# Weber HT—Texas Round 1

## 1AC

### Advantage 1-Credibility

#### Cyber militarization by the US is observed and modelled globally due to Snowden—perception of overbearing cyber power causes cyber retaliation, destroys legitimacy, and frustrates allies

Wallace, 13

(Ian Wallace, visiting fellow in the Center on 21st Century Security and Intelligence at Brookings. Wallace previously served as a senior official at the British Ministry of Defence, where he helped develop the UK government’s cyber strategy as well as Britain’s cyber relationship with the United States. “Militarizing the Internet?” <http://nationalinterest.org/commentary/militarizing-the-internet-8734?page=show>) Henge

Following a recent speech, Chairman of the Joint Chiefs of Staff General Martin Dempsey dismissed concerns about the U.S. militarization of cyberspace. “We have a Navy, but we are not being accused of militarizing the ocean,” he said. As the world reflects on and responds to the actions of former National Security Agency contractor Edward Snowden, and as the investigation of possible leaks by former Joint Chiefs vice chairman General James Cartwright unfolds, it is difficult to avoid wondering if General Dempsey’s answer is the best the administration can muster. An increasing number of adversaries and even allies are coming to believe that the United States is militarizing cyberspace—and that impression of hubris and irresponsibility is beginning to have a real-world impact. So what needs to be done? New thinking is required, in at least three ways: First, the administration needs to acknowledge that this is a problem. Second, a more holistic approach is required when making national-security decisions that affect the internet. Third, the government needs to learn to respond to these types of leaks in a way that does not make the situation worse. Acknowledging the Problem The Snowden leaks have brought Stuxnet, the U.S.-Israeli program allegedly used to attack Iranian computer systems, back into public debate—and reminded us that the real damage of the Snowden revelations will be international. President Obama looks set to weather the domestic storm, and after a round of outrage—some real, some feigned—the diplomatic fallout from the various spying allegations will eventually subside. Susan Rice, the new national-security adviser, might have been a little optimistic when she said, “I don’t think the diplomatic consequences, at least in the foreseeable future, are that significant.” She will have some difficult conversations with European leaders, annoyed at the reigniting of previous domestic controversies about the privacy implications of U.S. counterterrorism policy. But other priorities, including the economy, will ensure that U.S.-European relations remain firm. So it is difficult to imagine she will lose much sleep over Chinese complaints on the subject of cyber espionage. Yet the perception that the United States has become a danger to the global internet is a cause for concern. In their understandable anger at the considerable damage Snowden has done (in the near term at the very least) to the operations of NSA and their allies, U.S. security officials should not lose sight of this fact. Snowden’s claims build on the Stuxnet revelations. In doing so, they reinforce an impression of overbearing U.S. cyberpower (military and commercial) being used irresponsibly. That is strikingly at odds with the U.S. self-image as a standard bearer of internet freedom and “borderless” exchange, but it is a view that resonates around the world. At the most basic level, that sense of double standards legitimizes bad behavior directed back at the United States. Many in the U.S. private sector believe that the distributed denial of service attacks that they are suffering from Iranian-backed groups are a response to Stuxnet. So you can imagine how little sympathy such attacks elicit in parts of the world where there are already high levels of anti-U.S. sentiment. More practically, Stuxnet demonstrated the ways in which critical infrastructure can be attacked and removed any taboo that existed that might have prevented it. Not surprisingly, many researchers fear that it is only a matter of time before this country suffers a taste of its own medicine.

#### Cyber retaliation against the US escalates—kinetic response is part of National Military Strategy

Lawson 9 (Sean - assistant professor in the Department of Communication at the University of Utah, Cross-Domain Response to Cyber Attacks and the Threat of Conflict, 5/13, http://www.seanlawson.net/?p=477)

At a time when it seems impossible to avoid the seemingly growing hysteria over the threat of cyber war,[1] network security expert Marcus Ranum delivered a refreshing talk recently, “The Problem with Cyber War,” that took a critical look at a number of the assumptions underlying contemporary cybersecurity discourse in the United States. He addressed one issue in partiuclar that I would like to riff on here, the issue of conflict escalation–i.e. the possibility that offensive use of cyber attacks could escalate to the use of physical force. As I will show, his concerns are entirely legitimate as current U.S. military cyber doctrine assumes the possibility of what I call “cross-domain responses” to cyberattacks. Backing Your Adversary (Mentally) into a Corner Based on the premise that completely blinding a potential adversary is a good indicator to that adversary that an attack is iminent, Ranum has argued that “The best thing that you could possibly do if you want to start World War III is launch a cyber attack. [...] When people talk about cyber war like it’s a practical thing, what they’re really doing is messing with the OK button for starting World War III. We need to get them to sit the f-k down and shut the f-k up.” [2] He is making a point similar to one that I have made in the past: Taking away an adversary’s ability to make rational decisions could backfire. [3] For example, Gregory Witol cautions that “attacking the decision maker’s ability to perform rational calculations may cause more problems than it hopes to resolveÃ¢â‚Â¦ Removing the capacity for rational action may result in completely unforeseen consequences, including longer and bloodier battles than may otherwise have been.” [4] Ã¯Â»Â¿Cross-Domain Response So, from a theoretical standpoint, I think his concerns are well founded. But the current state of U.S. policy may be cause for even greater concern. It’s not just worrisome that a hypothetical blinding attack via cyberspace could send a signal of imminent attack and therefore trigger an irrational response from the adversary. What is also cause for concern is that current U.S. policy indicates that “kinetic attacks” (i.e. physical use of force) are seen as potentially legitimate responses to cyber attacks. Most worrisome is that current U.S. policy implies that a nuclear response is possible, something that policy makers have not denied in recent press reports. The reason, in part, is that the U.S. defense community has increasingly come to see cyberspace as a “domain of warfare” equivalent to air, land, sea, and space. The definition of cyberspace as its own domain of warfare helps in its own right to blur the online/offline, physical-space/cyberspace boundary. But thinking logically about the potential consequences of this framing leads to some disconcerting conclusions. If cyberspace is a domain of warfare, then it becomes possible to define “cyber attacks” (whatever those may be said to entail) as acts of war. But what happens if the U.S. is attacked in any of the other domains? It retaliates. But it usually does not respond only within the domain in which it was attacked. Rather, responses are typically “cross-domain responses”–i.e. a massive bombing on U.S. soil or vital U.S. interests abroad (e.g. think 9/11 or Pearl Harbor) might lead to air strikes against the attacker. Even more likely given a U.S. military “way of warfare” that emphasizes multidimensional, “joint” operations is a massive conventional (i.e. non-nuclear) response against the attacker in all domains (air, land, sea, space), simultaneously. The possibility of “kinetic action” in response to cyber attack, or as part of offensive U.S. cyber operations, is part of the current (2006) National Military Strategy for Cyberspace Operations [5]: (U) Kinetic Actions. DOD will conduct kinetic missions to preserve freedom of action and strategic advantage in cyberspace. Kinetic actions can be either offensive or defensive and used in conjunction with other mission areas to achieve optimal military effects. Of course, the possibility that a cyber attack on the U.S. could lead to a U.S. nuclear reply constitutes possibly the ultimate in “cross-domain response.” And while this may seem far fetched, it has not been ruled out by U.S. defense policy makers and is, in fact, implied in current U.S. defense policy documents. From the National Military Strategy of the United States (2004): “The term WMD/E relates to a broad range of adversary capabilities that pose potentially devastating impacts. WMD/E includes chemical, biological, radiological, nuclear, and enhanced high explosive weapons as well as other, more asymmetrical ‘weapons’. They may rely more on disruptive impact than destructive kinetic effects. For example, cyber attacks on US commercial information systems or attacks against transportation networks may have a greater economic or psychological effect than a relatively small release of a lethal agent.” [6] The authors of a 2009 National Academies of Science report on cyberwarfare respond to this by saying, “Coupled with the declaratory policy on nuclear weapons described earlier, this statement implies that the United States will regard certain kinds of cyberattacks against the United States as being in the same category as nuclear, biological, and chemical weapons, and thus that a nuclear response to certain kinds of cyberattacks (namely, cyberattacks with devastating impacts) may be possible. It also sets a relevant scale–a cyberattack that has an impact larger than that associated with a relatively small release of a lethal agent is regarded with the same or greater seriousness.” [7]

#### And they cause meltdowns—the threshold is low—more sophistication will make each attack worse than the last

Kesler, 11

(Brent Kesler, MA in international policy with a focus on terrorism from the Monterey Institute of International Studies; web developer and managing editor of Strategic Insights at the Naval Postgraduate School. “The Vulnerability of Nuclear Facilities to Cyber Attack” <http://edocs.nps.edu/npspubs/institutional/newsletters/strategic%20insight/2011/SI-v10-I1_Kesler.pdf>)

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 cyber security 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 make cyber attacks more precise, supplementing their methods with intelligence from other sources.

#### Meltdowns cause extinction—it outweighs any other impact

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

For years, Helen Caldicott warned it's coming. In her 1978 book, "Nuclear Madness," she said: "As a physician, I contend that nuclear technology threatens life on our planet with extinction. If present trends continue, the air we breathe, the food we eat, and the water we drink will soon be contaminated with enough radioactive pollutants to pose a potential health hazard far greater than any plague humanity has ever experienced." More below on the inevitable dangers from commercial nuclear power proliferation, besides added military ones. On March 11, New York Times writer Martin Fackler headlined, "Powerful Quake and Tsunami Devastate Northern Japan," saying: "The 8.9-magnitude earthquake (Japan's strongest ever) set off a devastating tsunami that sent walls of water (six meters high) washing over coastal cities in the north." According to Japan's Meteorological Survey, it was 9.0. The Sendai port city and other areas experienced heavy damage. "Thousands of homes were destroyed, many roads were impassable, trains and buses (stopped) running, and power and cellphones remained down. On Saturday morning, the JR rail company" reported three trains missing. Many passengers are unaccounted for. Striking at 2:46PM Tokyo time, it caused vast destruction, shook city skyscrapers, buckled highways, ignited fires, terrified millions, annihilated areas near Sendai, possibly killed thousands, and caused a nuclear meltdown, its potential catastrophic effects far exceeding quake and tsunami devastation, almost minor by comparison under a worst case scenario. 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. Nuclear Power: A Technology from Hell Nuclear expert Helen Caldicott agrees, telling this writer by phone that a potential regional catastrophe is unfolding. Over 30 years ago, she warned of its inevitability. Her 2006 book titled, "Nuclear Power is Not the Answer" explained that contrary to government and industry propaganda, even during normal operations, nuclear power generation causes significant discharges of greenhouse gas emissions, as well as hundreds of thousands of curies of deadly radioactive gases and other radioactive elements into the environment every year. Moreover, nuclear plants are atom bomb factories. A 1000 megawatt reactor produces 500 pounds of plutonium annually. Only 10 are needed for a bomb able to devastate a large city, besides causing permanent radiation contamination. Nuclear Power not Cleaner and Greener Just the opposite, in fact. Although a nuclear power plant releases no carbon dioxide (CO2), the primary greenhouse gas, a vast infrastructure is required. Called the nuclear fuel cycle, it uses large amounts of fossil fuels. Each cycle stage exacerbates the problem, starting with the enormous cost of mining and milling uranium, needing fossil fuel to do it. How then to dispose of mill tailings, produced in the extraction process. It requires great amounts of greenhouse emitting fuels to remediate. Moreover, other nuclear cycle steps also use fossil fuels, including converting uranium to hexafluoride gas prior to enrichment, the enrichment process itself, and conversion of enriched uranium hexafluoride gas to fuel pellets. In addition, nuclear power plant construction, dismantling and cleanup at the end of their useful life require large amounts of energy. There's more, including contaminated cooling water, nuclear waste, its handling, transportation and disposal/storage, problems so far unresolved. Moreover, nuclear power costs and risks are so enormous that the industry couldn't exist without billions of government subsidized funding annually. The Unaddressed Human Toll from Normal Operations Affected are uranium miners, industry workers, and potentially everyone living close to nuclear reactors that routinely emit harmful radioactive releases daily, harming human health over time, causing illness and early death. The link between radiation exposure and disease is irrefutable, depending only on the amount of cumulative exposure over time, Caldicott saying: "If a regulatory gene is biochemically altered by radiation exposure, the cell will begin to incubate cancer, during a 'latent period of carcinogenesis,' lasting from two to sixty years." In fact, a single gene mutation can prove fatal. No amount of radiation exposure is safe. Moreover, when combined with about 80,000 commonly used toxic chemicals and contaminated GMO foods and ingredients, it causes 80% of known cancers, putting everyone at risk everywhere. Further, the combined effects of allowable radiation exposure, uranium mining, milling operations, enrichment, and fuel fabrication can be devastating to those exposed. Besides the insoluble waste storage/disposal problem, nuclear accidents happen and catastrophic ones are inevitable. Inevitable Meltdowns Caldicott and other experts agree they're certain in one or more of the hundreds of reactors operating globally, many years after their scheduled shutdown dates unsafely. Combined with human error, imprudently minimizing operating costs, internal sabotage, or the effects of a high-magnitude quake and/or tsunami, an eventual catastrophe is certain. Aging plants alone, like Japan's Fukushima facility, pose unacceptable risks based on their record of near-misses and meltdowns, resulting from human error, old equipment, shoddy maintenance, and poor regulatory oversight. However, under optimum operating conditions, all nuclear plants are unsafe. Like any machine or facility, they're vulnerable to breakdowns, that if serious enough can cause enormous, possibly catastrophic, harm.

#### The cyber domain is a unique space where the US needs soft power—diffusion of power, rapid technological change, and it’s human made—deterrence is possible, but it’s different from other areas—cyber policy spills over

Nye, 10

(Joseph Nye, American political scientist and former Dean of the John F. Kennedy School of Government at Harvard University. He currently holds the position of University Distinguished Service Professor at Harvard University where he has been a member of the faculty since 1964. He is also the co-founder, along with Robert Keohane, of the international relations theory neoliberalism, developed in their 1977 book Power and Interdependence. Together with Keohane, he developed the concepts of asymmetrical and complex interdependence. They also explored transnational relations and world politics in an edited volume in the 1970s. More recently, he pioneered the theory of soft power. He is a fellows of the American Academy of Arts & Sciences and The British Academy. Nye is also a member of the American Academy of Diplomacy. The 2011 TRIP survey of over 1700 international relations scholars ranks Joe Nye as the sixth most influential scholar in the field of international relations in the past twenty years. In 2011, he was named by Foreign Policy magazine to its list of top global thinkers. “Cyber Power” <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>) Henge \*Tables omitted

