# 1AC

## 1AC - Arms Races

#### Contention 1 is Arms Races

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

Goldman 13

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

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

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

Moss 13

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

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

#### Cyber arms race causes world war

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

CSM 11

Christian Science Monitor

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

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

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

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

Austin, 8/6

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

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

#### Cyberwar escalates:

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

Clarke and Knake ‘12

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

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

#### b) Pressure to retaliate

Owens et al 9

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

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

## 1AC - Alliances

#### Contention 2 is Alliances

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

Dunlap 12

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

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

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

Lord et al 11

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

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

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

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

#### Status quo cyber doctrine undermines US credibility

Lawson ‘10

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

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

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

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

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

#### Coalition building key to solve extinction

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

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

#### Legitimacy is key to band-wagon

Lee 10

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

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

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

Kazianis 12

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

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

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

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

RTT 13

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

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

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

Yoshihara 10

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

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

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

Colby et al 13

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

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

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

Rehman 13

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

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

#### Their defense doesn’t apply

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

VornDick 7/30/12

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

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

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

Dobbins et al. ‘11

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

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

## 1AC - Plan

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

## 1AC - Solvency

#### Contention 3 is solvency

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

Bradbury 11

Assistant Attorney General for the Office of Legal Counsel

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

Evolving customary law. This approach also accommodates the reality that **how the U.S. chooses to use its armed forces will significantly influence the development of customary international law.** As the label implwies, **customary law can evolve depending on the accepted conduct of major nations like the United States. The real-world practice of the United States in adapting** the use of its military **to the new challenges raised by computer warfare will** (and should) **help clarify the accepted customs of war in areas where the limits are not clearly established today.** And if you just review the literature on cyber war, you quickly see that that’s where we are: precisely how the laws and customs of war should apply to offensive cyber operations is not yet crystallized in key respects. For example, there aren’t always bright lines to tell us when a cyber attack on computer systems constitutes an “armed attack” or a “use of force” that justifies a nation in launching a responsive military strike under Article 51 of the U.N. Charter. Some questions are easy: Hacking into a sensitive government computer system to steal information is an act of espionage, not an armed attack. It’s clearly not prohibited by the laws and customs of war. On the other hand, if the cyber intrusion inflicts significant physical destruction or loss of life by causing the failure of critical infrastructure, like a dam or water supply system, then it obviously would constitute an armed attack under the law of war and would justify a full military response if it could be attributed to a foreign power. Where committed as an offensive act of aggression, such an attack may violate international law. If significant enough, the effect of the attack will determine its treatment, not necessarily whether the attack is delivered through computer lines as opposed to conventional weapons systems. In these cases, the laws and customs of war provide a clear rule to apply. But there will be gray areas in the middle. Thus, it’s far less clear that a computer assault that’s limited to deleting or corrupting data or temporarily disabling or disrupting a computer network or some specific equipment associated with the network in a way that’s not life threatening or widely destructive should be considered a use of force justifying military retaliation, even if the network belongs to the military or another government agency. This was the case with the “distributed denial of service” attacks experienced by Estonia in 2007, which severely disrupted the country’s banking and communications systems. Suspecting that Russia was behind it, Estonia suggested that NATO declare that Estonia’s sovereignty had been attacked, which would have triggered the collective self-defense article of the NATO Treaty, but that suggestion was rebuffed on the ground that a cyber attack is not a clear military action.12 There’s an echo of that reasoning in Article 41 of the U.N. Charter, which says that a “complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications” is not a “measure . . . involving armed force.” And what about Stuxnet? As I understand it from public reports, Stuxnet was a computer worm that found its way into the systems controlling Iran’s nuclear program and gave faulty commands causing the destruction of the centrifuges used for enriching uranium. Suppose President Ahmadinejad claimed that Israel was behind the Stuxnet worm and claimed that Stuxnet constituted an armed attack on Iran that justified a military response against Israel. I suspect the United States would disagree. At the same time, when it comes to a cyber attack directed against U.S. computer systems, I certainly want the President to have leeway in determining whether or not to treat the attack as a use of force that supports military retaliation. Making such judgments is a traditional power exercised by the President, and I think he retains that leeway. Similarly, I submit, it’s not clearly established that a cyber attack aimed at disrupting a server or Web site located in a neutral country or in a country outside a theater of open hostilities would be a violation of that country’s neutrality. The server might be a valid military target because it’s being used for the communications or command and control of the enemy fighters in the area of hostilities (after all, al Qaeda regularly uses the Internet in planning and ordering operations). The server might have no connection to the host country’s military, government, or critical infrastructure, and it might be readily targeted for a computer attack without inflicting widespread damage on unrelated systems used for civilian purposes. Such a focused cyber operation — with little physical impact beyond the destruction of data or the crippling of a server — is very different from the kind of physical violation of territory — such as a conventional troop incursion or a kinetic bombing raid — that we ordinarily think of as constituting an affront to neutrality. Although every server has a physical location, the Internet is not segmented along national borders, and the enemy may gain greater tactical advantage from a server hosted half way around the world than from one located right in the middle of hostilities. The targeting of a server in a third country may well raise significant diplomatic difficulties (and I wouldn’t minimize those), but I don’t think the law-of-war principle of neutrality categorically precludes the President from authorizing such an operation by an execute order to Cyber Command. Conclusion. So here’s my thesis: To my view, the lack of clarity on certain of these issues under international law means that with respect to those issues, the President is free to decide, as a policy matter, where and how the lines should be drawn on the limits of traditional military power in the sphere of cyberspace. For example, that means that within certain parameters, the President could decide when and to what extent military cyber operations may target computers located outside areas of hot fighting that the enemy is using for military advantage. And when a cyber attack is directed at us, the President can decide, as a matter of national policy, whether and when to treat it as an act of war. The corollary to all this is that in situations where the customs of war, in fact, are not crystallized, the lawyers at the State Department and the Justice Department shouldn’t make up new red lines — out of some aspirational sense of what they think international law ought to be — that end up putting dangerous limitations on the options available to the United States. Certainly, the advice of lawyers is always important, especially so where the legal lines are established or firmly suggested. No one would contend that the laws of war have no application to cyber operations or that cyberspace is a law-free zone. But it’s not the role of the lawyers to make up new lines that don’t yet exist in a way that preempts the development of policy.14 **In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention on cyberwarfare — perhaps a kind of arms control agreement for cyber weapons.** I believe **there is no foreseeable prospect that that will happen. Instead, the outlines of accepted norms and limitations in this area will develop through the practice of leading nations**. And **the policy decisions made by the U**nited **S**tates in response to particular events **will have great influence** in **shaping** those **international norms**. I think that’s the way we should want it to work.

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

Goldsmith 10

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

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

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

Lewis 11

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

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

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

Dycus 10

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

In his celebrated concurring opinion in The Steel Seizure Case, **Justice Jackson cautioned that “only Congress itself can prevent power from slipping through its fingers.” Jackson’s warning seems especially pertinent today, as we prepare urgently for cyber warfare** – facing potentially enormous threats from yet unknown enemies, and finding ourselves dependent on staggeringly complex, unproven technology.3 **The executive branch**, which has special expertise and agility in national security matters generally, as well as substantial constitutional authority, **has taken the initiative in these preparations. Yet if Congress is to be faithful to the Framers’ vision of its role in the nation’s defense, it must tighten its grip and play a significant part in the development of policies for war on a digital battlefield.** It also must enact rules to help ensure that these policies are carried out. Congress must work hand in hand with the Executive, however, to confront these evolving threats. The importance of collaborative planning can be seen in a recent exchange of correspondence in which leaders of the Senate Select Committee on Intelligence wrote to the Director of National Intelligence to ask about “the adequacy of the Director of National Intelligence and Intelligence Community authorities over cybersecurity.” The Director answered: This is a very important issue . . . . A judgment regarding the adequacy of DNI authorities and any changes, additions, or clarifications will necessarily depend on the Administration’s strategic plan on cyber, and where the center of gravity will be within the Executive branch. . . . We have more work to do in the Executive Branch before I can give you a good answer.7 The strategic, technological, and political problems described here present challenges of unprecedented complexity. The risks of error both in the formulation of a cyber warfare policy and in its execution are substantial. And despite the importance of developing a coherent, coordinated response to this threat, it seems unlikely that we will find a way to overcome entirely the endless turf battles among federal agencies and congressional committees.8 Still, the need is so pressing and the stakes are so high that we cannot afford not to try. **The very future** of the Republic **may depend on our ability not only to protect ourselves from enemies armed with cyber weapons, but also to use such weapons wisely ourselves.** This article examines some of the relevant legal issues and suggests some possible solutions. I. CONGRESS’S ROLE IN DECIDING WHEN AND HOW TO GO TO WAR There is broad agreement that congressional authorization is needed to start a war. On the other hand, the President may act without Congress’s approval to repel an attack on the United States.10 Between these two extremes, the scope of the President’s unilateral authority to use military force is less well understood.11 Once hostilities are under way, there is a consensus that the President has the tactical powers of a Commander in Chief, although it may not always be clear which of the President’s actions are tactical and which are strategic.12 Before an attack can be launched, of course, Congress must have supplied the President with personnel and weapons.13 Moreover, Congress may regulate the President’s actions as Commander in Chief, except when the nation comes under sudden attack or the President exercises her tactical powers (and perhaps even then). In the Supreme Court’s 1800 decision in Bas v. Tingy, Justice Paterson, one of the Framers, echoed the other Justices in declaring that “[a]s far as congress authorized and tolerated the war on our part, so far may we proceed in hostile operations.”14 Four years later, in Little v. Barreme, the Court reiterated that the President must not exceed limits set forth in Congress’s authorization of hostilities.15 Since then, no court has ruled otherwise.16 In the intervening two centuries, Congress has adopted a number of measures to control the initiation or conduct of warfare. At the end of the Vietnam War, for example, Congress passed the War Powers Resolution (WPR),17 which requires the President to report to Congress within 48 hours the introduction of U.S. armed forces into hostilities or imminent hostilities, and to withdraw those forces within 60 days if Congress does not expressly approve of their continued deployment.18 Lambasted by some as an unconstitutional encroachment on presidential powers, the WPR has been followed (or at least lip service has been paid to it) by each President since the Nixon administration,19 and Congress has repeatedly referred to the WPR approvingly in subsequent legislation.20 **If Congress now fails to enact guidelines for cyber war**fare, **it might be perceived as inviting “measures on independent presidential responsibility**.”21 Chief Justice Marshall suggested in Little v. Barreme that **if Congress** had **remained silent, the President might have been free to conduct the Quasi-War with France as he saw fit**.22 But the national interest in electronic warfare, just as in that early maritime conflict, is so great that the planning and conduct of such a war should not be left entirely to the Executive. And because a **cyber war might be fought under circumstances that make it impossible for Congress to play a meaningful** contemporaneous **role, Congress ought to get** out **in front of events** now in order to be able **to participate in** the formulation of national **policy.**

