# 1AC

**Adv 1 – Arms Race**

#### Cyberwar coming now – only policy precedent solves

Jackson 11-8

William Jackson, cyber correspondent for *GCN,* “Can't the United States and China just get along in cyberspace?,” 11/8/13, <http://gcn.com/blogs/cybereye/2013/11/us-china-cyber-diplomacy.aspx> SJE

The relationship between the United States and China in cyberspace has been anything but chummy lately. Many in this country see China as a major source of sophisticated attacks against our commercial and government infrastructures. China responds that it’s not coming from them, and that they are getting hacked also. This has resulted in a poisonous atmosphere that the EastWest Institute calls a “serious challenge” to the friendship and prosperity of both countries. “Such accusations and arguments have fueled escalations so that the relationship is now strained, making even routine dialog apprehensive,” says a report produced for EWI’s recent World Cyberspace Cooperation Summit IV. “Neither side is comfortable with the policies and practices of the other.” The paper, written by Karl Frederick Rauscher and Zhou Yonglin, offers what they call “practical, down to earth guidance” for normalizing cyber relations between the two countries. What it boils down to is, “stuff happens;” cyberspace is no different from any other political or diplomatic domain and each country should accept that. The report does not address who is responsible for launching attacks against whom, and nowhere does it suggest that either side stop hacking the other. But it does acknowledge that unrestrained hacking for criminal or political purposes strains relationships. Both the United States and China are rich in potential targets and attack platforms, and the prevailing tone of discussion between them has been one of suspicion and blame. Ten recommendations are offered to help establish trust and develop effective countermeasures to improve cybersecurity. The initial recommendations establish a framework of trust, based both on formal policy and behavior. “Each party is evaluated based on adherence to its stated policy and plan of action.” These are basic steps, the authors say, but basics to date have been neglected, creating a crisis environment.

#### US posture invites escalating cycles of attacks

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](http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?_r=4&) 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

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

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.

#### Independent of other countries, the US is picking fights

Seitz 13 <Dan, writer for UPROXX, quoting Bruce Scneiner, American cryptographer, computer security and privacy specialist, and writer. He is the author of several books on general security topics, computer security and cryptography, Cybersecurity Expert Fears The US Is Starting A Cyber War, 6/20/13, <http://www.uproxx.com/technology/2013/06/cybersecurity-expert-fears-the-us-is-starting-a-cyber-war/#ixzz2kl7Vi62u>>

Bruce Schneier is one of the most respected computer security experts in the world. Any time you hear about a researcher embarrassing some enormous corporation by revealing a massive security flaw, they were inspired by Schneier’s belief in “full disclosure,” that is, if a security flaw isn’t made public, it won’t get fixed. So when this guy says the U.S. is going out and starting wars on the Internet, you should probably listen.¶ Schneier has two concerns, one fairly direct and one more complex. The first is [pretty simple](http://widget.uproxx.com/b/24/http%3A/edition.cnn.com/2013/06/18/opinion/schneier-cyberwar-policy/index.html).¶ …we’re penetrating and damaging foreign networks for both espionage and to ready them for attack. We’re creating custom-designed Internet weapons, pre-targeted and ready to be “fired” against some piece of another country’s electronic infrastructure on a moment’s notice.¶ In other words, yeah, China is hacking American systems, but it’s not like the US is just passively sitting there. The military is going out and picking fights; look no further than [Stuxnet and Flame](http://www.uproxx.com/technology/2012/05/todays-reminder-we-live-in-the-future-cyberwarfare-is-officially-a-thing/), two pieces of malware that almost everyone is convinced are state-sponsored by the US and Israel.

#### That independently escalates

Greenwald and MacAskill 6-7 (Glen (American political commentator, lawyer, columnist, blogger, and author) and Ewan (Staff Writer for the Guardian), “Obama orders US to draw up overseas target list for cyber-attacks”, The Guardian, 6-7-13, <http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas>, RSR)

Obama's move to establish a potentially aggressive cyber warfare doctrine will heighten fears over the increasing militarization of the internet.¶ The directive's publication comes as the president plans to confront his Chinese counterpart Xi Jinping at a summit in California on Friday over alleged Chinese attacks on western targets.¶ Even before the publication of the directive, Beijing had hit back against US criticism, with a senior official claiming to have "mountains of data" on American cyber-attacks he claimed were every bit as serious as those China was accused of having carried out against the US.¶ Presidential Policy Directive 20 defines OCEO as "operations and related programs or activities … conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States government networks."¶ Asked about the stepping up of US offensive capabilities outlined in the directive, a senior administration official said: "Once humans develop the capacity to build boats, we build navies. Once you build airplanes, we build air forces."¶ The official added: "As a citizen, you expect your government to plan for scenarios. We're very interested in having a discussion with our international partners about what the appropriate boundaries are."¶ The document includes caveats and precautions stating that all US cyber operations should conform to US and international law, and that any operations "reasonably likely to result in significant consequences require specific presidential approval".¶ The document says that agencies should consider the consequences of any cyber-action. They include the impact on intelligence-gathering; the risk of retaliation; the impact on the stability and security of the internet itself; the balance of political risks versus gains; and the establishment of unwelcome norms of international behaviour.¶ Among the possible "significant consequences" are loss of life; responsive actions against the US; damage to property; serious adverse foreign policy or economic impacts.¶ The US is understood to have already participated in at least one major cyber attack, the use of the Stuxnet computer worm targeted on Iranian uranium enrichment centrifuges, the legality of which has been the subject of controversy. US reports citing high-level sources within the intelligence services said the US and Israel were responsible for the worm.¶ In the presidential directive, the criteria for offensive cyber operations in the directive is not limited to retaliatory action but vaguely framed as advancing "US national objectives around the world".¶ The revelation that the US is preparing a specific target list for offensive cyber-action is likely to reignite previously raised concerns of security researchers and academics, several of whom have warned that large-scale cyber operations could easily escalate into full-scale military conflict**.**¶Sean Lawson, assistant professor in the department of communication at the University of Utah, argues: "When militarist cyber rhetoric results in use of offensive cyber attack it is likely that those attacks will escalate into physical, kinetic uses of force."

### Adv 2 - Alliances

#### Congressional restrictions necessary for allied cooperation

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](http://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.

#### U.S. must take the lead to create international norms for a cyber world

Negroponte and Palmisano 13 <Chairs of the Independent Task Force #70, Council on Foreign Relations, Defending an Open,¶ Global, Secure, and¶ Resilient Internet, 2013, <http://www.cfr.org/cybersecurity/defending-open-global-secure-resilient-internet/p30836>>#SPS

However, as more people are connected in cyberspace and more critical¶ services such as telecommunications, power, and transportation are¶ interconnected, societies are becoming more dependent and more vulnerable¶ to disruption. Escalating attacks on countries, companies, and¶ individuals, as well as pervasive criminal activity, threaten the security¶ and safety of the Internet. The number of high-profile, ostensibly statebacked¶ operations continues to rise, and future attacks will become¶ more sophisticated and disruptive. A global digital arms trade has now¶ emerged that sells sophisticated malicious software to the highest bidders,¶ including hacker tools and “zero-day exploits”—attacks that take¶ advantage of previously unknown vulnerabilities.¶ U.S. government officials have increasingly warned of the danger of¶ a massive, destructive attack, and the government and private sector are¶ scrambling to prevent and prepare for future cyberattacks. U.S. government¶ warnings and efforts are important, but the United States should do¶ more to prevent a potential catastrophic cyberattack. It also, in partnership¶ with its friends and allies, must work to define the norms of cyberconflict.From its beginning, the Internet has been open and decentralized;¶ its development and growth have been managed by a self-organizing,¶ self-policing, and self-balancing collection of private and public actors.¶ Today, as many countries seek increased security and control over the¶ type of information and knowledge that flows across the Internet, that¶ original vision is under attack. Some nation-states are seeking to fragment¶ and divide the Internet and assert sovereignty over it; they are¶ increasing their efforts to tightly regulate social, political, and economic¶ activity and content in cyberspace and, in many cases, to suppress¶ expression they view as threatening. At the December 2012 World Conference¶ on International Telecommunications (WCIT), some countries¶ moved to rewrite a 1988 treaty so that it sanctions government control¶ of Internet technology and content. A truly global platform is being¶ undermined by a collection of narrow national Internets.¶ For the past four decades, the United States was the predominant¶ innovator, promoter, and shaper of cyberspace, but the window for¶ U.S. leadership is now closing. In Asia, Latin America, and Africa, the¶ number of networked users is rapidly increasing. Cyberspace is now¶ becoming reflective of the world’s Internet users. The United States, with¶ its friends and allies, needs to act quickly to encourage a global cyberspace¶ that reflects shared values of free expression and free markets.¶ Successfully meeting the challenges of the digital age requires a rethinking¶ of domestic institutions and processes that were designed for the twentieth¶ century. The rapid rate of technological change cannot help but outpace¶ traditional legislative approaches and decision-making processes. The¶ threats of the past were relatively slow developing and geographically¶ rooted, so there was an appropriate distribution of authorities among¶ defense, intelligence, law enforcement, and foreign policy agencies.¶ Cyberattacks, however, can be launched from anywhere in the world,¶ including from networks inside the United States, and their effects can¶ be felt in minutes. Moreover, they do not always look like attacks. Many¶ threats and actual compromises appear as little inconsistencies. Stolen¶ data is not taken away, so the losses may never be noticed, but suddenly¶ companies have new competitors or foreign actors have an uncanny¶ insight into their enemies’ activities.¶ In the United States, a lack of a coherent vision, the absence of¶ appropriate authority to implement policy, and legislative gridlock are¶ significant obstacles to global leadership. The United States should act¶ affirmatively to articulate norms of behavior, regulation, and partnership,¶ or others will do so. In addition, the effects of domestic decisions spread¶ far beyond national borders and will affect not only users, companies,¶ nongovernmental organizations (NGOs), and policymakers in other¶ countries but also the health, stability, resilience, and integrity of the¶ global Internet. The bottom line is clear: digital foreign policy must begin¶ with domestic policy.¶ The opportunities for the United States in cyberspace are great, but¶ a path needs to be found between a cyberspace that has no rules and¶ one that permits governments to abuse their sovereignty. At the same¶ time, policymakers have to realize that even the most successful digital¶ policy will have limits to what it can accomplish. The United States’¶ commitment to free speech, for example, is rooted in its history and¶ culture, just as French and German attitudes are toward appropriate¶ limits on online hate speech or the sale of Nazi paraphernalia. These¶ differences are unlikely to completely disappear no matter how well¶ policy is crafted.

#### Squo offensive cyber policy creates perception of US weakness

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.

