## 1AC vs GW AS

### 1AC - Arms Races

#### Contention 1 is Arms Races

#### The cyber arms race is accelerating — major attacks are inevitable this year — the best data proves

Goldman 13

CNN Writer, Nations Prepare for Cyberwar, http://money.cnn.com/2013/01/07/technology/security/cyber-war/index.html

Security analysts are predicting that **2013 is when** nation-sponsored cyberwarfare goes mainstream -- and some think such attacks will lead to actual deaths. In 2012, **large-scale cyberattacks** targeted **at** the **Iran**ian government **were uncovered, and in return, Iran** is believed to have **launched massive attacks aimed at U.S. banks and Saudi oil companies. At least 12 of the world's 15 largest military powers are currently building cyberwarfare programs, according to James Lewis, a cybersecurity expert at** the **C**enter for **S**trategic and **I**nternational **S**tudies. So a **cyber Cold War is already in progress.** But some **security companies believe that battle will become even more heated this year. "Nation states and armies will be** more frequent **actors and victims** of cyberthreats**," a team of researchers at McAfee Labs,** an Intel (INTC, Fortune 500)subsidiary, **wrote** in a recent report. Michael **Sutton, head of security research at cloud** security **company** Zscaler, **said he expects governments to** spend furiously **on building up their** cyber **arsenals. Some may** even outsource attacks **to online hackers.** The Obama administration and many in Congress have been more vocal about how an enemy nation or a terrorist cell could target the country's critical infrastructure in a cyberattack. **Banks, stock exchanges, nuclear** power **plants and water purification systems are** particularly **vulnerable, according to numerous assessments delivered to Congress** last year.

#### Specifically, OCOs drive arms races and retaliation

Moss 13

Columnist at The Diplomat Trefor Moss is an independent journalist based in Hong Kong. He covers Asian politics, defence and security, and was Asia-Pacific Editor at Jane’s Defence Weekly until 2009, Is Cyber War the New Cold War?, 4/19/13, http://thediplomat.com/2013/04/19/is-cyber-war-the-new-cold-war/2/

Although setting up a cybersecurity working group with China, Washington has also signaled it intends to escalate. U.S. Cyber Command and NSA chief General Keith Alexander signaled this shift of policy gears earlier this month when he told Congress that of 40 new CYBERCOM teams currently being assembled, 13 would be focused on offensive operations. Gen Alexander also gave new insight into CYBERCOM’s operational structure. The command will consist of three groups, he said: one to protect critical infrastructure; a second to support the military’s regional commands; and a third to conduct national offensive operations. As cyber competition intensifies between the U.S. and China in particular, the international community approaches a crossroads. States might begin to rein in their cyber operations before things get further out of hand, adopt a rules-based system governing cyberspace, and start respecting one another’s virtual sovereignty much as they do one another’s physical sovereignty. Or, if attacks and counter-attacks are left unchecked, cyberspace may become the venue for a new Cold War for the Internet generation. Much as the old Cold War was characterized by indirect conflict involving proxy forces in third-party states, its 21stcentury reboot might become a story of virtual conflict prosecuted by shadowy actors in the digital realm. And as this undeclared conflict poisons bilateral relations over time, the risk of it spilling over into kinetic hostilities will only grow.

#### Cyber arms race causes world war

there are no checks on escalation, deterrence doesn’t apply, and only a certain commitment to the plan solves

CSM 11

Christian Science Monitor

(3/7, Mark Clayton, The new cyber arms race, www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race)

The new cyber arms race Tomorrow's wars will be fought not just with guns, but with the click of a mouse half a world away that will unleash weaponized software that could take out everything from the power grid to a chemical plant. Deep inside a glass-and-concrete office building in suburban Washington, Sean McGurk grasps the handle of a vault door, clicks in a secret entry code, and swings the steel slab open. Stepping over the raised lip of a submarinelike bulkhead, he enters a room bristling with some of the most sophisticated technology in the United States. Banks of computers, hard drives humming on desktops, are tied into an electronic filtering system that monitors billions of bits of information flowing into dozens of federal agencies each second. At any given moment, an analyst can pop up information on a wall of five massive television screens that almost makes this feel like Cowboys Stadium in Arlington, Texas, rather than a bland office building in Arlington, Va. The overriding purpose of all of it: to help prevent what could lead to the next world war. Specifically, the "Einstein II" system, as it is called, is intended to detect a large cyberattack against the US. The first signs of such an "~~electronic Pearl Harbor~~" might include a power failure across a vast portion of the nation's electric grid. It might be the crash of a vital military computer network. It could be a sudden poison gas release at a chemical plant or an explosion at an oil refinery. Whatever it is, the scores of analysts staffing this new multimillion-dollar "watch and warn" center would, presumably, be able to see it and respond, says Mr. McGurk, the facility director. The National Cybersecurity and Communications Integration Center (NCCIC, pronounced en-kick) is one of the crown jewels of the Department of Homeland Security (DHS). It is linked to four other key watch centers run by the FBI, the Department of Defense (DOD), and the National Security Agency (NSA) that monitor military and overseas computer networks. They are monuments to what is rapidly becoming a new global arms race. In the future, wars will not just be fought by soldiers with guns or with planes that drop bombs. They will also be fought with the click of a mouse a half a world away that unleashes carefully weaponized computer programs that disrupt or destroy critical industries like utilities, transportation, communications, and energy. Such attacks could also disable military networks that control the movement of troops, the path of jet fighters, the command and control of warships. "The next time we want to go to war, maybe we wouldn't even need to bomb a country," says Liam O'Murchu, manager of operations for Symantec Security Response, a Mountain View, Calif., computer security firm. "We could just, you know, turn off its power." In this detached new warfare, soldiers wouldn't be killing other soldiers on the field of battle. But it doesn't mean there might not be casualties. Knocking out the power alone in a large section of the US could sow chaos. What if there were no heat in New England in January? No refrigeration for food? The leak of a radiation plume or chemical gas in an urban area? A sudden malfunction of the stock market? A disrupted air traffic control system? These are the darkest scenarios, of course – the kind that people spin to sell books and pump up budgets for new cyberwar technology. Interviews with dozens of cyberconflict experts indicate that this kind of strategic, large-scale digital warfare – while possible – is not the most likely to happen. Instead, some see a prolonged period of aggressive cyberespionage, sabotage, and low-level attacks that damage electronic networks. As one recent study done for the Organization for Economic Cooperation and Development put it: "It is unlikely that there will ever be a true cyberwar." Yet others say that conclusion might be too conservative. The fact is, no one knows for sure where digital weaponry is heading. The cyber arms race is still in its infancy, and once a cybershot is fired, it's hard to predict where the fusillade might end. In the seconds or minutes it might take staffers at the NCCIC to detect an attack, it could have already spread to US water supplies, railway networks, and other vital industries. How does the US military respond – or even know whom to retaliate against? If it does hit back, how does it prevent cyberweapons from spreading damage electronically to other nations around the world? Policy experts are just beginning to ask some of these questions as the cyberweapons buildup begins. And make no mistake, it is beginning. By one estimate, more than 100 nations are now amassing cybermilitary capabilities. This doesn't just mean erecting electronic defenses. It also means developing "offensive" weapons. Shrouded in secrecy, the development of these weaponized new software programs is being done outside public view and with little debate about their impact on existing international treaties and on conventional theories of war, like deterrence, that have governed nations for decades. "Here's the problem – it's 1946 in cyber," says James Mulvenon, a founding member of the Cyber Conflict Studies Association, a nonprofit group in Washington. "So we have these potent new weapons, but we don't have all the conceptual and doctrinal thinking that supports those weapons or any kind of deterrence. Worse, it's not just the US and Soviets that have the weapons – it's millions and millions of people around the world that have these weapons." In the new cyber world order, the conventional big powers won't be the only ones carrying the cannons. Virtually any nation – or terrorist group or activist organization – with enough money and technical know-how will be able to develop or purchase software programs that could disrupt distant computer networks. And the US, because it's so wired, is more vulnerable than most big powers to this new form of warfare. It's the price the country may one day pay for being an advanced and open society. "If the nation went to war today, in a cyberwar, we would lose," Mike McConnell, director of national intelligence from 2007 to 2009, told a US Senate committee a year ago. "We're the most vulnerable. We're the most connected. We have the most to lose." Still, none of this means people should immediately run for a digital fallout shelter. Many analysts think the cyberwar threat is overblown, and the US is developing sophisticated defenses, such as the digital ramparts here in Arlington. The question is: Will it be enough, or will it all amount to a Maginot line? ALAMOGORDO REDUX The cyber equivalent of the dropping of the atom bomb on Hiroshima came last fall. That's when the world found out about Stuxnet, the software program that wasn't just another annoying virus. It was a sophisticated digital superweapon. Unlike typical malicious software – Trojans and viruses that lurk hidden in a computer to, say, steal a bank account password or some proprietary corporate information – Stuxnet was designed to inflict damage in the real world. In this case it was apparently intended to destroy machines critical to Iran's nuclear ambitions. The marauding software was introduced into Iranian computers in five locations sometime in 2009, probably, experts believe, by an infected "thumb drive," a portable memory stick, inserted into the network by unwitting Russian engineers who were working on the Iranian nuclear facility. Once inside the system, analysts say, Stuxnet sought out its target, the computer-controlled nuclear centrifuge system, and sabotaged the machinery. Experts believe, in the end, the software may have damaged up to 1,000 of the plant's centrifuges. It did so without any human help – without anyone clicking a mouse or guiding it electronically. Since its emergence, Stuxnet has demonstrated that cyberattacks will not remain just banal attempts to delete or steal information inside computers or on the Internet. It showed that a cyberweapon can destroy actual plants and equipment – strategically important equipment. It is a "game changer," McGurk told Congress last fall. Experts believe that Stuxnet was developed by a nation with a top-notch covert cyberweapons team, probably at a cost of millions of dollars. But now that elements of its software code – its electronic blueprint – are available on the Internet, it could be downloaded and reverse-engineered by organized crime groups, cyberweapons dealers, so-called "hactivist" organizations, rogue nations, and terrorists. The hactivist group Anonymous recently touted that it had acquired a copy of the Stuxnet code. Individual tinkerers are getting it, too. "What Stuxnet represents is a future in which people with the funds will be able to buy a sophisticated attack like this on the black market," says Ralph Langner, a German cyber-security researcher and Stuxnet expert. "Everyone can have their own cyberweapon." He adds that Stuxnet could be modified by someone who isn't even a control-systems expert into a "digital dirty bomb" that could damage or destroy virtually any industrial operating system it targets. Amr Thabet, an engineering student at the University of Alexandria in Egypt, typifies how easy it is to access the new world of cyberweaponry. During recent mass street protests in his country, he found time to post on his blog a portion of the Stuxnet cyberweapon he had reverse-engineered. The blog drew the attention of cybersecurity experts, who were unhappy, but not surprised, by what he had done. "This kid's work makes Stuxnet a lot more accessible and portable to other computer architectures," says Bob Radvanovsky, an industrial control-systems expert at Infracritical, a Chicago-based computer security organization. "It's something a number of people are doing for intellectual exercise – or for malicious purposes. It's not a good trend. If a college student is trying to dabble with this, who else on the dark nets with more nefarious intentions might be [as well]? In an e-mail interview, Mr. Thabet said he did it largely for the thrill. He noted that he spent two months deconstructing a small but crucial part of the code after he saw all the attention surrounding the discovery of Stuxnet last fall. "It's the first time I see a malware becomes like a gun or like a weapon close a whole company in few days," he writes in broken English. "You can say [Stuxnet] makes the malware a harder challenge and more dangerous. That's maybe what inspire me." THE 'WAR' HAS ... ALREADY BEGUN? Definitions of what constitute a "cyberattack" or "cyberwar" vary, but experts roughly agree the US is now immersed in a continuous series of cyberconflicts. These are with state and nonstate actors, from Russia and China to criminal gangs and online protest groups. "Are we in a cyberwar now?" asks John Bumgarner, research director at the US Cyber Consequences Unit, a Washington-based think tank, who once was a cyberwarrior with the US Army. "No, not yet. Are we being targeted and our nation's networks attacked and infiltrated by nations that may be our adversaries in the future? Yes." Melissa Hathaway, former acting senior director for cyberspace at the National Security Council, says the threat is less a military one by nation-states and more about the need to protect US intellectual property from spies and organized crime groups. "We are currently in an economic cyberwar," Ms. Hathaway says. "It is costing our corporations their innovation, costing Americans their jobs, and making us a country economically weaker over the long term. I don't see it emerging as a military conflict, but as an economic war in which malware and our own digital infrastructure is being used to steal our future." Others agree that a strategic cyberwar isn't likely right now. But they do see the potential for escalation beyond the theft of the latest blueprints for an electric car or jet-fighter engine, particularly as the technology of digital warfare advances and becomes a more strategic imperative. "We in the US tend to think of war and peace as an on-off toggle switch – either at full-scale war or enjoying peace," says Joel Brenner, former head of counterintelligence under the US Director of National Intelligence. "The reality is different. We are now in a constant state of conflict among nations that rarely gets to open warfare.... What we have to get used to is that even countries like China, with which we are certainly not at war, are in intensive cyberconflict with us." While he agrees the notion of big-scale cyberwarfare has been over-hyped, he says attacks that move beyond aggressive espionage to strikes at, or sabotage of, industrial processes and military systems "will become a routine reality." ANYTHING YOU CAN DO, WE CAN DO BETTER The attacks were coordinated but relatively unsophisticated: In the spring of 2007, hackers blocked the websites of the Estonian government and clogged the country's Internet network. At one point, bank cards were immobilized. Later, in 2008, similar cyberstrikes preceded the Russian invasion of Georgia. Moscow denied any involvement in the attacks, but Estonia, among others, suspected Russia. Whoever it was may not be as important as what it's done: touched off a mini cyber arms race, accelerated by the Stuxnet revelation. Germany and Britain announced new cybermilitary programs in January. In December, Estonia and Iran unveiled cybermilitias to help defend against digital attack. They join at least 20 nations that now have advanced cyberwar programs, according to McAfee, a Santa Clara, Calif., computer security firm. Yet more than 100 countries have at least some cyberconflict prowess, and multiple nations "have the capability to conduct sustained, high-end cyberattacks against the US," according to a new report by the Cyber Conflict Studies Association. McAfee identifies a handful of countries moving from a defensive to a more offensive posture – including the US, China, Russia, France, and Israel. Experts like Mr. Langner say the US is the world's cyber superpower, with weapons believed to be able to debilitate or destroy targeted computer networks and industrial plants and equipment linked to them. Indeed, China widely assumes that their nation's computer systems have been "thoroughly compromised" by the US, according to Dr. Mulvenon of the Cyber Conflict Studies Association, even as the Chinese penetrate deeper into US industrial and military networks. As well armed as the US is, however, its defenses are porous. The US may have the mightiest military in the world, but it is also the most computerized – everything from smart bombs to avionics to warship controls – making it unusually vulnerable to cyberassault. The DOD's communication system includes some 15,000 computer networks and 7 million computing devices. According to the Pentagon, unknown attackers try to breach its systems 6 million times a day. More than a few attempts have succeeded. Hackers are believed to have stolen key elements of the F-35 jet fighter a few years ago from a defense contractor. In 2008, infiltrators used thumb drives to infect the DOD's classified electronic network, resulting in what Deputy Defense Secretary William Lynn later called the "most significant breach of US military computers ever." Unlike many of its potential adversaries, the Pentagon is heavily reliant on computer networks. Over the past two decades, US industry, along with the military and federal agencies, have linked some networks and elements of the nation's infrastructure – power plants, air traffic control systems, rail lines – to the notoriously insecure Internet. It makes it easier, faster, and cheaper to communicate and conduct business – but at a cost. Almost all electrical power used by US military bases, for instance, comes from commercial utilities, and the power grid is a key target of adversaries. "We're pretty vulnerable today," says a former US national security official. "Our defense is superporous against anything sophisticated." Countries that are less wired are less vulnerable, which represents another danger. Some analysts even suggest that a small power like North Korea could do serious damage to the US in a cyberattack while sustaining relatively little itself. In a report presented at a NATO conference, former NSA expert Charlie Miller estimated that Pyongyang would need only about 600 cyber experts, three years, and $50 million to overtake and defeat America in a digital war. "One of North Korea's biggest advantages is that it has hardly any Internet-connected infrastructure to target," he says. "On the other hand, the US has tons of vulnerabilities a country like North Korea could exploit." The elite group of hackers sit at an oval bank of computers in a second-floor office on the wind-swept plains of Idaho. Their mission: infiltrate the computer network of Acme Products, an American industrial plant. They immediately begin probing for ways around the company's cyberdefenses and fire walls. Within minutes, they tap into the plant's electronic controls, sabotaging the manufacturing process. "They're already inside our system," howls an Acme worker, looking at his unresponsive computer after only 20 minutes. "They've got control of the lights. We can't even control our own lights!" Less than a half-hour later, a plastic vat is overflowing, spraying liquid into an industrial sink. The company's attempts to retake control of the system prove futile. Is the leak a toxic chemical? Something radioactive? Fortunately, in this case it is water, and the company itself is fictitious. This is simply an exercise by members of the DHS's Industrial Control System-Computer Emergency Readiness Team (ICS-CERT), simulating an attack and defense of a company. The message to emerge from the war game is unmistakably clear: Industrial America isn't well prepared for the new era of cyberwar, either. "We conduct these training classes to alert industry to what's really going on and educate them as to vulnerabilities they may not have thought of," says a senior manager at the Idaho National Laboratory (INL) in Idaho Falls, where the readiness team is located. Down the street, in another warehouselike building, high walls and locked doors shroud rooms where commercial vendors bring their industrial-control software to be probed for weaknesses by the cyber teams. Despite all the efforts here, experts say gaping holes exist in America's commercial electronic defenses. One reason is the vast number of people and organizations trying to penetrate the networks of key industries. Some people liken the intensity of the spying to the height of the postwar rivalry between the US and the Soviet Union – only the snooping now isn't just by a few countries. "I personally believe we're in the middle of a kind of cyber cold war," says a senior industrial control systems security expert at INL. "Over the past year our team has visited 30 to 40 companies in critical infrastructure industries – looking for threats on their [networks and industrial-control] systems – to see the level of penetration. In every case, teams of professionals were already there, embedded on every system." If only part of this infiltration turned out to be corporate espionage, that would be bad enough. But there's a more insidious threat lurking underneath. In his book "Cyber War," Richard Clarke, former counterterrorism chief with the National Security Council, writes that foreign nations are "preparing the battlefield" in key US industries and military networks, in part by creating "trapdoors" in electronic industrial-control systems. These trapdoors, in the form of nearly invisible software "rootkits," are designed to give the attacker access and control over industries' computer networks, which could later be used to disrupt or destroy operations – for instance, of the US power grid. "These hackers are invading the grid's control systems right now where it's easiest, getting themselves in position where they could control things if they wanted to," says the senior cybersecurity expert. "But they're not controlling them yet." Michael Assante, a former Navy cyberwarfare specialist and INL industrial-security expert, sees calculated hacking taking place as well. "I agree we have a lot of cyberespionage going on and a lot of preparation of the battlefield," he says in an interview at his home on a butte overlooking Idaho's Snake River Valley. "There's no question the grid is vulnerable." THE GENIE IS OUT OF THE HARD DRIVE Despite their dangers, cyberweapons hold clear appeal to the US and other nations. For one thing, they don't involve shooting people or inflicting casualties in a conventional sense. If fewer people die from bombs and bullets as a result of surreptitious software programs, nations may be more inclined to use them to try to deal with intractable problems. Cyberweapons may also be far cheaper than many conventional weapons. No doubt these are among the reasons President Obama has accelerated the development of US cybersecurity efforts, building on programs begun late in the tenure of President George W. Bush. In 2009, when announcing the new position of cybersecurity coordinator, Mr. Obama called digital infrastructure a "strategic national asset." Then, last spring, the Pentagon unveiled its joint US Cyber Command to accelerate and consolidate its digital warfare capabilities – including the ability to strike preemptively. Cyberspace was added to sea, air, land, and space as the fifth domain in which the US seeks "dominance." "Given the dominance of offense in cyberspace, US defenses need to be dynamic," wrote Mr. Lynn in Foreign Affairs magazine. "Milliseconds can make a difference, so the US military must respond to attacks as they happen or even before they arrive." Yet the digital war buildup could have far-reaching – and unexpected – consequences. Cyberweapons are hardly clinical or benign. They can infect systems globally in minutes that were not the intended target. Experts say Stuxnet, a self-propagating "worm," corrupted more than 100,000 Windows-based computers worldwide. Its damage could have been far more widespread if the digital warhead had been written to activate on any industrial-control system it found instead of just the one it targeted in Iran. Because strikes and counterstrikes can happen in seconds, conflicts could quickly escalate outside the world of computers. What, for instance, would the US do if an adversary knocked out a power plant – would it retaliate with digital soldiers or real ones? NATO and other organizations are already weighing whether to respond militarily against nations that launch or host cyberattacks against member states. "The US cybersecurity strategy since 2003 has stated that we're not just going to respond to cyberattacks with cyber," says Greg Rattray, a former director of cybersecurity for the National Security Council. "If somebody cripples the US electric grid, a nuclear power plant, or starts to kill people with cyberattacks, we have reserved the right to retaliate by the means we deem appropriate." Yet figuring out whom to retaliate against is far more complicated in a cyberwar than a conventional war. It's not just a matter of seeing who dropped the bombs. The Internet and the foggy world of cyberspace provide ample opportunity for anonymity. The US and other countries are working on technical systems that would allow them to reverse-engineer attacks, detecting identifying elements among tiny packets of information that bounce among servers worldwide. Yet even if cybersleuths can trace the source of a strike to an individual computer, it might be located in the US. Foreign governments could send elite hackers into other countries to infiltrate networks, making it harder to follow the electronic trail. "Access is the key thing," says Dr. Brenner, the former counterintelligence chief. "If we ever get to real hostilities, all these attacks are going to be launched from within the US...." All this makes it difficult to apply conventional doctrines of war, such as deterrence and first-strike capability, to the new era of cyberconflict. Does the US retaliate if it's unsure of who the enemy is? Can there be deterrence if retaliation is uncertain? There are more mundane questions, too: When does aggressive espionage cross a threshold and constitute an "attack"? "We live in a glass house so we better be careful about throwing rocks," says Hathaway of America's presumed prowess in offensive cyberwar and espionage tactics. "We don't have the resilience built into our infrastructure today to enter into such an escalated environment." In the face of such ambiguity, many experts say the US needs an overarching policy that governs the use of cyberweapons. On the plus side, multiple cyberattack technologies "greatly expand the range of options available to US policy makers as well as the policy makers of other nations...," the National Academy of Sciences concluded in a landmark 2009 study. On the other hand, "today's policy and legal framework for guiding and regulating the US use of cyberattack is ill-formed, undeveloped, and highly uncertain.”