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

Bastby 12

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

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

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

Hansen & Friedman 9

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

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

# 2AC

## Arms Races

#### a) Probability – attribution, prolif, and absence of firebreak

Krepinevich 12

Andrew Krepinevich, defense policy analyst who currently serves as President of the Center for Strategic and Budgetary Assessments, “Cyber Warfare: A ‘Nuclear Option?’,” 2012 SJE

This assessment finds that **we are far more likely to experience major cyber attacks than we are nuclear attacks. There are several reasons for this: ATTRIBUTION.** Since World War II, states have refrained from employing nuclear weapons out of fear that such weapons might be used against them. This is deterrence through the threat of massive retaliation. This form of **deterrence requires that the victim be able to identify the source of the attack. Yet attributing the source of a cyber attack is** likely to remain both **costly and difficult**. To be sure, even the remote prospect of being identified might be sufficient to deter a risk-averse leadership from committing to a major cyber attack. But what of **highly risk-tolerant leaders**—men like Adolf Hitler, Josef Stalin, Mao Zedong and Saddam Hussein? For leaders such as these, the **prospect of inflicting major harm on their enemies while avoiding retribution could prove irresistible**. Risk-tolerant leaders may also be tempted to engage in catalytic warfare in which they play the role of a third party covertly attempting to instigate or influence a war between two other parties. In a crisis between two powers, if one were to suffer a massive cyber attack, the natural inclination might be for the victim to assume the other state party to the crisis is responsible. Circumstances such as these could provide another layer of insulation from attribution for risk-tolerant leaders. Should a radical non-state entity acquire cyber weapons capable of inflicting large-scale destruction, there may be little if any restraint on their use. Such groups may care little about avoiding attribution; in fact, they may claim responsibility for an attack. As these groups have no infrastructure against which to iv Center for Strategic and Budgetary Assessments retaliate it is not likely that deterrence through the threat of punishment will prove effective. **PROLIFERATION.** There is also the problem of numbers. **It is highly likely that many more states** (and even non-state entities) **will develop imposing cyber arsenals rather than nuclear arsenals**. With many more decision-makers possessing these weapons, it cannot but increase the odds that they will be used. The combination of large numbers of major cyber competitors—perhaps including non-state entities—with highly risk-tolerant leaders suggests a significant potential for cyber proxy wars. While it is difficult to imagine a nuclear proxy war, this is not the case with regard to cyber weapons. The apparent **willingness on the part of states to use proxies to better avoid attribution** when stealing state secrets, intellectual property, and other valuable information **could lower the barriers**, especially for risk-tolerant leaders, **to engage in large-scale cyber war** against an enemy’s critical infrastructure. **ABSENCE OF A CLEAR CYBER “FIREBREAK.” In the case of nuclear weapons**, they are either being employed or they are not; **there is a clear firebreak between use and non-use. This is not the case with respect to cyber weapons.** Thus **it may be difficult for the leadership of one cyber power to determine when, in the mind of its enemy, it has crossed the line between cyber operations that are “acceptable” and those that will trigger a major escalation in the intensity of cyber activity that could lead to catastrophic attacks**. The picture is blurred even further owing to the fact that states are constantly under cyber attack from multiple sources, not just one. Matters are made murkier still by the similarities that exist between cyber reconnaissance operations and those designed to implant cyber weapons or conduct an attack.

#### b) Timeframe - shorter response times and great risk of miscalc

Dycus 10 (Stephen, Professor, Vermont Law School, “Congress’s Role in Cyber Warfare”, Journal of National Security Law and Privacy, Vol. 4, 2010, RSR)

**Cyber weapons bear a** striking **resemblance to nuclear weapons** in some ¶ important ways. An enemy’s **cyber attack would**, like a nuclear strike, ¶ **probably come without a clear warning**. **There are** as yet **no reliable** ¶ **defenses** against either a cyber attack or a nuclear attack. Collateral ¶ damage from a nuclear attack would almost certainly be very extensive and ¶ would linger for an extended period.48 **The direct and indirect effects of a** ¶ **cyber attack**, while different in kind and degree, still **could be widespread** ¶ **and indiscriminate.**49¶ **In other ways, cyber weapons are critically different** from their nuclear ¶ counterparts. For one thing, **the time frame for response to a cyber attack** ¶ **might be much narrower.** **A nuclear weapon** delivered by a land-based ¶ ICBM **could take 30 minutes to reach its target**. **An electronic attack would** ¶ **arrive instantaneously, and leave no time to consult** with or even inform ¶ anyone outside the executive branch **before launching a counterstrike**, if ¶ that were U.S. policy. ¶ **What most distinguishes digital warfare**, however, **is the** potential ¶ **difficulty in identifying the source of a cyber attack**. It is always possible, ¶ of course, that an enemy might covertly deliver a nuclear device to the U.S. ¶ homeland in a shipping container or a Cessna. But **the** apparent **ease with** ¶ **which a cyber attack may be carried out** without attribution **could make it** ¶ **impossible to fight back** at all. **If an attacker made it appear that the source** ¶ **was** an innocent neutral state or perhaps **another** enemy of the attacker, **a** ¶ **misdirected U.S. response might provoke a wider conflict**. **The** potential **difficulty in tracking the source** also **makes** a policy of **deterrence** based on ¶ a threat of retaliation far **less credible**. ¶ Given these characteristics of cyber warfare, and the continuing ¶ refinement of cyber weaponry, we approach a state of extreme strategic ¶ instability, with each nation on hair-trigger alert. **The execution of an illconceived cyber war policy** calling for a prompt response – or any response ¶ – to an attack or threatened attack **could have disastrous, unanticipated** ¶ **consequences**. It also might, depending on the circumstances, violate the ¶ law of armed conflict.