The evolution modern social science definitions of behavioral power is sometimes summarized as “the three faces of power.”8 The first aspect or “face” of power was defined by Robert Dahl in studies of New Haven in the 1950s.9 His focus on getting others to do what they would not otherwise do is widely used today even though it covers only part of power behavior. In the 1960s, the political scientists Peter Bachrach and Morton Baratz pointed out that Dahl’s definition missed what they called the “second face of power,” the dimension of agenda setting, or framing issues in such a way that the issue of coercion never arose.10 In the 1970s, the sociologist Steven Lukes pointed out that ideas and beliefs also help shape others’ preferences, and one can also exercise power by determining others’ wants.11 In 1990, I distinguished hard and soft power along a spectrum from command to co-optive behavior. Hard power behavior rests on coercion and payment. Soft power behavior rests on framing agendas, attraction or persuasion.12 Even large countries with impressive hard and soft power resources, such as the United States, find themselves sharing the stage with new actors and having more trouble controlling their borders in the domain of cyberspace. Cyberspace will not replace geographical space and will not abolish state sovereignty, but the diffusion of power in cyberspace will coexist and greatly complicate what it means to exercise power along each of these dimensions. Cyber Power Power based on information resources is not new; cyber power is. There are dozens of definitions of cyberspace but generally “cyber” is a prefix standing for electronic and computer related activities. By one definition: “cyberspace is an operational domain framed by use of electronics to …exploit information via interconnected systems and their associated infra structure.”13 Power depends on context, and cyber power depends on the resources that characterize the domain of cyberspace. We sometimes forget how new cyberspace is. In 1969, the Defense Department started a modest connection of a few computers called ARPANET, and in 1972, the codes for exchanging data (TCP/IP) were created to constitute a rudimentary internet capable of exchanging packets of digital information. The domain name system of internet addresses starts in 1983, and the first computer viruses were created about that time. The World Wide Web begins in 1989; Google the most popular search engine was founded in 1998; and the open source encyclopedia, Wikipedia, begins in 2001. In the late 1990s, businesses begin to use the new technology to shift production and procurement in complex global supply chains. Only recently has there been the bandwidth and server farms to support “cloud computing” in which companies and individuals can store their data and software on the Web. ICANN (the internet corporation for assigned names and numbers) was created in 1998, and the US government only began to develop serious national plans for cyber security in the past decade. In 1992, there were only a million users on the internet; within fifteen years that had grown to a billion.14 In its early days, libertarians proclaimed that “information wants to be free” and portrayed the internet as the end of government controls and the “death of distance.” In practice, governments and geographical jurisdictions play a major role, but the domain is also marked by power diffusion.15 One can conceptualize cyberspace in terms of many layers of activities, but a simple first approximation portrays it as a unique hybrid regime of physical and virtual properties.16 The physical infrastructure layer follows the economic laws of rival resources and increasing marginal costs, and the political laws of sovereign jurisdiction and control. The virtual or informational layer has economic network characteristics of increasing returns to scale, and political practices that make jurisdictional control difficult.17 Attacks from the informational realm where costs are low can be launched against the physical domain where resources are scarce and expensive. But conversely, control of the physical layer can have both territorial and extraterritorial effects on the informational layer. Cyber power behavior rests upon a set of resources that relate to the creation, control and communication of electronic and computer based information -- infrastructure, networks, software, human skills. This includes the Internet of networked computers, but also intranets, cellular technologies and space based communications. Defined behaviorally, cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. In one widely used definition, cyber power is “the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power.”18 Cyber power can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace. By analogy, sea power refers to the use of resources in the oceans domain to win naval battles on the ocean, to control shipping chokepoints like straits, and to demonstrate an offshore presence, but it also includes the ability to use such the oceans to influence battles, commerce, and opinions on land. In 1890, Alfred Thayer Mahan popularized the importance of sea power in the context of new technologies of steam propulsion, armor and long range guns. President Theodore Roosevelt responded by greatly expanding America’s blue water navy and sending it around the world in 1907. After the introduction of aircraft in World War I, military men began to theorize about the domain of air power and its ability to strike directly at an enemy’s urban center of gravity without armies having to first cross borders. Franklin Roosevelt’s investments in air power were vital in World War II. And after the development of inter continental missiles and surveillance and communications satellites in the 1960s, writers began to theorize about the particular domain of space power. John F. Kennedy launched a program to ensure an American lead in space and to put a man on the moon. In 2009, President Barack Obama called for a major new initiative in cyber power, and other governments have followed suit.19 As technological change reshapes power domains, political leaders soon follow. The cyber domain is unique in that it is ~~manmade~~ [human made], recent and subject to even more rapid technological changes than other domains. As one observer put it, “the geography of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the click of a switch.”20 It is cheaper and quicker to move electrons across the globe than to move large ships long distances through the friction of salt water. The costs of developing multiple carrier task forces and submarine fleets create enormous barriers to entry and make it still possible to speak of American naval dominance. While piracy remains a local option for non-state actors in areas like Somalia or the Malacca Straits, sea control remains out of the reach of non-state actors. Similarly, while there are many private and governmental actors in the air domain, a country can still seek to achieve air superiority through costly investments in 5th generation fighters and satellite support systems. In contrast, as mentioned above, the barriers to entry in the cyber domain are so low that non-state actors and small states can play significant roles at low levels of cost. In contrast to sea, air and space, “cyber shares three characteristics with land warfare – though in even greater dimensions: the number of players, ease of entry, and opportunity for concealment…On land, dominance is not a readily achievable criterion.”21 While a few states like the United States, Russia, Britain, France, and China are reputed to have greater capacity than others, it makes little sense to speak of dominance in cyber space as in sea power or air power. If anything, dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by non state actors. Extreme conflict in the cyber domain or “cyber war” is also different. In the physical world, governments have a near monopoly on large scale use of force, the defender has an intimate knowledge of the terrain, and attacks end because of attrition or exhaustion. Both resources and mobility are costly. In the virtual world, actors are diverse, sometimes anonymous, physical distance is immaterial, and a “single virtual offense is almost cost free.”22 Because the internet was designed for ease of use rather than security, the offense currently has the advantage over the defense. This might not remain the case in the long term as technology evolves, including efforts at “re-engineering” some systems for greater security, but it remains the case at this stage. The larger party has limited ability to disarm or destroy the enemy, occupy territory, or effectively use counter- force strategies. As we shall see below, deterrence is possible, but differs because of problems of attribution of the source of an attack. Ambiguity is ubiquitous and reinforces the normal fog of war. Redundancy, resilience and quick reconstitution become crucial components of defense. As one expert summarizes the situation, “attempts to transfer policy constructs from other forms of warfare will not only fail but also hinder policy and planning.”23 Cyber power affects many other domains from war to commerce. We can distinguish “intra cyberspace power” and “extra cyberspace power” just as with sea power, we can distinguish naval power on the oceans from naval power projection onto land . For example, carrier based aircraft can participate in land battles; trade and commerce may grow because of the efficiency of a new generation of container ships; and the soft power of a country may be increased by the visit of naval hospital ships in humanitarian missions. *Table 1 Omitted* As Table 1 illustrates, inside the cyber domain, information instruments can be used to produce soft power in cyber space through agenda framing, attraction or persuasion. For example, attracting the open source software community of programmers to adhere to a new standard is an example of soft power targeted within cyberspace. Cyber resources can also produce hard power inside cyber space. For example, states or nonstate actors can organize a distributed denial of service attack by using “botnets” of hundreds of thousands (or more) corrupted computers that swamp a company or country’s internet system and prevents it functioning. Organizing a botnet by infiltrating a virus into unguarded computers is relatively inexpensive, and botnets can be illegally rented on the internet for a few hundred dollars. Sometimes individual criminals do this for purposes of extortion. Other cases may involve “hacktivists” or ideologically motivated intruders. For example, Taiwanese and Chinese hackers regular deface each others’ web sites. In 2007, Estonia suffered a distributed denial of service attack that was widely attributed to “patriotic hackers” in Russia who were offended by Estonia’s movement of a World War II monument to Soviet soldiers. In 2008, shortly before Russian troops invaded, Georgia suffered a denial of service attack that shut down its internet access. ( In both instances, however, the Russian government seems to have abetted the hackers while maintaining “plausible deniability.”) Other forms of hard power within cyber space include insertion of malicious code to disrupt systems or to steal intellectual property. Criminal groups do it for profit, and governments may do it as a way of increasing their economic resources. China, for example, has been accused of such activities by a number of other countries. Proof of the origin or motive of such attacks is often very difficult as attackers can route their intrusions through servers in other countries to make attribution difficult. For example, many of the attacks on Estonian and Georgian targets were routed through American servers.24 Cyber information can also travel through cyberspace to create soft power by attracting citizens in another country. A public diplomacy campaign over the internet is an example. But cyber information can also become a hard power resource that can do damage to physical targets in another country. For example, many modern industries and utilities have processes that are controlled by computers linked in SCADA (supervisory control and data acquisition) systems. Malicious software inserted into these systems could be instructed to shut down a process which would have very real physical effects. For example, if a hacker or a government shut down the provision of electricity in a Northern city like Chicago or Moscow in the middle of February, the devastation could be more costly than if bombs had been dropped. In some facilities like hospitals, back-up generators can provide resilience in the case of a disruptive attack, but widespread regional blackouts would be more difficult to cope with. As the table above indicates, physical instruments can provide power resources that can be brought to bear on the cyber world. For instance, the physical routers and servers and the fiber optic cables that carry the electrons of the internet have geographical locations within governmental jurisdictions, and companies running and using the internet are subject to those governments’ laws. Governments can bring physical coercion to bear against companies and individuals; what has been called “the hallmark of traditional legal systems.” Legal prosecution made Yahoo control what it sent to France and Google removed hate speech from searches in Germany. Even though the messages were protected free speech in the companies’ “home country”, the United States, the alternative to compliance was jail time, fines, and loss of access to those important markets. Governments control behavior on the internet through their traditional physical threats to such intermediaries as internet service providers, browsers, search engines and financial intermediaries. 25 As for investment in physical resources that create soft power, governments can set up special servers and software designed to help human rights activists propagate their messages despite the efforts of their own governments to create information firewalls to block such messages. For of 2009, the American State Department invested in software and hardware that would enable the protesters to disseminate their messages. Finally, as Table 1 illustrates, physical instruments can provide both hard and soft power resources that can be used against the internet. The cyber information layer rests upon a physical infrastructure that is vulnerable to direct military attack or sabotage both by governments and non state actors such as terrorists or criminals. Servers can be blown up and cables can be cut. And in the domain of soft power, non-state actors and NGOs can organize physical demonstrations to name and shame companies (and governments) that they regard as abusing the Internet. For example, in 2006 protesters in Washington marched and demonstrated against Yahoo and other internet companies that had provided the names of Chinese activists that led to their arrest by the Chinese government. Another way of looking at power in the cyber domain is to consider the three faces or aspects of relational power. *Table 2 Omitted* One can find evidence of hard and soft power behavior in all three aspects as applied to cyberspace. The first face of power is the ability of an actor to make others do something contrary to their initial preferences or strategies. Examples related to hard power could included the denial of services attacks described above, as well as arresting or otherwise preventing dissident bloggers from sending their messages. For example, in December 2009, China sentenced Liu Xiaobo, a veteran human rights activist and blogger to 11 years in prison for “inciting subversion of state power,” and introduced new restrictions on registration and operation of websites by individuals. As one Chinese web hosting service provider commented, “for nine years I have run a successful and legal business, and now I have suddenly been told that what I do makes me a criminal.”26 In terms of soft power, an individual or organization might attempt to persuade others to change their behavior. The Chinese government sometimes used the internet to mobilize Chinese students to demonstrate against Japan when its officials took positions that offended Chinese views of the 1930s relationship. Al Qaeda videos on the internet designed to recruit people to their cause are another case of soft power being used to change people from their original preferences or strategies. The second face of power is agenda setting or framing in which an actor precludes the choices of another by exclusion of their strategies. If this is against their will, it is an aspect of hard power; if it is accepted as legitimate it is an instance of soft power. For example, on the February 2010 anniversary of the Iranian Revolution, the government slowed the internet to prevent protesters sending films of protests to be seen on YouTube as they had successfully done six months earlier. As one Iranian exile commented, “It was the day the Greens grew up and learned that fighting a government as determined as the Islamic Republic of Iran will require much more than Facebook fan pages, Twitter clouds, and emotional YouTube clips.”27 According to the Open Net Initiative, at least 40 countries use highly restrictive filters and firewalls to prevent the discussion of suspect materials. Eighteen countries engage in political censorship, which is described as “pervasive” in China, Vietnam and Iran, and “substantial” in Libya, Ethiopia, and Saudi Arabia. More than 30 states filter for social reasons, blocking content related to topics such as sex, gambling and drugs. Even the United States and many European states do this “selectively.”28 Sometimes this is accepted and sometimes not. If the filtering is secretive, it is hard for citizens to know what they do not know. First generation filtering technologies are installed at key Internet chokepoints, and work by preventing requests for a predetermined list of websites and addresses. They are often known to users, but they have been supplemented by more sophisticated technologies that are more stealthy, dynamic and targeted on opponents “just in time.”29 In some instances, what looks like hard power to one group, looks attractive to another. After riots in Xingjian in 2009, China closed thousands of websites and censored text messages which made communication more difficult for residents of that region, but it also cultivated homegrown alternatives to foreign based Web sites like YouTube, Facebook and Twitter which was attractive in the eyes of nationalistic “patriotic hackers.”30 Among American corporations, when the music industry sued more than 12,000 Americans for intellectual property theft in downloading music illegally, the threat was felt as hard power by those sued, and by many who were not sued as well. But when a transnational corporation like Apple decides not to allow certain applications to be downloaded to its I phones, many consumers are not even aware of the truncations of their potential agendas, and few understand the algorithms that guide their searches for information.31 The third face of power involves one actor shaping another’s initial preferences so that some strategies are not even considered. When companies chose to design one code rather than another into their software products, few consumers notice.32 Governments may carry out campaigns to delegitimize certain ideas such as the Falun Gong religion in China and restrict dissemination of its ideas on the internet and thus make it difficult for Chinese citizens to know about it. Saudi Arabia makes certain infidel web sites are unavailable to its citizens. The United States government has taken measures against credit card companies so that internet gambling is unavailable to its citizens. France and Germany prevent discussion of Nazi ideology on the internet. Occasionally, as with child pornography, there is broad cross cultural consensus on restricting certain ideas and pictures from being available. Actors and their Relative Power Resources The diffusion of power in the cyber domain is represented by the vast number of actors, and relative reduction of power differentials among them. Anyone from a teen age hacker to a major modern government can do damage in cyber space, and as the famous New Yorker cartoon once put it, “on the internet, no one knows you are a dog.” The infamous “Love Bug” virus unleashed by a hacker in the Philippines is estimated to have caused $15 billion in damage.33 Computer networks essential to the American military are attacked “hundreds of thousands of times every day”.34 Cybercriminal groups were said to have stolen over $1 trillion in data and intellectual property in 2008.35 One cyber espionage network — GhostNet — was found to be infecting 1,295 computers in 103 countries, of which 30 percent were high value governmental targets.36 Terrorist groups use the web to recruit new members and plan campaigns. Political and environmental activists disrupt web sites of companies and governments. What is distinctive about power in the cyber domain is not that governments are out of the picture as the early cyber libertarians predicted, but the different power resources that different actors possess, and the narrowing of the gap between state and non state actors in many instances. But relative reduction of power differentials is not the same as equalization. Large governments still have more resources. On the internet, all dogs are not equal. As a rough approximation, we can divide actors in cyberspace into three categories: governments, organizations with highly structured networks, and individuals and lightly structured networks. (Of course, there are many subcategories) Because the physical infrastructure of the internet remains tied to geography and governments are sovereign over geographical spaces, location still matters as a resource in the cyber domain. Governments can take steps to subsidize infrastructure, computer education, and protection of intellectual property that will encourage ( or discourage) the development of capabilities within their borders. The provision of public goods, including a legal and regulatory environment, can stimulate commercial growth of cyber capabilities. South Korea, for example, has taken a lead on public development of broad band capabilities. A reputation that is seen as legitimate, benign and competent can enhance (or conversely undercut) a government’s soft power with other actors in the cyber domain. Geography also serves as a basis for governments to exercise legal coercion and control. For example, after the Xinjiang riots in 2009, the Chinese government was able to deprive 19 million residents in an area twice as big as Texas of text messaging, international phone calls, and internet access to all but a few government controlled Web sites. The damage to business and tourism was significant, but the Chinese government was more concerned about political stability.37 In 2010, *Table 3 Omitted* when SWIFT, a private company that coordinates and logs money transfers among banks, moved key computer servers from the US to Europe, it meant that it now needed permission of the EU to hand over data voluntarily to the US Treasury for anti-terrorist purposes. When the European Parliament balked at approval of a Europe wide agreement, SWIFT announced that “there is no legal basis for us to hand over data from our European centers to the Treasury.”38 If a market is large, a government can exert its power extraterritorially. Europe’s tight privacy standards have had a global effect. When companies like Yahoo or Dow Jones have faced legal claims based on internet activity in France or Australia, they decided to comply rather than walk away from those markets. Obviously, this is a power resource available to governments with jurisdiction over large markets, but not necessarily to all governments. Governments also have the capacity to carry out offensive cyber attacks.39 For example, America’s Tenth Fleet and Twenty-fourth Air Force have no ships or planes. Their battlefield is cyberspace.40 Unfortunately, news accounts of “millions of attacks” use the term “attack” loosely to refer to everything from computer port scanning to hacking (illegal computer trespassing) and defacing websites to full scale operations designed to wreak physical destruction. One should distinguish simple attacks which use inexpensive tool kits which anyone can download from the internet from advanced attacks which identify new vulnerabilities that have not yet been patched, involve new viruses, and involve “zero day attacks” (first time use.) These attacks require more skill than simple hacking. Experts also distinguish cyber exploitation for spying purposes from cyber attack which has destructive or disruptive purposes. Governments carry out activities of both types. Little is publicly confirmed about cyber espionage, but most reports describe intrusions into computer systems as ubiquitous, and not limited to governments. There are reports of attacks related to warfare in the cases of Iraq in 2003 or Georgia in 2008, and sabotage of electronic equipment in covert actions.41 Israel is said to have used cyber means to defeat Syrian air defenses before bombing a secret nuclear reactor in September 2007.42 Most experts see cyber attack as an important adjunct rather than an overwhelming weapon (unlike nuclear) in inter-state wars. States intrude into each others’ cyber systems in “preparation of the battlefield” for what could be future conflicts. Both American and Chinese military theorists have discussed such steps , but little is publicly stated about offensive cyber doctrines. A National Research Council Report concluded in 2009 that “today’s policy and legal framework for guiding and regulating the U.S. use of cyberattack is ill-formed, undeveloped, and highly uncertain.”43 Presumably many large governments engage in such activity, though the success of such attacks would depend upon the target’s vulnerabilities, and thus premature exercise or disclosure would undercut their value. “Zero day” attacks without prior warning are likely to be the most effective, and even their effects may depend on measures the target has taken to develop resiliency, some of which may not be fully known to the attacker. Cyber attacks that deny service or disrupt systems are also carried out by non-state actors whether for ideological or criminal purposes, but such groups do not have the same capacities as large governments. In general, it is easy to mount low cost attacks such as denial of service against low value targets such as websites. Botnets of zombie computers are easy to rent, and websites are often vulnerable to such measures. But sophisticated attacks against high value targets such as defense communications systems require a higher cost of attack, which involves large intelligence agencies to intrude physically and/or crack highly encrypted codes. A teenage hacker and a large government can both do considerable damage over the internet, but that does not make them equally powerful in the cyber domain. Power diffusion is not the same as power equalization. Some government experts believe that concerted technological improvements in encryption and identity management could greatly reduce threats at the low end of the spectrum within five years.44 Some transnational corporations have huge budgets, skilled human resources, and control of proprietary code that gives them power resources larger than many governments. In 2009, Microsoft, Apple and Google had annual revenues of $58, 35, and 22 billion respectively, and together employed over 150,000 people.45 Amazon, Google, Microsoft, and others are competing in the development of cloud computing, and have server farms with more then 50,000 servers. Their transnational structure allows them to exploit markets and resources around the globe. IBM, for example, derives two thirds of its revenue from overseas, and only a quarter of its 400,000 work force is located in the United States.46 At the same time, to preserve their legal status as well as their brand equity, transnational corporations have strong incentives to stay compliant with local legal structures. No such legal niceties constrain the power of criminal organizations. Some are small “strike and exit” operations, which make their gains quickly before governments and regulators can catch up.47 Others have impressive transnational scale and presumably buy protection from weak governments. Before it was dismantled by law enforcement, the Darkmarket online network had over 2500 members across the world buying and selling stolen financial information, passwords, and credit cards.48 Up to a quarter of network-connected computers may be part of a botnet, and some botnets include millions of computers. While estimates vary, cyber crime may cost companies over a trillion dollars a year.49 Some criminal groups, such as the so called “Russian Business Network” may have inherited some capabilities of the Soviet state after its dissolution, and are alleged to retain informal connections with the government. According to a British official, “there were strong indications RBN had the local police, local judiciary and local government in St. Petersburg in its pocket. Our investigation hit significant hurdles.”50 Moreover, “the hacking skills of criminal groups may make them natural allies for nation-states looking for a way to augment their capabilities while denying involvement in cyber attacks.”51 The scale of some criminal operations is expensive and costly, but apparently profitable. In 2006, the US Government Accountability Office estimated that only five percent of cybercriminals were ever arrested or convicted.52 Terrorist groups make active use of cyber tools, as we saw earlier, though cyber terrorism narrowly defined as using virtual tools to wreak destruction (see the top row in Table 1) has thus far been rare. While there is nothing stopping terrorist groups from recruiting able computer specialists or purchasing malware from criminal groups on the internet, “cyber attacks appear much less useful than physical attacks: they do not fill potential victims with terror, they are not photogenic, and they are not perceived by most people as highly emotional events.”53 Of twenty-two plots disrupted since 9/11, all involved explosives or small arms, and “while the United States’ critical infrastructure from the electrical grid to the financial sector, is vulnerable to attack through cyberspace, al-Qaeda lacks the capability and motivation to exploit these vulnerabilities.”54 Others are not so sanguine. For example, Mike McConnell, former Director of National Intelligence believes that the vulnerabilities of financial and electrical systems present a huge target for any group that wishes to wreak destruction, and that such groups will develop the capabilities to become a greater threat than other nation states. In his words, “when terrorist groups have the sophistication, they’ll use it.”55 So far, terrorists seem to have decided that for their purposes, explosives provide a tool with more bang for the buck. But that does not mean that terrorist groups do not use the internet for promoting terrorism. As we saw earlier, it has become a crucial tool that allows them to operate as networks of decentralized franchises, create a brand image, recruit adherents, raise funds, provide training manuals and manage operations. It is far safer to send electrons than agents through customs and immigration controls. Thanks to cyber tools, Al Qaeda has been able to move from a hierarchical organization restricted to geographically organized cells to a horizontal global network to which local volunteers can self-recruit. As one expert on terrorism describes, the key place for radicalization is “neither Pakistan nor Yemen nor Afghanistan …but in a solitary experience of a virtual community: the ummah on the Web.”56 This is an example of how cyber tools begin to blur the lines between organizations with highly structured networks and individuals with lightly structured networks. As a number of examples above have shown, individuals can easily play in the cyber domain because of the low cost of investment for entry, virtual anonymity, and ease of exit. Sometimes they act with government approval and sometimes against them. For example, before the 2008 Russian attack on Georgia, “any civilian, Russian born or otherwise, aspiring to be a cyber warrior was able to visit pro- Russia websites to download the software and instructions necessary to launch denial of service attacks on Georgia.”57 During student protests in Iran in 2009, Twitter and social networking sites were crucial for organizing and reporting demonstrations. “The U.S. government asked Twitter executives not to take the site down for scheduled maintenance. They were worried that might interfere with how Twitter was being used to organize demonstrations.” Six months later, however, an unknown group called the Iranian Cyber Army successfully redirected Twitter traffic to a website with an anti-American message, and in February 2010, the Iranian government blocked most access to Twitter and other sites.58 It is worth noting that individual actors in the cyber domain benefit from asymmetrical vulnerability compared to governments and large organizations. They have very low investment and little to lose from exit and re-entry. Their major vulnerability is to legal and illegal coercion by governments and organizations if they are apprehended, but only a small per cent are actually caught. In contrast, corporations have important vulnerabilities because of large fixed investments in complex operating system, intellectual property, and reputation. Similarly, large governments depend on easily disrupted complex systems, political stability, and reputational soft power. While hit and run cyber strikes by individuals are unlikely to bring governments or corporations to their knees, they can impose serious costs of disruption to operations and to reputations with a miniscule investment. Governments are top dogs on the internet, but smaller dogs still bite, and dealing with those bites can lead to a complex politics.

#### The cyber realm has placed international war back on the table—only credible norms can maintain cyber peace—US actions are modelled and retaliatory—cyber legitimacy is key—offensive ops exacerbate tensions, leading to escalated global war

Kavanaugh and Stauffacher, 13

(Camino Kavanagh, pursuing a Ph.D. in the Department of War Studies at King’s College London. Her research is centered on transformation in strategic affairs, with a specific focus on how cyberspace has evolved into a domain of strategic competition between states and she engages in different initiatives and projects on this subject. Camino is also a Senior Fellow at NYU’s Centre on International Cooperation and currently serving as an advisor to the Kofi Annan Foundation on the evolution of organized crime and drug trafficking in West Africa. She has worked with United Nations peace operations in Guatemala and Burundi and other international organizations in Africa, Asia, and Latin America & the Caribbean. She has a MA in Contemporary War Studies and a MA in Human Rights Law. Daniel Stauffacher, a former Ambassador of Switzerland, has a Ph.D. in media and copyright law from the University of Zürich and a Master’s degree in International Economic Affairs from Columbia University. After working for a Swiss publishing company, he joined the UN in 1982 and worked in New York, Laos and China. Subsequently he joined the Swiss Federal Office for Foreign Economic Affairs (Bawi) in 1990, where he was a Director for Economic and Financial Co-operation with major Asian and Central and Eastern European countries. In 1995, he was posted to the Swiss Mission to the European Union in Brussels as Counsellor for Economic and Financial Affairs. From 1999 to 2005, he was Ambassador of Switzerland to the United Nations in Geneva and New York and the Swiss Federal Government’s Special Representative for the hosting and preparation of the United Nations World Summit for Social Development (Geneva, 2000) and of the UN World Summit on the Information Society (WSIS) that was held in Geneva in 2003 and in Tunis 2005. He was a member of UN SG Kofi Annan’s UN ICT Task Force and is a founding Trustee of Tim Berners Lee’s World Wide Web Foundation (www.webfoundation.org). Dr. Stauffacher is the Founder and Chairman of ICT4Peace Foundation (www.ICT4Peace.org), President of the Geneva Security Forum and a Board Member of the Gulf Research Foundation (GRC), Geneva. He is and serves as a Special Advisor to the UN Secretariat and the Swiss Federal Department for Foreign Affairs. “THE REACH OF SOFT POWER IN RESPONDING TO INTERNATIONAL CYBERSECURITY CHALLENGES” <http://ict4peace.org/wp-content/uploads/2013/09/The-Reach-of-Soft-Power-in-Responding-to-International-Cybersecurity-Challenges-v.-7-Sept.pdf>) Henge

For several decades, international relations and strategic studies scholars have sought to develop a better understanding of the transformation and diffusion of power and its impact on strategic and international affairs. In 2006, Lawrence Freedman noted that an important transformation in strategic affairs had taken place with the end of the Cold War and the demise of the Soviet Union. He challenged the claims of the theorists of a “revolution in military affairs” (RMA) that technology-driven changes in the battlefield underway since the 1990s would transform wars between powerful states into contests marked by information dominance, highly precise weapons and information technology, thus reducing war’s impact on civilian populations and infrastructure. In his writings on RMA, Freedman argued that the impact of the technological changes on the actual conduct of war “depended on the interaction of these developments with changes of quite a different type – in political affairs – which at that moment pointed away from “the decisive clash between [great] powers.” Freedman insisted that the RMA failed to respond to changing political conditions and adapt its military machinery to “the wars that might actually have to be fought” i.e. the “new wars” which were more asymmetrical, irregular and transnational in nature and more reflective of shifting power structures within states and across regions. The terrorist attacks on the United States, Spain and the United Kingdom were evidence of this reality, as were the unexpected drawn-out struggles in Iraq and Afghanistan. Several years later, as the effects of the September 2001 terrorist attacks on the United States dissipate and withdrawal from the Iraq and Afghanistan theatres nears completion, the discussion about a transformation in military and strategic affairs has revived. It has been driven by changes in technological factors in military doctrine and strategy; power relations between and within states; the structure of the military-industrial complex; social organization articulation of interests; and changes in the nature of the threats (real and perceived) faced by highly networked powers. At the crux of these more recent debates on transformation lies a new environment: cyberspace (or information space, depending on one’s strategic narrative).1 According to US policy makers, the national security threats posed by the malicious use of cyberspace are today ranked above threats posed by terrorism and failed or failing states.2 Many other states share this view and are organizing their security structures accordingly. As threats related to the different uses of cyberspace have intensified, the policy option of inter-state war was placed squarely back on the table by US decision-makers when cyberspace was defined as a strategic domain of conflict in 2009, and a dedicated military command established shortly thereafter. Indeed, statements by senior US policy makers on the threats from cyberspace have grown increasingly hawkish since the mid-2000s, with some suggesting the almost-inevitability of war between states within a domain that, in its essence, was the US’ own creation.3 Nonetheless, war between major powers over cyber attacks or war in cyberspace remains unlikely.4 At the same time, however, the gradual build up of cyber capabilities, underpinned in large part by the concept of information dominance for military purposes, has lead other powers to develop an offensive strategy in response, mainly played out in international fora. For example, as early as 1998 Russia tabled a resolution in the UN General Assembly’s First Committee on Disarmament on Developments in the Field of Information and Telecommunications in the Context of International Security. The unspoken aim of this resolution was to curb the technological superiority of the United States, and slow down the development of cyber and information communication technology capabilities that could be used against other states.5 Indeed, Russia viewed the “unprecedented level of development and application of modern, substantially new information technologies and means of telecommunication” as presenting new policy options in international affairs and matters of international security. More precisely, Russia worried that developments in the information field “would be used for purposes incompatible with the objectives of maintaining international stability and security and of observing the principles of the non-use of force, non-interference in internal affairs, and respect for human rights and freedoms.”6 The US establishment of a dedicated a strategic cyber command headed by the same person responsible for the state’s main espionage apparatus – the NSA - over a decade later inadvertently pushed many states towards the Russian camp.7 These developments stand in stark contrast to earlier discussions within WSIS and other international fora regarding the significant potential of ICTs in promoting peace and development.8 These challenges have emerged at a moment when the post-Cold War international “uni-polar” order is undergoing important changes with some states emerging to challenge US pre-eminence on several fronts, including governance of the Internet. 9 In some respects, the Internet governance agenda has become the center of gravity for efforts aimed at shifting information power away from the US and ‘taming’ its leadership on cyber security matters.10 In addition, some authoritarian governments are seeking to regain or maintain control of information flowing through their national borders,11 including as a means to push back against Western influence or interference. In Russia for example, repeated efforts have been made in international fora either directly or via the Shanghai Cooperation Organization (SCO) to fend off potential ‘information wars’ that could “[harm] social, political and economic systems, as well as spiritual, moral, and cultural spheres of other States.”12 In China, a speech by Jiang Zemin in 1998 marked the beginning of a policy anchored in information control as a means to protect the country from inter alia ‘infiltration, subversive activities, and separatist activities of international and domestic hostile forces” and ensure that the “Western mode of political systems is never copied.13 The International Code of Conduct for Information Security,14 China’s signing of the Shanghai Cooperation Organization’s 2009 Agreement on Information Security15 as well as more recent developments16 appear to confirm this policy, at least in relation to control of content. At the same time, it is evident that China recognizes the importance of the Internet to its economic development and for resolving issues of social importance, and is enthusiastically promoting its expansion. 17 Over time, such shifts may lead to a less restrictive flow of information across its Internet. The different shifts in the balance and tools of power coupled with the complexity and confusion inherent in the uses of cyberspace have contributed to erosion of trust between states. Recent events have added to concerns of how potential missteps in cyberspace or the offensive use of cyber capabilities could exacerbate existing (and not necessarily cyber-related) tensions, potentially leading to escalation and armed conflict.18 For example, both China and the United States have accused each other of conducting protracted cyber espionage activities; the United Kingdom has also been accused of similar activities. Recent revelations of the reach of NSA espionage activities has only served to exacerbate these tensions, while also weakening the foundations upon which some of the Western arguments concerning Internet freedom and governance were built. Moreover, the United States has developed a policy and a doctrine for offensive cyber operations.19 In fact, offensive cyber operations have now been formalized as an additional instrument of national power.20 It is probable that other countries are also developing these capabilities.21 Again, while it is highly unlikely that these or similar actions will lead to hostile action or a breakdown in diplomatic relations, they still impact considerably on perceptions of trust in international relations. Such actions also sharpen perceptions of power (political, military and economic) inherent in information dominance in and beyond the theatre of war, and enhance the desirability of increasing cyber capabilities as a means to attain strategic goals. In short, they encourage competition rather than cooperation between states. Conversely, these developments have also had the combined counter-intuitive effect of creating a form of “strategic pause” among the major powers, at least for now, and may allow for progress to be made toward a consensus on how to move forward collectively to ensure that international peace and security are not undermined by incidents in cyberspace or the use of offensive cyber capabilities against non-cyber targets.22 In this regard, states are making significant efforts to marshal soft power - the “ability to attract or co-opt as opposed to the use of coercion or the use of force” - to reach consensus on norms for responsible state behaviour in cyberspace as well as confidence building measures (CBMs). 23 Norms in particular are important given the current geopolitical information landscape, since they can “normalize the exercise of power in cyberspace,” serving as a form of deterrent for aggressive cyber behaviour. 24 Indeed, if complied with, norms can potentially “channel, constrain and constitute action through inducement and coercion; moral pressure and persuasion; and social learning and habit.”25 As noted at a recent meeting on Cybersecurity and Confidence Building Measures, CBMs can, on the other hand, serve to lay the foundation for agreeing on such norms and on measures to avoid miscalculation and escalation. They can also represent initial steps towards CBMs. U.S.-China and UK-China consultations on international cyber security are much more recent; while yet to yield concrete results, discussions seem to be moving forward. Meanwhile, similar official consultations on cyber security issues are emerging in bilateral talks among other states. In addition to these developments, the government of South Korea is now preparing for the next international conference on cyberspace, which will build on the earlier efforts of the United Kingdom and Hungary to broaden the dialogue beyond state actors, and assess progress to date. These are positive developments, which provide a degree of optimism that strategic restraint may become the rule rather than the exception in matters of offensive cyber operations, even if cyber- espionage will undoubtedly continue unabated.29 Indeed, these important steps suggest that states may be ready to move beyond earlier efforts marked by ideological differences and competing strategic interests between groups of states which hindered even minor agreements on norms and confidence building measures.30 Only time will tell however, whether these efforts to resolve highly complex interdependent issues, and which hinge significantly on the deployment of a soft power that is increasingly losing legitimacy, will balance out the current bellicose rhetoric and displays of increasingly sophisticated cyber capabilities. The fact that these capabilities are already being used (mainly covertly) both in and outside the theatre of war to meet domestic and foreign policy goals and broader strategic objectives does not necessarily bode well; hence the urgency to make progress on CBMs, norms and other related international regimes and processes related to the malicious uses of cyberspace, and expand the discussion beyond the state to other sectors, including, but not limited to, the private sector. In this regard, deeper engagement of civil society and academia will be imperative, 31 not only on Internet governance and Internet freedom issues where their voices and actions are already well anchored, but on broader international cybersecurity, including norms and CBMs processes. 32 Such engagement would also be more in tune with the role and influence these other actors de facto play in relation to cyberspace, but which is not always recognised or welcomed. Finally, the current predominant focus on state power and state-on-state rivalry with regard to cyberspace and ICTs risks once again removing attention from the “the wars that might actually have to be fought” i.e. the more asymmetrical transnational threats faced by all states – large and small, developed or developing – around which international collaboration is potentially much more achievable in the short-term, and which could establish the basis for more effective norms in the longer-term. States must work for a balance between both approaches.