#### Congressional constraints of OCOs are key to solve nuclear war

arms-racing, command and control hacking, crisis instability, and fracturing nuclear agreements

Austin, 8/6

Director of Policy Innovation at the EastWest Institute, Costs of American Cyber Superiority, http://www.chinausfocus.com/peace-security/costs-of-american-cyber-superiority/

The United States is racing for the technological frontier in military and intelligence uses of cyber space. It is ahead of all others, and has mobilized massive non-military assets and private contractors in that effort. This constellation of private sector opportunity and deliberate government policy has been aptly labeled in recent months and years by so many credible observers (in The Economist, The Financial Times and the MIT Technology Review) as the cyber industrial complex. The United States is now in the unusual situation where the head of a spy agency (NSA) also runs a major military unified command (Cyber Command). This is probably an unprecedented alignment of Praetorian political power in any major democracy in modern political history. This allocation of such political weight to one military commander is of course for the United States to decide and is a legitimate course of action. But it has consequences. The Snowden case hints at some of the blow-back effects now visible in public. But there are others, less visible. The NSA Prism program exists because it is technologically possible and there have been no effective restraints on its international targeting. This lack of restraint is especially important because the command and control of strategic nuclear weapons is a potential target both of cyber espionage and offensive cyber operations. The argument here is not to suggest a similarity between the weapons themselves, but to identify correctly the very close relationship between cyber operations and nuclear weapons planning. Thus the lack of restraint in cyber weapons might arguably affect (destabilize) pre-existing agreements that constrain nuclear weapons deployment and possible use. The cyber superiority of the United States, while legal and understandable, is now a cause of strategic instability between nuclear armed powers. This is similar to the situation that persisted with nuclear weapons themselves until 1969 when the USSR first proposed an end of the race for the technological frontier of potential planetary devastation. After achieving initial capability, the U.S. nuclear missile build up was not a rational military response to each step increase in Soviet military capability. It was a race for the technological frontier – by both sides – with insufficient recognition of the consequences. This conclusion was borne out by a remarkable Top Secret study commissioned in 1974 by the U.S. Secretary of Defense, Dr James Schlesinger. By the time it was completed and submitted in 1981, it assessed that the nuclear arms build-up by both sides was driven – not by a supposed tit for tat escalation in capability of deployed military systems – but rather by an unconstrained race for the technological limits of each side’s military potential and by its own military doctrinal preferences. The decisions of each side were not for the most part, according to this now declassified study, a direct response to particular systems that the other side was building. In 1969, the USSR acted first to propose an end to the race for the technological frontier of nuclear weapons because it knew it was losing the contest and because it knew there was political sentiment in the United States and in its Allied countries that supported limitations on the unbridled nuclear fetish. As we ponder the American cyber industrial complex of today, we see a similar constellation of opposition to its power emerging. This constellation includes not just the political rivals who see they are losing in cyber space (China and Russia), but nervous allies who see themselves as the likely biggest victims of the American race for cyber superiority, and loyal American military commanders who can see the risks and dangers of that quest. It is time for the United States to take stock of the collateral damage that its quest for cyber military power, including its understandable quest for intelligence superiority over the terrorist enemy, has caused amongst its allies. The loss has not yet been seen at the high political level among allies, in spite of several pro forma requests for information from countries such as Germany. The loss of U.S. credibility has happened more at the popular level. Around the world, once loyal supporters of the United States in its war on terrorism had a reasonable expectation to be treated as faithful allies. They had the expectation, perhaps naïve, that privacy was a value the Americans shared with them. They did not expect to be subject to such a crude distinction (“you are all non-Americans now”). They did not want to know that their entire personal lives in cyber space are now recoverable – should someone so decide – by the running of a bit of software in the NSA. After the Prism revelations, so many of these foreign citizens with an internationalist persuasion and solidarity for the United States now feel a little betrayed. Yet, in the long run, the most influential voice to end the American quest for cyber military superiority may come from its own armed forces. There are military figures in the United States who have had responsibility for nuclear weapons command and control systems and who, in private, counsel caution. They advocate the need to abandon the quest for cyber dominance and pursue a strategy of “mutual security” in cyber space – though that has yet to be defined. They cite military exercises where the Blue team gets little or no warning of Red team disruptive cyber attack on systems that might affect critical nuclear command and control or wider war mobilization functions. Strategic nuclear stability may be at risk because of uncertainty about innovations in cyber attack capability. This question is worth much more attention. U.S. national security strategy in cyber space needs to be brought under stronger civilian oversight and subject to **more** rigorous public scrutiny. The focus on Chinese cyber espionage has totally preempted proper debate about American cyber military power. Most in the United States Congress have lined up to condemn Snowden. That is understandable. But where are the critical voices looking at the bigger picture of strategic instability in cyberspace that existed before Snowden and has now been aggravated because of him? The Russian and Chinese rejections of reasonable U.S. demands for Snowden’s extradition may be every bit as reasonable given their anxiety about unconstrained American cyber superiority.

#### Cyberwar escalates:

#### A) Speed, scope, and spoofing

Clarke and Knake ‘12

(Richard (former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States) and Robert (Cybersecurity and homeland security expert at the Council on Foreign Relations), Cyber War: The Next Threat to National Security and What to Do About It, Harper Collins Books, 2012, RSR)

**In our hypothetical exercise, the Chinese response aimed at four U.S. navy facilities** but **spilled**¶ **over into several major cities in four countries**. (The North American Interconnects link electric¶ power systems in the U.S., Canada, and parts of Mexico.)¶ **To hide its tracks, the U.S**., in this scenario, **attacked the Chinese power grid from a computer**¶ **in Estonia**. To get to China from Estonia, the U.S. attack packets would have had to traverse¶ several countries, including Russia. To discover the source of the attacks on them, the Chinese¶ would probably have hacked into the Russian routers from which the last packets came. **In**¶ **response, China hit back at Estonia to make the point that nations that allow cyber attacks to**¶ **originate from their networks may end up getting punished even though they had not intentionally**¶ **originated the attack**.¶ **Even in an age of intercontinental missiles and aircraft, cyber war moves faster and crosses**¶ **borders more easily than any form of hostilities in history**. Once a nation-state has initiated cyber¶ war, **there is a high potential that other nations will be drawn in, as the attackers try to hide both**¶ **their identities and the routes taken by their attacks**. Launching an attack from Estonian sites¶ would be like the U.S. landing attack aircraft in Mongolia without asking for permission, and¶ then, having refueled, taking off and bombing China. **Because some attack tools**, such as worms,¶ once launched into cyberspace **can spread globally in minutes, there is the possibility of collateral**¶ **damage as these malicious programs jump international boundaries and affect unintended targets**.¶ But what about collateral damage in the country that is being targeted?

#### b) Pressure to retaliate

Owens et al 9

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

But **in many kinds of cyberattack, the magnitude of the impact of the** ¶ **first cyberattack will be uncertain** at first, and may remain so for a considerable period of time. **Decision makers may then be caught between two** ¶ **challenges—a policy need to respond quickly and the technical fact that it** ¶ **may be necessary to wait until more information about impact and damage can be obtained**. (As noted in Section 2.5, these tensions are especially ¶ challenging in the context of active defense.)¶ **Decision makers often feel intense pressure to “do something” immediately after the onset of a crisis**, and sometimes such pressure is warranted by the facts and circumstances of the situation. On the other hand, ¶ **the lack of immediate information may prompt decision makers to take a** ¶ **worst-case view of the attack and** thus to **assume that the worst that might** ¶ **have happened was indeed what actually happened**. **Such a situation has** ¶ **obvious potential for inappropriate and unintended escalation.**

### 1AC - Alliances

#### Contention 2 is Alliances

#### Congressional restrictions necessary for allied cooperation— restoring legitimacy to OCOs is key to cyber coalitions

Dunlap 12

Major General and Former Deputy Judge Advocate General (Lawless Cyberwar? Not If You Want to Win, www.americanbar.org/groups/public\_services/law\_national\_security/patriot\_debates2/the\_book\_online/ch9/ch9\_ess2.html)

Military commanders have seen the no-legal-limits movie before and they do not like it. In the aftermath of 9/11, civilian lawyers moved in exactly that direction. Former Attorney General Alberto Gonzales, for example, rejected parts of the Geneva Conventions as “quaint.” He then aligned himself with other civilian government lawyers who seemed to believe that the President’s war-making power knew virtually no limits. The most egregious example of this mindset was their endorsement of interrogation tecshniques now widely labeled as torture.25 The results of the no-legal-limits approach were disastrous. The ill-conceived civilian-sourced interrogation, detention, and military tribunal policies, implemented over the persistent objections of America’s military lawyers, caused an international uproar that profoundly injured critical relations with indispensable allies.26 Even more damaging, they put the armed forces on the road to Abu Ghraib, a catastrophic explosion of criminality that produced what military leaders like then U.S. commander in Iraq Lieutenant General Ricardo Sanchez labeled as a “clear defeat.”27 Infused with illegalities, Abu Ghraib became the greatest reversal America has suffered since 9/11. In fact, in purely military terms, it continues to hobble counterterrorism efforts. General David Petraeus observed that “Abu Ghraib and other situations like that are non-biodegradable. They don’t go away.” “The enemy,” Petraeus says, “continues to beat you with them like a stick.”28 In short, military commanders want to adhere to the law because they have hard experience with the consequences of failing to do so. Why, then, is Baker—and others—so troubled? Actually, there are legitimate concerns about America’s cyber capabilities, but the attack on the issues is misdirected. Indeed, if Baker substitutes the term policy maker for lawyer and the term policy for law, he might be closer to the truth in terms of today’s cyberwar challenges. To those with intimate knowledge of the intricacies of cyber war, it is not the “law,” per se, that represents the most daunting issue; to them, it ispolicy. For example, retired Air Force General Michael Hayden, the former head of the National Security Agency (NSA), and later Director of the CIA, told Congress in October of 2011 that America’s cyber defenses were being undermined because cyber information was “horribly overclassified.”29 That issue is not sourced in lawyers, but in policy makers who could solve the classification problem virtually overnight if they wanted to. That same month, General Keith B. Alexander, Commander of U.S. Cyber Command and current NSA Director, said that rules of engagement were being developed that would “help to define conditions in which the military can go on the offensive against cyber threats and what specific actions it can take.” General Alexander readily acknowledges the applicability of the law of armed conflict, but suggests that challenges exist in discerning the facts and circumstances to apply to the law.30 This gets to the “act of war” question Baker complains about. The law does provide a framework;31 it is up to decision makers to discern the facts to apply to that framework. Hard to do? Absolutely. But—frankly—such “fog of war” issues are not much different than those military commanders routinely confront in the other domains of conflict where difficult decisions frequently must be made on imperfect information. The ability (or inability) to determine facts is not a legal issue, but as much a technical problem for the specialists to solve. So if there is a difficulty in that regard, the complaint ought to be directed at cyber scientists or even policy strategists, but not the lawyers. Sure, the law requires an ability to determine the source of an attack before launching a military response, but so does good sense and effective military strategy. The same can be said for the legal requirement to assess the impact on civilians and civilian objects before launching a cyber attack. This is information that decision makers would want for political and policy reasons wholly independent of any legal requirements. As the great strategist Carl von Clausewitz observed, “War is the continuation of policy by other means.”32 Again, if the ability to make the calculations that political leaders and policy makers require as much as lawyers is inadequate, that is a technical, not legal, issue. When—and if—the facts and circumstances are determined, weighing them is what policy makers and military commanders “do.” Lawyers may help them, but ultimately it is the decision maker’s call, not the lawyer’s. Any reluctance of decision makers to make difficult fact determinations—if such reluctance does exist—is not, in any event, a deficiency of law, but ofleadership. Of course, such decisions are never exclusively about legal matters. Policy makers and commanders rightly take into account a variety of factors beyond the law. In actual practice, it appears that such considerations often are more limiting than the law. For example, the Washington Post reported that U.S. cyber weapons “had been considered to disrupt Gaddafi’s air defenses” early in NATO’s UN-sanctioned operations aimed at protecting Libyan civilians.33 However, the effort “was aborted,” the Post said, “when it became clear that there was not enough time for a cyber attack to work.” Conventional weapons, it was said, were “faster, and more potent,” a pure military rationale. None of this reflects even the slightest suggestion that “lawyers” or the law frustrated the execution of a cyber operation in Libya. No doubt there was discussion about cyber-reporting obligations under the War Powers Resolution, but Presidents have almost never seen that as a bar to military actions, so it can hardly be said to be something unique to cyber operations or that operated to actually block a cyber attack, per se. Rather, it is but one of the many political considerations applicable to military actions generally, cyber or otherwise. To be clear, the primary concern about the potential use of cyber weaponry against Libya wasnot anything generated by lawyers as Baker might put it, but rather by “administration officials and even some military officers” who, the New York Times says, “balked, fearing that it might set a precedent for other nations, in particular Russia or China, to carry out such offensives of their own.” Along this line, the Times quoted James Andrew Lewis, a senior fellow at the Center for Strategic and International Studies, as opining that the United States does not want to be the “ones who break the glass on this new kind of warfare.”34 Again, the legitimacy of these concerns aside, they illustrate— regardless—that while there may be unresolved policy questions inhibiting cyber operations, that is altogether different from the legal problems of Baker’s imaginings. The threat of cyberwar is certainly an extremely serious one, but surely not a greater peril than is nuclear war. Yet at least insofar as the U.S. military is concerned, nuclear operations can be made amenable to the law.35 In other words, if our survival does not require abandoning the rule of law with respect to nuclear weapons, there is certainly no reason to do so in the cyber realm. Does Baker nevertheless believe that the United States is so vulnerable to catastrophic cyber attack that the nation must reject any legal limits in its cyber response? If, indeed, the United States were as vulnerable to catastrophic attack as Baker would have us believe, al Qaeda or some extremist group certainly would have launched one by now. In point of fact, although cyber crime may be extensive, militarily significant cyber attacks apparently are not so easy to conduct as Baker seems to think. In reporting the rejection of cyber weaponry as a means of dismantling ibyan air defenses, The New York Times noted that: While popular fiction and films depict cyberattacks as easy to mount—only a few computer keystrokes needed—in reality it takes significant digital snooping to identify potential entry points and susceptible nodes in a linked network of communications systems, radars and missiles like that operated by the Libyan government, and then to write and insert the proper poisonous codes. Obviously, if cyber weaponry is technically difficult for the world’s foremost military to use even against a third-world power such as Libya, one may reasonably infer that it is markedly more difficult to use against a sophisticated first-world power, even for a peer or near peer of that power. Rejection of legal limits carries other, real-world consequences that are not in the United States’ cyber interests. An effective response to cyber threats is not an autarchic enterprise; it requires the cooperation of international allies. Baker’s “damn the law and lawyers” approach would [harm]~~cripple~~ our relations with the law-abiding nations whose cooperation we must have to address cyber threats. We need to keep in mind that the vast majority of adverse cyber incidents are criminal matters, and the resolution of them frequently necessitates the involvement of foreign police and judicial authorities who, by definition, require partners who are themselves committed to faithfulness to the rule of law. The importance of legal legitimacy cannot be overstated. As outlined above, few in uniform who have experienced the vicissitudes of war since 9/11 would underestimate the deleterious impact on coalition support that the mere perception of American lawlessness can have.

#### The small concession of the plan is key — it increases key flexibility and secures cyberspace

Lord et al 11

Vice President and Director of Studies at the Center for a New American Security

(Kristin M., Travis Sharp is the Bacevich Fellow at the Center for a New American Security. Joseph S. Nye, Jr. is University Distinguished Service Professor at the Kennedy School of

Government at Harvard University. Mike McConnell is Executive Vice President of Booz Allen Hamilton and former Director of National Intelligence and Director of the National Security Agency. Gary McGraw is Chief Technology Officer of Cigital, Inc., a software security consultancy, and author of eight books on software security. Nathaniel Fick is Chief Executive Officer of the Center for a New American Security. Thomas G. Mahnken is Jerome E. Levy Chair of Economic Geography and National Security at the U.S. Naval War College and a Visiting Scholar at the Johns Hopkins School of Advanced International Studies. Gregory J. Rattray is a Partner at Delta Risk LLC and Senior Vice President for Security at BITS, the technology policy division of The Financial Services Roundtable. Jason Healey is Director of the Cyber Statecraft Initiative at the Atlantic Council and Executive Director of the Cyber Conflict Studies Association. Martha Finnemore is Professor of Political Science and International Affairs at The George Washington University. David A. Gross is a Partner at Wiley Rein LLP and a former Ambassador and Coordinator for International Communications and Information Policy at the State Department. Nova J. Daly is a Public Policy Consultant at Wiley Rein LLP and former Deputy Assistant Secretary for Investment Security in the Office of International Affairs at the Treasury Department. M. Ethan Lucarelli is an Associate at Wiley Rein LLP. Roger H. Miksad is an Associate at Wiley Rein LLP. James A. Lewis is a Senior Fellow and Director of the Technology and Public Policy Program at the Center for Strategic and International Studies. Richard Fontaine is a Senior Fellow at the Center for a New American Security. Will Rogers is a Research Associate at the Center for a New American Security. Christopher M. Schroeder is an Internet entrepreneur, Chief Executive Officer of HealthCentral.com and a member of the Center for a New American Security’s board of advisors. Daniel E. Geer, Jr. is Chief Information Security Officer of In-Q-Tel, the independent investment firm that identifies innovative technologies in support of the missions of the U.S. intelligence community. Robert E. Kahn is President and Chief Executive Officer of the Corporation for National Research Initiatives and co-inventor of the TCP/IP protocol that is the foundation of the modern Internet. Peter Schwartz is Co-Founder and Chairman of Global Business Network and a member of the Center for a New American Security’s board of directors, “America’s Cyber Future Security and Prosperity in the Information Age volume I” June 2011, http:// www.cnas.org/files/documents/publications/CNAS\_Cyber\_Volume%20I\_0.pdf)

The United States should lead a broad, multi-stakeholder international cyber security coalition that supplements U.S. freedom of action in cyberspace with global norms that will help protect its interests. The United States must play a greater leadership role within a range of existing and emerging international coalitions if it wishes to shape the future of cyberspace and how it is governed.35 Exercising leadership may, in some circumstances, require the United States to curtail some freedom of action internationally in order to shape the behavior of others. It does this already by adhering to existing norms and agreements, such as the Law of Armed Conflict and World Trade Organization. As long as such tradeoffs remain consistent with American interests and values, this cooperative leadership model offers the best way for the United States to strengthen its cyber security. Since the United States pursues competing interests and values in cyberspace, it must develop policies that balance those interests and values. An effective cyber security strategy requires American policymakers to balance competing interests and values in a way that defends the nation without subverting what it stands for.

#### Status quo cyber doctrine undermines US credibility

Lawson ‘10

[Sean Lawson is an assistant professor in the Department of Communication at the University of Utah. His research focuses on the relationships among science, technology, and the development of military theory and discourse, in particular the intersections of national security and military thought with new media, information, and communication technologies.¶ http://www.forbes.com/sites/firewall/2010/05/13/offensive-cyberwar-operations-as-communication/ ETB]

What’s more, John Arquilla has advocated taking offensive action against terrorist websites, and a recent operation by the U.S. military that took down a forum allegedly being used by jihadists in Iraq indicates that at least a few folks in the U.S. military are acting in accord with his recommendations. In addition to the concern that some have raised over whether taking down jihadist websites deprives the U.S. of valuable sources of intelligence, we should also be asking what these types of offensive cyber actions communicate to adversaries and allies alike.¶ ADM Mullen has written about U.S. adversaries’ talent for detecting U.S. “say-do gaps” and then driving trucks through those gaps that end up damaging U.S. credibility (p. 4). He uses Abu Ghraib as an example, where what was done there was in sharp contrast to the things that U.S. leadership said about human rights, dignity, etc. Similarly, what kinds of “say-do gaps” might be created by offensive cyber operations meant to silence or disrupt adversary communications online? It might not be difficult for an even moderately observant adversary to point to a contradiction (real or not) between U.S. rhetoric about “Internet freedom” and freedom of speech and expression on the one hand and U.S. actions taken to silence its opponents on the other hand.¶ Keeping Dunlap’s classic essays in mind, might offensive actions like those recommended by Arquilla and potentially witnessed in the jihadist forum takedown case contribute to creating a perception of U.S. weakness, both in the information battle and the kinetic battle? Might U.S. attempts to silence opponents look like weakness in the proverbial “battle for hearts and minds?” A resort to silencing as a result of an inability to effectively engage? Despite all the talk of markets and freedom of expression, the market that the U.S. fears the most is the marketplace of ideas? Etc., etc., etc.

#### Alliances prevent nuclear war---key to burden sharing

Douglas Ross 99 is professor of political science at Simon Fraser University, Winter 1998/1999, Canada’s functional ¶ isolationism and the future of weapons of mass destruction, International Journal, p. lexis

Thus, an easily accessible tax base has long been available for spending much more on international security than recent governments have been willing to contemplate. ? Negotiating the landmines ban, discouraging trade in small arms, promoting the United Nations arms register are all worthwhile, popular activities that polish the national ? self-image. **But they should all be supplements to, not substitutes for, a proportionately equitable commitment of resources to the management and ? prevention of international conflict – and thus the containment of the WMD threat**. **Future American governments will not ‘police the ? world’ alone**. For almost fifty years the Soviet threat compelled disproportionate military expenditures and sacrifice by the United States. That world is gone. **Only by enmeshing the capabilities of the United States and other leading powers in a co-operative security management regime where the burdens are widely shared does the world community have any plausible hope of avoiding warfare involving nuclear or other WMD**

#### Coalition building key to solve extinction

Joseph Nye 8is professor of international relations at Harvard University, “American Power After the Financial Crises,” http://www.foresightproject.net/publications/articles/article.asp?p=3533, DOA: 7-23-13, y2k

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 stag**e. 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.**

#### Legitimacy is key to band-wagon

Lee 10

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 forunilateral 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 lawon 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.