**The US has to take the lead – we can shape norms in our favor.**

**Beidleman ‘9** (Scott, Lieutenant Colonel with the US Air Force, “Defining and Deterring Cyber War”, Strategic Research Project, 2009, RSR)

**The U.S. is uniquely suited to lead** this effort. “**The United States…acts as an**¶ **architect of global and regional security affairs for the purpose of containing new-era**¶ **dangers**.”120 More importantly, **this effort allows the U.S. to shape international norms**¶ **for states’ behavior in cyberspace in accordance with American national interests;**¶ **otherwise the U.S. risks forfeiting this advantage to other nations**. For example, **China**¶ **is engaged “in the debate of defining cyber warfare**, in part through the Shanghai¶ Cooperation Organization, **in order to have a hand in the shaping of a legal framework**¶ **and rules of engagement related to this new warfare**.”121

**NFU for cyber warfare solves cyber war between US and China**

**Thompson, 11**

(Mark, National Security writer for Time, "Cyberwishful Thinking", May 31, nation.time.com/2011/05/31/cyberwishful-thinking/ NL)

But others disagree. They argue that outlawing **major-league cyberwars** — or at least **regulating them in the same way arms-control pacts have contained nuclear weapons** — **is a** more **promising path**. “It’s like biological weapons,” says computer scientist Neil Rowe of the Naval Postgraduate School. He wants cyber weapons — just anthrax and botulism — banned by the international community. Cyberwar is just like “putting poision in a community’s water system,” he writes in a paper on “The Ethics of Cyberweapons in Warfare.”¶ Retired admiral Owens, who spent 33 years in uniform, doesn’t go that far. He’s willing to settle for what he calls “**a no-first-use cyber attack treaty**” between the U.S. and China, the two prime players in cyberspace. “A national cyber attack could have the same kinds of deaths and destruction as a nuclear attack,” he warns. Getting Beijing and Washington to commit to a no-first-use pledge, he says, **would be a gift to future generations** — “**before we get so serious about it that we’re unwilling to talk about it, or to give it up.**” But that, of course, assumes we didn’t cross that threshold yesterday.¶

## Alliances

#### Adherence to rule of law is key to international co-op on cyber

Dunlap ‘13

[Charles J. Dunlap, Jr. Major General, USAF (Ret.), Executive Director, Center on Law, Ethics, and National Security, Duke University School of Law. The Intersection of Law and Ethics in Cyberwar: Some Reflections. ETB]

Adherence to the rule of law is especially important in the cyber realm because ¶ nearly all experts agree that confronting the threat requires the cooperation of ¶ foreign countries in order to track and neutralize cyber threats – in peace or ¶ war.28 Nations vital to this effort, to include especially the world’s major ¶ democracies, doubtlessly would not be inclined to cooperate with any country ¶ that rejected limits on military operations, cyber or otherwise. Professors ¶ Michael Riesman and Chris T. Antoniou point out in their 1994 book, The ¶ Laws of War: ¶ In modern popular democracies, even a limited armed conflict ¶ requires a substantial base of public support. That support can ¶ erode or even reverse itself rapidly, no matter how worthy the ¶ political objective, if people believe that the war is being conducted ¶ in an unfair, inhumane, or iniquitous way.

#### International Actors trust congress

**Planet Washington 8/23/13**

[http://blogs.mcclatchydc.com/washington/2013/08/obama-defends-nsa-surveillance-acknowledges-public-mistrust-.html, mg]

Obama said the latest revelation of NSA survellience showed that "NSA had inadvertently, accidentally pulled the e-mails of some Americans in violation of their own rules, because of technical problems that they didn't realize."¶ He didn't say that a Foreign Intelligence Surveillence Court judge had found the agency broke the law, but did note that the judge forced changes.¶ "The point is, is that all these safeguards, checks, audits, oversight worked," Obama said.¶ **Obama said he was confident NSA wasn't abusing its authority**, but said, "what I recognize is that we're going to have to continue to improve the safeguards..and we do have to do a better job of giving people confidence in how these programs work."¶ He noted NSA has set up an "entire website" and is releasing more documents that had been classified.¶ "What I've said is that **I am open to working with Congress to figure out, can we get more transparency** in terms of how the oversight court works?" he said, adding, "there's no doubt that, for all the work that's been done to protect the American people's privacy, the capabilities of the NSA are scary to people."¶ Some **US allies have been outraged by the reports of NSA surveillance**, but Obama said many are doing the same thing.¶ "We've got to do it in the right way, we've got to do it in a way that makes sure that people know their own government is looking out for their interests, but we've also got to do it in a way that recognizes that we've got some hostile folks out there that potentially are trying to do us harm."¶ -

## Solvency

#### 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.**

#### No capability for hacker cyber attack now- state sponsorship key

Economist 12

“Hype and fear,” 6/8/12, <http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may> SJE

Cyber-disruption has nuisance value and may be costly to repair, but it can be mitigated by decent defences. Cyber-terrorism has remained largely in the imagination of film-makers, but would be worth worrying about if it became a reality. Stonesoft’s Mr Limnell reckons that, though al-Qaeda and its offshoots show little sign of acquiring the necessary skills, they could buy them. Mr Libicki is more sceptical. Big teams of highly qualified people are needed to produce Stuxnet-type effects, which may be beyond even sophisticated terrorist groups. Also, the larger the team that is needed, the more likely it is to be penetrated.

## OLC/XO

#### Doesn’t solve modeling

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

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

#### Perm — do both — Congressional involvement makes the plan popular — the CP links to politics

Corcoran 11 --- Professor of Law and Director at University of New Hampshire School of Law (March 2011, Erin M., University of New Hampshire Law Review, “Obama's Failed Attempt to Close Gitmo: Why Executive Orders Can't Bring About Systemic Change,” 9 U.N.H. L. Rev. 207))

Finally, this example highlights that issuing unilateral executive orders, and then asking Congress to fund those decisions, is much less effective than having Congress help create the framework for significant policy changes. Congress is an independent branch of government regardless of whether the members' party affiliation is the same as the President's. Since members of the House are elected every two years, they are particularly sensitive to the idiosyncratic whims of the constituents in their district. For the President, it is often easier to support sweeping change on a policy level. Although Senators are elected every six years, they are still bound to protect parochial concerns of their constituents. Congress members go home every weekend to their respective districts and must explain their votes, decisions, and legislative priorities to the voters often at supermarkets, churches, and bingo halls.¶ Often times, when members of Congress can control the message or create the narrative addressing the problem, they can show their [\*235] constituents how their votes are in line with constituent priorities and concerns. In contrast, when Congress is told to do what the President wants and fund a controversial proposal, the members are in less control of the message and less invested in the outcome.¶Furthermore, in the Senate, particularly in the Appropriations Committee, members work across the aisle. Until recently, appropriators tended to vote as a block regardless of party affiliation, protecting their funding prerogatives and funding for their home districts. For example, the Senate Supplemental Appropriations mark included funding to close Guantanamo Bay. Yet, during the Senate floor debate about closing Guantanamo Bay, ultimately it was the Chair of the Appropriations Committee who filed the amendment on the floor to strip funding out of the supplemental bill. n150 The Chair's action provided cover to other appropriators to vote in support of stripping the funding. Since the Chair authored the amendment, there was no longer any obligation to support the appropriations bill as it was marked up out of committee. Generally, appropriators vote together to protect funding when other senators attempt to strip funding out of appropriations bills or move funds from one account to fund a priority not accommodated by the appropriators. Since these members value collegiality, compromise, and consultation, it is no surprise that Obama's efforts to fund Guantanamo Bay closure was thwarted. If the Senate had been charged with crafting legislation, the members would have been committed to making sure they had the votes to pass it.¶ Overall, if the Obama Administration wants to close Guantanamo Bay, it must get Congress to lead the charge. This is going to be extremely difficult now with a Republican House of Representatives and Democrat Senate that holds the majority by the narrowest of margins. At this point, it seems as if the Administration has abandoned its campaign to close Guantanamo Bay. The only silver lining is that the Administration hopefully has learned important lessons on what works and what is a non-starter and can use this knowledge when advancing the President's future controversial policy changes.

#### Links to politics – congress wants to be involved

Sasso 2012

(Brandon Sasso, December 21, 2012, “House Republicans urge Obama not to issue cybersecurity order,” The Hill, http://thehill.com/blogs/hillicon-valley/technology/274391-house-republicans-urge-obama-not-to-issue-cybersecurity-order)

A group of 46 House Republicans, led by Reps. Marsha Blackburn (Tenn.) and Steve Scalise (La.), sent President Obama a letter on Friday urging him not to issue an executive order on cybersecurity.¶ "Instead of preempting Congress' will and pushing a top-down regulatory framework, your administration should engage Congress in an open and constructive manner to help address the serious cybersecurity challenges facing our country," the lawmakers wrote. ¶ The White House is currently drafting an executive order that would encourage operators of critical infrastructure, such as banks and electric grids, to meet cybersecurity standards. ¶ The administration says the order, which could come as early as January, is necessary to protect vital systems from hackers.¶ The White House began working on the order after Senate Republicans blocked the Democrats' preferred cybersecurity bill.¶ But in their letter, the House Republicans urged the administration to continue working with Congress.

