# 1AC

**Adv 1: Arms Race**

#### 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**](http://money.cnn.com/2012/11/05/technology/security/iran-cyberattack/index.html?iid=EL) **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**](http://money.cnn.com/2011/07/28/technology/government_hackers/index.htm?iid=EL) **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](http://money.cnn.com/quote/quote.html?symb=INTC&source=story_quote_link), [Fortune 500](http://money.cnn.com/magazines/fortune/fortune500/2012/snapshots/642.html?iid=EL))subsidiary, **wrote** in a [recent report](http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf). Michael **Sutton, head of security research at cloud** security **company** [Zscaler](http://www.zscaler.com/), **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](http://money.cnn.com/2012/04/27/technology/cispa-cybersecurity/index.htm?iid=EL) 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, OCO-driven retaliatory cycles and arms races

Moss 13

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

Although setting up a cybersecurity working group with China, Washington has also signaled it intends to escalate. U.S. Cyber Command and NSA chief General Keith Alexander signaled this shift of policy gears earlier this month when he [told Congress](http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?_r=4&) that of 40 new CYBERCOM teams currently being assembled, 13 would be focused on offensive operations. Gen Alexander also gave new insight into CYBERCOM’s operational structure. The command will consist of three groups, he said: one to protect critical infrastructure; a second to support the military’s regional commands; and a third to conduct national offensive operations. As cyber competition intensifies between the U.S. and China in particular, the international community approaches a crossroads. States might begin to rein in their cyber operations before things get further out of hand, adopt a rules-based system governing cyberspace, and start respecting one another’s virtual sovereignty much as they do one another’s physical sovereignty. Or, if attacks and counter-attacks are left unchecked, cyberspace may become the venue for a new Cold War for the Internet generation. Much as the old Cold War was characterized by indirect conflict involving proxy forces in third-party states, its 21stcentury reboot might become a story of virtual conflict prosecuted by shadowy actors in the digital realm. And as this undeclared conflict poisons bilateral relations over time, the risk of it spilling over into kinetic hostilities will only grow.

#### Cyber arms race causes world war

— 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

— otherwise nuclear war is inevitable from 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.

#### Cyber war escalates - 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 sfrom 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?

### Adv 2: Alliances

#### Congressional restrictions necessary for allied cooperation

Dunlap 12

Major General and Former Deputy Judge Advocate General (Lawless Cyberwar? Not If You Want to Win, [www.americanbar.org/groups/public\_services/law\_national\_security/patriot\_debates2/the\_book\_online/ch9/ch9\_ess2.html](http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch9/ch9_ess2.html))

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

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

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

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

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

Lawson ‘10

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

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

#### Coalition building key to solve extinction – disease, climate change, terrorism, and great power war

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

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

#### Legitimacy is key to band-wagon

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

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

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

Kazianis 12

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

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

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

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

RTT 13

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

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

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

Yoshihara 10

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

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

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

Colby et al 13

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

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

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

Rehman 13

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

**Despite** America’s **best efforts to construct stronger ties with China, relations** in-between both countries **have been** repeatedly **buffeted by** a series of **tensions** and misunderstandings. Many of these frictions appear to have **resulted from** a more [**assertive Chinese posture**](http://nation.time.com/2012/07/15/the-south-china-sea-from-bad-to-worse/) **in the South China Sea.** Almost every week, Asian **headlines seem** to be **dominated by reports of** jingoistic **statements over disputed islets, or** of a **renewed bout of aggressive maneuvering** by boats from one of Beijings numerous maritime agencies. When attempting to explain this upsurge in Chinese pugnacity, **analysts** have **pointed to** the rising power's selective interpretation of the law of the sea and growing **unwillingness to compromise** over what it calls its [“blue national soil”](http://www.washingtonpost.com/opinions/the-blue-national-soil-of-chinas-navy/2011/03/18/AB5AxAs_story.html), particularly when confronted with an increasingly intransigent domestic populace. Others have pointed to the more immediately tangible benefits to be derived from the presence of [numerous offshore oil and gas deposits](http://thediplomat.com/2012/02/04/beijings-south-china-sea-gamble/) within contested waters. Strangely enough, however, one of the principal explanations for China’s increased prickliness towards foreign military presence within its maritime backyard has yet to be clearly articulated. Indeed, not only is the South China Sea one of the world’s busiest trade thoroughfares, it also happens to be the roaming pen of China’s emerging ballistic missile submarine fleet, which is stationed at [Sanya](http://www.fas.org/blog/ssp/2008/04/new-chinese-ssbn-deploys-to-hainan-island-naval-base.php), on the tropical Island of Hainan. The United States, with its array of advanced anti-submarine warfare assets and hydrographic research vessels deployed throughout the region, gives Beijing the unwelcome impression that Uncle Sam can’t stop peering into its nuclear nursery. When Chinese naval strategists discuss their maritime environs, the sentiment they convey is one of [perpetual embattlement](http://www.nytimes.com/2012/09/28/opinion/between-US-and-Asia-the-best-defense-is-dialogue.html?_r=0). Pointing to the US’s extended network of allies in the Indo-Pacific region, and to their own relative isolation, Chinese strategists fear that Beijing’s growing navy could be ensnared within the first island chain-a region which they describe as stretching from Japan all the way to the Indonesian archipelago. Applying this maritime siege mentality to naval planning; they fret that the US Navy could locate and neutralize their fledgling undersea deterrent in the very first phases of conflict, before it even manages to slip through the chinks of first island chain. This concern helps explain China's growing intolerance to foreign military activities in the South China Sea. Tellingly, some of the most nerve-wracking **standoffs involving US and Chinese forces** have **unfolded in close proximity** to Hainan. The infamous [Ep-3 crisis](http://news.bbc.co.uk/2/hi/asia-pacific/1260290.stm), during which a US spy plane entered into collision with a Chinese fighter jet, occurred while the plane’s crew was attempting to collect intelligence on naval infrastructure development. Similarly, the [USNS Impeccable incident](http://www.nytimes.com/2009/03/12/washington/12web-china.html), during which a US hydrographic vessel was dangerously harassed by five Chinese ships, took place approximately seventy miles to the south of Hainan. During the confrontation, Chinese sailors reportedly attempted to unhook the Impeccable’s towed acoustic array sonars. In public, China's protests over foreign military activities are couched in territorial terms. In private, however, **Chinese policymakers readily acknowledge the centrality of the nuclear dimension**. Thus in the course of a discussion with a former Chinese official, I was told that “even though territorial issues are of importance, our major concern is the sanctity of our future sea-based deterrent.” He then went on to describe, with a flicker of amusement, how fishermen off the coast of Hainan regularly snag US sonars in their nets, and are encouraged to sell them back to the local authorities in exchange for financial compensation. Of course, such cat and mouse games are nothing new-and are perfectly legal- provided they occur within international waters or airspace. During the Cold War, American and Soviet ships would frequently conduct forward intelligence gathering missions, sometimes in very close proximity to each others’ shores. At the time, [American thinkers cautioned](http://books.google.com/books?hl=fr&lr=&id=rqnNaG2jL7wC&oi=fnd&pg=PR9&dq=barry+posen+inadvertent+escalation&ots=0esVgPTh4H&sig=maTUiyNXIx2Oo_eJFnvxIzPcf1M) that such **risky behavior could** potentially **lead to misinterpretation and nuclear disaster.** Unlike the Soviets, however, who could confine the movements of their boomers to the frigid, lonely waters of the Barents and Okhotsk seas, the Chinese have chosen to erect their nuclear submarine base smack-bang in the middle of one of the world’s busiest maritime highways. Needless to say, this location is hardly ideal. When it comes to picking strategic real-estate in their near seas, the Chinese have but a limited roster of options. After all, their maritime backyard is girded by a sturdy palisade of states which increasingly view China’s meteoric rise, and attendant truculence at sea, with a mixture of alarm and dismay. Like a dragon caught floundering in a bathtub, China’s naval ambitions are simply too broad and grandiose for its constricted maritime geography. This perceived lack of strategic depth provides a partial explanation to Beijing’s increased obduracy over territorial disputes in the South China Sea. In order to better protect its valuable subsurface assets, China aims to establish a ring of maritime watch towers or bastions around Hainan. Absolute control over the remote [Spratly islands](http://hir.harvard.edu/the-spratly-islands-dispute-order-building-on-china-s-terms), in addition to the more proximate Paracels, would greatly facilitate this concentric defensive configuration. Until not long ago, China’s strategic submarine force wasn’t really taken seriously. Their lone 0-92 Xia class boat was deemed too [antiquated](http://www.globalsecurity.org/wmd/world/china/type_92.htm)-and noisy-to be anything more than a symbol of Beijing’s desire for great power status. Some observers had ventured that China would be content to rely almost exclusively on its rapidly modernizing land-based missile system for its deterrent. Recent developments, however, suggest that this may be about to change. In its [latest report to Congress](http://www.reuters.com/article/2012/11/08/us-china-usa-military-idUSBRE8A705720121108), the US-China Economic and Security Review Commission stated that China could soon equip its new class of Jin submarines with the JL-2 ballistic missile, which has a range of approximately 4 600 miles. This would enable Beijing, the report adds, to establish a “near-continuous at-sea strategic deterrent”.  In all likelihood this force will be berthed at Hainan. The second **Obama** Administration **will** therefore **have the unenviable task of dealing with tensions in a region which is not only riddled with territorial divisions, but is** also **rapidly morphing into one of the world’s most sensitive nuclear hotspots.**