#### Chinese anti-access capabilities critically depend on cyber — allied cooperation is key to counter them

Kazianis 12

Assistant Editor for The Diplomat and a non-resident fellow at the Pacific Forum

(Harry, “A Plea for an Alliance-Based ‘AirSeaCyber’ Joint Operational Concept” July 17, 2012, http://rpdefense.over-blog.com/article-a-plea-for-an-alliance-based-airseacyber-joint-operational-concept-108240342.html)

In Pacific Forum’s PacNet #41 issue, Mihoko Matsubara correctly asserts that “countering cyber threats demands cooperation among nations, in particular public-private partnerships.” Cyber war has finally made its way onto the radar, and rightly so. Now **the U**nited **S**tates **military must integrate cyber** considerations **into** its new **AirSea Battle** concept. US Secretary of Defense Leon Panetta warned that the “~~next Pearl Harbor~~ we confront could very well be a cyber-attack that ~~cripples~~ our power systems, our grid, our security systems, our financial systems.” If true, **cyber must be front and center in** any military refocusing to **the Asia-Pacific**. Any **failure to** not correctly **plan** **against this** lethal form of asymmetric warfare **could** **be a catastrophic mistake**. The US seems to be focusing the military component of its widely discussed ‘pivot’ to Asia on China’s growing military capabilities. While neither side seeks confrontation and one hopes none will occur, **China’s development** **of** a highly capable Anti-Access/Area Denial (**A2/AD**) battle **plan to deter,** **slow, or deny** **entry** into a contested geographic area or combat zone **has been detailed** extensively. **Cyber war is clearly** **part of this** strategy, **with** Chinese **planners prepared to wage** ‘local **wars under conditions of informatization**,’ or high-intensity, information-centric regional military operations of short duration. Prudent military planners must be prepared to meet this potential threat. Other nations such as **North Korea and Iran are also developing A2/AD** capabilities with cyber based components that could challenge US or allied interests. In this type of threat environment, the **US**, along **with** its **allies**, **should develop** its own symmetric and asymmetric counter-strategies. **A joint operational concept** of AirSea Battle **that** **includes** a strong **cyber** component **would give US forces and their allies the best chance to defeat adversary A2/AD** forces. Of course, the current Joint Operational Access Concept does make strong mention of cyber operations. However, **an even stronger emphasis on cyber warfare is needed**. In short, AirSea Battle as an operational concept might already be obsolete and **it should be reconstituted as** an “**AirSeaCyber**” concept. If cyber is to become a full-fledged component of AirSea Battle, its conceptualization and integration are crucial. A simple first step must be the recognition that cyberspace is now one of the most important battlefield domains in which the US and allied militaries operate. It is not enough to exercise battlefield dominance in a physical sense with technologically advanced equipment. With vital but vulnerable computer networks, software, and operating systems a potential adversary may choose an asymmetric cyber ‘first-strike’ to damage its opponent’s networked combat capabilities. Enemy forces could attempt to ‘~~blind’~~ their opponent by ~~crippling~~ computer and network-centric command and control (C2), battlefield intelligence gathering, and combat capabilities by conducting advanced cyber operations. Simply put: **US and allied forces** **must** fully understand and **articulate the severity of the threat they face** before they can map out any national or multinational strategies. **Working** with potential cyber allies **to identify** **common threats and** working **to mitigate** possible **challenges is crucial.** **One viable partner** in creating effective cyber capabilities **is South Korea**. Seoul faces a number of problems from a growing North Korean asymmetric threat in a physical sense, as well as multiple challenges in cyberspace. General James Thurman, US Forces Korea Commander, recently noted that “North Korea employs sophisticated computer hackers trained to launch cyber infiltration and cyber-attacks.” Pyongyang utilizes cyber capabilities “against a variety of targets including military, governmental, educational and commercial institutions.” **With the US committed** **to** South **Korea’s defense**, **creating partnerships** in cyberspace **can only enhance such a relationship.** Both sides must look past physical threats and expand their partnership across this new domain of possible conflict. **Japan is another possible cyberspace partner.** As Matsubara accurately points out, “**They [US and Japan] have more to lose**. **If** cyber-**attacks** and espionage **undermine** **their** economies or military **capability**, larger geostrategic balances may be affected and **the** negative **consequences may spill over** to other countries.” Both nations have reported hacking incidents from Chinese-based hackers that have targeted defense-related industries and programs. With Japan and the US partnering on joint projects such as missile defense and F-35 fighter jet, the protection of classified information associated with these programs must be a top priority. As military allies, both must plan for possible regional conflict where cyber warfare could be utilized against them. Sadly, restraints could develop that might hamper such partnerships. One recent example: historical and political tensions have delayed and possibly halted a defense agreement between Japan and South Korea. The pact would have assisted in the direct sharing of sensitive military information concerning North Korea, China, and missile defenses. Presumably, cyber-related information would have been at the center of such sharing. The agreement was supported by Washington, which has been working to reinforce trilateral cooperation with the two countries, as essential Asian allies. With all three nations facing a common challenge from North Korea, such an agreement would have been highly beneficial to all parties. If other nations’ military planners rely heavily on asymmetric warfare strategies, **US planners** and their allies **must** also **utilize** such **capabilities** in developing their response. **Cyber warfare offers** proportionally the **strongest asymmetric capabilities at the lowest possible cost**. Almost **all** military C2 and deployed **weapons systems rely on** **computer** hardware and **software.** **As other nations’** military planners **develop** networked **joint operations** to multi-domain warfare, **they** also **open their systems for exploitation** by cyber-attack. US and allied technology experts must begin or accelerate long-range studies of possible adversaries’ hardware, software, computer networks, and fiber optic communications. **This will allow** US and **allied cyber commands to deploy malware,** viruses, and coordinated strikes on fiber-based communications networks that would launch any enemy offensive or defensive operations. **Cyber warfare,** if conducted in coordination with standard tactical operations, **could be the ultimate cross-domain** asymmetric **weapon** in modern 21st century warfare against any nation that utilizes networked military technologies. Any good operational concept must always attempt to minimize any negative consequences of its implementation. AirSeaCyber presents US policymakers and their allies with a toolkit to deal with the diverse global military challenges of the 21st Century. **The inclusion of cyber** obviously **declares** **that the US** **and** its **allies** **are prepared to enter a new domain** of combat operations. This focus could unnecessarily draw attention to a domain that should be left to ‘fight in the shadows’ to avoid engendering a new battleground with deadly consequences. Some argue that with the use of cyber weapons against Iran to degrade its ability to develop uranium enrichment technology, a dangerous new international norm – operational use of cyber weapons – is upon us. While these arguments have some validity, cyber war, whether against corporations, nation-states, or even individuals, is now part of daily life. To not prepare fully for this eventuality means facing battlefield obsolescence. Any student of history knows the results of preparing for the wars of years past-likely defeat. These are only a sample of capabilities that could be utilized to create a joint operational concept that transition from present AirSea Battle ideas into a more focused AirSeaCyber operational concept. Such notions are compliant with current fiscal realities, utilize modern military technologies, and can leverage existing alliance networks. Any operational concept that will guide US armed forces in the future is obsolete without intense conceptualizations of cyber warfare. **Working with allies to develop ties** in cyberspace in the Asia-Pacific **can only create a strong force multiplier effect** and should be considered a top priority.

#### China’s rapidly modernizing its military for an A2AD strategy — that fuels territorial disputes

RTT 13

China’s Anti-access And Area-denial Capabilities Bolstered: Pentagon Report, http://www.rttnews.com/2111200/china-s-anti-access-and-area-denial-capabilities-bolstered-pentagon-report.aspx

**A new report of the** U.S. **Defense Department** **says** that **China is** **increasing its** rapid **military modernization program**, **and** that **the** advanced **technologies** **bolster** China's **anti-access** **and area-denial** capabilities. The annual report -- titled "2013 Military and Security Developments Involving the People's Republic of China" -- was submitted to the Congress on Monday. It covers China's security and military strategies; developments in its military doctrine, force structure and advanced technologies; the security situation in the Taiwan strait; U.S.-China military-to-military contacts and the U.S. strategy for such engagement; and the nature of China's cyber activities directed against the Defense Department. David F. Helvey, Deputy Assistant Secretary of Defense for East Asia, briefed Pentagon reporters on the report. He noted that the report, which DoD coordinates with other agencies, "reflects broadly the views held across the United States government." **The report is factual** **and not speculative**, he noted. Helvey said the trends in this year's report show "a good deal of continuity in terms of the modernization priorities (of China)," despite the 2012 and 2013 turnover to new leadership in that Communist country. The document notes that **China** has **launched its first** aircraft **carrier** in 2012 **and has been sustaining investments in** advanced short- and medium-range conventional **ballistic missiles**, land-attack and anti-ship **cruise missiles**, counter-space weapons **and** military **cyberspace systems**. "The issue here is not one particular weapons system. **It's the integration** and overlapping nature **of** these weapons **systems** **into a regime** **that can** potentially impede or **restrict** free military **operations** **in the** Western **Pacific**. So that's something that we monitor and are concerned about," Helvey said. The report provided a lot of information, but also raises some questions. "What concerns me is the extent to which China's military modernization occurs in the absence of the kind of openness and transparency that others are certainly asking of China," he added. That lack of transparency has effects on the security calculations of others in the region, "and that's of greater concern," he noted. Addressing China's cyber capabilities, Helvey said "in 2012, numerous computer systems around the world, including those owned by the United States government, continued to be targeted for intrusions, some of which appear to be attributable directly to [Chinese] government and military organizations." The report noted that China has "increased assertiveness with respect to its maritime territorial claims" over the past year. **China disputes sovereignty with Japan over islands in the East China Sea, and has other territorial disputes with regional neighbors in the South China Sea.**

#### PLA doctrine proves Chinese aggression against Taiwan and the South China Sea are inevitable — A2AD is the linchpin of this capability

Yoshihara 10

(Dr. Toshi Yoshihara, Associate Professor in the Strategy and Policy Department at the Naval War College, former Visiting Professor at the U.S. Air War College, Ph.D. International Relations, The Fletcher School of Law and Diplomacy, Tufts University, M.A. International Relations, School of Advanced International Studies, Johns Hopkins University, B.S. International Relations, School of Foreign Service, Georgetown University, “Chinese Missile Strategy and the U.S. Naval Presence in Japan: The Operational View from Beijing,” Naval War College Review, 7-1-2010, (... denotes non-US-ASCII text omitted) http://www.faqs.org/periodicals/201007/2046727461.html)

In recent years, **defense analysts** in the United States have substantially **revised** their **estimates of China's** missile **prowess**. A decade ago, most observers rated Beijing's ballistic missiles as inaccurate, blunt weapons limited to terrorizing civilian populations. Today, the **emerging consensus** within the U.S. strategic community **is** that **China**'s arsenal **can** **inflict** **lethal harm** with precision **on a** wide **range of** military **targets**, including ports and airfields. As a consequence, many observers have jettisoned previously sanguine net assessments that conferred decisive, qualitative advantages to Taiwan in the cross-strait military balance. Indeed, the debates on China's coercive power and Taiwan's apparent inability to resist such pressure have taken on a palpably fatalistic tone. A 2009 RAND monograph warns that China's large, modern missile and air forces are likely to pose a virtually insurmountable challenge to Taiwanese and American efforts to command the air over the strait and the island. The authors of the report believe that massive ballistic-missile salvos launched against Taiwan's air bases would severely hamper Taipei's ability to generate enough fighter sorties to contest air superiority. They state: "As China's ability to deliver accurate fire across the strait grows, it is becoming increasingly difficult and soon may be impossible for the United States and Taiwan to protect the island's military and civilian infrastructures from serious damage."1 As a result, the authors observe, "China's ability to suppress Taiwan and local U.S. air bases with ballistic and cruise missiles seriously threatens the defense's ability to maintain control of the air over the strait."2 They further assert, "The United States can no longer be confident of winning the battle for the air in the air. This represents a dramatic change from the first five-plus decades of the China- Taiwan confrontation."3 An unclassified Defense Intelligence Agency report assessing the state of Taiwan's air defenses raises similar concerns. The study notes that Taiwanese fighter aircraft would be unable to take to the air in the absence of well-protected airfield runways, suggesting a major vulnerability to the island's airpower. The agency further maintains that Taiwan's capacity to endure missile attacks on runways and to repair them rapidly will determine the integrity of the island's air-defense system.4 While the report withholds judgment on whether Taipei can maintain air superiority following Chinese missile strikes in a conflict scenario, a key constituent of the U.S. intelligence community clearly recognizes a growing danger to Taiwan's defense. China's missiles also threaten Taiwan's ability to defend itself at sea. William Murray contends that China could sink or severely damage many of Taiwan's warships docked at naval piers with salvos of ballistic missiles. He argues that "the Second Artillery's [China's strategic missile command's] expanding inventory of increasingly accurate [short-range ballistic missiles] probably allows Beijing to incapacitate much of Taiwan's navy and to ground or destroy large portions of the air force in a surprise missile assault and follow-on barrages."5 These are stark, sobering conclusions. Equally troubling is growing evidence that China has turned its attention to Japan, home to some of the largest naval and air bases in the world. Beijing has long worried about Tokyo's potential role in a cross-strait conflagration. In particular, Chinese analysts chafe at the apparent American freedom to use the Japanese archipelago as a springboard to intervene in a Taiwan contingency. In the past, China kept silent on what the People's Liberation Army (PLA) would do in response to Japanese logistical support of U.S. military operations. **Recent PLA publications**, in contrast, **suggest** that the logic of **missile coercion** **against Taiwan could be** readily **applied** **to U.S.** forward **presence** in Japan. The writings convey a **high degree of confidence** that China's missile forces could compel Tokyo to limit American use of naval bases while selectively destroying key facilities on those bases. These doctrinal developments demand close attention from Washington and Tokyo, lest the transpacific alliance be caught flat-footed in a future crisis with Beijing. This article is a first step toward better understanding how the Chinese evaluate the efficacy of missile coercion against American military targets in Japan. This article focuses narrowly on Chinese assessments of U.S. naval bases in Japan, excluding the literature on such other key locations as the Kadena and Misawa air bases. The writings on the American naval presence are abundant and far more extensive than studies on the land and air components of U.S. basing arrangements. The dispatch of two carrier battle groups to Taiwan's vicinity during the 1996 cross-strait crisis stimulated Beijing's reevaluation of its military strategy toward the island. Not surprisingly, the Chinese are obsessed with the U.S. aircraft carrier, including the facilities and bases that support its operations. It is against this rich milieu that this study explores how the Chinese conceive their missile strategy to complicate American use of military bases along the Japanese archipelago. This article first explores the reasons behind Beijing's interest in regional bases and surveys the Chinese literature on the U.S. naval presence in Japan to illustrate the amount of attention being devoted to the structure of American military power in Asia. **Chinese analysts see U.S. dependence on a few locations for power projection as a major vulnerability. Second, it turns to Chinese doctrinal publications, which furnish astonishing details as to how the PLA might employ ballistic missiles** to complicate or deny U.S. use of Japanese port facilities. Chinese defense planners place substantial faith in the coercive value of missile tactics. Third, the article assesses China's conventional theater ballistic missiles that would be employed against U.S. regional bases. Fourth, it critiques the Chinese writings, highlighting some faulty assumptions about the anticipated effects of missile coercion. Finally, the study identifies some key operational dilemmas that the U.S.-Japanese alliance would likely encounter in a PLA missile campaign. EXPLAINING CHINA'S INTEREST IN REGIONAL BASES **Taiwan remains the** animating **force behind China's** strategic **calculus** with respect to regional bases in Asia. **Beijing's inability to respond** **to** the display of U.S. naval power at the height of **the** **1996** **Taiwan** Strait **crisis** proved highly embarrassing. There is evidence that the PLA had difficulty in monitoring the movement of the two carrier battle groups, much less in offering its civilian leaders credible military options in response to the carrier presence. This galling experience **steeled Beijing's resolve** **to preclude U.S.** naval **deployments near Taiwan** in a future crisis. Notably, the Yokosuka-based USS Independence (CV 62) was the first carrier to arrive at the scene in March 1996, cementing Chinese expectations that Washington would dispatch a carrier from Japan in a contingency over Taiwan. Beyond Taiwan, other territorial disputes along China's nautical periphery could involve U.S. naval intervention. A military crisis arising from conflicting Sino-Japanese claims over the Senkaku (Diaoyu) islands northwest of Taiwan could compel an American reaction. While doubts linger in some Japanese policy circles as to whether foreign aggression against the islands would trigger Washington's defense commitments as stipulated by the U.S.-Japanese security treaty, joint allied exercises and war games since 2006 suggest that the U.S. military is closely watching events in the East China Sea. Farther south, **Chinese territorial claims over large swaths of the South China Sea could also be sources of regional tensions. If a local tussle there escalated into a larger conflagration that threatened international shipping**, the U.S. Navy might be ordered to maintain freedom of navigation. In both scenarios, the U.S. carrier based in Japan and other strike groups operating near Asian waters would be called upon as first responders. Concrete territorial disputes that have roiled Asian stability are not the only reasons that American naval power would sortie from regional bases to the detriment of Chinese interests. More abstract and esoteric dynamics may be at work. For example, Chinese leaders fret about the so-called Malacca dilemma. China's heavy dependence on seaborne energy supplies that transit the Malacca Strait has set off Chinese speculation that the United States might seek to blockade that maritime choke point to coerce Beijing.6 This insecurity stems less from judgments about the possibility or feasibility of such a naval blockade than from the belief that a great power like China should not entrust its energy security to the fickle goodwill of the United States. If the U.S. Navy were ever called upon to fulfill an undertaking of such magnitude, forward basing in Asia would undoubtedly play a pivotal role in sustaining what could deteriorate into a protracted blockade operation. Chinese analysts have also expressed a broader dissatisfaction with America's self-appointed role as the guardian of the seas. Sea-power advocates have vigorously pushed for a more expansive view of China's prerogatives along the maritime periphery of the mainland. They bristle at the U.S. Navy's apparent presumption of the right to command any parcel of the ocean on earth, including areas that China considers its own nautical preserves. Some take issue with the 2007 U.S. maritime strategy, a policy document that baldly states, "We will be able to impose local sea control wherever necessary, ideally in concert with friends and allies, but by ourselves if we must."7 Lu Rude, a former professor at Dalian Naval Academy, cites this passage as evidence of U.S. "hegemonic thinking." He concludes, "Clearly, what is behind 'cooperation' is America's interests, having 'partners or the participation of allies' likewise serves America's global interests."8 Some Chinese, then, object to the very purpose of U.S. sea power in Asia, which relies on a constellation of regional bases for its effects to be felt (see map). Long-standing regional flash points and domestic expectations of a more assertive China as it goes to sea suggest that Beijing's grudging acceptance of U.S. forward presence could be eroding even more quickly than once thought. Against this backdrop of increasing Chinese ambivalence toward American naval power, U.S. basing arrangements in Japan have come into sharper focus. CHINESE VIEWS OF U.S. NAVAL BASES IN JAPAN Some Chinese strategists appraise Washington's military posture in the Asia-Pacific region in stark geopolitical terms. Applying the "defense perimeter of the Pacific" logic elaborated by Secretary of State Dean Acheson in the early Cold War, they see their na - tion enclosed by concentric, layered "island chains." The United States and its allies, they argue, can encircle China or blockade the Chinese mainland from island strongholds, where powerful naval expeditionary forces are based. Analysts who take such a view conceive of the island chains in various ways. Yu Yang and Qi Xiaodong, for example, describe U.S. basing architecture in Asia as a "three line configuration [...]."9 The first line stretches in a sweeping arc from Japan and South Korea to Diego Garcia in the Indian Ocean, forming a "zone of forward bases[...]." This broad notion that the U.S. presence in the western Pacific and the Indian Ocean constitutes a seamless, interlocking set of bases is widely shared in Chinese strategic circles.10 The second line connects Guam and Australia. The last line of bases runs north from Hawaii through Midway to the Aleutians, terminating at Alaska. While these island chains may bear little resemblance to actual U.S. thinking and planning, that the Chinese pay such attention to the geographic structure of American power in Asia is quite notable. These observers discern a cluster of mutually supporting bases, ports, and access points along these island chains. Among the networks of bases in the western Pacific, those located on the Japanese archipelago-the northern anchor of the first island chain-stand out, for the Chinese. Modern Navy, a monthly journal published by the Political Department of the People's Liberation Army Navy, produced a seven-part series on Japan's Maritime Self-Defense Force in 2004 and 2005. Notably, it devoted an entire article to Japan's main naval bases, including Yokosuka, Sasebo, Kure, and Maizuru.11 The depth of the coverage of these bases is rather remarkable, especially when compared to the sparse reporting on similar topics in the United States and in Japan. Perhaps no other place captures the Chinese imagination as much as Yokosuka, which analysts portray as the centerpiece of U.S. basing in Asia.12 One analysis depicts a "Northeast Asian base group [...]" radiating outward from Yokosuka to Sasebo, Pusan, and Chinhae.13 Writers provide a wide range of details about the Yokosuka naval base, including its precise location, the surrounding geography, the number of piers (particularly those suitable for aircraft carriers), the types and number of maintenance facilities, and the storage capacity of munitions, fuel, and other supply depots.14 Wu Jian, for instance, finds the geographic features of Yokosuka comparable to those of Dalian, a major base of the Chinese navy's North Sea Fleet.15 Beyond physical similarities, Yokosuka evokes unpleasant memories for the Chinese. One commentator recalls the U.S. transfer of 203 mm heavy artillery from Yokosuka to Nationalist forces on Jinmen during the 1958 Taiwan Strait crisis.16 Tracking more recent events, another observer notes that the Kitty Hawk Strike Group's deployments from Yokosuka to waters near Taiwan invariably coincided with the presidential elections on the island, in 2000, 2004, and 2008.17 As Pei Huai opines, "Yokosuka has all along irritated the nerves of the Chinese people."18 Moreover, Chinese analysts are keenly aware of Yokosuka's strategic position. As Du Chaoping asserts: Yokosuka is the U.S. Navy's main strategic point of concentration and deployment in the Far East and is the ideal American stronghold for employing maritime forces in the Western Pacific and the Indian Ocean regions. A carrier deployed there is akin to the sharpest dagger sheathed in the Western Pacific by the U.S. Navy. It can control the East Asian mainland to the west and it can enter the Indian Ocean to the southwest to secure Malacca, Hormuz, and other important thoroughfares.19 Ma Haiyang concurs: The Yokosuka base controls the three straits of Soya, Tsugaru, Tsushima and the sea and air transit routes in the Indian Ocean. As the key link in the "island chain," it can support ground operations on the Korean Peninsula and naval operations in the Western Pacific. It can support combat in the Middle East and Persian Gulf regions while monitoring and controlling the wide sea areas of the Indian Ocean. Its strategic position is extremely important.20 It is notable that both Du and Ma conceive of Yokosuka as a central hub that tightly links the Pacific and Indian oceans into an integrated theater of operations. Intriguingly, some Chinese commentators view Yokosuka as the front line of the U.S.-Japanese defense cooperation on missile defense. They worry that Aegis-equipped destroyers armed with ballistic-missile-defense (BMD) systems based in Yokosuka could erode China's nuclear deterrent. Indeed, analysts see concentrations of sea-based BMD capabilities falling roughly along the three island chains described above. Ren Dexin describes Yokosuka as the first line of defense against ballistic missiles, while Pearl Harbor and San Diego provide additional layers.21 Yokosuka is evocatively portrayed as the "forward battlefield position" (...), the indispensable vanguard for the sea-based BMD architecture.22 For some Chinese, these concentric rings or picket lines of sea power appear tailored specifically to bring down ballistic missiles fired across the Pacific from locations as diverse as the Korean Peninsula, 1mainland China, India, or even Iran.23 Specifically, Aegis ships in Yokosuka, Pearl Harbor, and San Diego would be positioned to shoot down missiles in their boost, midcourse, and terminal phases, respectively.24 Chinese observers pay special attention to Aegis deployments along the first island chain. Some believe that Aegis ships operating in the Yellow, East, and South China seas would be able to monitor the launch of any long-range ballistic missile deployed in China's interior and perhaps to intercept the vehicle in its boost phase. Dai Yanli warns, "Clearly, if Aegis systems are successfully deployed around China's periphery, then there is the possibility that China's ballistic missiles would be destroyed over their launch points."25 Ji Yanli, of the Beijing Aerospace Long March Scientific and Technical Information Institute, concurs: "If such [seabased BMD] systems begin deployment in areas such as Japan or Taiwan, the effectiveness of China's strategic power and theater ballistic-missile capabilities would weaken tremendously, severely threatening national security."26 Somewhat problematically, the authors seemingly assume that Beijing would risk its strategic forces by deploying them closer to shore, and they forecast a far more capable Aegis fleet than is technically possible in the near term. The indispensability of the ship-repair and maintenance facilities at Yokosuka emerges as another common theme in the Chinese literature. Analysts in China often note that Yokosuka is the only base west of Hawaii that possesses the wherewithal to handle major carrier repairs. Some have concluded that Yokosuka is irreplaceable as long as alternative sites for a large repair station remain unavailable. Li Daguang, a professor at China's National Defense University and a frequent commentator on naval affairs, casts doubt on Guam as a potential candidate, observing that the island lacks the basic infrastructure and economies of scale to service carriers.27 China's Jianchuan Zhishi (Naval and Merchant Ships) published a translated article from a Japanese military journal, Gunji Kenkyu (Japan Military Review), to illustrate the physical limits of Guam as a permanent home port for carriers.28 Chinese analysts also closely examine Sasebo, the second-largest naval base in Japan. Various commentators call attention to its strategic position near key sea-lanes and its proximity to China.29 As Yu Fan notes, "This base is a large-scale naval base closest to our country. Positioned at the intersection of the Yellow Sea, the East China Sea, and the Sea of Japan, it guards the southern mouth of the Korea Strait. This has very important implications for controlling the nexus of the Yellow Sea, the East China Sea, and the Sea of Japan and for blockading the Korea Strait."30 It is clear, then, that Chinese strategists recognize the importance of U.S. naval bases in Japan for fulfilling a range of regional and extraregional responsibilities. Indeed, some believe that the American strategic position in Asia hinges entirely on ready military access to bases on the Japanese islands. Tian Wu argues that without bases in Japan, U.S. forces would have to fall back to Guam or Hawaii. Tian bluntly asserts: If the U.S. military was ever forced to withdraw from Okinawa and Japan, then it would be compelled to retreat thousands of kilometers to set up defenses on the second island chain. Not only would it lose tremendous strategic defensive depth, but it would also lose the advantageous conditions for conducting littoral operations along the East Asian mainland while losing an important strategic relay station to support operations in the Indian Ocean and the Middle East through the South China Sea.31 This emerging discourse offers several clues about Beijing's calculus in regard to U.S. naval basing arrangements in Japan. Chinese strategists see these bases as collectively representing both a threat to Chinese interests and a critical vulnerability for the United States. Bases in Japan are the most likely locations from which the United States would sortie sea power in response to a contingency over Taiwan. At the same time, the Chinese are acutely aware of the apparent American dependence on a few bases to project power. Should access to and use of these bases be denied for political or military reasons, they reason, Washington's regional strategy could quickly unravel. While the commentaries documented above are by no means authoritative in the official sense, they are clearly designed to underscore the strategic value and the precariousness of U.S. forward presence in Japan. U.S. BASES IN JAPAN AND CHINESE MISSILE STRATEGY Authoritative PLA documents correlate with this emerging consensus that U.S. bases on the Japanese home islands merit close attention in strategic and operational terms. Indeed, Chinese doctrinal writings clearly indicate that the American presence in Japan would likely be the subject of attack if the United States were to intervene in a cross-strait conflict. The unprecedented public availability of primary sources in China in recent years has opened a window onto Chinese strategic thought, revealing a genuinely competitive intellectual environment that has substantially advanced Chinese debates on military affairs. This growing literature has also improved the West's understanding of the PLA. In an effort to maximize this new openness in China, this article draws upon publications closely affiliated with the PLA, including those of the prestigious Academy of Military Science and the National Defense University, that address coercive campaigns against regional bases in Asia.32 Some are widely cited among Western military analysts as authoritative works that reflect current PLA thinking. Some likely enjoy official sanction as doctrinal guidance or educational material for senior military commanders. The authors of the studies are high-ranking PLA officers who are either leading thinkers in strategic affairs and military operations or boast substantial operational and command experience. These works, then, collectively provide a sound starting point for examining how regional bases in Asia might fit into Chinese war planning. Among this literature, The Science of Military Strategy stands out in Western strategic circles as an authoritative PLA publication. The authors, Peng Guangqian and Yao Youzhi, advocate an indirect approach to fighting and prevailing against a superior adversary in "future local wars under high-technology conditions."33 To win, the PLA must seek to avoid or bypass the powerful field forces of the enemy while attacking directly the vulnerable rear echelons and command structures that support frontline units. Using the human body as an evocative metaphor for the adversary, Peng and Yao argue, "As compared with dismembering the enemy's body step by step, destroying his brain and central nerve system is more meaningful for speeding up the course of the war."34 To them, the brain and the central nervous system of a war machine are those principal directing and coordinating elements without which the fighting forces wither or collapse. The aim, then, is to conduct offensive operations against the primary sources of the enemy's military power, what the authors term the "operational system." They declare, "After launching the war, we should try our best to fight against the enemy as far away as possible, to lead the war to enemy's operational base, even to his source of war, and to actively strike all the effective strength forming the enemy's war system."35 In their view, operational systems that manage command and control and logistics (satellites, bases, etc.), are the primary targets; they relegate tactical platforms that deliver firepower (warships, fighters, etc.) to a secondary status. To illustrate the effects of striking the source of the enemy's fighting power, Peng and Yao further argue: To shake the stability of enemy's war system so as to paralyze his war capabilities has already become the core of the contest between the two sides in the modern hightech local war. So, more attention should be paid to striking crushing blows against the enemy's structure of the operational system . . . especially those vulnerable points which are not easy to be replaced or revived, so as to make the enemy's operational system seriously unbalanced and lose initiative in uncontrollable disorder.36 The authors are remarkably candid about what constitutes the enemy's operational system. Particularly relevant to this study is their assertion that the supply system emerges as a primary target: The future operational center of gravity should not be placed on the direct confrontation with the enemy's assault systems. We should persist in taking the information system and support system as the targets of first choice throughout. . . . In regard to the supply system, we should try our best to strike the enemy on the ground, cut the material flow of his efficacy sources so as to achieve the effect of taking away the firewood from the caldron.37 Destruction of the supply system in effect asphyxiates the adversary. In order to choke off the enemy's capacity to wage war, Peng and Yao contend, a "large part of the supply systems must be destroyed."38 Their prescriptions for winning local high-tech wars suggest that the horizontal escalation of a conflict to U.S. regional bases in Asia is entirely thinkable. Even more troubling, some Chinese appear to envision the application of substantial firepower to pummel the U.S. forward presence. While The Science of Military Strategy should not be treated as official strategic guidance to the PLA, its conceptions of future conflict with a technologically superior adversary provide a useful framework for thinking about what a Chinese missile campaign against regional bases might entail. There is substantial evidence in Chinese doctrinal writings that PLA defense planners anticipate the possibility of a sizable geographic expansion of the target set, to include U.S. forward presence in East Asia. Although the documents do not explicitly refer to naval bases in Japan, they depict scenarios strongly suggesting that Yokosuka is a primary target. In the hypothetical contingencies posited in these writings, U.S. intervention is a critical premise, if not a given. In particular, Chinese planners expect Washington to order the deployment of carrier strike groups near China's coast, a prospect that deeply vexes Beijing. It is in this context of a highly stressful (though by no means inconceivable) scenario that U.S. military bases come into play in Chinese operational thinking. **For PLA planners, the primary aims are to deter, disrupt, or disable the employment of carriers** at the point of origin, namely, the bases from which carriers would sortie. Given the limited capability, range, and survivability of China's air and sea power, **most studies foresee the extensive use of long-range conventional ballistic missiles to achieve key operational objectives** against U.S. forward presence. In Intimidation Warfare, Zhao Xijun proposes several novel missile tactics that could be employed to deter the use of naval bases in times of crisis or war.39 Zhao proposes demonstration shots into sea areas near the enemy state to compel the opponent to back down. Zhao explains, "Close-in (near border) intimidation strikes involve firing ballistic missiles near enemy vessels or enemy states (or in areas and sea areas of enemy-occupied islands). It is a method designed to induce the enemy to feel that it would suffer an unbearable setback if it stubbornly pursues an objective, and thus abandons certain actions."40 One tactic that Zhao calls a "pincer, close-in intimidation strike" is particularly relevant to missile options against U.S. military bases. Zhao elaborates: "Pincer close-in intimidation strikes entail the firing of ballistic missiles into the sea areas (or land areas) near at least two important targets on enemy-occupied islands (or in enemy states). This enveloping attack, striking the enemy's head and tail such that the enemy's attention is pulled in both directions, would generate tremendous psychological shock."41 Zhao also proposes an "island over-flight attack" as a variation of the pincer strike. He states: For high-intensity intimidation against an entrenched enemy on an island, an island over-flight attack employs conventional ballistic missiles with longer range and superior penetration capabilities to pass over the enemy's important cities and other strategic targets to induce the enemy to sense psychologically that a calamity will descend from the sky. This method could produce unexpected effects.42 While these missile tactics are primarily aimed at coercing Taiwan, they could also, in theory, be applied to any island nation. Reminiscent of the 1996 crossstrait crisis, the PLA could splash single or multiple ballistic missiles into waters near Yokosuka (shot across Honshu Island, over major metropolitan cities) in the hopes that an intimidated leadership in Tokyo would stay out of a contingency over Taiwan, deny American access to military facilities, or restrict U.S. use of naval bases in Japan. Should deterrence through intimidation fail, the Chinese may seek to complicate U.S. naval operations originating from bases located in the Japanese home islands. The Science of Second Artillery Campaigns, the most authoritative work on the PLA's strategic rocket forces, furnishes astonishingly vivid details on the conditions under which China might seek to conduct conventional missile operations against outside intervention.43

