# 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, cyber attacks risk 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.

#### And independently, cyber preemption escalates to shooting war

Clarke 2009

(Richard Clarke, special adviser to the president for cybersecurity in the George W. Bush administration and chairman of Good Harbor Consulting, November/December 2009, “War from Cyberspace,” The National Interest, <http://web.clas.ufl.edu/users/zselden/coursereading2011/Clarkecyber.pdf>)

As in the 1960s, **the speed of war is rapidly accelerating.** Then, long-range ¶ ¶ missiles could launch from the prairie of ¶ ¶ Wyoming and hit Moscow in only thirtyfive minutes. Strikes in cyber war move at ¶ ¶ a rate approaching the speed of light. And ¶ ¶ **this speed favors a strategy of preemption, which means the chances that people can become trigger-happy are high.** **This**, in ¶ ¶ turn, **makes cyber war all the more likely.** ¶ ¶ If a cyber-war commander does not attack quickly, his network may be destroyed first. **If a commander does not preempt an enemy, he may find that the target nation has suddenly raised new defenses or even disconnected from the worldwide Internet.** ¶ ¶ There seems to be a premium in cyber war ¶ ¶ to making the first move.¶ ¶ And much as in the nuclear era, **there is a real risk of escalation with cyber war.** ¶ ¶ Nuclear war was generally believed to be ¶ ¶ something that might quickly grow out of ¶ ¶ conventional combat, perhaps initiated with ¶ ¶ tanks firing at each other in a divided Berlin. The speed of new technologies created ¶ ¶ enormous risks for crisis instability and miscalculation. Today, **the risks of miscalculation are even higher, enhancing the chances that what begins as a battle of computer programs ends in a shooting war.** Cyber ¶ ¶ war, with its low risks to the cyber warriors, ¶ ¶ may be seen by a decision maker as a way ¶ ¶ of sending a signal, making a point without ¶ ¶ actually shooting. An attacker would likely ¶ ¶ think of a cyber offensive that knocked out ¶ ¶ an electric-power grid and even destroyed ¶ ¶ some of the grid’s key components (keeping ¶ ¶ the system down for weeks), as a somewhat ¶ ¶ antiseptic move; a way to keep tensions ¶ ¶ as low as possible. But **for the millions of people thrown into the dark** and perhaps ¶ ¶ the cold, unable to get food, without access ¶ ¶ to cash and dealing with social disorder, ¶ ¶ **it would be in many ways the same as if bombs had been dropped on their cities. Thus, the nation attacked might well respond with “kinetic activity.”**

#### Cyberwar escalates:

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

Clarke and Knake ‘12

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

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

#### b) Pressure to retaliate

Owens et al 9

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

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

#### C) Signaling failures

Mulvenon et al. 10

[Edited by Dr. James C. Mulvenon and ¶ Dr. Gregory J. Rattray ¶ Authors: Matt Devost, Maeve Dion, Jason Healey, ¶ Bob Gourley, Samuel Liles, James C. Mulvenon, Hannah Pitts, Gregory J. Rattray. Addressing Cyber Instability. Cyber Conflict Studies Association. ETB]

**Signaling**, whether **prior to the initiation of conflict** or during its ¶ various escalatory and de-escalatory phases, **is critical to understanding the dynamics of strategic conflict**. In the nuclear era, ¶ Schelling argued: ¶ ...violence is most successful when held in reserve and ¶ made contingent upon the adversary’s behavior. Nuclear ¶ diplomacy is the manipulation of latent violence – ¶ violence that can be withheld or inflicted in the future. It ¶ is also understood, however, that the power to hurt and the credibility of threats to do so may be communicated ¶ by some actual violence.60¶ Most nuclear strategists concentrated their attention on ¶ signaling of intent below the nuclear threshold, primarily through ¶ words or conventional forces. Here again Jervis’ work on ¶ perception and misperception as well as Mearsheimer’s work on ¶ conventional deterrence are dispositive.61 Edgier strategists, such ¶ as Herman Kahn, believed that intra-nuclear war was not only ¶ possible but desirable, and laid out highly detailed escalation ¶ control theories based on the ability to communicate to the ¶ adversary with both words and weapons at every stage of nuclear ¶ conflict. ¶ **While signaling in nuclear conflict was hardly easy, cyber conflict contains additional complexities. On the level of deterrence** ¶ **signaling, Libicki identifies “three sources of confusion”: (1)** ¶ **attribution; (2) BDA** [battle damage assessment], **and (3) third-party** ¶ **interference**.62 The first and last of these have been touched on ¶ earlier in this chapter, and BDA is discussed below in the sections ¶ on “uncertainty” and “repeatability” of cyber-based effects. For his ¶ part, Libicki recommends full disclosure of cyber attack, at least to ¶ bolster the credibility of retaliation. For once, Schelling supports ¶ Libicki when the former argues: ¶ In the case of a planned, deliberate, surprise attack, the ¶ aggressor has every reason to disguise the truth. But in ¶ the case of ‘inadvertent war,’ both sides have a strong ¶ interest in conveying the truth if the truth can in fact be ¶ conveyed in a believable way in time to prevent the ¶ other side’s mistaken decision.63¶ Yet this view is strongly contested by those unwilling to ¶ sacrifice sources and methods for a single iterative move in a ¶ longer game.64 ¶ **Perhaps the more interesting signaling issue is cyber’s** ¶ **possible use as sub-nuclear signaling. Cyber**, for example, **could be** ¶ **used as a vector to establish the credibility of future violence**. ¶ **However, the plausible deniability of cyber attacks cuts both ways** ¶ **in this situatio**n. On the positive side a cyber signal could ¶ communicate the credible threat of escalatory violence, but the ¶ deniability could give the adversary necessary relief from an ¶ automatic or mechanistic escalatory response. On the negative ¶ side, **a deniable cyber signal could simply complicate the signaling by introducing more ambiguity about the attacker’s identity,** ¶ **intentions, and thresholds.** Indeed, it is difficult to distinguish ¶ between cyber attacks meant to influence decisions and cyber ¶ attacks geared to limit the victims’ options for retaliation. **Worse yet, a cyber signaling attack could unintentionally damage** ¶ **communications infrastructure and therefore undermine its very utility as a means to signal**. Finally, **cyber signaling runs into major** ¶ **problems with respect to adversaries with underdeveloped cyber** ¶ **capabilities or those who use cyber proxies, since the target of the** ¶ **signal may be too unintelligent to comprehend it or too weak to enforce his will on those he represents.**65 Perversely, **the important** ¶ **role of these wild-card proxies**, such as those pro-Russian hackers ¶ who were allegedly involved in the 2007 Estonia attacks and the ¶ 2008 Georgia attacks, **may in fact lend more credence to** ¶ **Schelling’s notion of the “threat that leaves something to chance,”** ¶ **which requires participants to credibly communicate threats in** ¶ **which “the final decision is not altogether under the control of the** ¶ **entity making the threat**.”66

### Adv 2: Alliances

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

Dunlap 12

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

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

Lord et al 11

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

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

Government at Harvard University. Mike McConnell is Executive Vice President of Booz Allen Hamilton and former Director of National Intelligence and Director of the National Security Agency. Gary McGraw is Chief Technology Officer of Cigital, Inc., a software security consultancy, and author of eight books on software security. Nathaniel Fick is Chief Executive Officer of the Center for a New American Security. Thomas G. Mahnken is Jerome E. Levy Chair of Economic Geography and National Security at the U.S. Naval War College and a Visiting Scholar at the Johns Hopkins School of Advanced International Studies. Gregory J. Rattray is a Partner at Delta Risk LLC and Senior Vice President for Security at BITS, the technology policy division of The Financial Services Roundtable. Jason Healey is Director of the Cyber Statecraft Initiative at the Atlantic Council and Executive Director of the Cyber Conflict Studies Association. Martha Finnemore is Professor of Political Science and International Affairs at The George Washington University. David A. Gross is a Partner at Wiley Rein LLP and a former Ambassador and Coordinator for International Communications and Information Policy at the State Department. Nova J. Daly is a Public Policy Consultant at Wiley Rein LLP and former Deputy Assistant Secretary for Investment Security in the Office of International Affairs at the Treasury Department. M. Ethan Lucarelli is an Associate at Wiley Rein LLP. Roger H. Miksad is an Associate at Wiley Rein LLP. James A. Lewis is a Senior Fellow and Director of the Technology and Public Policy Program at the Center for Strategic and International Studies. Richard Fontaine is a Senior Fellow at the Center for a New American Security. Will Rogers is a Research Associate at the Center for a New American Security. Christopher M. Schroeder is an Internet entrepreneur, Chief Executive Officer of HealthCentral.com and a member of the Center for a New American Security’s board of advisors. Daniel E. Geer, Jr. is Chief Information Security Officer of In-Q-Tel, the independent investment firm that identifies innovative technologies in support of the missions of the U.S. intelligence community. Robert E. Kahn is President and Chief Executive Officer of the Corporation for National Research Initiatives and co-inventor of the TCP/IP protocol that is the foundation of the modern Internet. Peter Schwartz is Co-Founder and Chairman of Global Business Network and a member of the Center for a New American Security’s board of directors, “America’s Cyber Future Security and Prosperity in the Information Age volume I” June 2011, [http:// www.cnas.org/files/documents/publications/CNAS\_Cyber\_Volume%20I\_0.pdf](http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20I_0.pdf))

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

#### Squo offensive cyber doctrine creates a credibility gap that contributes to a perception of US weakness and undermines credibility

Lawson ‘10

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

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

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

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

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

#### Coalition building key to solve extinction – 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

Lee 10

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

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

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

Kazianis 12

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

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

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

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

RTT 13

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

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

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

Yoshihara 10

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

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

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

Colby et al 13

Elbridgc A. Colby. cochair, is a principal analyst and drvison lead for global strategic affairs at the Center for Naval Analyses (CNA). where he focuses on strategy 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.**

#### Their defense doesn’t apply

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

VornDick 7/30/12

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

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

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

Dobbins et al. ‘11

[Ambassador James F. Dobbins, a veteran diplomat and the current director of the RAND International Security and Defense Policy Center as well the US special representative for Afghanistan and Pakistan. David C. Gompert was Principal Deputy Director of National Intelligence from 2009 to 2010. During 2010, he served as Acting Director of National Intelligence, in which capacity he provided strategic oversight of the U.S. Intelligence Community, and acted as the President's chief intelligence advisor. Gompert is currently Distinguished Visiting Professor for National Security Studies at the United States Naval Academy, and Adjunct Senior Fellow of the RAND Corporation. He is a Trustee of Hopkins House Academy, a Director of the Rufus Porter Museum, a Director of Global Integrated Security (USA), Inc., a member of the Advisory Board of the Naval Academy Center for Cyber Security Studies, and Chairman of the Advisory Board of the Institute for the Study of Early Childhood Education. David A. Shlapak, Senior International Policy Analyst @ RAND. Andrew Scobell is a senior political scientist at the RAND Corporation. Prior to this he was an associate professor of international affairs at the George H. W. Bush School of Government and Public Service (with tenure) and director of the China certificate program at Texas A&M University in College Station, Texas. From 1999 until 2007, he was associate research professor in the Strategic Studies Institute at the U.S. Army War College and adjunct professor of political science at Dickinson College. <http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP344.pdf> ETB]

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

### 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

#### The plan solves –

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

Bradbury 11

Assistant Attorney General for the Office of Legal Counsel

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

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

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

Goldsmith 10

, Professor of Law at Harvard, Can we stop the Cyber Arms Race, Jack Goldsmith teaches at Harvard Law School and is on the Hoover Institution's Task Force on National Security and Law. He was a member of a 2009 National Academies committee that issued the report "[Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities](http://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 — Congressionally initiated restriction is necessary to reverse the signal of independent presidential authority— now is key

Dycus 10

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

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

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

Bastby 12

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

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

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

Hansen & Friedman 9

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

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

# 2AC

### Arms Races

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

**Ballenstedt 10-2**

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

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

**Air gapping empirically fails**

**Cobos ‘12**

[Major Mark A. Cobos, United States Army, School of Advanced Military Studies

United States Army Command and General Staff College Fort Leavenworth, Kansas. “Nodes and Codes: The Reality of Cyber Warfare.” ETB]

In the fall of 2010, at the same time the Symantec Trio and Ralph Langner described Stuxnet’s systematic progress from infected flash drive to centrifuge destruction in the blogosphere, William **Lynn** published an eye-opening article in *Foreign Affairs* entitled “Defending a New Domain.” The Deputy US Secretary of Defense **opened** the article **by describing a previously classified incident in which a flash drive infected with malicious code established a “digital beachhead” on a US military laptop** in the Middle East **that it used to send data from classified military networks to servers under foreign control. Lynn emphasized the vulnerability of data in supposedly secure networks that utilize an “air gap,” physically separating secure and unsecure networks like the public internet. The article’s timing, discussion of infection methods, and revelation of an attack on an “air gapped” US network echoed the Stuxnet themes concurrently debated** in the Symantec and Langner blogs. Lynn concluded the article by declaring.