#### Coalition building key to solve every global issue

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

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**](http://nation.time.com/2012/07/15/the-south-china-sea-from-bad-to-worse/) **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”](http://www.washingtonpost.com/opinions/the-blue-national-soil-of-chinas-navy/2011/03/18/AB5AxAs_story.html), 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](http://thediplomat.com/2012/02/04/beijings-south-china-sea-gamble/) 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](http://www.fas.org/blog/ssp/2008/04/new-chinese-ssbn-deploys-to-hainan-island-naval-base.php), 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](http://www.nytimes.com/2012/09/28/opinion/between-US-and-Asia-the-best-defense-is-dialogue.html?_r=0). 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](http://news.bbc.co.uk/2/hi/asia-pacific/1260290.stm), 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](http://www.nytimes.com/2009/03/12/washington/12web-china.html), 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](http://books.google.com/books?hl=fr&lr=&id=rqnNaG2jL7wC&oi=fnd&pg=PR9&dq=barry+posen+inadvertent+escalation&ots=0esVgPTh4H&sig=maTUiyNXIx2Oo_eJFnvxIzPcf1M) 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](http://hir.harvard.edu/the-spratly-islands-dispute-order-building-on-china-s-terms), 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](http://www.globalsecurity.org/wmd/world/china/type_92.htm)-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](http://www.reuters.com/article/2012/11/08/us-china-usa-military-idUSBRE8A705720121108), 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.**

### 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.

### Solvency

#### First, norm-setting other countries model our use of OCOs

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 implies, **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://www.anagram.com/berson/nrcoiw.pdf).", <http://articles.washingtonpost.com/2010-02-01/opinions/36895669_1_botnets-cyber-attacks-computer-attacks>

In a [speech this month on "Internet freedom](http://www.state.gov/secretary/rm/2010/01/135519.htm)," Secretary of State Hillary **Clinton** [**decried the cyberattacks**](http://www.washingtonpost.com/wp-dyn/content/article/2010/01/21/AR2010012101699.html) 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](http://www.nytimes.com/2009/04/28/us/28cyber.html?_r=2) 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](http://news.bbc.co.uk/2/hi/8033440.stm), 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](http://newsroom.mcafee.com/article_display.cfm?article_id=3617), 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 — Congress is necessary to reverse 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

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.**

#### Prez will adhere to congressional constraints- fear of political costs

Bradley and Morrison ‘13

[Curtis A., William Van Alstyne Professor of Law, Duke Law School. Trevor W., Liviu Librescu Professor of Law, Columbia Law School. Columbia Law Review 113. <http://www.columbialawreview.org/wp-content/uploads/2013/05/Bradley-Morrison.pdf> ETB]

**In addition to the constraining influence arising from the internalization of legal norms** by executive branch lawyers and other officials, **law** ¶ **could constrain the President if there are “external” sanctions for** ¶ **violating it.** The core idea here is a familiar one, often associated with ¶ Holmes’s “bad man”139: One who obeys the law only because he ¶ concludes that the cost of noncompliance exceeds the benefits is still ¶ subject to legal constraint if the cost of noncompliance is affected by the ¶ legal status of the norm. This is true even though the law is likely to ¶ impose less of a constraint on such “bad men” than on those who have ¶ internalized legal norms, and even though it is likely to be difficult in ¶ practice to disentangle internal and external constraints. ¶ Importantly, **external sanctions for noncompliance need not be** ¶ **formal. If the existence or intensity of an informal sanction is affected by** ¶ **the legal status of the norm in question, compliance with the norm in** ¶ **order to avoid the sanction should be understood as an instance of law** ¶ **having a constraining effect**. **In the context of presidential compliance** ¶ **with the law, one can plausibly posit a number of such informal** ¶ **sanctions. One operates on the level of** professional **reputation,** and may ¶ be especially salient for lawyers in the executive branch. If a lawyer’s own ¶ internalization of the relevant set of legal norms is insufficient to prevent ¶ him from defending as lawful actions that he knows are obviously beyond ¶ the pale, he might respond differently if he believed his legal analysis ¶ would or could be disclosed to the broader legal community in a way that ¶ would threaten his reputation and professional prospects after he leaves ¶ government.140 (This concern might help further explain the OLC and other Justice Department officials’ resistance to the White House in the ¶ warrantless surveillance example discussed above.) ¶ Although **fear of harm to their professional reputations may indeed** ¶ **help constrain government lawyers**, if that were the only operative ¶ external sanction in this context it would be fair to ask whether it ¶ translated into a real constraint on the President in high-stakes contexts. ¶ But it is not the only potential sanction. **A** related and perhaps **more** ¶ **significant sanction may operate directly on political leaders within the** ¶ **government, including the President himself: partisan politics**. **If being** ¶ **perceived to act lawlessly is politically costly, a President’s political rivals** ¶ **will have an incentive to invoke the law to oppose him**. Put another way, ¶ **legal argumentation might have a salience with the media, the public at** ¶ **large, and influential elites that could provide presidential opponents in** ¶ **Congress and elsewhere with an incentive to criticize executive actions in** ¶ **legal terms. If such criticism gains traction in a given context, it could** ¶ **enable the President’s congressional opponents to impose even greater** ¶ **costs on him** through a variety of means, **ranging from oversight hearings** ¶ **to,** in the extreme case, threats of **impeachment**. Thus, **so long as the** ¶ **threat of such sanctions is credible, law will impose an external** ¶ **constraint**—whether or not the President himself or those responsible ¶ for carrying out his policies have internalized the law as a normative ¶ matter. **The prospect of political sanctions might help explain,** for ¶ example, **why modern Presidents do not seem to seriously contemplate** ¶ **disregarding Supreme Court decisions**.141 **And if Presidents are constrained to follow the practice-based norm of judicial supremacy, they** ¶ **may be constrained to follow other normative practices that do not** ¶ **involve the courts**. ¶ **Work by political scientists concerning the use of military force is at** ¶ **least suggestive of how a connection between public sanctions and law** ¶ **compliance might work**. As this work shows, **the opposition party in** ¶ **Congress, especially during times of divided government, will have both** ¶ **an incentive and the means to use the media to criticize unsuccessful** ¶ **presidential uses of force. The additional political costs that the** ¶ **opposition party is able to impose in this way will in turn make it less** ¶ **likely that Presidents will engage in large-scale military operations.1**42 It is ¶ at least conceivable, as the legal theorist Fred Schauer has suggested, that ¶ **the political cost of pursuing an ultimately unpopular policy initiative** ¶ (such as engaging in a war) **goes up with the perceived illegality of the initiative**.143 If that is correct, then **actors will require more assurance of** ¶ **policy success before potentially violating the law. This should count as a** ¶ **legal constraint on policymaking even if the relevant actors themselves** ¶ **do not see any normative significance in the legal rule in question.**

#### **Focusing on the transcendent political discourse surrounding OCOs is necessary - we must begin with pragmatic solutions to state-centered problems.**

Mellor 13

The Australian National University, ANU College of Asia and the Pacific, Department Of International Relations,
“Why policy relevance is a moral necessity: Just war theory, impact, and UAVs,” European University Institute, Paper Prepared for BISA Conference 2013, DOA: 8-14-13

This section of the paper considers more generally the need for just war theorists to engage with policy debate about the use of force, as well as to engage with the more fundamental moral and philosophical principles of the just war tradition. It draws on John Kelsay’s conception of just war thinking as being a social practice,35 as well as on Michael Walzer’s understanding of the role of the social critic in society.36 It argues that the just war tradition is a form of “practical discourse” which is concerned with questions of “how we should act.”37 Kelsay argues that: [T]he criteria of jus ad bellum and jus in bello provide a framework for structured participation in a public conversation about the use of military force . . . citizens who choose to speak in just war terms express commitments . . . [i]n the process of giving and asking for reasons for going to war, those who argue in just war terms seek to influence policy by persuading others that their analysis provides a way to express and fulfil the desire that military actions be both wise and just.38 He also argues that “good just war thinking involves continuous and complete deliberation, in the sense that one attends to all the standard criteria at war’s inception, at its end, and throughout the course of the conflict.”39 This is important as it highlights the need for just war scholars to engage with the ongoing operations in war and the specific policies that are involved. The question of whether a particular war is just or unjust, and the question of whether a particular weapon (like drones) can be used in accordance with the jus in bello criteria, only cover a part of the overall justice of the war. Without an engagement with the reality of war, in terms of the policies used in waging it, it is impossible to engage with the “moral reality of war,”40 in terms of being able to discuss it and judge it in moral terms Kelsay’s description of just war thinking as a social practice is similar to Walzer’s more general description of social criticism. The just war theorist, as a social critic, must be involved with his or her own society and its practices. In the same way that the social critic’s distance from his or her society is measured in inches and not miles,41 the just war theorist must be close to and must understand the language through which war is constituted, interpreted and reinterpreted.42 It is only by understanding the values and language that their own society purports to live by that the social critic can hold up a mirror to that society to demonstrate its hypocrisy ///and to show the gap that exists between its practice and its values.43 The tradition itself provides a set of values and principles and, as argued by Cian O’Driscoll, constitutes a “language of engagement” to spur participation in public and political debate.44 This language is part of “our common heritage, the product of many centuries of arguing about war.”45 These principles and this language provide the terms through which people understand and come to interpret war, not in a deterministic way but by providing the categories necessary for moral understanding and moral argument about the legitimate and illegitimate uses of force.46 By spurring and providing the basis for political engagement the just war tradition ensures that the acts that occur within war are considered according to just war criteria and allows policy-makers to be held to account on this basis. Engaging with the reality of war requires recognising that war is, as Clausewitz stated, a continuation of policy. War, according to Clausewitz, is subordinate to politics and to political choices and these political choices can, and must, be judged and critiqued.47 Engagement and political debate are morally necessary as the alternative is disengagement and moral quietude, which is a sacrifice of the obligations of citizenship.48 This engagement must bring just war theorists into contact with the policy makers and will require work that is accessible and relevant to policy makers, however this does not mean a sacrifice of critical distance or an abdication of truth in the face of power. By engaging in detail with the policies being pursued and their concordance or otherwise with the principles of the just war tradition the policy-makers will be forced to account for their decisions and justify them in just war language. In contrast to the view, suggested by Kenneth Anderson, that “the public cannot be made part of the debate” and that “[w]e are necessarily committed into the hands of our political leadership”,49 it is incumbent upon just war theorists to ensure that the public are informed and are capable of holding their political leaders to account. To accept the idea that the political leadership are stewards and that accountability will not benefit the public, on whose behalf action is undertaken, but will only benefit al Qaeda,50 is a grotesque act of intellectual irresponsibility. As Walzer has argued, it is precisely because it is “our country” that we are “especially obligated to criticise its policies.”51 This paper has discussed the empirics of the policies of drone strikes in the ongoing conflict with those associate with al Qaeda. It has demonstrated that there are significant moral questions raised by the just war tradition regarding some aspects of these policies and it has argued that, thus far, just war scholars have not paid sufficient attention or engaged in sufficient detail with the policy implications of drone use. As such it has been argued that it is necessary for just war theorists to engage more directly with these issues and to ensure that their work is policy relevant, not in a utilitarian sense of abdicating from speaking the truth in the face of power, but by forcing policy makers to justify their actions according to the principles of the just war tradition, principles which they invoke themselves in formulating policy. By highlighting hypocrisy and providing the tools and language for the interpretation of action, the just war tradition provides the basis for the public engagement and political activism that are necessary for democratic politics.52