#### Taiwan crisis is imminent and causes nuclear war

Colby et al 13

Elbridgc A. Colby. cochair, is a principal analyst and drvison lead for global strategic affairs at the Center for Naval Analyses (CNA). where he focuses on strateg deterrence, nuclear weapons, and related issues. Previously, he served as policy adviser to the secretary of defense’s representative for the new Strategic Arms Reduction Treaty, as an expert adviser to the Congressional Strategic Posture Commission, as a staff member on the President’s Commission on the Intdhgcnce Capa biLities of the US. Regarding WMD. and in a number of other government positions. Mr. Colby also serves or has served as a consultant to a number of U.S government bodies. He publishes and speaks regularly on strategic issues in the United States. Europe, and Asia. Mr. Colby is a graduate of Harvard College and Yale Law School and is a member of the Council on Foreign Rdations (term) and of the International Institute of Strategic Studies Abraham M. Denmark. cochair. is vice president for political and security affairs at the National Bure-au of Asian Research (NBR) and is an Asia-Pacific security adviser at the Center for Naval Analyses. He manages NBR research programs, dialogues, projects, and initiatives reLated to po. litical and security issues in the Asia-Pacific region. He has experience both inside and outside of government, having previously worked as a fellow at the Center for a New American Security and as country director for China affairs in the Office of the Secretary of Deknse. Mr. Denmark holds an MA. in international security from the Josef Korbel Schoel of International Studies at the University of Denver and has studied at China’s Foreign Atfairs University and Peking Universit, Nuclear Weapons and U.S.-China Relations, http://csis.org/files/publication/130307\_Colby\_USChinaNuclear\_Web.pdf

Taiwan. **Taiwan remains the single most plausible and dangerous source of tension and conflict between the United States and China.** Beijing continues to be set on a policy to prevent Taiwan’s independence, and the United States maintains the capability to come to Taiwan’s defense. **Although** the **tensions** across the Taiwan Strait have **subsided** since both Taipei and Beijing embraced a policy of engagement in 2008, **the situation remains combustible,** complicated, **by** rapidly-**diverging** cross-strait military **capabilities and persistent political disagreements**. Moreover, for the foreseeable future **Taiwan is the contingency in which** **nuclear weapons would most likely become a major factor**, **because the fate** of the island **is** **intertwined** both **with the** legitimacy of the **C**hinese **C**ommunist **P**arty **and** the reliability of **U.S. defense commitments** in the Asia-Pacific region.

#### So does conflict over the South China Sea

Rehman 13

Stanton Nuclear Security Fellow, Iskander Rehman was an associate in the Nuclear Policy Program at the Carnegie Endowment and a Stanton Nuclear Security Fellow. His research focuses on security and crisis stability in Asia, specifically the geopolitical ramifications of naval nuclearization in the Indian Ocean, 3/9/13, Dragon in a Bathtub: Chinese Nuclear Submarines and the South China Sea, http://carnegieendowment.org/2013/03/09/dragon-in-bathtub-chinese-nuclear-submarines-and-south-china-sea/fpjl

**Despite** America’s **best efforts to construct stronger ties with China, relations** in-between both countries **have been** repeatedly **buffeted by** a series of **tensions** and misunderstandings. Many of these frictions appear to have **resulted from** a more **assertive Chinese posture in the South China Sea.** Almost every week, Asian **headlines seem** to be **dominated by reports of** jingoistic **statements over disputed islets, or** of a **renewed bout of aggressive maneuvering** by boats from one of Beijings numerous maritime agencies. When attempting to explain this upsurge in Chinese pugnacity, **analysts** have **pointed to** the rising power's selective interpretation of the law of the sea and growing **unwillingness to compromise** over what it calls its “blue national soil”, particularly when confronted with an increasingly intransigent domestic populace. Others have pointed to the more immediately tangible benefits to be derived from the presence of numerous offshore oil and gas deposits within contested waters. Strangely enough, however, one of the principal explanations for China’s increased prickliness towards foreign military presence within its maritime backyard has yet to be clearly articulated. Indeed, not only is the South China Sea one of the world’s busiest trade thoroughfares, it also happens to be the roaming pen of China’s emerging ballistic missile submarine fleet, which is stationed at Sanya, on the tropical Island of Hainan. The United States, with its array of advanced anti-submarine warfare assets and hydrographic research vessels deployed throughout the region, gives Beijing the unwelcome impression that Uncle Sam can’t stop peering into its nuclear nursery. When Chinese naval strategists discuss their maritime environs, the sentiment they convey is one of perpetual embattlement. Pointing to the US’s extended network of allies in the Indo-Pacific region, and to their own relative isolation, Chinese strategists fear that Beijing’s growing navy could be ensnared within the first island chain-a region which they describe as stretching from Japan all the way to the Indonesian archipelago. Applying this maritime siege mentality to naval planning; they fret that the US Navy could locate and neutralize their fledgling undersea deterrent in the very first phases of conflict, before it even manages to slip through the chinks of first island chain. This concern helps explain China's growing intolerance to foreign military activities in the South China Sea. Tellingly, some of the most nerve-wracking **standoffs involving US and Chinese forces** have **unfolded in close proximity** to Hainan. The infamous Ep-3 crisis, during which a US spy plane entered into collision with a Chinese fighter jet, occurred while the plane’s crew was attempting to collect intelligence on naval infrastructure development. Similarly, the USNS Impeccable incident, during which a US hydrographic vessel was dangerously harassed by five Chinese ships, took place approximately seventy miles to the south of Hainan. During the confrontation, Chinese sailors reportedly attempted to unhook the Impeccable’s towed acoustic array sonars. In public, China's protests over foreign military activities are couched in territorial terms. In private, however, **Chinese policymakers readily acknowledge the centrality of the nuclear dimension**. Thus in the course of a discussion with a former Chinese official, I was told that “even though territorial issues are of importance, our major concern is the sanctity of our future sea-based deterrent.” He then went on to describe, with a flicker of amusement, how fishermen off the coast of Hainan regularly snag US sonars in their nets, and are encouraged to sell them back to the local authorities in exchange for financial compensation. Of course, such cat and mouse games are nothing new-and are perfectly legal- provided they occur within international waters or airspace. During the Cold War, American and Soviet ships would frequently conduct forward intelligence gathering missions, sometimes in very close proximity to each others’ shores. At the time, American thinkers cautioned that such **risky behavior could** potentially **lead to misinterpretation and nuclear disaster.** Unlike the Soviets, however, who could confine the movements of their boomers to the frigid, lonely waters of the Barents and Okhotsk seas, the Chinese have chosen to erect their nuclear submarine base smack-bang in the middle of one of the world’s busiest maritime highways. Needless to say, this location is hardly ideal. When it comes to picking strategic real-estate in their near seas, the Chinese have but a limited roster of options. After all, their maritime backyard is girded by a sturdy palisade of states which increasingly view China’s meteoric rise, and attendant truculence at sea, with a mixture of alarm and dismay. Like a dragon caught floundering in a bathtub, China’s naval ambitions are simply too broad and grandiose for its constricted maritime geography. This perceived lack of strategic depth provides a partial explanation to Beijing’s increased obduracy over territorial disputes in the South China Sea. In order to better protect its valuable subsurface assets, China aims to establish a ring of maritime watch towers or bastions around Hainan. Absolute control over the remote Spratly islands, in addition to the more proximate Paracels, would greatly facilitate this concentric defensive configuration. Until not long ago, China’s strategic submarine force wasn’t really taken seriously. Their lone 0-92 Xia class boat was deemed too antiquated-and noisy-to be anything more than a symbol of Beijing’s desire for great power status. Some observers had ventured that China would be content to rely almost exclusively on its rapidly modernizing land-based missile system for its deterrent. Recent developments, however, suggest that this may be about to change. In its latest report to Congress, the US-China Economic and Security Review Commission stated that China could soon equip its new class of Jin submarines with the JL-2 ballistic missile, which has a range of approximately 4 600 miles. This would enable Beijing, the report adds, to establish a “near-continuous at-sea strategic deterrent”.  In all likelihood this force will be berthed at Hainan. The second **Obama** Administration **will** therefore **have the unenviable task of dealing with tensions in a region which is not only riddled with territorial divisions, but is** also **rapidly morphing into one of the world’s most sensitive nuclear hotspots.**

#### Their defense doesn’t apply

#### Chinese fear of US cyber unilateralism means escalation is probable

VornDick 7/30/12

[Wilson VornDick is a lieutenant commander in the U.S. Navy, where he is assigned to the Pentagon. Previously, he worked at the Chinese Maritime Studies Institute at the U.S. Naval War College. http://nationalinterest.org/commentary/the-real-us-chinese-cyber-problem-8796?page=1 ETB]

Yet, Chinese media reports have filled some of the void with regards to ROE(交战规则 jiaozhan guize). Despite a lack of battle-tested ROE experience, China has linked ROE with cyber warfare and basically has asserted that the United States lacks a legal basis for any unilateral cyber rules of engagement of its own. This is because the Chinese fear that unilateral action by the United States, such as establishing a cyber ROE, would set the stage for future U.S. preemptive action in anticipation of a cyber attack that could target China.¶ Cyber in China’s Recent Defense White Paper¶ These pronouncements come at the heels of China’s recently published defense white paper that publicly promulgates its military’s intentions. “Cyber” is mentioned only twice in the entire paper. China did recognize however, that “changes in the form of war from mechanization to informationization are accelerating,” while “major powers are vigorously developing new and more sophisticated military technologies so as to ensure that they can maintain strategic superiorities in international competition in such areas as . . . cyber space.” China also unequivocally stated in the document that it would “counterattack” if attacked.¶ Troubling Prospects for U.S.-Chinese Cyber Operations¶ This is particularly troubling for Chinese and American authorities because it is unclear whether or not they could manage their cyber responses in a measured and proportional way if an unofficial or official outbreak of digital force, intentional or not, were to occur. The severity of this issue is intensified by the lack of official Chinese pronouncements or transparency on their cyber operations. Clandestine cyber units, such as the PLA-sponsored Unit 61398 in Shanghai, operate with destructive global reach, adding a layer of uncertainty to an illicit cyber response.¶ After a thorough analysis of the defense white paper, it is clear that the Chinese leadership is reticent to articulate their intentions in cyber warfare. For defense purposes, this is troublesome for Washington. There is a variety of political and military reasons for this course of action. Perhaps this Chinese reluctance in setting the guidelines of response stems from the lack of pressure from the United States and other nations. In any case, it is doubtful that the leadership would state a different course of action than its professed desire to conduct only defensive and nonaggressive operations.

#### Cyber stimulates risk taking and lowers conflict inhibition

Dobbins et al. ‘11

[Ambassador James F. Dobbins, a veteran diplomat and the current director of the RAND International Security and Defense Policy Center as well the US special representative for Afghanistan and Pakistan. David C. Gompert was Principal Deputy Director of National Intelligence from 2009 to 2010. During 2010, he served as Acting Director of National Intelligence, in which capacity he provided strategic oversight of the U.S. Intelligence Community, and acted as the President's chief intelligence advisor. Gompert is currently Distinguished Visiting Professor for National Security Studies at the United States Naval Academy, and Adjunct Senior Fellow of the RAND Corporation. He is a Trustee of Hopkins House Academy, a Director of the Rufus Porter Museum, a Director of Global Integrated Security (USA), Inc., a member of the Advisory Board of the Naval Academy Center for Cyber Security Studies, and Chairman of the Advisory Board of the Institute for the Study of Early Childhood Education. David A. Shlapak, Senior International Policy Analyst @ RAND. Andrew Scobell is a senior political scientist at the RAND Corporation. Prior to this he was an associate professor of international affairs at the George H. W. Bush School of Government and Public Service (with tenure) and director of the China certificate program at Texas A&M University in College Station, Texas. From 1999 until 2007, he was associate research professor in the Strategic Studies Institute at the U.S. Army War College and adjunct professor of political science at Dickinson College. http://www.rand.org/content/dam/rand/pubs/occasional\_papers/2011/RAND\_OP344.pdf ETB]

**The difficulties of direct defense could be greatly accelerated by Chinese** development and ¶ **use of cyber-attack** and ASAT weapons, given the dependence of U.S. forces and operating ¶ concepts on computer-networked and space-based C4ISR. For this reason, the PLA appears to ¶ think that hostilities in space and cyber-space would favor China, and so might initiate them. ¶ At the same time, as China extends the reach of its own forces and C4ISR into the Pacific, they will become vulnerable to U.S. cyber-attack and ASAT. In any case, **any Sino-U.S. armed** ¶ **conflict will be increasingly affected if not decided by warfare in these new domains.** ¶ **The erosion of capabilities for direct defense will push the U**nited **S**tates **toward enhanced** ¶ **weapons**, ranges, geography, and targets both to regain survivability and to strike Chinese ¶ forces, launchers, sensors, and other capabilities on the mainland (or elsewhere in the region ¶ outside of the immediate theater). In addition, as the PLA develops cyber and ASAT capabilities but also comes to rely more on advanced C4ISR, the United States will have to consider ¶ striking Chinese satellites and computer networks. These trends will thus lead both sides to ¶ widen their choice of targets in order to achieve dominance over any particular geographic ¶ objective, however limited. ¶ **The increasing difficulty in ensuring direct defense can be consequential even if Sino-U.S.** ¶ **hostilities are unlikely, for they could stimulate Chinese risk-taking, increase U.S. inhibitions,** ¶ **and weaken the resolve of U.S. allies and China’s neighbors in facing a China more insistent** ¶ **on settling disputes on its terms.** These trends are the result of underlying general technological progress, sustainable growth in military spending, PLA reform and doctrinal adaptation, ¶ and geographic distances for China and the United States. On the other hand, most of China’s ¶ neighbors are growing economically and in technological sophistication, and some may choose ¶ to keep pace in quality if not quantity with Chinese advances in the military field.

### 1AC - Plan

#### The United States federal government should substantially increase restrictions on the war powers authority of the president of the United States by removing the authority to authorize the preemptive use of large-scale cyber-attacks, except in direct support of authorized United States military operations.

### 1AC - Solvency

#### Contention 3 is solvency

#### First, norm-setting — all eyes are on the U.S. —other countries model our use of OCOs — clear restrictions on use are essential

Bradbury 11

Assistant Attorney General for the Office of Legal Counsel

(Steven, The Developing Legal Framework for Defensive and Offensive Cyber Operations, http://harvardnsj.org/wp-content/uploads/2011/02/Vol.-2\_Bradbury\_Final1.pdf)

Evolving customary law. This approach also accommodates the reality that **how the U.S. chooses to use its armed forces will significantly influence the development of customary international law.** As the label implwies, **customary law can evolve depending on the accepted conduct of major nations like the United States. The real-world practice of the United States in adapting** the use of its military **to the new challenges raised by computer warfare will** (and should) **help clarify the accepted customs of war in areas where the limits are not clearly established today.** And if you just review the literature on cyber war, you quickly see that that’s where we are: precisely how the laws and customs of war should apply to offensive cyber operations is not yet crystallized in key respects. For example, there aren’t always bright lines to tell us when a cyber attack on computer systems constitutes an “armed attack” or a “use of force” that justifies a nation in launching a responsive military strike under Article 51 of the U.N. Charter. Some questions are easy: Hacking into a sensitive government computer system to steal information is an act of espionage, not an armed attack. It’s clearly not prohibited by the laws and customs of war. On the other hand, if the cyber intrusion inflicts significant physical destruction or loss of life by causing the failure of critical infrastructure, like a dam or water supply system, then it obviously would constitute an armed attack under the law of war and would justify a full military response if it could be attributed to a foreign power. Where committed as an offensive act of aggression, such an attack may violate international law. If significant enough, the effect of the attack will determine its treatment, not necessarily whether the attack is delivered through computer lines as opposed to conventional weapons systems. In these cases, the laws and customs of war provide a clear rule to apply. But there will be gray areas in the middle. Thus, it’s far less clear that a computer assault that’s limited to deleting or corrupting data or temporarily disabling or disrupting a computer network or some specific equipment associated with the network in a way that’s not life threatening or widely destructive should be considered a use of force justifying military retaliation, even if the network belongs to the military or another government agency. This was the case with the “distributed denial of service” attacks experienced by Estonia in 2007, which severely disrupted the country’s banking and communications systems. Suspecting that Russia was behind it, Estonia suggested that NATO declare that Estonia’s sovereignty had been attacked, which would have triggered the collective self-defense article of the NATO Treaty, but that suggestion was rebuffed on the ground that a cyber attack is not a clear military action.12 There’s an echo of that reasoning in Article 41 of the U.N. Charter, which says that a “complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications” is not a “measure . . . involving armed force.” And what about Stuxnet? As I understand it from public reports, Stuxnet was a computer worm that found its way into the systems controlling Iran’s nuclear program and gave faulty commands causing the destruction of the centrifuges used for enriching uranium. Suppose President Ahmadinejad claimed that Israel was behind the Stuxnet worm and claimed that Stuxnet constituted an armed attack on Iran that justified a military response against Israel. I suspect the United States would disagree. At the same time, when it comes to a cyber attack directed against U.S. computer systems, I certainly want the President to have leeway in determining whether or not to treat the attack as a use of force that supports military retaliation. Making such judgments is a traditional power exercised by the President, and I think he retains that leeway. Similarly, I submit, it’s not clearly established that a cyber attack aimed at disrupting a server or Web site located in a neutral country or in a country outside a theater of open hostilities would be a violation of that country’s neutrality. The server might be a valid military target because it’s being used for the communications or command and control of the enemy fighters in the area of hostilities (after all, al Qaeda regularly uses the Internet in planning and ordering operations). The server might have no connection to the host country’s military, government, or critical infrastructure, and it might be readily targeted for a computer attack without inflicting widespread damage on unrelated systems used for civilian purposes. Such a focused cyber operation — with little physical impact beyond the destruction of data or the crippling of a server — is very different from the kind of physical violation of territory — such as a conventional troop incursion or a kinetic bombing raid — that we ordinarily think of as constituting an affront to neutrality. Although every server has a physical location, the Internet is not segmented along national borders, and the enemy may gain greater tactical advantage from a server hosted half way around the world than from one located right in the middle of hostilities. The targeting of a server in a third country may well raise significant diplomatic difficulties (and I wouldn’t minimize those), but I don’t think the law-of-war principle of neutrality categorically precludes the President from authorizing such an operation by an execute order to Cyber Command. 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 U**nited **S**tates 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.