#### Legitimacy is key to band-wagoning alliances and heg

Lavina Rajendram Lee 10 is a lecturer in the Department of Modern History, Politics and International Relations at Macquarie University, Australia, and has a PhD in International Relations from the University of Sydney. “US Hegemony and International Legitimacy,” 1-25-10, <http://www.routledge.com/books/details/9780415552363/>, Accessed date: 11-7-12 y2k

This book examines US hegemony and international legitimacy in the post-Cold War era, focusing on its leadership in the two wars on Iraq. The preference for unilateral action in foreign policy under the Bush Administration, culminating in the use of force against Iraq in 2003, has unquestionably created a crisis in the legitimacy of US global leadership. Of central concern is the ability of the United States to act without regard for the values and interests of its allies or for international law on the use of force, raising the question: does international legitimacy truly matter in an international system dominated by a lone superpower? US Hegemony and International Legitimacy explores the relationship between international legitimacy and hegemonic power through an in depth examination of two case studies – the Gulf Crisis of 1990-91 and the Iraq Crisis of 2002-03 – and examines the extent to which normative beliefs about legitimate behaviour influenced the decisions of states to follow or reject US leadership. The findings of the book demonstrate that subordinate states play a crucial role in consenting to US leadership and endorsing it as legitimate and have a significant impact on the ability of a hegemonic state to maintain order with least cost. Understanding of the importance of legitimacy will be vital to any attempt to rehabilitate the global leadership credentials of the United States under the Obama Administration.

#### Alliances solve multiple extinction scenarios

Nye 8 (Joseph, professor of International Relations at Harvard University, *“American Power After the Financial Crises,”* Foresight Project, 2008, http://www.foresightproject.net/publications/articles/article.asp?p=3533)

Power always depends on context, and in today's world, it is distributed in a pattern that resembles a complex three-dimensional chess game. On the top chessboard, military power is largely unipolar and likely to remain so for some time. But on the middle chessboard, economic power is already multi-polar, with the US, Europe, Japan and China as the major players, and others gaining in importance. The bottom chessboard is the realm of transnational relations that cross borders outside of government control, and it includes actors as diverse as bankers electronically transferring sums larger than most national budgets at one extreme, and terrorists transferring weapons or hackers disrupting Internet operations at the other. It also includes new challenges like pandemics and climate change. On this bottom board, power is widely dispersed, and it makes no sense to speak of unipolarity, multi-polarity or hegemony. Even in the aftermath of the financial crisis, the giddy pace of technological change is likely to continue to drive globalisation, but the political effects will be quite different for the world of nation states and the world of non-state actors. In inter-state politics, the most important factor will be the continuing "return of Asia". In 1750, Asia had three-fifths of the world population and three-fifths of the world's product. By 1900, after the industrial revolution in Europe and America, Asia's share shrank to one-fifth of the world product. By 2040, Asia will be well on its way back to its historical share. The "rise" in the power of China and India may create instability, but it is a problem with precedents, and we can learn from history about how our policies can affect the outcome. A century ago, Britain managed the rise of American power without conflict, but the world's failure to manage the rise of German power led to two devastating world wars. In transnational politics, the information revolution is dramatically reducing the costs of computing and communication. Forty years ago, instantaneous global communication was possible but costly, and restricted to governments and corporations. Today it is virtually free to anyone with the means to enter an internet café. The barriers to entry into world politics have been lowered, and non-state actors now crowd the stage. In 2001, a non-state group killed more Americans than the government of Japan killed at Pearl Harbor. A pandemic spread by birds or travelers on jet aircraft could kill more people than perished in the first or second world wars. This is a new world politics with which we have less experience. The problems of power diffusion (away from states) may turn out to be more difficult than power transition among states. The problem for American power in the 21st century is that there are more and more things outside the control of even the most powerful state. Although the United States does well on the traditional measures, there is increasingly more going on in the world that those measures fail to capture. Under the influence of the information revolution and globalisation, world politics is changing in a way that means Americans cannot achieve all their international goals acting alone. For example, international financial stability is vital to the prosperity of Americans, but the United States needs the cooperation of others to ensure it. Global climate change too will affect the quality of life, but the United States cannot manage the problem alone. And in a world where borders are becoming more porous than ever to everything from drugs to infectious diseases to terrorism, America must mobilise international coalitions to address shared threats and challenges. As the largest country, American leadership will remain crucial. The problem of American power after this crisis is not one of decline, but realisation that even the largest country cannot achieve its aims without the help of others

#### Heg solves global nuclear war—multiple hotspots

Brooks, Ikenberry, and Wohlforth, 13 [Stephen G. Brooks, G. John Ikenberry, and William C. Wohlforth, STEPHEN G. BROOKS is Associate Professor of Government at Dartmouth College. G. JOHN IKENBERRY is a Professor of Politics and International Affairs at Princeton University and Global Eminence Scholar at Kyung Hee University in Seoul. WILLIAM C. WOHLFORTH is a Professor of Government at Dartmouth College, January 2013, Lean Forward In Defense of American Engagement, <http://www.twc.edu/sites/default/files/assets/academicCourseDocs/22.%20Brooks,%20Lean%20Forward.pdf>, B. Morales]

¶ They are wrong. In making their case, advocates of retrenchment overstate the costs of the current grand strategy and understate its benefits. In fact, the budgetary savings of lowering the United States' international profile are debatable, and there is little evidence to suggest that an internationally engaged America provokes other countries to balance against it, becomes overextended, or gets dragged into unnecessary wars.¶ The benefits of deep engagement, on the other hand, are legion. U.S. security commitments reduce competition in key regions and act as a check against potential rivals. They help maintain an open world economy and give Washington leverage in economic negotiations. And they make it easier for the United States to secure cooperation for combating a wide range of global threats. Were the United States to cede its global leadership role, it would forgo these proven upsides while exposing itself to the unprecedented downsides of a world in which the country was less secure, prosperous, and influential.¶ AN AFFORDABLE STRATEGY¶ Many advocates of retrenchment consider the United States' assertive global posture simply too expensive. The international relations scholar Christopher Layne, for example, has warned of the country's "ballooning budget deficits" and argued that "its strategic commitments exceed the resources available to support them." Calculating the savings of switching grand strategies, however, is not so simple, because it depends on the expenditures the current strategy demands and the amount required for its replacement -- numbers that are hard to pin down.¶ If the United States revoked all its security guarantees, brought home all its troops, shrank every branch of the military, and slashed its nuclear arsenal, it would save around $900 billion over ten years, according to Benjamin Friedman and Justin Logan of the Cato Institute. But few advocates of retrenchment endorse such a radical reduction; instead, most call for "restraint," an "offshore balancing" strategy, or an "over the horizon" military posture. The savings these approaches would yield are less clear, since they depend on which security commitments Washington would abandon outright and how much it would cost to keep the remaining ones. If retrenchment simply meant shipping foreign-based U.S. forces back to the United States, then the savings would be modest at best, since the countries hosting U.S. forces usually cover a large portion of the basing costs. And if it meant maintaining a major expeditionary capacity, then any savings would again be small, since the Pentagon would still have to pay for the expensive weaponry and equipment required for projecting power abroad.¶ The other side of the cost equation, the price of continued engagement, is also in flux. Although the fat defense budgets of the past decade make an easy target for advocates of retrenchment, such high levels of spending aren't needed to maintain an engaged global posture. Spending skyrocketed after 9/11, but it has already begun to fall back to earth as the United States winds down its two costly wars and trims its base level of nonwar spending. As of the fall of 2012, the Defense Department was planning for cuts of just under $500 billion over the next five years, which it maintains will not compromise national security. These reductions would lower military spending to a little less than¶ ¶ three percent of GDP by 2017, from its current level of 4.5 percent. The Pentagon could save even more with no ill effects by reforming its procurement practices and compensation policies.¶ Even without major budget cuts, however, the country can afford the costs of its ambitious grand strategy. The significant increases in military spending proposed by Mitt Romney, the Republican candidate, during the 2012 presidential campaign would still have kept military spending below its current share of GDP, since spending on the wars in Afghanistan and Iraq would still have gone down and Romney's proposed nonwar spending levels would not have kept pace with economic growth. Small wonder, then, that the case for pulling back rests more on the nonmonetary costs that the current strategy supposedly incurs.¶ UNBALANCED¶ One such alleged cost of the current grand strategy is that, in the words of the political scientist Barry Posen, it "prompts states to balance against U.S. power however they can." Yet there is no evidence that countries have banded together in anti-American alliances or tried to match the United States' military capacity on their own -- or that they will do so in the future.¶ Indeed, it's hard to see how the current grand strategy could generate true counterbalancing. Unlike past hegemons, the United States is geographically isolated, which means that it is far less threatening to other major states and that it¶ faces no contiguous great-power rivals that could step up to the task of balancing against it. Moreover, any competitor would have a hard time matching the U.S. military. Not only is the United States so far ahead militarily in both quantitative and qualitative terms, but its security guarantees also give it the leverage to prevent allies from giving military technology to potential U.S. rivals. Because the United States dominates the high-end defense industry, it can trade access to its defense market for allies' agreement not to transfer key military technologies to its competitors. The embargo that the United States has convinced the EU to maintain on military sales to China since 1989 is a case in point.¶ If U.S. global leadership were prompting balancing, then one would expect actual examples of pushback -- especially during the administration of George W. Bush, who pursued a foreign policy that seemed particularly unilateral. Yet since the Soviet Union collapsed, no major powers have tried to balance against the United States by seeking to match its military might or by assembling a formidable alliance; the prospect is simply too daunting. Instead, they have resorted to what scholars call "soft balancing," using international institutions and norms to constrain Washington. Setting aside the fact that soft balancing is a slippery concept and difficult to distinguish from everyday diplomatic competition, it is wrong to say that the practice only harms the United States. Arguably, as the global leader, the United States benefits from employing soft-balancing-style leverage more than any other country. After all, today's rules and institutions came about under its auspices and largely reflect its interests, and so they are in fact tailor-made for soft balancing by the United States itself. In 2011, for example, Washington coordinated action with several Southeast Asian states to oppose Beijing's claims in the South China Sea by pointing to established international law and norms.¶ Another argument for retrenchment holds that the United States will fall prey to the same fate as past hegemons and accelerate its own decline. In order to keep its ambitious strategy in place, the logic goes, the country will have to divert resources away from more productive purposes -- infrastructure, education, scientific research, and so on -- that are necessary to keep its economy competitive. Allies, meanwhile, can get away with lower military expenditures¶ ¶ and grow faster than they otherwise would.¶ The historical evidence for this phenomenon is thin; for the most part, past superpowers lost their leadership not because they pursued hegemony but because other major powers balanced against them -- a prospect that is not in the cards today. (If anything, leading states can use their position to stave off their decline.) A bigger problem with the warnings against "imperial overstretch" is that there is no reason to believe that the pursuit of global leadership saps economic growth. Instead, most studies by economists find no clear relationship between military expenditures and economic decline.¶ To be sure, if the United States were a dramatic outlier and spent around a quarter of its GDP on defense, as the Soviet Union did in its last decades, its growth and competitiveness would suffer. But in 2012, even as it fought a war in Afghanistan and conducted counterterrorism operations around the globe, Washington spent just 4.5 percent of GDP on defense -- a relatively small fraction, historically speaking. (From 1950 to 1990, that figure averaged 7.6 percent.) Recent economic difficulties might prompt Washington to reevaluate its defense budgets and international¶ commitments, but that does not mean that those policies caused the downturn. And any money freed up from dropping global commitments would not necessarily be spent in ways that would help the U.S. economy.¶ Likewise, U.S. allies' economic growth rates have nothing to do with any security subsidies they receive from Washington. The contention that lower military expenditures facilitated the rise of Japan, West Germany, and other countries dependent on U.S. defense guarantees may have seemed plausible during the last bout of declinist anxiety, in the 1980s. But these states eventually stopped climbing up the global economic ranks as their per capita wealth approached U.S. levels -- just as standard models of economic growth would predict. Over the past 20 years, the United States has maintained its lead in per capita GDP over its European allies and Japan, even as those countries' defense efforts have fallen further behind. Their failure to modernize their militaries has only served to entrench the United States' dominance.¶ LED NOT INTO TEMPTATION¶ The costs of U.S. foreign policy that matter most, of course, are human lives, and critics of an expansive grand strategy worry that the United States might get dragged into unnecessary wars. Securing smaller allies, they argue, emboldens those states to take risks they would not otherwise accept, pulling the superpower sponsor into costly conflicts -- a classic moral hazard problem. Concerned about the reputational costs of failing to honor the country's alliance commitments, U.S. leaders might go to war even when no national interests are at stake.¶ History shows, however, that great powers anticipate the danger of entrapment and structure their agreements to protect themselves from it. It is nearly impossible to find a clear case of a smaller power luring a reluctant great power into war. For decades, World War I served as the canonical example of entangling alliances supposedly drawing great powers into a fight, but an outpouring of new historical research has overturned the conventional wisdom, revealing that the war was more the result of a conscious decision on Germany's part to try to dominate Europe than a case of alliance entrapment.¶ If anything, alliances reduce the risk of getting pulled into a conflict. In East Asia, the regional security agreements that Washington struck after World War II were designed, in the words of the political scientist Victor Cha, to "constrain anticommunist allies in the region that might engage in aggressive behavior against adversaries that could entrap the United States in an unwanted larger war." The same logic is now at play in the U.S.-Taiwanese relationship.¶ ¶ After cross-strait tensions flared in the 1990s and the first decade of this century, U.S. officials grew concerned that their ambiguous support for Taiwan might expose them to the risk of entrapment. So the Bush administration adjusted its policy, clarifying that its goal was to not only deter China from an unprovoked attack but also deter Taiwan from unilateral moves toward independence.¶ For many advocates of retrenchment, the problem is that the mere possession of globe-girdling military capabilities supposedly inflates policymakers' conception of the national interest, so much so that every foreign problem begins to look like America's to solve. Critics also argue that the country's military superiority causes it to seek total solutions to security problems, as in Afghanistan and Iraq, that could be dealt with in less costly ways. Only a country that possessed such awesome military power and faced no serious geopolitical rival would fail to be satisfied with partial fixes, such as containment, and instead embark on wild schemes of democracy building, the argument goes.¶ Furthermore, they contend, the United States' outsized military creates a sense of obligation to do something with it even when no U.S. interests are at stake. As Madeleine Albright, then the U.S. ambassador to the un, famously asked Colin Powell, then chairman of the Joint Chiefs of Staff, when debating intervention in Bosnia in 1993, "What's the point of having this superb military you're always talking about if we can't use it?"¶ If the U.S. military scrapped its forces and shuttered its bases, then the country would no doubt eliminate the risk of entering needless wars, having tied itself to the mast like Ulysses. But if it instead merely moved its forces over the horizon, as is more commonly proposed by advocates of retrenchment, whatever temptations there were to intervene would not disappear. The bigger problem with the idea that a forward posture distorts conceptions of the national interest, however, is that it rests on just one case: Iraq. That war is an outlier in terms of both its high costs (it accounts for some two-thirds of the casualties and budget costs of all U.S. wars since 1990) and the degree to which the United States shouldered them alone. In the Persian Gulf War and the interventions in Bosnia, Kosovo, Afghanistan, and Libya, U.S. allies bore more of the burden, controlling for the size of their economies and populations.¶ Besides, the Iraq war was not an inevitable consequence of pursuing the United States' existing grand strategy; many scholars and policymakers who prefer an engaged America strongly opposed the war. Likewise, continuing the current grand strategy in no way condemns the United States to more wars like it. Consider how the country, after it lost in Vietnam, waged the rest of the Cold War with proxies and highly limited interventions. Iraq has generated a similar reluctance to undertake large expeditionary operations -- what the political scientist John Mueller has dubbed "the¶ Iraq syndrome." Those contending that the United States' grand strategy ineluctably leads the country into temptation need to present much more evidence before their case can be convincing.¶ KEEPING THE PEACE¶ Of course, even if it is true that the costs of deep engagement fall far below what advocates of retrenchment claim, they would not be worth bearing unless they yielded greater benefits. In fact, they do. The most obvious benefit of the current strategy is that it reduces the risk of a dangerous conflict. The United States' security commitments deter states with aspirations to regional hegemony from contemplating expansion and dissuade U.S. partners from trying to solve security problems on their own in ways that would end up threatening other states.¶ Skeptics discount this benefit by arguing that U.S. security guarantees aren't necessary to prevent dangerous rivalries from erupting. They maintain that the high costs of territorial conquest and the many tools countries can use to signal¶ ¶ their benign intentions are enough to prevent conflict. In other words, major powers could peacefully manage regional multipolarity without the American pacifier.¶ But that outlook is too sanguine. If Washington got out of East Asia, Japan and South Korea would likely expand their military capabilities and go nuclear, which could provoke a destabilizing reaction from China. It's worth noting that during the Cold War, both South Korea and Taiwan tried to obtain nuclear weapons; the only thing that stopped them was the United States, which used its security commitments to restrain their nuclear temptations. Similarly, were the United States to leave the Middle East, the countries currently backed by Washington -- notably, Israel, Egypt, and Saudi Arabia -- might act in ways that would intensify the region's security dilemmas.¶ There would even be reason to worry about Europe. Although it's hard to imagine the return of great-power military competition in a post-American Europe, it's not difficult to foresee governments there refusing to pay the budgetary costs of higher military outlays and the political costs of increasing EU defense cooperation. The result might be a continent incapable of securing itself from threats on its periphery, unable to join foreign interventions on which U.S. leaders might want European help, and vulnerable to the influence of outside rising powers.¶ Given how easily a U.S. withdrawal from key regions could lead to dangerous competition, advocates of retrenchment tend to put forth another argument: that such rivalries wouldn't actually hurt the United States. To be sure, few doubt that the United States could survive the return of conflict among powers in Asia or the Middle East -- but at what¶ cost? Were states in one or both of these regions to start competing against one another, they would likely boost their military budgets, arm client states, and perhaps even start regional proxy wars, all of which should concern the United States, in part because its lead in military capabilities would narrow.¶ Greater regional insecurity could also produce cascades of nuclear proliferation as powers such as Egypt, Saudi Arabia, Japan, South Korea, and Taiwan built nuclear forces of their own. Those countries' regional competitors might then also seek nuclear arsenals. Although nuclear deterrence can promote stability between two states with the kinds of nuclear forces that the Soviet Union and the United States possessed, things get shakier when there are multiple nuclear rivals with less robust arsenals. As the number of nuclear powers increases, the probability of illicit transfers, irrational decisions, accidents, and unforeseen crises goes up.

