons project is put on ice. Most actions the Iranians have undertaken are quite reversible and the most difficult issues have been postponed to a final agreement.

The Obama administration – unlike Israel, the Saudis and other Gulf states – is willing to accept Tehran’s demand to keep some uranium enrichment capability.

Nevertheless, the US is demanding that Iran reduce the number of its centrifuges from the current 19,000 to fewer than 5,000. America is also demanding the closure of the supposedly impregnable underground enrichment facility at Fordow; the dismantling of the heavy-water nuclear reactor at Arak; an account from Iran of all its past weaponization activities; and an inspection regime even more rigorous than required by Iran’s signature of the IAEA’s “additional protocol.”

Iran has rejected most of these demands. President Hassan Rouhani has promised his people that none of Iran’s existing nuclear facilities will be destroyed; that Arak will be kept, to supply only medical isotopes; and that Iran has the right to what he calls “industrial-scale” enrichment, which could mean as many as 50,000 centrifuges.

Unfortunately, America’s leverage at the negotiating table is diminishing. The military option, at least from the US perspective, has essentially been taken off the table, at least as long as the interim agreement is in place.

And it is highly likely that this interim arrangement will be extended at least once before it becomes irrefutably clear that Iran, or at least the mullahs safely ensconced at the helm of the Islamic Republic, have no intention of abandoning their aspirations for nuclear weapon capability.

Meanwhile, Iran’s economy is recovering. The World Bank’s recently released Global Economic Prospects report projects that Iran’s real GDP is expected to grow 1% in 2014. The World Bank sees even higher GDP growth in 2015 and 2016. The International Monetary Fund also sees Iran’s economy beginning to rebound, with estimated growth of 1.3% and 1.98% in 2014 and 2015, respectively. These rosy forecasts contrast sharply with the two years of economic contraction in 2012 and 2013.

There are quite a few reasons for the Islamic Republic’s economic recovery. In part it can be attributed to an overall global resurgence. It might also have something to do with better fiscal and monetary policies implemented by Iran since Rouhani’s election in June. Also, US President Barack Obama has vowed to veto any attempts by the Senate to pass more (conditional) sanctions, which essentially serves as a green light for businesses to reestablish ties, though the Senate is getting close to the 67 votes needed to override a presidential veto.

Next week, Rouhani will be in Davos to address the World Economic Forum and court business as part of the normalization of the Islamic Republic’s status in the international community.

Prospects look bleak for any real diplomatic breakthrough.

Obama, in an extensive interview with The New Yorker’s David Remnick, estimated that the chances for a final agreement with Iran – along with resolutions of the Israeli-Palestinian and Syrian conflicts – are “less than fifty-fifty.”

In all three arenas, which Obama sees as connected, “we may be able to push the boulder partway up the hill and maybe stabilize it so it doesn’t roll back on us.” Hardly a reassuring assessment of the chances for stopping Iran’s march to nuclear weapons.

## Security / Afro-pessimism Critique

### 1AR Cyber Security good

#### Deterrence works by changing the incentive model of adversaries.

Kramer et. al 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)

Ends, Ways, and Means

The goal of a cyber deterrence strategy would be to influence an adversary’s decisionmaking calculus so decisively that it will not launch cyber attacks against the United States, its military forces, or its allies. Coordinated actions reduce the chances for attacker success, so that the dangers, costs, risks, and uncertainties of a cyber attack are perceived to outweigh any expected success, benefits, or rewards. In the case of an adversary who seeks to use threats of cyber attacks, or actual attacks, to coerce the United States into conduct that would serve its larger interests and goals, a cyber deterrence strategy will work if the adversary judges that this attempted coercion would not succeed and that the attack would provoke U.S. retaliation, resulting in a net strategic setback for the would-be attacker. For example, if Iran were to contemplate cyber attacks to try to coerce the United States into making political concessions in the Persian Gulf and Middle East, it might be deterred from this course if its decisionmakers were to judge that the cyber attack would not physically succeed in inflicting the desired damage; that even if the attack succeeded, the United States would not make the desired concessions; or that the United States would be likely to retaliate in ways that inflict unacceptable damage on Iran in return, in the cyber realm or elsewhere.