### Plan

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

### Solvency

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

Bradbury 11

Assistant Attorney General for the Office of Legal Counsel

(Steven, The Developing Legal Framework for Defensive and Offensive Cyber Operations, <http://harvardnsj.org/wp-content/uploads/2011/02/Vol.-2_Bradbury_Final1.pdf>)

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

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

Goldsmith 10

, Professor of Law at Harvard, Can we stop the Cyber Arms Race, Jack Goldsmith teaches at Harvard Law School and is on the Hoover Institution's Task Force on National Security and Law. He was a member of a 2009 National Academies committee that issued the report "[Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities](http://www.anagram.com/berson/nrcoiw.pdf).", <http://articles.washingtonpost.com/2010-02-01/opinions/36895669_1_botnets-cyber-attacks-computer-attacks>

In a [speech this month on "Internet freedom](http://www.state.gov/secretary/rm/2010/01/135519.htm)," Secretary of State Hillary **Clinton** [**decried the cyberattacks**](http://www.washingtonpost.com/wp-dyn/content/article/2010/01/21/AR2010012101699.html) that threaten U.S. economic and national security interests. "Countries or individuals that engage in cyber attacks should face consequences and international condemnation," she warned, alluding to the China-Google kerfuffle. **We should "create norms** of behavior among states **and encourage respect for the** global **networked commons**." Perhaps so. But **the problem with Clinton's call for** accountability and **norms** on the global network -- a call frequently heard in policy discussions about cybersecurity -- **is the enormous array of cyberattacks originating from the U**nited **S**tates. **Until we acknowledge these** attacks **and signal how we might control them, we cannot make progress on preventing cyberattacks emanating from other countries.** An important weapon in the cyberattack arsenal is a botnet, a cluster of thousands and sometimes millions of compromised computers under the ultimate remote control of a "master." Botnets were behind last summer's attack on South Korean and American government Web sites, as well as prominent attacks a few years ago on Estonian and Georgian sites. They are also engines of spam that can deliver destructive malware that enables economic espionage or theft. **The U**nited **S**tates **has the most**, or nearly the most, **infected botnet computers and is thus the country from which a good chunk of botnet attacks stem**. The government could crack down on botnets, but doing so would raise the cost of software or Internet access and would be controversial. So it has not acted, and the number of dangerous botnet attacks from America grows. The United States is also a leading source of "hacktivists" who use digital tools to fight oppressive regimes. Scores of individuals and groups in the United States design or employ computer payloads to attack government Web sites, computer systems and censoring tools in Iran and China. These efforts are often supported by U.S. foundations and universities, and by the federal government. Clinton boasted about this support seven paragraphs after complaining about cyberattacks. Finally, the U.S. government has perhaps the world's most powerful and sophisticated offensive cyberattack capability. This capability remains highly classified. But the [New York Times has reported](http://www.nytimes.com/2009/04/28/us/28cyber.html?_r=2) that the Bush administration used cyberattacks on insurgent cellphones and computers in Iraq, and that it approved a plan for attacks on computers related to Iran's nuclear weapons program. And the government is surely doing much more. "We have U.S. warriors in cyberspace that are deployed overseas" and "live in adversary networks," says Bob Gourley, the former chief technology officer for the Defense Intelligence Agency. These warriors are now under the command of Lt. Gen. Keith Alexander, director of the National Security Agency. The NSA, the world's most powerful signals intelligence organization, is also in the business of breaking into and extracting data from offshore enemy computer systems and of engaging in computer attacks that, in the NSA's words, "disrupt, deny, degrade, or destroy the information" found in these systems. When the Obama administration created "cyber command" last year to coordinate U.S. offensive cyber capabilities, it nominated Alexander to be in charge. Simply put, **the U**nited **St**ates **is** in a big way **doing the** very **things** that **Clinton criticized**. We are not, like the Chinese, stealing intellectual property from U.S. firms or breaking into the accounts of democracy advocates. But we are aggressively using the same or similar computer techniques for ends we deem worthy. Our potent offensive cyber operations matter for reasons beyond the hypocrisy inherent in undifferentiated condemnation of cyberattacks. Even if we could stop all cyberattacks from our soil, we wouldn't want to. On the private side, hacktivism can be a tool of liberation. On the public side, the best defense of critical computer systems is sometimes a good offense. "My own view is that the only way to counteract both criminal and espionage activity online is to be proactive," [Alexander said last year](http://news.bbc.co.uk/2/hi/8033440.stm), adding that if the Chinese were inside critical U.S. computer systems, he would "want to go and take down the source of those attacks." Our **adversaries are aware** of our prodigious and growing offensive cyber capacities and exploits. In a [survey published Thursday by the security firm McAfee](http://newsroom.mcafee.com/article_display.cfm?article_id=3617), more **i**nformation **t**echnology **experts** from critical infrastructure firms **around the world expressed concern about the U**nited **St**ates **as a source of** computer network **attacks** than about any other country. **This** awareness, **along with our vulnerability** to cyberattacks, **fuels a dangerous public and private cyber arms race in an arena where** the **offense** already **has a natural advantage**.

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

Lewis 11

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

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

#### Second it solves perception — Congress is necessary to reverse independent presidential authority— now is key

Dycus 10

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

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

#### Congressional restrictions on OCOs send a global signal of cyber leadership

Bastby 12

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

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

#### 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.**

#### Covert designation fuels suspicion and can’t solve cyber war

**Wright 11**, Executive director of studies at The Chicago Council on Global Affairs

(Thomas, 6/26, America has double standards in fighting cyberwar, [www.ft.com/cms/s/0/c8002f6a-a01b-11e0-a115-00144feabdc0.html#axzz1QYnW3i1w](http://www.ft.com/cms/s/0/c8002f6a-a01b-11e0-a115-00144feabdc0.html#axzz1QYnW3i1w))

While it has several advantages, **treating American cyber-destruction as a covert operation will severely undermine the new cyber-strategy. Suspicion that the US uses cyber­weapons whenever convenient will hamper its attempts to press other states to be transparent about their intentions**. **In particular, it takes the pressure off China, widely believed to be the leading state source of cyberattacks. It may also dissuade the US from developing the technology to trace the source of an attack.**

# 2AC

## 2AC EU SOPO

### NUQ

#### EU Sopo irreversibly low

Eyal 13

Jonathan Eyal, Straits Times, “Fading global influence and reputation of Europe a major cause for concern,” 4/9/13, <https://www.chinapost.com.tw/commentary/the-china-post/special-to-the-china-post/2013/04/09/375533/Fading-global.htm> SJE