# 2AC

### 2AC T

We meet – the president can use OCOs right now

#### No framework for OCO use now

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]

Behind the scenes, however, the Obama administration and Pentagon ¶ officials considered heavily modifying this battle-tested approach with a radical, new addition: offensive cyberattacks.4¶ In the lead-up to the March ¶ 19 attack, the administration debated disabling and destroying the Libyan ¶ air defense network and command and control nodes through concerted ¶ computer attacks that would prevent Libyan radars from effectively tracking ¶ allied aircraft.5¶ During these discussions, the administration raised a ¶ number of questions without clear answers, most notably whether a ¶ cyberattack could trigger invocation of the requirements of the War Powers ¶ Resolution.6¶ Although ultimately deciding to rely on more traditional ¶ kinetic operations, the administration’s internal discussions highlight an ¶ emerging area of importance and uncertainty in both national security and ¶ the law: what domestic legal rules do and should govern the use of offensive cyber operations (“OCOs”), and how do these new capabilities play into the long-standing debate over the proper balance between congressional and executive war-making power?7¶ Yet a surprising amount of uncertainty exists as to which—if any— domestic laws constrain the use of OCOs and how they fit into the congressional-executive balance**.** As policymakers, scholars, and journalists ¶ have lamented, a coherent policy framework governing the use of OCOs does not exist and many questions remain unanswered.8¶ Would an attack using cyber weapons trigger the requirements of the War Powers ¶ Resolution?9¶ Would OCOs be subject to reporting requirements under the ¶ Intelligence Authorization Act?10 Conversely, do cyber operations grant the ¶ executive branch another tool with which it can prosecute attacks but avoid ¶ reporting and responding to congressional inquiries? These questions are ¶ largely unanswered both because the rise of OCOs is a relatively recent ¶ phenomenon and because much of the information about U.S. technical ¶ capability in this field is highly classified.11

We meet – we are a restriction

Don’t vote on it for a terrible interp – our interp is that a restriction is an actual restriction. What does that mean?

Just a part we also don’t restrict – that’s inevitable

They over-limit, we would have to restrict everything

Reasonability prevents a race to the bottom

### 2AC

#### Yes Cyberwar – 5 Reasons

#### A. Goldsmith 10 – U.S. broke the taboo with Stuxnet, now every country is scrambling for OCOs

#### B. Moss 13 – Low level attacks happening now, U.S. is planning to escalate

#### C. CSM 12 – No precedent difficulty in applying status quo norms

#### D. Austin 8/6 – complete military control means there is no stabilizing force

#### E. Obama’s new aggressive doctrine ensures.

Greenwald and MacAskill 6-7

(Glen (American political commentator, lawyer, columnist, blogger, and author) and Ewan (Staff Writer for the Guardian), “Obama orders US to draw up overseas target list for cyber-attacks”, The Guardian, 6-7-13, <http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas>, RSR)

Obama's move to establish a potentially aggressive cyber warfare doctrine will heighten fears over the increasing militarization of the internet.¶ The directive's publication comes as the president plans to confront his Chinese counterpart Xi Jinping at a summit in California on Friday over alleged Chinese attacks on western targets.¶ Even before the publication of the directive, Beijing had hit back against US criticism, with a senior official claiming to have "mountains of data" on American cyber-attacks he claimed were every bit as serious as those China was accused of having carried out against the US.¶ Presidential Policy Directive 20 defines OCEO as "operations and related programs or activities … conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States government networks."¶ Asked about the stepping up of US offensive capabilities outlined in the directive, a senior administration official said: "Once humans develop the capacity to build boats, we build navies. Once you build airplanes, we build air forces."¶ The official added: "As a citizen, you expect your government to plan for scenarios. We're very interested in having a discussion with our international partners about what the appropriate boundaries are."¶ The document includes caveats and precautions stating that all US cyber operations should conform to US and international law, and that any operations "reasonably likely to result in significant consequences require specific presidential approval".¶ The document says that agencies should consider the consequences of any cyber-action. They include the impact on intelligence-gathering; the risk of retaliation; the impact on the stability and security of the internet itself; the balance of political risks versus gains; and the establishment of unwelcome norms of international behaviour.¶ Among the possible "significant consequences" are loss of life; responsive actions against the US; damage to property; serious adverse foreign policy or economic impacts.¶ The US is understood to have already participated in at least one major cyber attack, the use of the Stuxnet computer worm targeted on Iranian uranium enrichment centrifuges, the legality of which has been the subject of controversy. US reports citing high-level sources within the intelligence services said the US and Israel were responsible for the worm.¶ In the presidential directive, the criteria for offensive cyber operations in the directive is not limited to retaliatory action but vaguely framed as advancing "US national objectives around the world".¶ The revelation that the US is preparing a specific target list for offensive cyber-action is likely to reignite previously raised concerns of security researchers and academics, several of whom have warned that large-scale cyber operations could easily escalate into full-scale military conflict**.**¶Sean Lawson, assistant professor in the department of communication at the University of Utah, argues: "When militarist cyber rhetoric results in use of offensive cyber attack it is likely that those attacks will escalate into physical, kinetic uses of force."

#### A. Self interest and decades of peace prove.

McClatchy 10[MCCLATCHY WASHINGTON BUREAU | BY WARREN P. STROBEL AND JONATHAN S. LANDAY, “Experts say war unlikely North, South Korea” May 25]

Although the isolated, communist North's behavior is notoriously unpredictable and sometimes seems irrational, all-out war between it and the democratic, capitalist South still seems unlikely, analysts said, given the stakes. Nevertheless, tensions on the Korean peninsula, where some 28,500 U.S. troops provide a tripwire for U.S. military intervention if the North attacks, are likely to rise in coming days. North Korea would likely lose any conflict with the South, but not before inflicting massive damage on South Korea's capital, Seoul, a 30-minute drive south of the demilitarized zone that has divided the two Koreas since 1953. U.S. intelligence officials estimate that some 11,000 North Korean artillery pieces are in sheltered positions within range of Seoul and probably could destroy much of the city before they could be knocked out. "The tensions certainly have increased," but there is no sign that North Korea is mobilizing its 1.2 million-strong military, said a U.S. defense official, who requested anonymity in order to speak more freely. "They have masses (of troops) down on the DMZ (demilitarized zone), but they do a normal shift or rotation," he said. South Korean officials said they were bracing for fresh provocations from the North, especially at sea. On Monday, South Korean President Lee Myung-bak blamed North Korea for the March 26 sinking of the corvette Cheonan, which killed 46 of its crew, and said he was curbing trade with North Korea and banning its ships from transiting South Korean waters. "That could get sort of ugly if (North Korean vessels) don't stop, and chances are they won't," said Art Brown, formerly the top U.S. intelligence analyst for East Asia. "It's unlikely they will do nothing. I tend to think they're not going to try Korean War, version two." Still, Brown and other former top U.S. officials said that serious clashes between the Koreas during the past 57 years haven't led to warfare -- and sometimes have provided opportunities for rapprochement.

### 2AC flex

#### 1. No Link – plan allows flexibility while still solving our internal links

**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)

**Balancing our desire for military flexibility** **with the need to address the fact that cyber war could**¶ **damage the U.S. significantly, it may be possible to craft international constraints short of a complete ban.**¶ An international agreement that banned, under any circumstances, the use of cyber weapons is the most¶ extreme form of a ban. In the previous chapter, we looked briefly at the proposal of a no-first-use¶ agreement, which is a lesser option. **A no-first-use agreement could simply be a series of mutual**¶ **declarations**, or it could be a detailed international agreement. **The focus could be on keeping cyber**¶ **attacks from starting wars**, not on limiting their use once a conflict has started. We could apply the pledge¶ to all nations, or only to those nations that made a similar declaration or signed an agreement.¶ **Saying we won’t be the first ones to use cyber weapons may in fact have more than just diplomatic**¶ **appeal in the international arena**. **The existence of the pledge might make it less likely that another nation**¶ **would initiate cyber weapons use because to do so would violate an international norm that employing**¶ **cyber weapons crosses a line, is escalatory, and potentially destabilizing**. **The nation that goes first and**¶ **violates an agreement has added a degree of international opprobrium to its actions and created** in the¶ global community **a presumption of misconduct. International support for that nation’s** underlying **position**¶ in the conflict **might** thus **be undermined and the potential for international sanctions increased.**

#### 2. Congressional statue that clarifies the legal limit of Cyber-war is key to warfighting – generals think that executive planning causes battlefield incoherence

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-http://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 techniques now widely labeled as torture.¶ 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. 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 Lt. Gen. Ricardo Sanchez labeled as a “clear defeat.”¶ 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. Gen. David Petraeus observed that “Abu Ghraib and other situations like that are nonbiodegradable. They don't go away.” Petraeus told the New York Times, “The enemy continues to beat you with them like a stick.” 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, are Mr. Baker and others so troubled? Actually, there are legitimate concerns about America’s cybercapabilities, but the attack on the issues is misdirected. Indeed, if Mr. Baker substitutes the word policymaker for lawyer and the word 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 cyberwar, it is not the law, per se, that represents the most daunting issue; to them, it is policy.¶ For example, retired Air Force Gen. Michael Hayden, the former head of the National Security Agency and later director of the CIA, told Congress in October 2011 that America’s cyberdefenses were being undermined because cyberinformation was “horribly overclassified.” That issue is not sourced in lawyers but in policymakers who could solve the classification problem virtually overnight if they wanted.¶ That same month, Gen. 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 cyberthreats and what specific actions it can take.” Gen. 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.¶ This gets to the “act of war” question Mr. Baker complains about. The law does provide a framework; 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 from those military commanders routinely confront in the other domains of conflict where difficult decisions frequently must be made on imperfect information.