The same strategic calculus applies to Chinese use of cyber threats and attacks, as well as actions by other plausible adversaries in the cyber domain. Potential U.S. counteractions in such situations are encapsulated in the three principal ways of pursuing deterrence articulated in the JOC model: deterrence by denying benefits, deterrence by imposing costs, and deterrence by offering incentives for adversary restraint.

Deterrence by denying benefits entails credibly threatening to deprive the attacker of the benefits or gains being sought: convincing it that a cyber attack will not achieve its goals. Deterrence by imposing costs entails credibly threatening to impose costs, losses, and risks that are too painful to accept, thus convincing the adversary that punishment would outweigh any expected successes. Deterrence by encouraging restraint means convincing the adversary that not attacking will result in an acceptable, attractive outcome.

#### No risk of endless warfare

Gray 7—Director of the Centre for Strategic Studies and Professor of International Relations and Strategic Studies at the University of Reading, graduate of the Universities of Manchester and Oxford, Founder and Senior Associate to the National Institute for Public Policy, formerly with the International Institute for Strategic Studies and the Hudson Institute (Colin, July, “The Implications of Preemptive and Preventive War Doctrines: A Reconsideration”, <http://www.ciaonet.org/wps/ssi10561/ssi10561.pdf>)

7. A policy that favors preventive warfare expresses a futile quest for absolute security. It could do so. Most controversial policies contain within them the possibility of misuse. In the hands of a paranoid or boundlessly ambitious political leader, prevention could be a policy for endless warfare. However, the American political system, with its checks and balances, was designed explicitly for the purpose of constraining the executive from excessive folly. Both the Vietnam and the contemporary Iraqi experiences reveal clearly that although the conduct of war is an executive prerogative, in practice that authority is disciplined by public attitudes. Clausewitz made this point superbly with his designation of the passion, the sentiments, of the people as a vital component of his trinitarian theory of war. 51 It is true to claim that power can be, and indeed is often, abused, both personally and nationally. It is possible that a state could acquire a taste for the apparent swift decisiveness of preventive warfare and overuse the option. One might argue that the easy success achieved against Taliban Afghanistan in 2001, provided fuel for the urge to seek a similarly rapid success against Saddam Hussein’s Iraq. In other words, the delights of military success can be habit forming. On balance, claim seven is not persuasive, though it certainly contains a germ of truth. A country with unmatched wealth and power, unused to physical insecurity at home—notwithstanding 42 years of nuclear danger, and a high level of gun crime—is vulnerable to demands for policies that supposedly can restore security. But we ought not to endorse the argument that the United States should eschew the preventive war option because it could lead to a futile, endless search for absolute security. One might as well argue that the United States should adopt a defense policy and develop capabilities shaped strictly for homeland security approached in a narrowly geographical sense. Since a president might misuse a military instrument that had a global reach, why not deny the White House even the possibility of such misuse? In other words, constrain policy ends by limiting policy’s military means. This argument has circulated for many decades and, it must be admitted, it does have a certain elementary logic. It is the opinion of this enquiry, however, that the claim that a policy which includes the preventive option might lead to a search for total security is **not at all convincing**. Of course, folly in high places is always possible, which is one of the many reasons why popular democracy is the superior form of government. It would be absurd to permit the fear of a futile and dangerous quest for absolute security to preclude prevention as a policy option. Despite its absurdity, this rhetorical charge against prevention is a stock favorite among prevention’s critics. It should be recognized and dismissed for what it is, a debating point with little pragmatic merit. And strategy, though not always policy, **must be nothing if not pragmatic**.

#### We should treat war and other violence differently. The tradeoff only goes in the other direction – we lose what is distinctive about organized violence.