Many strategic experts still believe Europe's current financial crisis is just an aberration which will soon pass. Although the Europeans infuriated the rest of the world with their never-ending series of last-minute summits and telephone calls, leaders and their finance ministers have held the bloc together in the face of growing strains between states, a rising political backlash and market alarm. No government has defaulted on its debts. Europe ended up doing the right thing, albeit only after trying everything else. So, given a bit of luck and a bit of economic growth, Europe could return to its traditional role on the world stage. Sadly, however, the chances of this happening remain slim. To start with, Europe's problem is not temporary but endemic: Its economic model is no longer sustainable, and the painful readjustment process will take at least a decade. The current crisis is, therefore, not an exception but the new European norm. And it will have profound consequences, by diminishing Europe's global footprint. Evidence for this is everywhere. There is no common European position on China. There is also no common European interpretation about the significance of the U.S. pivot to Asia, arguably one of the most strategically significant decisions of our times. Many of the smaller EU countries have already closed scores of overseas embassies: Their foreign ministries now do little more than follow the world from the newspapers. Meanwhile, most European leaders nowadays talk about where their next “tranche” of bailout cash may come from. Global problems are left to lower-level officials who can handle them but cannot make serious decisions. Overseas aid — hitherto a source of pride and influence for Europe — is also shrinking, with the notable exception of Britain, where the government has decided to maintain aid expenditure not because it believes in it, but largely in order to dispel domestic accusations that it is heartless. To make matters worse, the EU's foreign policy is suffering a double dip: the loss of relative influence compared with other powers, supplemented now with loss of foreign policy resources not just in relative but absolute terms. As a result, Europe's famed “carrot-and-stick” approach to global partners no longer makes sense: The carrot — in the shape of Europe's stagnant economy — is no longer enticing for other countries to accept, and the stick — EU sanctions against those it does not like — is no longer credible.

### No Link

#### US and EU influence don’t trade off

Grant 03

Charles Grant, director of the Center for European Reform, 03 [april/may, cer bulletin, issue 29, “The Decline of American Power” http://www.cer.org.uk/articles/29\_grant.html, accessed 7-17-07]

When the war is over, the western allies will have a strong interest in helping each other to rebuild their soft power. Even the Washington hawks should see that many of the most pressing challenges in global economic governance, the reconstruction of failed states, and the fight against terror and weapons proliferation cannot be tackled except through broad alliances and international institutions. President Bush could do wonders for America's image by adopting a more diplomatic style and by focusing on the Middle East peace process. Tony Blair will need to show his European partners that Britain's support for the US is not unconditional and that it has a European destiny. Jacques Chirac should accept the reality of EU enlargement, learn to make friends in Eastern Europe, and abandon the idea that the rationale of EU foreign policy is to resist the US. The example of the European Union shows that soft power is not a zero-sum game: it has enabled all the member-states to enhance their influence and well-being. A stronger West needs countries with more power hard and soft on both sides of the Atlantic.

#### No tradeoff

Nye 04

Joseph Nye, Dean of the Kennedy School at Harvard, SOFT POWER 2004, p 82.

#### Not only can European soft power be used to counter American soft power and raise the price of unilateral actions, but it can also be a source of assistance and reinforcement for American soft power and increase the likelihood of the United States’ achieving its objectives. Soft power can be shared and used in a cooperative fashion. European promotion of democracy and human rights helps advance shared values that are consistent with American objectives. The Islamist extremists of Al Qaeda are fighting against Western values, not just American values, and European public diplomacy that counters their appeal is benefi Middle East conflict won’t escalate – local conflicts do not spillover

Cook, Takeyh, and Maloney 7

Steven A. Cook (fellow at the Council on Foreign Relations) Ray Takeyh (fellows at the Council on Foreign Relations) and Suzanne Maloney (senior fellow at Saban Center) June 28 2007 “Why the Iraq war won't engulf the Mideast”, International Herald Tribune

Finally, there is no precedent for Arab leaders to commit forces to conflicts in which they are not directly involved. The Iraqis and the Saudis did send small contingents to fight the Israelis in 1948 and 1967, but they were either ineffective or never made it. In the 1970s and 1980s, Arab countries other than Syria, which had a compelling interest in establishing its hegemony over Lebanon, never committed forces either to protect the Lebanese from the Israelis or from other Lebanese. The civil war in Lebanon was regarded as someone else's fight. Indeed, this is the way many leaders view the current situation in Iraq. To Cairo, Amman and Riyadh, the situation in Iraq is worrisome, but in the end it is an Iraqi and American fight. As far as Iranian mullahs are concerned, they have long preferred to press their interests through proxies as opposed to direct engagement. At a time when Tehran has access and influence over powerful Shiite militias, a massive cross-border incursion is both unlikely and unnecessary. So Iraqis will remain locked in a sectarian and ethnic struggle that outside powers may abet, but will remain within the borders of Iraq. The Middle East is a region both prone and accustomed to civil wars. But given its experience with ambiguous conflicts, the region has also developed an intuitive ability to contain its civil strife and prevent local conflicts from enveloping the entire Middle East.

cial to the United States.

#### No widespread prolif

Hymans 12

Jacques E. C. Hymans is Associate Professor of IR at USC [April 16, 2012, “North Korea's Lessons for (Not) Building an Atomic Bomb,” *Foreign Affairs*, http://www.foreignaffairs.com/articles/137408/jacques-e-c-hymans/north-koreas-lessons-for-not-building-an-atomic-bomb?page=show]

Washington's miscalculation is not just a product of the difficulties of seeing inside the Hermit Kingdom. It is also a result of the broader tendency to overestimate the pace of global proliferation. For decades, Very Serious People have predicted that strategic weapons are about to spread to every corner of the earth. Such warnings have routinely proved wrong -- for instance, the intelligence assessments that led to the 2003 invasion of Iraq -- but they continue to be issued. In reality, despite the diffusion of the relevant technology and the knowledge for building nuclear weapons, the world has been experiencing a great proliferation slowdown. Nuclear weapons programs around the world are taking much longer to get off the ground -- and their failure rate is much higher -- than they did during the first 25 years of the nuclear age. As I explain in my article "Botching the Bomb" in the upcoming issue of Foreign Affairs, the key reason for the great proliferation slowdown is the absence of strong cultures of scientific professionalism in most of the recent crop of would-be nuclear states, which in turn is a consequence of their poorly built political institutions. In such dysfunctional states, the quality of technical workmanship is low, there is little coordination across different technical teams, and technical mistakes lead not to productive learning but instead to finger-pointing and recrimination. These problems are debilitating, and they cannot be fixed simply by bringing in more imported parts through illicit supply networks. In short, as a struggling proliferator, North Korea has a lot of company.