### Adv 2

**Independently, US-China cyber war collapses the economy and halts US-Sino cooperation on Iran and North Korea**

**Dobbins et al. ‘11**

[Ambassador James F. Dobbins, a veteran diplomat and the current director of the RAND International Security and Defense Policy Center as well the US special representative for Afghanistan and Pakistan. David C. Gompert was Principal Deputy Director of National Intelligence from 2009 to 2010. During 2010, he served as Acting Director of National Intelligence, in which capacity he provided strategic oversight of the U.S. Intelligence Community, and acted as the President's chief intelligence advisor. Gompert is currently Distinguished Visiting Professor for National Security Studies at the United States Naval Academy, and Adjunct Senior Fellow of the RAND Corporation. He is a Trustee of Hopkins House Academy, a Director of the Rufus Porter Museum, a Director of Global Integrated Security (USA), Inc., a member of the Advisory Board of the Naval Academy Center for Cyber Security Studies, and Chairman of the Advisory Board of the Institute for the Study of Early Childhood Education. David A. Shlapak, Senior International Policy Analyst @ RAND. Andrew Scobell is a senior political scientist at the RAND Corporation. Prior to this he was an associate professor of international affairs at the George H. W. Bush School of Government and Public Service (with tenure) and director of the China certificate program at Texas A&M University in College Station, Texas. From 1999 until 2007, he was associate research professor in the Strategic Studies Institute at the U.S. Army War College and adjunct professor of political science at Dickinson College. <http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP344.pdf> ETB]

Having conducted repeated intrusions into U.S. networks to exfiltrate sensitive data ¶ without U.S. reprisal, the People’s Liberation Army (PLA) might seek and receive authority ¶ to interfere with U.S. intelligence collection and dissemination on Chinese strategic-nuclear ¶ programs. Chinese civilian leaders might not grasp that such operations would be defined ¶ as cyber-attack by the United States and thus lead to retaliation. The attack could disrupt ¶ systems the United States relies on for critical intelligence, including warning. If confident ¶ that the PLA was the attacker, the United States might decide to retaliate. Given that corresponding PLA intelligence networks are not easily accessed, and choosing to signal dangers of ¶ escalation, the United States might retaliate against networks that support Chinese transport ¶ systems, including commercial shipping as well as military logistics. The impact on Chinese ¶ trade could be immediate. In addition, because the U.S. ability to observe Chinese forces had ¶ been impaired, Pacific Command (PACOM) might be told to increase the readiness of its ¶ forces. While **China** does not want armed conflict, it **could respond by conducting “soft-kill”** ¶ **attacks** (e.g., link interference) **on U.S. satellites** **that serve** the Pacific **command, control**, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) grid, to which ¶ the United States responds in kind. Because both Chinese and U.S. network defenses are of ¶ limited value against such large and sophisticated attacks, **both sides might resort to counterattacks** in hopes of restoring deterrence. ¶ **In the ensuing escalation, both China and the U**nited **St**ates **could suffer** temporary but ¶ **major disruptions of critical networks, precipitating shocks in stock, currency, credit, and trade** ¶ **markets**. Although both sides avoid escalation to armed force, **economic damage would be** ¶ **considerable**. **Sino-U.S. cooperation on Iran would likely come to a halt, and the situation in** ¶ **Korea could heat up.** There are no lives lost—just extensive harm, heightened antagonism, and ¶ loss of confidence in network security. There would be no “winner.”

**Economic collapse causes nuclear conflicts**

**Burrows and Harris 9**

Mathew J. Burrows counselor in the National Intelligence Council and Jennifer Harris a member of the NIC’s Long Range Analysis Unit “Revisiting the Future: Geopolitical Effects of the Financial Crisis” The Washington Quarterly 32:2 https://csis.org/files/publication/twq09aprilburrowsharris.pdf

Increased Potential for Global Conflict¶ Of course, the report encompasses more than economics and indeed believes the¶ future is likely to be the result of a number of intersecting and interlocking¶ forces. With so many possible permutations of outcomes, each with ample opportunity for unintended consequences, there is a growing sense of insecurity.¶ Even so, history may be more instructive than ever. **While we continue to¶ believe that the Great Depression is not likely to be repeated, the lessons to be¶ drawn from that period include the harmful effects on fledgling democracies and¶ multiethnic societies** (think Central Europe in 1920s and 1930s) **and** on¶ the sustainability of **multilateral institutions** (think League of Nations in the¶ same period). **There is no reason to think that this would not be true in the¶ twenty-first as much as in the twentieth century. For that reason, the ways in¶ which the potential for greater conflict could grow would seem to be even more¶ apt in a constantly volatile economic environment** as they would be if change¶ would be steadier.¶ In surveying those risks, the report stressed the likelihood that terrorism and¶ nonproliferation will remain priorities even as resource issues move up on the¶ international agenda. **Terrorism’s appeal will decline if economic growth¶ continues** in the Middle East and youth unemployment is reduced. For those¶ terrorist groups that remain active in 2025, however, the diffusion of¶ technologies and scientific knowledge will place some of the world’s most¶ dangerous capabilities within their reach. Terrorist groups in 2025 will likely be a¶ combination of descendants of long established groupsinheriting¶ organizational structures, command and control processes, and training¶ procedures necessary to conduct sophisticated attacksand newly emergent¶ collections of the angry and disenfranchised that become self-radicalized,¶ particularly in the absence of economic outlets that would become narrower¶ in an economic downturn.¶ **The most dangerous casualty of any economically-induced drawdown of U.S.¶ military presence would almost certainly be the Middle East.** Although Iran’s¶ acquisition of nuclear weapons is not inevitable, **worries about a nuclear-armed¶ Iran could lead states in the region to develop new security arrangements with¶ external powers, acquire additional weapons, and consider pursuing their own¶ nuclear ambitions.** It is not clear that the type of stable deterrent relationship¶ that existed between the great powers for most of the Cold War would emerge¶ naturally in the Middle East with a nuclear Iran. **Episodes of low intensity¶ conflict and terrorism taking place under a nuclear umbrella could lead to an¶ unintended escalation and broader conflict** if clear red lines between those states¶ involved are not well established. The close proximity of potential nuclear rivals¶ combined with underdeveloped surveillance capabilities and mobile¶ dual-capable Iranian missile systems also will produce inherent difficulties in¶ achieving reliable indications and warning of an impending nuclear attack. **The¶ lack of strategic depth in neighboring states like Israel, short warning and missile¶ flight times, and uncertainty of Iranian intentions may place more focus on¶ preemption rather than defense**, potentially leading to escalating crises.**Types of conflict that the world continues¶ to experience, such as over resources, could¶ reemerge, particularly if protectionism grows and¶ there is a resort to neo-mercantilist practices.**¶ Perceptions of renewed energy scarcity will drive¶ countries to take actions to assure their future¶ access to energy supplies. In the worst case, **this¶ could result in interstate conflicts** if government¶ leaders deem assured access to energy resources,¶ for example, to be essential for maintaining domestic stability and the survival of¶ their regime. Even actions short of war, however, will have important geopolitical¶ implications. Maritime security concerns are providing a rationale for naval¶ buildups and modernization efforts, such as China’s and India’s development of¶ blue water naval capabilities. **If** the **fiscal** **stimulus** focus for these countries indeed¶ **turns inward,** one of **the most obvious funding targets may be military**. **Buildup** of¶ regional naval capabilities **could lead to increased tensions**, rivalries, and**¶ counterbalancing** moves, but it also will create opportunities for multinational¶ cooperation in protecting critical sea lanes. With water also becoming scarcer in¶ Asia and the Middle East, **cooperation** to manage changing water resources **is**¶ likely to be increasingly **difficult** both within and between states **in a** more¶ **dog-eat-dog world**.¶

**US-China co-op key to solve Iranian prolif**

**Tisdall ‘05**

Simon Tisdall, World Briefing Columnist, The Guardian (London), September 21, 2005

**North Korea's** unexpected **pledge** this week **to abandon its nuclear weapons appears to be the result of a** highly unusual **diplomatic pincer movement by the US and China.** The manoeuvre **has potentially positive implications for resolving the nuclear stalemate with** another so-called axis of evil state, **Iran**. **The deal** forged at the six-party talks hosted by China in Beijing remains highly fragile, as yesterday's renewed demands from Pyongyang show. But if made to stick, diplomats believe that it **may come to be seen as a landmark in Sino-US strategic security cooperation and a paradigm for ending the west's dispute with Tehran.** After two years of fruitless talks, the turning point seems to have come not in Beijing but in New York, at a private meeting last week at the UN between George Bush and the Chinese leader, Hu Jintao. The US president is said to have warned his counterpart that in the absence of progress, the US may step up pressure on North Korea's weak and inherently unstable regime - with unpredictable consequences. "If the talks had failed again, it would have harmed China's credibility," said an Asian diplomat familiar with the Beijing talks. But China had more powerful motives, too. As its economy and international standing have grown, its broader interests in solving the dispute have increasingly fallen into line with Washington's. "China has its own security and economic concerns. It sees North Korea as a destabilising factor in the region. It wants to keep it as a buffer state, to keep the status quo. It doesn't want the Korean peninsula to be nuclearised or destroyed," the diplomat said. Beijing also feared Pyongyang's nuclear arms could lead its regional ri val, Japan, and South Korea to acquire similar weapons while encouraging a heightened US military presence. The US decision to offer security guarantees, aid and technology to North Korea, having long refused to do so, also reflects a more consensual perspective in Washington. That change is attributed in part to Condoleezza Rice's appointment as America's top diplomat and the reassignment to the UN of John Bolton, the former arms control chief whose abrasive style antagonised Pyongyang. But **preoccupations with Iraq**, growing worries about **Iran**, plus Japanese and South Korean concerns about escalation have also **helped persuade the White House that** China's insistence on **engagement, rather than confrontation, may best serve its interests**. The US eschewed bilateral contacts after the 2002 rupture that led North Korea to quit the nuclear non-proliferation treaty. Now its chief negotiator, Christopher Hill,hailing the deal as a "turning point", may visit Pyongyang. The contradictions between this new US approach and its policy towards Iran may become increasingly difficult to justify internationally. Mohamed ElBaradei, the UN nuclear agency chief, made the comparison this week while warning against American (and Iranian) "brinkmanship". Iranian officials say privately that Washington's refusal to meet bilaterally, indirect threats of military coercion, and economic sanctions all hinder progress on the nuclear issue. Beijing seems to agree. With its UN veto in its pocket, it has opposed punitive measures against Iran, an important oil and gas exporter, while insisting engagement is the best path forward. Ironically, **it may be China, Washington's** new-found **"strategic partner"** in the east, **which** also **holds the key to the west's Iranian impasse.**

**Iran nuclearization causes extinction**

**Rosenbaum ‘12**

<http://www.slate.com/articles/news_and_politics/the_spectator/2012/03/nuclear_war_in_iran_six_questions_to_consider_about_whether_and_how_it_might_happen_.single.html>

A. Recently I was at a dinner with a writer who had just interviewed Obama. And when I asked him this question, he said he was absolutely convinced that Obama would be willing to order a strike. But not because of Israel. Or the Israel lobby. Rather, because of his longtime grounding in the thinking of the anti-nuclear proliferation movement.¶ It sounds unlikely at first, but it makes a certain kind of sense: Obama wrote a seminar paper at Columbia about the nuclear freeze movement, after all. He probably won the Nobel Prize because of his speech calling for the abolition of all nuclear weapons (remember that?) and, this reporter suspects, he believes that **Iranian possession of a nuclear weapon will mean a Middle East arms race. Saudi Arabia, Turkey, Sudan, Egypt, even the Emirates will want them, while Israel already has a couple hundred nuclear warheads, and Pakistan around a hundred. Sooner or later, this proliferating arms race will lead to regional (or even global) nuclear war**.¶ I still can’t decide if I can visualize Obama ordering a reluctant military to start another war for the sake of nonproliferation. It sounds counterintuitive, does it not, but it now seems that Iranian nuclear capability to build a bomb—not even the actual "breakout" race to assemble it—is a "red line” for the president. Maybe the attack he's alluding to with his "all options are on the table" rhetoric will start and end such a war. I've come to the tragic conclusion that the world will not really move to ban nuclear weapons until it gets another taste of their sinister sting, another preview of the Armageddon they promise in the form of a "small" nuclear war. Obama has said he doesn’t want a “temporary” solution—but more likely it would be a war that would never end, in terms of consequences.