#### Norms are essential to solve — they can’t be created unless OCOs are addressed

Goldsmith 10

, Professor of Law at Harvard, Can we stop the Cyber Arms Race, Jack Goldsmith teaches at Harvard Law School and is on the Hoover Institution's Task Force on National Security and Law. He was a member of a 2009 National Academies committee that issued the report "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.", http://articles.washingtonpost.com/2010-02-01/opinions/36895669\_1\_botnets-cyber-attacks-computer-attacks

In a speech this month on "Internet freedom," Secretary of State Hillary **Clinton decried the cyberattacks** that threaten U.S. economic and national security interests. "Countries or individuals that engage in cyber attacks should face consequences and international condemnation," she warned, alluding to the China-Google kerfuffle. **We should "create norms** of behavior among states **and encourage respect for the** global **networked commons**." Perhaps so. But **the problem with Clinton's call for** accountability and **norms** on the global network -- a call frequently heard in policy discussions about cybersecurity -- **is the enormous array of cyberattacks originating from the U**nited **S**tates. **Until we acknowledge these** attacks **and signal how we might control them, we cannot make progress on preventing cyberattacks emanating from other countries.** An important weapon in the cyberattack arsenal is a botnet, a cluster of thousands and sometimes millions of compromised computers under the ultimate remote control of a "master." Botnets were behind last summer's attack on South Korean and American government Web sites, as well as prominent attacks a few years ago on Estonian and Georgian sites. They are also engines of spam that can deliver destructive malware that enables economic espionage or theft. **The U**nited **S**tates **has the most**, or nearly the most, **infected botnet computers and is thus the country from which a good chunk of botnet attacks stem**. The government could crack down on botnets, but doing so would raise the cost of software or Internet access and would be controversial. So it has not acted, and the number of dangerous botnet attacks from America grows. The United States is also a leading source of "hacktivists" who use digital tools to fight oppressive regimes. Scores of individuals and groups in the United States design or employ computer payloads to attack government Web sites, computer systems and censoring tools in Iran and China. These efforts are often supported by U.S. foundations and universities, and by the federal government. Clinton boasted about this support seven paragraphs after complaining about cyberattacks. Finally, the U.S. government has perhaps the world's most powerful and sophisticated offensive cyberattack capability. This capability remains highly classified. But the New York Times has reported that the Bush administration used cyberattacks on insurgent cellphones and computers in Iraq, and that it approved a plan for attacks on computers related to Iran's nuclear weapons program. And the government is surely doing much more. "We have U.S. warriors in cyberspace that are deployed overseas" and "live in adversary networks," says Bob Gourley, the former chief technology officer for the Defense Intelligence Agency. These warriors are now under the command of Lt. Gen. Keith Alexander, director of the National Security Agency. The NSA, the world's most powerful signals intelligence organization, is also in the business of breaking into and extracting data from offshore enemy computer systems and of engaging in computer attacks that, in the NSA's words, "disrupt, deny, degrade, or destroy the information" found in these systems. When the Obama administration created "cyber command" last year to coordinate U.S. offensive cyber capabilities, it nominated Alexander to be in charge. Simply put, **the U**nited **St**ates **is** in a big way **doing the** very **things** that **Clinton criticized**. We are not, like the Chinese, stealing intellectual property from U.S. firms or breaking into the accounts of democracy advocates. But we are aggressively using the same or similar computer techniques for ends we deem worthy. Our potent offensive cyber operations matter for reasons beyond the hypocrisy inherent in undifferentiated condemnation of cyberattacks. Even if we could stop all cyberattacks from our soil, we wouldn't want to. On the private side, hacktivism can be a tool of liberation. On the public side, the best defense of critical computer systems is sometimes a good offense. "My own view is that the only way to counteract both criminal and espionage activity online is to be proactive," Alexander said last year, adding that if the Chinese were inside critical U.S. computer systems, he would "want to go and take down the source of those attacks." Our **adversaries are aware** of our prodigious and growing offensive cyber capacities and exploits. In a survey published Thursday by the security firm McAfee, more **i**nformation **t**echnology **experts** from critical infrastructure firms **around the world expressed concern about the U**nited **St**ates **as a source of** computer network **attacks** than about any other country. **This** awareness, **along with our vulnerability** to cyberattacks, **fuels a dangerous public and private cyber arms race in an arena where** the **offense** already **has a natural advantage**.

#### It’s reverse causal — lack of norms guarantee escalatory conflict — the U.S. is key

Lewis 11

Senior Fellow at CSIS (James Andrew, Confidence-building and international agreement in cybersecurity, citizenlab.org/cybernorms2012/Lewis2011.pdf)

**Alternatives to a formal cyber treaty** began to appear as early as 2008. Rejecting formal treaties, these alternatives **drew upon the experience of global efforts to control proliferation to develop a generalized model applicable to cybersecurity. Instead of a binding legal commitment, they proposed that states develop norms for responsible state behaviour in cyberspace. Non-proliferation provides many examples of non-binding norms that exercise a powerful influence on state behaviour. Norms shape behaviour and limit the scope of conflict. Norms create expectations and understandings among states on international behaviour, a framework for relations that provides a degree of predictability in interactions** in security, trade or politics. In this context, cybersecurity becomes the ability of states to protect their national sovereignty and advance their national interests. Cybersecurity creates new challenges for international security, as states are bound more closely together and as the perception of “transnational” risk increases, but it is largely a still undefined element in this web of relationships among states. **The idea of a norms-based approach has growing international support and, as in the nonproliferation arena, widespread adoption of norms could pave the way for more formal agreements in the future**. In July 2010 a Group of Governmental Experts (GGE) convened by the United Nations Secretary-General was able to produce an agreed report on “Developments in the Field of Information and Telecommunications in the Context of International Security”. This was unprecedented; in addition to the inability of a treaty to win consensus, a previous GGE endeavour in 2004 had failed. But the 2010 report itself is only 1,200 words long. In contrast, the first GGE had reportedly produced lengthy and detailed drafts that failed to win consensus. The brevity of the 2010 report was one element of its success (and this is a useful guidepost for future GGEs on cybersecurity), but brevity is also an indicator of the larger problems that hamper building international consensus. The successful GGE conclusion in 2010 reflected a shared perception among the government experts that **the risk of cyberconflict had become a serious threat to international peace and stability and** that **the absence of international agreement increased the risk of a destabilizing cyber incident that could spiral into** a **larger and more damaging conflict**. The states represented on the GGE were united by a deep concern over the possibility of **unconstrained cyberwarfare** and how this **might escalate out of control into physical violence**. They agreed that discussions of **norms** and rules **for the use of force in cyberspace**, along with other CBMs, **would improve international security and the stability of both cyberspace and the international system.** Winning even limited GGE agreement was difficult. It should be noted however that public accounts from both academic and media sources have largely glossed over significant differences expressed within the 2010 GGE. While the experts agreed on the increasing cyber threat, there was, however, little else where there was common understanding. Some states believe that **existing international norms and laws are inadequate for cyberconflict**. Other states argue that the existing laws of armed conflict are sufficient for cybersecurity, and are deeply apprehensive of doing anything that would appear to constrain freedom of speech. A central issue, as is often the case in multilateral discussion, is the extent to which states might concede a degree of sovereignty in exchange for greater security.

#### Second it solves perception — Congressionally initiated restriction is necessary to reverse the signal of independent presidential authority— now is key

Dycus 10

Professor of National Security Law Stephen is a Professor of national security law at Vermont Law School, former member of the National Academies committee on cyber warfare, LLM, Harvard University, LLB, BA, Southern Methodist University, “Congress’ Role in Cyber Warfare,” Journal of National Security Law & Policy, 4(1), 2010, p.161-164, http://www.jnslp.com/read/vol4no1/11\_Dycus.pdf

In his celebrated concurring opinion in The Steel Seizure Case, **Justice Jackson cautioned that “only Congress itself can prevent power from slipping through its fingers.” 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. 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.** 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.” 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. 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 war**fare, **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.**

#### Congressional restrictions on OCOs send a global signal of cyber leadership that solves reckless use of OCOs

Bastby 12

Chairwoman of the American Bar Association’s Privacy and Computer Crime Committee (Judy, CEO of Global Cyber Risk, “U.S. Administration's Reckless Cyber Policy Puts Nation at Risk” June 4, 2012, http://www.forbes.com/sites/jodywestby/2012/06/04/u-s-administrations-reckless-cyber-policy-puts-nation-at-risk/2/)

Perhaps **more important than** being out of the cyber **coordination** loop**, is the how the U.S.’s attitude is being perceived** by others **in the international community**. If the U.S. were a member of IMPACT and taking an active role in the investigation, it would be upholding its role as a global cybersecurity power. Instead, **the U.S. appears as the shirking nation** state quietly **standing on the sidelines while being accused of engaging in cyberwar**fare tactics. “**People look to the U.S., Russia, and China for leadership and when the U.S. is absent, they will turn to the other two**,” observes Dr. Amin. **The** U.S. **Administration’s** **failure** to **develop a strong foreign policy** **with respect to cybersecurity** **reveals** **a** gross **lack of attention at the highest levels of** the U.S. **Government** to one of the country’s most vulnerable areas — the IT systems that underpin the functioning of our society and economy. This **failure begins at basic strategy levels and extends to** reckless **disregard for the consequences of** the risky covert **Stuxnet** operation and failure to secure classified information about the program. For example, in May 2011, government delegations from around the world gathered in Geneva for the World Summit on the Information Society (WSIS), one of the most important communications and technology conferences globally. Noticeably, the U.S. did not have a delegation present. Yet, it was during the WSIS event that the U.S. Administration chose to release its International Strategy for Cyberspace – from Washington, D.C. rather than Geneva. WSIS participants were dumbstruck. For the few private sector Americans who were present, including myself, it was embarrassing. If in fact the Administration did authorize targeting Iranian nuclear systems with Stuxnet and/or Flame, it was a dangerous and reckless decision, especially since the U.S. Government has no idea how many computers in America may be infected with malware capable of being activated by Iran or one of its allies in retaliation. Such “backdoor” malware is capable of having enormous consequences to life and property. A similar CIA covert operation successfully destroyed a Soviet pipeline. In 1982, President Reagan approved a plan to transfer software used to run pipeline pumps, turbines, and valves to the Soviet Union that had embedded features designed to cause pump speeds and valve settings to malfunction. The plot was revealed in a 2004 Washington Post article by David Hoffman in advance of its discussion in former Air Force Secretary Thomas C. Reed’s book, At the Abyss: An Insider’s History of the Cold War. Reed recalled to Hoffman that, “The result was the most monumental non-nuclear explosion and fire ever seen from space.” Unlike Stuxnet, however, the program remained classified for 22 years until the CIA authorized Reed to discuss it in his book. Sanger’s information came from loose-lipped persons involved with the Stuxnet operation. Before pulling a trigger (or launching malware) a nation should assess its strengths and resources and its correlation of vulnerabilities, which, in 2012, includes understanding what an adversary can do when firing back using cyber capabilities. In addition, before launching covert operations, such as Stuxnet, a nation also should ensure that the secrecy of the intelligence operations can be maintained. Conversations with Hill staffers indicate that **Congress believes the State Department’s 2011 appointment of Coordinator for Cyber Issues has sufficiently addressed concerns** about the lack of U.S. involvement in international cybersecurity matters. Clearly, **this is narrow**, wishful **thinking**. **Congress needs to** stop focusing on what it believes it should force businesses to do about cybersecurity and instead focus on what it should **demand that the U.S. Government do to protect our critical infrastructure businesses and avoid retaliatory cyber attacks**. The kind of **reckless cyber diplomacy and foreign policy now at work has put our nation at risk and demonstrates cyber irresponsiblity, not cyber leadership.**

#### Congress must initiate the restriction — anything else is perceived as abdication

Hansen & Friedman 9

Professors at the New England School of Law, (Victor and Lawrence, The Case for Congress: Separation of Powers and the War on Terror, p.130)

The problem, of course, is that much of this **congressional involvement has come** much **too late** in the process and only after significant damage to our constitutional values had been inflicted by the Bush administration. **If Congress only acts after being goaded** by the courts, or only after high profile scandals have come to light, or only after the President’s policies have prolonged wars and made us at the same time less secure and less free, then **we** have **reached** a level of **constitutional brinkmanship which can only be regarded as intolerable.** Likewise, members of Congress would be sorely mistaken if they believed that these legislative initiatives have once and for all ended the possibility of executive assertions of dominance in these areas. Put simply, **Congress cannot afford to wait for** some **crisis to act.** As we have already discussed, the consequences are too dire. As many of the post-September 11 policy decisions of the Bush administration demonstrate, a President who acts without securing the benefits of the deliberative process established in the Constitution is likely to fail in making us more secure while maintaining basic liberties. Moreover, **when Congress only engages in these issues after the fact, its relevance as an institution is undermined. Unless Congress is** as **proactive** and assertive of its constitutionally appointed responsibilities as the executive is about its authority, the **checks and balances of our system simply will not work. Congress will be relegated to a second tier institution** in the realm of national security, and **it will be ever more difficult for Congress to stand up to an** assertive and **aggressive president.**

## 2AC

### 2AC T - Offense

#### We meet – their evidence misunderstands Operational preemption vs. true pre-emption

Mueller 06 <Karl P., Senior Political Scientist at RAND Corporation, et. al, 2006, "Striking First: Preemptive and Preventive Attack in U.S. National Security Policy" on www.rand.org>#SPS

Preemptive and preventive attacks have important differences; in addition to those already noted, international law holds that truly preemptive attacks are an acceptable use of force in self-defense, while preventive attacks usually are not. However, they are driven by similar logic, and since it is often useful to talk about both at the same time, the authors use the term anticipatory attack to refer to the broader category that includes both types of strategies. Anticipatory attack can be viewed as a continuum ranging from purely preemptive to purely preventive actions: All of them are offensive strategies carried out for defensive reasons, based on the belief that otherwise an enemy attack is (or may be) inevitable, and it would be better to fight on one’s own terms. Preemptive and preventive attacks are distinct from 'operational preemption,' taking military actions within an ongoing conflict that are intended to reduce the enemy’s capabilities or to achieve other effects by acting before the enemy launches an attack or takes some other undesirable action, such as deploying or dispersing its forces. Anticipatory attacks often involve operational preemption, but need not do so, and operational preemption may occur in any sort of conflict."

#### Offensive Cyber operations are destructive military cyber operations

Lin, 10 (Herbert S. Lin, Chief Scientist at the Computer Science and Telecommunications Board, National Research Council of the National Academies; “Offensive Cyber Operations and the Use of Force,” Journal Of National Security Law &Policy Vol. 4:63. http://jnslp.com/wp-content/uploads/2010/08/06\_Lin.pdf)

“For purposes of this article,the term “offensive cyber operations” will include military operations and activities in cyberspace for cyber attack against and (or) cyberexploitation of adversary information systems and networks.When greater specificity is needed, the terms “cyber attack” and “cyberexploitation” will be used. Although the objectives and the legal and policy constructs relevant to cyber attack and cyberexploitation are quite different(see the table in the Appendix to this article), the technological underpinnings and associated operational considerations of both are quite similar.Cyber attacks and cyberexploitation require a vulnerability, access to that vulnerability, and a payload to be executed.In a noncyber context, a vulnerability might be a lock to a file cabinet that could be easily picked. Access would be an available path for reaching the file cabinet. From an intruder’s perspective, access to a file cabinet located on the International Space Station would pose a very different problem from that posed by the same cabinet located in an office in Washington, D.C. The payload is responsible for executing the action taken by the intruder after the lock is picked. For example, the intruder can destroy the papers inside, or alter some of the information in those papers. The primary technical difference between cyber attack and cyberexploitation is in the nature of the payload to be executed – a cyber attack payload is destructive whereas a cyberexploitation payload acquires information nondestructively. In addition, because a cyberexploitation should not be detected, the cyber operation involved must only minimally disturb the normal operating state of the computer involved. In other words, the intelligence collectors need to be able to maintain a clandestine presence on the adversary computer or network despite the fact that information exfiltrations.

### 2AC Case - Arms Races

#### The US is uniquely vulnerable post-shutdown

Ballenstedt 10-2

Brittany Ballenstedt, *Defense One,* “Is the Shutdown Making Us Vulnerable to a Cyber Attack?,” 10/2/13, <http://www.defenseone.com/threats/2013/10/shutdown-making-us-vulnerable-cyber-attack/71218/> SJE

With electronic infrastructure still up and running despite the government shutdown, the lack of staff support in information security shops is likely affecting the government’s ability to respond to cyber threats and attacks and creating potential ripple effects for cybersecurity going forward. “What I would expect is that, by and large, just like the other services, information security is vastly undersupported, and that means that the exceptional circumstances are a problem,” said Tim Erlin, director of IT security and risk strategy at security software firm Tripwire. “When there’s an alarm or alert, the number of people available to investigate and deal with the consequences has been drastically reduced. It’s not that nobody will see the alarm; it’s that the response will be limited.” The shutdown situation also poses threats similar to those on holidays, weekends and late nights when IT staff are operating with skeleton crews, said Lamar Bailey, Tripwire’s director of security research and development. Hostile nation states may look to exploit the shutdown as much as possible while federal agencies are distracted, he said. “If a zero day came out today, it would be hard for government to respond,” Bailey said. “And next week, if the [shutdown] is still going on, there’s going to be a skeleton crew who can start rolling out the patches.” There also is the ripple effect that having federal employees and contractors away from their jobs will mean that they will have a backlog of work when they return in order to return systems to a stable state. “This creates a backlog and distracts people from securing the systems,” Erlin said.

#### Cyber deterrence low now and fails

Clarke and Knake ‘10

[Richard Alan Clarke is the former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States. Robert K. Knake, Former international affairs fellow in residence @ CFR. Cyber War. ETB]

‘

**With a nuclear detonation, one could be fairly certain about** ¶ **what would happen to the target. I**f the target was a military base, ¶ it would become unusable for years, if not forever. On my first day ¶ of graduate school at MIT in the 1970s, I was given a circular slide ¶ rule, which was a nuclear­effect calculator. Spin one circle and you ¶ picked the nuclear yield, say 200 kilotons. Spin another circle and ¶ you could choose an airburst or a groundburst. Throw in how far ¶ away from the target you might be in a worst case and your handy ¶ little spinning device told you how many pounds of explosive pres­¶ sure per square inch would be created and how many would be ¶ needed to collapse a hardened underground missile silo in on itself, ¶ before becoming little radioactive pieces of dust thrown way up ¶ in the atmosphere. **A cyber warrior may possibly have similar certainty that were he to hit some system** with a sophisticated cyber ¶ weapon, **that system**, say a modern freight railroad, **would likely** ¶ **stop cold. What he may not know is whether the railroad has a reliable resiliency plan, a backup command­and­control network that** ¶ **he does not know about because the enemy is keeping it secret and** ¶ **not using it until it’s needed**. Just as a secret intrusion­prevention ¶ system might surprise us when it’s suddenly turned on in a crisis, ¶ a secret continuity­of­operations system that could quickly get the target back up and running is also a form of defense against cyber ¶ attack.¶ **The potential surprise capability of an opponent’s defense makes** ¶ **deterrence in cyber war theory fundamentally different from deterrence theory in nuclear strategy**. **It was abundantly clear in nuclear** ¶ **strategy that there was an overwhelming case of what was called** ¶ **“offensive preference,”** that is to say, any defense deployed or even ¶ devised could easily be overwhelmed by a well­timed surprise attack. ¶ It costs far less to modify one’s missile offense to deal with defensive ¶ measures than the huge costs necessary to achieve even minimally ¶ effective missile protection. **Whatever the defense did, the offense** ¶ **won with little additional effort.** **In addition, no one thought for a** ¶ **moment that the Soviet Union or the United States could secretly** ¶ **develop and deploy an effective missile­defense system.** Ronald Rea­¶ gan hoped that by spending billions of dollars on research, the U.S. ¶ could change the equation and make strategic nuclear missile de­¶ fense possible. Decades later it has not worked, and today the U.S. ¶ hopes, at best, to be able to stop a small missile attack launched by ¶ accident or a minor power’s attack with primitive missiles. Even that ¶ remains doubtful.¶ **In** strategic **nuclear war theory, the destructive power of the of­**¶ **fense was well known, no defense could do much to stop it, the** ¶ **offense was feared, and nations were thereby deterred from using** ¶ **their own nuclear weapons or taking other provocative steps that** ¶ **might trigger a nuclear response.** **Deterrence derived from suffi cient certainty. In the case of cyber war, the power of the offense** ¶ **is largely secret; defenses of some efficacy could possibly be created** ¶ **and might even appear suddenly in a crisis, but it is unlikely any** ¶ **nation is effectively deterred today from using its own cyber weap­**¶ **ons in a crisis; and the potential of retaliation with cyber weapons** ¶ **probably does not yet deter any nation from pursuing whatever** ¶ **policy it has in mind.** Assume for the sake of discussion that the United States (or some ¶ other nation) had such powerful offensive cyber weapons that it ¶ could overcome any defense and inflict significant disruption and ¶ damage on some nation’s military and economy. If the U.S. sim­¶ ply announced that it had that capability, but disclosed no details, ¶ many opponents would think that we were bluffing. Without de­¶ tails, without ever having seen U.S. cyber weapons in action, few ¶ would so fear what we could do as to be deterred from anything.¶ The U.S. could theoretically look for an opportunity to punish ¶ some bad actor nation with a cyber attack just to create a demon­¶ stration effect. (The U.S. used the F­117 Stealth fighter­bomber in ¶ the 1989 invasion of Panama not because it feared Panamanian ¶ air defenses, but because the Pentagon wanted to show off its new ¶ weapon to deter others. The invasion was code­named Operation ¶ Just Cause, and many in the Pentagon quipped that the F­117 was ¶ sent in “just cause we could.”) **The problem with the idea of using** ¶ **cyber weapons in the next crisis that comes up is that many sophisticated cyber attack techniques may be similar to the cryptologist’s** ¶ **“onetime pad” in that they are designed for use only once**. **When** ¶ **the cyber attack weapons are used, potential opponents are likely** ¶ **to detect them and apply all of their research capability in coming** ¶ **up with a defense.**¶If the U.S. cannot deter others with its secret cyber weapons, is it ¶ possible that the U.S. itself may be deterred by the threat from other ¶ nations’ cyber warriors? In other words, are we today self­deterred ¶ from conventional military operations because of our cyber war vul­¶ nerabilities? If a crisis developed in the South China Sea, as in the ¶ exercise described above, I doubt that today anyone around the table ¶ in the Situation Room would say to the President, “You better not ¶ send those aircraft carriers to get China to back down in that oil dis­¶ pute. If you do that, Mr. President, Beijing could launch a cyber at­¶ tack to crash our stock market, ground our airlines, halt our trains, and plunge our cities into a sustained blackout. There is nothing we ¶ have today that could stop them, sir.”¶ Somebody should say that, because, of course, it’s true. But would ¶ they? Very unlikely. The most senior American military officer just ¶ learned less than two years ago that his operational network could ¶ probably be taken down by a cyber attack. The Obama White ¶ House did not get around for a year to appointing a “cyber czar.” ¶ America’s warriors think of technology as the ace up their sleeves, ¶ something that lets their aircraft and ships and tanks operate better ¶ than any in the world. It comes hard to most of the U.S. military ¶ to think of technology as something that another nation could use ¶ effectively against us, especially when that technology is some geek’s ¶ computer code and not a stealthy fighter­bomber.¶ So, **we cannot deter other nations with our cyber weapons**. **In** ¶ **fact, other nations are so undeterred that they are regularly hack­**¶ **ing into our networks. Nor are we likely to be deterred from doing** ¶ **things that might provoke others into making a major cyber attack**. ¶ Deterrence is only a potential, something that we might create in the ¶ mind of possible cyber attackers if (and it is a huge if) we got serious ¶ about deploying effective defenses for some key networks. Since we ¶ have not even started to do that, **deterrence theory**, the sine qua non ¶ of strategic nuclear war prevention, **plays no significant role in stop­**¶ **ping cyber war today.**

#### No deterrent value to OCO’s

Lewis ‘13

[James Andrew Lewis is a senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies (CSIS), where he writes on technology, security and the international economy. Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service Officer and as a member of the Senior Executive Service. <http://www.worldpoliticsreview.com/articles/13009/thresholds-of-uncertainty-collective-defense-and-cybersecurity> ETB]

While the deterrent value of offensive cyber-capabilities is practically nonexistent, cyber-operations will form part of any military response to actions against NATO members. The U.S. and allies could also consider pre-emptive measures that involved action against the opponents’ networks. In addition to the U.S., a few allies have significant offensive capabilities, and others are developing them. Decisions on appropriate responses to cyberattack raise the issue of how to incorporate offensive cyber into alliance military doctrine. NATO could choose to treat offensive cyber-capabilities in the same way it treats nuclear weapons, but there is reluctance, perhaps due to the exceptionally covert nature of cyberwarfare, to do so. Offensive capabilities could be considered independent, with the national government retaining control and release authority. NATO commanders would have to request the release of these capabilities, noting that the period for decision on warning and release might in some circumstances be compressed from hours into minutes. In any event, all of these issues must be addressed for any collective cyberdefense to be effective.