Tarak **BARKAWI** Associate Professor of Politics at the New School for Social Research **’12** “Of Camps and Critiques: A Reply to ‘Security, War, Violence’” *Millennium* 41 (1) p. 129-130

A final totalising move in ‘Security, War, Violence’ is the idea that the study of war should be subsumed under the category of ‘violence’. The reasons offered for this are: violence does not entail a hierarchy in which war is privileged; a focus on violence encourages us to see war in relational terms and makes visible other kinds of violence besides that of war; and that the analysis of violence somehow enables the disentangling of politics from war and a proper critique of liberal violence.22 I have no particular objection to the study of violence, and I certainly think there should be more of it in the social sciences. However, why and how this obviates or subsumes the study of war is obscure to me. Is war not historically significant enough to justify inquiry into it? War is a more specific category relative to violence in general, referring to reciprocal organised violence between political entities. I make no claims that the study of war should be privileged over that of other forms of violence. Both the violence of war, and that of, say, patriarchy, demand scholarly attention, but they are also distinct if related topics requiring different forms of theorisation and inquiry. As for relationality, the category of war is already inherently relational; one does not need the concept of violence in general to see this. What precisely distinguishes war from many other kinds of violence, such as genocide or massacre, is that war is a relational form of violence in which the other side shoots back. This is ultimately the source of war’s generative social powers, for it is amidst the clash of arms that the truths which define social and political orders are brought into question. A broader focus on violence in general risks losing this central, distinctive character of the violence of war. Is it really more theoretically or politically adequate to start referring to the Second World War as an instance of ‘violence’? Equally, while I am all for the analysis of liberal violence, another broad category which would include issues of ‘structural violence’, I also think we have far from exhausted the subject of liberalism and war, an important area of inquiry now dominated by the mostly self-serving nostrums of the liberal peace debates.

#### 2) Perticular security solutions are necessary – No one can solve the REASONS countries are attacking, we can only work on changing incentive models to deal with proximate causes. –

#### 3) We’ll preempt their deterrence bad and security arguments here—they ignore the importance of FEELING secure—only deterrence can provide competing nations with *stable*, *peaceful* *identities*—This de-escalates all violence, ends arms races and creates a norm against hostility globally—It’s the biggest impact.

Deibert 13 -- Ronald J. Deibert is professor of political science and director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto. His research interests include global security, human rights and the geopolitics of cyberspace and information controls. He has published numerous articles, chapters and books on issues related to technology, media and world politics, including co-authoring the *Tracking Ghostnet* report, which documents an alleged cyberespionage network affecting over 1,200 computers in more than 103 countries. Ronald is co-founder and principal investigator of the OpenNet Initiative and the Information Warfare Monitor, and he presently serves on the editorial board of the journals *International Political Sociology, Security Dialogue, Explorations in Media Ecology, Review of Policy Research* and *Astropolitics*. He is a consultant and adviser to governments, international organizations and civil society/non-governmental organizations on issues relating to cyber security, cybercrime, online free expression and access to information. He is a recipient of the Order of Ontario and Queen Elizabeth II Diamond Jubilee medal, and has a Ph.D. in political science from the University of British Columbia (Ronald J. "Bounding Cyber Power: Escalation and Restraint in Global Cyberspace," Internet Government Papers, Paper No. 6, October 2013

There is an urgent need for the articulation of an alternative cyber-security strategy for civic networks and from the perspective of liberal democracy. For many who would characterize themselves as part of global civil society, “security” is seen as anathema. In today’s world of exaggerated threats and self-serving hyperbole, it is easy to dismiss security as a myth to be demolished, rather than engaged.28 Securitization isgenerally associated with the defence industry, Pentagon strategists, intelligence agencies and many others question whether employing the language of security only plays into this complex. But the vulnerabilities of cyberspace are very real, the underbelly of cybercrime is undeniably huge (and growing), an arms race in cyberspace is escalating and major governments are poised to set the rules of the road that may impose top-down solutions that subvert the domain as we know it**.** Dismissing these vulnerabilities as manufactured myths propagated by power elites will only marginalize civic networks from the conversations where policies are being forged.