**Cooperation over Korea key to check war**

**Xu ‘01**

Xianquan Xu, Senior Research Fellow, Chinese Academy, International Trade and Economic Coop, 2001

(China, the United States, and the Global Economy, Shuxun Chen & Charles Wolf, p. 268)

In terms of security and stability in Northeast Asia, outstanding is North Korea and its nuclear weapon and ballistic missile capabilities. Moreover, North Korea is heavily armed with over one million troops and has also developed other weapons of mass destruction, such as chemical weapons. North Korea's ideological isolation and economic failure heighten the risk for a military miscalculation. Although dialogue and negotiations with North Korea have increased in recent years, **North Korea** in general **remains one of the most uncertain and explosive regimes in the world**. While having much less influence over Pyongyang than most of Kim II Sung's time, **China has been critical in averting a second conflict on the Peninsula**, China explic­itly opposes any military action from the south against the north, and **China still holds the most influence over North Korea in any major crisis**. Therefore, although the United States has been making the most initiatives on security issues with North Korea**, China's support and cooperation remains crucial to any lasting success.** Such joint diplomacy should include resolving questions about Pyongyang's nuclear program, persuading North Korea to halt further missile testing, and coordinating humanitarian relief. As members of the Four Party Talks on Korean security, the United States and China should continue their cooperation in dissuading North Korea from obstructing progress or from bolting from the process altogether. The **talks remain one of the most important channels to diffuse ten­sions** between North and South Korea—**a** near-**term interest that Washington and Beijing share**.

**Goes nuclear**

**Chol, ’02**

(Kim Myong, The Agreed Framework is Brain Dead, <http://www.nautilus.org/fora/security/0212A_Chol.html>)

The second choice is for the Americans to initiate military action to knock out the nuclear facilities in North Korea. Without precise knowledge of the location of those target facilities, **the American policy planners face the real risk of North Korea launching a full-scale war against South Korea, Japan and the U.S. The North Korean retaliation will most likely leave South Korea and Japan totally devastated with the Metropolitan U.S. being consumed in nuclear conflagration**. Looking down on the demolished American homeland, American policy planners aboard a special Boeing jets will have good cause to claim, "We are winners, although our homeland is in ashes. We are safely alive on this jet." The third and last option is to agree to a shotgun wedding with the North Koreans. It means entering into package solution negotiations with the North Koreans, offering to sign a peace treaty to terminate the relations of hostility, establish full diplomatic relations between the two enemy states, withdraw the American forces from South Korea, remove North Korea from the list of axis of evil states and terrorist-sponsoring states, and give North Korea most favored nation treatment. The first two options should be sobering nightmare scenarios for a wise Bush and his policy planners. If they should opt for either of the scenarios, that would be their decision, which the North Koreans are in no position to take issue with. **The Americans would realize too late that the North Korean mean what they say. The North Koreans will use all their resources in their arsenal to fight a full-scale nuclear exchange with the Americans in the last war of** man [human]-**kind. A nuclear-armed North Korea would be most destabilizing in the region and the rest of the world** in the eyes of the Americans. They would end up finding themselves reduced to a second-class nuclear power

### Politics

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

Kaplan 10-3

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

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

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

Todd 10-3

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

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

#### 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).

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

Allen, 9/27

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

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

#### No impact – multiple factors check

FXStreet.com, 9/25

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

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

#### XO solves

Weisenyhal 9/30

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

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

#### No impact to econ decline

Miller 2k

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

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

#### PC is low and decreasing

Steinhauser, 9/26

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

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

### Cy deterrence

**Cyber det low and fails**

**Clarke and Knake ‘10**

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

‘

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

**Non-unique — cyber arms race and use is inevitable now — I did that analysis on case — it’s try or die for a restrained strategy — active defense causes Cyberwar**

**McGraw 12,** Member of the IEEE Computer Society Board of Governors, Gary McGraw is a recognized authority on software security. He is an author of many books and over a 100 [peer-reviewed](http://en.wikipedia.org/wiki/Peer-reviewed) publications in this field, authors a monthly security column for [informIT](http://en.wikipedia.org/wiki/InformIT" \o "InformIT), and is an editor of Addison-Wesley Software Security series. In addition, Gary McGraw serves on the Dean’s Advisory Council for the School of Informatics of Indiana University, and produces the monthly Silver Bullet Security Podcast for IEEE Security & Privacy magazine (syndicated by informIT). Gary is the Chief Technical Officer at [Cigital Inc.](http://en.wikipedia.org/wiki/Cigital" \o "Cigital) In addition, he serves on the advisory boards of several companies, including [Dasient](http://en.wikipedia.org/wiki/Dasient" \o "Dasient), [Fortify Software](http://en.wikipedia.org/wiki/Fortify_Software), Invincea, and Raven White. He holds dual PhD in Cognitive Science and Computer Science from Indiana University. In the past, Gary McGraw has served on the [IEEE Computer Society](http://en.wikipedia.org/wiki/IEEE_Computer_Society) Board of Governors.

Creating a cyber-rock is cheap. Buying a cyber-rock is even cheaper since zero-day attacks exist on the open market for sale to the highest bidder. In fact, if the bad guy is willing to invest time rather than dollars and become an insider, cyber-rocks may in fact be free of charge, but that is a topic for another time. Given these price tags, it is safe to assume that some nations have already developed a collection of cyber-rocks, and that many other nations will develop a handful of specialized cyber-rocks (e.g., as an extension of many-year-old regional conflicts). If we follow the advice of Hayden and Chabinsky, we may even distribute cyber-rocks to private corporations. Obviously, active defense is folly if all it means is unleashing the cyber-rocks from inside of our glass houses since everyone can or will have cyber-rocks. Even worse, unlike very high explosives, or nuclear materials, or other easily trackable munitions (part of whose deterrence value lies in others knowing about them), no one will ever know just how many or what kind of cyber-rocks a particular group actually has. Now that we have established that cyber-offense is relatively easy and can be accomplished on the cheap, we can see why reliance on offense alone is inadvisable. What are we going to do to stop cyberwar from starting in the first place? The good news is that war has both defensive and offensive aspects, and understanding this fundamental dynamic is central to understanding cyberwar and deterrence. The kind of defense I advocate (called "passive defense" or "protection" above) involves security engineering -- building security in as we create our systems, knowing full well that they will be attacked in the future. One of the problems to overcome is that exploits are sexy and engineering is, well, not so sexy.

**Deterrence doesn’t apply to cyberspace**

**Weiner 12, research intern for the Project on Nuclear Issues**, Boss, Internally cites Dr. Lewis who is the director of the Center for Homeland Security and Defense, <https://www.hsdl.org/hslog/?q=node/9216> \*\*Note: Sarah Weiner is Cal debate coach, however this evidence relies upon Dr. Lewis’s findings and was written before the announcement of the topic \*\*

Others vehemently disagree with this presupposition. Jim Lewis, for example, [argued](http://www.stimson.org/about/news/jim-lewis-of-csis-speaks-at-stimson-on-cyber-deterrence/) earlier this month at an event at the Stimson Center that **deterrence will not work in the cyber domain**. He emphasized that difficulties in attributing attacks, “holding hostage” adversaries’ cyber and physical assets, and achieving a proportional response all decrease the credibility of US threats and reduce the costs of an adversaries’ hostile cyber operations. And Dr. Lewis has considerable evidence on his side: public and private entities in the US experience cyber-attacks on a daily basis. If these attacks are deterrable, **we are doing a terrible job** of leveraging our capabilities. For a number of reasons, trying to apply nuclear deterrence logic to cyber warfare feels a bit too much like trying to fit a square peg into a round hole. That does not mean, however, that we should abandon all attempts to draw analogies between cyber and nuclear strategy. Despite a few close calls, the basic principles of nuclear deterrence and mutually assured destruction have prevented the use of nuclear weapons for over 60 years. Understanding the reason why this largely effective and stable model of deterrence cannot map cleanly onto the cyber world may help us better conceptualize strategies for cyber-deterrence. The first difficulty is establishing an analogue between a nuclear attack and a cyber-attack. We know when a nuclear bomb explodes, and we know it is unacceptable. The spectrum of cyber-attacks, however, spans far, far below the destructiveness of a nuclear strike. Denial-of-service attacks, such as Iran’s [recent shutdown](http://online.wsj.com/article/SB10000872396390444657804578052931555576700.html) of several banks’ websites, are a world away from the detonation of any weapon, not to mention a nuclear weapon. This creates the problem of credibility and proportionality Dr. Lewis spoke about: responding to such low-level attacks with a military use of force is so disproportionate that it is not a credible threat. ¶ If the US instead decides to use cyber capabilities to deter cyber-attacks, it runs into a second problem. Cyber “weapons” cannot be used in the same way we use nuclear weapons because, unlike nuclear weapons, the demonstration of a cyber-capability quickly renders that capability useless. If the US were to release the details of a cyber-weapon, intended to signal a retaliatory capability, potential adversaries could attempt to steal the technology and/or harden their cyber defenses against the US weapon’s specific attributes. This is the opposite of nuclear deterrence, in which the US pursues the most credible and reliable force so that other nations know precisely how damaging a US counterstrike would be. Demonstrating that a nation could effectively mount a second-strike in response to a nuclear attack creates a stabilizing dynamic of mutually assured destruction in which no nation believes it could gain militarily by launching a nuclear attack. The trouble with cyber weapons, however, is that they cannot be so transparently deployed. **The only effective cyber-attack is an unexpected attack, and that does nothing for signaling or deterrence.**

#### Massive alt causes to flex

Rozell 12

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

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

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

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

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

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

Waxman ‘11

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

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

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

### CP

**Turn — Miscalc — only the plan solves deterrence failures**

**Lord et al 11, Vice President and Director of Studies at the Center for a New American Security**

(Kristin M., Travis Sharp is the Bacevich Fellow at the Center for a New American Security. Joseph S. Nye, Jr. is University Distinguished Service Professor at the Kennedy School of Government at Harvard University. Mike McConnell is Executive Vice President of Booz Allen Hamilton and former Director of National Intelligence and Director of the National Security Agency. Gary McGraw is Chief Technology Officer of Cigital, Inc., a software security consultancy, and author of eight books on software security. Nathaniel Fick is Chief Executive Officer of the Center for a New American Security. Thomas G. Mahnken is Jerome E. Levy Chair of Economic Geography and National Security at the U.S. Naval War College and a Visiting Scholar at the Johns Hopkins School of Advanced International Studies. Gregory J. Rattray is a Partner at Delta Risk LLC and Senior Vice President for Security at BITS, the technology policy division of The Financial Services Roundtable. Jason Healey is Director of the Cyber Statecraft Initiative at the Atlantic Council and Executive Director of the Cyber Conflict Studies Association. Martha Finnemore is Professor of Political Science and International Affairs at The George Washington University. David A. Gross is a Partner at Wiley Rein LLP and a former Ambassador and Coordinator for International Communications and Information Policy at the State Department. Nova J. Daly is a Public Policy Consultant at Wiley Rein LLP and former Deputy Assistant Secretary for Investment Security in the Office of International Affairs at the Treasury Department. M. Ethan Lucarelli is an Associate at Wiley Rein LLP. Roger H. Miksad is an Associate at Wiley Rein LLP. James A. Lewis is a Senior Fellow and Director of the Technology and Public Policy Program at the Center for Strategic and International Studies. Richard Fontaine is a Senior Fellow at the Center for a New American Security. Will Rogers is a Research Associate at the Center for a New American Security. Christopher M. Schroeder is an Internet entrepreneur, Chief Executive Officer of HealthCentral.com and a member of the Center for a New American Security’s board of advisors. Daniel E. Geer, Jr. is Chief Information Security Officer of In-Q-Tel, the independent investment firm that identifies innovative technologies in support of the missions of the U.S. intelligence community. Robert E. Kahn is President and Chief Executive Officer of the Corporation for National Research Initiatives and co-inventor of the TCP/IP protocol that is the foundation of the modern Internet. Peter Schwartz is Co-Founder and Chairman of Global Business Network and a member of the Center for a New American Security’s board of directors, “America’s Cyber Future Security and Prosperity in the Information Age volume I” June 2011, [http:// www.cnas.org/files/documents/publications/CNAS\_Cyber\_Volume%20I\_0.pdf](http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20I_0.pdf))