### 2AC Case - Alliances

#### US will preemptively strike China with the plan

Sanger and Shanker, 13

(David E Sanger and Thom Shanker, reporters for the New York Times, "Broad Powers Seen for Obama in Cyberstrikes", Feb 3, [www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?pagewanted=all&\_r=0](http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?pagewanted=all&_r=0) NL)

Cyberweaponry is the newest andperhaps most complex arms raceunder way. The Pentagon has created a new Cyber Command, and computer network warfare is one of the few parts of the military budget [that is expected to grow](http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html). Officials said that the new cyberpolicies had been guided by a decade of evolution in counterterrorism policy, particularly on the division of authority between the military and the intelligence agencies in deploying cyberweapons. Officials spoke on condition of anonymity because they were not authorized to talk on the record.¶ Under current rules, the military can openly carry out counterterrorism missions in nations where the United States operates under the rules of war, like Afghanistan. But the intelligence agencies have the authority to carry out clandestine drone strikes and commando raids in places like Pakistan and Yemen, which are not declared war zones. The results have provoked wide protests.¶ Mr. Obama is known to have approved the use of cyberweapons only once, early in his presidency, when [he ordered an escalating series of cyberattacks against Iran’s nuclear enrichment facilities](http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html). The operation was code-named Olympic Games, and while it began inside the Pentagon under President George W. Bush, it was quickly taken over by the National Security Agency, the largest of the intelligence agencies, under the president’s authority to conduct covert action.¶ As the process of defining the rules of engagement began more than a year ago, one senior administration official emphasized that the United States had restrained its use of cyberweapons. “**There are levels of cyberwarfare that are far more aggressive than anything that has been used** or recommended to be done,” the official said. ¶ The attacks on Iran illustrated that a nation’s infrastructure can be destroyed without bombing it or sending in saboteurs.¶ **While many potential targets are military, a country’s power grids, financial systems and communications networks can also be crippled**. Even more complex, nonstate actors, like terrorists or criminal groups, can mount attacks, and it is often difficult to tell who is responsible. Some critics have said the cyberthreat is being exaggerated by contractors and consultants who see billions in potential earnings.¶ One senior American official said that officials quickly determined that the **cyberweapons** were **so powerful** that — like [nuclear weapons](http://topics.nytimes.com/top/news/science/topics/atomic_weapons/index.html?inline=nyt-classifier) — they should be unleashed only on the direct orders of the commander in chief. ¶ A possible exception would be in cases of narrowly targeted tactical strikes by the military, like turning off an air defense system during a conventional strike against an adversary.¶ “There are very, very few instances in cyberoperations in which the decision will be made at a level below the president,” the official said. That means the administration has ruled out the use of “automatic” retaliation if a cyberattack on America’s infrastructure is detected, even if the virus is traveling at network speeds.¶ While the rules have been in development for more than two years, they are coming out at a time of greatly increased cyberattacks on American companies and critical infrastructure. The [Department of Homeland Security](http://topics.nytimes.com/top/reference/timestopics/organizations/h/homeland_security_department/index.html?inline=nyt-org) recently announced that an American power station, which it did not name, was crippled for weeks by cyberattacks.[The New York Times reported last week that it had been struck](http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html), for more than four months, by a cyberattack emanating from China. [The Wall Street Journal](http://www.nytimes.com/2013/02/01/technology/wall-street-journal-reports-attack-by-china-hackers.html) and [The Washington Post](http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html) have reported similar attacks on their systems.¶ “While this is all described in neutral terms — what are we going to do about cyberattacks — the underlying question is, ‘What are we going to do about China?’ ” said Richard Falkenrath, a senior fellow at the Council on Foreign Relations. “There’s a lot of signaling going on between the two countries on this subject.”¶ International law allows any nation to defend itself from threats, and the United States has applied that concept to conduct pre-emptive attacks.

#### US-China cyber war escalates- stimulates risk taking and lowers conflict inhibition

Dobbins et al. ‘11

[Ambassador James F. Dobbins, a veteran diplomat and the current director of the RAND International Security and Defense Policy Center as well the US special representative for Afghanistan and Pakistan. <http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP344.pdf> ETB]

The difficulties of direct defense could be greatly accelerated by Chinesedevelopment and ¶ use of cyber-attackand ASAT weapons, given the dependence of U.S. forces and operating ¶ concepts on computer-networked and space-based C4ISR. For this reason, the PLA appears to ¶ think that hostilities in space and cyber-space would favor China, and so might initiate them. ¶ At the same time, as China extends the reach of its own forces and C4ISR into the Pacific, they will become vulnerable to U.S. cyber-attack and ASAT. In any case, any Sino-U.S. armed conflict will be increasingly affected if not decided by warfare in these new domains. The erosion of capabilities for direct defense will push the United States toward enhanced weapons, ranges, geography, and targets both to regain survivability and to strike Chinese ¶ forces, launchers, sensors, and other capabilities on the mainland (or elsewhere in the region ¶ outside of the immediate theater). In addition, as the PLA develops cyber and ASAT capabilities but also comes to rely more on advanced C4ISR, the United States will have to consider ¶ striking Chinese satellites and computer networks. These trends will thus lead both sides to ¶ widen their choice of targets in order to achieve dominance over any particular geographic ¶ objective, however limited. ¶ The increasing difficulty in ensuring direct defense can be consequential even if Sino-U.S. hostilities are unlikely, for they could stimulate Chinese risk-taking, increase U.S. inhibitions, and weaken the resolve of U.S. allies and China’s neighbors in facing a China more insistent on settling disputes on its terms. These trends are the result of underlying general technological progress, sustainable growth in military spending, PLA reform and doctrinal adaptation, ¶ and geographic distances for China and the United States. On the other hand, most of China’s ¶ neighbors are growing economically and in technological sophistication, and some may choose ¶ to keep pace in quality if not quantity with Chinese advances in the military field.

### 2AC XO CP

#### Doesn’t solve - binding precedent is key to norm building, other countries don’t trust presidential unilateralism on cyber and the mere fear of preemption is sufficient to lock in structural instability- that’s Huston and Morgan

#### Doesn’t solve modeling

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

When our **founders** were drafting the Constitution, they **went out of their way to give warmaking powers to Congress, not the President.**¶ **They understood that if the President could make war on his own, he’d be no different than a king.**¶ And they also understood, as James Madison said, that such power “would be too much temptation” for one man.¶ And so they vested that power in Congress.¶ But since World War II, one President after another has usurped that power.¶ The latest usurper is President Obama, who did so in Libya, and with drones, and now is prepared to do so in cyberspace.¶ According to The New York Times, **the Obama Administration has concluded that the President has the authority to launch preemptive cyberattacks.**¶ **This is a** very **dangerous**, and very undemocratic **power grab.**¶ **There are no checks** or balances **when the President, alone, decides when to engage in an act of war.**¶ And **this** new aggressive stance **will lead to a cyber arms race.** The United States has evidently already used cyber weapons against Iran, and so many **other countries will assume** that **cyber warfare is** an **acceptable** tool **and** will try to **use it themselves.**¶ **Most troubling, U.S. cybersupremacy—and that is Pentagon doctrine—will also raise fears among nuclear powers like Russia, China, and North Korea that the United States may use a cyberattack as the opening move in a nuclear attack.**¶ For **if the United States can knock out the command and control structure of an enemy’s nuclear arsenal, it can then launch an all-out nuclear attack on that enemy with impunity. This would make such nuclear powers more ready to launch their nuc**lear weapon**s preemptively for fear that they would be rendered useless.** So **we’ve just moved a little closer to midnight**.¶ Now, I don’t think Obama would use cyberwafare as a first strike in a nuclear war. But **our adversaries may not be so sure, either about Obama or his successors.**¶ **They, too, worry about the temptations of a President**.

#### Perm do both

#### Perm key to public legitimacy

Brecher 13

(Aaron P., Michigan Law Review, "Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations," [www.michiganlawreview.org/assets/pdfs/111/3/Brecher.pdf](http://www.michiganlawreview.org/assets/pdfs/111/3/Brecher.pdf), AJK)

**Though separation of powers analysis is normally applied as a tool for** ¶ **judicial scrutiny, whether a major cyberattack can be said to have been conducted with the** blessing of both Congress and the president **is of serious constitutional** import. The fact that activities **may not be subject to judicial** ¶ **review** **makes it even more important that the two other major constitutional actors** in the American system **conduct themselves with their** ¶ **constitutional obligations in mind.** Also, a careful understanding of **how** the¶ **s**eparation **o**f **p**owers **applies to a novel means of** statecraft and **warfare** **can contribute to the public understanding of the national constitutional ethos**.144¶ **A cyberattack’s massive potential for unintended consequences demands a** ¶ **cautious constitutional approach to the conduct.** The covert action statute serves this function by enabling the president to act with congressional approval.

#### Perm- do the counterplan- there is no opportunity cost to the aff because the link is generated through fiat of the CP rather than to the aff

#### Congressional power of the purse rolls back the CP

Fisher 4, Senior Specialist in Separation of Powers with the Congressional Research Service, LOC [Louis, Presidential War Power: Second Edition, Revised, p. 274-277]

Statutory Restrictions

Instead of relying on unpredictable court decisions, Congress must learn to invoke the powerful weapons at its command. Through its prerogative to¶ authorize programs and appropriate funds, it can define and limit presidential power. In domestic as well as in foreign affairs, Congress can withhold all or part of an appropriation and may attach riders to appropriations measures to proscribe certain actions.44¶ Some claim that the power of the purse is ineffective in restraining presidential wars. Senator Jacob Javits (R-N.Y.) said that Congress "can hardly cut off appropriations when 500,000 American troops are fighting for their lives, as in Vietnam."45 The short answer is that Congress can, and has, used the power of the purse to restrict presidential war power. If members of Congress are worried about American troops fighting for their lives in a futile war, those lives are not protected by voting for continued funding. The proper and responsible action is to terminate appropriations and bring the troops home. Members need to make that case to their constituents. It can be done.¶ The Supreme Court has held that the President as Commander in Chief "is authorized to direct the movements of the naval and military forces placed by law at his command, and to employ them in the manner he may deem most effectual to harass and conquer and subdue the enemy."46 The power to move forces "placed by law" at his command implies that Congress can, by statute, control the scope of the commander-in-chief powers. Many such restrictions have been enacted. Following are some contemporary examples.¶ In 1973, Congress used the power of the purse to end the war in Vietnam. Three years later it prohibited the CIA from operating in Angola other than to gather intelligence. Legislation also prohibited the Agency from conducting military or paramilitary operations in Angola and denied any appropriated funds to finance directly or indirectly any type of military assistance to Angola.47¶ In 1984, Congress adopted the Boland Amendment to prohibit assistance of any kind by the Reagan administration to support the Contras in Nicaragua. The all-embracing language read: "During fiscal year 1985, no funds available to the Central Intelligence Agency, the Department of¶ Defense, or any other agency or entity of the United States involved in intelligence activities may be obligated or expended for the purpose or which would have the effect of supporting, directly or indirectly, military or paramilitary operations in Nicaragua by any nation, group, organization, movement, or individual." 48 No constitutional objection to this provision was ever voiced publicly by President Reagan, the White House, the Justice Department, or any other agency of the executive branch.¶ Two years later, Congress restricted the President's military role in Central America by stipulating that U.S. personnel "may not provide any training or other service, or otherwise participate directly or indirectly in the provision of any assistance, to the Nicaraguan democratic resistance pursuant to this title within those land areas of Honduras and Costa Rica which are within 20 miles of the border with Nicaragua."9 The statute defined U.S. personnel to mean "any member of the United States Armed Forces who is on active duty or is performing inactive duty training" and any employee of any department, agency, or other component of the executive branch.50 The clear purpose was to prevent military activities in Honduras and Costa Rica from spilling over into Nicaragua. The Reagan administration never offered any constitutional objections to this statutory restriction.¶ Also in 1986, Congress passed this prohibition on placing U.S. personnel in Nicaragua: "No member of the United States Armed Forces or employee of any department, agency, or other component of the United States Government may enter Nicaragua to provide military advice, training, or logistical support to paramilitary groups operating inside that country. Nothing in this title shall be construed as authorizing any member or unit of the Armed Forces of the United States to engage in combat against the government of Nicaragua.”51¶ In 1991, when Congress authorized President Bush to use military force against Iraq, the authority was explicitly linked to UN Security Council Resolution 678, which was adopted to expel Iraq from Kuwait.52 Thus, the legislation did not authorize any wider action, such as using U.S. forces to invade and occupy Iraq. In 1993, Congress established a deadline for troops to leave Somalia. No funds could be used for military action after March 31, 1994, unless the President requested an extension from Congress and received legislative authority

#### Future presidents roll back

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

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

#### Congressional restrictions on executive cyberwar power is critical to maintain SOP

Lorber 13

[Eric, J.D. Candidate, University of Pennsylvania Law School, Ph.D Candidate, Duke University

Department of Political Science. Journal Of Constitutional Law 15.3 <https://www.law.upenn.edu/live/files/1773-lorber15upajconstl9612013>. ETB]

Yet addressing these questions is increasingly important for two reasons. ¶ First, **as states such as China, Israel, Russia, and the U**nited **S**tates **use these weapons now and likely will do so more in future conflicts, determining the domestic legal strictures governing their use would provide policymakers and military planners a better sense of how to operate in cyberspace**.12¶ Second**, the possible employment of these tools adds yet another wrinkle to the battle between the executive and legislative branches over war-making authority**.13 In particular, if neither the War Powers Resolution nor the ¶ Intelligence Authorization Act governs OCOs**, the executive may be allowed** ¶ **to employ U.S. military power** in a manner largely **unchecked by congressional authority**.**14 As a result, the employment of these tools i**mplicates—and perhaps **problematically shifts—the balance between the executive**’s commander-in-chief power15 **and Congress’**s war-making ¶ authority

#### extinction

Jamison 93

Linda S. Jamison, Deputy Director of Governmental Relations @ CSIS, Spring 1993, Executive-Legislative Relations after the Cold War, Washington Quarterly, v.16, n.2, p. 189

Indeed there are very few domestic issues that do not have strong international implications, and likewise there are numerous transnational issues in which all nations have a stake. Environmental degradation, the proliferationof weapons of mass destruction, population control, migration, international narcotics trafficking, the spread of AIDS, andthe deterioration of the human condition in the less developed world are circumstancesaffecting all corners ofthe globe. Neither political isolation nor policy bifurcation is an option for the United States. Global circumstances have drastically changed with the end of the Cold War and the political and policy conditions that sustained bipartisan consensus are not applicable to the post-war era. The formulation of a new foreign policy must be grounded in broad-based principles that reflect domestic economic, political and social concerns while providing practical solutions to new situations. Toward a cooperative US Foreign Policy for the 1990s: Ifthe federalgovernment is to meetthenewinternational policychallengesof the post-cold war era, institutional dissension caused by partisan competition and executive-legislative friction must give way to a new way of business**.** Policy flexibility must be the watchword of the 1990s in the foreign policy domainif the United States is to have any hope of securing its interests in theuncertainyears ahead**.** One former policymaker, noting the historical tendency of the United States to make fixed “attachments,” has argued that a changing world dictates policy flexibility, where practical solutions can be developed on principles of broad-based policy objectives (Fulbright 1979). Flexibility, however, will not be possible without interbranch cooperation. The end of the Cold War and the new single-party control of the White House and Congress provide a unique opportunity to reestablish foreign policy cooperation. Reconfiguring post cold war objectives requires comprehension of the remarkable transformations in world affairs and demands an intense political dialogue that goes beyond the executive branch (Mann 1990, 28-29).

#### Unfettered presidential powers cause nuclear war

Forrester 89

Professor, Hastings College of the Law (Ray, August 1989, ESSAY: Presidential Wars in the Nuclear Age: An Unresolved Problem, 57 Geo. Wash. L. Rev. 1636)

\*evidence is gendered modified

On the basis of this report, the startling fact is that **one** man **[person] alone has the ability to start a nuclear war**. A basic theory--if not the basic theory of our Constitution--is that **concentration of power** in any one person, or one group, **is dangerous to** mankind **[humanity]. The Constitution**, therefore, **contains a strong system of checks and balances, starting** **with the separation of powers** between the President, Congress, and the Supreme Court. The message is that no one of them is safe with unchecked power. Yet, in what is probably the most dangerous governmental power ever possessed, we find the potential for world destruction lodged in the discretion of one person. As a result of public indignation aroused by the Vietnam disaster, in which tens of thousands lost their lives in military actions initiated by a succession of Presidents, Congress in 1973 adopted, despite presidential veto, the War Powers Resolution. Congress finally asserted its checking and balancing duties in relation to the making of presidential wars. Congress declared in section 2(a) that its purpose was to fulfill the intent of the framers of the Constitution of the United States and insure that the collective judgment of both the Congress and the President will apply to the introduction of United States Armed Forces into hostilities, or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and to the continued use of such forces in hostilities or in such situations. The law also stated in section 3 that [t]he President in every possible instance shall consult with Congress before introducing United States Armed Forces into hostilities or into situations where imminent involvement in hostilities is clearly indicated. . . . Other limitations not essential to this discussion are also provided. The intent of the law is clear. Congress undertook to check the President, at least by prior consultation, in any executive action that might lead to hostilities and war.  [\*1638]  President Nixon, who initially vetoed the resolution, claimed that it was an unconstitutional restriction on his powers as Executive and Commander in Chief of the military. His successors have taken a similar view. Even so, some of them have at times complied with the law by prior consultation with representatives of Congress, but obedience to the law has been uncertain and a subject of continuing controversy between Congress and the President. Ordinarily, the issue of the constitutionality of a law would be decided by the Supreme Court. But, despite a series of cases in which such a decision has been sought, the Supreme Court has refused to settle the controversy. The usual ground for such a refusal is that a "political question" is involved. The rule is well established that the federal judiciary will decide only "justiciable" controversies. "Political questions" are not "justiciable." However, the standards established by the Supreme Court in 1962 in [Baker v. Carr, 369 U.S. 186,](http://www.lexisnexis.com/us/lnacademic/mungo/lexseestat.do?bct=A&risb=21_T9842011382&homeCsi=7338&A=0.48452774259109876&urlEnc=ISO-8859-1&&citeString=369%20U.S.%20186&countryCode=USA) to determine the distinction between "justiciable controversies" and "political questions" are far from clear. One writer observed that the term "political question" [a]pplies to all those matters of which the court, at a given time, will be of the opinion that it is impolitic or inexpedient to take jurisdiction. Sometimes this idea of inexpediency will result from the fear of the vastness of the consequences that a decision on the merits might entail. Finkelstein, Judicial Self-Limitation, 37 HARV. L. REV. 338, 344 (1924)(footnote omitted). It is difficult to defend the Court's refusal to assume the responsibility of decisionmaking on this most critical issue. The Court has been fearless in deciding other issues of "vast consequences" in many historic disputes, some involving executive war power. It is to be hoped that the Justices will finally do their duty here. But **in the meantime the spectre of single-minded power persists, fraught with all of the frailties** of human nature **that each human possesses, including the President**. World history is filled with tragic examples. Even if the Court assumed its responsibility to tell us whether the Constitution gives Congress the necessary power to check the President, the War Powers Resolution itself is unclear. Does the Resolution require the President to consult with Congress before launching a nuclear attack? It has been asserted that "introducing United States Armed Forces into hostilities" refers only to military personnel and does not include the launching of nuclear missiles alone. In support of this interpretation, it has been argued that Congress was concerned about the human losses in Vietnam and in other presidential wars, rather than about the weaponry. Congress, of course, can amend the Resolution to state explicitly that "the introduction of Armed Forces" includes missiles as well as personnel. However, the President could continue to act without prior consultation by renewing the claim first made by President  [\*1639]  Nixon that the Resolution is an unconstitutional invasion of the executive power. Therefore, the real solution, in the absence of a Supreme Court decision, would appear to be a constitutional amendment. All must obey a clear rule in the Constitution. The adoption of an amendment is very difficult. Wisely, Article V requires that an amendment may be proposed only by the vote of two-thirds of both houses of Congress or by the application of the legislatures of two-thirds of the states, and the proposal must be ratified by the legislatures or conventions of three-fourths of the states. Despite the difficulty, the Constitution has been amended twenty-six times. Amendment can be done when a problem is so important that it arouses the attention and concern of a preponderant majority of the American people. But the people must be made aware of the problem. It is hardly necessary to belabor the relative importance of the control of nuclear warfare. A constitutional amendment may be, indeed, the appropriate method. But the most difficult issue remains. What should the amendment provide? How can the problem be solved specifically? The Constitution in section 8 of Article I stipulates that "[t]he Congress shall have power . . . To declare War. . . ." The idea seems to be that only these many representatives of the people, reflecting the public will, should possess the power to commit the lives and the fortunes of the nation to warfare. This approach makes much more sense in a democratic republic than entrusting the decision to one person, even though he may be designated the "Commander in Chief" of the military forces. His power is to command the war after the people, through their representatives, have made the basic choice to submit themselves and their children to war. **There is a recurring relevation of a paranoia of power**throughout human history **that has impelled one leader after another** to draw their people **into wars** which, in hindsight, were foolish, unnecessary, and, in some instances, downright insane. Whatever may be the psychological influences that drive the single decisionmaker to these irrational commitments of the lives and fortunes of others, the fact remains that the **behavior is** a **predictable** one **in any government that does not provide an effective check and balance against uncontrolled power in the hands of one human**. We, naturally, like to think that our leaders are above such irrational behavior. Eventually, however, human nature, with all its weakness, asserts itself whatever the setting. At least that is the evidence that experience and history give us, even in our own relatively benign society, where the Executive is subject to the rule of law.  [\*1640]  Vietnam and other more recent engagements show that it can happen and has happened here. But the "nuclear football"--the ominous "black bag" --remains in the sole possession of the President. And, most important, his **[the] decision to launch a nuclear missile would be**, in fact if not in law, a **declaration of nuclear war, one which** the nation and, indeed, **humanity** in general, probably **would be unable to survive**.