## 2AC Politics

### 2AC

#### ZERO chance of passage – the GOP are pushing piecemeal reform, Obama isn’t pushing, and PC fails

Lerer & Tiron 10/31 Lisa Lerer and Roxana Tiron is Bloomberg Staff Reporters, “Who's Afraid of Immigration Reform?” <http://www.businessweek.com/articles/2013-10-31/immigration-reform-unlikely-amid-congresss-partisan-ill-will>, DOA: 11-1-13, y2k

After the government shutdown ended, President Obama said he wanted Congress again to take up languishing immigration legislation, with the goal of passage by yearend. That’s unlikely, and not just because a majority of House Republicans still oppose a bill that includes a path to citizenship for undocumented workers. Democrats from states with large numbers of Hispanic voters, who are concerned Obama is so intent on signing an immigration law that he might water it down to attract GOP support, are in no hurry to meet his deadline if it means compromising on citizenship. “There are some Democrats who would rather get it done, and others who would rather have the issue” linger, says Tamar Jacoby, president of ImmigrationWorks USA, a network of business groups that promotes legal immigration. Not that the two parties are in a mood to talk about immigration—or anything else. The shutdown and debt limit fight further poisoned Republicans’ already toxic relationship with the White House and Democratic leaders. “There’s no discussion about immigration” on either side, says Texas Republican John Carter. In September he left a bipartisan group that was working on a deal in the House. “I have a heart for fixing immigration, but not sure the will is there.” Beyond setting a goal and saying he doesn’t want to “leave this problem to keep festering,” the president has largely been quiet on the issue since the government reopened. He’s not giving big speeches or going out barnstorming aboard his bus. After coming away from the shutdown empty-handed, Republicans are wary of doing anything to help Obama’s agenda. “If he leans into it too aggressively, it makes it harder for Republicans to get to yes,” says Frank Sharry, executive director of America’s Voice, a pro-immigration group. “He wants a result so badly that he’s willing to step back so Republicans can step forward.” House Speaker John Boehner has said the House won’t back the comprehensive immigration bill the Senate passed in June and instead will take action on smaller-scale, piecemeal measures. Speaking to reporters on Oct. 23, he said he’s still hopeful. The House Judiciary Committee has approved legislation dealing with enforcement, employment verification, and agricultural and high-skilled workers. California Republican Darrell Issa, chairman of the House Committee on Oversight and Government Reform, is working on a proposal that would offer temporary legal status to qualifying undocumented immigrants, according to spokesman Frederick Hill. Even if the bills were to pass the House, they’d likely die in the Senate. Two months may seem like long enough to work out some of those differences, but there are only a handful of working days left on the congressional calendar this year, and no one in Washington will be up for haggling over a contentious piece of legislation during the holidays. Democrats have hinted to reporters that despite Obama’s desire for a bill, they’re content to shelve the issue until next summer, when their leverage improves. Election-minded Republicans may then be more eager to take up the legislation as a way to woo Hispanic voters. Such calculations underestimate how angry Republicans are at Obama and how little they want to hand him anything resembling a victory. More than citizenship or border security, ill will could be the thing that stops immigration reform. “This notion that they’re going to get in a room and negotiate a deal with the president on immigration is much more difficult to do because of the way that president has behaved towards his opponents over the last few weeks,” Florida Republican Senator Marco Rubio, who helped write the Senate immigration bill, told Fox News (FOX) on Oct. 20. Republican Representative Raúl Labrador of Idaho was less diplomatic in expressing why a deal may be a long way off. Obama “tried to destroy the Republican Party,” he told an audience of Republicans on Oct. 16. “Anything we do right now with this president on immigration will be with that same goal in mind, which is to destroy the Republican Party and not to get good policies.”

#### Piecemeal means no solvency

NBC 10/20

("Did shutdown 'poison the well' for immigration reform?" http://nbcpolitics.nbcnews.com/\_news/2013/10/20/21026903-did-shutdown-poison-the-well-for-immigration-reform?lite)

“We’re not going to have an immigration reform bill this year, or next year, that doesn’t deal with the 11 million,” Fitz predicted. “People are hungering for a solution. These piecemeal measures may step in the right direction for some, but they’re clearly not going to solve the whole problem.”

#### Boehner won’t break the Hastert rule

Workpermit.Com 10/30 “Boehner 'hopeful' that US immigration reform will happen this year,” 30 October 2013

<http://www.workpermit.com/news/2013-10-30/boehner-hopeful-that-us-immigration-reform-will-happen-this-year>, DOA: 11-1-13, y2k

The speaker of the US House of Representatives, John Boehner, has said that he is 'hopeful' that 'the House' will pass immigration reform this year. He told journalists on October 23rd 2013, 'I think immigration is an important subject that needs to be addressed and I'm hopeful [that it will be]'. However, Mr Boehner refused to answer journalists' questions as to when he might introduce a bill. Democrats may be sceptical about Mr Boehner's claim to be 'hopeful'; as speaker, Mr Boehner is responsible for putting bills before the House for a vote. He has so far refused to put a bill already passed by the Senate before the House because a majority of Republicans oppose it. Under the US system, for a bill to become law, it must be passed by both houses of Congress; the upper house, the Senate and the lower house, the House of Representatives. In July, the Senate passed the Border Security, Economic Opportunity and Immigration Modernization Act 2013 (The Border Security Act'). This bill would, if it became law, introduce comprehensive immigration reform. Mr Boehner has so far refused to put that bill before the House for a vote, thereby preventing it from becoming law. Hastert Rule Mr Boehner says that 'the Hastert Rule' prevents him from doing so. The Hastert Rule is an informal principle which has no basis in the Constitution. It is named after the former Republican speaker Dennis Hastert who was speaker from 1999-2007. The rule means that a speaker of the House will only put legislation before the House if 'a majority of the majority' that is to say, over half of all members of the larger party in the House support it. The 'rule' is not really a rule at all and even Speaker Hastert said in 2013, 'The Hastert Rule never really existed. It's kind of a nonentity as far as I'm concerned'. Nonetheless, many speakers of the House use their position to prevent the House from voting on bills brought by the opposing party. Democrats are urging Speaker Boehner to waive the Hastert Rule and allow a vote on the Border Security Act. But, so far at least, Mr Boehner has refused. The House has 435 seats. There are currently 231 Republicans, so for Boehner to allow a vote without breaking the Hastert Rule, at least 116 Republicans will have to express support for the bill. At present, there are nowhere near that many. Boehner 'standing in the way of democracy' Democrats claim that Boehner is thwarting the will of the people. They cite polls which show that about 60% of Americans support reform. House Democrats believe that there are enough Republicans in the House who support the Act for it to become law if Mr Boehner will allow a vote. Mr Boehner has broken the Hastert Rule five times already in 2013. Democrats are hopeful that he will do it again. But Mr Boehner is under great pressure from right-wing Republicans elected since 2009 with the support of the right-wing Tea Party movement. These Representatives are against 'big government' and have done everything that they can to thwart President Obama since they reached Congress. Their opposition to the President has led them to vote against almost any legislation that the Democrats have proposed. Tea Party Republicans particularly angry at the moment They are currently particularly angry after they attempted, and failed, to make the President reform his 'Obamacare' health insurance programme in return for authorising the federal budget. The Tea Party contingent is said by Washington commentators to be particularly keen to prevent the President from scoring any 'victories' in the remainder of the political year. The President has promised to make immigration reform a priority of his second term. This will make the Tea Party Republicans particularly keen to thwart him. The Tea Party Republicans are also largely against the Border Security Act. This is mostly because the bill, which aims to comprehensively reform the US immigration, will establish a 'pathway to citizenship' for most of the 11.5m people living in the US illegally. Republicans, and particularly Tea Party Republicans, say that to do so would be to reward people for breaking US law (by entering or remaining in the US illegally).

#### XO solves

Mike Lillis, 2/16/2013 (staff writer, “Dems: Obama can act unilaterally on immigration reform,” <http://thehill.com/blogs/regwatch/administration/283583-dems-recognize-that-obama-can-act-unilaterally-on-immigration-reform>, Accessed 2/21/2013, rwg)

President Obama can – and will – take steps on immigration reform in the event Congress doesn't reach a comprehensive deal this year, according to several House Democratic leaders.¶ While the Democrats are hoping Congress will preclude any executive action by enacting reforms legislatively, they say the administration has the tools to move unilaterally if the bipartisan talks on Capitol Hill break down. Furthermore, they say, Obama stands poised to use them.¶ "I don't think the president will be hands off on immigration for any moment in time," Rep. Xavier Becerra (D-Calif.), the head of the House Democratic Caucus, told reporters this week. "He's ready to move forward if we're not."