### Advantage 2-Democracy

#### The perception of state-based cyber authority encourages autocracy—emerging powers will adopt a statist approach to the internet

Wallace, 13

(Ian Wallace, visiting fellow in the Center on 21st Century Security and Intelligence at Brookings. Wallace previously served as a senior official at the British Ministry of Defence, where he helped develop the UK government’s cyber strategy as well as Britain’s cyber relationship with the United States. “Militarizing the Internet?” <http://nationalinterest.org/commentary/militarizing-the-internet-8734?page=show>) Henge

But a more subtle and damaging effect relates to how the internet operates. The United States and its allies are currently engaged in a low-profile but highly consequential tussle for the future of the internet. Although out of day-to-day public view, this matters, as the internet now underpins the global economy. While it is self-evident to us that minimizing government involvement is precisely what ensures the success of the internet, it is equally clear to authoritarian states like Russia and China that the internet (including the content it carries) must to be controlled. This latter view is exemplified by the desire of Russia, China and others to see the International Telecommunications Union, an adopted member of the United Nations family, expand its role into setting international rules for the internet. Despite alarmist concerns to the contrary, there is no practical way in which the United Nations (or any other organization) could “take over” the internet. But if the United States starts to be seen as a danger to others, new barriers will emerge and everyone will lose. It is probably now unrealistic to expect the most authoritarian states to buy into the current manifestation of the so-called “multistakeholder” governance model. That is especially true for weaker states who believe they have reason to fear Washington or its allies (think the Middle East), but the fact that emerging powers like India and Brazil still flirt with a more statist approach to internet governance is a worrying portent of trouble ahead. Such positions cannot be blamed solely on Stuxnet and Snowden’s disclosures, but they certainly don’t help. Likewise, involvement of U.S. brands Google, Facebook, Microsoft and others in spying operations only plays to the paranoia of those who see such firms—Washington’s true cyber power—as extensions of the American state.

#### Democratic peace theory is the most empirically supported causal explanation for nonviolence—multiple explanations prove democratization is sufficient to prevent conflict—socio-economic developments can only create peace when filtered through democracies—debating over DPT is uniquely good for academia

Hegre, 14

(Håvard Hegre Department of Peace and Conflict Research, Uppsala University & Peace Research Institute Oslo (PRIO) “Democracy and armed conflict” SAGE) Henge

Introduction The idea that democracies rarely if ever fight each other is often traced back to Immanuel Kant (1795/1991). The citizens of a (democratic) republic will hesitate before embarking on a war, for ‘this would mean calling down on themselves all the miseries of war’ (p. 100).1 The modern debate on the ‘democratic peace’ surged from the obscurity of the Wisconsin Sociologist (Babst, 1964) during the Cold War to a place of prominence in international relations around the turn of the millennium. By that time, there was a consensus that democracies do not fight each other in interstate wars. In parallel with the establishment of empirical evidence for an interstate democratic peace, several studies also indicate that democratic states have less frequent domestic armed conflicts. The argument that democracy causes peace has important implications, and may even have profoundly influenced US policies in the buildup to the 2003 Gulf War (Owen, 2005; Gat, 2005; Russett, 2005). The democratic peace debate fundamentally influenced IR scholarship also beyond its substantive importance. It brought a major shift toward the acceptance of large-N statistical studies within IR, as represented by the seminal designs of Bremer (1992) and Maoz & Russett (1992). Along with the studies of the more general ‘liberal peace’, the debate stimulated the introduction of several methodological innovations within the field, such as the treatment of reverse causation or temporal dependence. Much of this innovation was stimulated by the emerging practice of posting replication datasets, pioneered by JPR and scholars such as John Oneal and Bruce Russett.2 Below, I summarize the empirical evidence for the interstate and domestic peace propositions and the main theoretical arguments explaining them, and note the most important objections. Several similarities between the two forms of the democratic peace emerge. This is particularly true for what I see as the most critical challenge to the democratic peace, namely that both democracy and peace are due to pre-existing socio-economic conditions. This objection has considerable leverage, but it also seems clear that these conditions are unlikely to bring about lasting peace alone, without democratic institutions. Main empirical findings The interstate democratic peace The interstate democratic peace has been studied at several ‘levels of analysis’ (Gleditsch & Hegre, 1997). At the dyadic level, there is considerable agreement that the ‘absence of war between democratic states comes as close as anything we have to an empirical law in international relations’ (Levy, 1989: 270).3 Important studies in favor of the proposition are Rummel (1983), Doyle (1983, 1986), and a string of studies by Bruce Russett and coauthors (e.g. Maoz & Russett, 1992, 1993; Russett & Oneal, 2001). Following the review of Gleditsch (1992), JPR became a major outlet for the debate.4 The dyadic finding has to a large degree withstood a series of counter-arguments. I discuss these in detail below. There is less compelling evidence for democratic countries being less warlike overall – the ‘monadic’ level of the democratic peace. The bulk of the early large-N studies (e.g. Small & Singer, 1976; Weede, 1984), agree with Chan (1984) who found that ‘relatively free’ countries participated in war just as much as the ‘less free’. Gleditsch & Hegre (1997) show that democracies rarely initiate wars, and Hegre (2008) that they are more peaceful overall when controlling for their military potential. Research at the system level has recently attracted renewed attention.5 Gleditsch & Hegre (1997) suggest that a world with an intermediate share of democracy may be associated with more war since the probability of war on average is highest in dyads with one democracy and one non-democracy. However, an increase in the proportion of countries that are democratic may alter the dyadic and monadic probabilities as systemic democratization affects international interactions (Russett, 1993; Huntley, 1996; Mitchell, Gates & Hegre, 1999; Kadera, Crescenzi & Shannon, 2003). Cederman (2001) rephrases the standard account of Kant (1795/1991), seeing the development of the democratic peace as a dialectic process where states gradually learn to form (democratic) pacific unions. He shows that the risk of war between democracies has been falling over the past two centuries. The risk of non-democratic war has also declined, but less swiftly. Relatedly, Mitchell (2002) shows that non-democracies in the Americas became much more likely to settle territorial claims peacefully when the proportion of democracies in the system increased. Gartzke & Weisiger (2013), on the other hand, argue that regime type becomes a less salient indicator of ‘otherness’ as more states become democratic, and their empirical analysis indicates that the risk of conflict between democracies has increased as the world has become more democratic.6 Studies using tools of network analysis also indicate systemic effects of democracy. Dorussen & Ward (2010) and Lupu & Traag (2013) find support for the democratic peace while accounting for the pacifying impact of trade networks. Maoz (2006) finds that large ‘democratic cliques’ in networks dampen conflicts, but Cranmer & Desmarais (2011) conclude that the support for this claim is weak when using a more appropriate statistical method. The internal democratic peace A number of studies find empirical confirmation of an ‘inverted-U’ relationship between level of democracy and the probability of onset of internal armed conflict. Semidemocratic regimes have a higher risk of internal conflict than consistent autocracies or democracies (Boswell & Dixon, 1990; Muller & Weede, 1990; Hegre et al., 2001; Fearon & Laitin, 2003). The existence of this ‘inverted U’ has been challenged, however (Elbadawi & Sambanis, 2002; Collier & Hoeffler, 2004; Vreeland, 2008).7 In any case, very few studies find traces of a monotonic effect of democracy. When controlling for GDP per capita or other indicators of socio-economic development, democratically governed countries have no lower risk of internal armed conflict than autocratic ones Buhaug (2006) finds that semi-democracies have a higher risk of wars over government than autocracies and democracies, but that democracies are more likely to experience conflicts over territory than the other two regime types. Cederman, Hug & Krebs (2010) find democratization to affect conflicts over government, but not over territory. Although democratic institutions by themselves are ineffective in reducing risk of internal conflict onset, several studies find that they affect how internal conflicts evolve. Lacina (2006) and Gleditsch, Hegre & Strand (2009) show that internal wars in democracies are less lethal. Democratic governments make use of less violence against civilians (Eck&Hultman, 2007) and engage in less repression (Davenport, 2007b; Colaresi & Carey, 2008),9 but rebel groups tend to make more extensive use of violence against civilians when fighting democratic regimes (Eck & Hultman, 2007). Possibly because of the stronger constraints on the use of violence against insurgents, democracies tend to have longer internal wars (Gleditsch, Hegre & Strand, 2009).10 Some studies, such as Mukherjee (2006), find that post-conflict democracies have a lower risk of conflict recurrence. Other studies report contrasting results (Walter, 2004; Quinn, Mason & Gurses, 2007; Collier, Hoeffler & So¨derbom, 2008). Explanations Interstate conflict Although there is scholarly agreement that democracies rarely if ever have fought each other, there is less consensus as to why. The following five sets of explanations are important: First, the normative explanation (Doyle, 1986;Maoz& Russett, 1993) holds that ‘the culture, perceptions, and practices that permit compromise and the peaceful resolution of conflicts without the threat of violence within countries come to apply across national boundaries toward other democratic countries as well’ (Ember, Ember & Russett, 1992: 576). States ‘externalize’ the domestic norms that encourage compromise solutions and reciprocation, and strictly inhibit the complete removal from political life of the loser in political contest. The absence of a monadic democratic peace is troublesome for the normative explanation, in particular since it implies that the probability of conflict between democracies and non-democracies must be higher than that between two non-democracies (Raknerud & Hegre, 1997). Rosato (2003) points to the frequent violation of liberal norms when democracies have decided to go to war – in imperial wars, as well as in frequent US interventions intended to overthrow democratically elected governments (Rosato, 2003: 589–590).11 Another notable caveat noted as early as in Kant (1795/1991), is the incentive to intervene in non-democracies to press for democratization (Peceny, 1999; Gleditsch, Christiansen & Hegre, 2007). A particularly critical view of democratic war behavior is found in Geis, Brock & Mu¨ller (2006). Second, according to the legislative constraints explanation, democratic leaders are constrained by other bodies (such as parliaments) which ensure that the interests of citizens and powerful organizations are taken into account. Debate is public, so information on the real costs of war is likely to enter the decision calculus. Democratic political leaders will be removed from office if they circumvent these constraints.12 Democracies’ ability to signal resolve is a third explanation. Why are states not able to agree to a solution that reflects the distribution of power and the actors’ ‘resolve’, without incurring the costs of war (Fearon, 1995)? One answer is that if crisis escalation is not very costly, both parties have an incentive to exaggerate their power or resolve, mobilize, and back down when the bluff is discovered. Fearon (1994) argues that audience costs – the costs that a leader suffers when backing down – lock leaders into their positions, increasing the costs of bluffing. Democracies have higher audience costs, Fearon argues, and may more credibly commit to policies with little crisis-inducing behavior to signal intentions.13 Making use of various empirical strategies to distinguish the explanations, Schultz (1999) and Prins (2003) find stronger support for the signaling argument than for the constraints explanation. Weeks (2008) builds on this argument by showing that single-party regimes also indicate behavior in line with a signaling argument. Downes & Sechser (2012), Snyder & Borghard (2011), and Trachtenberg (2012), on the other hand, find little empirical evidence for the audience cost argument.14 Fourth, in a mobilization argument Bueno deMesquita et al. (1999, 2003) argue that the democratic re-election pressures on leaders tend to make them more careful to select only wars they are likely to win, and to mobilize more resources for the war efforts they select than do autocratic leaders. This makes democracies unattractive targets, since they are likely to win the wars they fight (Reiter & Stam, 1998).15 Both of these tendencies tend to reduce the probability of war between democracies. One aspect of the effectiveness of democracies in war is their ability to form large alliances in important wars (Doyle, 1986; Raknerud & Hegre, 1997). The empirical analysis in Gartzke & Gleditsch (2004), however, suggests that democracies are less reliable allies. Leeds, Mattes & Vogel (2009), on the other hand, find that countries with democratic institutions are much less likely to abrogate international commitments than autocratic countries in instances where domestic leadership transitions result in leaders with different primary bases of societal support. Fifth, Gartzke (1998) points out that the democratic peace finding might be due to joint interests. Democracies may fail to disagree sufficiently on international policies to be willing to suffer the costs of war. Such joint interests may be due to the fact that most democracies were on the same side during the Cold War (Farber & Gowa, 1995).16 The failure to observe a monadic democratic peace (Gartzke & Weisiger, 2013: 172) and the observation of an ‘autocratic peace’ (Werner, 2000; Peceny, Beer & Sanchez-Terry, 2002) support this argument. 17 An autocratic peace can hardly be explained by constraints inherent in autocratic regimes, but must be due to shared interests. Gartzke (1998, 2000) shows that controlling for joint interests weakens the magnitude and significance of the evidence for a democratic peace.18 Joint interests and joint regime types may be linked through three pathways. First, joint democracy may itself give rise to joint interests, such as an interest in the promotion of democratic regimes or through similar incentives for political leaders to expand the territory they control. The profitability of occupation is less certain for democratic leaders than for autocratic countries, since the benefits of occupation have to be shared between almost as many as those who bear the costs (Rosecrance, 1986). Moreover, in order to extract much from the conquered territory, the people resident there have to be denied the political rights that are held by the citizens of the occupying country. 19 Hence, joint democracy may lead to the mutual acceptance of international borders, removing an important source of war (Huth & Allee, 2002). Relatedly, Schweller (1992) argues that regime type affects how declining powers behave. When challenged by rising powers, realist theory posits that leading powers wage preventive wars to maintain their military hegemony. Preventive wars are less attractive to democratic leaders. If the rising power is another democracy, the historical absence of war between democracies indicates that the threat is minimal. If it is non-democratic, the public is wary of the risks and costs of a war where the danger is not imminent, and the formation of alliances to counterbalance the non-democratic threat is often a preferable strategy.20 Internal conflict The earliest arguments for an internal democratic peace are related to the normative and structural explanations of the interstate variant. Democracy is seen as a system for peaceful resolution of conflicts, as conflicting claims by rival social groups are solved by majority votes or consensual agreements. If individuals are denied the political rights and the economic benefits they believe they are entitled to, they may react with aggression and organize violent political opposition. If conflict results from ‘relative deprivation’ (Davies, 1962; Gurr, 1968), democracies should be more peaceful internally than other regime types. Armed rebellion will not be profitable since democracies both allow discontent to be expressed and have mechanisms to handle it. Another argument holds that democratic institutions alter the risk of internal conflicts by facilitating effective bargaining and reducing commitment problems. Acemoglu & Robinson (2006: 24–25) note that citizens are excluded from de jure power in a nondemocracy. Still, they always enjoy some de facto power that sometimes allows citizens to obtain policy concessions from the elites in the short run. It is uncertain whether these will be maintained, however, since the balance between various social groups is transitory. Citizens, then, should demand that today’s de facto power is translated into de jure power that secures long-term concessions. This demand may be backed by a threat of revolution – a civil war. The elites cannot credibly commit to a promise of policy concessions in the indefinite future, however, as long as de facto power is transitory. Democratic institutions are the solution to this commitment problem (Acemoglu & Robinson, 2006). This explains democratization and shows why democratic institutions reduce the risk of (revolutionary) civil wars. Fearon (1995) likewise argues that bargaining failures and commitment problems are important explanations of war, and Fearon (2004: 288) argues that democratic regimes facilitate bargaining and credible commitments for internal conflicts.21 If either of these accounts is true, fully fledged democracies are less conflict-prone than repressive autocracies. One possible reason for not observing this is that democracies often are faced with opportunistic rebels whose aims do not reflect the interests of broad social groups. For internal conflicts, a parallel to the mobilization argument formulated for interstate conflict would encounter difficulties. Both democracies and non-democracies use military force to counter illegitimate armed opposition, but autocracies may make much more extensive use of repression without losing legitimacy – using violence to silence opponents, censorship, arbitrary imprisonment without trial, etc. Autocracies may indiscriminately target entire population groups to coerce influential individuals (Davenport& Armstrong, 2004; Carey, 2010).22 Autocracies also buy off other parts of the opposition by granting ministerial posts and by the selective channeling of public funds (Fjelde & de Soysa, 2009). The combination of these two methods allows effective divide-andrule strategies. Autocracies also repress the formation of organizations before they can reach the stage of armed insurgencies. Hence, regimes that feature both democratic and autocratic characteristics are partly open yet lack effective means of solving conflicts. In such political systems, repression is difficult since some organization of opposition groups and some opposition expression of discontent are allowed, but mechanisms to act on the expressed discontent are incomplete (cf. Davies, 1962; Boswell & Dixon, 1990; Muller &Weede, 1990; Hegre et al., 2001). Hence, repression is ineffective if ‘grievance’ is not simultaneously being addressed, which is why we observe an inverted-U relationship between democracy and peace. All in all, precisely because of the constraints on indiscriminate use of force, democracies may be disadvantaged when faced by opportunistic rebel groups. This claim has recently been contested, however. Analyzing data for insurgencies over the 1800–2006 period, Lyall (2010) finds no evidence that democracies are more frequently defeated or have to sustain conflict for longer periods. Does democracy cause peace? Empirically, the correlation between democracy and interstate peace is well established, as is the correlation between consolidated democracies and absence of internal conflict. Still, this does not necessarily mean that democracy causes peace. Two main objections have been raised to that causal inference – peace may cause democracy, or some other societal factors may cause both democracy and peace. Since these counter-arguments largely focus on what explains democratic institutions at the country level, the arguments apply to the domestic as well as the interstate democratic peace. Putting the cart before the horse? An implicit assumption in many statistical studies of the democratic peace is that the causal arrow goes from democracy to peace. Although not dismissing the pacifying effect of democracy completely, Thompson (1996) and Rasler & Thompson (2004) show that geopolitical constraints that were in place before democratization can account for the subsequent peace. Layne (1994: 45) argues that democratic regimes can afford democratic systems, ‘because there is no imminent external threat that necessitates a powerful governmental apparatus to mobilize resources for national security purposes’. Boix (2011) shows that democratization has been more frequent during periods where democracies have been hegemonic powers. Gates, Knutsen & Moses (1996: 5) add that peace leads to trade, investment, and economic growth, and thereby to democratization. Indeed, the idea of a reverse causation goes at least back to Wright (1965/1942: 841). Mousseau & Shi (1999) discuss the temporal aspects of the issue, and conclude that there is little evidence that autocratization tends to occur during or after wars – in fact, the opposite may be the case when democracies win the wars (Mitchell, Gates & Hegre, 1999). The main threat to the democratic peace proposition is change toward autocracy in anticipation of war. By means of interrupted time-series analysis, Mousseau & Shi (1999) find no clear trend of states changing toward autocracy before wars. Using instrument-variable methods, Kim & Rousseau (2013) agree that the democracy– peace correlation holds even when accounting for the pre-existing amount of violence in a region. Reiter (2001) finds that international conflict rarely blocks transitions to democracy. The simultaneous-equation analysis in Reuveny & Li (2003) shows that conflict reduces democracy, but also that democracy reduces conflict.23 In all, most attempts to ascertain the direction of causality by means of appropriately designed statistical methods seem to support the core tenet of the democratic peace, although there are dissenting voices such as James, Solberg & Wolfson (1999). Gibler (2007) formulates a more specific reversecausation argument. He points to Boix (2003) who notes the importance of the settlements of territorial claims in 17th- and 18th-century Europe. Without these, the fundamental economic changes required for democratization would not have happened.24 Such territorial agreements, then, indirectly give rise to clusters of democracies that have joint interests in keeping a separate peace. The empirical analysis in Gibler (2007) indicates that exogenous predictors of border stability tend to decrease the likelihood of territorial disputes and increase the probability of joint democracy, and that the evidence for the democratic peace is weaker when predictors of border stability are controlled for. The conclusions remain in doubt, however, as Park & Colaresi (forthcoming) report inability to replicate the results. Gibler & Tir (2010) expand the notion of territorial settlements to one of ‘positive territorial peace’, and show that peaceful territorial transfers lead to democratization and lower levels of militarization. The issue of reverse causation has not been equally prominent in the study of democracy and internal conflict, with some notable exceptions in particular in studies of repression and violence (Carey, 2006; Moore, 1998). The relative-deprivation argument, however, implies reverse causation. If deprivation is due to the lack of political rights, and civil war is a useful strategy to obtain such rights, war should lead to democracy. In contrast to this expectation, however, Gleditsch &Ward (2006) do find that civil wars tend to undermine democracies but do not affect the durability of autocracies. What drives democratization and peace? Perhaps the most serious challenge to the democratic peace comes from arguments suggesting that both democracy and peace are outcomes of more fundamental societal changes. Most of these are associated with socioeconomic development. Institutional consolidation. A possible indication of this is that the interstate democratic peace is weaker for young democracies (Maoz & Russett, 1992). Indeed, the process of democratization may increase the risk of war in the short run (Mansfield & Snyder, 1995).25 Relatedly, changes in the political institutions of a country are likely to be accompanied by a heightened risk of civil war (cf. Snyder, 2000; Hegre et al., 2001; Fearon & Laitin, 2003; Cederman, Hug & Krebs, 2010). Firstly, changes in a democratic direction are likely to be accompanied by reduced repression, allowing communal groups to mobilize. In addition, it takes a long time to make new institutions sufficiently efficient to accommodate deep social conflicts. Groups that increase their political influence will raise their expectations of real improvements in their living conditions, but these can be slow to materialize. Losers from the institutional changes, then, have an incentive to incite armed insurgencies to re-establish the previous status quo. Fearon & Laitin (2003: 85) interpret the inverted-U finding for internal conflicts as due not to the institutional characteristics themselves, but to an underlying conflict over the setup of the system: ‘‘‘anocracies’’ are weak regimes, lacking the resources to be successful autocrats or containing an unstable mix of political forces that makes them unable to move to crush nascent rebel groups’. This interpretation is supported by Gleditsch & Ruggeri (2010). Their proxy of instability (a variable recording recent irregular transitions of power) is associated with a high risk of conflict onset. Moreover, when controlling for it, they find a monotonic negative relationship between democracy and risk of conflict. Elections provide a special case of change – not to the institutions, but to the de jure distribution of power within electoral regimes. In new democracies, there is considerable uncertainty whether the main actors are truly committed to respecting the outcomes of elections. Most actors prefer to secure power by means of electoral victory since it bolsters the legitimacy of their rule. If they lose, however, they may find an attempt to seize power by force preferable to accepting the defeat. Several studies confirm that elections tend to be followed by an increased risk of internal conflict (Collier, Hoeffler & So¨derbom, 2008) or ethnic conflict (Cederman, Gleditsch & Hug, 2013). Market norms. Mousseau (2000) argued that both democratic consolidation and the democratic peace are due to a specific set of norms of contracting. These norms emerge in economically developed countries by a ‘process of cultural materialism’. Economic development requires a complex division of labor which typically is achieved through a dense web of voluntary contracts. These contracts pave the way for democratization since they foster norms of negotiation, trust, equity between contractees, and respect for property rights. The international manifestation of such norms is more peaceful behavior, since wars of conquest would violate these norms. An implication of this argument is that only developed democracies can maintain a separate peace. This expectation is supported in a set of statistical studies of interstate conflict (Mousseau, 2000; Mousseau, Hegre & Oneal, 2003; Hegre, 2000) and internal conflict (Hegre, 2003; Collier & Rohner, 2008). Controlling for a more direct measure of ‘contractintensive economies’ (CIE), Mousseau (2009: 82) concludes that ‘democracy is not a likely cause of peace among nations’. Dafoe, Oneal & Russett (2013), however, reject this conclusion. Still, they do find support for the effect of CIEs controlling for joint democracy and acknowledge that there is some overlap between the democratic peace and the effect of CIEs (Dafoe, Oneal & Russett, 2013: 209).26 Lootability. Another aspect of economic development is that it favors non-lootable or non-appropriable assets over lootable assets – ‘commerce’ is gradually replacing ‘conquest’ since ‘labor, capital, and information are mobile and cannot be definitively seized’ (Rosecrance, 1986: 48). This development-related change has an analogy in internal conflicts. When land-based assets such as most primary commodities are economically dominant, states have strong incentives to use physical force to retain control, and potential insurgents have similar incentives to try to seize control over the central power or to obtain larger autonomy for a region. This argument reflects the importance placed on primary commodity exports by Collier & Hoeffler (2004) and Fearon & Laitin (2003). Several rebel economic activities require high rebel territorial control, such as taxation of natural resource production, rich landowners, or household incomes (Fearon & Laitin, 2003). In the words of Boix (2008: 432), ‘In economies where wealth is either mobile or hard to tax or confiscate, sustained political violence to grab those assets does not pay off since their owners can either leave in response to the threat of confiscation or are indispensable to the optimal exploitation of assets.’ Boix finds strong empirical evidence for this account. It is supported by numerous empirical studies that show that extensive reliance on the export of oil – a highly appropriable asset – is associated with conflict as well as authoritarian rule (Fearon & Laitin, 2003; Fjelde, 2009; Ross, 2001). Relatedly, the models of democratization in Boix (2003) and Acemoglu & Robinson (2006) provide an explicit link between democratization and civil war – elites agree to democratization because they fear a revolution staged by the poor. Democratization, they argue, is least likely when inequality is extensive, since the redistributive tax rate preferred by the median voter then will be very high. Revolutions, then, will be more frequent in unequal societies, since the elites have a stronger incentive to resist democratization. If the assets that the rich control are in the form of land or other resources that cannot be moved out of the country, the poor will be able to impose radical taxes if they get to control the tax rate (Boix, 2003). If most of the wealth is in the form of financial capital, a larger fraction of it is ‘safe’ from taxation, and democratization is less threatening. Moreover, where lootable assets are predominant, rebel groups have incentives to stage limited campaigns not to entirely take over the government, but to secure local access to profitable natural resources. Joint interests. The democratic peace seen as merely ‘joint interests’ (Gartzke, 1998) may also be a function of economic development, as noted in Rosecrance (1986) and Gartzke (2007). Well into the 20th century, an ‘obsession with land’ was the major cause of war since states could improve their position by seizing other nations’ territory (Rosecrance, 1986: 48). During the 20th century, however, mobile factors of production – capital and labor – surpassed land in importance for productive strength. At the same time, nationalist resistance to occupation became more frequent, increasing the cost of extracting resources from a territory (also see Boix, 2003: 44–45). In addition, the diversity of resources employed speaks against a military strategy (Rosecrance, 1986; Brooks, 1999). Development may provide the motive and means for a state to seize a particular territory from another by force, but it also increases its dependence on third parties. War hampers trade with third parties either because of political reactions or because the heightened risk resulting from conflict increases the price of traded goods. The constraints imposed on developed states through their extensive trade with a great number of other nations are apt to outweigh the prospect of gaining control over one particular territory.27 Developed societies that are economically reliant on the revenues from international trade and investment place much more emphasis on the protection of property, political stability, and the integrity of international borders than on expanding own territories. Developed societies, then, have a joint interest in restricting attempts to expand territories, such as Saddam Hussein’s conquest of Kuwait, and a lack of interest in contesting own borders. Similar joint-interest explanations also apply to internal conflicts and to the incentives to resist democratization. Economic development, in particular the reliance on relations with international markets, also means that a large set of actors become reliant on preserving political stability. Interdependence. In several theories of democratization (Dahl, 1971; Olson, 1993; Boix, 2003), the high costs of violence and repression in densely interacting societies is an important factor. Dahl (1971) sees ‘modern dynamic pluralist’ societies as an essential prerequisite for democracy – democracy prevails because citizens can credibly threaten to hurt the elites economically by means of strikes, protests or exiting the country. The diversification and division of labor in developed economies leads to both democracy and internal peace. For interstate conflict, a similar argument states that strong dependence on trade and on capital constrains belligerent actors (Angell, 1910; Russett & Oneal, 2001). Domestic and foreign capital is likely to flee the country if war breaks out. Less capital-intensive economies are less constrained by these considerations (Gartzke, Li & Boehmer, 2001). In a critical review of the democratic peace, Gat (2005, 2006: 658) argues that it has overlooked the industrial revolution: ‘Rather than the cost of war becoming prohibitive . . . it was mainly the benefits of peace that increased dramatically once the Malthusian trap was broken, tilting the overall balance between war and peace for . . . industrializing and industrial societies, regardless of their regime, for which wealth acquisition ceased to be a zero-sum game.’ The capitalist peace. Gartzke (2007) argues that the liberal peace really is a ‘capitalist peace’. The rhetoric value of this term is greater than its precision. In effect, Gartzke’s argument draws on several of the effects of socio-economic development reviewed above. Interdependence and mobility of assets are equally important as the particular economic freedoms and financial structures traditionally associated with ‘capitalism’. Echoing Rosecrance, Gartzke (2007: 172) argues that development ‘leads states to prefer trade to theft’, but does not weaken their resolve to defend their borders. At the same time, developed states are typically militarily powerful and are able to wage wars over long distances. Since many wars are fought over non-territorial issues (e.g. to defend a particular political system in another state, or to prevent the development of nuclear capabilities), developed states are willing to fight long-distance wars where conquest is not the motivation. This leads Gartzke to expect that development leads contiguous dyads to be less likely to experience militarized interstate disputes and non-contiguous dyads to be more likely to do so. He finds support for both these hypotheses, and finds that the terms representing the democratic peace are non-significant when controlling for the ‘capitalist’ factors. Gartzke & Hewitt (2010) obtain similar results for international crises. The capitalist peace challenge to the democratic peace is taken up by Dafoe (2011) and Choi (2011), who show that the democratic peace retains support in the model of Gartzke (2007) with some specification changes that most analysts would agree are improvements to the original. The complete replication results presented in Choi (2011) show, however, that the substantial effect of the democratic peace is weaker when controlling for ‘capitalist’ factors than without, and Gartzke’s main hypotheses retain support in their replications. Any residual effects of democracy? The arguments reviewed here may imply that socioeconomic development is an important pre-condition for the democratic peace, in the context of both interstate and internal conflicts. It would be premature to conclude that development completely removes the importance of democratic institutions, however. First, if the economic underpinnings for democracy were sufficient for citizens’ welfare, we would not have seen the systematic trend of transitions toward democracy when states become economically more developed (Przeworski et al., 2000; Boix, 2003, 2011). Because of commitment problems, the ‘invisible hand’ of the market is insufficient to prevent conflict. Both elites and citizens see the need to design institutions that formalize access to decisionmaking power and also bind both sides to this formalization should the underlying balance of power change at some point in the future. One might also argue that development presupposes some kernels of democratization. For instance, the emergence of market norms crucially depends on the protection of property. Effective autocratic governments can protect property against ‘roving bandits’, but have a harder time assuring market actors that they will resist the temptation to confiscate the property of citizens. This, according to Olson (1993: 572), can only happen when rulers have very long time horizons, and long time horizons are credible only in democratic systems: ‘History provides not even a single example of a long and uninterrupted sequence of absolute rulers who continuously respected the property and contract-enforcement rights of their subjects.’ Indeed, Olson (1993: 574) claims that ‘Individual rights to property and contract enforcement were probably more secure in Britain after 1689 than anywhere else, and it was in Britain, not very long after the Glorious Revolution, that the Industrial Revolution began.’ If so, democracy is causally prior to development. At least, it is likely that democracy and economic modernization have developed in a dialectic process not unlike the Kantian learning process discussed in Cederman (2001). This process is probably related to a general shift in norms against the use of violence. Several of the long-range processes discussed in Gat (2006) and Pinker (2011) may be seen as informing explanations of democratization as much as explanations for the decline of war. Moreover, democracy and development may require each other to produce socially optimal outcomes. Mousseau (2000) and Mousseau, Hegre & Oneal (2003) find that the effect of democracy is contingent on development. Dafoe, Oneal & Russett (2013: 206) acknowledge that democracy and development might mutually reinforce each other: ‘Economic norms may express themselves more forcefully in liberal polities; moral concerns weigh more heavily when people are rich; the stability and bargaining credibility made possible by democracy . . . is more robust when governments are dependent on capital.’ Moreover, development in general strengthens and stabilizes democratic institutions (Przeworski et al., 2000; Gates et al., 2006),28 and developed democracies should therefore be better able to constrain leaders and affect their audience costs and incentives to avoid failed wars. In the case of domestic conflict,Hegre (2003),Collier& Rohner (2008), and Gleditsch, Hegre & Strand (2009) also find democracy to reduce the risk of internal conflict more effectively in high-income countries. This may be because the democratic strategies for maintaining order may be more costly than the autocratic strategies. Identifying and prosecuting individuals within groups that make use of illegal means of protest takesmore resources than indiscriminate repression of the entire group. To maintain a democratic civil peace, the government must be capable of not only actively affecting the societal distribution of resources but also preventing abuses of one social group by another. Most democracy datasets measure the extent to which governments are accountable and constrained, but rarely capture their capabilities to implement their decisions. Hegre & Nygård (forthcoming) indicate that such capabilities are just as important as the de jure institutions. Relatedly, political systems that combine democratic and autocratic features, for instance, may be regarded as having low capability because of their lack of consistency (Gates et al., 2006; Gleditsch & Ruggeri, 2010). Kalyvas & Balcells (2010), moreover, show that after the end of the Cold War, an increasing proportion of internal conflicts have been ‘symmetric non-conventional’ where both the government and the rebels lack the capacity to fight regular wars. This trend coincides with an increased number of low-income, low-capacity democracies, in particular in sub-Saharan Africa. Development also affects the policy incentives for democratically elected leaders. Illiterate populations are often unable to make use of the democratic institutions to constrain the elected leaders. Elected offices are extremely valuable to their incumbents in societies with immobile assets and extensive inequality (Boix, 2008), widespread corruption, and few alternative economic opportunities, inducing incumbents to concentrate on retaining power rather than serving the electorate. In sum, leaders in low-income democracies may be both less able and less willing to address social conflicts that underlie ‘relative-deprivation’ mechanisms. Development does not have the same effect in nondemocratic systems. Hegre (2003) indicates that violent conflict becomes more frequent in authoritarian states as they modernize. This is in conflict with the empirical implications of the ‘opportunity’ (Collier & Hoeffler, 2004) or ‘feasibility’ accounts of conflict (Collier, Hoeffler & Rohner, 2009). Development, to the extent it fosters ‘modern dynamic pluralist’ societies, may tend to shift the balance in favor of ‘justice-seeking’ rather than ‘loot-seeking’ motivations for internal conflicts, since the education, urbanization, and economic leverage associated with development raise the political expectations of citizens and help them resolve their collective action problems. It is clear that demands for democratization tend to intensify with higher education levels and the increased dispersion of economic leverage in modern economies. As exemplified by the recent conflicts in Libya and Syria, elites that resist these demands run a risk of escalating such conflict to civil war. Economic development may be a necessary condition for the democratic peace, but not a sufficient one. On the other hand, the autocratic means to maintain order do not become more effective with increasing development. First, widespread repression is more likely to meet widespread popular resentment the more educated the population is. With more human and social capital at hand, citizens are better able to force a repressive government to change its behavior. Eventually, the elites may be forced to open up the political system to allow the formation of democratic political systems. This transition process is often associated with civil conflict. Conclusions This review has discussed recent research on the relationship between democracy and armed conflict, covering both conflicts internal to countries and interstate conflicts. Although there are many differences between the interstate and domestic conflict, the review indicates there are also several similarities. In particular, some important challenges to the democratic peace apply to both types of conflict. The most fundamental challenge, in my view, is that there might be underlying social changes that explain both the development of democratic institutions and peaceful resolution of social conflicts. These changes are typically summarized as socio-economic development, and typically work through the incentives for using physical force for political goals. At the same time, as recently seen in Syria, relative economic development in itself is not sufficient to prevent armed conflict. Democratic institutions are formal codifications of nonviolent conflict resolution procedures. Socioeconomic development is likely to change societies such that nonviolent conflict resolution is an underlying pareto-optimal equilibrium, allowing actors to agree to such codifications. In the absence of formal codifications, however, actors may be unwilling to trust that this underlying equilibrium exists. Hence, democratic institutions may be necessary to allow the beneficial changes due to development to be manifested as more peaceful societies.