#### 4. 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.

#### **5. No link – we only limit out LARGE SCALE, PRE\_EMPTIVE attacks – we can still respond quickly**

#### Congressional oversight gaps cause confusion and executive fights --- hampers cyber counterterror

Brennan 12 (Lt Colonel John – US Army, “United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?” 15 March 2012, Civilian Research Project; U.S. Army War College)

Although indentifying international terrorists in cyberspace is critical to successful counterterrorism operations, it is only half of the battle in bringing them to justice. Monitoring terrorists’ electronic communications is extremely important, but further work is required by the CT community to isolate, and eventually kill or capture the terrorists overseas. Manipulation or disruption of a terrorist organization’s computer networks is a potential means to this end, and it is also a possible tactic that is employed to preempt a cyber or kinetic terrorist attack.37 The laws that govern the actual manipulation of terrorists’ electronic accounts and devices in order to make them more targetable, are not explicit or simply do not exist. The primary document that gives the President of the United States the authority to conduct offensive CT cyber operations overseas is the 2001 Authorization of the Use of Military Force, which gives the president the authority to “use all necessary and appropriate force” to protect the country for further attacks.38 The extrapolation of this authority which permits the targeting of al-Qa’ida and its adherents, was employed in order to legally kill Anwar al Awlaki (an American citizen) in Yemen, and was invoked in permitting the planned (but not executed) computer network attack against his online magazine, Inspire.39 Regardless of these authorities, General Keith B. Alexander, the Commander of U. S. Cyber Command, has expressed similar misgivings as Mr. O’Connell in response to Congressional inquiries concerning the efficacy of cyber laws. During his confirmation hearings that resulted in his appointment to the post of the commander of U. S. Cyber Command in 2010, General Alexander stated that there is a, “mismatch between our technical capabilities to conduct operations and the governing laws and policies.”40 When he assumed the mantle of command of this first-ever joint and interagency cyber unit, General Alexander retained his title and position as the Director of the National Security Agency (DIRNSA). This dual command role placed him in the unique position to not only locate and intercept enemy internet communications, but to also conduct computer network attacks on the terrorists’ networks as well.41 The essence of this new command permits a more efficient cyber warfare capability which can theoretically operate seamlessly under both Titles 10 and 50 of the U. S. Code.42 With over 1.8 billion Internet users and 4.6 billion cellular phone subscribers who generate approximately 90 trillion emails per annum, the establishment of U. S. Cyber Command from within the NSA was an extremely useful beginning.43 A subordinate command to the United States Strategic Command (USSTRATCOM), Cyber Command was delegated Title 10 authority over military operations in cyberspace.44 On the other hand, Cyber Command also possesses the ability to conduct covert actions within cyber space under Title 50.45 This duplicitous legal framework is a result of current cyber policies and can create confusion over who is permitted to actually authorize a cyber operation.46 In the end, this policy friction can translate into delays while the required approvals are garnered, and could result in missing a fleeting opportunity to kill or capture a terrorist. U. S. Computer Network Operations Policy As a matter of current U. S. policy, the decision to label a computer network operation (CNO) as a traditional military activity (TMA), thereby falling under the purview of Title 10 of the United States Code (USC), or as a covert action under Title 50 of the USC, has spurred a great deal of discussion at the highest levels of the U. S. Government.47 Although cyber warfare is only one aspect of the overall current Title 10/50 debate that is raging within Congress and the various departments within the executive branch, one cannot legitimately discuss the policies that govern the approvals to conduct CNOs without touching upon this current source of friction.48 Much of the policy concerning the details of computer network operations is classified, but is gaining in importance such that many policy experts are speaking about it, some albeit from under the cloak of anonymity.49 As Andru E. Wall suggests, the confusion over Title 10 and Title 50 authorities appears to have, “…more to do with congressional oversight and its attendant internecine power struggles than with operational or statutory authorities,” despite the fact that by design, Title 10 and 50 authorities are mutually supporting and were not intended to be competing.50 Retired Admiral Dennis C. Blair (former ODNI) proclaimed that, “This infuriating business about who’s in charge and who gets to call the shots is just making us look muscle-bound.” ADM Blair went on to bemoan the “over-legalistic” approach to CT cyber--despite the fact that current cyber laws are woefully inadequate to address the, …”complexity of the global information network.”51(Wall 2011101) Current media reports indicate that the use of specially-designed cyber tools in order to target states or non-state actors requires presidential approval. An example of this approval policy was seen last year when media reports indicated that the Stuxnet cyber-worm was allegedly implanted in an Iranian nuclear facility, an act that American military cyber warriors will not publicly confirm.52 This computer virus subtly attacked the computers that controlled the enormous Iranian nuclear centrifuges and caused them to self-destruct. Although the Stuxnet infestation in Natanz was a major attack with immense international political consequences, media reporting suggests that less contentious operations against terrorists’ computer networks have taken on a similarly hierarchical approval process, even though these computer network operations support the local war fighters in Afghanistan or Iraq.53 For instance, in the early years of the Iraq war, numerous attempts to hack into terrorists’ email accounts and send erroneous information from them, in order to expose other members of AQI or cause potential organizational rifts was strictly forbidden without the approval of the CENTCOM Commander.54 The reasoning behind this elevated approval policy centers upon the fact that terrorists frequently use American or allied internet service providers (ISPs) to access and manipulate the internet during the conduct of their own cyber operations.55 The consequences of this arrangement, which could ultimately involve the U. S. Government manipulating an American or allied server network in order affect a terrorist organization, makes many national leaders leery of employing the capability in the first place.56 The ongoing debate between elements of the DoD, who feel that certain cyber operations are a traditional military activity and should be governed by the laws of armed conflict and Title 10 of the U.S. Code, and leaders within the Intelligence Community (IC) who contend that any and all cyber operations are inherently covert and should be under the purview of Title 50, shows no signs of abating. An example of this conundrum occurred in June, 2010 when the U. S. was allegedly contemplating a cyber attack on Insipire Magazine.57 The U. K.’s GCHQ Intelligence Service actually conducted an attack, dubbed “Operation Cupcake” while the CIA and Cyber Command were reportedly still haggling over whether attacking the site was a traditional military activity (TMA), thereby considered a Title 10 action, or a covert action under Title 50.58 Although this operation had little kinetic effect, it was disruptive as GCHQ managed to effectively replace the bomb-making recipes on the Inspire site with actual cupcake baking recipes.59 The delay caused by the policy debate within the executive branch ultimately led to a missed opportunity. The effect of a potential delay could have been much more significant had the stakes been higher, particularly if the purpose of the proposed CT cyber operation was to thwart an impending attack.60 Another potential genesis for the policy debate is the inconsistent verbiage used between the Military and the IC when categorizing operations in cyberspace. For example, if any data within an enemy computer network is modified, then the operation is labeled a Computer Network Attack (CNA) by the military.61 The IC considers data manipulation as an Offensive Cyber Operation (OCO), a title which is much more palatable to CT lawyers than the term Computer Network Attack, even though the intent and outcome of the operations are identical.62 The differences between these labels are frequently referenced in policy debates, which ultimately slow down the process of finding and interdicting terrorists.

### 2AC Iran DA

#### 1. Biden and Kerry are pushing the deal, negotiatons fail in the status quo AND Congress will just put them into the defense bill which Obama can’t block

Gardner 11/13 (Timothy, Reuters writer, <http://www.huffingtonpost.com/2013/11/13/congress-iran-sanctions_n_4270351.html>, “Members Of Congress Question Obama's Plea For Iran Sanctions Hold”, AB)

Vice President Joe Biden, Secretary of State John Kerry and other top officials visited Capitol Hill to warn senators that implementing the new measures could scuttle delicate talks between Iran and world powers over Tehran's nuclear program. "The risk is that if Congress were to unilaterally move to raise sanctions it could break faith in those negotiations and actually stop them and break them apart," Kerry told reporters before the closed-door briefing. But some key lawmakers said after the meeting that they had not been convinced. "It was a very unsatisfying briefing," said Senator Bob Corker, the top Republican on the Senate Foreign Relations Committee. However the banking committee acts, some senators said they might sidestep the panel and insert a tough new Iran sanctions measure into the annual defense authorization bill, which Obama would find hard to veto. Republican Senator Lindsey Graham, a member of the Senate Armed Services Committee, said that was one possible route for new sanctions. He dismissed Kerry's assertion that new sanctions would torpedo the Geneva talks.

#### 2. DA not intrinsic – it’s in the agenterial ambit of the US to do both

#### 3. If easing sanctions do pass, they won’t be enough to do anything—only small relief will go through

Gardner and Zengerle 10/16

[10/16/13, Timothy Gardner and Patricia Zengerle, “Any U.S. sanctions relief on Iran likely to start slowly”, http://www.reuters.com/article/2013/10/16/us-usa-iran-relief-idUSBRE99F14P20131016]

Any easing by Washington of sanctions on Iran in exchange for Tehran taking steps to scale back its nuclear program is likely to be fleeting and symbolic, with any moves for bigger concessions likely to be blocked by Congress. At talks in Geneva on the nuclear program with six world powers on Tuesday, Iran's negotiators presented a proposal on defusing a decade-old standoff. But both sides said it was too early to talk of a breakthrough Even if Iran promises to take serious steps, it is unlikely to satisfy key members of the US Congress, which generally takes a harder line on Iran than President Barack Obama's administration. Lawmakers including Robert Menendez, the chairman of the Senate Foreign Relations Committee, have signaled they want Tehran to stop even low-level enrichment of uranium used in generating power before they would take steps to wind down existing sanctions, or even agree not to put through tougher ones. "Sanctions relief is easier said than done," said Ali Vaez, an Iran analyst at the International Crisis Group, an organization that seeks to prevent and resolve conflict. "Without a fundamental reorientation of Iran's approach, a significant relaxation in sanctions is not in the cards." The sanctions Washington would likely wind down first are morsels such as easing restrictions on medical supplies, travel and the sale of spare airplane parts and service for US-built aircraft in Iran. "Many of these are low impact, they are not going to turn Iran's economy around," said Greg Theilmann, a fellow at the Arms Control Association, and a former top intelligence official at the State Department.