#### Disad isn’t intrinsic to the aff – it’s within the agential ambit of the USFG to do the plan and pass debt ceiling

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

Kriner 10

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

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

#### Plan breaks the GOP – ensures passage

Dickerson 1/18

(John, Chief Political Correspondent at the Slate, Political Director of CBS News, Covered Politics for Time Magazine for 12 Years, Previous White House Correspondent, Go for the Throat!, http://tinyurl.com/b7zvv4d)

[www.slate.com/articles/news\_and\_politics/politics/2013/01/barack\_obama\_s\_second\_inaugural\_address\_the\_president\_should\_declare\_war.single.html](http://www.slate.com/articles/news_and_politics/politics/2013/01/barack_obama_s_second_inaugural_address_the_president_should_declare_war.single.html), CMR

On Monday, President Obama will preside over the grand reopening of his administration. It would be altogether fitting if he stepped to the microphone, looked down the mall, and let out a sigh: so many people expecting so much from a government that appears capable of so little. A second inaugural suggests new beginnings, but this one is being bookended by dead-end debates. Gridlock over the fiscal cliff preceded it and gridlock over the debt limit, sequester, and budget will follow. After the election, the same people are in power in all the branches of government and they don't get along. There's no indication that the president's clashes with House Republicans will end soon. Inaugural speeches are supposed to be huge and stirring. Presidents haul our heroes onstage, from George Washington to Martin Luther King Jr. George W. Bush brought the Liberty Bell. They use history to make greatness and achievements seem like something you can just take down from the shelf. Americans are not stuck in the rut of the day. But this might be too much for Obama’s second inaugural address: After the last four years, how do you call the nation and its elected representatives to common action while standing on the steps of a building where collective action goes to die? That bipartisan bag of tricks has been tried and it didn’t work. People don’t believe it. Congress' approval rating is 14 percent, the lowest in history. In a December Gallup poll, 77 percent of those asked said the way Washington works is doing “serious harm” to the country. The challenge for President Obama’s speech is the challenge of his second term: how to be great when the environment stinks. Enhancing the president’s legacy requires something more than simply the clever application of predictable stratagems. Washington’s partisan rancor, the size of the problems facing government, and the limited amount of time before Obama is a lame duck all point to a single conclusion: The president who came into office speaking in lofty terms about bipartisanship and cooperation can only cement his legacy if he destroys the GOP. If he wants to transform American politics, he must go for the throat. President Obama could, of course, resign himself to tending to the achievements of his first term. He'd make sure health care reform is implemented, nurse the economy back to health, and put the military on a new footing after two wars. But he's more ambitious than that. He ran for president as a one-term senator with no executive experience. In his first term, he pushed for the biggest overhaul of health care possible because, as he told his aides, he wanted to make history. He may already have made it. There's no question that he is already a president of consequence. But there's no sign he's content to ride out the second half of the game in the Barcalounger. He is approaching gun control, climate change, and immigration with wide and excited eyes. He's not going for caretaker. How should the president proceed then, if he wants to be bold? The Barack Obama of the first administration might have approached the task by finding some Republicans to deal with and then start agreeing to some of their demands in hope that he would win some of their votes. It's the traditional approach. Perhaps he could add a good deal more schmoozing with lawmakers, too. That's the old way. He has abandoned that. He doesn't think it will work and he doesn't have the time. As Obama explained in his last press conference, he thinks the Republicans are dead set on opposing him. They cannot be unchained by schmoozing. Even if Obama were wrong about Republican intransigence, other constraints will limit the chance for cooperation. Republican lawmakers worried about primary challenges in 2014 are not going to be willing partners. He probably has at most 18 months before people start dropping the lame-duck label in close proximity to his name. Obama’s only remaining option is to pulverize. Whether he succeeds in passing legislation or not, given his ambitions, his goal should be to delegitimize his opponents. Through a series of clarifying fights over controversial issues, he can force Republicans to either side with their coalition's most extreme elements or cause a rift in the party that will leave it, at least temporarily, in disarray.

#### The plan’s not perceived

Schmitt 13, **co-director of the Marilyn Ware Center for Security Studies at AEI** and the director of AEI's Program on American Citizenship. Mr. Schmitt is a former staff director of the Senate Select Committee on Intelligence. He was executive director of the President's Foreign Intelligence Advisory Board during President Ronald Reagan's second term. Mr. Schmitt's security work focuses on longer-term strategic issues that will affect America's security at home and its ability to lead abroad, while his work in the area of citizenship focuses on challenges to maintaining and sustaining a strong civic culture. His books include Of Men and Materiel: The Crisis in Military Resources (AEI Press, 2007), to which he was a contributing author and editor with Tom Donnelly; Silent Warfare: Understanding the World of Intelligence (Brassey’s, 2002), coauthored with Abram Shulsky and now in its third edition; and U.S. Intelligence at the Crossroads: Agendas for Reform (Brassey’s, 1995), a coedited volume to which he is a contributing author. His two most recent books, to which he is also editor and contributing author, are The Rise of China: Essays on the Future Competition (Encounter Books, May 2009) and Safety, Liberty and Islamist Terrorism: American and European Approaches to Domestic Counterterrorism (AEI Press, 2010), <http://www.aei-ideas.org/2011/12/authorization-for-cyber-attacks/>

**The press (and the White House) has been obsessed by the detention provision** in the recently agreed upon FY2012 **Defense Authorization bill, but one of the items that** slipped under the radar **is language authorizing the American military to engage in offensive operations in cyberspace.** Under Sec. 954,

### 2AC Fight Back Link

#### Obama won’t fight the plan

Howell and Pevehouse 7

William Howell and Jon Pevehouse, Associate Professors at the Harris School of Public Policy at the University of Chicago, 2007, When Congress Stops Wars, Foreign Affairs, EBSCO

After all, when presidents anticipate congressional resistance they will not be able to overcome, they often abandon the sword as their primary tool of diplomacy. More generally, when the White House knows that Congress will strike down key provisions of a policy initiative, it usually backs off. President Bush himself has relented, to varying degrees, during the struggle to create the Department of Homeland Security and during conflicts over the design of military tribunals and the prosecution of U.S. citizens as enemy combatants. Indeed, by most accounts, the administration recently forced the resignation of the chairman of the Joint Chiefs of Staff, General Peter Pace, so as to avoid a clash with Congress over his reappointment.

**2AC Econ**

#### 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).

#### It’s resilient

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."

#### US not key to global economy

Wassener 9

Wassener, MSC in IR, 9—London School of Economics and Political Science, MSc , International Relations, Politics (Bettina, In Asia, a Derided Theory Returns, 1 July 2009, <http://query.nytimes.com/gst/fullpage.html?res=9C0CEFDE163EF932A35754C0A96F9C8B63>)