#### Empirical validity is sufficient justification for action—prior questions are reductionist views of IR and cause a vicious cycle

Owen, university of Southampton, 02 (David Owen, Reader of Political Theory at the Univ. of Southampton, Millennium Vol 31 No 3 2002 p. 655-7)

Commenting on the ‘philosophical turn’ in IR, Wæver remarks that ‘[a] frenzy for words like “epistemology” and “ontology” often signals this philosophical turn’, although he goes on to comment that these terms are often used loosely.4 However, loosely deployed or not, it is clear that debates concerning ontology and epistemology play a central role in the contemporary IR theory wars. In one respect, this is unsurprising since it is a characteristic feature of the social sciences that periods of disciplinary disorientation involve recourse to reflection on the philosophical commitments of different theoretical approaches, and there is no doubt that such reflection can play a valuable role in making explicit the commitments that characterise (and help individuate) diverse theoretical positions. Yet, such a philosophical turn is not without its dangers and I will briefly mention three before turning to consider a confusion that has, I will suggest, helped to promote the IR theory wars by motivating this philosophical turn. The first danger with the philosophical turn is that it has an inbuilt tendency to prioritise issues of ontology and epistemology over explanatory and/or interpretive power as if the latter two were merely a simple function of the former. But while the explanatory and/or interpretive power of a theoretical account is not wholly independent of its ontological and/or epistemological commitments (otherwise criticism of these features would not be a criticism that had any value), it is by no means clear that it is, in contrast, wholly dependent on these philosophical commitments. Thus, for example, one need not be sympathetic to rational choice theory to recognise that it can provide powerful accounts of certain kinds of problems, such as the tragedy of the commons in which dilemmas of collective action are foregrounded. It may, of course, be the case that the advocates of rational choice theory cannot give a good account of why this type of theory is powerful in accounting for this class of problems (i.e., how it is that the relevant actors come to exhibit features in these circumstances that approximate the assumptions of rational choice theory) and, if this is the case, it is a philosophical weakness—but this does not undermine the point that, for a certain class of problems, rational choice theory may provide the best account available to us. In other words, while the critical judgement of theoretical accounts in terms of their ontological and/or epistemological sophistication is one kind of critical judgement, it is not the only or even necessarily the most important kind. The second danger run by the philosophical turn is that because prioritisation of ontology and epistemology promotes theory-construction from philosophical first principles, it cultivates a theory-driven rather than problem-driven approach to IR. Paraphrasing Ian Shapiro, the point can be put like this: since it is the case that there is always a plurality of possible true descriptions of a given action, event or phenomenon, the challenge is to decide which is the most apt in terms of getting a perspicuous grip on the action, event or phenomenon in question given the purposes of the inquiry; yet, from this standpoint, ‘theory-driven work is part of a reductionist program’ in that it ‘dictates always opting for the description that calls for the explanation that flows from the preferred model or theory’.5 The justification offered for this strategy rests on the mistaken belief that it is necessary for social science because general explanations are required to characterise the classes of phenomena studied in similar terms. However, as Shapiro points out, this is to misunderstand the enterprise of science since ‘whether there are general explanations for classes of phenomena is a question for social-scientific inquiry, not to be prejudged before conducting that inquiry’.6 Moreover, this strategy easily slips into the promotion of the pursuit of generality over that of empirical validity. The third danger is that the preceding two combine to encourage the formation of a particular image of disciplinary debate in IR—what might be called (only slightly tongue in cheek) ‘the Highlander view’—namely, an image of warring theoretical approaches with each, despite occasional temporary tactical alliances, dedicated to the strategic achievement of sovereignty over the disciplinary field. It encourages this view because the turn to, and prioritisation of, ontology and epistemology stimulates the idea that there can only be one theoretical approach which gets things right, namely, the theoretical approach that gets its ontology and epistemology right. This image feeds back into IR exacerbating the first and second dangers, and so a potentially vicious circle arises.

#### Qualitative research is good—best way to support causal conclusions

Maxwell ’12 Joseph A. Maxwell, “The Importance of Qualitative Research for Causal Explanation in Education,” Qualitative Inquiry 2012 18: 655-661, Sage

In conclusion, I am making two claims. First, I am arguing that qualitative researchers can draw and support causal conclusions—that this is not an inappropriate aspiration. We are able to do this by focusing on the causal processes, mental as well as physical, that result in particular outcomes, rather than by simply demonstrating that a relationship exists between particular variables. Not all qualitative researchers aspire to draw such conclusions, and that is legitimate, but there are no good philosophical or methodological prohibitions against our doing this. I am not just arguing that we can do this, but that we’re good at it. We have the methods that allow us to both develop and test causal explanations in education. However, we could be better at it. Drawing causal conclusions is challenging even in the best of conditions, and attempting to generalize such conclusions is even more difficult. If we want to credibly make such claims to a wider audience, we need to be systematic and rigorous in providing evidence that supports these claims and that addresses potential validity threats to these claims; I provide elsewhere a detailed discussion of methods that qualitative researchers can use for this (Maxwell, 2004b, 2011a). However, in doing this, we also need to challenge the positivist assumptions that typically inform “evidence-based” approaches to research (Maxwell, 2009). Second, I am arguing that educational research, and social research generally, requires such qualitative approaches if it is to credibly identify the actual causes that influence a particular outcome, let alone to make claims about the broader efficacy of any intervention. Pawson (2006) argued, The nature of causality in social programmes is such that any synthesis of evidence on whether they work will need to investigate how they work. This requires unearthing information on mechanisms, contexts, and outcomes. The central quest is to understand the conditions of programme efficacy and this will involve the synthesis in investigating for whom, in what circumstances, and in what respects a family of programmes work. (p. 25) The idea that randomized experiments or structural equation models can provide valid general conclusions about the effect of an intervention, in the absence of any understanding of the actual causal processes that were operating, the specific contexts in which these processes were situated, or the meaning that the intervention and contexts had for participants, is an illusion. We need qualitative methods and approaches in order to understand “what works” and why.

#### Absolute causality may be impossible, but analyzing probability is key

Campbell and Currie, 6

Scott Campbell and Greg Currie, University of Nottingham, “Against Beck: In Defence of Risk Analysis,” Philosophy of the Social Science, June 2006

Beck’s next objection is that good science demands impossible standards for proving a causal link. According to Beck, the better the scientist, the more rigorous will be his insistence on strict proof for the claim that X caused Y, for example, that power lines cause leukemia. “The insistence on strict proof of causality is a central element of scientific rationality,” he says (1992, 63). But strict proof of causality is almost impossible to come by, which means that industry and government always end up denying that there is any risk. The stricter the proof required, then, the more risks and hazards industry is free to produce. As Beck says, by turning up the standard of scientific accuracy, the circle of recognized risks justifying action is minimized, and consequently, scientific license is implicitly granted for the multiplication of risks. To put it bluntly: insisting on the purity of the scientific analysis leads to the pollution and contamination of air, foodstuffs, water, soil, plants, animals and people. (1992, 62) This is simply not true, though. It is in fact granted by all writers on scientific method that strict proof in science is impossible, and most writers emphasize the role of probability. While a causal link between smoking and cancer has not been strictly proved, epidemiological studies have shown that there is a strong correlation between them, and that is good scientific reason—given that other possible causes have been tested for—to think that smoking causes cancer. This is not proof, but high probability. (Some cigarette companies still insist on strict proof, of course—but this is widely regarded by scientists as specious reasoning.) When a risk expert denies that computer monitors (i.e., VDTs) cause cancer, he isn’t doing this just on the basis that there is no strict proof of a causal link; he is doing it on the basis that there is little or no good supporting evidence, not enough even to tip the balance of probabilities toward the link. And legislation designed to help clean up the environment is almost always based on probability, not strict proof. Beck might reply that his argument will still go through on the basis of probability rather than proof, the point being that science will not judge anything to be a risk unless it can be shown to be very probable. But risk analysis will factor in low-probability events as well as high-probability events. For instance—as Beck himself complains—risk analysts often allo- cate a low probability to nuclear mishaps. And environmental legislation is often based on low-probability events—and rightfully so, according to many environmentalists. And because risk is a function of harm as well as probability, even a low-probability event can be risky if the harm is high enough.

### 1AC—Plan

#### The United States Congress should substantially increase restrictions on the offensive cyber operations war power authority of the President of the United States.