#### 4. Deal will be ineffective and wont solve stability

Rafizadeh 11/15 (Dr. Majid Rafizadeh, an Iranian-American political scientist and scholar, is president of the International American Council and he serves on the board of Harvard International Review at Harvard University. Rafizadeh is also a senior fellow at Nonviolence International Organization based in Washington DC and a member of the Gulf project at Columbia University. He served as ambassador for the National Iranian-American Council, conducted research at Woodrow Wilson International Center for Scholars, and taught at University of California Santa Barbara, “Iran has never been ready for a nuclear deal”, <http://english.alarabiya.net/en/views/news/middle-east/2013/11/15/Iran-has-never-been-ready-for-a-nuclear-deal.html>, AB)

One of the crucial repercussions and negative consequences of the Obama administration’s rush to make a deal with Iranian leaders would be the alienation of many American allies in the region. The geopolitical, geostrategic, and security concerns of American regional allies have not been addressed in case Iran does indeed become a nuclear power soon. A one-sided deal, or striking any deal with Iran that would give them the time to reach the nuclear breakaway capacity, will have a tremendous impact on the security of other regional countries, as well as on Iran’s regional hegemonic ambitions and the overall balance of power in the region. Finally, by reaching an ineffective deal and by currently allowing Iranian leaders to play games with these talks, Obama’s administration is giving Iran the time to reach the nuclear breakaway capacity and become the region’s nuclear power.

#### 5. No PC

Feldman 11/16/13 (Eric Bolling, Guilfoyle Battle Juan Williams Over How ‘Destructive’ Obama’s Been, <http://www.mediaite.com/tv/eric-bolling-guilfoyle-battle-juan-williams-over-how-%E2%80%98destructive%E2%80%99-obamas-been/>, AB)

The main issue Bolling raised was whether the Obamacare rollout trainwreck is proof positive of the absolute collapse, or at least remission, of liberalism. Michelle Fields pointed out that people used to be so confident Obama would be “liberalism’s reviver and savior,” and now he’s just “digging its grave.” Guilfoyle contended Obama has “no political capital or goodwill left,” and it’s shown the American people what kind of sickness big government really brings.

#### 6. Obama will just veto the bill if he doesn’t like it

7. Opposition to sanctions now

Brown 11/15 (Hayes Brown, think progress writer, 11/15/13, “Push For More Sanctions On Iran Draws Scant Support In Congress”, <http://thinkprogress.org/security/2013/11/15/2949351/iran-sanctions-letter/>, AB)

A letter urging the Senate to pass further sanctions on Iran’s nuclear program failed to receive half as many supporters as a letter earlier this year calling on the Obama administration to increase diplomatic overtures towards Tehran. House Homeland Security Committee chairman Rep. Michael McCaul (R-TX) spearheaded the more recent letter, which urges the Senate’s leaders to take up a package of new sanctions against Iran that passed the House earlier this year. “The possibility of tighter sanctions will enhance our leverage in the nuclear standoff between the Iran’s Supreme Leader and the international community,” the letter argues. “We should ensure that tougher penalties will be available should Tehran be found to be using the negotiations as a stalling tactic.” McCaul’s letter is heralded as bipartisan on the site of Rep. Grace Meng (D-NY), with 53 Republicans and 10 Democrats having signed onto the document. However, the letter’s 63 signatories don’t match up with a message to President Obama earlier this year pressing for an increase in diplomacy with Iran while warning of taking actions that might throw any talks off. That effort bore the signatures of 128 members of the body, more than a quarter of the House’s total membership, including 16 Republicans.

### A2 Iran Mod

#### The risk of prolif is low – too expensive

Tepperman 9

Jonathan Tepperman Newsweek Aug 29, 2009 “Why Obama Should Learn to Love the Bomb” <http://www.newsweek.com/id/214248/page/1>

The risk of an arms race—with, say, other Persian Gulf states rushing to build a bomb after Iran got one—is a bit harder to dispel. Once again, however, history is instructive. "In 64 years, the most nuclear-weapons states we've ever had is 12," says Waltz. "Now with North Korea we're at nine. That's not proliferation; that's spread at glacial pace." Nuclear weapons are so controversial and expensive that only countries that deem them absolutely critical to their survival go through the extreme trouble of acquiring them. That's why South Africa, Ukraine, Belarus, and Kazakhstan voluntarily gave theirs up in the early '90s, and why other countries like Brazil and Argentina dropped nascent programs. This doesn't guarantee that one or more of Iran's neighbors—Egypt or Saudi Arabia, say—might not still go for the bomb if Iran manages to build one. But the risks of a rapid spread are low, especially given Secretary of State Hillary Clinton's recent suggestion that the United States would extend a nuclear umbrella over the region, as Washington has over South Korea and Japan, if Iran does complete a bomb. If one or two Gulf states nonetheless decided to pursue their own weapon, that still might not be so disastrous, given the way that bombs tend to mellow behavior.

#### No impact to Iran proliferation.

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.

#### **6. 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.”

#### 7. Mission failure is inevitable without Congressional deliberation

**Griffin 12** – Professor of Constitutional Law @ Tulane University [Stephen Griffin, “The Tragedy of the War Power: Presidential Decisionmaking from Truman to Obama,” APSA 2012 Annual Meeting Paper, July 15, 2012, Pg. http://ssrn.com/abstract=2107467

As a comparison of the relative ability of the executive and legislative branches to make speedy decisions, Hamilton’s argument is certainly plausible as far as it goes, but in the kind of government we have had since the Cold War began, it does not take us very far. Swift decisionmaking has little to do with a presidential decision to initiate the kind of war that has occupied us here. Wars involving the potential of thousands of American casualties, millions of foreign casualties, and the expenditure of hundreds of billions of dollars are usually not based on off-the-cuff decisions. Korea (especially taking into consideration the decision to cross the 38th parallel), Vietnam and the 1991 Gulf War were enormous undertakings and required layers of complex interagency decisionmaking, not a single swift move. Indeed, these considerations were part of what made it necessary in 1947 to establish the NSC to coordinate policy within the executive branch.

During the Cold War and after, the pre-Pearl Harbor constitutional order was identified with isolationism and no one thought a return to that policy after 1945 was realistic. But while it is relevant to ask if there was an alternative, there is no escaping the ineluctable reality that the post-1945 order was a tragedy waiting to happen. That order was inconsistent with the historical meaning of the Constitution and the original constitutional order remained relevant to making decisions for war. Whether the post-1945 order was necessary or not, it introduced deep tensions into the American system of governance.

The case studies presented above show that the interagency process taking place inside the executive branch was not an adequate substitute for the constitutionally mandated interbranch process. The inability of the executive branch to deliberate and make effective decisions on its own manifested itself in surprising ways. The executive branch has repeatedly failed to engage in effective war planning. With respect to Korea, Truman had to cope with the novelty of limited war and the fact that he would have been criticized by Republicans if he had ordered MacArthur to stop at the 38th parallel to restore the status quo ante. Nonetheless, it was his decision alone to unite the peninsula, a decision made essentially on the fly. In turn, that caused China to intervene. Korea then became a conflict of unanticipated scope that ended in stalemate and ruined Truman’s last years in office. True to his initial decision to intervene, Truman did not share responsibility with Congress and so Congress escaped both a valuable learning experience and the blame for the war.