The **Department of Defense**, the **intelligence community**, the Department of **Justice, Congress and the White House should** **clarify** legal **authorities** related to military and intelligence operations in cyberspace. GEN Alexander told Congress in March 2011 that the U.S. military does not yet possess the legal authorities it needs to respond to a cyber attack against the United States or its allies.197 LtGen Robert Schmidle, Jr., deputy commander of Cyber Command, elaborated that “**There is a real dearth of doctrine and policy** in the world of cyberspace,” **pointing to the lack of coordination and guidance from civilian leadership**.198 This **lack of clarity is understandable** as cyber operations evolve faster than legal and political processes, but it could **cause confusion and disorganization during a major cyber attack**. By **delineating the authorities granted** to the military, the U.S. government **will reduce uncertainty and** thereby **increase its ability to use the capabilities** it has more effectively and **without undue hesitati**on. This outcome will **raise the retaliatory costs suffered by potential adversaries** if they attack the United States and the attacks can be attributed to them, which **will help deter them in the first place**.

### 2ac- Agamben

#### Life should be valued as apriori – it precedes the ability to value anything else

Amien **Kacou. 2008**. WHY EVEN MIND? On The A Priori Value Of “Life”, Cosmos and History: The Journal of Natural and Social Philosophy, Vol 4, No 1-2 (2008) cosmosandhistory.org/index.php/journal/article/view/92/184

Furthermore, that manner of **finding things good** that is in pleasure **can certainly not exist in any world without consciousness (i.e., without “life,”** as we now understand the word)—slight analogies put aside. In fact, we can begin to develop a more sophisticated definition of the concept of “pleasure,” in the broadest possible sense of the word, as follows: it is the common psychological element in all psychological experience of goodness (be it in joy, admiration, or whatever else). In this sense, pleasure can always be pictured to “mediate” all awareness or perception or judgment of goodness: there is pleasure in all consciousness of things good; pleasure is the common element of all conscious satisfaction. In short, it is simply the very experience of liking things, or the liking of experience, in general. In this sense, **pleasure is, not only uniquely characteristic of life but also, the core expression of goodness in life—the most general sign or phenomenon for favorable conscious valuation**, in other words. This does not mean that “good” is absolutely synonymous with “pleasant”—what we value may well go beyond pleasure. (The fact that we value things needs not be reduced to the experience of liking things.) However, what we value beyond pleasure remains a matter of speculation or theory. Moreover, we note that a variety of things that may seem otherwise unrelated are correlated with pleasure—some more strongly than others. In other words, there are many things the experience of which we like. For example: the admiration of others; sex; or rock-paper-scissors. But, again, what they are is irrelevant in an inquiry on a priori value—what gives us pleasure is a matter for empirical investigation. Thus, we can see now that, in general, **something primitively valuable is attainable in living—that is, pleasure itself.** And it seems equally clear that we have a priori logical reason to pay attention to the world in any world where pleasure exists. Moreover, **we can now also articulate a foundation for a security interest in our life: since the good of pleasure can be found in living** (to the extent pleasure remains attainable),[17] **and only in living, therefore, a priori, life ought to be continuously (and indefinitely) pursued at least for the sake of preserving the possibility of finding that good.** However, this platitude about the value that can be found in life turns out to be, at this point, insufficient for our purposes. It seems to amount to very little more than recognizing that our subjective desire for life in and of itself shows that life has some objective value. For what difference is there between saying, “living is unique in benefiting something I value (namely, my pleasure); therefore, I should desire to go on living,” and saying, “I have a unique desire to go on living; therefore I should have a desire to go on living,” whereas the latter proposition immediately seems senseless? In other words, “life gives me pleasure,” says little more than, “I like life.” Thus, we seem to have arrived at the conclusion that **the fact that we already have some (subjective) desire for life shows life to have some (objective) value.** But, if that is the most we can say, then it seems our enterprise of justification was quite superficial, and the subjective/objective distinction was useless—for all we have really done is highlight the correspondence between value and desire. Perhaps, our inquiry should be a bit more complex.

**Risk framing empowers agency and is key to solve the alt by broadening coalitions AGAINST the state**

**Borraz, ‘7** [OLIVIER BORRAZ Centre de Sociologie des Organisations, Sciences Po-CNRS, Paris, “Risk and Public Problems,” Journal of Risk Research, 10, 7, Oct 2007, 941-957]

First, risk is the result of a dynamic, haphazard, controversial and unstable process of construction. In a sense, risk is never entirely stabilized, it is associated with many uncertainties, its status like its boundaries change, following the dynamics of contention which contributed to its emergence. More than a frame, risk is thus closer to a state in the life of a public problem (Gilbert, 2003b), a state characterized by fluidity in its boundaries, struggles over the definition of the risk, debates as to who is accountable, etc. Labelling a problem as a risk exerts pressure on political authorities, in a way which tests their capacity to act. It is also an opportunity for rules and power relations to be redefined. Generally, the boundary between risk and crisis is unclear (Besanc ̧on et al., 2004). Second, risk is inseparable from wider political controversies and conflicting values, ideas and interests. Whatever the issue, be it limited in scale (sewage sludge or mobile phone masts) or on the contrary high profile (nuclear waste, global warming, asbestos, GMO), the move into the state of risk allows for links to be made with broader political, economic, social, moral, ethical or environmental issues. The risk of an activity is always more than just a health or environmental safety issue: it also questions the multiple dimensions surrounding that activity (its benefits, use, effects, etc.).

**Perm solves and case is a net benefit – only by strategically utilizing biopolitical tools like apocalyptic imagery and policy reform can we resist biopower**

JL **Schatz. 2012**. Professor of English and Feminist Evolutionary Studies & Director of Debate at Binghamton University. The Importance of Apocalypse: The Value of End-Of-The-World Politics While Advancing Ecocriticism. Journal of Ecocriticism: A New Journal of Nature, Society and Literature. 4(2)

Anything is justified in the name of saving the environment because it is a question of our very survival. Here we find the logic of things like resource wars that strive to secure geopolitical interests in order to get others to clean up their acts in the name of environmental security4. **From this perspective the mobilizing potentials of apocalyptic imagery can influence populations for the purposes of war instead of positive ecological awareness.** **This fear causes such critics to refrain from utilizing descriptions of omnicide while simultaneously criticizing the most effective tactic activists on the frontlines have**. Luke and Darier’s Foucauldian approach to ecocriticism is not without value. They demonstrate how “discourse delineate[s] ... the terms of intelligibility whereby a particular ‘reality’ can be known and acted upon. When we speak of a discourse we may be referring to a specific group of texts, but also importantly to the social practices to which those texts are inextricably linked” (Doty, 1996: 6). Power continuously operates in both hegemonic and resistant ways regardless if we are monkey-wrenching, speaking at a political press conference, or using the written language of the academic. No matter the form, the way we articulate our discourse must construct reality in a precise way in order to render it intelligible for others to understand. Judith Butler notes that “the media’s evacuation of the human through the image has to be understood ... in terms of the broader problem that normative schemes of intelligibility establish what will and will not be human” (146)5. Once other animals and the environment are understood as less than human their lives become inconsequential compared to the short-term benefit of human civilization. To this ends—despite Luke and Darier’s fear of being coopted—**apocalyptic imagery can help** in two regards. First, it helps **people recognize the interconnection of the global ecology in order to appreciate the similarity between humans and other species**. Second, **it provides a self-motivating reason for people to change their behavior to avert extinction even when confronting those who refuse to recognize the intrinsic value of non-human animals**. In either case **omnicidal images change** both the **mindset and** the **actions** of those we encounter, thereby fostering new directions for humanity to evolve. **Any hesitancy to deploy images of apocalypse out of the risk of acting in a biopolitical manner ignores how any particular metaphor—apocalyptic or not—always risks getting coopted. It does not excuse inaction. Clearly hegemonic forces have already assumed control of determining environmental practices when one looks at the debates surrounding** offshore **drilling**, **climate change**, **and biodiversity** within the halls of Congress. “As this ideological quagmire worsens, urgent problems ... will go unsolved ... only to fester more ominously into the future. ... [E]cological crisis ... cannot be understood outside the larger social and global context ... of internationalized markets, finance, and communications” (Boggs 774). **If it weren’t for people such as Watson connecting things like whaling to the end of the world it wouldn’t get the needed coverage to enter into public discourse. It takes big news to make headlines and hold attention spans in the electronic age**. Sometimes it even takes a reality TV show on Animal Planet. As Luke reminds us, “Those who dominate the world exploit their positions to their advantage by defining how the world is known. Unless they also face resistance, questioning, and challenge from those who are dominated, they certainly will remain the dominant forces” (2003: 413). **Merely sitting back and theorizing over metaphorical deployments does a grave injustice to the gains activists are making on the ground. It** also **allows hegemonic institutions to continually define the debate over the environment by framing out any attempt for significant change, whether it be radical or reformist**. **Only by jumping on every opportunity for resistance can ecocriticism have the hopes of combatting the current ecological reality.** This means we must recognize that we cannot fully escape the master’s house since the surrounding environment always shapes any form of resistance. Therefore, **we ought to act even if we may get coopted**. As Foucault himself reminds us, “instead of radial ruptures more often one is dealing with mobile and transitory points of resistance, producing cleavages in a society that shift about[.] ... And **it is** doubtless **the strategic codification of these points of resistance that makes a revolution possible**, somewhat similar to the way in which the state relies on the institutional ntegration of power relationships. It is in this sphere of force relations that we must try to analyze the mechanisms of power” (96-­‐97). Here Foucault “asks us to think about resistance differently, as not anterior to power, but a component of it. If we take seriously these notions on the exercise and circulation of power, then we ... open ... up the field of possibility to talk about particular kinds of environmentalism” (Rutherford 296). This is not to say that all actions are resistant. Rather, the revolutionary actions that are truly resistant oftentimes appear mundane since it is more about altering the intelligibility that frames discussions around the environment than any specific policy change. Again, this is why people like Watson use one issue as a jumping off point to talk about wider politics of ecological awareness. Campaigns that look to the government or a single policy but for a moment, and then go on to challenge hegemonic interactions with the environment through other tactics, allows us to codify strategic points of resistance in numerous places at once. Again, this does not mean we must agree with every tactic. It does mean that even failed attempts are meaningful. For example, while PETA’s ad campaigns have drawn criticism for comparing factory farms to the Holocaust, and featuring naked women who’d rather go naked than wear fur, their importance extends beyond the ads alone6. By bringing the issues to the forefront they draw upon known metaphors and reframe the way people talk about animals despite their potentially anti-Semitic and misogynist underpinnings. Michael Hardt and Antonio Negri’s theorization of the multitude serves as an excellent illustration of how **utilizing the power of the master’s biopolitical tools can become powerful enough to deconstruct its house despite the risk of cooptation or backlash**. For them, the multitude is defined by the growing global force of people around the world who are linked together by their common struggles without being formally organized in a hierarchal way. While Hardt and Negri mostly talk about the multitude in relation to global capitalism, their understanding of the commons and analysis of resistance is useful for any ecocritic. They explain, [T]he multitude has matured to such an extent that it is becoming able, through its networks of communication and cooperation ... [and] its production of the common, to sustain an alternative democratic society on its own. ... Revolutionary politics must grasp, in the movement of the multitudes and through the accumulation of common and cooperative decisions, the moment of rupture ... that can create a new world. In the face of the destructive state of exception of biopower, then, there is also a constituent state of exception of democratic biopolitics[,] ... creating ... a new constitutive temporality. (357) Once one understands the world as interconnected—instead of constructed by different nationstates and single environments—conditions in one area of the globe couldn’t be conceptually severed from any other. In short, we’d all have a stake in the global commons. **Ecocritics can then utilize biopolitics to shape discourse and fight against governmental biopower by waking people up to the pressing need to inaugurate a new future for there to be any future. Influencing other people through argument and end-of-the-world tactics is not the same biopower of the state so long as it doesn’t singularize itself but for temporary moments.** Therefore, “it is not unreasonable to hope that in a biopolitical future (after the defeat of biopower) war will no longer be possible, and the intensity of the cooperation and communication among singularities ... will destroy its [very] possibility” (Hardt & Negri 347). In the context of capitalism, when wealth fails to trickle down it would be seen as a problem for the top since it would stand testament to their failure to equitably distribute wealth. In the context of environmentalism, not-in-my-backyard reasoning that displaces ecological destruction elsewhere would be exposed for the failure that it is. There is no backyard that is not one’s own. Ultimately, **images of planetary doom demonstrate how we are all interconnected and** in doing so **inaugurate a new world where multitudes, and not governments, guide the fate of the planet.**