HONG KONG -- For a while, when the global economic crisis was at its worst, it was a dirty word that only the most provocative of analysts dared to use. Now, the D-word -- decoupling -- is making a comeback, and nowhere more so than in Asia. Put simply, the term refers to the theory that emerging countries -- whether China or Chile -- will become more independent of the ups and downs in the United States as their economies become stronger and more sophisticated. For much of last year, the theory held up. Many **emerging economies** had **steered clear of investments that dragged down a string of banking behemoths in the West**, and saw nothing like the turmoil that began to engulf the United States and Europe in 2007. But then, last autumn, when the collapse of Lehman Brothers caused the global financial system to convulse and consumer demand to shrivel, emerging economies around the world got caught in the downdraft, and the D-word became mud. Now, the tables are turning again, especially in Asia, where many emerging economies are showing signs of a stronger recovery than in the West. And economists here have begun to use the D-word in public once again. ''Decoupling is happening for real,'' **the chief Asia-Pacific economist at Goldman Sachs in Hong Kong**, Michael Buchanan, **said in a recent interview**. Or as the senior Asia economist at HSBC, Frederic Neumann, said, ''Decoupling is not a dirty word.'' To be sure, the once sizzling pace of Asian economic growth has slowed sharply as exports to and investments from outside the region slumped. Across Asia, millions of people have lost their jobs as business drops off and companies cut costs and output. Asia is heavily dependent upon selling its products to consumers in the United States and Europe, and many executives still say a strong U.S. economy is a prerequisite for a return to the boom of years past. Nevertheless, the theory of decoupling is back on the table. **For the past couple of months, data from around the world have revealed a growing divergence between Western economies and those in much of Asia**, notably China and India. The World Bank last week forecast that the economies of the euro zone and the United States would contract 4.5 percent and 3 percent, respectively, this year -- in sharp contrast to the 7.2 percent and 5.1 percent economic growth it forecasts for China and India. **Forecasts from the Organization for Economic Cooperation and Development** that **were** also **published last week backed up this general trend**. Major statistics for June, due Wednesday, are expected to show manufacturing activity in China and India are on the mend. By contrast, purchasing managers' indexes for Europe and the United States are forecast to be merely less grim than before but still show contractions. Why this diverging picture? **The crisis hit Asia much later**. **While the U.S. economy began languishing in** 20**07**, **Asian economies were still doing well right up until the collapse of Lehman Brothers** last September. What followed was a rush of stimulus measures -- rate cuts and government spending programs. In Asia's case, these came soon after things soured for the region; in the United States, they came much later in the country's crisis. Moreover, **developing** Asian **economies were in pretty good shape when the crisis struck**. The last major crisis to hit the region -- the financial turmoil of 1997-98 -- forced governments in Asia to introduce overhauls that ultimately left them with lower debt levels, more resilient banking and regulatory systems and often large foreign exchange reserves. Another crucial difference is that **Asia**, unlike the United States and Europe, **has not had a banking crisis**. Bank profits in Asia have plunged and some have had to raise extra capital **but** there have been no major collapses and no bailouts. ''The single most important thing to have happened in Asia is that there has not been a banking crisis,'' said Andrew Freris, a regional strategist at BNP Paribas in Hong Kong. ''Asia is coming though this crisis with its banking system intact. Yes, some banks may not be making profits -- but **it is cyclical and not systemic**.'' The lack of banking disasters also has meant that, unlike in Europe and the United States, **Asian governments have not had to spend cash to clean the balance sheets of faltering banks**. In other words, all of the stimulus spending is going into the economy. The effect is greater and more immediate. Add to that the fact that companies and households in Asia are typically not burdened with the kind of debt that is forcing Americans and Europeans to cut back consumption and investment plans. Asians are generally big savers; those in developing nations have limited health care and pension systems to fall back on. So they put aside cash for retirement, sickness and their children's education, rather than maxing out multiple credit cards. Paul Schulte of Nomura said this difference was leading to a long-term shift.

## 2AC Funding CP

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

#### Perm- do the counterplan

#### Non- intrinsic counterplans are a voting issue- they are unpredictable making impossible to garner 2ac offense while artificially inflating neg benefits- skews the debate too far in favor of the neg

#### Doesn’t solve any advantage

#### a) Norms won’t be created by complete abdication, we have to create checks and balances – that’s Bradbury and Goldsmith

#### Links to politics

Kimery 12 <Anthony, ¶ Online Editor and Manager of KMD Media's Online Media Division, Anthony "Tony" Kimery is one of the founding editors of Homeland Security Today. A respected award-winning editor and journalist, he's covered homeland, national and global security, intelligence and defense issues for three decades., Senate Cybersecurity Bill Shot Down Amid Partisan Acrimony, US Chamber Opposition, 08/02/2012, <http://www.hstoday.us/single-article/senate-cybersecurity-bill-shot-down-amid-partisan-acrimony-us-chamber-opposition/338eb768f7b3094acaa7b6ef21ffdeba.html>>#SPS

In a 52-46 vote Thursday, the Senate chose to cut off debate on the long-in-the-works Cybersecurity Act of 2012 (S. 3414), essentially terminating any chances that the bill would finally be passed. Sixty votes were needed to defeat a GOP-led filibuster in response to what Senate Minority Leader Sen. Mitch McConnell (R-Ky.) charged was the refusal by to Sen. Majority Leader Harry Reid (D-Nev.) to allow Republicans to offer amendments to the bill.¶ ¶ “Members on both sides of the aisle have recommendations for improving our cyberdefenses, and some of them thought this bill would provide an opportunity to propose those ideas through amendments -- especially since Democrats didn’t allow for an opportunity to do so in committee,” McConnell complained, adding, “Frankly, I was a little surprised the Majority Leader decided to file cloture and end debate before it even started.”¶ ¶ For his part, Reid said prior to the vote that, “This is another filibuster that could have been prevented by [Republicans] working to get a list of amendments.”¶ ¶ Rep. Jim Langevin (D-RI), co-founder of the Congressional Cybersecurity Caucus, said in a statement Thursday afternoon in reaction to the Senate’s inability to advance the bill that, “Despite a bipartisan attempt to reach an accommodation, the Senate’s efforts to improve our cybersecurity were derailed today by the obstruction of a group of Republican members, led by Minority Leader Mitch McConnell. Congress has now again failed to address one of the greatest security risks facing the American people. Just a week after the head of the National Security Agency reported a 17-fold increase in cyber attacks against our most vital and valuable industries, it is inexplicable that some of my colleagues still have not gotten the message about the threats to critical infrastructure."¶ ¶ “We have been warned repeatedly by our most senior and respected security officials that the country could experience major economic and physical damage if we do not address the vulnerabilities of critical infrastructure networks," Langevin said, adding, "opponents of legislation would have us believe that industry will act voluntarily to secure infrastructure, but the facts say otherwise. For years, the owners of our key infrastructure have had the opportunity to act, but far too many have proven unwilling to bear the costs, preferring to take the chance that they won’t be the ones that get hit."¶ ¶ Langevin continued: “This should be a time for leadership and for putting aside partisan ideology to fulfill our most fundamental obligation: protecting national security. Instead, many members, including some who have built a strong and admirable reputation on national security issues, have seemingly decided that no cost is too great to violate their anti-regulations dogma. They prefer to ignore the devastating consequences of a successful cyberattack, putting the profits of a small group of companies ahead of the public’s safety. Yet, if and when an attack occurs, the unfortunate reality is that it will be the American taxpayer who will be left to deal with the aftermath and foot the bill."¶ ¶ Langevin commended "the senators who made a tremendous effort to bring the parties together and find a compromise, particularly my fellow Rhode Islander, Sen. [Sheldon] Whitehouse, who understands the challenges we face in cyberspace and the pressing need for action, as well as" all the other senators who tirelessly worked on the bill. "They showed remarkable leadership and did everything they could to reach a compromise. Unfortunately, it appears their opponents would rather wait for disaster to strike before they act. While this is an incredibly disappointing development, I will continue to advocate for the enactment of the strongest possible cyberprotections for the American people.”¶ ¶ The bill was recently significantly [rewritten](http://www.hstoday.us/industry-news/general/single-article/senate-to-begin-debate-of-cybersecurity-act-despite-mccain-s-protests/c5cce425767af0ef16c7fdd66c981c1b.html) to accommodate a variety of concerns, including several new privacy-oriented changes, and had been supported by the Silicon Valley Leadership group, an organization of 375 member companies that include Facebook, Google and Adobe. Earlier this week the group had written to the five co-sponsors of the legislation indicating its support for the bill.