In addition, the case studies show that there is considerable evidence that the executive branch has had problems determining on war aims. President George H. W. Bush studiously avoided consulting Congress during the crucial period of decision in fall 1990 when it became possible to contemplate turning Operation Desert Shield into Desert Storm. This meant that he did not have to resolve on a unified set of war aims that would have been a necessary part of convincing Congress to authorize the war. Like Truman, Bush waited until it was too late to convince Congress and the public that the war had a point beyond forcing Iraq out of Kuwait. Thus the war had no substantial implications for policy and could not even help Bush remain in office. Not submitting the war to a timely congressional decision that Bush would have respected turned out not only to be counterproductive in terms of policy, but contrary to Bush’s political interests. Similarly, President George W. Bush failed to clarify what the war in Afghanistan was for beyond the removal of al Qaeda from Afghan territory. Partly as a consequence, the war became an endless struggle against the Taliban in both Afghanistan and Pakistan that is still ongoing as of 2012. It is striking that the executive, often represented by presidentialists as the branch that is most decisive and expert on matters of war, could consistently both fail to deliberate and fail to reach agreement on its goals in going to war. This suggests strongly that the pressures to shirk hard choices are too great to be overcome by one branch working alone. As I have argued throughout this article, the post-1945 constitutional order tended to derange the policy process inside the executive branch, producing not a set of swift successful decisions, but rather a series of policy disasters. The formulation of policy on Vietnam in the Johnson administration, for example, showed serious deficiencies that have not been taken into account by contemporary presidentialists. In essence, the advisers in the White House and the different departments in the executive branch found it impossible to move beyond the narrow orbit established by the president. Rather, the president and the idiosyncratic process he establishes tends to dominate the undoubted policymaking expertise of the different departments. The lack of planning for the aftermath of the Iraq War, with the president and policymakers in the White House falling prey to all sorts of false assumptions, showed that nothing had changed since Vietnam. I have also highlighted the costs of decisions for war on presidents. In doing so, I am not arguing that presidents who go to war suffer some sort of trauma. But there is good evidence that decisions for war are considerably different from other sorts of policy decisions. They can clearly impair presidential decision making, as was the case with Presidents Johnson and Nixon and probably both Bushes, father and son. There can be other, more subtle effects on policy. War can take up so much of the president’s time that other pressing concerns, including those related to foreign affairs, are crowded out. So President Johnson probably lost several chances to negotiate meaningful arms control agreements with the Soviet Union.217 This helped undermine the structure of détente in the 1970s by continuing the arms race. Preparing for and fighting the 1991 Gulf War so exhausted President Bush and his advisers that they had less capacity to make decisions with respect to the postwar environment in Iraq.218 This helped undermined the credibility of Bush’s decision not to depose Saddam Hussein. The 2003 Iraq War so consumed President George W. Bush and his advisers that they lost track of the situation in Afghanistan, leaving to President Obama the knotty task of sorting out the mess. As the discussion in this article has thus demonstrated, the defects of the post-1945 constitutional order are manifest. Experience has shown that the executive branch is incapable of handling the deliberation necessary for decisions for war on its own. Perhaps this is what we should expect, given the continued tidal pull of the original constitutional order. Yet it is still striking how consistently poor executive decision making for war has been in the post-1945 period. These defects create several distinct challenges for executive enthusiasts. For example, supporters of the presidentialist position often stress its unitary character. With a single person at the helm, the executive branch can act quickly to address foreign crises. We can now see more clearly that when the executive branch is not subject to oversight it is too easy either for presidents to dominate their advisers, thus suppressing valuable policy input (Johnson) or to so rearrange the White House policy process that an effective decisionmaking process becomes nearly impossible (Bush II). This supports the inference, which may come as a surprise to presidentialists, that a chief purpose of interbranch deliberation is to ensure that the executive branch is truly unitary and effective with respect to the all-important decision for war. Oversight also has the potential to counter the scenario in which the president totally dominates his advisers. Congressional hearings might give advisers a public forum in which they can finally get through to the president, although this is obviously a more difficult case. Without oversight, policy in the executive branch can be unsound or even deranged. One pathway to policy disaster, seen in Vietnam, is that the various departments responsible for war are never forced to agree on a unified set of goals and what means are necessary to achieve those goals. Without strong external compulsion it is too easy for the different parts of the executive branch to fall to quarreling amongst themselves without any ability to resolve their differences. When the State Department, Defense Department and the CIA fail to agree, the NSC process has been insufficient to create a consensus on a proposed course of policy. While it is reasonable to assume that the nation requires a unified foreign policy, nothing in the internal architecture of the executive branch that guarantees unity. Again, this can strike us as surprising, because the executive branch is a hierarchy and we expect presidents to have the ability to lead. Experience shows, however, that leadership is usually expressed either through domination involving the suppression of dissident views or by the president being unable or unwilling to manage the many different parts of the executive branch together with their often strong-willed department heads. Striking the appropriate balance has been difficult for presidents who are, after all, politicians, not experienced managers. Another pathway to disaster already mentioned is that it has proven difficult for the executive branch to determine war aims. Understandably the president and his advisers tend to respond to the exigencies of the moment, rather than concerning themselves with how a given military operation relates to the overall strategy of the U.S. in foreign affairs. The executive branch does not have any inherent ability to relate short-term responses to long-term goals. As we saw with the 1991 Gulf War, this inability to justify a war in terms of long-term goals can run contrary to the president’s own political interests. It is not necessary to assume anything about the policy knowledge of individual members of Congress or the quality of congressional hearings to appreciate that a world in which the executive branch is required to justify itself publicly provides a significant incentive for the president to insist on a unified approach to policy. It is plausible that repeated iterations of oversight would build up congressional expertise in foreign policy and thus begin a meaningful cycle of accountability where each branch could learn over time from experience. While there is a sense in which everyone accepts that oversight is a traditional function of Congress, it is noteworthy that there was no strong tradition of external review established in the early Cold War. The situation with respect to the CIA eventually became notorious, with a small group of senators handling oversight on a basis akin to a private club.219 But the situation with respect to foreign affairs in general was little better, with many hearings and exchanges held in executive session or off the books in private gatherings. While it is a mistake to think that the congressional leadership had no influence over the early Cold War administrations, the lack of public oversight meant that the proper incentives were never provided to executive branch agencies. As recounted by historian Robert Johnson, later in the Cold War the influence and prestige of the Senate Foreign Relations Committee waned in comparison with the growing power of the Armed Services Committee.220 This further undermined accountability and was emblematic of the dominant militarized approach to the Cold War. While the executive branch was retooled to a certain extent for Cold War duty after 1947, nothing was done to the structure of Congress. Members of Congress assumed that the existing committee structure would suffice. Eventually the costs of this approach became apparent, at least with respect to intelligence policy. Part of the intelligence reforms of the 1970s was to establish committees to oversee the intelligence community. The subsequent difficulties with implementing this oversight have been well analyzed by a number of scholars and presidential commissions, including the 9/11 Commission. Some of the ignored proposals of the 9/11 Commission had to do with changes to congressional oversight of intelligence.221 What oversight there is has been rendered less effective by the use of term limits for service on the intelligence committees and the fact that budgetary authority is located elsewhere.222 As Amy Zegart concluded in her study of Congress, the intelligence community and 9/11: It was no secret that this fragmented oversight system desperately needed fixing. Restructuring the Congress was recommended in seven of the twelve intelligence and terrorism studies between 1991 and 2001. Yet Congress never acted. In fact, Congress was the only government entity that failed to implement a single recommendation for reform during the decade—a record worse than either the CIA’s or the FBI’s.223 One purpose of the interbranch cycle of accountability is to test the executive branch’s claims with respect to war and foreign affairs. Of all the shibboleths of the Cold War, none have arguably done more harm than the idea that the executive branch’s undoubted expertise with respect to diplomacy is relevant to the expertise necessary for planning and running a war. The experience of presidential administrations in the post-1945 period is clear – there is no such thing as a civilian “expert” in making the policy choices and decisions necessary for war. Even if we accept the reasonable point that military leaders are expert in planning and running military operations, this sort of expertise is built up over many years of service and such experience was not available to any post-1945 president except Eisenhower. Consider that the substantial expertise FDR had acquired with respect to foreign policy by the time he was elected to a third term in 1940 is barred to any contemporary president by the 22nd Amendment. Further, cabinet officials and advisers are rarely drawn from a pool of those expert in war. As we drew away from the World War II generation, the Secretaries of State and Defense have usually been different sorts of careerists or politicians. While there is nothing inherently wrong with this, none of them were experts in making war decisions.224 In fact, there have been too few major wars for any civilian adviser to acquire the sort of experience necessary before true expertise is possible. At the same time, the major wars since 1945 show that effective consultation with Congress is pragmatically possible. Because American armies have been fighting far from home in the post-World War II period, considerable time has been required to transport them to the theatre of conflict and assemble the necessary enormous amount of supply material. Aside from true crises such as the 1962 Cuban missile crisis, there has always been plenty of time for interbranch deliberation over the decision to go to war. This has not always been highlighted by presidents. In Korea, many weeks were required before the Inchon landing and break-out from the Pusan perimeter became possible. In Vietnam, it took two years, until 1967, for General Westmoreland to assemble the supply chain necessary to support the kind of military operations he envisioned in 1965.225 The build-up time required to simply provide an effective defense for Saudi Arabia (Operation Desert Shield) in the Gulf War was seventeen weeks. More weeks were required to attain an offensive capability. Months were required after 9/11 before there were sufficient regular armed forces in Afghanistan and the same was true for the Iraq War. The fact of a crisis or apparent emergency that arguably requires a military response does not necessarily mean that there is little time for proper interbranch deliberation. The war powers debate should occur on the terrain of a realistic appraisal of presidential success in making decisions for war and the possible contributions a true interbranch dialogue could make to effective decisionmaking. Such an appraisal is not found in recent works by executive enthusiasts. Eric Posner and Adrian Vermeule, for example, have recently provided a provocative theoretical grounding for executive enthusiasm. 226 They present a tightly woven argument that challenges what they describe as the “Madisonian” understanding of separation of powers. Their target, which they call “liberal legalism,” is the idea that the executive can be constrained primarily through legal means, including the constitutional law promulgated by judges as well as statutes passed by Congress.227 While their argument is wide-ranging, extending to administrative law and “global liberal legalism,” my comments here are directed at the parts of their argument most nearly relevant to war and foreign affairs. There is arguably a subtle bias in the Posner and Vermeule analysis. They criticize the eighteenth-century “Madisonian” view of how an executive should be constrained. But why constrain the executive at all? Here Posner and Vermeule confine themselves to critiquing what might be called an eighteenth-century view of the dangers posed by the executive – chiefly the threat to civil liberties and the possibility, which they rightly discount, that the American term-limited president might turn into a tyrant.228 But they do not consider reasons for caution about the executive branch connected with our twentieth-century experience with war and foreign affairs. They believe one fatal problem with liberal legalism is that Congress can never catch up with emergencies. The nature of emergencies is that rules cannot be created in advance to handle them. By contrast, the executive is well suited to handling fast-changing situations – “in emergencies, only the executive can supply new policies and real-world action with sufficient speed to manage events.”229 While this is superficially plausible, it will have a strange ring to anyone who lived through Hurricane Katrina in 2005. Of course, this does not mean Congress somehow would have done better. Posner and Vermeule’s analysis is relentlessly comparative. The fact that the executive inevitably makes mistakes and fails sometimes does not show that liberal legalism is a workable alternative. What Posner and Vermeule do not consider is the enormous influence, amply demonstrated by the narrative I have presented, of the original constitutional order. Because Posner and Vermeule do not consider how constitutional orders work, they miss the significance of the original constitutional design. My argument has concerned war and foreign affairs. But it supports the general inference that the original design made it difficult for either branch to make good policy on its own. Sound policy with respect to war requires the branches to cooperate. While political parties have made such cooperation more difficult, parties are an example of how constitutional change tends to add to, rather than completely replacing, the original constitutional order.230 The discussion in this article has shown that policymaking in the executive branch becomes deranged without the oversight and input of the legislature. Posner and Vermeule have no way to account for this because they assume that executive branch is generally competent not only to execute the law but to make policy on its own. Strangely, they do not consider the generally poor record of the executive branch in war making in the post-1945 period. This period is littered not simply with mistakes, but with policy catastrophes that undermined the stability of the government as a whole. It is also noteworthy that Posner and Vermeule focus on the executive branch without managing to say much about the person of the president or how the president runs the White House. The post-World War II experience showed that the president was incapable of managing the tasks of war without the substantial support of Congress. Briefly summarized, the biggest problem with the arguments of executive enthusiasts is that they reflect pre-Vietnam understandings of how the executive branch makes decisions in foreign policy. It is as if the substantial and closely documented historical scholarship on the Vietnam War has made no impression on legal scholars who study presidential power. These scholars continue to treat the executive branch as if it were a black box full of the “best and the brightest” – knowledgeable experts willing to make hard choices and swift, yet measured and effective decisions.231 History shows differently. Conclusion War is a unique kind of policy. Even “limited” wars tend to subordinate the rest of the nation’s foreign policy to their requirements rather than the reverse. This has meant that in starting any major military conflict, the president is almost literally betting the ranch. All the more reason to ensure that there is sufficient deliberation before going forward. In the restrained phrasing of political scientist James Kurth, the U.S. would have been better off had “an authentic democratic process” been used to approve wars since 1945.232 The question for the future is whether such a process is possible. Pg. 31-37

### 2AC CP

1. Perm do both

2. Austin 8/6

#### Perm- do the plan and the counterplan

**Perm- do the counterplan**

#### Doesn’t solve any advantage- no internal link ev specific to merely shifting authority being sufficient to remedy our internal links- solvency burden is on the neg

#### 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**.

#### CP is a rubber stamp – only the aff can solve perception

Somin, George Mason Law Prof, 13 (Ilya, 4-23-13, “Hearing on ‘Drone Wars: The Constitutional and Counterterrorism Implications of Targeted Killing’: Testimony before the United States Senate Judiciary Subcommittee on the Constitution, Civil Rights, and Human Rights,” accessed 10-2-13,<http://www.law.gmu.edu/assets/files/faculty/Somin_DroneWarfare_April2013.pdf>, hec)

Alternatively, one can envision some kind of more extensive due process within the executive branch itself, as advocated by Neal Katyal of the Georgetown University Law Center. But any internal executive process has the flaw that it could always be overridden by the president, and possibly other high-ranking executive branch officials. Moreover, lower-level executive officials might be reluctant to veto drone strikes supported by their superiors, either out of careerist concerns, or because administration officials are naturally likely to share the ideological and policy priorities of the president. An external check on targeting reduces such risks. External review might also enhance the credibility of the target-selection process with informed opinion both in the United States and abroad.