#### Agamben’s use of the concept “bare life” is devoid of historical context to the point of meaninglessness

Thomas **Lemke. 2011**. Former assistant professor of sociology at Wuppertal U and research fellow at the Institute for Social Research in Frankfurt. Biopolitics: an advanced introduction. P 63

Agamben's attempt to correct and amend Foucault (cf. 1998, 9) also abandons the latters central insight, namely, that biopolitics is a historical phenomenon that cannot be separated from the development of modern states, the emergence of the human sciences, and the formation of capitalist relations of production. **Without the biopolitical project's necessary placement within a historical-social context, "bare life" becomes an abstraction whose complex conditions of emergence must remain as obscure as its political implications. Agamben tends to erase the historical difference between antiquity and the present, as well as the differences between the Middle Ages and modernity.** Not only does **he avoid the question of what biopolitics has to do with a political economy of life**; he also suppresses the significance that gender has for his line of inquiry. He does not investigate to what extent the production of "bare life" is also a patriarchal project, one that codifies gender difference through a strict and dichotomous apportionment of nature and politics (cf. DeuberMankowsky 2002).

#### no root cause of war

Greg **Cashman**. **2000**. Professor of Political Science at Salisbury State University “What Causes war?: An introduction to theories of international conflict” pg. 9

Two warnings need to be issued at this point. First, **while we have been using a single variable explanation of war merely for the sake of simplicity, multivariate explanations of war are likely to be much more powerful. Since social and political behaviors are extremely complex, they are almost never explainable through a single factor. Decades of research have led most analysts to reject monocausal explanations of war**. For instance, international relations theorist J. David **Singer suggests that we ought to move away from the concept of “causality” since it has become associated with the search for a single cause of war; we should instead redirect our activities toward discovering “explanations”—a term that implies multiple causes of war, but also a certain element of randomness or chance in their occurrence.**

#### Agamben collapses the distinction between democracies and totalitarianism and overexaggerates the extent of bare life

Thomas **Lemke. 2011**. Former assistant professor of sociology at Wuppertal U and research fellow at the Institute for Social Research in Frankfurt. Biopolitics: an advanced introduction. P 55-6.

**Agambens reconstruction of the interrelationships between sovereign rule and biopolitical exception results in an unsettling outcome.** The thesis of the concentration camp as "the hidden matrix of the politics in which we still live" (Agamben 2000, 44) makes claims for an inner link between the emergence of human rights and the development of concentration camps. In this sense, **there is no sharp division between parliamentary democracies and totalitarian dictatorships, liberal constitutional states and authoritarian regimes**. Agambens claim of an "inner solidarity between democracy and totalitarianism" (1998,10) has provoked much resistance. Although his thesis of the camp as "biopolitical paradigm of the modern" (ibid., 117) in no way makes relative or trivializes Nazi extermination policies, it remains the case that Agamben ignores important and essential differences. **The criticism that Agamben "levels" differences is a less relevant argument than his lack of concretization and the excessive dramatization that may lead, ultimately, to the impression that homo sacer is "forever and everywhere"** (Werber 2002, 622).

# 1AR

### K

#### Emergencies don’t turn the case – their theory ignores too many other factors

Posner and Vermeule 3

(\*Eric A. Posner, Kirkland & Ellis Professor of Law, The University of Chicago, \*\*Adrian Vermeule, Professor of Law, The University of Chicago, “ACCOMMODATING EMERGENCIES” THE LAW SCHOOL THE UNIVERSITY OF CHICAGO, September 2003, <http://www.law.uchicago.edu/files/files/48.eap-av.emergency.pdf>, KB)

The ratchet theory and the panic theory have become fixed points in the debate ¶ about emergency powers, yet have escaped rigorous analysis. As we will show, both ¶ theories have conceptual, normative, and empirical difficulties. The ratchet theory lacks a ¶ mechanism that permits constitutional powers to rise and prevents them from falling, and ¶ makes implausible assumptions about the rationality of individuals who consent to ¶ constitutional changes during emergencies. Those who fear the ratchet’s power point to ¶ constitutional trends—such as the rise of executive power—that are the result of longterm technological and demographic changes, not of recurrent emergencies; and they ¶ ignore the possibility of constitutional trends in the opposite direction, such as the rise of ¶ individual rights. (If there is such a trend, it is not a ratchet process either; we include a ¶ critique of an optimistic variant of the emergency ratchet, in which a succession of ¶ emergencies causes government to display ever-increasing respect for civil liberties). As ¶ for the panic theory, it assumes that people can, while panicked, get outside themselves ¶ and constrain their own fear. Although people and officials panic, we have found little ¶ evidence that constitutions or other laws or institutions can control the panic, and cause ¶ people to lose their fear, or else choose, while panicked, laws that they would choose if ¶ they were not panicked. Finally, defenders of either theory do not examine their ¶ normative premises sufficiently: it is not clear that panics and ratchets, if they occur, are ¶ bad things. Fear is often the correct response to a threat; panics can shatter constitutional ¶ structures, but sometimes constitutional structures should be shattered. Ratchets put the ¶ status quo out of reach, but sometimes that is where it should be.

#### Military will adhere to the law- fear the consequences

Dunlap ‘12

[Maj. Gen. Charles J. Dunlap Jr. (Ret.), Professor of the Practice of Law¶ Executive Director, Center on Law, Ethics and National Security @ Duke. In Patriot Debates: Contemporary Issues in National Security Law. <http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch9/ch9_ess2.html> ETB]

This raises an important question: Should America wage war— cyber or otherwise—without legal “limits”? Military commanders have seen the no-legal-limits movie before and they do not like it. In the aftermath of 9/11, civilian lawyers moved in exactly that direction. Former Attorney General Alberto Gonzales, for example, rejected parts of the Geneva Conventions as “quaint.” He then aligned himself with other civilian government lawyers who seemed to believe that the President’s war-making power knew virtually no limits. The most egregious example of this mindset was their endorsement of interrogation techniques now widely labeled as torture.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.

**No risk of continual war making – institutional safeguards check**

Allen **Buchanan 7**, Professor of Philosophy and Public Policy at Duke, 2007 (Preemption: military action and moral justification, pg. 128)

The intuitively plausible idea behind the 'irresponsible act' argument is that, other things being equal, the higher the stakes in acting and in particular the greater the moral risk, the higher are the *epistemic requirements* for justified action. The decision to go to war is generally a high stakes decision par excellence and the moral risks are especially great, for two reasons. First, unless one is justified in going to war, one's deliberate killing of enemy combatants will he murder, indeed mass murder. Secondly, at least in large-scale modem war, it is a virtual certainty that one will kill innocent people even if one is justified in going to war and conducts the war in such a way as to try to minimize harm to innocents. Given these grave moral risks of going to war, quite apart from often substantial prudential concerns, some types of justifications for going to war may simply be too subject to abuse and error to make it justifiable to invoke them. The 'irresponsible act' objection is not a consequentialist objection in any interesting sense. It does not depend upon the assumption that every particular act of going to war preventively has unacceptably bad consequences (whether in itself or by virtue of contributing lo the general acceptance of a principle allowing preventive war); nor does it assume that it is always wrong lo rely on a justification which, if generally accepted, would produce unacceptable consequences. Instead, the "irresponsible act' objection is more accurately described as an agent-centered argument and more particularly an argument from moral epistemic responsibility. The 'irresponsible act' objection to preventive war is highly plausible if— but only if—one assumes that the agents who would invoke the preventive-war justification are, as it were, *on their own* in making the decision to go to war preventively. In other words, the objection is incomplete unless the context of decision-making is further specified. Whether the special risks of relying on the preventive-war justification are unacceptably high will depend, *inter alia,* upon whether the decision-making process includes effective provisions for redu­cing those special risks. Because the special risks are at least in significant part epistemic—due to the inherently speculative character of the preventive war-justification—the epistemic context of the decision is crucial. Because institutions can improve the epistemic performance of agents, it is critical to know what the institutional context of the preventive-war decision is, before we can regard the 'irresponsible agent' objection as conclusive. Like the 'bad practice' argument, this second objection to preventive war is inconclusive because it does not consider— and rule out—the possibility that well-designed institutions for decision-making could address the problems that would otherwise make it irresponsible for a leader to invoke the preventive-war justification.

#### 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.**

**Institutional checks on biopower can be effective**

Nasser **Hussain and** Melissa **Ptacek. 2000**. Department of History, University of California, Berkeley, Law And Society Review, v34 n2.

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

#### The concept of bare life reinforces the ideology they critique – it is more useful to overcome the limits of power through the political action of the aff

**Cesarino & Negri. 2004**. (Cesare, associate professor of cultural studies, Antonio, professor emeritus @ the Collège International de Philosophie, “It’s a Powerful Life: A Conversation on Contemporary Philosophy,” Cultural Critique, Vol. 57, Spring 2004, pg. 172-173)

I believe Giorgio is writing a sequel to Homo Sacer, and I feel that this new work will be resolutive for his thought—in the sense that he will be forced in it to resolve and find a way out of the ambiguity that has qualified his understanding of naked life so far. He already attempted something of the sort in his recent book on Saint Paul, but I think this attempt largely failed: as usual, this book is extremely learned and elegant; it remains, however, somewhat trapped within Pauline exegesis, rather than constituting a full-fledged attempt to reconstruct naked life as a potentiality for exodus, to rethink naked life fundamentally in terms of exodus. I believe that **the concept of naked life** is not an impossible, unfeasible one. I believe it is possible to push the image of power to the point at which a defenseless human being [un povero Cristo] is crushed, to conceive of that extreme point at which power tries to eliminate that ultimate resistance that is the sheer attempt to keep oneself alive. From a logical standpoint, it is possible to think all this: the naked bodies of the people in the camps, for example, can lead one precisely in this direction. But this is also the point at which this concept **turns into ideology: to conceive of the relation between power and life in such a way actually ends up bolstering and reinforcing ideology. Agamben**, in effect, **is saying that such is the nature of power**: in the final instance, **power reduces each and every human being to such a state of powerlessness. But this is absolutely not true**! On the contrary: the **historical process takes place and is produced thanks to a continuous constitution and construction, which undoubtedly confronts the limit over and over** again—but this is an extraordinarily rich limit, in which desires expand, and in which life becomes increasingly fuller. Of course it is possible to conceive of the limit as absolute powerlessness, especially when it has been actually enacted and enforced in such a way so many times. And yet, **isn't such a conception of the limit precisely what the limit looks like from the standpoint of constituted power as well as from the standpoint of those who have already been totally annihilated by such a power**—which is, of course, one and the same standpoint? **Isn't this the story about power that power itself would like us to believe in and reiterate? Isn't it far more politically useful to conceive of this limit from the standpoint of those who are not yet or not completely crushed by power, from the standpoint of those still struggling to overcome such a limit, from the standpoint of the process of constitution,** from the standpoint of power [potenza]?