#### CP ends all OCO’s, that’s bad:

#### OCO’s key to airpower

Shaud and Lowther 11 < John A., PhD, USAF, retired, is director, Air Force Research Institute, Maxwell AFB, Alabama, where he directs an 80-person organization charged with conducting independent research, outreach, and engagement to enhance national security and assure the effectiveness of the US Air Force; Adam B., PhD, is a faculty researcher and defense analyst at the Air Force Research Institute, Maxwell AFB, An Air Force Strategic Vision for 2020–2030, Spring 2011, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA537570>>#SPS

For the Air Force, power projection can take many forms—as either ¶ hard or soft power. While power projection is synonymous with capabilities such as penetrating long-range strike, airlift, and aerial refueling, the ¶ future will also call for something new to the Air Force—offensive cyber ¶ capabilities. As the Air Force moves forward, the force structure—and, ¶ consequently, force-development programs—must change to emphasize ¶ these requirements, which will include integrating (manned and unmanned) air, space, and cyber capabilities. In other words, when formulating options to defend the nation’s interests, Airmen should present ¶ choices that represent the full range of integrated capabilities. This approach will position the service to capitalize on technological ¶ developments before and after 2030. Near-term changes in organization, ¶ doctrine, training, education, and force management will be required. For ¶ example, the current requirements of rated personnel (six-, nine-, and 12-¶ year flying gates) make it difficult to provide opportunities for them to ¶ acquire skills in space or cyber fields during their formative operational ¶ years. Providing limited exposure to traditional Air Force operations for ¶ individuals in the space and cyber career fields similarly undermines their ¶ understanding of airpower. By 2030, Airmen operating in a joint environment will be expected to present comprehensive options that represent the ¶ full capabilities of the Air Force rather than presenting compartmentalized ¶ solutions.¶ The key strategic problem from the perspective of potential adversaries ¶ is to deny the United States access to bases and targets. The proliferation ¶ of robust and redundant air defenses is a legacy of the Cold War, but this ¶ has taken on new importance for adversaries. In the near term, most nations ¶ will be unable to compete with the United States’ technological advantages ¶ in conventional combat. However, this will change as 2030 approaches. ¶ Future battlefields may look more like the recent Russo-Georgian conflict, ¶ in which a cyber offensive preceded Russia’s conventional attack. Conflicts ¶ will be more specifically targeted in terms of time and space, and the first ¶ salvos of a conflict may not be detected until the second- and third-order ¶ effects of initial strikes manifest themselves.¶

#### Solves global conflict escalation

Khalilzad and Lesser, 1

(PhD from the University of Chicago, counselor at CSIS, permanent representative to the UN, \*\*Senior Transatlantic Fellow at the US German Marshall Fund, former Vice President and Director of Studies at the Pacific Council on International Policy, RAND, “Sources of Conflict in the 21st Century”, p.164-5, http://www.rand.org/pubs/monograph\_reports/MR897/MR897.chap3.pdf)

This subsection attempts to synthesize some of the key operational implications distilled from the analyses relating to the rise of Asia and the potential for conflict in each of its constituent regions. The first key implication derived from the analysis of trends in Asia suggests that American air and space power will continue to remain critical for conventional and unconventional deterrence in Asia. This argument is justified by the fact that several subregions of the continent still harbor the potential for full-scale conventional war. This potential is most conspicuous on the Korean peninsula and, to a lesser degree, in South Asia, the Persian Gulf, and the South China Sea. In some of these areas, such as Korea and the Persian Gulf, the United States has clear treaty obligations and, therefore, has preplanned the use of air power should contingencies arise. U.S. Air Force assets could also be called upon for operations in some of these other areas. In almost all these cases, U.S. air power would be at the forefront of an American politico-military response because (a) of the vast distances on the Asian continent; (b) the diverse range of operational platforms available to the U.S. Air Force, a capability unmatched by any other country or service; (c) the possible unavailability of naval assets in close proximity, particularly in the context of surprise contingencies; and (d) the heavy payload that can be carried by U.S. Air Force platforms. These platforms can exploit speed, reach, and high operating tempos to sustain continual operations until the political objectives are secured. The entire range of warfighting capability—fighters, bombers, electronic warfare (EW), suppression of enemy air defense (SEAD), combat support platforms such as AWACS and J-STARS, and tankers—are relevant in the Asia-Pacific region, because many of the regional contingencies will involve armed operations against large, fairly modern, conventional forces, most of which are built around large land armies, as is the case in Korea, China-Taiwan, India-Pakistan, and the Persian Gulf.

## Cyber Kritik

### Debate about Cyber Preemption Good

**Debate about the repercussions of cyber preemption is good- key to generating literature on dangers of cyber war, which checks its use**

**Magnuson ‘9**

[Stew, National Defense Magazine. <http://www.nationaldefensemagazine.org/archive/2009/June/Pages/USPlanstoDestroyEnemyComputerNetworksQuestioned.aspx> ETB]

¶ Retired Adm. William **Owen**, **former vice chairman of the Joint Chiefs of Staff,** said he **sees little evidence that there is a government-wide understanding of the repercussions of launching an attack on enemy computers. And that goes for the military as well.**¶¶ “My guess is that most of **the generals and admirals don’t really understand** **what** the hell **we’re** **playing with here** and we need to find a way to get some focused attention” on this topic, he told National Defense.¶ ¶ Owen is the co-author of a National Research Council report, “Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber-Attack Capabilities.”¶ ¶ The study — two-and-a-half years in the making — concludes that **policies and regulations for carrying out computer attacks are “ill-formed, undeveloped and highly uncertain,”** said Kenneth Dam, a former deputy secretary of state who also contributed to the report.¶ ¶ The authors could not identify any single authority in the government responsible for coordinating cyber-attacks or promulgating policy — if there is any policy at all. Further, there are no congressional committees designated to oversee the government’s efforts. ¶ ¶ In short, if the United States government goes on the offense in cyberspace, there may be a lack of accountability, the report concluded.¶ ¶ Secrecy has impeded widespread debate about the nature and implications of cyber-attack, the authors asserted. Much of the defense community’s efforts in this realm are top secret.¶ ¶ “It’s not so much secrecy, it’s actual silence. It just isn’t discussed,” Dam said at a press briefing. **There needs to be a public debate about the repercussions of launching cyber-attacks**, the report said. **In the early days of nuclear weapons, there was a great deal of literature coming out of think tanks, universities and other institutions about when and how to use atomic bombs. That just isn’t happening in this new kind of warfare**, Dam added.

### Worst Case Cyber Planning Good

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

**Clarke and Knake ‘10**

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

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

**A2 China Cyber War Link**

#### Escalations of a US-China cyberwar is unlikely, but the magnitude means the scenario warrant consideration

**Mazanec ‘9**

[Brian M. Mazanec is a senior intelligence analyst at SRA International who has supported various agencies within the Intelligence Community, the Joint Staff, the Office of the Secretary of Defense, the Defense Threat Reduction Agency, and the Department of Homeland Security. The Journal of International Security Affairs #16. <http://www.securityaffairs.org/issues/2009/16/mazanec.php> ETB]

The most severe application of PRC cyberwarfare would, for obvious reasons, occur in the context of an unlimited total war with the U.S. Such a conflict would witness the full display of all PLA capabilities, both conventional and asymmetric, and potentially even nuclear.¶ It should be noted, however, that such a scenario is exceedingly unlikely. According to the U.S.-China Economic and Security Review Commission, PRC leaders believe future wars “will be limited in geographical scope, duration, and political objectives, and will be highly dependent on command, control, communications, and computer (C4) systems.”[18](http://www.securityaffairs.org/issues/2009/16/mazanec.php#footnotes) Yet the catastrophic effects of such a confrontation suggest that, however remote, the scenario warrants examination.