#### Future presidents roll back

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

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

#### Triggers litigation, OLC can’t speak to statutes, and White House Counsel Circumvents

Bruce **Ackerman 11**, Sterling Professor of Law and Political Science at Yale University, “LOST INSIDE THE BELTWAY: A REPLY TO PROFESSOR MORRISON,” Harvard Law Review Forum Vol 124:13, http://www.harvardlawreview.org/media/pdf/vol124forum\_ackerman.pdf

To see why, consider that the relationship between the WHC and the OLC is utterly mysterious to most lawyers, let alone to most Americans. So imagine the scene when some future White House Counsel issues a legal opinion, rubberstamping the President’s latest power- grab, with the peroration: “Ever since Lloyd Cutler assumed the position as White House Counsel in NVTV, this office has, from to time, taken the lead in explaining the constitutional foundations for major presidential initiatives . . . .” ¶ Given pervasive ignorance dealing with Beltway arcana, this famous precedent will go a long way toward legitimating the White House decision to cut out the OLC. Instead of conceding impropriety, our hypothetical Counsel can summon up the great spirit of Lloyd Cutler in support of his leading role. After establishing his distinguished pedigree, Counsel can reinforce his claim to authority with a host of additional arguments: After all, there’s nothing in the Constitution that requires the President to prefer the OLC to the WHC. Article II simply tells the President to “take Care that the Laws be faithfully executed”69 — it doesn’t tell him where to get his legal advice. Moreover, as Morrison acknowledges, the OLC’s traditional role is principally based on executive order, not Congressional statutes.70 If the President prefers to treat his Counsel as a modern-day Cutler, there can be no question that the bureaucracy and military will follow his lead — at least until the courts enter into the field. ¶ Undoubtedly, the Cutler precedent won’t stifle all grumbling from Beltway cognoscenti.71 But it will make it much tougher to convince the generality of lawyerdom, as well as the broader public, that they are witnessing a dreadful act of legal usurpation — even if that’s precisely what is happening.72

#### OLC Links to Politics

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

These two events neatly encapsulate the dilemma for OLC, and indeed all the president’s legal advisers. If OLC tries to block the president from acting in the way he sees fit, it takes the risk that he will disregard its advice and marginalize the institution. If OLC gives the president the advice that he wants to hear, it takes the risk that it will mislead him and fail to prepare him for adverse reactions from the courts, Congress, and the public. Can OLC constrain the executive? That is the position taken by many scholars, most notably Jack Goldsmith. 18 The underlying idea here is that even if Congress and the courts cannot constrain the executive, perhaps offices within the executive can. The opposite view, advanced by Bruce Ackerman, is that OLC is a rubber stamp. 19 I advocate a third view: OLC does not constrain the executive but enables him to accomplish goals that he would not otherwise be able to accomplish. It is more accurate to say that OLC enables than constrains. B. OLC as a Constraint on the Executive A number of scholars have argued that OLC can serve as an important constraint on executive power. I will argue that OLC cannot act as a constraint on executive power. Indeed, its only function is the opposite—as an “enabler” (as I will put it) or extender of executive power. A president must choose a course of action. He goes to OLC for advice. Ideally, OLC will provide him good advice as to the legality of the course of action. It will not provide him political advice and other relevant types of advice. The president wants to maximize his political advantage, 21 and so he will follow OLC’s advice only if the legal costs that OLC identifies are greater than the political benefits. On this theory, OLC will properly always give the president neutral advice, and the president will gratefully accept it although not necessarily follow it. If the story ended here, then it would be hard to see what the controversy over OLC could be about. As an adviser, it possesses no ability to constrain the executive. It merely provides doctrinal analysis, in this way, if it does its job properly, merely supplying predictions as to how other legal actors will react to the president’s proposed action. The executive can choose to ignore OLC’s advice, and so OLC cannot serve as a “constraint” on executive power in any meaningful sense. Instead, it merely conveys to the president information about the constraints on executive power that are imposed from outside the executive branch. However, there is an important twist that complicates the analysis. The president may choose to publicize OLC’s opinions. Naturally, the president will be tempted to publicize only favorable opinions. When Congress 22 claims that a policy is illegal, the president can respond that his lawyers advised him that the policy is legal. This response at least partially deflects blame from the president. There are two reasons for this. First, the Senate consented to the appointment of these lawyers; thus, if the lawyers gave bad advice, the Senate is partly to blame, and so the blame must be shared. Second, OLC lawyers likely care about their future prospects in the legal profession, which will turn in part on their ability to avoid scandals and to render plausible legal advice; they may also seek to maintain the office’s reputation. When OLC’s opinions are not merely private advice, but are used to justify actions, then OLC takes on a quasi-judicial function. Presidents are not obliged to publicize OLC’s opinions, but clearly they see an advantage to doing so, and they have in this way given OLC quasi-judicial status. But if the president publicizes OLC opinions, he takes a risk. The risk is that OLC will publicly advise him that an action is illegal. If OLC approval helps deflect blame from the president, then OLC disapproval will tend to concentrate blame on the president who ignores its advice. Congress and the public will note that after all the president is ignoring the advice of lawyers that he appointed and thus presumably he trusts, and this can only make the president look bad. To avoid such blame, the president may refrain from engaging in a politically advantageous action. In this way, OLC may be able to prevent the president from taking an action that he would otherwise prefer. At a minimum, OLC raises the political cost of the action. I have simplified greatly, but I believe that this basic logic has led some scholars to believe that OLC serves as a constraint on the president. But this is a mistake. OLC strengthens the president’s hand in some cases and weakens them in others; but overall it extends his power—it serves as enabler, not constraint. To see why, consider an example in which a president must choose an action that lies on a continuum. One might consider electronic surveillance. At one extreme, the president can engage in actions that are clearly lawful—for example, spying on criminal suspects after obtaining warrants from judges. At the other extreme, the president can engage in actions that are clearly unlawful—for example, spying on political opponents. OLC opinions will not affect Congress’s or the public’s reaction to either the obviously lawful or the obviously unlawful actions. But then there are middle cases. Consider a policy L, which is just barely legal, and a policy I, which is just barely illegal. The president would like to pursue policy L but fears that Congress and others will mistakenly believe that L is illegal. As a result, political opposition to L will be greater than it would be otherwise. In such a case, a favorable advisory opinion from a neutral legal body that has credibility with Congress will help the president. OLC’s approval of L would cause political opposition (to the extent that it is based on the mistaken belief that L is unlawful) to melt away. Thus, OLC enables the president to engage in policy L, when without OLC’s participation that might be impossible. True, OLC will not enable the president to engage in I, assuming OLC is neutral. And, indeed, OLC’s negative reaction to I may stiffen Congress’ resistance. However, the president will use OLC only because he believes that OLC will strengthen his hand on net.

#### Congressional failure to act leads to massive expansion in prez power - now key

Dycus 10

[Stephen, Professor, Vermont Law School. JOURNAL OF NATIONAL SECURITY LAW &POLICY 4.155.

<http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf> ETB]

**If Congress now fails to enact guidelines for cyber warfare, it might** ¶ **be perceived as** inviting “measures on independent presidential ¶ responsibility**.**”21 Chief Justice **Marshall suggested in Little v. Barreme that** ¶if Congress had remained silent, the President might have been free to ¶ conduct the Quasi-War with France as he saw fit.22 But **the national interest** ¶ **in electronic warfare**, just as in that early maritime conflict, **is so great that** ¶ **the planning and conduct of such a war should not be left** entirely to the ¶ Executive. **And because a cyber war might be fought under circumstances** ¶ **that make it impossible for Congress to play a meaningful contemporaneous** ¶ **role,** Congress ought to get out in front of events now **in order to be able to** ¶ **participate in the formulation of national policy.**

#### Unfettered presidential powers cause nuclear war

Forrester 89

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

\*evidence is gendered modified

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

## Terror

#### No threat – weak leadership and no recent attacks

**Zenko and Cohen 12**, \*Fellow in the Center for Preventive Action at the Council on Foreign Relations, \*Fellow at the Century Foundation, (Micah and Michael, "Clear and Present Safety," March/April, Foreign Affairs, www.foreignaffairs.com/articles/137279/micah-zenko-and-michael-a-cohen/clear-and-present-safety

NONE OF this is meant to suggest that the United States faces no major challenges today. Rather, the point is that the problems confronting the country are manageable and pose minimal risks to the lives of the overwhelming majority of Americans. None of them -- separately or in combination -- justifies the alarmist rhetoric of policymakers and politicians or should lead to the conclusion that Americans live in a dangerous world.¶ Take terrorism. Since 9/11, no security threat has been hyped more. Considering the horrors of that day, that is not surprising. But the result has been a level of fear that is completely out of proportion to both the capabilities of terrorist organizations and the United States' vulnerability. On 9/11, al Qaeda got tragically lucky. Since then, the United States has been preparing for the one percent chance (and likely even less) that it might get lucky again. But al Qaeda lost its safe haven after the U.S.-led invasion of Afghanistan in 2001, and further military, diplomatic, intelligence, and law enforcement efforts have decimated the organization, which has essentially lost whatever ability it once had to seriously threaten the United States.¶ According to U.S. officials, al Qaeda's leadership has been reduced to two top lieutenants: Ayman al-Zawahiri and his second-in-command, Abu Yahya al-Libi. Panetta has even said that the defeat of al Qaeda is "within reach." The near collapse of the original al Qaeda organization is one reason why, in the decade since 9/11, the U.S. homeland has not suffered any large-scale terrorist assaults. All subsequent attempts have failed or been thwarted, owing in part to the incompetence of their perpetrators. Although there are undoubtedly still some terrorists who wish to kill Americans, their dreams will likely continue to be frustrated by their own limitations and by the intelligence and law enforcement agencies of the United States and its allies.¶