#### Social movements must work with and along-side legal institutions. Rejection of the law kills solvency.

Peter Gabel, former President and Professor of Law at New College of California, 2009 (“LAW AND ECONOMICS, CRITICAL LEGAL STUDIES, AND THE HIGHER LAW: CRITICAL LEGAL STUDIES AS A SPIRITUAL PRACTICE.” 36 Pepp. L. Rev. 515. Lexis )

This calls not for a rejection of past CLS work, but for a reclaiming of the spiritual dimension of that work. And this in turn requires a reunderstanding of the indeterminacy critique as being merely an analytical moment within the synthesis of a moral critique, as a kind of analytical insight that indicates that the world is open-textured but not going nowhere, and that legal reasoning's claims that would fix the world in idealized, reified abstractions legitimizing injustice and alienation are actually a passivizing defense against the freedom and creative challenge of social vulnerability and uncharted possibility. [\*530] But this also requires a new agenda for our movement that cooperates with the world-wide spiritual-political initiatives that have sprung up since the post-'60s era from which CLS first emerged, and that would be tremendously supportive of our efforts. These spiritual-political initiatives include the religious renewal movements that are linking the spiritual ideal of the beloved community to social action and social change; spiritually informed secular movements like the Network of Spiritual Progressives that are trying to invent new forms of spiritual activism while rethinking foreign and domestic social policy reforms to emphasize spiritual transformation rather than merely liberal redistribution of resources and rights; 31 and the efforts of the environmental and ecology movements to link the redemption of the planet with social healing and sustainable, cooperative economies. All of these efforts require a new legal culture that links justice with explicitly spiritual outcomes - outcomes that foster empathy, compassion, and social connection rather than the vindication of liberal rights in a legal order founded upon the fear-based separation of self and other. One lesson that CLS scholarship itself has taught is that it is impossible for a social transformation movement to be successful without an ability to express its own ideals as also ideals of justice that can achieve legitimate political expression through legal culture. Without that, as Karl Klare, Alan Freeman, and many others have shown, 32 the movement's radical ideals will be recast and stolen away by the liberal interpretations those movements will suffer through the prism of legal assumptions that actually contradict them. Thus while the movement must create the "parallel universe" that can affirm the ontological/epistemological validity of the possibility of a society based on love and mutual recognition, the movement also requires a legal expression of itself that declares this same realization of love and mutual recognition to be indispensable to just outcomes of social conflicts. Such a parallel justice system has already begun to sprout up across the legal landscape, alongside the antagonism of self and other, presupposed and reinforced by the mainstream's adversary system. Among its manifestations are the truly remarkable restorative justice movement, which understands crime and social violence as expressive of a breakdown in community and aspires to apology and forgiveness through direct encounters between victims and offenders as a means of restoration of the communal fabric; 33 the transformative and understanding-based mediation movements that make compassion a central objective to the resolution of civil conflicts; 34 the new [\*531] forms of spiritually-informed law practice that are redefining the lawyer-client relationship as a non-technical, holistic relationship in which lawyers bring a substantive moral and healing vision to bear on the client's perception of his or her "interests," and the relation of those interests to the well-being of the larger community; 35 and the transformation of legal education away from a focus on the mere manipulation of existing rules and doctrine, toward a more humane and spiritually integrated conception of law and justice. What these new efforts need from a revitalized critical legal studies movement is a scholarship and pedagogy that provides in every field a critique of existing law and legal culture that reveals the limitations of the liberal world-view out of which the existing order was constructed in the centuries since the Enlightenment, and that points toward the socially connected community that ought to be its successor. It is this intellectual piece of the puzzle that is lacking from all of the recent efforts to transform legal practice in the ways I have just described; all of these efforts without exception, as far as I know, challenge the individualized, antagonistic, and despiritualized character of the adversary system without challenging the substantive content of existing law or the analytical thought process of legal reasoning. Both of these elements of legal culture - the critique of the substance of legal rules and doctrine, and the critique of detached, analytical rule-application through abstract, logical technique resting on a normative foundation - require a cadre of intellectuals to help disassemble what is and point to what ought to be, as a "moment" in the transformation from the individualistic, liberal world we inhabit to a post-liberal socially connected, loving, and compassionate world to which we aspire. So, for example, a CLS course in Contracts should subordinate its use of the indeterminacy critique to a meaning-centered critique emphasizing how the rules presupposing the legitimacy and desirability of individualistic, self-interested bargains (adjusted by a touch of concern for "the reliance interest") among an infinite number of socially disconnected strangers bound by no common moral purpose or spiritually bonded social community outside their respective blood relatives are rapidly destroying the planet, in part, by making use of liberal abstractions like freedom of choice that make it appear that this lonely destiny is what people really want. Or a course in [\*532] Torts should make it clear to students that there is more to the obligations born of our essential connection to each other as social beings than the duty to not pull chairs out from under each other as we are about to sit down to dinner, or not to smash into each others' cars, or injure each other with exploding Coke bottles - that the bond of recognition itself, and what Emmanuel Levinas calls the ethical demand of the face of the Other, 36 means we have a duty to "rescue" each other, that we must take care of each other, including the poor, the homeless, and those who lack health care. CLS scholars and teachers should extend - and in many instances already have extended - this kind of critical analysis to every area of law, including developing a critical reflection on the Constitution as a liberal and individualistic document that was a great advance in its time but now must be transformed to embrace a newly evolving vision of spiritual community that was not even conceived of as a universal necessity in the late eighteenth century when it was drafted. Concomitant with the transformation of doctrine must come a transformation of remedy, beyond money damages passed between socially separated litigants conceived as interested only in material outcomes, and beyond a due process model of civil and criminal procedure that links justice to merely the vindication of rights through the dutiful monitoring of a fact-based public hearing that leaves the parties as disconnected or more disconnected than when their legal process began. And finally, supporting such a re-visioning of doctrine, remedy, and process must be a rethinking of legal reasoning itself that goes beyond the normative circularity of the application of indeterminate rules presupposing the legitimacy of the secular liberal order toward a morally grounded reflection anchored in the common effort to realize the values of love, compassion, and mutual concern and well-being that are being carried forward by the movement itself as it tries to link the transformative element of its own social being with a new legal knowledge that would be expressive of it. If CLS would embrace the moral and spiritual agenda that I'm proposing here, it would instantly revitalize itself. Everywhere today there are law students and young legal scholars trying to figure out how to devote their lives and work to addressing the problems of global warming and the destruction of the environment, to overcoming the social violence and irrationality of religious fundamentalism and pathological, secular nationalism, and to challenging the human indifference of corporate globalization and its blind and reeling world markets. But Marxist materialism can no longer speak to these new generations of potential activists who have become aware that these problems require a spiritually grounded solution, and after a thirty-year assault by the New Right, no one [\*533] believes any longer in the model of regulatory government as morally capable of containing and altering a civil society founded upon Fear of the Other and private self-interest. A new spiritual activism actually connecting Self and Other is clearly what is needed, and it is already coming into being in hundreds of hopeful incarnations. If CLS were to rediscover itself as the legal-intellectual expression of that world-wide effort, it could once again challenge legal education and legal scholarship to become vehicles of the creation of a better world, connecting the worthwhile body of work already produced by its older generations with new, more spiritually confident work yet to be written by the young.

#### Prsident wont ignore

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.**

#### external checks are effective

Aziz Z. Huq 12, Assistant Professor of Law, University of Chicago Law School, "Binding the Executive (by Law or by Politics)", May 25, [www.law.uchicago.edu/files/file/400-ah-binding.pdf](http://www.law.uchicago.edu/files/file/400-ah-binding.pdf)

Paulson ’ s genuflection and Obama ’ s reticence, I will contend here, are symptomatic of our political system ’ s operation rather than being aberration al . It is generally the case that even in the heart of crisis, and even on matters where executive competence is supposedly at an acme , legislators employ formal institutional powers not only to delay executive initiatives but also affirmatively to end presidential policies. 20 Numerous examples from recent events illustrate the point. Congressional adversaries of Obama, for instance, cut off his policy of emptying Guantánamo Bay via appropriations riders. 21 Deficit hawks spent 2011 resisting the President’s solutions to federal debt, while the President declined to short - circuit negotiations with unilateral action. 22 Even in military matters, a growing body of empirical research suggests Congress often successfully influences the course of overseas engagements to a greater degree than legal scholars have discerned or acknowledged. 23¶ That work suggests that the failure of absolute congressional control over military matters cannot be taken as evidence of “the inability of law to constrain the executive ” in more subtle ways (p 5). The conventional narrative of executive dominance , in other words, is at best incomplete and demands supplementing .¶ This Review uses The Executive Unbound as a platform to explore how the boundaries of discretionary executive action are established. As the controversial national security policies of the Bush administration recede in time, the issue of executive power becomes ripe for reconsideration. Arguments for or against binding the executive are starting to lose their partisan coloration. There is more room to investigate the dynamics of executive power in a purely positive fashion without the impinging taint of ideological coloration.¶ Notwithstanding this emerging space for analys i s, t here is still surprising inattention to evidence of whether the executive is constrained and to the positive question of how constraint works. The Executive Unbound is a significant advance because it takes seriously this second “ mechanism question. ” Future studies of the executive branch will ignore its i mportant and trenchant analysis at their peril. 24 Following PV ’ s lead, I focus on the descriptive , positive question of how the executive is constrained . I do speak briefly and in concluding to normative matters . B ut f irst and foremost, my arguments should be understood as positive and not normative in nature unless otherwise noted.¶ Articulating and answering the question “ W hat binds the executive ?” , The Executive Unbound draws a sharp line between legal and political constraints on discretion — a distinction between laws and institutions on the one hand, and the incentives created by political competition on the other hand . While legal constraints usually fail, it argues, political constraints can prevail. PV thus postulate what I call a “strong law/ politics dichotomy. ” My central claim in this Review is that this strong law/politics dichotomy cannot withstand scrutiny. While doctrinal scholars exaggerate law ’s autonomy, I contend, the realists PV underestimate the extent to which legal rules and institutions play a pivotal role in the production of executive constraint. Further, the political mechanisms they identify as substitutes for legal checks cannot alone do the work of regulating executive discretion. Diverging from both legalist and realist positions, I suggest that law and politics do not operate as substitutes in the regulation of executive authority. 25 They instead work as interlocking complements. An account of the borders of executive discretion must focus on the interaction of partisan and electoral forces on the one hand and legal rules. It must specify the conditions under which the interaction of political actors’ exertions and legal rules will prove effective in limiting such discretion.