**A2- “Cyber War” K**

**Keeping the metaphor of cyber war alive is key to recognizing its deceptive potential**

**Rid ‘13**

[Dr Thomas Rid is a Reader in War Studies at King's College London., International Studies Today, April/May 2013. <http://www.bisa.ac.uk/files/Permanent%20Files/IST%20AprilMay%202013.pdf>

**Metaphors and analogies,** philosophers ¶ of language know**, may die.** They die ¶ through extensive, repetitive, and ¶ widespread use in a new con-text. ¶ Once a metaphor is dead, we no longer ¶ recognize it as such, as in ‘firewall’, ¶ ‘Trojan’, or indeed ‘pilot,’ an expression ¶ that has been used to mean guiding or ¶ steering a boat since the 1500s. Language ¶ becomes richer as metaphors wither. **But once analogies are dead, recognizing their deceptive potential also becomes more difficult. It is,** therefore, **in our keen interest to keep some metaphors alive - long live ‘cyber war’.**

### Cyber War Probable

**Cyberwar is probable- multiple IR theories prove**

**Junio ‘13**

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

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

### Cyber Threats Real

**Cyber threats are real – they facilitate dangerous armed social movements**

**Deibert and Rohozinski 2010**

(Ronald J, professor of Political Science and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto, and Rafal, Canadian expert and practitioner active in the fields of information security, cyber warfare, and the globalization of armed violence at the University of Toronto, 2010, International Studies Association, “Risking Security: Policies and Paradoxes of Cyberspace Security,” International Political Sociology, vol. 4, p. 22, BS)

Even among democratic states, **the explosion of civic networks has presented serious challenges**, though of a slightly different nature. **Just as progressive and social justice groups have made use of the Internet to advance global norms, so too have a wide variety of militant groups, extremists, criminal organizations, and terrorists to serve more ulterior purposes. Cyberspace has facilitated their activities** in much the same way as it has for more benign civil society networks that often get more attention, but **the aims of these groups are often criminal, covert, and sometimes violent. We call these risks through the network dark nets**, of which there are two different sorts (Deibert and Rohozinski 2008). **The most well known of the dark nets are armed social movements, which can represent a multiplicity of local causes, but whose ability to share tactics, contacts, and at times, drink from the same ideological well, make them appear as a uniﬁed global network. In the post-9/11 era, Al Qaeda and the Jihad movements/// represent the most visible manifestation of this kind of armed social movement. However, they are by no means the ﬁrst and only networks of this kind.** Many of the ‘‘new wars’’ (as Mary Kaldor calls them) that occurred during the 1990s were fought essentially as transnational civil wars where participants pursued both guerilla and conventional warfare against government and rival groups (Kaldor 1999). **In conﬂicts that included Sri Lanka, Somalia, former Yugoslavia, West Africa and Chechnya, ‘‘new wars’’ demonstrated that armed social movements are capable of challenging and at times defeating state actors without the need of state-based patrons or backers. More importantly, this new generation of armed social actors has also increasingly embraced cyberspace** (Rohozinski 2004). **They recognize the capacity afforded by cyberspace to ‘‘effect’’ both their supporters and opponents**. Signiﬁcantly, it was these groups, rather than militaries of the First World War, that were the ﬁrst to leverage cyberspace as means to wage information operations redeﬁning the main battleﬁeld away from the military and towards the political sphere (Weimann 2006b). **Beginning with the ﬁrst Chechen war, the video taping of attacks on the Russian military became more important than the military signiﬁcance of the attacks themselves.** When shown to supporters, as well as the Russian public (via rebroadcast in Russian television, and later on the Internet) their shock value was enough to convey the impression that the Russian military was being defeated. Similar tactics were adopted and further reﬁned by Hezbollah in its resistance against Israeli occupation of Southern Lebanon prior to their withdrawal in 2001, and again in the 2006 summer war. Attacks were documented and produced in the form of music videos, that were both broadcast across Hezbollah’s terrestrial TV station, (al Manar) as well as made available for download from a website, the movement established as part of its strategic communications and information warfare strategy (Pahlavi 2007; Wehrey 2002). **These video shorts proved highly effective**, and have since undergone several signiﬁcant evolutions, paralleling the spread and popularity of such on-line resources as YouTube and Twitter that are used by ‘‘civil’’ networks. **They are now one of the key instruments used by these movements to attract interest in their causes and are a signiﬁcant feature of the more than 4,500+ active jihad websites, chat rooms, and forums** (Weimann 2006a; Kimmage 2008). As the resources necessary for producing multimedia technologies continue to fall, and access to inexpensive digital cameras and computers increases, the threshold and number of video and other multimedia products in circulation has grown exponentially, while the age of the producers has declined. During the early months of the second Intifada, for example, several of the more compelling PowerPoint slides circulating on the Internet depicting the brutality of the Israeli reoccupation of the West bank were produced by a 14-year-old living in a refugee camp in Lebanon.

# 1AR

### CP

#### 1. Yes Restrictions Solve

#### A. Dycus evidence says that abdication on the part of Congress is what is allowing the president to define his terms – only the plan reverses that.

#### B. Hansen and Friedman evidence says that the president will stop if we take a stand NOW, but continued abdication will make it impossible in the future

#### 2. 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.**

### 1AR Intrinsicness

#### Here’s evidentiary support

Lee 9-9

(ESTHER YU-HSI LEE, immigration Reporter/Blogger for ThinkProgress, “House Republicans Stall On Immigration Reform, Blaming Other Priorities” SEPTEMBER 9, 2013, <http://thinkprogress.org/immigration/2013/09/09/2588011/immigration-reform-burner/>, KB)

As much as House Republicans are aiming to push immigration reform off the slate for another year, there is no clear reason as to why reform cannot be taken up simultaneously with any of the other issues. House Judiciary Committee Chairman Bob Goodlatte (R-VA), who has called the 2010 DREAM Act “unfair” and “ripe for fraud,” recently called the Senate immigration bill, “unconstitutional” and would allow “dangerous criminals to be released back onto our streets.”

### Plan Popular

#### We’re bipart

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).

### Uniqe

#### PC fails on CIR – Obama has zero relationship with House Republicans

Linda Feldmann, 10/16/2013 (staff writer, “Debt limit deal: Obama may have won, but victory is hardly lasting,” <http://www.csmonitor.com/USA/Politics/2013/1016/Debt-limit-deal-Obama-may-have-won-but-victory-is-hardly-lasting>, Accessed 10/16/2013, rwg)

And yet Obama is talking as if he can pick up with his domestic policy agenda without skipping a beat. On Tuesday, he told a Spanish-language TV station in Los Angeles that he plans to renew his push for comprehensive immigration reform.¶ Once the fiscal crisis has been resolved, he said, “the day after I’m going to be pushing to say, call a vote on immigration reform."¶ That hardly seems credible, given Obama’s barely existent relationship with congressional Republicans, says Steven Schier, a political scientist at Carleton College in Northfield, Minn.¶ “You have to build confidence through negotiations and ongoing relations over time,” he says. “I don’t see how this current crisis helped him build any relations that will move other legislative priorities forward.”

#### Obama is NOT exerting PC and it fails

Konrad Yakabuski 10/31 is a columnist @ Globe and Mail, “How Obama became a ‘bystander’ president,” 10-31-13, http://www.theglobeandmail.com/commentary/from-dreamy-infatuation-to-bystander-president/article15167598/How Obama became a ‘bystander’ president, DOA: 11-1-13, y2k

Remember Obama Girl, the bikini-clad ingénue who lit up YouTube in 2007 by announcing her crush on the future president? She’s been replaced in the popular consciousness by Obamacare Girl, the anonymous face of Barack Obama’s troubled health-care reform. Her smiling mug dominated the homepage of Obamacare’s still malfunctioning website until her picture was removed this week, proving that the site’s operators could at least do one thing right. The journey from Obama Girl to Obamacare Girl, from infatuation with the dreamy Mr. Right to alternating exasperation and boredom with Mr. Righteous, is a sad story of betrayal. Candidate Obama was the star of one of the most brilliant election campaigns in U.S. history, a modern John Kennedy who would erase the country’s red-blue and black-white cleavages by sheer force of personality. But President Obama is an insular leader who, at home and abroad, alienates the people he needs to persuade to get things done. Fresh from his apparent (and rare) victory over the Tea Party Republicans who forced this month’s government shutdown, Mr. Obama should be riding high, using his replenished political capital to move forward on immigration and budget reform and asserting the U.S. role in world affairs. Instead, even The New York Times fears he has become a “bystander” president. It was bad enough that Vladimir Putin hoisted him on his own petard over Mr. Obama’s on-again off-again plan to strike President Bashar al-Assad’s forces in Syria. Mr. Putin’s humiliating outmanoeuvring of Mr. Obama, which yielded a deal to destroy the Syrian regime’s chemical weapons stash, may be for the better. But it exposed Mr. Obama’s confused foreign policy. He avoided the Syrian issue as long as he could and only improvised his way out when cornered. No wonder Forbes just named Mr. Putin as the world’s most powerful person, bumping Mr. Obama from top spot.