### Solvency

#### Congressional oversight solves without destroying flex—circumvention isn’t a reason to vote neg

Dycus, 10

(Stephen Dycus, Professor, Vermont Law School; internationally recognized authority on national security law and environmental law. He was founding chair of the National Security Law Section of the Association of American Law Schools. He is the lead author of "National Security Law" (the field's leading casebook) and "Counterterrorism Law", and he was founding co-editor in chief of the Journal of National Security Law & Policy. “Congress’s Role in Cyber Warfare” <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>) Henge

In his celebrated concurring opinion in The Steel Seizure Case, 1 Justice Jackson cautioned that “only Congress itself can prevent power from slipping through its fingers.”2 Jackson’s warning seems especially pertinent today, as we prepare urgently for cyber warfare – facing potentially enormous threats from yet unknown enemies, and finding ourselves dependent on staggeringly complex, unproven technology.3 The executive branch, which has special expertise and agility in national security matters generally, as well as substantial constitutional authority, has taken the initiative in these preparations.4 Yet if Congress is to be faithful to the Framers’ vision of its role in the nation’s defense, it must tighten its grip and play a significant part in the development of policies for war on a digital battlefield.5 It also must enact rules to help ensure that these policies are carried out. Congress must work hand in hand with the Executive, however, to confront these evolving threats. The importance of collaborative planning can be seen in a recent exchange of correspondence in which leaders of the Senate Select Committee on Intelligence wrote to the Director of National Intelligence to ask about “the adequacy of the Director of National Intelligence and Intelligence Community authorities over cybersecurity.”6 The Director answered: This is a very important issue . . . . A judgment regarding the adequacy of DNI authorities and any changes, additions, or clarifications will necessarily depend on the Administration’s strategic plan on cyber, and where the center of gravity will be within the Executive branch. . . . We have more work to do in the Executive Branch before I can give you a good answer.7 The strategic, technological, and political problems described here present challenges of unprecedented complexity. The risks of error both in the formulation of a cyber warfare policy and in its execution are substantial. And despite the importance of developing a coherent, coordinated response to this threat, it seems unlikely that we will find a way to overcome entirely the endless turf battles among federal agencies and congressional committees.8 Still, the need is so pressing and the stakes are so high that we cannot afford not to try. The very future of the Republic may depend on our ability not only to protect ourselves from enemies armed with cyber weapons, but also to use such weapons wisely ourselves. This article examines some of the relevant legal issues and suggests some possible solutions. I. CONGRESS’S ROLE IN DECIDING WHEN AND HOW TO GO TO WAR There is broad agreement that congressional authorization is needed to start a war.9 On the other hand, the President may act without Congress’s approval to repel an attack on the United States.10 Between these two extremes, the scope of the President’s unilateral authority to use military force is less well understood.11 Once hostilities are under way, there is a consensus that the President has the tactical powers of a Commander in Chief, although it may not always be clear which of the President’s actions are tactical and which are strategic.12 Before an attack can be launched, of course, Congress must have supplied the President with personnel and weapons.13 Moreover, Congress may regulate the President’s actions as Commander in Chief, except when the nation comes under sudden attack or the President exercises her tactical powers (and perhaps even then). In the Supreme Court’s 1800 decision in Bas v. Tingy, Justice Paterson, one of the Framers, echoed the other Justices in declaring that “[a]s far as congress authorized and tolerated the war on our part, so far may we proceed in hostile operations.”14 Four years later, in Little v. Barreme, the Court reiterated that the President must not exceed limits set forth in Congress’s authorization of hostilities.15 Since then, no court has ruled otherwise.16 In the intervening two centuries, Congress has adopted a number of measures to control the initiation or conduct of warfare. At the end of the Vietnam War, for example, Congress passed the War Powers Resolution (WPR),17 which requires the President to report to Congress within 48 hours the introduction of U.S. armed forces into hostilities or imminent hostilities, and to withdraw those forces within 60 days if Congress does not expressly approve of their continued deployment.18 Lambasted by some as an unconstitutional encroachment on presidential powers, the WPR has been followed (or at least lip service has been paid to it) by each President since the Nixon administration,19 and Congress has repeatedly referred to the WPR approvingly in subsequent legislation.20 If Congress now fails to enact guidelines for cyber warfare, it might be perceived as inviting “measures on independent presidential responsibility.”21 Chief Justice Marshall suggested in Little v. Barreme that if Congress had remained silent, the President might have been free to conduct the Quasi-War with France as he saw fit.22 But the national interest in electronic warfare, just as in that early maritime conflict, is so great that the planning and conduct of such a war should not be left entirely to the Executive. And because a cyber war might be fought under circumstances that make it impossible for Congress to play a meaningful contemporaneous role, Congress ought to get out in front of events now in order to be able to participate in the formulation of national policy. II. CONGRESS’S ROLE IN INTELLIGENCE AND COVERT ACTIONS The National Security Act of 194723 showed Congress’s determination to exert some control over this nation’s intelligence apparatus. That determination was strengthened after the disclosure of widespread intelligence abuses by the CIA and other agencies.24 In 1991, in response to the Iran-Contra Affair, Congress adopted a measure directing the President to keep the congressional intelligence committees “fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity.”25 The term “intelligence activity” expressly includes “covert actions,”26 which additionally require a written finding by the President that they are “necessary to support identifiable foreign policy objectives of the United States and [are] important to the national security of the United States.”27 Intelligence activities are also understood to include “all activities that elements of the Intelligence Community are authorized to conduct pursuant to [Executive Order No. 12,333],” the executive charter for such activities.28 The “intelligence community” includes the Office of the Director of National Intelligence, CIA, NSA, other Defense Department intelligence components, and other federal intelligence elements,29 which are authorized to engage in, inter alia, intelligence collection and analysis and “activities to protect against international terrorism . . . and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents.”30 This broad mandate certainly encompasses many U.S. efforts to defend against cyber attack and to employ cyber weapons offensively. By this definition, most preparations for and conduct of cyber warfare should be reported to the intelligence committees as “intelligence activities.” It is significant that the reporting requirement in the 1991 law is not limited to agencies within the intelligence community. Yet this legislation provides no guarantee that Congress will receive the information it needs to play a meaningful role in the development or execution of cyber warfare policy. It is not known, for example, precisely what it means for the intelligence committees to be “fully and currently” informed, what kinds of intelligence activities are regarded as “significant” enough to report, or who decides.31 Other sections of the 1991 law call on all agencies involved in intelligence activities, not just the President, to keep the intelligence committees informed about those activities, but only “[t]o the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters.”32 The “due regard for” language might be invoked to keep Congress in the dark. Under the 1991 law, “covert actions,” those with respect to which “it is intended that the role of the United States Government will not be apparent or acknowledged publicly,”33 need only be reported to a small group of legislators known as the “Gang of Eight,”34 and then only in a “timely fashion,” a term not defined by statute.35 Characterization of U.S. planning and execution of electronic warfare as “covert” could enable reporting to the smaller group, making it more difficult for Congress to play a significant role.36 Moreover, any reporting might be delayed indefinitely.37 Another potential obstacle to congressional involvement is the reportedly common but statutorily unauthorized practice of informal reporting to an even smaller “Gang of Four” – the leaders of the intelligence committees – generally for sensitive non-covert intelligence activities.38 The Defense Department is heavily engaged in preparations for cyber warfare, having recently announced the establishment of a new U.S. Cyber Command.39 But congressional oversight of the work of this command could be hampered by the military’s reported practice of labeling its clandestine activities – those that are intended to be secret, but that can be publicly acknowledged if discovered or inadvertently revealed – as “operational preparation of the environment,” rather than intelligence activities, even though they may pose the same diplomatic and national security risks.40 As thus characterized, these activities might not be reported to the intelligence committees.41 Any oversight that occurred would be conducted instead by the House and Senate Armed Services Committees.42 Such a division of responsibilities might create dangerous confusion. Congressional involvement also might be frustrated by the statutory exclusion of “traditional . . . military activities or routine support to such activities” from the definition of “covert action.”43 If secret military preparations for cyber war are regarded as “traditional military activities,” under the rationale outlined above they might escape both the presidential findings requirement for covert actions and any reporting to the intelligence committees.44 III. A LEGISLATIVE 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 ill-conceived 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. IV. OUTSOURCING CYBER WAR? Private companies furnish most of the computer hardware and software employed by the defense and intelligence communities. Many of the specific, tailored applications of such technology for national security purposes have also been developed by private companies under contract. All this makes perfect sense, given the high level of expertise in cyber technology outside the government. It echoes the well-established practice of buying uniforms and weapons from private suppliers. What may be surprising is that private companies have sometimes been employed to operate this technology – for example, in collecting and analyzing intelligence.51 These companies are guided by the terms of their contracts, including any provisions for ongoing government supervision, and by company policies. But contractor employees may feel divided loyalties because their first duty is to their employers’ shareholders. And because the delegation of responsibilities adds at least one link to the chain of command, the process of monitoring and disciplining such employees is necessarily more difficult than controlling government personnel.52 Not surprisingly, the terms of most of these contracts are classified, so public accountability is almost nonexistent. Private contractors are already engaged in work related to cyber warfare.53 It is not known publicly whether those contractors are making operational decisions or engaging directly in cyber warfare on behalf of the United States. But such actions would surely fall within the definition of “inherently governmental functions” – those that are “so intimately related to the public interest as to require performance by Federal Government employees,” including activities that “require . . . the exercise of discretion in applying Federal Government authority.”54 A Department of Defense instruction elaborates on the meaning of the term “inherently governmental functions” in the context of war fighting: The U.S. government has exclusive responsibility for discretionary decisions concerning the appropriate, measured use of combat power. . . . Because combat operations authorized by the U.S. government entail the exercise of sovereign government authority, involve substantial discretion, and can significantly affect the life, liberty, or property of private persons or international relations, they are IG [inherently governmental] . . . and cannot be legally contracted.55 Given the extraordinary risks associated with cyber weapons, Congress should not rely on executive agencies to decide which cyber warfare functions to outsource.56 It should expressly bar delegation to private contractors of authority for operation of cyber weapons, either offensive or defensive, and it ought to expressly prohibit any expenditure of appropriated funds for that purpose.57 V. A FIRM CONGRESSIONAL HANDSHAKE WITH THE EXECUTIVE Congress obviously cannot act alone to develop a cyber warfare policy for the United States. Its members and staff lack the technical expertise, agility, and organization to wield this new, evolving weaponry. On the other hand, Congress’s job in our constitutional system is to set national policy for the executive branch to execute. Especially in the matter of cyber warfare, where the diplomatic and strategic stakes are potentially as high as they are in any kinetic conflict, Congress has a critical role to play. It has perspective gained from long experience in foreign affairs and a host of related issues, and it may be more responsive to the popular will. The solution to this apparent conundrum may be found in a close collaboration between the political branches in the planning and implementation of rules for cyber warfare.58 Congress needs to act now to create authority and set boundaries within which the President may develop more refined protocols. This legislative development should be guided by advice from executive branch officials. The process must be cooperative rather than competitive. The resulting rules will necessarily be partly statutory, partly executive. The recent White House Cybersecurity Policy Review recommended that the “Administration should partner appropriately with Congress to ensure [that] adequate law, policies, and resources are available to support the U.S. cybersecurity-related missions.”59 Set out below are some steps that Congress might take to create an appropriate partnership. Some of these steps involve changes in congressional committees and responsibilities. Others would require coordination of cybersecurity functions within the executive branch. Still others would direct the President to keep Congress fully informed about anticipated and actual uses of cyber weapons. Several would restrict potential executive branch actions that seem – as a matter of policy – particularly unwise. 1. Designate a single committee in each House with primary responsibility for cyber warfare in order to develop a coherent and consistent legislative approach.60 2. Charge the designated committees with the development of broad policy and oversight of its implementation for both offensive and defensive uses of cyber weapons, given the close, perhaps indistinguishable, connection between the two uses. 3. Make the designated committees responsible for oversight of the relevant activities of the White House and every government agency concerned with cyber warfare, including the Defense Department, and their contractors, whether overt, clandestine, or covert. 4. Designate a lead federal agency to coordinate ongoing planning among agencies.61 The congressional committees would then have a principal point of contact for the collaborative development of policy. 5. Designate a lead agency to execute the cybersecurity plan.62 6. Order the preparation of a National Cybersecurity Strategy at prescribed intervals.63 This document should be declassified to the greatest extent possible, in order to inform every member of Congress and the public about the basic elements of U.S. cyber policy. 7. Require frequent, periodic briefings of the congressional committees, to enable serious consultation and advice in both directions as cyber policy evolves over time. These briefings should include information about rules of engagement, procedures for deciding to use cyber weapons, and any delegations of authority for such use. 8. Require consultation with the designated congressional committees in every possible instance before any significant use of cyber weapons.64 9. Require a written finding by the President, in advance of any significant use of cyber weapons whenever reasonably possible, or within a day or two afterward, that such use is or was necessary to the national security of the United States, that such use is or was as limited in scope as possible and consistent with the laws of armed conflict, and that Congress was consulted or could not be consulted because of the urgency of the threat. 10. Require immediate reports to the designated committees of any significant use of cyber weapons, either offensive or defensive. 11. Expressly forbid any withholding of information from the committees based on classification or for other reasons of secrecy. 12. Direct that all required reports be delivered to the designated committees as a whole, not merely to selected members.65 13. Expressly forbid automated offensive responses to actual or threatened cyber attacks on the United States under any circumstances. Given the potential for misperception or misinterpretation of an enemy attack, the difficulty of identifying the attacker and of assessing any resulting damage, and the risk of inadvertent escalation, any such response should be directed by a sentient human hand, informed by as much consultation with various government officials as the circumstances will permit.66 14. Create a government structure to coordinate assistance to private entities that come under cyber attack, so that such entities do not take matters into their own hands.67 15. Review and appropriately amend existing legislation designed to protect privacy within the United States.68 Needed amendments might require technical fixes, such as review of email traffic in anonymized form, or appointment of privacy officers in agencies responsible for implementation of cyber policy.69 16. Require the public disclosure of U.S. cyber warfare policy to the greatest extent possible, in order to inform those in government who are not directly involved in its development, to promote public debate, and to let potential enemies know that the United States has a viable policy in place.70 17. Prohibit the outsourcing of responsibility for operating cyber weapons systems either defensively or offensively. Because of the grave potential consequences and the attendant need for close control and accountability, such operations should be undertaken only by government officials. These recommendations are, of course, riddled with terms that require careful definition. They also omit many critical details. Specific provisions relating to timing of notices and the requirement of consultation, for example, must be worked out between the political branches. Congress’s active role in the development and implementation of cyber warfare policy is no guarantee of national security. The policy might be flawed in various ways. There is also a risk that whatever policy is adopted will not be properly executed or that its execution will have unintended results. The policy might be misunderstood or might not provide clear or appropriate guidance in the urgent circumstances facing its interpreter. The person charged with implementing the policy might make a mistake – for example, by interpreting a potential enemy’s electronic espionage as an attack. Available cyber weaponry might not work as planned. Or a purely defensive move by U.S. operators might be construed by another nation as offensive, and provoke an attack. Nor can the clearest policy, statutory or executive, guarantee compliance by an Executive determined to ignore it.71 The rules might be construed by the President in a way that reduces the importance of Congress’s role. Or they might be challenged in court. Congress should not, however, hesitate to take the steps outlined here merely because they might produce unintended results or because they could be difficult to enforce. Exactly the same criticisms could be leveled at almost any reorganization or legislative initiative. The high stakes in this instance, and Congress’s constitutional responsibility for formulation of national security policy, mean that Congress cannot sit this one out. It might be suggested that these proposed measures would dangerously tie the President’s hands, thereby limiting her freedom to respond to unpredictable future national security threats. The very point of the recommendations, however, is that Congress should place limits on the President’s actions – to require her to share the responsibility for deciding to go to war. Even then, if the nation comes under sudden cyber or kinetic attack the President will remain free to respond as she sees fit. The United States faces unprecedented challenges from enemies equipped with new weaponry possessing vast, evolving destructive potential. The two political branches must draw on their respective expertise and experiences to work together to meet these challenges, as the Framers intended.

#### US OCO policy creates norms—it’s reverse causal

Bradbury, 11

(Steven G. Bradbury is an attorney at the Washington, D.C office of Dechert LLP. Bradbury was head of the Office of Legal Counsel (OLC) in the United States Department of Justice during the George W. Bush administration. “The Developing Legal Framework for Defensive and Offensive Cyber Operations” <http://harvardnsj.org/wp-content/uploads/2011/04/Vol.-2_Bradbury_Final.pdf>) Henge

Conclusion. So here’s my thesis: To my view, the lack of clarity on certain of these issues under international law means that with respect to those issues, the President is free to decide, as a policy matter, where and how the lines should be drawn on the limits of traditional military power in the sphere of cyberspace. For example, that means that within certain parameters, the President could decide when and to what extent military cyber operations may target computers located outside areas of hot fighting that the enemy is using for military advantage. And when a cyber attack is directed at us, the President can decide, as a matter of national policy, whether and when to treat it as an act of war. The corollary to all this is that in situations where the customs of war, in fact, are not crystallized, the lawyers at the State Department and the Justice Department shouldn’t make up new red lines — out of some aspirational sense of what they think international law ought to be — that end up putting dangerous limitations on the options available to the United States. Certainly, the advice of lawyers is always important, especially so where the legal lines are established or firmly suggested. No one would contend that the laws of war have no application to cyber operations or that cyberspace is a law-free zone. But it’s not the role of the lawyers to make up new lines that don’t yet exist in a way that preempts the development of policy.14 In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention on cyberwarfare — perhaps a kind of arms control agreement for cyber weapons. I believe there is no foreseeable prospect that that will happen. Instead, the outlines of accepted norms and limitations in this area will develop through the practice of leading nations. And the policy decisions made by the United States in response to particular events will have great influence in shaping those international norms. I think that’s the way we should want it to work.

#### The plan best captures the middle ground between absolute transparency and secrecy—perception controls the reality of the international system

Wallace, 13

(Ian Wallace, visiting fellow in the Center on 21st Century Security and Intelligence at Brookings. Wallace previously served as a senior official at the British Ministry of Defence, where he helped develop the UK government’s cyber strategy as well as Britain’s cyber relationship with the United States. “Militarizing the Internet?” <http://nationalinterest.org/commentary/militarizing-the-internet-8734?page=show>) Henge

Balancing Cyber Reward and Internet Risk Policymakers must not only ask whether a national-security cyber operation is legal, but also whether it is wise. And that probably means involving new stakeholders. Decisions that make perfect sense in the context of national security or counterterrorism may look less sensible when judged in the context of the possibility of repercussions for global trade or, say, the ability to establish norms on the cyber theft of intellectual property. This does not mean that we should abandon the use of cyberpower to support national-security goals. To do so would be to cede unnecessarily a U.S. advantage to the nation’s adversaries. But it may raise the bar. Done right, cyber capabilities have the undoubted potential to save lives. For example, when considering the thinking behind Stuxnet, it is hard to object to a plan in which no one was killed and which may have played a part in slowing down Iranian progress toward a nuclear capability (averting the possibility of U.S. or Israeli attacks and a messy war in the Middle East). But there are downsides, too, and the right people need to be in the room so that the balance of risk and reward is properly understood. The president does not need to act on all the advice he is given, but his decisions should be fully informed. Getting the Messaging Right This is not straightforward: unlike the U.S. Navy in General Dempsey’s example, the purpose and organization of DOD’s cyber power is deliberately shrouded in secrecy. There are good reasons for this confidentiality: it is easier to attack than defend in cyberspace, and there is an advantage in having advance knowledge of your adversaries’ systems. This makes it hard to explain openly what the U.S. military and intelligence community do in cyberspace. At the same time, however, the public and media are becoming increasingly aware of the importance of the global internet in their daily lives. One consequence of a requirement for high levels of operational security and keen public interest is a ready environment for leaks. In other words, these will not be the last “cyber” leaks. And if recent events prove anything, it is that leakers come in all shapes and sizes. The challenge going forward will be to find an appropriate response. Not commenting may be the least bad response to the Stuxnet claims, but anything that makes the Iranians look like the innocent victims of U.S. bullying is hardly without drawbacks. Meanwhile, focusing on the legality of internet surveillance as long as it is directed at “non-U.S. persons” does nothing to enhance the country’s reputation abroad. The global context has changed, and somehow the messaging has to catch up. None of this is meant to condone the practice of leaking. Secrets are essential to good government, especially national security. But the government must be careful to apply an accurate assessment of the risk of disclosure to its national-security decision making and, should the need arise, be prepared to justify its actions internationally and domestically. Sometimes it is useful to create doubt in the minds of adversaries about your true capabilities, but the secrecy surrounding cyber weapons can also create instability and competition. Perception quickly becomes the reality that matters internationally. Managing this new environment will require levels of self-awareness and cross-agency work that will be novel and challenging. But nothing less will do if the United States wants to avoid being out-maneuvered in the geopolitics of the internet age.

## 2AC

### 2AC—XO

#### No predictable lit on self-restraint in the context of war powers—irrelevant if it’s real world, scholarship still assumes external checks

Sales, 12

(Nathan Sales, Assistant Professor of Law, George Mason University School of Law. “Self-Restraint and National Security “ <http://jnslp.com/wp-content/uploads/2012/08/08__Sales_Master_6-28-12-NS.pdf>) Henge

Much of the caselaw and scholarship concerning national security rests on the assumption that the executive branch is institutionally prone to overreach – that, left to its own devices, it will inch ever closer to the line that separates illegal from legal, and sometimes enthusiastically leap across it. The obvious conclusion is that external, principally judicial, checks are needed to keep the Executive in line.2 In many cases the Executive does indeed push the envelope. But not always.3 The government often has powerful incentives to stay its own hand – to forbear from military and intelligence operations that it believes are perfectly legal. Officials may conclude that a proposed mission – a decapitation strike on al Qaeda’s leadership, say, or the use of mildly coercive interrogation techniques on a captured terrorist – is entirely permissible under domestic and international law. Yet they nevertheless might rule it out. In other words, the government sometimes adopts self-restraints that limit its ability to conduct

#### Permutation do both—XOs that support legislation are best—CP alone links to politics and wrecks legitimacy—also causes inter-branch tension

Belco and Rottinghaus, 13

(Brandon Rottinghaus, Senator Don Henderson Scholar, University of Houston, Department of Political Science. Michelle Belco, University of Houston, Department of Political Science. “In Lieu of Legislation: Executive Unilateral Preemption or Support during the Legislative Process” Sage) Henge

In exercising their executive power within the legislative arena, presidents generally pursue a “legislative presidency” (Wayne 1978). From the president’s perspective, this is a tenuous choice because the process of passing legislation is afflicted by collective action problems, an outlay of political capital, lengthy debates, and large transaction costs but provides certainty in achieving a lasting policy outcome (Moe and Howell 1999, 146). In an effort to improve their chances for success, a president may choose to enter the legislative arena using several means sanctioned by the Constitution or the strategic use of executive power: suggest an agenda item to Congress as outlined by Article II, Section 1 of the Constitution issue an executive statement of administrative procedure (Rice 2012); and issue a veto threat in advance of a veto (Deen and Arnold 2002) and the use of the veto (Cameron 2000, 28). Each of these tools provides the executive with some strategic participation in the legislative process. Beyond the conventionally proscribed techniques for the president’s legislative functions, presidents may also use direct or unilateral action as a means of improving their success in implementing their policy agenda outside the legislative arena (Cooper 2002; Mayer 2001; Warber 2006). Direct action is strategically useful for presidents when faced with a legislative arena that forces them to share political powers (Howell 2003, 2005; Mayer 2001; Moe and Howell 1999). The process of issuing unilateral orders is generally described as an alternative to pursuing legislation by bargaining with Congress (Howell 2003; Moe and Howell 1999). This approach enables the executive to “act quickly and with flexibility in responding to problems and changing political, economic and social circumstances as they arise” (Moe and Howell 1999, 138). This unilateral approach, however, is not always independent of the legislative process. As Jones (2005, 253) argues, Efforts to comprehend presidential power in lawmaking require study of congressional power even if the president acts “with the stroke of a pen” as when issuing executive orders. Those who are separated must agree or acquiesce if there is to be law. Neustadt ([1960] 1990, x) suggests that presidents are “dependent on consent from other sharers” in government, especially Congress, because “he must bargain with them, buttressing his share with his resources in their eyes of personal reputation and of public standing.” If unilateral orders can be used as a bargaining tool in the legislative process, when presidents issue a unilateral order during the legislative process, under what conditions does that order preempt or support proposed legislation? Using an original data set of unilateral orders (executive orders and proclamations) from Presidents Ford through George W. Bush (93rd to 110th Congresses), we analyze when and how presidents unilaterally preempt or support proposed legislation. Although the literature suggests that presidential strategies of bargaining or using unilateral actions are opposed to one another, our approach unites Neustadt’s “power stakes” (how presidential resources influence bargaining) with theories of direct presidential action. We argue that the president will act using a unilateral order during the legislative process to preserve a policy trajectory in Congress favorable to the executive or to shift policy closer to his ideal point. Our theory suggests flexibility in a president’s use of unilateral orders in the legislative arena: sometimes to halt the legislative process, sometimes to foster it, depending on the institutional context. We argue that unilateral orders are used while negotiating in the legislative process. This notion expands the conceptual study of the executive’s use of unilateral power to the legislative arena, a linkage yet unexplored. In doing so, we seek to develop a better understanding of shared rather than separate powers in the context of executive–legislative relations where unilateral orders can be used to augment the legislative process. Presidents and Unilateral Action in the Legislative Arena When considering whether to issue a unilateral order, presidents face an integrated cost–benefit trade-off, especially with respect to the legislative makeup of Congress and the possible intervention of the judiciary (Moe and Howell 1999). The executive must weigh the costs and benefits of legislation against the costs and benefits of unilateral action. Deering and Maltzman (1999, 770) argue that “a president’s willingness to issue an executive order depends upon both his positive power to get legislation enacted by Congress and his negative power to stop legislation overturning such an order.” Invoking unilateral powers to circumvent legislation specifically involves weighing the cost of angering a recalcitrant Congress with the benefits of acting with dispatch. As Mayer (2009, 439) suggests, presidents prefer legislation as a means to achieve policy goals but may opt for unilateral action as their “second-best” option when they face strong Congressional opposition. Such a complicated decision is not strictly combative nor is it totally cooperative— there is variation depending on the president’s authority to act, the political environment and the institutional arrangements. Presidents may use unilateral orders to set the political agenda of the nation without input from members of Congress (Fine and Warber 2012); however, this runs the risk of circumventing the negotiating process with members of Congress with whom the president must later bargain. Neustadt ([1960] 1990) warns directly of this problem when he counsels that presidents should prefer to bargain with Congress (see Mayer 2009, 428). Yet, a president’s short-term interest in pursuing successful policy outcomes may outweigh his desire to work with Congress on a mutually agreeable political outcome (Krause and Melusky 2012), especially if Congress and the president are at loggerheads over legislation. Presidents may disagree with the ideological or political direction of legislation and issue a preemptive order as an alternative to Congressional action. This too runs the risk of angering Congress who may choose to respond with additional legislation (Howell 2003) or otherwise revoke the order by statute. However, invoking a unilateral order during the legislative process may be a way of gaining participation of members by addressing topics already on the Congressional agenda. Consultation with Congress is especially likely when the president’s objective is to change the agreed-upon status quo (Moe and Howell 1999) by issuing an order supporting proposed legislation. Therefore, presidents, in their desire to work with Congress, may issue a unilateral order to achieve a mutually agreeable policy solution. There is less cost here to the president with respect to angering Congress as the president is “fast tracking” the proposed Congressional legislation into policy, especially if the president is executing the will of Congress through prearranged policy (Fisher 2007, 109; Warber 2006).