#### law can effectively restrain the executive

Aziz Z. Huq 12, Assistant Professor of Law, University of Chicago Law School, "Binding the Executive (by Law or by Politics)", May 25, [www.law.uchicago.edu/files/file/400-ah-binding.pdf](http://www.law.uchicago.edu/files/file/400-ah-binding.pdf)

The Executive Unbound paints a n image of executive discretion almost or completely unbridled by law or coequal branch. But PV also concede that “ the pre sident can exert control only in certain [policy] areas ” (p 59). 51 They give no account, however, of what limits a President ’ s discretionary actions. To remedy that gap, this Section explores how the President has been and continues to be hemmed in by Congress and law. My aim here is not to present a comprehensive account of law as a constraining mechanism. Nor is my claim that law is always effective. Both as a practical matter and as a result of administrative law doctrine, the executive has considerable a uthority to leverage ambiguities in statutory text into warrants for discretionary action. 52 Rather, my more limited aspiration here is to show that Congress and law do play a meaningful role in cabining executive discretion than The Executive Unbound credits . I start with Congress and then turn to the effect of statutory restrictions on the presidency.¶ Consider first a simple measure of Presidents ’ ability to obtain policy change : Do they obtain the policy changes they desire? Every President enters office with an agenda they wish to accomplish. 53 President Obama came into office, for example, promising health care reform, a cap - and - trade solution to climate change, and major immigration reform. 54 President George W. Bush came to the White House committed to educational reform, social security reform, and a new approach to energy issues. 55 One way of assessing presidential influence is by examining how such presidential agendas fare , and asking whet her congressional obstruction or legal impediments — which could take the form of existing laws that preclude an executive policy change or an absence of statutory authority for desired executive action — is correlated with presidential failure. Such a correlation would be prima facie evidence that institutions and laws play some meaningful role in the production of constraints on executive discretion. ¶ Both recent experience and long - term historical data suggest presidential agenda items are rarely achieved , and that legal or institutional impediments to White House aspirations are part of the reason . In both the last two presidencies, the White House obtained at least one item on its agenda — education for Bush and health care for Obama — but failed to secure othe rs in Congress . Such limited success is not new. His famous first hundred days notwithstanding, Franklin Delano Roosevelt saw many of his “ proposals for reconstruction [of government] . . . rejected outright. ” 56 Even in the midst of economic crisis, Congres s successfully resisted New Deal initiatives from the White House . This historical evidence suggests that the diminished success of presidential agendas cannot be ascribed solely to the narrowing scope of congressional attention in recent decades; it is a n older phenomenon. Nevertheless, in more recent periods, presidential agendas have shrunk even more . President George W. Bush ’ s legislative agenda was “ half as large as Richard Nixon ’ s first - term agenda in 1969 – 72, a third smaller than Ronald Reagan ’ s firs t - term agenda in 1981 – 84, and a quarter smaller than his father ’ s first - term agenda in 1989 – 92. ” 57 The White House not only cannot always get what it wants from Congress but has substantially downsized its policy ambitions.¶ Supplementing this evidence of pr esidential weakness are studies of the determinants of White House success on Capitol Hill . These find that “ presidency - centered explanations ” do little work. 58 Presidents ’ legislative agendas succeed not because of the intrinsic institutional characteristi cs of the executive branch, but rather as a consequence of favorable political conditions within the momentarily dominant legislative coalition. 59 Again, correlational evidence suggests that institutions and the legal frameworks making up the statutory status quo ante play a role in delimiting executive discretion.

#### Best recent scholarship and examples prove

Aziz Z. Huq 12, Assistant Professor of Law, University of Chicago Law School, "Binding the Executive (by Law or by Politics)", May 25, [www.law.uchicago.edu/files/file/400-ah-binding.pdf](http://www.law.uchicago.edu/files/file/400-ah-binding.pdf)

There is some merit to this story. But in my view it again understates the observed effect of positive legal constraints on executive discretion. Recent scholarship, for example, has documented congressional influence on the shape of military policy via framework statutes . This work suggests Congress influences executive actions during military engagements through hearings and legislative proposals. 75 Consistent with this account, two legal scholars have recently offered a revisionist history of constitutional war powers in which “ Congress has been an active participant in setting the terms of battle, ” in part because “ congressional willingness to enact [ ] laws has only increased ” over time. 76 In the last decade, Congress has often taken the initiative on national security, such as enacting new statutes on military commissions in 2006 and 2009. 77 Other recent landmark security reforms, such as a 2004 statute restr ucturing the intelligence community, 78 also had only lukewarm Oval Office support. 79 Measured against a baseline of threshold executive preferences then , Congress has achieved nontrivial successes in shaping national security policy and institutions through both legislated and nonlegislated actions even in the teeth of White House opposition. 80¶ The same point emerges more forcefully from a review of our “ fiscal constitution. ” 81 Article I, § 8 of the Constitution vests Congress with power to “ lay and collect Tax es ” and to “ borrow Money on the credit of the United States, ” while Article I, § 9 bars federal funds from being spent except “ in Consequence of Appropriations made by Law. ” 82 Congress has enacted several framework statutes to effectuate the “ powerful limitations ” implicit in these clauses. 83 The resulting law prevents the President from repudiating past policy commitments (as Skowronek suggests) as well as imposing barriers to novel executive initiatives that want for statutory authorization . 84¶ Three statutes merit attention here. First, the Miscellaneous Receipts Act of 1849 85 requires that all funds “ received from customs, from the sales of public lands, and from all miscellaneous sources, for the use of the United States, shall be paid . . . into the treasur y of the United States. ” 86 It ensures that the executive cannot establish off - balance - sheet revenue streams as a basis for independent policy making. Second, the Anti - Deficiency Act, 87 which was first enacted in 1870 and then amended in 190 6 , 88 had the effect of cementing the principle of congressional appropriations control. 89 With civil and criminal sanctions, it prohibits “ unfunded monetary liabilities beyond the amounts Congress has appropriated, ” and bars “ the borrowing of funds by federal a gencies . . . in anticipation of future appropriations. ” 90 Finally, the Congressional Budget and Impoundment Control Act of 1974 91 (Impoundment Act) channels presidential authority to decline to expend appropriated funds. 92 It responded to President Nixon ’ s e xpansive use of impoundment. 93 Congress had no trouble rejecting Nixon ’ s claims despite a long history of such impoundments. 94 While the Miscellaneous Receipts Act and the Anti - Deficiency Act appear to have succeeded, the Impoundment Act has a more mixed rec ord. While the Supreme Court endorsed legislative constraints on presidential impoundment, 95 President Gerald Ford increased impoundments through creative interpretations of the law. 96 But two decades later, Congress concluded the executive had too little di scretionary spending authority and expanded it by statute. 97 ¶ Moreover, statutory regulation of the purse furnishes a tool for judicial influence over the executive. Judicial action in turn magnifies congressional influence. A recent study of taxation litiga tion finds evidence that the federal courts interpret fiscal laws in a more pro - government fashion during military engagements supported by both Congress and the White House than in the course of unilateral executive military entanglements. 98 Although the r esulting effect is hard to quantify, the basic finding of the study suggests that fiscal statutes trench on executive discretion not only directly, but also indirectly via judicially created incentives to act only with legislative endorsement. 99¶ To be sure, a persistent difficulty in debates about congressional efficacy, and with some of the claims advanced in The Executive Unbound , is that it is unclear what baseline should be used to evaluate the outcomes of executive - congressional struggles. What counts, that is, as a “win” and for whom? What, for example, is an appropriate level of legislative control over expenditures? In the examples developed in this Part , I have underscored instances in which a law has been passed that a President disagrees with in substantial part, and where there are divergent legislative preferences reflected in the ultimate enactment. I do not mean to suggest, however, that there are not alternative ways of delineating a baseline for analysis. 100¶ In sum, there is strong evidence that law and lawmaking institutions have played a more robust role in delimiting the bounds of executive discretion over the federal sword and the federal purse than The Executive Unbound intimates. Congress in fact impedes presidential agendas. The White House in practice cannot use presidential administration as a perfect substitute. Legislation implementing congressional control of the purse is also a significant, if imperfect, tool of legislative influence on the ground. This is true even when Presidents influence the budgetary agenda 101 and agencies jawbone their legislative masters into new funding. 102 If Congress and statutory frameworks seem to have such nontrivial effects on the executive ’ s choice set , this at minimum i mplies that the conditions in which law matters are more extensive than The Executive Unbound suggests and that an account of executive discretion that omits law and legal institutions will be incomplete .

**Our risk assessment critical to transforming the public sphere—leads to democratic decision making**

**Borraz, 2007** [OLIVIER BORRAZ Centre de Sociologie des Organisations, Sciences Po-CNRS, Paris, “Risk and Public Problems,” Journal of Risk Research, 10, 7, Oct 2007, 941-957]

These studies seem to suggest that risk is a way of framing a public problem in such a way as to politicize the search for solutions. This politicization entails, in particular, a widening of the range of stakeholders, a reference to broader political issues and debates, the search for new decision- making processes (either in terms of democratization, or renewed scientific expertise), and the explicit mobilization of non-scientific arguments in these processes. But if this is the case, then it could also be true that risk is simply one way of framing public problems. Studies in the 1990s, in particular, showed that a whole range of social problems (e.g., poverty, housing, unemployment) had been reframed as health issues, with the result that their management was transferred from social workers to health professionals, and in the process was described in neutral, depoliticized terms (Fassin, 1998). Studies of risk, on the contrary, seem to suggest that similar social problems could well be re-politicized,

i.e., taken up by new social movements, producing and using alternative scientific data, calling for more deliberative decision-making procedures, and clearly intended to promote change in the manner in which the state protects the population against various risks (health and environment, but also social and economic). In other words, framing public problems as risks could afford an opportunity for a transformation in the political debate, from more traditional cleavages around social and economic issues, to rifts stemming from antagonistic views of science, democracy and the world order.

**Perm solves and case is a net benefit – only by strategically utilizing biopolitical tools like apocalyptic imagery and policy reform can we resist biopower**

JL **Schatz. 2012**. Professor of English and Feminist Evolutionary Studies & Director of Debate at Binghamton University. The Importance of Apocalypse: The Value of End-Of-The-World Politics While Advancing Ecocriticism. Journal of Ecocriticism: A New Journal of Nature, Society and Literature. 4(2)