Dycus

### 2AC K

#### 1. FRAMEWORK—The aff is a normative statement. Vote aff if plan is a good idea, neg if it isn’t.

#### A. Solves their offense –the impact of the K is a reason the aff is bad.

#### B. Aff choice – they arbitrarily steal 9 minutes of offense, destroys the aff’s only advantage.

#### C. Policy simulation key to creativity and decisionmaking—the detachment that they criticize is key to its revolutionary benefits

Eijkman 12

The role of simulations in the authentic learning for national security policy development: Implications for Practice / Dr. Henk Simon Eijkman. [electronic resource] <http://nsc.anu.edu.au/test/documents/Sims_in_authentic_learning_report.pdf>. Dr Henk Eijkman is currently an independent consultant as well as visiting fellow at the University of New South Wales at the Australian Defence Force Academy and is Visiting Professor of Academic Development, Annasaheb Dange College of Engineering and Technology in India. As a sociologist he developed an active interest in tertiary learning and teaching with a focus on socially inclusive innovation and culture change. He has taught at various institutions in the social sciences and his work as an adult learning specialist has taken him to South Africa, Malaysia, Palestine, and India. He publishes widely in international journals, serves on Conference Committees and editorial boards of edited books and international journal

Policy simulations stimulate Creativity Participation in policy games has proved to be a highly effective way of developing new combinations of experience and creativity, which is precisely what innovation requires (Geurts et al. 2007: 548). Gaming, whether in analog or digital mode, has the power to stimulate creativity, and is one of the most engaging and liberating ways for making group work productive, challenging and enjoyable. Geurts et al. (2007) cite one instance where, in a National Health Care policy change environment, ‘the many parties involved accepted the invitation to participate in what was a revolutionary and politically very sensitive experiment precisely because it was a game’ (Geurts et al. 2007: 547). Data from other policy simulations also indicate the uncovering of issues of which participants were not aware, the emergence of new ideas not anticipated, and a perception that policy simulations are also an enjoyable way to formulate strategy (Geurts et al. 2007). Gaming puts the players in an ‘experiential learning’ situation, where they discover a concrete, realistic and complex initial situation, and the gaming process of going through multiple learning cycles helps them work through the situation as it unfolds. Policy gaming stimulates ‘learning how to learn’, as in a game, and learning by doing alternates with reflection and discussion. The progression through learning cycles can also be much faster than in real-life (Geurts et al. 2007: 548). The bottom line is that problem solving in policy development processes requires creative experimentation. This cannot be primarily taught via ‘camp-fire’ story telling learning mode but demands hands-on ‘veld learning’ that allow for safe creative and productive experimentation. This is exactly what good policy simulations provide (De Geus, 1997; Ringland, 2006). In simulations participants cannot view issues solely from either their own perspective or that of one dominant stakeholder (Geurts et al. 2007). Policy simulations enable the seeking of Consensus Games are popular because historically people seek and enjoy the tension of competition, positive rivalry and the procedural justice of impartiality in safe and regulated environments. As in games, simulations temporarily remove the participants from their daily routines, political pressures, and the restrictions of real-life protocols. In consensus building, participants engage in extensive debate and need to act on a shared set of meanings and beliefs to guide the policy process in the desired direction

#### 2. Even if there is no objective truth, rationality can provide justified belief, and we should still act as if there were.

Sherry 96 – Suzanna, “The Sleep of Reason”, Georgetown Law Journal, Feb, lexis

In order to make even such a limited defense, however, I must first confront [\*473] the broad epistemological challenge: that truth -- or intellectual authority -- does not exist apart from the social and political hierarchies that create and sustain it. If the most radical social constructivists are right, and there is no such thing as truth or objectivity, defending the Enlightenment is like trying to collect water in a sieve. Fortunately, it is not necessary to resolve this philosophical dispute in order to proceed. First, the question I am addressing is not whether the Enlightenment reliance on reason and empiricism is in fact the only epistemology, but whether we ought to proceed as if it were, at least in the public arena. Even **if there are multiple** and contradictory **truths, some may be better suited for public adoption than others.** There is a difference between objective truth and justified beliefs, and **suggesting** that only **beliefs informed by reason are justified does not take any stand on the existence** or accessibility **of** **objective truth**. n110 Further, **neither reason nor truth need be transcendent or objective to inform debate**. As many scholars have recognized, postmodernism has not prevented us from acting as if truth exists. n111 Indeed, we can probably do no less: to act on the postmodern insights would be "like saying that, since philosophers are still debating Descartes' epistemology, one need not take notice of traffic signals in the meantime (since they might not really exist)." n112 Moreover, although it may be less relevant in "soft" disciplines like law, some truth does exist: "**If there were no facts,** surgeons couldn't operate, buildings would collapse, and **airplanes wouldn't get off the ground**." n113 Finally, as William Marshall has pointed out, the search for truth remains an important human enterprise even if objective truth does not exist, because "the human imagination is compelled not only by truth but also by the idea of truth." n114 Similarly, **even if there is no epistemology unconnected to power relationships**, we tend to -- and perhaps **we must -- behave as if there were**. It remains only to give that epistemology content.

#### 3. Aff answers their deterrence arguments – cyber weapons break down deterrence, making nuclear war actually possible,

#### 4. Permutation – do the plan and break the mental chains of deterrence. No reason these two actions are mutually exclusive.

**5. Images of nuclear apocalypse are necessary to problematize their usage**

James **Foard. 1997**. Associate Professor of Religion, Arizona State, “Imagining Nuclear Weapons: Hiroshima, Armageddon, and the Annihilation of the Students of Ichijo School,” Journal of the American Academy of Religion, http://jaar.oxfordjournals.org/cgi/reprint/LXV/1/1.pdf TBC 7/1/10)

**This ambivalence about Hiroshima has been partially ameliorated by displacing it with Armageddon in our imagination of nuclear weapons** In America **the images of the atomic bomb**, particularly after the Soviet Union's successful test in 1949 (Boyer.341), **were pressed into the service of apocalyptic speculations**, both scientific and otherwise, a process which has until recently assigned the horror that Hiroshima represented to a superpower war in an imagined future (cf. Pease'562). Specifically, **images of a nuclear Armageddon have helped us perform two sorts of cultural tasks fundamental for imagining nuclear weapons**: those involving difference and those involving representation. By "difference" I mean both **the articulation of what makes nuclear weapons different from other weapons and the consequent reflection on the different human situation engendered by them**. By "representation" I mean **the expressions which seek to describe the use of nuclear weapons and incorporate that description into structures of meaning Armageddon permits us to define the difference of nuclear weapons by their capacity to destroy the human species** in a war that no one will win. It also has suggested to many, particularly literary critics but also some nuclear strategists, that nuclear war is but an imaginary event, divorced from reality, such that all representations are, to use the most famous phrase, "fabulously textual" (Derrida'23).

#### 6. Living in the simulation does not mean we believe the simulation – we live in a world full of simulations from video-games to mock interviews, that doesn’t cause their impact.

#### 7. IR theory proves cyberwar is probable- multiple mechanisms

Junio ‘13

[Timothy J. Junio (Tim)is a doctoral candidate of political science at the¶ University of Pennsylvania and a predoctoral fellow at the Center for¶ International Security and Cooperation (CISAC) at Stanford University.¶ He also develops new cyber capabilities at the Defense Advanced¶ Research Projects Agency (DARPA). How Probable is Cyber War? Bringing¶ IR Theory Back In to the Cyber Conflict Debate, Journal of Strategic Studies, 36:1,¶ 125-133. ETB]

Two recent articles in the pages of this journal contribute to an¶ important debate about how information technology (IT) inﬂuences¶ international politics.1¶ Thomas Rid and Adam Liff argue that cyber¶ ‘war’ has never happened and probably will not happen. A fundamental¶ problem with these articles is that Rid and Liff do not commit to a¶ theoretical framework regarding the causes of war. Doing so yields an¶ opposite conclusion: international relations theory identiﬁes many¶ mechanisms that may cause violent escalation with cyber weapons.¶ This brief response article explains why cyber war is sufﬁciently¶ probable to merit serious attention from scholars and practitioners,¶ and proposes a theoretical research agenda. First, domestic political¶ factors – such as states’ command and control over cyber operations –¶ must be problematized. The principal-agent approach demonstrates¶ how variation in incentives and preferences may make militaries more¶ likely to favor cyber attack than other kinds of bureaucracies. This¶ matters in societies with poor civilian control over the military. Second,¶ the unique material qualities of IT must be evaluated alongside¶ traditional mechanisms that cause war. For instance, the attribution¶ problem and computational complexity in modeling cyber operations¶ may increase the odds of inadvertent cyber war by causing states to¶ retaliate against the wrong targets or miscalculate the potential costs¶ and gains of attacking.

#### 8. Perm do the plan and non-mutually exclusive parts of the alternative.

#### 9. Thinking about worst-case cyber scenarios is good- key to preparedness and reduces chances of cyber war

**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]

In the seminal 1983 movie about computers and war, War Games, ¶ starring a young Matthew Broderick, the tinny computer voice ¶ asked haltingly, “Do you want to play a game of thermonuclear war?” ¶ Why don’t we play a game of cyber war in order to elucidate some of ¶ the policy choices that shape a strategy. DoD runs such exercises, ¶ called Cyber Storm, annually. The CIA’s annual cyber war exercise, ¶ Silent Horizon, has been happening since 2007. For the purposes of ¶ this analysis, I’ll make the same request of you that I made of students ¶ at Harvard’s Kennedy School and national security bureaucrats sitting ¶ around the White House Situation Room conference table: “Don’t ¶ fight the scenario.” By that I mean, **do not spend a lot of time rejecting** ¶ **the premise that circumstances could happen someday that would** ¶ **result in the U.S. being on the edge of conflict with Russia or China. When U.S. cyber warriors talk about the “big one,” they usually** ¶ **have in mind a conflict in cyberspace with Russia or China**, the two ¶ nations with the most sophisticated offensive capability other than ¶ the U.S. **No one wants hostilities with those countries to happen.** ¶ **Thinking about it, for the purposes of understanding what cyber** ¶ **war would look like, does not make it more likely**. In fact, **by under­**¶ **standing the risks of our current cyber war posture, we might reduce** ¶ **the chances of a real cyber war.** **And if, despite our intentions, a** ¶ **cyber war does happen, it would be best to have thought in advance** ¶ **about how it could unravel.**¶ **Certainly, I did not want to see the attack of 9/11 happen, but I** ¶ **had chaired countless** “tabletop exercises,” or **war game scenarios,** **to** ¶ **get myself and the bureaucracy ready in case something like it did** ¶ **happen**. **When it came, we had already thought through how to re­**¶ **spond on the day of an attack and the few days thereafter**. We spent ¶ enormous effort to try to prevent attacks, but we also devoted some ¶ time to thinking about what we would do if one succeeded. **Had we** ¶ **not done so, that awful day would have been even worse**. **So**, **in that** ¶ **spirit of learning by visualizing, let’s think about a period of rising** ¶ **tensions** between the U.S. and China.