#### XOs are illegitimately perceived—can’t solve if Congress doesn’t approve actions—can’t solve long-term—every president gets XOs revoked

Powell, 14

(Jim Powell is Senior Fellow at the Cato Institute, with which he has been associated since 1988. He has also done work for the Manhattan Institute, the Institute for Humane Studies, Citizens for a Sound Economy, the National Right to Work Committee and Americans for Free Choice in Medicine. Powell is an author on the history of liberty. “How President Obama Could be Swept Away with His Executive Orders That Defy Congress and the Courts” <http://www.cato.org/publications/commentary/how-president-obama-could-be-swept-away-executive-orders-defy-congress>) Henge

Apparently President Obama has become convinced that he can make magic with that pen he keeps talking about, the one he plans to use for signing executive orders to revive his beleaguered presidency. Executive orders are irresistible, because a president doesn’t have to propose anything, debate the issues, endure hearings or solicit votes. An executive order can be issued in a few minutes — behind closed doors and away from bright lights. Paul Begala, who was an advisor to President Bill Clinton, reportedly remarked, “Stroke of the pen, law of the land, kinda cool.” What about the Constitution? It describes presidential power broadly. There isn’t anything in the Constitution that authorizes an executive order or limits what a president can do with it. Executive orders arise from “implied constitutional and statutory authority,” the Congressional Research Service reported. “If issued under a valid claim of authority and published in the Federal Register, executive orders may have the force and effect of law.” Many executive orders are in a twilight zone of dubious constitutional legitimacy if not open defiance of the Constitution, especially when they amount to lawmaking without congressional approval. Presidents have made extravagant claims with their executive orders, as Harry Truman did when he issued executive order 10340 that directed the Secretary of Commerce to stop a steelworkers strike by seizing privately-owned steel mills. Truman insisted that a prolonged strike would impair the government’s ability to fight his undeclared “police action” in Korea. Truman’s Solicitor General Philip B. Perlman declared that Article II, Section 2 of the Constitution “constitutes a grant of all the executive powers of which the Government is capable.” The case came before the Supreme Court as Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952). Justice Robert Jackson — like Truman, a Democrat — was incredulous at the administration’s position. He said, “The example of such unlimited executive power that must have most impressed the forefathers was the prerogative exercised by King George III. The description of its evils in the Declaration of Independence leads me to doubt that they were creating their new Executive in his image. Continental European examples were no more appealing. And, if we seek instruction from our own times, we can match it only from the executive powers in those governments we disparagingly describe as totalitarian. I cannot accept the view that the clause is a grant in bulk of all conceivable executive power.” Justice Hugo Black, another Democrat, wrote the majority opinion invalidating the seizures. Black explained that an executive order (1) “must stem either from an act of Congress or from the Constitution itself” and (2) an executive order is on dubious ground if it’s “incompatible with the express or implied will of Congress.” There have been thousands of executive orders, so it’s hard for government to keep track of them all, and it’s even harder for ordinary citizens. In 1974, the Senate Committee on National Emergencies and Delegated Emergency Powers was surprised to discover that “Since March 9, 1933, the United States has been in a state of declared national emergency. There are now in effect four presidentially-proclaimed states of national emergency. In addition to the national emergency declared by President Roosevelt [during the Great Depression], there are also the national emergency proclaimed by President Truman on December 16, 1950, during the Korean conflict, and the states of national emergency declared by President Nixon on March 23, 1970 and August 15, 1971.” The committee report continued, “These proclamations give force to 470 provisions of Federal law, delegating to the President extraordinary powers, ordinarily exercised by the Congress, which affect the lives of American citizens in a host of all-encompassing manners…The President may seize property, organize and control the means of production, seize commodities, assign military forces abroad, institute martial law, seize and control all transportation and communication, regulate the operation of private enterprise, restrict travel, and in a plethora of particular ways, control the lives of all Americans.” President Obama’s admirers like to talk about the wonderful things can be done with executive orders, but the historical record has been mixed. Some have been fine, while many have backfired badly. Executive orders go back to the beginning of our country, although they weren’t called that. Usually they were referred to as proclamations. President George Washington’s first proclamation was on October 3, 1789. He said, “Both Houses of Congress have by their joint Committee requested me to recommend to the People of the United States a day of public thanksgiving.” This was authorized by Congress. Washington’s Neutrality Proclamation wasn’t authorized by Congress. Issued on April 22, 1793, it declared that the United States would be neutral in the war between France and Great Britain, which had begun two months before. Members of Washington’s cabinet, including Secretary of State Thomas Jefferson, agreed that the United States was too fragile to become involved in another war. So far, so good. “ While executive orders are attractive to presidents because they can be issued quickly, they can be revoked quickly, too.” Abraham Lincoln expanded presidential powers via proclamations and executive orders. He did this in the name of suppressing rebellion rather than waging war, since the Constitution gave Congress the power to declare war. In April 1861, a Maryland militia officer named John Merryman was arrested and detained at Fort McHenry in Baltimore. He was said to have damaged Union facilities and trained Confederate soldiers. His lawyer obtained a writ of habeas corpus from Chief Justice Roger B. Tawney who directed George Cadwalader, the commander at Fort McHenry, to produce Merryman and explain the facts and the legal basis for detention. Cadwalader refused, saying that Lincoln had suspended habeas corpus. Tawney cited him for contempt, but a marshal couldn’t enter the fort to deliver the contempt citation. Tawney wrote what became known as the Ex Parte Merryman opinion, saying, in part, that “If the authority which the Constitution has confided to the judiciary department may upon any pretext be usurped by the military power, the people of the United States are no longer living under a government of laws.” On September 24, 1862, Lincoln issued a proclamation officially suspending habeas corpus, which meant that the government could detain people indefinitely. Lincoln “managed the home front, in part,”historian Mark E. Neely, Jr. reported, “by means of military arrests of civilians — thousands and thousands of them.” Lincoln had issued executive orders expanding the amount of Union territory subject to military control, particularly southern Illinois, Indiana and Ohio where “copperheads” were operating. In 1864, the Union army arrested Lambdin Milligan and four others in southern Indiana. They were charged with plotting to free Confederate prisoners-of-war. A military court sentenced the men to death, but they appealed for their constitutional right to habeas corpus. After the Civil War, in 1866, the Supreme Court noted that Indiana wasn’t under attack, and civilian courts were functioning, so Milligan and the others were entitled to a jury trial there. Justice David Davis wrote: “The Constitution of the United States is a law for rulers and people, equally in war and in peace, and covers with the shield of protection all classes of men, at all times, in all circumstances.” Historian James G. Randall reflected, “No president has carried the power of presidential edict and executive order — independently of Congress — so far as [Lincoln] did. It would not be easy to state what Lincoln conceived to be the limit of his powers.” Lincoln’s best-known executive order was the Emancipation Proclamation. He hoped to provoke a slave revolt in the Confederacy and make it easier for the Union to win the Civil War. Accordingly, on September 22, 1862, he issued a preliminary Emancipation Proclamation. It applied to any state that didn’t return to the Union by January 1, 1863. No states returned. At that point, Lincoln issued the historic Emancipation Proclamation. It applied to slaves in the Confederacy — territory that the Union didn’t control. It neither abolished slavery nor extended citizenship to former slaves, but it did make the abolition of slavery a war aim. Until the early 20th century, executive orders were generally undocumented. They were addressed to a particular government agency which had the only copy. Nobody seemed to know how many executive orders there were. As late as the 1930s, there was an account, published in the New York Times, claiming that “there are no readily available means of ascertaining the true texts and history of the thousand or more executive orders issued since March 4, 1933.” The peacetime expansion of federal power began with Theodore Roosevelt who issued 1,006 executive orders, more than any previous president. They performed a wide range of administrative functions, especially the disposition of government-owned land. TR emphatically rejected the view that “what was necessary for the nation could not be done by the President unless he could find some specific authorization to do it…it was not only [the president’s] right but his duty to do anything that the needs of the nation demanded unless such action was forbidden by the Constitution or by the laws.” TR also said: “I think [the presidency] should be a very powerful office, and I think the President should be a very strong man who uses without hesitation every power the position yields.” He continued, “I believe in a strong executive. I believe in power.” According to biographer Henry Pringle, “It seldom occurred to Roosevelt that the duty of the executive was to carry out the mandates of the legislative. In so far as he was able, he reversed the theory. Congress, he felt, must obey the president.” He wanted the Supreme Court to obey him, too. Roosevelt acknowledged, “I did greatly broaden the use of executive power.” At times, TR seemed drunk with power, as when he remarked: “I don’t think that any harm comes from the concentration of power in one man’s hands.” Woodrow Wilson issued 1,791 executive orders. For instance, executive order 1810 (August 7, 1913) prohibited anyone from operating a flying machine or balloon across the Panama Canal Zone. Wilson issued executive order 1860 (November 11, 1913) to dictate interest rates for the Canal Zone — a surprising number of Wilson’s executive orders had to do with administering that little territory. Most of Wilson’s executive orders were issued during World War I. For instance, on April 14, 1917, he issued executive order 2594 to establish the Committee on Public Information — war propaganda. On April 28th, he issued executive order 2604 for censorship of messages sent via the trans-Atlantic cables. Executive order 2679-A (August 10, 1917) established the Food Administration. Executive order 2697 (September 7, 1917) required that anyone wishing to export coins, bullion or currency must file an application in triplicate with the nearest Federal Reserve bank. Executive order 2736 (October 23, 1917) authorized Food Administrator Herbert Hoover to requisition food. Executive order 2953 (September 12, 1918) authorized the sale of property seized in accordance with the Trading with the Enemy Act. Franklin D. Roosevelt issued 3,723 executive orders, more than any other U.S. president. In his Inaugural Address, he said: “I shall ask the Congress for the one remaining instrument to meet the [depression] crisis — broad executive power to wage a war against the emergency, as great as the power that would be given me if we were in fact invaded by a foreign foe.” On March 6, 1933, FDR issued Proclamation 2029 that cited Wilson’s Trading with the Enemy Act to justify ordering banks closed for a National Bank Holiday. FDR sent his Emergency Banking bill to the House of Representatives, and it was passed after only 38 minutes of debate — apparently without members reading it. In 1933, FDR issued executive order 6102 that made it illegal for Americans to own gold bullion or gold certificates, even though historically gold provided the best protection against inflation and monetary crises. Violators faced the prospect of a fine up to $10,000 or up to 10 years in prison. Since economic fascism was popular during the early 1930s, FDR issued executive orders to suspend antitrust laws and establish German-style cartels in dozens of industries, restricting total industry output, allocating market shares and fixing above-market wages and prices. Above-market wages discouraged employers from hiring, and above-market prices discouraged consumers from buying, so these executive orders weren’t good for the country. Among them: \* 6204-A, for the rayon weaving industry \* 6205-C, for the silk manufacturing industry \* 6216, for the ship building and ship repairing industries \* 6242-B, for electrical manufacturing \* 6248, for the corset and brassiere industries \* 6250, for theaters \* 6253, for the fishing tackle industry \* 6254, for the iron and steel industries \* 6255, for the forest products industry \* 6256, for the petroleum industry \* 6543-A, for the drapery and upholstery industries With executive orders, FDR multiplied the number of government bureaucracies. He established the Civilian Conservation Corps by issuing executive order 6101. The Public Works Administration followed with executive order 6174. Then came these executive orders: \* 6225, the Central Statistical Board \* 6340, the Commodity Credit Corporation \* 6420-B, the Civil Works Administration \* 6433-A, the National Emergency Council \* 6470, the Public Works Emergency Housing Corporation \* 6474, the Federal Alcohol Control Administration \* 6514, the Electric Home and Farm Authority \* 6581, the Export-Import Bank of Washington \* 6623, the Federal Employment Stabilization Office \* 6632, the National Recovery Review Board \* 6770, the Industrial Emergency Committee \* 6777, the National Resources Board \* 7027, the Resettlement Administration \* 7034, the Works Progress Administration While some of the programs provided relief for desperate people, they failed to achieve a sustained revival of private sector job creation. Indeed, relief spending was the main reason government spending doubled and taxes tripled during the New Deal era (1933-1940). Where did the tax revenue come from? The biggest source of federal revenue was the federal excise tax on cigarettes, beer, soda, chewing gum and other cheap pleasures consumed disproportionately by poor and middle income people. This means the cost of relief programs for poor and middle income people was borne mainly by poor and middle income people. In May 1939, FDR’s Secretary of the Treasury Henry Morgenthau lamented, “We are spending more than we have ever spent before, and it does not work. After eight years of this administration, we have just as much unemployment as when he started.” New Deal unemployment averaged 17 percent, and it didn’t go down significantly until the government began removing more than 10 million men from the civilian work force via military conscription for World War II. FDR’s most controversial executive order was 9066 which he issued on February 19, 1942. It established the War Relocation Authority to forcibly move Japanese-Americans away from the Pacific Coast into “relocation camps” for the duration of World War II. About 70 percent of these people were second-generation, born in the United States. Three individuals, Fred Korematsu, Gordon Hirabayashi and Minoru Yasui, were convicted of refusing to comply with internment. The case went up to the Supreme Court which upheld FDR’s executive order in Korematsu v. United States, 323 U.S. 214 (1944). The majority opinion asserted that protecting against potential Japanese espionage was more important than protecting individual rights. Six of FDR’s 8 appointees sided with him against the interned Japanese. The lone Republican appointee, Owen Roberts, was opposed. FDR’s Solicitor General Charles Fahey, who argued the case before the Supreme Court, allegedly suppressed reports by the FBI and the Office of Naval Intelligence, showing that there wasn’t any evidence Japanese-Americans posed a security threat to the United States. The suppressed reports came to light years later, and the convictions were overturned November 10, 1983 by the U.S. District Court for the Northern District of California, thereby eliminating the case as a possible precedent for future arbitrary imprisonment. President Nixon issued two executive orders that had unfortunate consequences. On August 15, 1971, he announced his New Economic Policy, which happened to be what Bolshevik firebrand Vladimir Lenin called one of his misadventures. Nixon issued executive order 11615 that declared: “to stabilize the economy, reduce inflation, and minimize unemployment, it is necessary to stabilize prices, rents, wages, and salaries.” These controls failed to stop inflation which hit double-digits during the 1970s, and they caused chronic shortages, rationing and business disruption — making it harder to create private sector jobs. By maintaining below-market prices, controls simultaneously encouraged producers to provide less, while encouraging consumers to demand more. Hence, the shortages. Although this experience with price controls had been a flop, Nixon decided to try again. On June 13, 1973, he signed executive order 11723 that called for a freeze on prices, while he continued to control wages, salaries and rents. Nixon’s executive orders made a bad situation worse. For instance, his price control administrator C. Jackson Grayson confessed: “lumber controls were beginning to lead to artificial middlemen, black markets and sawmill shutdowns. Companies trapped with low base-period profit margins were beginning to consider selling out those with higher base periods, sending their capital overseas, or reducing their efforts. Instances of false job upgrading — which were actually ‘raises’ in disguise — were reported. To keep away from profit-margin controls, companies were considering dropping products where costs, and thus prices, had increased. And shortages of certain products (like molasses and fertilizer) were appearing because artificially suppressed domestic prices had allowed higher world prices to pull domestic supplies abroad.” In 1999, Bill Clinton waged war with executive orders. He issued executive order 13088 that declared the governments of the Federal Republic of Yugoslavia (Serbia and Montenegro) and the Republic of Serbia posed “an extraordinary threat to the national security and foreign policy of the United States.” Therefore, Clinton proclaimed a “national emergency.” He ordered the seizure of property belonging to the named governments in the United States, and he prohibited Americans from conducting commercial transactions with those governments. Clinton’s executive order 13119 declared that the region was a war zone. Executive order 13120 summoned military reserve units for active duty. None of this was authorized by Congress. On the contrary, Congress voted down a resolution to declare war. Congress wouldn’t “authorize” the air war. Clinton ignored Congress and kept America in the war. When, on June 10, 1999, NATO announced it was over, Clinton ordered American soldiers to serve in the Kosovo Force. Not long after that, we found ourselves in an open-ended national emergency declared on September 14, 2001 and extended since by both George W. Bush and Barack Obama. This means the president has standby powers from hundreds of statutes that would enable him to re-introduce military conscription, seize private property and in myriad ways establish a government-run economy. How could an executive order be revoked? First, an executive order can be revoked by another executive order. Probably all presidents revoke some executive orders by their predecessors. For example, Bill Clinton’s executive order 12919, issued on June 3, 1994, was about national security. It revoked all or part of more than a dozen executive orders issued between 1939 and 1991. President Obama revoked executive orders 13258 (2002) and 13422 (2007), both of which were issued by George W. Bush, and Obama amended executive order 12866 (1993) which had been issued by Bill Clinton. These executive orders had to do with regulatory processes. So, while executive orders are attractive to presidents because they can be issued quickly, they can be revoked quickly, too. Second, an executive order can be revoked by legislation. Reportedly every president since Grover Cleveland has had some of his executive orders modified or revoked by legislation. The Congressional Research Service cited a number of examples: “in 2006, Congress revoked part of an executive order from November 12, 1838, which reserved certain public land for lighthouse purposes. Congress has also explicitly revoked executive orders in their entirety, such as the Energy Policy Act of 2005 which revoked a December 13, 1912 executive order that created Naval Petroleum Reserve Number 2.” An executive order by President George H.W. Bush, to establish a human fetal tissue bank for research purposes, was revoked when Congress declared that ‘the provisions of Executive Order 12806 shall not have any legal effect.’” Third, an executive order can be revoked by a federal appeals court or the Supreme Court. For example, President Clinton’s executive order12954 prohibited the federal government from hiring contractors who replaced strikers. He argued that strikers can become violent when they’re replaced, so it would be better to appease strikers and support union workplace monopolies by banning replacements. But executive order 12954 conflicted with a 7-0 U.S. Supreme Court decision in NLRB v. Mackay Radio & Telegraph Company, 304 U.S. 333 (1938),. In part, that court decided “[The employer] is not bound to discharge those hired to fill the places of strikers.” D.C. Circuit Judge Laurence Silberman said, “We think it untenable to conclude that there are no judicially enforceable limitations on presidential actions [enabling] the President to bypass scores of statutory limitations on governmental authority.” Accordingly, the U.S. Court of Appeals for the D.C. Circuit revoked Clinton’s executive order in Chamber of Commerce v. Reich, 74 F.3d 1322 (D.C. Cir. 1996). While executive orders look like an easy option for a beleaguered president, they increase the temptation to over-reach. They’re likely to inflame controversy and motivate opponents to further mobilize their forces. In the end, when opponents come to power again, whatever has been established with executive orders is most vulnerable to being swept away by a whirlwind

### ---Covert Action

#### The covert action statute mandates basically nothing

Erwin, 13

(Marshall Curtis Erwin, Analyst in Intelligence and National Security at the Congressional Research Service. “Covert Action: Legislative Background and Possible Policy Questions” <https://fas.org/sgp/crs/intel/RL33715.pdf>) Henge

The current statute with regard to covert action remains virtually unchanged since it was signed into law in 1991.28 In essence it codified elements of the “Casey Accords,” the President’s 1988 national security directive, and various legislative initiatives. The legislation approved that year, according to the conferees,29 for the first time imposed the following requirements pertaining to covert action:

• A finding must be in writing.

• A finding may not retroactively authorize covert activities which have already occurred.

• The President must determine that the covert action is necessary to support identifiable foreign policy objectives of the United States.

• A finding must specify all government agencies involved and whether any third party will be involved.

• A finding may not authorize any action intended to influence United States political processes, public opinion, policies, or media.

• A finding may not authorize any action which violates the Constitution of the United States or any statutes of the United States.

• Notification to the congressional leaders specified in the bill must be followed by submission of the written finding to the chairmen of the intelligence committees.

• The intelligence committees must be informed of significant changes in covert actions.

• No funds may be spent by any department, agency, or entity of the executive branch on a covert action until there has been a signed, written finding.