Anything is justified in the name of saving the environment because it is a question of our very survival. Here we find the logic of things like resource wars that strive to secure geopolitical interests in order to get others to clean up their acts in the name of environmental security4. **From this perspective the mobilizing potentials of apocalyptic imagery can influence populations for the purposes of war instead of positive ecological awareness.** **This fear causes such critics to refrain from utilizing descriptions of omnicide while simultaneously criticizing the most effective tactic activists on the frontlines have**. Luke and Darier’s Foucauldian approach to ecocriticism is not without value. They demonstrate how “discourse delineate[s] ... the terms of intelligibility whereby a particular ‘reality’ can be known and acted upon. When we speak of a discourse we may be referring to a specific group of texts, but also importantly to the social practices to which those texts are inextricably linked” (Doty, 1996: 6). Power continuously operates in both hegemonic and resistant ways regardless if we are monkey-wrenching, speaking at a political press conference, or using the written language of the academic. No matter the form, the way we articulate our discourse must construct reality in a precise way in order to render it intelligible for others to understand. Judith Butler notes that “the media’s evacuation of the human through the image has to be understood ... in terms of the broader problem that normative schemes of intelligibility establish what will and will not be human” (146)5. Once other animals and the environment are understood as less than human their lives become inconsequential compared to the short-term benefit of human civilization. To this ends—despite Luke and Darier’s fear of being coopted—**apocalyptic imagery can help** in two regards. First, it helps **people recognize the interconnection of the global ecology in order to appreciate the similarity between humans and other species**. Second, **it provides a self-motivating reason for people to change their behavior to avert extinction even when confronting those who refuse to recognize the intrinsic value of non-human animals**. In either case **omnicidal images change** both the **mindset and** the **actions** of those we encounter, thereby fostering new directions for humanity to evolve. **Any hesitancy to deploy images of apocalypse out of the risk of acting in a biopolitical manner ignores how any particular metaphor—apocalyptic or not—always risks getting coopted. It does not excuse inaction. Clearly hegemonic forces have already assumed control of determining environmental practices when one looks at the debates surrounding** offshore **drilling**, **climate change**, **and biodiversity** within the halls of Congress. “As this ideological quagmire worsens, urgent problems ... will go unsolved ... only to fester more ominously into the future. ... [E]cological crisis ... cannot be understood outside the larger social and global context ... of internationalized markets, finance, and communications” (Boggs 774). **If it weren’t for people such as Watson connecting things like whaling to the end of the world it wouldn’t get the needed coverage to enter into public discourse. It takes big news to make headlines and hold attention spans in the electronic age**. Sometimes it even takes a reality TV show on Animal Planet. As Luke reminds us, “Those who dominate the world exploit their positions to their advantage by defining how the world is known. Unless they also face resistance, questioning, and challenge from those who are dominated, they certainly will remain the dominant forces” (2003: 413). **Merely sitting back and theorizing over metaphorical deployments does a grave injustice to the gains activists are making on the ground. It** also **allows hegemonic institutions to continually define the debate over the environment by framing out any attempt for significant change, whether it be radical or reformist**. **Only by jumping on every opportunity for resistance can ecocriticism have the hopes of combatting the current ecological reality.** This means we must recognize that we cannot fully escape the master’s house since the surrounding environment always shapes any form of resistance. Therefore, **we ought to act even if we may get coopted**. As Foucault himself reminds us, “instead of radial ruptures more often one is dealing with mobile and transitory points of resistance, producing cleavages in a society that shift about[.] ... And **it is** doubtless **the strategic codification of these points of resistance that makes a revolution possible**, somewhat similar to the way in which the state relies on the institutional ntegration of power relationships. It is in this sphere of force relations that we must try to analyze the mechanisms of power” (96-­‐97). Here Foucault “asks us to think about resistance differently, as not anterior to power, but a component of it. If we take seriously these notions on the exercise and circulation of power, then we ... open ... up the field of possibility to talk about particular kinds of environmentalism” (Rutherford 296). This is not to say that all actions are resistant. Rather, the revolutionary actions that are truly resistant oftentimes appear mundane since it is more about altering the intelligibility that frames discussions around the environment than any specific policy change. Again, this is why people like Watson use one issue as a jumping off point to talk about wider politics of ecological awareness. Campaigns that look to the government or a single policy but for a moment, and then go on to challenge hegemonic interactions with the environment through other tactics, allows us to codify strategic points of resistance in numerous places at once. Again, this does not mean we must agree with every tactic. It does mean that even failed attempts are meaningful. For example, while PETA’s ad campaigns have drawn criticism for comparing factory farms to the Holocaust, and featuring naked women who’d rather go naked than wear fur, their importance extends beyond the ads alone6. By bringing the issues to the forefront they draw upon known metaphors and reframe the way people talk about animals despite their potentially anti-Semitic and misogynist underpinnings. Michael Hardt and Antonio Negri’s theorization of the multitude serves as an excellent illustration of how **utilizing the power of the master’s biopolitical tools can become powerful enough to deconstruct its house despite the risk of cooptation or backlash**. For them, the multitude is defined by the growing global force of people around the world who are linked together by their common struggles without being formally organized in a hierarchal way. While Hardt and Negri mostly talk about the multitude in relation to global capitalism, their understanding of the commons and analysis of resistance is useful for any ecocritic. They explain, [T]he multitude has matured to such an extent that it is becoming able, through its networks of communication and cooperation ... [and] its production of the common, to sustain an alternative democratic society on its own. ... Revolutionary politics must grasp, in the movement of the multitudes and through the accumulation of common and cooperative decisions, the moment of rupture ... that can create a new world. In the face of the destructive state of exception of biopower, then, there is also a constituent state of exception of democratic biopolitics[,] ... creating ... a new constitutive temporality. (357) Once one understands the world as interconnected—instead of constructed by different nationstates and single environments—conditions in one area of the globe couldn’t be conceptually severed from any other. In short, we’d all have a stake in the global commons. **Ecocritics can then utilize biopolitics to shape discourse and fight against governmental biopower by waking people up to the pressing need to inaugurate a new future for there to be any future. Influencing other people through argument and end-of-the-world tactics is not the same biopower of the state so long as it doesn’t singularize itself but for temporary moments.** Therefore, “it is not unreasonable to hope that in a biopolitical future (after the defeat of biopower) war will no longer be possible, and the intensity of the cooperation and communication among singularities ... will destroy its [very] possibility” (Hardt & Negri 347). In the context of capitalism, when wealth fails to trickle down it would be seen as a problem for the top since it would stand testament to their failure to equitably distribute wealth. In the context of environmentalism, not-in-my-backyard reasoning that displaces ecological destruction elsewhere would be exposed for the failure that it is. There is no backyard that is not one’s own. Ultimately, **images of planetary doom demonstrate how we are all interconnected and** in doing so **inaugurate a new world where multitudes, and not governments, guide the fate of the planet.**

**Rejection of sovereign exception fails and results in more violence**

**Moreiras, 2004**. professor, romance studies and literature – Duke University. Alberto, CR: The New Centennial Review, 4.3.

But Rasch remains a Schmittian, not a Benjaminian. For him, **no interruption of the political principle of reason—the ultimate principle of political order, the nomos of the nomos, the principle of sovereign exception**, which he persuasively shows to be a case of the logical law of the excluded middle (Rasch 2002, 38–42)—**is possible without risking the collapse of the political into an eschatology of the end of the world, which is the same as an eschatology of radical origin: “to be liberated from the structure of sovereignty is to be returned to a natural state of innocence**” (48). **Rasch is suspicious of** Benjamin’s—and **Agamben’s**—**pure violence as the harbinger of a “completely new politics” that might in fact accomplish nothing but an exclusion of the political** (38). As he says in a different essay**, “the political does not exist to usher in the good life by eliminating social antagonism; rather, it exists to serve as the medium for an acceptably limited and therefore productive conflict in the inevitable absence of any final, universally accepted vision of the good life”** (Rasch n.d., 30–31). **Rasch opposes a politics of the katechon—a properly Schmittian politics of the containment of evil—to the messianic politics of the reestablishment of natural innocence that he detects in Agamben’s Homo Sacer**.12 Is there, in fact, in Agamben’s State of Exception, an “appeal to the ontological hope” of “infinite perfectibility” (Rasch n.d., 29)? And, a fortiori, is that also what is behind Derrida’s Voyous? The crucial question here concerns the determination of a practical understanding of the political beyond every messianic delusion. **Messianic delusion turns every politics into a kind of ultrapolitics whose political effectivity then wavers between the inane and the catastrophic**. An alternative question is: are onto-theological politics the only possible politics for our age? R E A S O N B E YOND R E A S O N Autoimmunity is said to refer to “this strange illogical logic through which a living being can spontaneously destroy, in an autonomous fashion, that which, in it, is destined to protect it against the other, to immunize it against the intrusive aggression of the other” (Derrida 2003, 173). Autoimmunity is therefore a kind of “death drive” (215) that can be related to the structure of betrayal as self-betrayal, which, as we saw, Lacan considers a radical structure of the human relationship to being. For Lacan, the abandonment of the ethical imperative not to give ground on one’s desire is ultimately an accommodation to the real from which there is no return; the path back of the “ordinary man” into his own business is blocked once he has paid the price of accommodation to the service of goods and has betrayed the structure of his desire: “once one has crossed that boundary . . . there is no way back. It might be possible to do some repair work, but not to undo it” (Lacan 1992, 321). This betrayal formalizes politics—just as it formalizes religion—for Lacan. Lacanian politics, to the extent that they are understood to be a politics of the subject, are framed by a postrevolutionary service of goods, in which a sublimated jouissance waits infinitely, and uselessly, for the formation of the universal State. Is an alternative frame for contemporary politics available? Both Derrida and Agamben radicalize Schmitt’s intuition regarding the necessity of a transformation in the concept of the political given the exhaustion of the political order of modernity. The political order of modernity has exhausted itself through autoimmunitary developments— something that Schmitt anticipated both in his partisan theory, through the projection of the figure of the total counterpartisan that follows “the inevitability of a moral compulsion,” and in his investigation of the notion of a nomos of the earth, which reaches an unexpected arrest in the notion of the Kantian unjust enemy. If both Derrida and Agamben can be said to be Schmittian to a certain extent, in spite of their fundamental antagonism to the German thinker, it is precisely insofar as both of them take as point of departure for their investigations of political sovereignty some of Schmitt’s crucial theories. Derrida makes it very clear through a sort of disavowing avowal: “One did not have to wait for Schmitt to know that the sovereign is he who decides exceptionally and performatively on the exception, he who guards or gives himself the right to suspend the law; or to know that this juridico-political concept, like all the others, secularizes a theological heritage” (2003, 211–12). And Agamben of course makes Schmitt a crucial reference in both Homo Sacer and State of Exception.13 Both of them are interested, not, like Rasch, in a reassertion of sovereignty as the only possible pragmatic framing for a conceptualization of the political today, but rather in a dismantling of the claims of sovereignty as ultimate political claims, or as the ultimate claims of the political. They want to explore the contemporary troubles of sovereignty, troubles in sovereignty—what Derrida can and does call in French mal de souveraineté (196). These troubles are autoimmunity troubles: sovereignty ultimately suffers from itself, as it is its action that ultimately dooms it to face, in a certain far-from-reassuring impotence, the absolute threat or the anomic terror of the real. Can we then think of politics not beyond sovereignty, but rather as not exhausted by the sovereign frame? Is there a position—a properly political position—that can establish a distance from sovereignty without dreaming, like the Lacanian ordinary man, of the messianic fulfillment of the universal State, when desire will coincide absolutely with itself (and when, therefore, there will be nothing but the sovereign, as sovereign desire)? If there is a position, if it is possible to work out a position that can think of sovereignty without being absolutely circumscribed by sovereignty, that position will have accomplished a derangement of onto-theology. It will not have gotten rid of it, just as it will not have gotten rid of sovereignty, but it will have displaced onto-theology, and its political translation as sovereignty theory, from the horizon of the political. Derrida uses the shorthand “nonsovereign god” for this possibility, echoing Heidegger but also displacing Heidegger.14 And **Agamben talks about the liberation of anomy, as a solicitation of the deep historical compromise of violence and the law. If violence becomes the “thing” of politics for Agamben, this is so to the extent that “human action” must “rescind the link between violence and the law” in order to expose the violence of the law, rather than the lawfulness of violence** (which is the Schmittian project). But the reference to human action is already revealing of a limit in **Agamben’s project**. Certainly human action is an unavoidable referent for politics. But Agamben is still under the Lacanian determination, if on the side of the hero. His project**, a liberation of pure violence, is a tragic project to the extent that it leads the hero towards** what Sophocles calls **até.** Of até Lacan says: “It is an irreplaceable little word. It designates the limit that human life can only briefly cross. The text of the Chorus is significant and insistent—ektos atas. Beyond this até, one can only spend a brief period of time, and that’s where Antigone wants to go. . . . One learns from Antigone’s own mouth testimony on the point she has reached: she literally cannot stand it any more. . . . She lives with the memory of the intolerable drama of the one whose descendence has just been destroyed in the figure of her two brothers. She lives in the house of Creon; she is subject to his law; and that is something she cannot bear” (Lacan 1992, 262–63). **Agamben, like the tragic hero, situates himself “with relation to the goal of desire”** (265), **namely, in the relentless pursuit of a liberation from the sovereign law that has created a permanent state of exception: the ineluctable violence of the state as the house of Creon. To liberate pure violence in order to destroy the law**: of this one could say what Lacan says of the tragic hero, namely, “he knows what he is doing. He always manages to cause things to come crashing down on his head” (275). Agamben defines the contemporary state as one in which “the norm rules, but it is not applied (it does not have force) and . . . acts that have no legal value acquire the force. . . . The state of exception is an anomic space, where what is set in place is a force of law without law . . . , where act and power are radically separated” (52). If the contemporary state, the contemporary embodiment of the law, is absolute exception, understood as absolute oppression, and if only a liberation of violence from its lawful capture can release an appropriate politics, this politics’ human action, like Antigone, stands in “as a pure and simple relationship of the human being to that of which he miraculously happens to be the bearer, namely, the signifying cut that confers on him the indomitable power of being what he is in the face of everything that may oppose him. Anything at all may be invoked in connection with this, and that’s what the Chorus does in the fifth act when it evokes the god that saves. Dionysos is this god; otherwise why would he appear here? There is nothing Dionysiac about the act and the countenance of Antigone. Yet she pushes to the limit the realization of something that might be called the pure and simple desire of death as such. She incarnates that desire” (282). **A politics of heroic desire, in the ineluctable fulfillment of the ethical imperative, might be conceived to be an antisovereign politics, but it is still a subjective politics of catastrophe. At the limit, the hero does not abandon the horizon of sovereignty: the hero simply inverts it, and puts it at the service of an intensely mystical jouissance**, “the passage that allows access to the justice that one of Benjamin’s posthumous fragments defines as a state of the world in which it appears as an absolutely inappropriatable and unjuridifiable good” (Agamben 2003, 83).