#### Terror risk down – foreign aid has reduced safe heavens in Pakistan

PTI ‘13

(PTI “US assistance to Pakistan helps reduce terrorism: John Kerry” Apr 11, 2013, 09.55 AM IST <http://timesofindia.indiatimes.com/world/pakistan/US-assistance-to-Pakistan-helps-reduce-terrorism-John-Kerry/articleshow/19488742.cms>, TSW)

WASHINGTON: The US assistance to Pakistan has helped in reducing the conditions that foment extremism in the country, US secretary of state John Kerry said as the State Department in its annual budget sought USD 1.3 billion in economic and military assistance for the South Asian nation.¶ "Our economic and military assistance to Pakistan helps reduce the conditions that enable extremism and its calling card - terrorism - to disrupt and destroy," said John Kerry in an eight-page budget letter to the US Congress on Wednesday.¶ "We are helping Pakistan to continue its development as a responsible and responsive international partner. For Pakistan we request USD 1.3 billion in financial year 2014 to fund civil and military assistance along with supporting the existing diplomatic platform," Kerry said.¶ According to a State Department fact sheet, the budgetary provisions for Pakistan includes programs that increase stability, strengthens democratic institutions and helps in countering violent extremism.¶ It also invests in energy, economic growth, stabilisation of border areas, education, health and counter insurgency and counter terrorism capabilities.¶ The budgetary provisions support the US government's civilian presence in the country and modernises security forces but eliminates the Pakistan Counterinsurgency Capability Fund, the State Department said.¶ "In Pakistan, we're looking at programs to make sure that we are putting the dollar where it's going to have the greatest impact," the State Department said.¶ The USD 1.3 billion proposed by the State Department includes USD 860 million as non-military assistance and about USD 300 million as military assistance.¶ On foreign military financing (FMF), it said, "there were implementation issues, but also we feel our FMF program is the primary way we're going to be dealing with the security relationship at this point with the Pakistanis."¶ The USD 1.3 billion aid to Pakistan is in addition to the USD 1.4 billion proposed by the President Barack Obama in his annual budget under the overseas contingency operations (OCO).

#### Obama weak now- Syria deal

Maloof 9/13

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

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

#### Massive alt causes to flex

Rozell 12

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

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

#### **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.”

**ZERO risk of WMD terror – their evidence is alarmist**

**Mueller ’12** (John, Senior Research Scientist at the Mershon Center for International Security Studies and Adjunct Professor in the Department of Political Science, both at Ohio State University, and Senior Fellow at the Cato Institute. Mark G. Stewart is Australian Research Council Professorial Fellow and Professor and Director at the Centre for Infrastructure Performance and Reliability at the University of Newcastle in Australia, The Terrorism Delusion, *International Security*, Vol. 37, No. 1 (Summer 2012), pp. 81–110)

Over the course of time, such essentially **delusionary thinking has been internalized and institutionalized** in a great many ways. For example, an extrapolation of **delusionary proportions is evident in** the **common** **observation** **that**, because **terrorists** were able, mostly by thuggish means, to crash airplanes into buildings, they **might** therefore **be able to construct a nuclear bomb.** In 2005 an **FBI** report **found that, despite years of well-funded sleuthing, the Bureau had yet to uncover a single true al-Qaida sleeper cell in the U**nited **S**tates. The report was secret but managed to be leaked. Brian Ross, “Secret FBI Report Questions Al Qaeda Capabilities: No ‘True’ Al Qaeda Sleeper Agents Have Been Found in U.S.,” ABC News, March 9, 2005. Fox News reported that the FBI, however, observed that “just because there’s no concrete evidence of sleeper cells now, doesn’t mean they don’t exist.” “FBI Can’t Find Sleeper Cells,” Fox News, March 10, 2005. Jenkins has run an internet search to discover how often variants of the term “al-Qaida” appeared within ten words of “nuclear.” There were only seven hits in 1999 and eleven in 2000, but the number soared to 1,742 in 2001 and to 2,931 in 2002. 47 By 2008, Defense Secretary Robert Gates was assuring a congressional committee that what keeps every senior government leader awake at night is “the thought of a terrorist ending up with a weapon of mass destruction, especially nuclear.” 48 Few of the sleepless, it seems, found much solace in the fact that **an al-Qaida computer seized in Afghanistan in 2001 indicated that the group’s budget for** research on **w**eapons of **m**ass **d**estruction (almost all of it **focused on primitive chemical weapons** work) **was $2,000** to $4,000. 49 In the wake of the killing of Osama bin Laden, **officials now have many more al-Qaida computers,** and **nothing** in their content appears to **suggest** that the group had **the time** or **inclination**, **let alone the money, to** set up and **staff** a uranium-seizing operation, as well as **a** fancy, **super-high-tech**nology **facility to fabricate a bomb**. **This is a process that requires trusting corrupted foreign collaborators and other criminals, obtaining and transporting highly guarded material, setting up a machine shop staffed with top scientists and technicians, and rolling the heavy, cumbersome, and untested finished product into position to be detonated by a skilled crew—all while attracting no attention from outsiders.** 50 If the miscreants in the American cases have been unable to create and set off even the simplest conventional bombs, it stands to reason that **none of them were** very **close to** **creating, or having anything to do with,** **nuclear weapons**—or for that matter **biological**, **radiological**, **or chemical ones**. In fact, with perhaps one exception, **none seems to have even dreamed of the prospect**; and the exception is José Padilla (case 2), who apparently mused at one point about creating a dirty bomb—a device that would disperse radiation—or even possibly an atomic one. His idea about isotope separation was to put uranium into a pail and then to make himself into a human centrifuge by swinging the pail around in great arcs. **Even if a weapon were made abroad and then brought into the U**nited **S**tates, **its detonation would require individuals** in-country **with the capacity to** receive and **handle the complicated weapons and** then to **set them off.** Thus far, **the talent pool appears**, to put mildly, **very thin**. **There is delusion**, as well, in the legal expansion **of the concept of “w**eapons of **m**ass **d**estruction.” The concept had once been taken as a synonym for nuclear weapons or was meant to include nuclear weapons as well as weapons yet to be developed that might have similar destructive capacity. After the Cold War, it was expanded to embrace chemical, biological, and radiological weapons even though those weapons for the most part are incapable of committing destruction that could reasonably be considered “massive,” particularly in comparison with nuclear ones.

## PTX

#### Won’t pass - election fears and Obama’s approach prolongs Republican backlash

Kaplan 10-3

[Rebecca, serves as City Councilmember At-Large for Oakland, California, CBS News, “Why is it so difficult to end the government shutdown?” <http://www.cbsnews.com/8301-250_162-57605784/why-is-it-so-difficult-to-end-the-government-shutdown/>]