#### 10. Even if our lives are valueless, there is value in protecting future generations

Nick **Bostrom**, Professor in the Faculty of Philosophy & Oxford Martin School, Director of the Future of Humanity Institute, and Director of the Programme on the Impacts of Future Technology at the University of Oxford, recipient of the 2009 Eugene R. Gannon Award for the Continued Pursuit of Human Advancement, holds a Ph.D. in Philosophy from the London School of Economics, **2011** (“The Concept of Existential Risk,” Draft of a Paper published on ExistentialRisk.com, Available Online at <http://www.existentialrisk.com/concept.html>, Accessed 07-04-2011)

We have thus far considered existential risk from the perspective of utilitarianism (combined with several simplifying assumptions). We may briefly consider how the issue might appear when viewed through the lenses of some other ethical outlooks. For example, the philosopher Robert Adams outlines a different view on these matters. I believe **a better basis for ethical theory** in this area **can be found in** quite a different direction—in **a commitment to the future of humanity as a vast project, or network of overlapping projects, that is generally shared by the human race. The aspiration for a better society**—more just, more rewarding, and more peaceful—**is a part of this project. So are the potentially endless quests for scientific knowledge and philosophical understanding, and the development of artistic and other cultural traditions. This includes** the particular cultural traditions to which we belong, in all their accidental historic and ethnic diversity. It also includes **our interest in the lives of our children and grandchildren, and the hope that they will be able**, in turn, **to have the lives of their children and grandchildren as projects. To the extent that a policy or practice seems likely to be favorable or unfavorable to the carrying out of this complex of projects in the nearer or further future, we have reason to pursue or avoid it**. … **Continuity is as important to our commitment to the project of the future of humanity as it is to our commitment to the projects of our own personal futures. Just as the shape of my whole life, and its connection with my present and past, have an interest that goes beyond that of any isolated experience, so too the shape of human history over an extended period of the future, and its connection with the human present and past, have an interest that goes beyond that of the** (total or average) **quality of life of a population-at-a-time, considered in isolation from how it got that way**. **We owe**, I think, some **loyalty to this project of the human future. We** also **owe it a respect that we would owe it even if we were not of the human race ourselves**, but beings from another planet who had some understanding of it. (28: 472-473) **Since an existential catastrophe would either put an end to the project of the future of humanity or drastically curtail its scope for development, we** would seem to **have a strong prima facie reason to avoid it**, in Adams’ view. We also note that **an existential catastrophe would entail the frustration of many strong preferences**, suggesting that from a preference-satisfactionist perspective it would be a bad thing. In a similar vein, **an ethical view emphasizing that public policy should be determined through informed democratic deliberation by all stakeholders would favor existential-risk mitigation if we suppose**, as is plausible, **that a majority of the world’s population would come to favor such policies upon reasonable deliberation** (even if hypothetical future people are not included as stakeholders). **We might also have custodial duties to preserve the inheritance of humanity passed on to us by our ancestors and convey it safely to our descendants**.[24] **We do not want to be the failing link in the chain of generations, and we ought not to delete or abandon the great epic of human civilization that humankind has been working on for thousands of years, when it is clear that the narrative is far from having reached a natural terminus**. Further, **many theological perspectives deplore naturalistic existential catastrophes, especially ones induced by human activities**: If God created the world and the human species, one would imagine that He might be displeased if we took it upon ourselves to smash His masterpiece (or if, through our negligence or hubris, we allowed it to come to irreparable harm).[25]

#### 10. Abandoning rational epistemology ensures massive violence, destruction of debate, and death of political participation.

Sherry 96 – Suzanna, “The Sleep of Reason”, Georgetown Law Journal, Feb, lexis

Some, however, have suggested that the historical era of the Enlightenment was unique, and that epistemological pluralism would, in the modern world, create little danger of internecine warfare. 139 This optimism overlooks one of the fundamental differences between rational and **antirational epistemologies**: [\*479] because the latter **rest on faith** **rather than reason, they are likely to be impervious to persuasion and** resistant to **compromise**. 140 Moreover, without the skeptical cast of mind fostered by Enlightenment epistemology, antirational epistemologies -- especially religion, with its extrahuman source of authority -- are likely to be conducive to particularly deep conviction. **Deep conviction**, in turn, **is a breeding ground for** exactly **the religious wars of previous centuries**: In Abrams v. United States, Justice Holmes argued that a logical result of deep conviction is intolerance. As Dean Bollinger has added, failing to attempt to silence what one believes to be false might be seen as a sign of weak conviction. . . . To the zealous adherent, **intolerance and persecution become**, in a sense, **the measure of her commitment to** her religious **beliefs**. 141Even in the United States, where religion has largely been domesticated (as Michael Perry puts it), 142 we have not been spared all of the violence associated with pre-Enlightenment religious wars. Although, as Perry points out, "we are not the former Yugoslavia or India," 143 the Branch Davidians, the World Trade Center **bombers**, the abortion clinic killings, **and the growth of** various **organizations -- on the left and the right, not all** of them **religious -- that use irrational arguments to** reject and **resist the authority of government**, by violence if necessary, **should** **give us pause before abandoning the fruits of the Enlightenment**. 144 Indeed, as one historian has pointed out: If we have now entered an era in which those on the right have been joined by some on the left in assailing reason as faulty because it does not correspond to the essential and incontestable truths they have come to know emotionally, or by virtue of their membership in particular groups, the prospects for deliberative democracy are bleak indeed. . . . **If truth resides in difference** and emotion, **then war rather than persuasion is the only possible consequence** **of speaking such a truth to power**. 145

# 1AR

#### No pass – Boehner

Sherman 11-14

(Jake Sherman, covers Congress for POLITICO, “John Boehner: ‘No reason’ to lift Iran sanctions” 11/14/13, <http://www.politico.com/story/2013/11/iran-sanctions-john-boehner-99872.html>, KB)

Speaker John Boehner said the United States shouldn’t lift any sanctions on Iran until they stop “all development of their nuclear program.”¶ Speaking to reporters in the Capitol Thursday morning, Boehner said “there is no reason for us to lift” sanctions on Iran until they completely halt their nuclear program.¶ “We’ve been down this road with Iran many times,” he said.¶ The Obama administration has been seeking a deal that would temporarily relax some sanctions in exchange for Iran scaling back its uranium enrichment program. The White House, State and Treasury departments have been lobbying Senate Democrats and Republicans to hold off on additional economic sanctions aimed at Iran’s oil industry. They are meeting resistance in the Senate.¶ The House earlier this year passed a stiff Iranian sanction package.

### 2AC AT Kriner

#### Plan boosts Obama’s capital without triggering a fight over authority

Kriner 10

Douglas Kriner, Assistant Profess of Political Science at Boston University, 2010, After the Rubicon: Congress, Presidents, and the Politics of Waging War, p. 59-60

Presidents and politicos alike have long recognized Congress's ability to reduce the political costs that the White House risks incurring by pursuing a major military initiative. While declarations of war are all but extinct in the contemporary period, Congress has repeatedly moved to authorize presidential military deployments and consequently to tie its own institutional prestige to the conduct and ultimate success of a military campaign. Such authorizing legislation, even if it fails to pass both chambers, creates a sense of shared legislative-executive responsibility for a military action's success and provides the president with considerable political support for his chosen policy course.34 Indeed, the desire for this political cover—and not for the constitutional sanction a congressional authorization affords—has historically motivated presidents to seek Congress's blessing for military endeavors. For example, both the elder and younger Bush requested legislative approval for their wars against Iraq, while assiduously maintaining that they possessed sufficient independent authority as commander in chief to order the invasions unilaterally.35 This fundamental tension is readily apparent in the elder Bush's signing statement to HJ Res 77, which authorized military action against Saddam Hussein in January of 1991. While the president expressed his gratitude for the statement of congressional support, he insisted that the resolution was not needed to authorize military action in Iraq. "As I made clear to congressional leaders at the outset, my request for congressional support did not, and my signing this resolution does not, constitute any change in the long-standing positions of the executive branch on either the President's constitutional authority to use the Armed Forces to defend vital U.S. interests or the constitutionality of the War Powers Resolution."36

### 1AR Plan Popular

#### We’re bipart – senate has voted on cyber oversight bills and it’s been a landslide – that’s Perera

#### Plan’s popular - Obama will issue unpopular XOs on cyber – triggers their link

Russia Times 13

“Obama to 'bypass Congress' on CISPA with cybersecurity executive order”¶ [http://rt.com/usa/congress-executive-actions-president-958/,Feb. 11, mg]

**Unable to reach a deal with Congress,** President **Obama plans to use his power to exert executive actions against the will of lawmakers. The president will issue orders addressing controversial topics including cybersecurity**.¶ Although President Obama has issued fewer executive orders than any president in over 100 years, he is making extensive plans to change that, Washington Post reports quoting people outside the White House involved in discussions on the issues. **Due to conflicts with a Congress that too often disagrees on proposed legislation, Obama plans to act alone and is likely "to rely heavily" on his executive powers in future,** according to the newspaper.¶ Obama’s first executive order is expected to be issued this week when the president calls for the creation of new standards on what private-sector companies must do to protect their computer systems from a cybersecurity breach.¶ The order is a direct response to Congress’ refusal to pass the Cyber Intelligence Sharing and Protection Act (CISPA) last year, which the administration deemed crucial to prevent crippling attacks on the nation’s infrastructure. But members of Congress who opposed the legislation cited serious privacy concerns with giving the government greater access to Americans’ personal information that only private companies and servers might have access to.¶ **Despite opposition from lawmakers, the president will use his executive powers** to issue an order **addressing cybersecurity** initiatives.¶ “It is a very dangerous road he’s going down contrary to the spirit of the Constitution,” Sen. Charles E. Grassley (R-Iowa) told the Washington Post. “Just because Congress doesn’t act doesn’t mean the president has a right to act.”¶