### 1AR – VTL / Overview

#### Comparative evidence – extinction is worse than everything

Richard Ochs 2002 DC Black Panther, president of the Aberdeen Proving Ground Superfund Citizens Coalition, member of the Depleted Uranium Task force of the Military Toxics Project and a member of the Chemical Weapons Working Group. After completing a course in Atomic and Nuclear Physics at Muhlenberg College, he transferred to the University of Maryland, where he had a split major in history and political science. He was a founding member of the Students for a Democratic Society at College Park, June 9th 2002, “BIOLOGICAL WEAPONS MUST BE ABOLISHED IMMEDIATELY”, <http://www.freefromterror.net/other_articles/abolish.html>

Potentially worse than that, bio-engineered agents by the hundreds with no known cure could wreck even greater calamity on the human race than could persistent radiation. AIDS and ebola viruses are just a small example of recently emerging plagues with no known cure or vaccine. Can we imagine hundreds of such plagues? HUMAN EXTINCTION IS NOW POSSIBLE. Ironically, the Bush administration has just changed the U.S. nuclear doctrine to allow nuclear retaliation against threats upon allies by conventional weapons. The past doctrine allowed such use only as a last resort when our nation’s survival was at stake. Will the new policy also allow easier use of US bioweapons? How slippery is this slope? Against this tendency can be posed a rational alternative policy. To preclude possibilities of human extinction, "patriotism" needs to be redefined to make humanity’s survival primary and absolute. Even if we lose our cherished freedom, our sovereignty, our government or our Constitution, where there is life, there is hope. What good is anything else if humanity is extinguished? This concept should be promoted to the center of national debate.. For example, for sake of argument, suppose the ancient Israelites developed defensive bioweapons of mass destruction when they were enslaved by Egypt. Then suppose these weapons were released by design or accident and wiped everybody out? As bad as slavery is, extinction is worse. Our generation, our century, our epoch needs to take the long view. We truly hold in our hands the precious gift of all future life. Empires may come and go, but who are the honored custodians of life on earth? Temporal politicians? Corporate competitors? Strategic brinksmen? Military gamers? Inflated egos dripping with testosterone? How can any sane person believe that national sovereignty is more important than survival of the species? Now that extinction is possible, our slogan should be "Where there is life, there is hope." No government, no economic system, no national pride, no religion, no political system can be placed above human survival. The egos of leaders must not blind us. The adrenaline and vengeance of a fight must not blind us. The game is over. If patriotism would extinguish humanity, then patriotism is the highest of all crimes.

### Links

#### State key to solve warming

Monbiot 08 (George Monbiot, English Writer and Environmental and Political Activist, 9-4-2008, “Identity Politics in Climate Change Hell,” http://www.celsias.com/article/identity-politics-climate-change-hell/)