As the government shutdown enters its third day, **Democrats and Republicans seem no closer to bridging their differences than they were when the shutdown began** early Tuesday morning. **It's difficult to say when the standoff will end**. The two **shutdowns** that occurred **in 1995 and 1996 lasted** a total of **27 days. And** back then, the **conditions** for getting to a deal **were much better**.¶ Republicans won the House and Senate in the 1994 midterm elections - the first time the party had a House majority in 40 years. That set up a showdown between House Speaker Newt Gingrich, who had run on a conservative platform, and then-President Bill Clinton. That dispute came in 1995, when Gingrich wanted to balance the budget in a short time frame and Clinton wanted money spent on Democratic priorities. After two separate shutdowns and several weeks, the pressure was too high on Republicans and they cut a deal with Clinton: he would get his priorities, but would have to balance the budget for 10 years.¶ "They were kind of testing each other," said former Rep. Tom Davis, R-Va., who was a freshman in Congress at the time. Afterward, Davis noted, Clinton and Gingrich would go on to work together on a host of issues including welfare reform. The economy boomed, helping to mitigate budget issues.¶ Republicans who were lawmakers or aides in Congress in 1995 cite a variety of reasons that the shutdown ended. For Davis, it was the mounting public pressure on Republicans and their rapidly dropping poll numbers that helped spur a compromise. "There was a revolt, and they simply couldn't hold their members after a while," he said of the Republican leadership. It didn't help that Republicans were afraid of losing the first majority they'd had in decades. Davis recalls going to former Rep. Dick Armey, then the Republican Majority leader from Texas, and saying, "We're getting our butts kicked."¶ But Bob Walker, then a Republican congressman from Pennsylvania, had a different take from the conventional narrative that Republicans had caved. "We stayed focused in 1995 on the fact that what the end result for us was to get a pathway to a balanced budget, and so in the end when we got an agreement to just begin the process of moving toward a balanced budget," he said. "We declared victory on that and we were prepared to then get the government back into action."¶ **This time, it's not so easy for Republicans to achieve even a piece of their chief goal** - to dismantle the Affordable Care Act. The law is President Obama's signature policy achievement, and its constitutional authority was affirmed by the Supreme Court. Democrats in the Senate and Mr. Obama himself have proven with the shutdown fight that they are determined to keep the law intact.¶ "We didn't get an immediate balanced budget obviously but what we got was a seven-year plan toward a balanced budget that then ended up being accomplished in there years," Walker said of the House Republicans in 1995. But nowadays, he said, "I'm not certain I see where the bottom lines are."¶ As shutdown continues, Obama says Wall Street "should be concerned"¶ Government shutdown: Is Congress acting selfishly?¶ Yet another explanation of why the 1995-1996 shutdown ended had to do with presidential politics. Former Senate Majority Leader Bob Dole, R-Kansas, was eyeing a presidential bid against Clinton in 1996.¶ "He just got sick of it. I think he started seeing that this was directly impacting his ability to run for president," said John Feehery, a political strategist who was the communications director for then-House Majority Whip Tom DeLay during the shutdown. Dole was key to engineering an end to the shutdown, a fact that was apparent to everyone - even Democrats.¶ "It was a huge factor," said American University professor Patrick Griffin, who served as Clinton's assistant for legislative affairs from 1994 to 1996. "We could always sense that there was no love lost between him and [Gingrich] - on the [Contract with America], on the shutdown. It was just not Dole's style...he was wasting time, he was not being able to get his campaign."¶ If anything, presidential politics will lengthen the shutdown. Mr. **Obama has no re-election campaign** to worry about - like Clinton did at the time - **and Republican** presidential **campaigns cannot be won without pleasing an active base that hates the healthcare law. It would be difficult for any Republican to help broker a compromise that preserved most of Obamacare and then woo Republican primary voters**.¶ **Not that many Republicans feel as if they can work with** Mr. **Obama**. "Many people in Congress ...believe that the president treats them with contempt and so the atmosphere for negotiating is not very good. That's a big difference," said Walker.¶ House Speaker John Boehner, R-Ohio, and Mr. Obama have tried and failed to negotiate big deals several times**. Since the** government **shut down** on Tuesday, **they've barely talked** aside from a meeting the president held with top congressional leaders Wednesday afternoon. And a recent Politico story that detailed how Boehner and Senate Majority Leader Harry Reid, R-Nev., worked together to preserve congressional subsidies for healthcare coverage will likely have poisoned the well between the leaders of the two chambers.¶ That wasn't the case with Gingrich and Clinton, despite their differences. "Both President Clinton and Speaker Gingrich had a pretty civil and reasonably good personal relationship," said Mack McLarty, Clinton's first chief of staff as president. Both hailed from the south, and had "very inquisitive minds" about the world around them.¶ Perhaps **the biggest roadblock to a deal**, however, **is the** increasingly partisan nature **of Congress caused by congressional redistricting that puts many members into seats where fewer and fewer constituents are from the opposite party**. In 1995, more than 34 percent of Republican representatives in the House were elected in districts that had voted for Clinton as president. Now, only seven percent of House members come from districts that voted for Mr. Obama.¶ There's a larger proportion of hardline conservatives in the House in 2013, and they have so far been more successful at driving the agenda than their more moderate counterparts. "The-rank-and-file members are sick and tired of the rebels running the thing but there's too many of them who vote with the rebels to protect their flank," Feehery said, referring to Republicans who are worried about receiving a primary challenge from the right.¶ **With so many factors working against a deal, it's hard to see a way out of the crisis**. The only thing that's guaranteed to inject some urgency into the debate is the looming deadline to raise the debt ceiling on Oct. 17. While a government shutdown can have minimal effects on the financial markets, the possibility of the U.S. defaulting is much more likely to cause financial panic that could push lawmakers into a deal.¶ Plus, **if the spending and debt ceiling deals** morph into one**, there may be more issues on the table to discuss such as the sequester and the whole federal budget. That**, Walker said, **will** give Republicans more areas where they can look for victory.

#### The plan is a concession – dems would have to vote for the plan which appeases the GOP – causes a deal

Todd 10-3

“A Potential Way out,” <http://firstread.nbcnews.com/_news/2013/10/03/20801495-first-thoughts-a-potential-way-out>

“We have to get something out of this”: This is where Rep. Marlin Stutzman’s (R-IN) amazing and revealing quote comes into play. “We’re not going to be disrespected,” the Tea Party congressman said, per NBC's Frank Thorp. “We have to get something out of this. And I don’t know what that even is.” Let that quote sink: Stutzman is admitting that conservatives don’t even know what they want out of this fight. As we said yesterday, the deeper a hole you did, the harder it is to get out because suddenly you get this war mentality where you can’t fathom “surrendering” to the other side’s terms. And what Boehner seems to be almost BEGGING Democrats for is a fig leaf of something so that Republicans can get “something” out of this. If there is a “something” that Democrats MIGHT offer, keep an eye on the medical-device tax. It’s a way for Senate Democrats to recruit Senate Republicans to make a statement to House Republicans. Reid can say it is NOT connected to the shutdown, but they pass it as a stand-alone, send it to the House, and let Boehner spin it any way he wants to simply get the government open.

#### FERC thumps

Dixon 10/1

(Darius Dixon, Politico, “Obama FERC nominee Ron Binz withdraws amid coal pushback”, <http://www.politico.com/story/2013/10/ron-binz-ferc-nominee-withdraws-name-97623.html>, October 1, 2013)

President Barack Obama’s nominee to lead the Federal Energy Regulatory Commission abandoned his quest Tuesday, complaining that the fight over his confirmation had become a “blood sport” for partisan attacks and opponents backed by the coal industry. The collapse of Ron Binz’s nomination to lead the little-known agency was a stunning setback for Obama, who had succeeded in winning Senate confirmations for far more controversial nominees at Environmental Protection Agency, the Pentagon and the Labor Department. Continue Reading The consultant and career energy regulator had won over supporters from the green energy world — some of whom took the unusual step of hiring a public relations firm to advance his cause. But Binz said he couldn’t overcome a furious opposition campaign in which his record was “spun and respun” to make him appear biased against fossil fuels. “The caricature that they created had nothing to do with who I am and nothing to do with what I might’ve brought to FERC. It was just a blood sport,” Binz told POLITICO in his first extensive interview since Obama nominated him in June. “I came to Washington with this 35-year career behind me only to encounter a fictional Ron Binz, a fictional character that I didn’t recognize and I would never even support,” he added. Conservative and libertarian groups celebrated Binz’s withdrawal as a setback for Obama’s climate agenda, while his supporters lamented that partisan bickering had defeated a qualified candidate.

#### No link — the plan’s not controversial

**Perera 6/26**, SACS calls for new oversight of Cyber Command, David Perera is executive editor of the FierceMarkets Government Group, which includes FierceGovernment, FierceGovernmentIT, FierceHomelandSecurity, and FierceMobileGovernment. He has reported on all things federal since January 2004 and is co-author of [Inside Guide to the Federal IT Market](http://store.brightkey.net/mconcepts_ebiz/OnlineStore/ProductDetail.aspx?ProductId=201530), a book published in October 2012., <http://www.fiercegovernmentit.com/story/sasc-calls-new-oversight-cyber-command/2013-06-26>

The Senate Armed Services Committee says it has concerns that oversight of Cyber Command and the cyber mission within the Defense Departments "is fragmented and weak," calling for creation of a Senate-confirmed position within the undersecretary of defense for policy to supervise and manage the funds of offensive cyber forces.

**The Senate committee voted 23-3** on June 14 to report its version of the fiscal 2014 national defense authorization act ([S. 1197](http://hdl.loc.gov/loc.uscongress/legislation.113s1197)), detailing its intentions in a newly released legislative [report](http://www.gpo.gov/fdsys/pkg/CRPT-113srpt44/pdf/CRPT-113srpt44.pdf)(.pdf).

#### It’s super popular

**Bradbury 11**, Steven G. Bradbury is an attorney at the Washington, D.C office of [Dechert LLP](http://en.wikipedia.org/wiki/Dechert_LLP).