### 2AC Credibility DA

#### Obama weak now- Syria deal

Maloof 9/13

F. Michael Maloof, senior staff writer for WND and the G2Bulletin, is a former security policy analyst in the Office of the Secretary of Defense¶ Read more at <http://www.wnd.com/2013/09/putin-makes-obama-look-indecisive-weak/#JFIueVqdjRHQa1GD.99> ETB

If Kerry and Lavrov come up with a plan, it will further consolidate Putin’s efforts in the Middle East, at U.S. expense.¶ “If the U.S. administration were to ignore Russian protests and proceed with a (military) strike with at least rhetorical coalition support, Russia would have little to show for its claimed influence in the Middle East,” according to the open intelligence group Stratfor.¶ “However, if Russia could effectively stunt the U.S.-led military campaign through an airy diplomatic proposal, then Russia will have played a hand in directly showcasing U.S. unreliability to its allies,” it said.¶ A proposal could make the U.S. look weak and indecisive while Moscow comes off “as the voice of reason” in a war that no one wants, and it will be all the Obama administration’s doing.

#### Obama is sending global signals of weakness and uncertainty

Forbes 9/1

<http://www.forbes.com/sites/dougschoen/2013/09/01/weak-on-syria-weak-in-the-world/> ETB

Put another way, the President made it clear a year ago that there was a red line that the Syrians should not cross. All evidence suggests that they have surely crossed it and instead of striking, the President lectures the American people, and indeed the world, on American democracy.¶ Indeed, just this morning, a Syrian state state-run newspaper called Obama’s decision to seek Congressional approval before taking military action “the start of the historic American retreat.” It doesn’t get clearer than that.¶ This is not a president who shies away from using his executive power. He has altered ObamaCare, pushed his gun control agenda to strengthen national background checks, delayed the deportation of illegal immigrants when Congress wouldn’t agree amongst many other examples. But he has now suddenly decided that before he takes action, action that is within his purview, he is going to seek Congressional approval that is almost impossible to predict as to whether it will be granted or not.¶ If Obama really wanted to go ahead he would have brought congress back into session immediately and not waited more than 10 days thereby giving the Syrians time to plan for an attack – should one ultimately come. And even then, Obama has made it clear any such attack will be limited in nature and scope and will not involve regime change.¶ It follows that the message Obama’s speech yesterday sends is a muddled one at best.¶ It said to the mullahs in Iran and their Supreme Leader Ali Khamenei that they can continue to pursue their nuclear program by enriching uranium and refining plutonium without having to fear that they will be precipitously attacked by the US.¶ And to Russia’s President Putin, who has been an unbendable ally of Assad, providing him with arms and anti-aircraft weaponry, Obama has shown that the balance of power in the Middle East has almost certainly shifted away from the US. This is all the more alarming as Putin said just yesterday that the idea that the Syrian regime used chemical weapons is “absolute nonsense.”¶ What’s more, with a totally incoherent American policy on Egypt wherein it is unclear who and what we support, the US’s approach to the Syria further paints a bleak picture of American power and potency. Indeed, with our only real achievement in the region being the recent appearance of convincing the Arabs and Israelis to come to the peace table, an image of American uncertainty is radiating across the globe.¶ And although this would be a serious accomplishment if progress is made, our inaction on Syria signals to Israel, one of our strongest allies, that we are not willing to stick our neck out for them, their safety and way of life.¶ To our allies around the world who have said that if we do not stand firm we will send the wrong message to the Syrians, Obama offered not much of a response other than to tell them, in so many words, that they may well have to go it alone.¶ The US has not been sending clear messages. And though it may be apparent to me that the President’s move was calculated to force responsibility on a reluctant Congress and to play to 80% of the American people who have said in polls that they are against intervention in Syria, that does not mean that the US is offering anything but a confused image of our mission in the world to both our allies and foes.¶ Thus, in the short term the President may have managed to escape from the political quandary he faces. But in the longer term, America looks weaker, feckless and more uncertain.¶ President Obama has, if nothing else, compounded the view of a weak leader heading an unsure nation. This is an image we can ill afford to project.

#### Massive alt causes to flex

Rozell 12

(Mark Rozell, Professor of Public Policy, George Mason University, “From Idealism to Power: The Presidency in the Age of Obama” 2012, <http://www.libertylawsite.org/book-review/from-idealism-to-power-the-presidency-in-the-age-of-obama/>, KB)

A substantial portion of Goldsmith’s book presents in detail his case that **various forces** outside of government, and some within, **are responsible for hamstringing the president** in unprecedented fashion: **Aggressive**, often intrusive, **journalism, that at times endangers national security; human rights and other advocacy groups**, some **domestic and** other **cross-national, teamed with big resources and talented, aggressive lawyers, using every legal category and technicality possible to complicate executive action**; **courts** thrust into the mix, **having to decide critical national security law controversies**, even when the judges themselves have little direct knowledge or expertise on the topics brought before them; **attorneys within the executive branch** itself **advising against actions** based on often narrow legal interpretations and with little understanding of the broader implications of tying down the president with legalisms.

#### Stronger statutory checks on Presidential war powers increase credibility

Matthew C. Waxman 13, Professor of Law at Columbia Law School; Adjunct Senior Fellow for Law and Foreign Policy, Council on Foreign Relations, “The Constitutional Power to Threaten War”, Forthcoming in Yale Law Journal, vol. 123 (2014), 8/25/2013, PDF

A second argument, this one advanced by some congressionalists, is that stronger legislative checks on presidential uses of force would improve deterrent and coercive strategies by making them more selective and credible. The most credible U.S. threats, this argument holds, are those that carry formal approval by Congress, which reflects strong public support and willingness to bear the costs of war; requiring express legislative backing to make good on threats might therefore be thought to enhance the potency of threats by encouraging the President to seek congressional authorization before acting.181 A frequently cited instance is President Eisenhower’s request (soon granted) for standing congressional authorization to use force in the Taiwan Straits crises of the mid- and late-1950s – an authorization he claimed at the time was important to bolstering the credibility of U.S. threats to protect Formosa from Chinese aggression.182 (Eisenhower did not go so far as to suggest that congressional authorization ought to be legally required, however.) “It was [Eisenhower’s] seasoned judgment … that a commitment the United States would have much greater impact on allies and enemies alike because it would represent the collective judgment of the President and Congress,” concludes Louis Fisher. “Single-handed actions taken by a President, without the support of Congress and the people, can threaten national prestige and undermine the presidency. Eisenhower’s position was sound then. It is sound now.”183 A critical assumption here is that legal requirements of congressional participation in decisions to use force filters out unpopular uses of force, the threats of which are unlikely to be credible and which, if unsuccessful, undermine the credibility of future U.S. threats. A third view is that legal clarity is important to U.S. coercive and deterrent strategies; that ambiguity as to the President’s powers to use force undermines the credibility of threats. Michael Reisman observed, for example, in 1989: “Lack of clarity in the allocation of competence and the uncertain congressional role will sow uncertainty among those who depend on U.S. effectiveness for security and the maintenance of world order. Some reduction in U.S. credibility and diplomatic effectiveness may result.”184 Such stress on legal clarity is common among lawyers, who usually regard it as important to planning, whereas strategists tend to see possible value in “constructive ambiguity”, or deliberate fudging of drawn lines as a negotiating tactic or for domestic political purposes.185 A critical assumption here is that clarity of constitutional or statutory design with respect to decisions about force exerts significant effects on foreign perceptions of U.S. resolve to make good on threats, if not by affecting the substance of U.S. policy commitments with regard to force then by pointing foreign actors to the appropriate institution or process for reading them.

#### It’s impossible for the president to remain adequately flexible on cyber

Waxman ‘11

[Associate Professor, Columbia Law School; Adjunct Senior Fellow, Council on Foreign

Relations; Member of the Hoover Institution Task Force on National Security and Law. THE YALE JOURNAL OF INTERNATIONAL LAW 36:421. <http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf> ETB]

Such interpretive reorientation raises subsidiary doctrinal issues that¶ might not sit comfortably with extant U.S. legal positions about the resort to¶ force more generally. For example, in recent years the U.S. government has pushed an interpretation of anticipatory self-defense—the doctrinal notion that¶ a state may resort to self-defensive force in advance of an imminent attack,¶ rather than having to wait to suffer the first blow—that permits flexibility in¶ assessing the “imminence” of a threat so as to take account of the difficulty of¶ assessing when contemporary security threats are temporally immediate.72 If cyber-attacks with certain effects give rise to rights of self-defense, could an impending one give rise to such a right in advance as well? Moreover, how would a state even assess imminence in this context?73 Anticipatory selfdefense is especially difficult to evaluate in this context because even if hostile¶ cyber-attack capabilities and intentions are identified, there may be little or no¶ indication of their future timing. It may also be impossible to assess their likely consequences in advance, because modern society’s heavy reliance on¶ interconnected information systems means that the indirect secondary or¶ tertiary effects of cyber-attacks may be much more consequential than the¶ direct and immediate ones.

#### **No impact to prez powers**

Healy 11

Gene Healy is a vice president at the Cato Institute and the author of The Cult of the Presidency, The CATO Institute, June 2011, "Book Review: Hail to the Tyrant", http://www.cato.org/publications/commentary/book-review-hail-tyrant

Legal checks “have been relaxed largely because of the need for centralized, relatively efficient government under the complex conditions of a modern dynamic economy and a highly interrelated international order.” What’s more, the authors insist, America needs the legally unconstrained presidency both at home (given an increasingly complex economy) and abroad (given the shrinking of global distances).

These are disputed points, to say the least. If Friedrich Hayek was at all correct about the knowledge problem, then if anything increasing economic complexity argues for less central direction. Nor does the fact that we face “a highly interrelated international order” suggest that we’re more vulnerable than we were in 1789, as a tiny frontier republic surrounded by hostile tribes and great powers. Economic interdependence — and the rise of other modern industrial democracies — means that other players have a stake in protecting the global trading system.

Posner and Vermuele coin the term “tyrannophobia,” which stands for unjustified fear of executive abuse. That fear is written into the American genetic code: the authors call the Declaration of Independence “the ur-text of tyrannophobia in the United States.” As they see it, that’s a problem because “the risk that the public will fail to trust a well-motivated president is just as serious as the risk that it will trust an ill-motivated one.” They contend that our inherited skepticism toward power exacerbates biases that lead us to overestimate the dangers of unchecked presidential power. Our primate brains exaggerate highly visible risks that fill us with a sense of dread and loss of control, so we may decline to cede more power to the president even when more power is needed.

Fair enough in the abstract — but Posner and Vermuele fail to provide a single compelling example that might lead you to lament our allegedly atavistic “tyrannophobia.” And they seem oblivious to the fact that those same irrational biases drive the perceived need for emergency government at least as much as they do hostility towards it. Highly visible public events like the 9/11 attacks also instill dread and a perceived loss of control, even if all the available evidence shows that such incidents are vanishingly rare. The most recent year for which the U.S. State Department has data, 2009, saw just 25 U.S. noncombatants worldwide die from terrorist strikes. I know of no evidence suggesting that unchecked executive power is what stood between us and a much larger death toll.

Posner and Vermuele argue that only the executive unbound can address modernity’s myriad crises. But they spend little time exploring whether unconstrained power generates the very emergencies that the executive branch uses to justify its lack of constraint. Discussing George H.W. Bush’s difficulties convincing Congress and the public that the 1991 Gulf War’s risks were worth it, they comment, “in retrospect it might seem that he was clearly right.” Had that war been avoided, though, there would have been no mass presence of U.S. troops on Saudi soil — “Osama bin Laden’s principal recruiting device,” according to Paul Wolfowitz — and perhaps no 9/11.

Posner and Vermuele are slightly more perceptive when it comes to the home front, letting drop as an aside the observation that because of the easy-money policy that helped inflate the housing bubble, “the Fed is at least partly responsible for both the financial crisis of 2008-2009 and for its resolution.” Oh, well — I guess we’re even, then.

Sometimes, the authors are so enamored with the elegant economic models they construct that they can’t be bothered to check their work against observable reality. At one point, attempting to show that separation of powers is inefficient, they analogize the Madisonian scheme to “a market in which two firms must act in order to supply a good,” concluding that “the extra transaction costs of cooperation” make “the consumer (taxpayer) no better off and probably worse off than she would be under the unitary system.”

But the government-as-firm metaphor is daffy. In the Madisonian vision, inefficiency isn’t a bug, it’s a feature — a check on “the facility and excess of law-making … the diseases to which our governments are most liable,” per Federalist No. 62. If the “firm” in question also generates public “bads” like unnecessary federal programs and destructive foreign wars — and if the “consumer (taxpayer)” has no choice about whether to “consume” them — he might well favor constraints on production.

From Franklin Roosevelt onward, we’ve had something close to vertical integration under presidential command. Whatever benefits that system has brought, it’s imposed considerable costs — not least over 100,000 U.S. combat deaths in the resulting presidential wars. That system has also encouraged hubristic occupants of the Oval Office to burnish their legacies by engaging in “humanitarian war” — an “oxymoron,” according to Posner. In a sharply argued 2006 Washington Post op-ed, he noted that the Iraq War had killed tens of thousands of innocents and observed archly, “polls do not reveal the opinions of dead Iraqis.”

#### No impact to Iran

Sadr 5

Ehsaneh I. Sadr (graduate student in the department of government and politics at the University of Maryland, College Park) SUMMER 2005 “THE IMPACT OF IRAN’S NUCLEARIZATION ON ISRAEL” MIDDLE EAST POLICY, VOL. XII, NO. 2

The above analysis indicates that a nuclearized Iran is extremely unlikely to pose an existential threat to Israel. The doctrine of Mutually Assured Destruction holds in the Iranian context: Iran’s clerical rulers, anxious to protect their own power, citizens and civilization, will not launch a war that will lead to their own destruction. Iran’s rulers are extremely unlikely to pass nuclear material on to terrorist actors whose loyalty they cannot ensure. They are also unlikely to step up conventional or terrorist harassment of Israel for fear of the escalation of hostilities to nuclear warfare. The impact of Iran’s acquisition of nuclear weapons upon Israel’s regional interests is less problematic than one might think. Although the regime-change option would be off the table, it is not clear that it has ever been a feasible alternative given current geopolitical realities. Any increase in domestic political support for the Iranian regime is likely to be temporary. Iran may indeed be empowered to pursue its own regional interests, but such pursuit is not necessarily bad for Israeli interests. Finally, it will be many years before Iran’s weapons stockpile begins to approach Israel’s and the latter is compelled to engage in an expensive arms race. Indeed, there is reason to believe that Iran’s access to nuclear weapons may increase the prospects for regional stability and even Middle East peace. Given the horrendous consequences of an accidental nuclear war, it will be imperative that Iran and Israel develop some sort of ability to communicate with one another directly. It is not outside the realm of possibility that the institutionalization of such communications may be the first step in the normalization of relations between the two countries and the future integration of Israel into its neighborhood.

### 2AC Neolib K

#### No alternative - can’t solve our aff

they causes transition wars – causes extinction

Kothari 82 (Rajni, Professor of Political Science – University of Delhi, Toward a Just Social Order, p. 571)

Attempts at global economic reform could also lead to a world racked by increasing turbulence, a greater sense of insecurity among the major centres of power -- and hence to a further tightening of the structures of domination and domestic repression – producing in their wake an intensification of the old arms race and militarization of regimes, encouraging regional conflagrations and setting the stage for eventual global holocaust.

####  neolib is good – we control uniqueness

Chandy and Gertz 11 (Laurence – Fellow, Global Economy and Development at Brookings and Geoffrey – Research Analyst, Global Economy and Development – both @ Brookings Inst., January 2011, http://nextbigfuture.com/2011/02/poverty-in-numbers-changing-state-of.html)

Our results indicate that the world has seen a dramatic decrease in global poverty over the past six years, and that this trend is set to continue in the four years ahead. We estimate that between 2005 and 2010, the total number of poor people around the world fell by nearly half a billion people, from over 1.3 billion in 2005 to un- der 900 million in 2010. Looking ahead to 2015, extreme poverty could fall to under 600 million people—less than half the number regularly cited in describing the number of poor people in the world today. Poverty reduc- tion of this magnitude is unparalleled in history: never before have so many people been lifted out of poverty over such a brief period of time. When measured as a share of population, progress remains impressive, but is more in line with past trends. In the early 1980s, more than half of all people in developing countries lived in extreme poverty. By 2005, this was down to a quarter. According to our estimates, as of 2010 less than 16 percent remained in poverty, and fewer than 10 percent will likely be poor by 2015. The first Millennium Development Goal defines a target (MDG1a) of halving the rate of global poverty by 2015 from its 1990 level. In an official report prepared for the U.N. MDG conference this past September, the World Bank stated that we are 80 percent of the way toward this target and are on track to meet it by 2015, though the Bank warned that “the economic crisis adds new risks to prospects for reaching the goal.”3 Our assessment is considerably more upbeat. We believe that the MDG1a target has already been met—ap- proximately three years ago.4 Furthermore, by 2015, we will not only have halved the global poverty rate, as per MDG1a, but will have halved it again. Over the past half century, the developing world, including many of the world’s poorest countries, have seen dramatic improvements in virtually all non-income measures of well-being: since 1960, global infant mortality has dropped by more than 50 percent, for example, and the share of the world’s children enrolled in primary school increased from less than half to nearly 90 percent between 1950 and today.5 Likewise there have been im- pressive gains in gender equality, access to justice and civil and political rights. Yet, through most of this period, the incomes of rich and poor countries diverged, and income poverty has proven a more persistent challenge than other measures of wellbeing.6 The rapid decline in global poverty now underway—and the early achieve- ment of the MDG1a target—marks a break from these trends, and could come to be seen as a turning point in the history of global development. In which countries and regions is poverty falling? Today’s massive reduction in global poverty represents the aggregate of a number of individual regional and national success stories. Unlike previous decades, like the ’80s (when the poverty rate increased in Africa) and the ’90s (when it in- creased in Latin America and the former Soviet Union), poverty reduction is currently taking place in all regions of the world (Table 1). The sharpest fall in poverty is occurring in Asia. South Asia alone is expected to see a reduction in the number of its poor of more than 430 million over the 10-year period we study, representing a fall in its poverty rate of over 30 percentage points. East Asia already recorded a vast drop in poverty between 1980 and 2005, and this trend is continuing: a further 250 million people in the region are expected to escape poverty by 2015, two-thirds of whom have likely already done so. Perhaps the greatest surprise, however, is the one taking place in Sub-Saharan Africa. Between 1980 and 2005, the region’s poverty rate had consistently hovered above 50 percent. Given the continent’s high population growth, its number of poor rose steadily. The current period is different. For the first time, Sub-Saharan Africa’s poverty rate has fallen below 50 percent. The total number of poor people in the region is falling too, albeit slowly. Better still, by 2015, the poverty rate is expected to fall below 40 percent—a rate China did not achieve until the mid-90s.

neolib is inevitable – working within the system key

Shaviro 05 (Steven, professor of Film, Culture, and English at the University of Washington, http://www.shaviro.com/Blog/?p=425, 7/6)

The language of capitalism is the language of desire, and utopia, and salvation. And that is the secret of its success. The market always leaves us unsatisfied; but for this very reason it always gets us to come back for more. In the last analysis, there is no arguing against desire. Leftists won’t get very far by urging people to live within their means, or by telling them to settle for what they need instead of what they want. We should leave such exhortations to the Federal Reserve Bank. But also — and this is the most difficult part — we won’t get away from the logic of commodities and the market by appealing to utopian yearnings and hopes of redemption. For these longings are the very ones that motivate us to go shopping. They have been subsumed, all too successfully, within the circuits of consumption. The only way out is the way through. The only answer to capitalist desire’s constant cries of “more!” is to up the ante still further, as in Blake’s aphorism: “More! More! is the cry of a mistaken soul, less than All cannot satisfy Man.” It is therefore only by embracing the logic of capitalist (and specifically, post-Fordist) aestheticism that we can hope to open a path ‘beyond’ it. The best guide in these matters is Andy Warhol, who wrote that “buying is much more American than thinking… Americans are not so interested in selling — in fact, they’d rather throw out than sell. What they really like to do is buy — people, money, countries.” The supply-side way of encouraging people to buy is beauty, style, or more precisely cool. When leftist critics denounce the market’s promotion of style over substance, when they deplore, as Stuart Ewen does, “the cycle of waste upon which the market is built,” they are missing the point that this wastefulness is not a bug, but a feature. It’s flexible accumulation’s answer to the dilemma of overproduction. Without it, the whole system would come tumbling down — and not in a way that would lead to a change for the better. We need to be wasteful, to throw things out, in order to clear room in our closets for new stuff. And we need to change our fashions, and upgrade our gadgets, as often as possible, in order (as Virginia Postrel puts it) to “reinvent ourselves, emphasizing and developing previously unknown or subordinate aspects of our personalities.” Far from creating scarcity by diverting resources, conspicuous waste is our only exemption from the ruthless reign of Malthusian scarcity, Darwinian struggle, and “the discipline of the market.” A visit to the mall puts beauty into our otherwise blighted lives. The thing to remember is that, even when we strive to resist the commodity’s allure, and the ubiquitous domination of the marketplace, it is only in the terms set forth by the commodity itself that we can do so. We must say of the commodity what Derrida says of metaphysics: “We have no language — no syntax and no lexicon — which is foreign to this history; we can pronounce not a single destructive proposition which has not already had to slip into the form, the logic, and the implicit postulations of precisely what it seeks to contest.” The Situationist strategy of radical negativity and absolute refusal is a self-congratulatory self-deception, or at best a show of empty bravado. Like it or not, the situation that we face today is the opposite of the one described by Audre Lord: for it is only with the master’s tools that we can possibly hope to dismantle the master’s house.