If you want a glimpse of how the movement against climate change could crumble faster than a summer snowflake, read Ewa Jasiewicz’s article , published on the Guardian’s Comment is Free site. It is a fine example of the identity politics that plagued direct action movements during the 1990s, and from which the new generation of activists has **so far been mercifully free**. Ewa rightly celebrates the leaderless, autonomous model of organising that has made this movement so effective. The two climate camps I have attended – this year and last – were among the most inspiring events I’ve ever witnessed. I am awed by the people who organised them, who managed to **create**, under extraordinary pressure, **safe, functioning, delightful spaces in which we could debate the issues and plan** the **actions** which thrust Heathrow and Kingsnorth into the public eye. Climate camp is a tribute to the anarchist politics that Jasiewicz supports. But in seeking to extrapolate from this experience to a wider social plan, she makes two grave errors. The first is to confuse ends and means. She claims to want to stop global warming, but she makes that task 100 times harder by rejecting all state and corporate solutions. It seems to me that what she really wants to do is to create an anarchist utopia, and use climate change as an excuse to engineer it. Stopping runaway climate change **must take precedence over every other aim**. Everyone in this movement knows that there is very little time: the window of opportunity in which we can prevent two degrees of warming is closing fast. We have to use all the resources we can lay hands on, and these must include both governments and corporations. Or perhaps she intends to build the installations required to turn the energy economy around - wind farms, wave machines, solar thermal plants in the Sahara, new grid connections and public transport systems - herself? Her article is a terryifying example of the ability some people have to put **politics first and facts second** when confronting **the greatest challenge humanity** now **faces**. The facts are as follows. Runaway climate change is bearing down on us fast. We require a massive political and economic response to prevent it. Governments and corporations, whether we like it or not, currently control both money and power. Unless we manage to mobilise them, we stand a snowball’s chance in climate hell of stopping the collapse of the biosphere. Jasiewicz would ignore all these inconvenient truths because they conflict with her politics. “Changing our sources of energy without changing our sources of economic and political power”, she asserts, “will not make a difference. Neither coal nor nuclear are the “solution”, we need a revolution.” So before we are allowed to begin cutting greenhouse gas emissions, we must first overthrow all political structures and replace them with autonomous communities of happy campers. All this must take place within a couple of months, as there is so little time in which we could prevent two degrees of warming. This is magical thinking of the most desperate kind. If I were an executive of E.On or Exxon, I would be delighted by this **political posturing**, as it provides a **marvellous distraction** from our real aims. To support her argument, Jasiewicz misrepresents what I said at climate camp. She claims that I “confessed not knowing where to turn next to solve the issues of how to generate the changes necessary to shift our sources of energy, production and consumption”. I confessed nothing of the kind. In my book Heat I spell out what is required to bring about a 90% cut in emissions by 2030. Instead I confessed that I don’t know how to solve the problem of capitalism without resorting to totalitarianism. The issue is that capitalism involves lending money at interest. If you lend at 5%, then one of two things must happen. Either the money supply must increase by 5% or the velocity of circulation must increase by 5%. In either case, if this growth is not met by a concomitant increase in the supply of goods and services, it becomes inflationary and the system collapses. But a perpetual increase in the supply of goods and services will eventually destroy the biosphere. So how do we stall this process? Even when usurers were put to death and condemned to perpetual damnation, the practice couldn’t be stamped out. Only the communist states managed it, through the extreme use of the state control Ewa professes to hate. I don’t yet have an answer to this conundrum. Does she? Yes, let us fight both corporate power and the undemocratic tendencies of the state. Yes, let us try to crack the problem of capitalism and then fight for a different system. But let us not confuse this task with the immediate need to stop two degrees of warming, or allow it to interfere with the carbon cuts that have to begin now. Ewa’s second grave error is to imagine that society could be turned into a giant climate camp. Anarchism is a great means of organising a self-elected community of like-minded people. It is a disastrous means of organising a planet. Most anarchists envisage their system as the means by which the oppressed can free themselves from persecution. **But i**f everyone is to be free from the coercive power of the state, this must apply to the oppressors as well as the oppressed. The **richest and most powerful communities** on earth - be they geographical communities or communities of interest - will be as **unrestrained** by external forces as the poorest and weakest. As a friend of mine put it, “when the anarchist utopia arrives, the first thing that will happen is that every Daily Mail reader in the country will pick up a gun and go and kill the nearest hippy.” This is why, though both sides furiously deny it, the outcome of both market fundamentalism and anarchism, if applied universally, is identical. The anarchists associate with the oppressed, the market fundamentalists with the oppressors. But by eliminating the state, both remove such restraints as prevent the strong from crushing the weak. Ours is not a choice between government and no government. It is a choice between government and the mafia. Over the past year I have been working with groups of climate protesters who have changed my view of what could be achieved. Most of them are under 30, and they bring to this issue a clear-headedness and pragmatism that I have never encountered in direct action movements before. They are prepared to take extraordinary risks to try to defend the biosphere from the corporations, governments and social trends which threaten to make it uninhabitable. They do so for one reason only: that they love the world and fear for its future. It would be a tragedy if, through the efforts of people like Ewa, they were to be diverted from this urgent task into the identity politics that have **wrecked so many movements**.

SQ solves waste and black leaders are on board

Politics365 12 [http://politic365.com/2012/01/27/nuclear-report-impact-on-minority-communities/]

In his State of the Union address, President Obama laid out his vision for a “future where we’re in control of our own energy, and our security and prosperity aren’t so tied to unstable parts of the world.” On the heels of this declaration, the [Blue Ribbon Commission on America’s Nuclear Future](http://www.brc.gov) released its final report “detailing comprehensive recommendations for creating a safe, long-term solution for managing and disposing of the nation’s spent nuclear fuel and high-level radioactive waste.” Nuclear waste management appears to be a vital part of the Obama Administration’s effort to harness America’s domestic energy potential.