Bradbury was head of the [Office of Legal Counsel](http://en.wikipedia.org/wiki/Office_of_Legal_Counsel) (OLC) in the [United States Department of Justice](http://en.wikipedia.org/wiki/United_States_Department_of_Justice) during the [George W. Bush administration](http://en.wikipedia.org/wiki/George_W._Bush_administration), 2005-January 2009. Appointed the Principal Deputy Assistant Attorney General for OLC in April 2004, he became the Acting Assistant Attorney General in 2005. He was nominated by President [George W. Bush](http://en.wikipedia.org/wiki/George_W._Bush) to be the Assistant Attorney General for OLC in June 2005. His nomination was approved by the [Senate Judiciary Committee](http://en.wikipedia.org/wiki/Senate_Judiciary_Committee) in November 2005 but was never voted on by the full Senate, The Developing Legal Framework for Defensive and Offensive Cyber Operations, This speech was the Keynote address at the Harvard National Security Journal Symposium, <http://harvardnsj.org/wp-content/uploads/2011/02/Vol.-2_Bradbury_Final1.pdf>

Congressional reporting. The National Security Act also ¶ requires the President and DNI to ensure that the Intelligence Committees ¶ of the House and Senate are fully and currently informed of all intelligence ¶ and counterintelligence activities, to the extent consistent with the ¶ protection of sensitive sources and methods or other exceptionally sensitive ¶ matters.10¶ With respect to covert actions, the Act requires the President to ¶ report presidential findings supporting covert actions to the Intelligence ¶ Committees, but where the President determines that it’s essential because ¶ of “extraordinary circumstances affecting vital interests of the United ¶ States,” the President may limit access to the so-called “Gang of Eight” —¶ the chairs and ranking members of the two Intelligence Committees, the ¶ Speaker and minority leader of the House, and the majority and minority ¶ leaders of the Senate, along with whatever other congressional leaders the ¶ President chooses to include.11¶ The **committee chairs hate when briefings are limited to the Gang of Eight, because they catch hell from the members** of their committees who ¶ are outside the circle. So when former-Senator Obama first became President, there was hope among some in Congress that he would eliminate the Gang of Eight briefings. But when Congress proposed an Intelligence ¶ Authorization bill that would do just that, President **Obama threatened to veto** it. Once he became head of the Executive Branch, he clearly ¶ understood the importance of being able to limit the scope of briefings for ¶ the most sensitive matters. So the statute still allows for Gang of Eight ¶ briefings In contrast to these title 50 intelligence activities, military operations conducted under title 10 authorities are subject to oversight by the Armed Services Committees of Congress. (Title 10 of the U.S. Code governs DoD’s ¶ military authorities and the military command structure; title 50 governs the ¶ Intelligence Community and intelligence activities.)¶ And make no mistake, in the world of Washington, it really does ¶ matter whether an activity is characterized as covert action or a traditional ¶ military action because different Executive Branch departments or agencies ¶ will have ownership of the operation and different committees of Congress ¶ will have oversight jurisdiction, and they all jealously guard their respective ¶ domains.

#### PC isn’t key and Obama isn’t spending it

Allen, 9/27

Politics reporter for Politico (Jonathan, “President Obama’s distance diplomacy” <http://www.politico.com/story/2013/09/government-shutdown-barack-obama-house-gop-97483.html?hp=t3_3>)

The White House’s distance diplomacy with Republicans is an approach that tacitly acknowledges three inescapable realities: There’s no one to negotiate with on the GOP side; Obama’s direct involvement in a pact would poison it for many rank and file Republicans; and Democrats don’t trust him not to cut a lousy deal.¶ Indeed, Democrats are urging Obama to stay at arm’s length from Congress so there’s no confusion over his message that he won’t negotiate on an increase in the debt limit, which the nation is expected to breach as early as Oct. 17 without legislative action.¶ “I believe the president has made it very clear, as we have tried to make it clear: There are no negotiations. We’re through,” Senate Majority Leader Harry Reid (D-Nev.) told POLITICO.¶ In past installments of the fiscal-failure soap opera, overheated rhetoric about government shutdowns and a default on the national debt has been matched by sober and direct deal-making behind the scenes — usually in the form of a virtual handshake between Vice President Joe Biden and Senate Minority Leader Mitch McConnell.¶ In the winter 2010 debate over tax cuts, Biden and McConnell agreed to extend all of the Bush-era tax cuts for two years, infuriating the left. In 2011, Boehner and Obama secretly discussed for weeks a possible grand-bargain deal — but when the details were leaked, Democrats were furious and the negotiations fell apart. And in 2012, Biden and McConnell averted the so-called fiscal cliff — but that greatly upset Reid, who believed the White House gave away too much to Republicans whose backs were against the wall.¶ Indeed, many Democrats had buyer’s remorse on aspects of those agreements, particularly a budget sequestration plan that has squeezed domestic and military spending, and the locking in of much of the Bush tax rates.¶ When Chief of Staff Denis McDonough and other senior White House aides quietly discussed budget issues with a group of Senate Republicans earlier this year, top Democrats believed it made little sense to continue negotiations that appeared to be going nowhere and didn’t seem likely to help their party.¶ So they’ve asked Obama himself to steer clear of this round of the debt fight and try to force Republicans to come to him. The Senate, on a party line 54-44 vote on Friday, sent a bill that would keep the government operating but dropped a House provision defunding Obamacare. Now the House is expected to load up the measure with more provisions that aren’t acceptable to Democrats — though it has been hard for House GOP leaders to herd their troops on a budget bill and a separate plan to raise the debt ceiling.¶ “You first need the Republicans to have a position to negotiate – they don’t yet,” Sen. Chuck Schumer (D-N.Y.), who often advises the White House on strategy, said Friday when asked about Obama’s posture. “Until the House Republican Caucus figures out what it wants to do, nobody can deal with them.”¶ Other than a terse phone call to Speaker John Boehner last Friday to reiterate that he won’t negotiate on the debt limit, Obama hasn’t talked to House Republicans — the key constituency in the fight.¶ The White House has let Reid take the lead in the latest fights, even scrapping a potential meeting at the White House with Obama and the three other congressional leaders to allow the process to play out on Capitol Hill. With Republicans fighting with each other over Obamacare, Democrats believe it makes far more sense to keep the focus on the GOP intraparty warfare, rather than risk putting Obama middle of a politically sensitive negotiation.¶ Republicans sourly note that Obama has been quicker to talk with Russian President Vladimir Putin — and now Iranian President Hassan Rouhani — than with House Speaker John Boehner.¶ “Grandstanding from the president, who refuses to even be a part of the process, won’t bring Congress any closer to a resolution,” said Brendan Buck, a spokesman for House Speaker John Boehner.¶ When McDonough went to the Hill this week for closed-door talks, it was to reassure fellow Democrats that the president wouldn’t fold early, as he’s been accused of doing in past budget battles.¶ Obama isn’t expected to meet with congressional leaders until after the Tuesday deadline to stop a government shutdown.¶ Asked if he believed that Obama would eventually have to engage directly in the fiscal fights, Reid said: “Not on the debt ceiling and not on the CR. Maybe on something else – but not these two. We have to fund the government and pay our bills.”¶ Whether Obama can sustain his no-negotiation position on the debt ceiling remains to be seen. Senate Republicans — even those who have balked at calls to use the threat of a government shutdown to defund Obamacare — say the president won’t get a clean debt ceiling increase.¶ “It’s what’s wrong with the government right now,” said Sen. Roy Blunt (R-Mo.), who voted to break a GOP-led filibuster blocking the continuing resolution. “I suppose the Congress might say we don’t want a negotiation on the debt ceiling either.”¶ If Obama can’t get 60 votes in the Senate for a clean debt ceiling increase, he will very likely to have to engage in direct talks with Republicans, even Democrats privately concede.¶ But for now, Democratic leaders say the president is doing what he has to: Making speeches to attack Republicans, and letting his allies on the Hill deal with the nitty-gritty of legislating and horse-trading.¶ Republican Rep. Mike Rogers (R-Mich.), who has worked with the White House on national security issues, says the president’s always had a “laissez-faire” approach to Congress.

#### No impact – multiple factors check

FXStreet.com, 9/25

An investing website (“4 Reasons Why You Shouldn't Worry Over This Year's Debt Ceiling Deadline” <http://www.fxstreet.com/analysis/piponomics/2013/09/25/>)

The U.S. debt ceiling deadline may be looming like dark clouds over the market horizon, but I've found a few reasons why this issue might not be such a big deal after all.¶ 1. In 2011 the market was also dealing with:¶ Back when the debt ceiling issue popped up in 2011, risk appetite was really low since markets were also troubled by Greece's potential default, Portugal's and Japan's debt downgrades, the prospect of another global recession, plus ongoing riots in the U.K. Clearly, the global economy had more problems than a math book!¶ This time around though, market sentiment is much different as major economies like the euro zone, the U.K., and even Japan and China are all looking at optimistic economic growth prospects. With that, the debt ceiling issue might simply make a tiny dent in risk appetite.¶ 2. The Fed is still stimulating the markets.¶ In the FOMC statement last week, the Fed decided to keep supporting the U.S. economy by refusing to taper its monthly asset purchases. Aside from helping sustain the progress in lending and spending, this could eventually stimulate the global economy as it would also ensure healthy demand and robust trade activity.¶ 3. The Dollar Index is hinting at a repeat of history.¶ If you look at the USDX chart you'll see that the dollar fell 200 pips from mid-July until early August when the debt ceiling deadline was due. It then encountered support at the 74.00 psychological area and even reached the 80.00 area by October.¶ This time around the USDX is consolidating at the 81.00 support on the daily chart. If history is to repeat itself, then the 200-pip fall from early September has already run its course. Does this mean that we're about to see a dollar rally soon?¶ 4. We've seen this before.¶ In 2011 the U.S. government alleviated the markets' fears by raising the debt ceiling and promising to reduce future increases in government spending. Then, in 2013, they got over the fiscal cliff hurdle by passing a last-minute bill that includes a $600 billion tax revenue in a span of ten years. And then there's the budget sequestration issue, which has gone relatively smoothly since early this year despite the onslaught of criticism.