**Neolib is sustainable and inevitable---no alt**

**Jones 11**—Owen, Masters at Oxford, named one of the Daily Telegraph's 'Top 100 Most Influential People on the Left' for 2011, author of "Chavs: The Demonization of the Working Class", The Independent, UK, "Owen Jones: Protest without politics will change nothing", 2011, www.independent.co.uk/opinion/commentators/owen-jones-protest-without-politics-will-change-nothing-2373612.html

My first experience of police kettling was aged 16. It was May Day 2001, and the anti-globalisation movement was at its peak. The turn-of-the-century anti-capitalist movement feels largely forgotten today, but it was a big deal at the time. To a left-wing teenager growing up in an age of unchallenged neo-liberal triumphalism, just to have "anti-capitalism" flash up in the headlines was thrilling. Thousands of apparently unstoppable protesters chased the world's rulers from IMF to World Bank summits – from Seattle to Prague to Genoa – and the authorities were rattled.¶ Today, as protesters in nearly a thousand cities across the world follow the example set by the Occupy Wall Street protests, it's worth pondering what happened to the anti-globalisation movement. Its activists did not lack passion or determination. But they did **lack a coherent alternative to the neo-liberal project**. With no clear political direction, **the movement was easily swept away** by the jingoism and turmoil that followed 9/11, just two months after Genoa.¶ Don't get me wrong: the Occupy movement is a glimmer of sanity amid today's economic madness. By descending on the West's financial epicentres, it reminds us of how a crisis caused by the banks (a sentence that needs to be repeated until it becomes a cliché) has been cynically transformed into a crisis of public spending. The founding statement of Occupy London puts it succinctly: "We refuse to pay for the banks' crisis." The Occupiers direct their fire at the top 1 per cent, and rightly so – as US billionaire Warren Buffett confessed: "There's class warfare, all right, but it's my class, the rich class, that's making war, and we're winning."¶ The Occupy movement has provoked fury from senior US Republicans such as Presidential contender Herman Cain who – predictably – labelled it "anti-American". They're right to be worried: those camping outside banks threaten to refocus attention on the real villains, and to act as a catalyst for wider dissent. But a **coherent alternative to the tottering global economic order remains,** it seems, **as distant as ever. Neo-liberalism crashes around, half-dead, with no-one to administer the killer blow.¶** There's always a presumption that a crisis of capitalism is good news for the left. Yet in the Great Depression, fascism consumed much of Europe. The economic crisis of the 1970s did lead to a resurgence of radicalism on both left and right. But, spearheaded by Thatcherism and Reaganism, the New Right definitively crushed its opposition in the 1980s.This time round, there doesn't even seem to be an alternative for the right to defeat. That's not the fault of the protesters. In truth, the left has never recovered from being virtually **smothered out of existence**. It was the victim of a perfect storm: the rise of the New Right; neo-liberal globalisation; and the repeated defeats suffered by the trade union movement.¶ But, above all, it was the aftermath of the collapse of Communism that did for the left. As US neo-conservative Midge Decter triumphantly put it: "It's time to say: We've won. Goodbye." From the British Labour Party to the African National Congress, left-wing movements across the world hurtled to the right in an almost synchronised fashion. It was as though the left wing of the global political spectrum had been sliced off. That's why, **although we live in an age of revolt, there remains no left to give it direction and purpose.**

**No impact**

**Larrivee 10**— PF ECONOMICS AT MOUNT ST MARY’S UNIVERSITY – MASTERS FROM THE HARVARD KENNEDY SCHOOL AND PHD IN ECONOMICS FROM WISCONSIN, 10 [JOHN, A FRAMEWORK FOR THE MORAL ANALYSIS OF MARKETS, 10/1, <http://www.teacheconomicfreedom.org/files/larrivee-paper-1.pdf>]

 The Second Focal Point: Moral, Social, and Cultural Issues of Capitalism **Logical errors abound** in critical commentary on capitalism. Some critics observe a problem and conclude: “I see X in our society. We have a capitalist economy. Therefore capitalism causes X.” They draw their conclusion by looking at a phenomenon as it appears only in one system. Others merely follow a host of popular theories according to which capitalism is particularly bad. 6 The solution to such flawed reasoning is to be comprehensive, to look at the good and bad, in market and non-market systems. Thus the following section considers a number of issues—greed, selfishness and human relationships, honesty and truth, alienation and work satisfaction, moral decay, and religious participation—that have often been associated with capitalism, but have also been problematic in other systems and usually in more extreme form. I conclude with some evidence for the view that markets foster (at least some) virtues rather than undermining them. My purpose is not to smear communism or to make the simplistic argument that “capitalism isn’t so bad because other systems have problems too.” The critical point is that **certain people thought** various **social ills resulted from capitalism, and on this basis they took action to establish alternative economic systems** to solve the problems they had identified. That **they failed to solve the problems, and** in fact **exacerbated them** while also creating new problems, implies that capitalism itself wasn’t the cause of the problems in the first place, at least not to the degree theorized.

**Neolib’s key to heg---makes the global order stable and cooperative**

Eric S. **Edelman 10**, former Under Secretary of Defense for Policy, was Principal Deputy Assistant to the Vice President for National Security Affairs, 2010, “Understanding America’s Contested Primacy,” Center for Strategic and Budgetary Assessments

Huntington has pointed out that US primacy at the end of the Cold War was important for two other reasons. The first was that no other power in the international system could “make comparable contributions to international order and stability.” The second was that the perceived failure of the Soviet model left the United States “as the only major power whose national identity is defined by a set of universal political and economic values.” Because these values were not central to the national identity of other powers they did not have the same drive as the United States to promote them in international affairs. This willingness to provide certain global public goods that increased the chances of international cooperation was also acknowledged by Robert Jervis, who was otherwise skeptical about the effort to maintain US primacy. It also facilitated acceptance of US primacy and the unipolar system by other countries. Those observations remain valid today.24¶ Although the point remains controversial it seems apparent that America, while clearly creating some resentments with its policies, continues to be seen (particularly by governments) as relatively benign in its interactions with other powers. America shares a fundamental view of the world rooted in the neoliberal orthodoxy of free marketsopen societies, and democratic institutions that emerged as a consensus prescription for peace and prosperity after the collapse of communism. This “transnational liberalism” inclines national elites to see a broad confluence of interest with the United States and reduces their tendency to try and counterbalance American power. As the guarantor of the international world economy and a provider of security and stability because of its alliance system, the United States provides global public goods which others cannot provide. In that sense the question that Stanley Hoffman posed some years ago of whether the United States should pursue primacy or world order seems to be a false dichotomy. As Michael Mandelbaum has persuasively argued, to the degree that there is world order, it exists because American primacy, combined with the triumph of neoliberal ideas, has allowed the United States to provide governmental functions to the rest of the world, chief among them being the maintenance of the global commons — air, sea, and space.25

### 2AC Rule of Law K

#### 3. Perm – do both – that solves

Zizek 89, Senior Researcher in the Department of Philosophy at the University of Ljubljana, Slovenia, Codirector of the Center for Humanities at Birkbeck College, University of London, and Distinguished Fashion Expert for Abercrombie and Fitch Quarterly, ’89 (Slavoj, Autumn, “Looking Awry” October, Vol 50 p 30-55, JSTOR)

By means of a metaphor of the way anamorphosis functions in painting, Bushy tries to convince the queen that her sorrow has no foundation, that its reasons are null, but the crucial point is the way his metaphor splits, redoubles itself, i.e., the way he entangles himself in contradiction. First ("sorrow's eye, glazed with blinding tears, / Divides one thing entire to many objects"), he refers to the simple, commonsense opposition between a thing as it is "in itself," in reality, and its "shadows," reflections in our eyes, subjective impressions multiplied because of our anxieties and sorrows. When we are worried, a small difficulty assumes giant proportions; we see the thing as far worse than it really is. The metaphor at work here is that of a glass surface sharpened, cut in such a way that it reflects a multitude of images; instead of the tiny substance, we see its "twenty shadows." In the following verses, however, things become complicated. At first sight it seems that Shakespeare only illustrates the fact that "sorrow's eye . . . divides one thing entire to many objects" with a metaphor from the domain of painting ("Like perspectives, which rightly gaz'd upon/Show nothing but confusion; ey'd awry/Distinguish form"), but what he really accomplishes is a radical change of terrain. From the metaphor of a sharpened glass surface he passes to the metaphor of anamorphosis, the logic of which is quite different. A detail of a picture that "rightly gaz'd," i.e., from a straightforward, frontal view, appears a blurred spot, assumes clear, distinct shapes once we look at it "awry," from aside. The verses which apply this metaphor back to the queen's anxiety and sorrow are thus profoundly ambivalent: "so your sweet majesty, / Looking awry upon your lord's departure, / Finds shapes of grief more than himself to wail; / Which, look'd on as it is, is nought but shadows / Of what is not." That is to say, if we take the comparison between the queen's look and the anamorphic look literally, we would be obliged to state that precisely by "looking awry," i.e., from aside, she sees the thing in its clear and distinct form, in opposition to the "straightforward," frontal view which sees only an indistinct confusion (and, incidentally, the further development of the drama fully justifies the queen's most sinister presentiments), But, of course, Bushy did not "want to say" this. His intention was to say quite the opposite: by means of an imperceptible subreption, he returned to the first metaphor (that of a sharpened glass) and "wanted to say" that, because her view is distorted by sorrow and anxiety, the queen sees causes for alarm where a closer, matter-of-fact look attests that there is next to nothing in it. What we have here are thus two realities, two "substances." On the level of the first metaphor, we have the commonsense reality as "substance with twenty shadows," as a thing split into twenty reflections by our subjective view; in short, as a substantial "reality" distorted by our subjective perspective (inflated by our anxiety, etc.). If we look at a thing straight on, from a matter-of-fact perspective, we see it "as it really is," while the look puzzled by our desires and anxieties ("looking awry") gives us a distorted, blurred image of the thing. On the level of the second metaphor (anamorphosis), however, the relation is exactly the opposite: if we look at a thing straight on, i.e., from a matter-of-fact, disinterested, "objective" perspective, we see nothing but a formless spot. The object assumes clear and distinctive features only if we look at it "from aside," i.e., with an "interested" look, with a look supported, permeated, and "distorted" by a desire. This is precisely the Lacanian objet petit a, the object-cause of desire, an object which is, in a way, posited by the desire itself. The paradox of desire is that it posits retroactively its own cause, i.e., an object that can be perceived only by the look "distorted" by desire, an object that does not exist for an "objective" look. In other words, the objet petit a is always, by definition, perceived in a distorted way, because, outside this distortion, "in itself," it does not exist, i.e., because it is nothing but the embodiment, the materialization of this distortion, of this surplus of confusion and perturbation introduced by desire into so-called "objective reality." Objet petit a is "objectively" nothing, it is nothing at all, nothing of the desire itself which, viewed from a certain perspective, assumes the shape of "something." It is, as is formulated in an extremely precise manner by the queen in her response to Bushy, her "something grief" begot by "nothing" ("For nothing hath begot my something grief "). Desire "takes off" when "something" (its object-cause) embodies, gives positive existence to its "nothing," to its void. This "something" is the anamorphic object, a pure semblance that we can perceive clearly only by "looking awry." It is precisely (and only) the logic of desire that belies the notorious wisdom that "nothing comes from nothing." In the movement of desire, "something comes from nothing." It is true that the object-cause of desire is a pure semblance, but this does not prevent it from triggering off a whole chain of consequences which regulate our "material," "effective" life and deeds.

#### Extinction justifies sacrificing the lesser number

Kateb 92 – Prof Politics, Princeton (George, The Inner Ocean, p 12)

The state (or some other agent) may kill some (or allow them to be killed), if the only alternative is letting every-one die. It is the right to life which most prominently figures in thinking about desperate situations. I cannot see any resolution but to heed the precept that "numbers count." Just as one may prefer saving one's own life to saving that of another when both cannot be saved, so a third parry—let us say, the state—can (perhaps must) choose to save the greater number of lives and at the cost of the lesser number, when there is otherwise no hope for either group.

#### Upholding life is the ultimate moral standard.

Uyl and Rasmussen, profs. of philosophy at Bellarmine College and St. John’s University, 1981 (Douglas Den and Douglas, “Reading Nozick”, p. 244)

Rand has spoken of the ultimate end as the standard by which all other ends are evaluated. When the ends to be evaluated are chosen ones the ultimate end is the standard for moral evaluation. Life as the sort of thing a living entity is, then, is the ultimate standard of value; and since only human beings are capable of choosing their ends, it is the life as a human being-man's life qua man-that is the standard for moral evaluation.

#### 5. Domination is inevitable

Thayer, ‘4 [Bradley, Associate Professor for the Department of Defense & Strategic Studies and a former Fellow @ the Belfer Center for Science and International Affairs at the Kennedy School of Government at Harvard University, Darwin and International Relations: On the Evolutionary Origins of War and Ethnic Conflict]

Evolutionary theory allows realists to advance offensive realist arguments without seeking an ultimate cause in either the anarchic international state system or in theological or metaphysical ideas. Realism based on evolutionary theory reaches the same conclusions, but the ultimate causal mechanism is different: human evolution in the anarchic and perilous conditions of the late-Pliocene, Pleistocene, and most of the Holocene epochs. Specially, evolutionary theory explains why humans are egoistic, strive to dominate others, and make in-group/out-group distinctions. These adaptations in turn serve as a foundation for offensive realism. The central issue here is what causes states to behave as offensive realists predict. Mearsheimer advances a powerful argument that anarchy is the fundamental cause of such behavior. The fact that there is no world government compels the leaders of states to take steps to ensure their security, such as striving to have a powerful military, aggressing when forced to do so, and forging and maintaining alliances. This is what neorealists call a self-help system: leaders of states are forced to take these steps because nothing else can guarantee their security in the anarchic world of international relations. I argue that evolutionary theory also offers a fundamental cause for offensive realist behavior. Evolutionary theory explains why individuals are motivated to act as offensive realism expects, whether an individual is a captain of industry or a conquistador. My argument is that anarchy is even more important than most scholars of international relations recognize. The human environment of evolutionary adaptation was anarchic; our ancestors lived in a state of nature in which resources were poor and dangers from other humans and the environment were great-so great that it is truly remarkable that a mammal standing three feet high-without claws or strong teeth, not particularly strong or swift-survived and evolved to become what we consider human. Humans endured because natural selection gave them the right behaviors to last in those conditions. The environment produced the behaviors examined here: egoism, domination, and the in-group/out-group distinction. These specific traits are sufficient to explain why leaders will behave, in the proper circumstances, as offensive realists expect them to behave. That is, even if they must hurt other humans or risk injury to themselves, they will strive to maximize their power, defined as either control over others (for example, through wealth or leadership) or control over ecological circumstances (such as meeting their own and their family’s or tribe’s need for food, shelter, or other resources). Evolutionary theory explains why people seek control over environmental circumstances-humans are egoistic and concerned about food-and why some, particularly males, will seek to dominate others by maintaining a privileged position in a dominance hierarchy. Clearly, as the leaders of states are human, they too will be influenced by evolutionary theory as they respond to the actions of other states and as they make their own decisions.

#### Rule of law is inevitable and key to prevent the worst parts of realism - key to solve extinction

Moshev, Outstanding Achievement in Journalism and Mass Communication at American University in Bulgaria, 2003 (Mois Oct 15, “Realism is Still the Best Perspective”)

The basic implication for the relevance of realism would be instability in the international system and the possibility (or presence) of war. Even at this very moment it is quite possible that some country is secretly (or openly like the USA or Israel) arming and getting ready to aggressively act on its own interests. At least a few such interests could be listed: territorial claims (say, in the Middle East or India to name just a couple), charges in unilateralism and imperialism (e.g. some European states can blame the US for that), national security (Israel attacking Syria or US attacking North Korea). Besides, there are wars going on in Africa, India/Pakistan, and the Middle East. These facts and possibilities confirm the fundamental assumption of realism: human nature is bad, and therefore people are not able to govern themselves. If this happened (which would mean complete anarchy on all levels) it may lead to total destruction of humanity – ethnical conflicts may break out everywhere, for instance. The lack of rationality and reason in people should be made up for by a rational state. Since the existence of a government is necessary, then war is necessary, or as Randolph Bourne argues, “War is the health of the State”1 – it unites the people and starts processes that improve production and economy (but helps the ruling elite more). Therefore, war has not been left behind – anarchy requires it. Despite all the liberal talks about international bodies, which aim at reducing anarchy, states are far from being protected from aggression or other problems. Most of these bodies are merely economical, and most simply do not work. The United Nations (often blamed for too much talk, little action) did not stop the US from attacking Iraq. The World Bank and the IMF did not help reduce poverty in Africa and Southern America. These bodies were simply an attempt of gaining influence/power over other states and have never really succeeded. Even international organisations that ‘work’ are more like forums and the actual implementation of their ideas happens mainly within and through a state. The country that is considered by some the most ‘globalised’ (actually globalising) – the USA – is simply acting for its own security. Since the election of Roosevelt (1932) and the introduction of the New Deal (and even before that) the United States have been acting in a very ‘realistic’ manner – strong nation, thriving economy, huge accumulation of power2, some even claim developments towards fascism. Events like 9/11 3 strengthened issues of national security. The War on Terrorism and the Patriotic Act (and possibly the War on Drugs) are a straightforward effort of preserving US security. An approach other than realistic would fail to control such a huge population (China although a communist state is rather realistic too). Leo Strauss, the ‘conservative king of America’, whose ideas shaped US foreign policy during and after the Reagan administration, asks “Are political entities, not compelled to use force and fraud … if they are to prosper?”4 Force is still a way to prosperity and some have no remorse for using it. The US (and UK) actions are but a reaction to an insecure international situation, which proves realism to be relevant. The current international conditions are not stable – anarchy is still present. A war is always possible, and every contrary argument would be a mere delusion. It might be argued that a large-scale war is possible at this moment. The idea of ‘democratic peace’ 5 would fail immediately if even one democratic state starts arming, or its interests are deeply offended and it reacts. The only factor that keeps a number of wars from breaking out is the balance of power – even the US have a reason for being afraid to attack directly (despite Iraq, which probably did not upset anyone’s interests too badly). The last, but not least, advantage of realism is its “practicality”6 – it is still the best perspective as long as action and function are concerned. Normative and deeply philosophical approaches rarely have actual results, in contrast to realism.

#### democracy prevents the dark sites they talk about

**Dean 4** – Prof Sociology, Macquarie U (Mitchell, Four Theses on the Powers of Life and Death, http://www.usyd.edu.au/contretemps/5december2004/dean.pdf

In a passage from the latter, Foucault shows that the genocidal character of National Socialism did not simply arise from its extension of bio-power (1979, 149-50). Nazism was concerned with the total administration of the life, of the family, of marriage, procreation, education and with the intensification of disciplinary micro-powers. But it articulated this with another set of features concerned with ‘the oneiric exaltation of a superior blood’, of fatherland, and of the triumph of the race. In other words, if we are to understand how the most dramatic forces of life and death were unleashed in the twentieth century, we have to understand how bio-power was articulated with elements of sovereignty and its symbolics. Pace Bauman, it is not simply the development of instrumental rationality in the form of modern bio-power, or a bureaucratic power applied to life that makes the Holocaust possible. It is the system of linkages, re-codings and re-inscriptions of sovereign notions of fatherland, territory, and blood within the new bio-political discourses of eugenics and racial hygiene that makes the unthinkable thinkable. The fact that all modern states must articulate elements of sovereignty with bio-politics also allows for a virtuous combination. The virtue of liberal and democratic forms of government is that they deploy two instruments to check the unfettered imperatives of bio-power, one drawn from political economy and the other from sovereignty itself (cf. Foucault, 1997a, 73-9). Liberalism seeks to review the imperative to govern too much by pointing to the quasi-natural processes of the market or of the exchanges of commercial society that are external to government. To govern economically means to govern through economic and other social processes external to government and also to govern in an efficient, cost-effective way. Liberalism also invokes the freedom and rights of a new subject - the sovereign individual. By 'governing through freedom' and in relation to freedom, advanced liberal democracies are able to differentiate their bio-politics from that of modern totalitarian states and older police states.

#### Focusing on discourse, representations and epistemology FAILS and allows for real atrocities to occur

Tuathail, 96 (Gearoid, Department of Georgraphy at Virginia Polytechnic Institute, Political Geography, 15(6-7), p. 664, science direct)

While theoretical debates at academic conferences are important to academics, the discourse and concerns of foreign-policy decision- makers are quite different, so different that they constitute a distinctive problem- solving, theory-averse, policy-making subculture. There is a danger that academics assume that the discourses they engage are more significant in the practice of foreign policy and the exercise of power than they really are. This is not, however, to minimize the obvious importance of academia as a general institutional structure among many that sustain certain epistemic communities in particular states. In general, I do not disagree with Dalby’s fourth point about politics and discourse except to note that his statement-‘Precisely because reality could be represented in particular ways political decisions could be taken, troops and material moved and war fought’-evades the important question of agency that I noted in my review essay. The assumption that it is representations that make action possible is inadequate by itself. Political, military and economic structures, institutions, discursive networks and leadership are all crucial in explaining social action and should be theorized together with representational practices. Both here and earlier, Dalby’s reasoning inclines towards a form of idealism. In response to Dalby’s fifth point (with its three subpoints), it is worth noting, first, that his book is about the CPD, not the Reagan administration. He analyzes certain CPD discourses, root the geographical reasoning practices of the Reagan administration nor its public-policy reasoning on national security. Dalby’s book is narrowly textual; the general contextuality of the Reagan administration is not dealt with. Second, let me simply note that I find that the distinction between critical theorists and post- structuralists is a little too rigidly and heroically drawn by Dalby and others. Third, Dalby’s interpretation of the reconceptualization of national security in Moscow as heavily influenced by dissident peace researchers in Europe is highly idealist, an interpretation that ignores the structural and ideological crises facing the Soviet elite at that time. Gorbachev’s reforms and his new security discourse were also strongly self- interested, an ultimately futile attempt to save the Communist Party and a discredited regime of power from disintegration. The issues raised by Simon Dalby in his comment are important ones for all those interested in the practice of critical geopolitics. While I agree with Dalby that questions of discourse are extremely important ones for political geographers to engage, there is a danger of fetishizing this concern with discourse so that we neglect the institutional and the sociological, the materialist and the cultural, the political and the geographical contexts within which particular discursive strategies become significant. Critical geopolitics, in other words, should not be a prisoner of the sweeping ahistorical cant that sometimes accompanies ‘poststructuralism nor convenient reading strategies like the identity politics narrative; it needs to always be open to the patterned mess that is human history.

## 1AR

### 1AR AT: Israel/Iran

#### Newest developments prove no war -- relations increasing now

Mathews 13 (Owen Matthews, contributing editor, June 22nd 2013, “China: the Middle East’s new power broker”, http://www.spectator.co.uk/features/8940201/china-the-middle-easts-new-power-broker/, AB)

It’s exactly ten years since Iranian dissidents first blew the cover of a secret uranium-enrichment facility under a mountain at Natanz, in a bleak stretch of desert near Isfahan. Ever since, relations between Israel and Iran have headed inexorably towards war. Israeli leaders have insisted that they are ready to launch a military strike — unilaterally if necessary — against Iran if the uranium enrichment continues. Iranian leaders, liberals and hardliners alike, have been equally adamant that the centrifuges will continue to spin. For Israeli hawks like prime minister Benjamin Netanyahu, the question has been not whether to strike Iran, but when.But in the past few weeks, the diplomatic geometry has shifted — and for the first time in a decade there are signs that the spiral towards conflict could be broken. Iran’s new president, Hassan Rouhani, has announced that he wishes to re-establish diplomatic relations with the United States. But perhaps equally importantly, China has quietly emerged as the new behind-the-scenes dealmaker in the Middle East. As the US comes closer to energy self-sufficiency and reduces its military presence in the Middle East, China is beginning to realise that its own energy security — and economic security — depends on maintaining peace in the region. After years of trying to stay out of Arab-Israeli politics, in May -Beijing invited Netanyahu and Mahmoud Abbas for talks on the Palestinian peace process. Another ultra-discreet meeting took place earlier this month at Green Templeton College in Oxford. Chinese and Israeli generals met to talk about establishing a back-channel dialogue directly between Israel, the US and Iran — with China as the honest broker.China’s interest in averting war is clear: it imports 12 per cent of its oil from Iran, and over half from the Persian Gulf. ‘To sustain its prosperity China must foster stability,’ Lord Mandelson told the delegates at the Oxford meeting. ‘China can less and less afford to sit on sidelines as conflicts worsen. China has too much at stake to continue to sit out every conflict and leave it to everyone else to deal with.’ Hitherto China, like Russia, has insisted on the principle of non-intervention in internal conflicts. It has opposed western military interventions from Yugoslavia to Iraq to Syria. ‘But the nature of the issues now facing China means it no longer has the luxury of standing by,’ said Mandelson. ‘Let us not say intervene, let us say engage. This is not interference — this is the exercise of responsibility.’ The bottom line is that the Chinese are in a unique position to break the deadlock on talks with Iran. Sanctions have undoubtedly hurt Tehran, but failed to weaken its resolve to enrich uranium. The problem is, in part, that the US and Britain are fatefully tainted in Iranian eyes by a history of meddling in Persian politics — capitulation to the Great and Little Satans would be electoral suicide. China, on the other hand, could play several vital roles. First, its status as Iran’s biggest foreign investor and trading partner puts it in a position to offer significant rewards for good behaviour — and restoring Iran’s sanctions-devastated economy is one of President Rouhani’s top priorities. Secondly, China can offer security guarantees to reassure Iran that it doesn’t necessarily need a nuclear bomb. Perhaps, Professor Sir John Hanson, an old Iran hand and former warden of Green College, suggested to the meeting, China could propose ‘a regional security organisation that does not include western powers’ — maybe within the framework of the China-led Shanghai Co-operation Organisation, which currently includes Russia and Central Asia with Iran as an official observer. Thirdly, and perhaps most importantly, China’s role as a middleman could let Iran back down without losing face — a concept central to both Chinese and Iranian cultures — or being seen to surrender to western powers. In the words of one member of the Chinese delegation, ‘If you surround an enemy from all sides, he has no choice but to fight — he has nowhere to escape to.’ Crucially, the Green Templeton meeting ended with an agreement to reconvene at a more private location with both Iranian and US representatives present.