### 2AC—Simulate Aff

#### The ballot should simulate the effects of the aff—KT fairness—also decision-making, political engagement on this topic is key to exposing hypocrisy and making the govt. accountable

Mellor, 13

Ewan E. Mellor [European University Institute, Political and Social Sciences, Graduate Student, Paper Prepared for BISA Conference 2013, “Why policy relevance is a moral necessity: Just war theory, impact, and UAVs”]

**This section of the paper considers** more generally **the need for** just war **theorists to engage with policy debate about the use of force**, as well as to engage with the more fundamental moral and philosophical principles of the just war tradition. **It draws on John Kelsay’s conception of just war thinking as being a social practice**,35 **as well as on** Michael **Walzer’s understanding of the role of the social critic in society**.36 It argues that **the just war tradition is a form of “practical discourse” which is concerned with questions of “how we should act.**”37¶ Kelsay argues that:¶ [T]he criteria of jus ad bellum and jus in bello provide a framework for structured participation in a public conversation about the use of military force . . . citizens who choose to speak in just war terms express commitments . . . [i]n the process of giving and asking for reasons for going to war, those who argue in just war terms seek to influence policy by persuading others that their analysis provides a way to express and fulfil the desire that military actions be both wise and just.38¶ He also argues that “**good just war thinking involves continuous and complete deliberation**, in the sense that one attends to all the standard criteria at war’s inception, at its end, and throughout the course of the conflict.”39 **This is important as it highlights the need for** just war **scholars to engage with the ongoing operations in war and the specific policies that are involved**. The question of whether a particular war is just or unjust, and the question of whether a particular weapon (like drones) can be used in accordance with the jus in bello criteria, only cover a part of the overall justice of the war. **Without an engagement with the reality of war, in terms of the policies used in waging it, it is impossible to engage with the “moral reality of war,”**40 **in terms of being able to discuss it and judge it in moral terms**.¶ Kelsay’s description of just war thinking as a social practice is similar to Walzer’s more general description of social criticism. **The** just war **theorist, as a social critic, must be involved with his or her own society and its practices**. In the same way that the social critic’s distance from his or her society is measured in inches and not miles,41 **the** just war **theorist must be close to and must understand the language through which war is constituted, interpreted and reinterpreted**.42 **It is only by understanding the values and language that their own society purports to live by that the social critic can hold up a mirror to that society to**¶ **demonstrate its hypocrisy and to show the gap that exists between its practice and its values**.43 **The tradition** itself provides a set of values and principles and, as argued by Cian O’Driscoll, **constitutes a “language of engagement” to spur participation in public and political debate.**44 This language is part of “our common heritage, the product of many centuries of arguing about war.”45 These principles and this language provide the terms through which people understand and come to interpret war, not in a deterministic way but by providing the categories necessary for moral understanding and moral argument about the legitimate and illegitimate uses of force.46 **By spurring and providing the basis for political engagement the just war tradition ensures that the acts that occur within war are considered according to just war criteria and allows policy-makers to be held to account on this basis**.¶ **Engaging with the reality of war requires recognising that war is**, as Clausewitz stated, **a continuation of policy**. **War**, according to Clausewitz, **is subordinate to politics and to political choices and these political choices can, and must, be judged and critiqued**.47 ***Engagement and political debate are morally necessary as the alternative is disengagement and moral quietude, which is a sacrifice of the obligations of citizenship***.48 ***This engagement must bring*** just war ***theorists into contact with the policy makers and will require work that is accessible and relevant to policy makers***, **however this does not mean a sacrifice of critical distance or an abdication of truth in the face of power**. By engaging in detail with the policies being pursued and their concordance or otherwise with the principles of the just war tradition **the policy-makers will be forced to account for their decisions and justify them in just war language**. In contrast to the view, suggested by Kenneth Anderson, that “the public cannot be made part of the debate” and that “[w]e are necessarily committed into the hands of our political leadership”,49 **it is incumbent upon** just war **theorists to ensure that the public are informed and are capable of holding their political leaders to account**. To accept the idea that the political leadership are stewards and that accountability will not benefit the public, on whose behalf action is undertaken, but will only benefit al Qaeda,50 is a grotesque act of intellectual irresponsibility. As Walzer has argued, **it is precisely because it is “our country” that we are “especially obligated to criticise its policies**.”51

### 2AC—Util

#### Ethical policymaking requires util

Gvosdev 5 – Rhodes scholar, PhD from St. Antony’s College, executive editor of The National Interest (Nikolas, The Value(s) of Realism, SAIS Review 25.1, pmuse)

As the name implies, realists focus on promoting policies that are achievable and sustainable. In turn, **the morality of a** foreign **policy** action **is judged by its results, not** by the **intentions** of its framers. **A** foreign **policymaker must weigh the consequences of any** course of **action and assess the resources at hand** to carry out the proposed task. As Lippmann warned, Without the controlling principle that the nation must maintain its objectives and its power in equilibrium, its purposes within its means and its means equal to its purposes, its commitments related to its resources and its resources adequate to its commitments, it is impossible to think at all about foreign affairs.8 Commenting on this maxim, Owen Harries, founding editor of The National Interest, noted, "This is a truth of which Americans—more apt to focus on ends rather than means when it comes to dealing with the rest of the world—need always to be reminded."9 In fact, Morgenthau noted that "there can be no political morality without prudence."10 This virtue of prudence—which Morgenthau identified as the cornerstone of realism—should not be confused with expediency. Rather, it takes as its starting point that **it is more moral** to fulfill one's commitments than to make "empty" promises, and **to seek solutions that minimize harm and produce sustainable results**. Morgenthau concluded: [End Page 18] Political realism does not require, nor does it condone, indifference to political ideals and moral principles, but it requires indeed a sharp distinction between the desirable and the possible, between what is desirable everywhere and at all times and what is possible **under the concrete circumstances of time and place**.11 This is why, prior to the outbreak of fighting in the former Yugoslavia, U.S. and European realists urged that Bosnia be decentralized and partitioned into ethnically based cantons as a way to head off a destructive civil war. Realists felt this would be the best course of action, especially after the country's first free and fair elections had brought nationalist candidates to power at the expense of those calling for inter-ethnic cooperation. They had concluded—correctly, as it turned out—that the United States and Western Europe would be unwilling to invest the blood and treasure that would be required to craft a unitary Bosnian state and give it the wherewithal to function. Indeed, at a diplomatic conference in Lisbon in March 1992, the various factions in Bosnia had, reluctantly, endorsed the broad outlines of such a settlement. For the purveyors of moralpolitik, this was unacceptable. After all, for this plan to work, populations on the "wrong side" of the line would have to be transferred and resettled. Such a plan struck directly at the heart of the concept of multi-ethnicity—that different ethnic and religious groups could find a common political identity and work in common institutions. When the United States signaled it would not accept such a settlement, the fragile consensus collapsed. The United States, of course, cannot be held responsible for the war; this lies squarely on the shoulders of Bosnia's political leaders. Yet Washington fell victim to what Jonathan Clarke called "faux Wilsonianism," **the belief that** "high-flown **words matter more than rational calculation" in formulating** effective **policy**, which **led U.S**. policymakers **to dispense with** the equation of "**balancing commitments and resources**."12 Indeed, as he notes, the **Clinton** administration had **criticized peace plans calling for** decentralized **partition in Bosnia "with lofty rhetoric without proposing a practical alternative." The subsequent war led to the deaths of** tens of **thousands** and left more than a million people homeless. After three years of war, the Dayton Accords—hailed as a triumph of American diplomacy—created a complicated arrangement by which the federal union of two ethnic units, the Muslim-Croat Federation, was itself federated to a Bosnian Serb republic. Today, Bosnia requires thousands of foreign troops to patrol its internal borders and billions of dollars in foreign aid to keep its government and economy functioning. Was the aim of U.S. policymakers, academics and journalists—creating a multi-ethnic democracy in Bosnia—not worth pursuing? No, not at all, and this is not what the argument suggests. But aspirations were not matched with capabilities. **As a result of holding out for the "most moral" outcome** and encouraging the Muslim-led government in Sarajevo to pursue maximalist aims **rather than finding a workable compromise that could have avoided bloodshed** and produced more stable conditions, the peoples of **Bosnia suffered greatly**. In the end, **the final settlement was very close** [End Page 19] **to the one** that realists had **initially** proposed—and the one that had also been roundly **condemned on moral grounds.**

### 2AC—Agamben

#### We don’t reinforce the exception—external limitation solves sov power—cross-apply the circumvention cards

Ramsey, 13

(Michael D. Ramsey Hugh and Hazel Darling Foundation Professor of Law & Director, International & Comparative Law Programs at the University of San Diego. “Judge Brett Kavanaugh on Executive Power and Prosecutorial Discretion” <http://originalismblog.typepad.com/the-originalism-blog/2013/08/judge-brett-kavauagh-on-the-dispensing-power-and-prosecutorial-discretionmichael-ramsey.html>) Henge

From the D.C. Circuit in In re Aiken County (decided 8/13/13): "This case raises significant questions about the scope of the Executive’s authority to disregard federal statutes. …" In a potentially important separation of powers case, the D.C. Circuit (Judge Kavanaugh writing) ordered the Nuclear Regulatory Commission to proceed with the licensing process for the Yucca Mountain facility, as required by statute. Some excerpts (Kavanaugh, joined by Randolph; Garland dissenting): Our analysis begins with settled, bedrock principles of constitutional law. Under Article II of the Constitution and relevant Supreme Court precedents, the President must follow statutory mandates so long as there is appropriated money available and the President has no constitutional objection to the statute. So, too, the President must abide by statutory prohibitions unless the President has a constitutional objection to the prohibition. If the President has a constitutional objection to a statutory mandate or prohibition, the President may decline to follow the law unless and until a final Court order dictates otherwise. But the President may not decline to follow a statutory mandate or prohibition simply because of policy objections. Of course, if Congress appropriates no money for a statutorily mandated program, the Executive obviously cannot move forward. But absent a lack of funds or a claim of unconstitutionality that has not been rejected by final Court order, the Executive must abide by statutory mandates and prohibitions. Those basic constitutional principles apply to the President and subordinate executive agencies. And they apply at least as much to independent agencies such as the Nuclear Regulatory Commission. … In this case, however, the Nuclear Regulatory Commission has declined to continue the statutorily mandated Yucca Mountain licensing process.

#### Permutation do both—we can work within a dominant system and still resist

Michel Foucault, biopower dude, 1980, Philosophy, Politics, and Culture, pg. 154

FOUCAULT We must escape from the dilemma of being either for or against. After all, it is possible to face up to a government and remain standing. To work with a government implies neither subjection nor total acceptance. One may work with it and yet be restive. I even believe that the two things go together.

#### Whatever being is impossible

Daly, 04 (<http://www.borderlandsejournal.adelaide.edu.au/vol3no1_2004/daly_noncitizen.htm>, The non-citizen and the concept of 'human rights', Frances Daly, Australian National University 2004).

What it is that we might want a human potentiality to mean is, of course, a complex, difficult and open-ended issue. But **it is important for us to ask whether a human potentiality must start from emptiness. Agamben repeatedly refers to the need to begin from a place of 'amorphousness' and 'inactuality', assuming that there is something that will necessarily follow from the simple fact of human existence – but why should we assume this**? What might constitute or form this potentiality is surely concerned with what is latent but as yet unrealized. For Agamben, there is nothing latent that is not already tainted by a sense of a task that must be done (Agamben, 1993: 43). **There is no ability to achieve any displacement with what is present within values of community and justice, there is only an immobilizing nothingness that assumes a false essence, vocation or destiny. If the 'whatever' being that he contends is indeed emerging, and it possesses, as he argues, "an original relation to desire", it is worthwhile asking what this desire is for** (Agamben, 1993: 10). If it is simply life itself, then it is not clear why this should be devoid of any content. **Any process of emptying out, of erasing and abolishing, such as that which Agamben attempts, is done for a reason - it involves critique and rejection, on the basis, necessarily, that something else is preferable. But Agamben provides us with very little of what is needed to understand how we might engage with this option**.

#### Agamben’s critique is too totalizing—the plan is a justified use of sovereign power to limit executive overreach

Hussain, 2000(Department of History at Berkeley Nasser, 34 Law & Soc'y Rev. 495, lexis).

Here once again we are forced to question Agamben's teleological mode of thought. **Is this sovereign power represented in the concentration camps really a constitutive feature of sovereignty** tout court? Even limiting ouselves to the remarks above, we can imagine a liberal critique of this position that asks from where come the limitations that Agamben concedes previous Weimar governments had observed. **Surely, one does not have to accept in its entirety a normative liberal conception of sovereign power in order to appreciate that the demand for a factual accounting for the decision on the exception, and institutional checks upon the totalization of the space of exception, can nonetheless** - at least in certain instances - **be effective.** Indeed, one could go further and suggest that **a liberal theory of sovereign power understands full well the paradoxical relation between** law and fact, **norm and exception; and, precisely in light of such an understanding constructs an institutional system that cannot resolve the paradox but nonetheless attempts to prevent it from reaching an intensified and catastrophic conclusion**. Given that Agamben is a nuanced and fair-minded thinker, one must wonder about why he largely ignores such a system. We think that one possible answer is that, just as for Agamben the source of the problem is not the institutional operation of sovereign power, but its object - bare life - so too the solution is not a proliferation of institutional safeguards but a rethinking of that mode of being. In this regard, we find his concluding musings on Heidigger to be suggestive.

#### Biopower can also be positive

Dickinson 04 - Associate Professor, History Ph.D., U.C. Berkeley - 2004 (Edward Ross, “Biopolitics, Fascism, Democracy: Some Reflections on Our Discourse About “Modernity,” Central European History, vol. 37, no. 1, 1–48)

Of course, at the most simple-minded level, it seems to me that **an assessment of the potentials of modernity that ignores the ways in which biopolitics has made life tangibly better is somehow deeply flawed. To give just one example, infant mortality in Germany in 1900 was just over 20 percent;** or, in other words, one in five children died before reaching the age of one year. By 1913, it was 15 percent; and **by 1929** (when average real purchasing power was not significantly higher than in 1913) **it was only 9.7 percent**.93 **The expansion of infant health programs— an enormously ambitious, bureaucratic, medicalizing, and sometimes intrusive, social engineering project— had a great deal to do with that change. It would be bizarre to write a history of biopolitical modernity that ruled out an appreciation for how absolutely wonderful and astonishing this achievement— and any number of others like it — really was.** There was a reason for the “Machbarkeitswahn” of the early twentieth century: many marvelous things were in fact becoming machbar. In that sense, it is not really accurate to call it a “Wahn” (delusion, craziness) at all; nor is it accurate to focus only on the “inevitable” frustration of “delusions” of power. Even in the late 1920s, many social engineers could and did look with great satisfaction on the changes they genuinely had the power to accomplish.

### 2AC—Politics

#### Can’t escalate

Ferguson ‘6 (Niall, Professor of History at Harvard University, Senior Research Fellow of Jesus College, Oxford, and Senior Fellow of the Hoover Institution, Stanford, LA Times, July 24)

Could today's quarrel between Israelis and Hezbollah over Lebanon produce World War III? That's what Republican Newt Gingrich, the former speaker of the House, called it last week, echoing earlier fighting talk by Dan Gillerman, Israel's ambassador to the United Nations. Such language can — for now, at least — safely be dismissed as hyperbole. This crisis is not going to trigger another world war. Indeed, I do not expect it to produce even another Middle East war worthy of comparison with those of June 1967 or October 1973. In 1967, Israel fought four of its Arab neighbors — Egypt, Syria, Jordan and Iraq. In 1973, Egypt and Syria attacked Israel. Such combinations are very hard to imagine today. Nor does it seem likely that Syria and Iran will escalate their involvement in the crisis beyond continuing their support for Hezbollah. Neither is in a position to risk a full-scale military confrontation with Israel, given the risk that this might precipitate an American military reaction. Crucially, Washington's consistent support for Israel is not matched by any great power support for Israel's neighbors. During the Cold War, by contrast, the risk was that a Middle East war could spill over into a superpower conflict. Henry Kissinger, secretary of State in the twilight of the Nixon presidency, first heard the news of an Arab-Israeli war at 6:15 a.m. on Oct. 6, 1973. Half an hour later, he was on the phone to the Soviet ambassador in Washington, Anatoly Dobrynin. Two weeks later, Kissinger flew to Moscow to meet the Soviet leader, Leonid Brezhnev. The stakes were high indeed. At one point during the 1973 crisis, as Brezhnev vainly tried to resist Kissinger's efforts to squeeze him out of the diplomatic loop, the White House issued DEFCON 3, putting American strategic nuclear forces on high alert. It is hard to imagine anything like that today. In any case, this war may soon be over. Most wars Israel has fought have been short, lasting a matter of days or weeks (six days in '67, three weeks in '73). Some Israeli sources say this one could be finished in a matter of days. That, at any rate, is clearly the assumption being made in Washington.

#### Support for the bill is down, and the bill’s not up for a vote soon.

Benen 2/04 (Steve Benen, Senate effectively scraps Iran sanctions bill

02/04/14, http://www.msnbc.com/rachel-maddow-show/senate-effectively-scraps-iran-sanctions-bill)

A month ago, proponents of a bipartisan bill on new Iranian sanctions had reason to be optimistic. Despite White House arguments that the bill risked sabotaging delicate international diplomacy, the Senate bill had 59 co-sponsors. The question wasn’t whether the bill would pass the Senate, but rather, whether it could garner a veto-proof super-majority.¶ ¶ The tide turned quickly. Last week, some of the Senate Democrats who had endorsed the legislation began backing off. And this week, supporters effectively shelved the entire bill.¶ Proponents of Iran sanctions have all but abandoned their search for a highly symbolic 60th co-sponsor who would give their bill a filibuster-proof majority and reverse the push against immediate action.¶ ¶ The number of Democrats and Republicans on the bill has been stuck at 59 for more than three weeks, with the White House effectively locking up the Democratic Caucus with a threat to veto a bill it says could doom nuclear talks and precipitate war.¶ Even the list of 59 co-sponsors is misleading given recent developments. Sen. Joe Manchin (D-W.Va.) told MSNBC’s Chris Matthews last week, “I did not sign it with the intention that it would ever be voted upon or used upon while we were negotiating,”, adding, “[W]e’ve got to give peace a chance here and we’ve got to support this process.” Soon after, Sens. Chris Coons (D-Del.) and Kirsten Gillibrand (D-N.Y.) said they, too, were prepared to give the Obama administration time to pursue a peaceful solution. By the end of the weeks, Sens. Ben Cardin (D-Md.) and Richard Blumenthal (D-Conn.) were also comfortable with a delay.¶ ¶ All are technically still considered co-sponsors, but it’s clear that support for the sanctions bill has slowly collapsed. It’s not that the legislation is poised for defeat; it’s that the measure won’t even get a vote anytime soon.

#### The bill’s toast, supporters backed down and there’s no indication of a veto proof majority

Weber 1/30 (Peter Weber | January 30, 2014, What sank the Senate's Iran sanctions bill?, http://theweek.com/article/index/255771/what-sank-the-senates-iran-sanctions-bill)

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]

#### Govt. wants the aff to shore up fragmented cyber ops

Perera, 13

(David Perera is executive editor of the FierceMarkets Government Group, which includes FierceGovernment, FierceGovernmentIT, FierceHomelandSecurity, and FierceMobileGovernment. “SASC calls for new oversight of Cyber Command” <http://www.fiercegovernmentit.com/story/sasc-calls-new-oversight-cyber-command/2013-06-26>) Henge

The Senate Armed Services Committee says it has concerns that oversight of Cyber Command and the cyber mission within the Defense Departments "is fragmented and weak," calling for creation of a Senate-confirmed position within the undersecretary of defense for policy to supervise and manage the funds of offensive cyber forces. The Senate committee voted 23-3 on June 14 to report its version of the fiscal 2014 national defense authorization act (S. 1197), detailing its intentions in a newly released legislative report (.pdf). In the report, the committee says fragmented oversight of Cyber Command and the cyber mission is partly unavoidable, "inasmuch as cyber operations affect every segment of the department, making clear lines of jurisdiction and responsibility impossible to draw." Different defense organizations are in charge of defensive and offensive cybersecurity, while others have responsibility over "technology, architectures, and acquisition, and another for policy and operational considerations." The committee doesn't propose a broad consolidation--although among its other proposals besides creation of the new supervisory position within the USD(P) is to fold the duties of the DoD chief information officer into the deputy chief information officer and give the DCMO authority over the National Security Agency's Information Assurance Directorate. SASC also proposes the chartering of a joint software assurance office as a means of satisfying a provision from the fiscal 2013 authorization act that mandates the use of automated vulnerability analysis tools for DoD systems. The center "would be a logical choice for managing the purchase and distribution of licenses for commercial automated code analysis tools" and for managing the development of improvements to software code analysis tools, the report says. Defense acquisition of cloud computing would also come under increased scrutiny under the SASC proposal through a requirement that the undersecretaries of defense for acquisition technology and logistics, and for intelligence, the DoD CIO and the chair of the Joint Requirement Oversight Council supervise the development and implementation of cloud capabilities for intelligence, surveillance, and reconnaissance data analysis. The supervision would entail enforcing requirements for interoperability and attribute-based access controls for all ISR cloud systems within military services and agencies, as well as enterprisewide data discovery across domains, and the "correlation of data stored in cloud and non-cloud databases, relational and non-relational databases." The intelligence community in particular has embraced NoSQL databases. The committee also calls for a comprehensive Internet mapping capability, stating that "charting this new terrain is as fundamental to operations in cyberspace as maps of physical terrain have always been to military campaigns."

#### New drone oversight thumps the link

Schmitt, 14

(Eric Schmitt, New York Times. “Congress Restricts Drones Program Shift” <http://www.nytimes.com/2014/01/17/us/politics/congress-restricts-drones-program-shift.html?_r=0>) Henge

WASHINGTON — In an unusual move, Congress is placing restrictions on the Obama administration’s plan to shift responsibility for armed drones more toward the military and away from the C.I.A., congressional and administration officials said Thursday. Lawmakers inserted wording into a classified annex to the $1.1 trillion federal budget approved by Congress this week that would make it more difficult to transfer control over the drone campaign or the authority to carry out strikes. The scope of the restrictions remained unclear because of their classification. But the provision does not appear to entirely block a shift described last May by administration officials as a ramification of President Obama’s intention to move the country off a decade-long war footing. RELATED COVERAGE Speaker John A. Boehner on Wednesday after the vote on a spending bill that left some conservative groups fuming.In Defeat for Tea Party, House Passes $1.1 Trillion Spending BillJAN. 15, 2014 Lawmakers allowed the president to waive the constraints under certain circumstances or to permit the transfer if the administration certifies that the military meets certain standards in drone operations, congressional aides said Thursday. Even before the new provision in the budget bill, administration and congressional officials said the schedule for shifting control to the military was being revised — if not shelved. “D.O.D. has some work to do,” a senior House Intelligence Committee staff aide said Thursday, referring to the Department of Defense. “It’s a lot more challenging than they thought.” But the measure, first reported on The Washington Post’s website on Wednesday night, is a rare move by Congress to dictate how covert operations like the drone program are carried out. It also reflects the simmering suspicion among many lawmakers on the Intelligence Committees that the military’s Joint Special Operations Command is not up to the task of killing terrorism suspects with Predator or Reaper drones, a notion the Pentagon rejects.

#### Political capital theory is useless

Hirsh, 2-7

(Michael Hirsh is a Chief Correspondent at National Journal. “There’s no such thing as political capital” 2-7-13 <http://www.nationaljournal.com/magazine/there-s-no-such-thing-as-political-capital-20130207>) Henge

The real problem is that the idea of political capital—or mandates, or momentum—is so poorly defined that presidents and pundits often get it wrong. “Presidents usually over-estimate it,” says George Edwards, a presidential scholar at Texas A&M University. “The best kind of political capital—some sense of an electoral mandate to do something—is very rare. It almost never happens. In 1964, maybe. And to some degree in 1980.” For that reason, political capital is a concept that misleads far more than it enlightens. It is distortionary. It conveys the idea that we know more than we really do about the ever-elusive concept of political power, and it discounts the way unforeseen events can suddenly change everything. Instead, it suggests, erroneously, that a political figure has a concrete amount of political capital to invest, just as someone might have real investment capital—that a particular leader can bank his gains, and the size of his account determines what he can do at any given moment in history. Naturally, any president has practical and electoral limits. Does he have a majority in both chambers of Congress and a cohesive coalition behind him? Obama has neither at present. And unless a surge in the economy—at the moment, still stuck—or some other great victory gives him more momentum, it is inevitable that the closer Obama gets to the 2014 election, the less he will be able to get done. Going into the midterms, Republicans will increasingly avoid any concessions that make him (and the Democrats) stronger. 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, § Marked 08:36 § 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.”

#### Winners win

Hirsh 2/7 (Michael, National Journal, “There’s no such thing as political capital” 2-7-13 <http://www.nationaljournal.com/magazine/there-s-no-such-thing-as-political-capital-20130207>)

In terms of Obama’s second-term agenda, what all these shifting tides of momentum and political calculation mean is this: Anything goes. Obama has no more elections to win, and he needs to worry only about the support he will have in the House and Senate after 2014. But if he picks issues that the country’s mood will support—such as, perhaps, immigration reform and gun control—there is no reason to think he can’t win far more victories than any of the careful calculators of political capital now believe is possible, including battles over tax reform and deficit reduction.¶ Amid today’s atmosphere of Republican self-doubt, a new, more mature Obama seems to be emerging, one who has his agenda clearly in mind and will ride the mood of the country more adroitly. If he can get some early wins—as he already has, apparently, on the fiscal cliff and the upper-income tax increase—that will create momentum, and one win may well lead to others. “Winning wins.”