#### XO solves

Weisenyhal 9/30

(Joe Weisenthal 9/30, Executive Editor for Business Insider, “It Increasingly Looks Like Obama Will Have To Raise The Debt Ceiling All By Himself,” <http://www.businessinsider.com/it-increasingly-looks-like-obama-will-have-to-raise-the-debt-ceiling-all-by-himself-2013-9>)

With no movement on either side and the debt ceiling fast approaching, there's increasing talk that the solution will be for Obama to issue an executive order and require the Treasury to continue paying U.S. debt holders even if the debt ceiling isn't raised.¶ Here's Greg Valliere at Potomac Research:¶ HOW DOES THIS END? What worries many clients we talk with is the absence of a clear end-game. We think three key elements will have to be part of the final outcome: First, a nasty signal from the stock market. Second, a daring move from Barack Obama to raise the debt ceiling by executive order if default appears to be imminent. Third, a capitulation by Boehner, ending the shut-down and debt crisis in an arrangement between a third of the House GOP and virtually all of the Democrats. ¶ Valliere isn't the only one seeing this outcome.¶ Here's David Kotok at Cumberland Advisors:¶ We expect this craziness to last into October and run up against the debt limit fight. In the final gasping throes of squabbling, we expect President Obama to use the President Clinton designed executive order strategy so that the US doesn’t default. There will then ensue a protracted court fight leading to a Supreme Court decision. The impasse may go that far. This is our American way. “Man Plans and God Laughs” says the Yiddish Proverb.¶ Indeed, back in 2011, Bill Clinton said he'd raise the debt ceiling by invoking the 14th Amendment rather than negotiate with the House GOP.¶ This time around, again, Clinton is advising Obama to call the GOP's bluff.

#### No impact to econ decline

Miller 2k

(Morris, economist, adjunct professor in the University of Ottawa’s Faculty of Administration, consultant on international development issues, former Executive Director and Senior Economist at the World Bank, Winter, Interdisciplinary Science Reviews, Vol. 25, Iss. 4, “Poverty as a cause of wars?” p. Proquest)

The question may be reformulated. Do wars spring from a popular reaction to a sudden economic crisis that exacerbates poverty and growing disparities in wealth and incomes? Perhaps one could argue, as some scholars do, that it is some dramatic event or sequence of such events leading to the exacerbation of poverty that, in turn, leads to this deplorable denouement. This exogenous factor might act as a catalyst for a violent reaction on the part of the people or on the part of the political leadership who would then possibly be tempted to seek a diversion by finding or, if need be, fabricating an enemy and setting in train the process leading to war. According to a study undertaken by Minxin Pei and Ariel Adesnik of the Carnegie Endowment for International Peace, there would not appear to be any merit in this hypothesis. After studying ninety-three episodes of economic crisis in twenty-two countries in Latin America and Asia in the years since the Second World War theyconcluded that:19 Much of the conventional wisdom about the political impact of economic crises may be wrong ... The severity of economic crisis - as measured in terms of inflation and negative growth - bore no relationship to the collapse of regimes ... (or, in democratic states, rarely) **to** an outbreak of violence ... In the cases of dictatorships and semidemocracies, the ruling elites responded to crises by increasing repression (thereby using one form of violence to abort another).

#### Best data proves

Globe and Mail ‘10

(5/31/10, BRIAN MILNER, "While gloom says bear, TIGER points to bull", lexis, WEA)

**Even at the height of the remarkable rebound** of 2009 that brought stocks back from the dead zone, **the bears never retreated** to their lairs. **Negative sentiment** among investors **remained stubbornly high, no matter how promising the economic indicators** looked. And **then** along **came the Greeks and their** little sovereign **debt** problem, **the Chinese and** their public hand-wringing over **asset bubbles and the North Koreans** **and their** latest idiotic **sabre-ratting** to remind nervous markets just how fragile the nascent global recovery could turn out to be. The latest survey of American investors last week showed bearish sentiment hovering close to 30 per cent, with plenty of room for an uptick in the months ahead, as the optimists come to realize that a V-shaped recovery was never in the cards after the worst global financial and economic crisis since the Great Depression. The world's most overexposed permabear, Nouriel Roubini, is still grabbing headlines with his dire Greece-is-just-the-tip-of-the-iceberg warnings. (Well, he does have a new book to sell.) And such high-profile Canadian bruins as gold-loving money manager Eric Sprott and eminent strategist and data miner David Rosenberg have never veered from their sombre outlooks. The fact that May turned into a particularly brutal month for just about everything but U.S. Treasuries - even after last week's modest rebound, the Dow posted its worst performance for the month in 70 years - only added fuel to arguments that worse, much worse, is yet to come. I mention all this to Eswar Prasad, when I reach the Cornell University economics professor at his hotel in Beijing. Prof. Prasad is a noted China watcher who once headed the IMF's China division and still keeps in close touch with top government finance officials. But on this call, I'm more interested in one of his other hats as a shrewd analyst of global economic and market trends. "**My inclination also is to be a bear**," the affable academic says. "**But** the data don't supportmybearishness as much as I would like. **One has to be a little cautious**, because these are based on a variety of **indicators**. Some of them certainly **show more strength than** I had **realized**." The data he's talking about come out of his work on a new composite index derived from a broad set of economic, market and confidence measures in the G20 countries and designed to provide a quarterly snapshot of the global recovery. "All signs are that the recovery has some momentum," says Prof. Prasad, who developed the index at the Brookings Institution, a Washington think tank where he is also a senior fellow. "But I wouldn't call it solid enough momentum that we can consider it 'in the bag.'" **The new index**, cutely named TIGER (Tracking Indices for the Global Economic Recovery), is a joint effort by Brookings and the Financial Times. And TIGER **shows that since the world began climbing out of the deep trough** about the middle of last year, **big** emerging economies have roared ahead, while the developed world has experienced much more uneven results. Industrial production and trade have bounced back **handsomely** - total exports from the big emerging countries now exceed pre-crisis levels - but the employment picture remains cloudy and consumption has yet to develop a new head of steam. "It'smucheasier at this stage to list all the things that could derailtherecovery," Prof. Prasad says. "But all of those things are still conjectural. The reality, and the data, is that things are looking better."

#### PC is low and decreasing

Steinhauser, 9/26

CNN Political Editor (Paul, “Obama's support slips; controversies, sluggish economy cited” <http://www.cnn.com/2013/09/26/politics/cnn-poll-of-polls-obama/?hpt=po_c2>)

As he battles with congressional Republicans over the budget and the debt ceiling, and as a key component of his health care law kicks in, new polling suggests that President Barack Obama's standing among Americans continues to deteriorate.¶ The president's approval rating stands at 45%, according to a CNN average of four national polls conducted over the past week and a half. And a CNN Poll of Polls compiled and released Thursday also indicates that Obama's disapproval rating at 49%.¶ In the afterglow of his re-election and second inauguration, the percentage of those approving of Obama's job performance hovered in the low 50s as the year began, according to CNN Poll of Poll averages.¶ But his numbers slipped to the upper 40s by spring and now have edged down to the mid 40s. At the same time, his disapproval numbers have edged up from the low 40s to right around the 50% mark.¶ Anxiety and skepticism over the Affordable Care Act, better known as Obamacare, continuing concerns over the sluggish economy, and a drop in the president's approval on foreign policy -- once his ace in the hole -- all appear to be contributing to the slide of Obama's general approval rating.¶ "Not a precipitous drop, but more like a continued erosion in the president's numbers," says CNN Chief Political Correspondent Candy Crowley. "The Boston Marathon bombings, Edward Snowden's 'big brother' revelations, the 'non-coup' in Egypt, the 'now we bomb, now we don't' policy in Syria, an economic recovery that remains disappointing, the uncertainty of how/what will change under the new health care system, shall I go on?"¶ "It all adds up to an awful lot of uncertainty and unfairly or not, uncertainty tends to breed lower poll numbers for the guy in charge," added Crowley, anchor of CNN's "State of the Union."¶ Besides being the main indicator of a president's standing with the public, a presidential approval rating is a good gauge of his clout in dealing with Congress.¶ The drop in his numbers comes as the president pushes back against attempts by congressional Republicans to use deadlines to keep the federal government funded and to extend the nation's debt ceiling to try and defund the health care law.¶ A slew of national polls conducted this month indicate that a majority doesn't support shutting down the government in order to defund Obamacare.¶ But if the fight shifts to the debt ceiling, public opinion appears to turn against the president, who reiterated on Thursday that he will not negotiate with the GOP in Congress over extending the debt ceiling.