Black elected officials from across the country agree that nuclear energy is a key component of our country’s energy equation. In late 2009, the National Black Caucus of State Legislators (“NBCSL”), an organization of more than 600 state legislators, [adopted a resolution](http://nbcsl.org/public-policy/resolutions/item/93-energy-transportation--environment-resolution-ete-10-06.html) encouraging the Administration to be more assertive in its pursuit of a nuclear energy agenda.  What’s more, the organization expressly supported the “creation of a National Blue Ribbon Commission to provide long term policy guidance for used fuel recycling and eventual disposal.”

According to Georgia State Rep. Calvin Smyre, Chair of NBCSL’s Foundation, “nuclear energy can benefit our communities in a variety of ways.  It can improve health outcomes by being a clean energy source, reduce consumers’ energy bills, and serve as the kind of job creator we so desperately need right now.”

#### 4) Cyber Link – This is ONLY descriptive of the squo

Owens et al. 09 (WILLIAM A. OWENS, AEA Holdings, Inc., Co-chair KENNETH W. DAM, University of Chicago, Co-chair THOMAS A. BERSON, Anagram Laboratories GERHARD CASPER, Stanford University DAVID D. CLARK, Massachusetts Institute of Technology RICHARD L. GARWIN, IBM Fellow Emeritus JACK L. GOLDSMITH III, Harvard Law School CARL G. O’BERRY, The Boeing Company JEROME H. SALTZER, Massachusetts Institute of Technology (retired) MARK SEIDEN, MSB Associates SARAH SEWALL, Harvard University WALTER B. SLOCOMBE, Caplin & Drysdale WILLIAM O. STUDEMAN, U.S. Navy (retired) MICHAEL A. VATIS, Steptoe & Johnson LLP, “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities”, pdf)

A historical analogy might be drawn to the study of nuclear issues. In many ways, today’s state of affairs regarding public discourse on cyberattack is analogous to the nuclear debate of 50 years ago. At that time, nuclear policy issues were veiled in secrecy, and there was little public debate about them. Herman Kahn’s books (On Thermonuclear War, Thinking the Unthinkable) were the first that addressed in the open literature what it might mean to fight a nuclear war. These seminal pieces did much to raise the public profile of these issues and stimulated an enormous amount of subsequent work outside government that has had a real impact on nuclear policy. From our perspective as the co-chairs of this study, the topic of cyberattack is so important across a multitude of national interests—not just defense or even just national security—that it deserves robust and open discussion and debate, both among thoughtful professionals in the policy, military, intelligence, law enforcement, and legal fields and among security practitioners in the private sector. But for such discussion and debate to be productive, they must be based on some common foundation of information about the topic at hand. Thus,the report’s role in providing education and background is in our view its most important function.

### Perm

#### No alt

Flood ’04 (Andrew, Anarchist organizer and writer, “Civilization, Primitivism, Anarchism,” http://www.anarkismo.net/newswire.php?story\_id=1451)

No. The primitivists seem to forget that we live in a class society. The population of the earth is divided into a few people with vast resources and power and the rest of us. It is not a case of equal access to resources, rather of quite incredible unequal access. Those who fell victim to the mass die off would not include Rubert Murdoch, Bill Gates or George Bush because these people have the money and power to monopolise remaining supplies for themselves.¶ Instead the first to die in huge number would be the population of the poorer mega cities on the planet. Cairo and Alexandria in Egypt have a population of around 20 million between them. Egypt is dependent both on food imports and on the very intensive agriculture of the Nile valley and the oasis. Except for the tiny wealthy elite those 20 million urban dwellers would have nowhere to go and there is no more land to be worked. Current high yields are in part dependent on high inputs of cheap energy.¶ The mass deaths of millions of people is not something that destroys capitalism.

 Indeed at periods of history it has been seen as quite natural and even desirable for the modernization of capital. The potato famine of the 1840's that reduced the population of Ireland by 30% was seen as desirable by many advocates of free trade.(16) So was the 1943/4 famine in British ruled Bengal in which four million died(17). For the capitalist class such mass deaths, particularly in colonies afford opportunities to restructure the economy in ways that would otherwise be resisted.