# 1AC

**Adv 1: Arms Race**

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

Goldman 13

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

Security analysts are predicting that **2013 is when** nation-sponsored **cyberwarfare goes mainstream** -- and some think such attacks will lead to actual deaths. In 2012, **large-scale cyberattacks** targeted **at** the **Iran**ian government **were uncovered, and in return, Iran** is believed to have **launched** [**massive attacks aimed at U.S. banks**](http://money.cnn.com/2012/11/05/technology/security/iran-cyberattack/index.html?iid=EL) **and Saudi oil companies. At least 12 of the world's 15 largest military powers are currently building cyberwarfare programs, according to James Lewis, a cybersecurity expert at** the **C**enter for **S**trategic and **I**nternational **S**tudies. So a [**cyber Cold War**](http://money.cnn.com/2011/07/28/technology/government_hackers/index.htm?iid=EL) **is already in progress.** But some **security companies believe that battle will become even more heated this year. "Nation states and armies will be more frequent actors and victims** of cyberthreats**," a team of researchers at McAfee Labs,** an Intel ([INTC](http://money.cnn.com/quote/quote.html?symb=INTC&source=story_quote_link), [Fortune 500](http://money.cnn.com/magazines/fortune/fortune500/2012/snapshots/642.html?iid=EL))subsidiary, **wrote** in a [recent report](http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf). Michael **Sutton, head of security research at cloud** security **company** [Zscaler](http://www.zscaler.com/), **said he expects governments to spend furiously on building up their** cyber **arsenals. Some may** even **outsource attacks to online hackers.** The Obama administration and many in Congress have been [more vocal](http://money.cnn.com/2012/04/27/technology/cispa-cybersecurity/index.htm?iid=EL) about how an enemy nation or a terrorist cell could target the country's critical infrastructure in a cyberattack. **Banks, stock exchanges, nuclear** power **plants and water purification systems are** particularly **vulnerable, according to numerous assessments delivered to Congress** last year.

#### Specifically, OCO-driven retaliatory cycles and arms races

Moss 13

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

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

#### Cyber arms race causes world war

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

CSM 11

Christian Science Monitor

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

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

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

— otherwise nuclear war is inevitable from arms-racing, command and control hacking, crisis instability, and fracturing nuclear agreements

Austin, 8/6

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

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

#### Cyber war escalates - Speed, scope, and spoofing

Clarke and Knake ‘12

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

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

### Adv 2: Alliances

#### Congressional restrictions necessary for allied cooperation

Dunlap 12

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

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

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

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

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

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

Lawson ‘10

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

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

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

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

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

#### Legitimacy is key to band-wagon

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

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

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

Kazianis 12

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

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

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

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

RTT 13

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

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

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

Yoshihara 10

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

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

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

Colby et al 13

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

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

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

Rehman 13

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

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

### Plan

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

### Solvency

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

Bradbury 11

Assistant Attorney General for the Office of Legal Counsel

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

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

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

Goldsmith 10

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

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

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

Lewis 11

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

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

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

Dycus 10

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

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

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

Bastby 12

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

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

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

Hansen & Friedman 9

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

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

# 2AC

## Allies

**2. Cycles of hostility have already begun even if they are constructed. Their K ignores real threats that are entrenched by past representations**

**Pan ‘4**

(Chengxin, Australian National University, DISCOURSES OF ‘CHINA’ IN INTERNATIONAL RELATIONS: A STUDY IN WESTERN THEORY AS (IR) PRACTICE, Doctoral Thesis, p. 240-241)

Thus understood, these Chinese reactions, hostile as they might be, can no longer be oversimplified or totalised as entrenched, xenophobic antiAmericanism per se.141 Rather, it seems that they are highly predicated on the ways in which China is treated by the West. In spite of this, however, they need to be taken seriously. This is because the accumulation of these reactive, nationalist, and essentialist sentiments could easily turn into “a narcissistic, megalomanic affirmation of China” and “fascistic arrogance and self-aggrandizement.”142 Taking on a life of their own, this highly appealing vision of China could then negatively impact on its relations with the West in the long term. Among other things, this new appreciation of a sense of national humiliation has given rise to the questioning of the fundamental direction of Chinese foreign policy as pursued by the neoliberal ruling elites. For example, one influential commentator argues that the problem in Sino-Western relations is not that “we Chinese” are unwilling to learn from outside, but that the West-led outside world does not welcome “us” to do so.143 Indeed, for many Chinese intellectuals, this now widely held perception reverberates strongly with the longstanding agony that Western ‘teachers’ never really welcomed their Chinese ‘students’ to learn their real secrets. Out of this doubt over Western sincerity have now grown both a strong criticism of China’s neoliberal views of the outside world as ‘one-sided wishful thinking,’ and a heightened fascination with realism and power politics in China’s strategic thinking and IR studies, to which my analysis will now turn.

## Solvency

#### 5. Our impacts aren’t constructed until they prove it.

Yudkowsky 6 – Eliezer Yudkowsky, Research Fellow at the Singularity Institute for Artificial Intelligence that has published multiple peer-reviewed papers on risk assessment. Cognitive biases potentially affecting judgment of global risks Forthcoming in Global Catastrophic Risks, eds. Nick Bostrom and Milan Cirkovic. August 31, 2006.

Every true idea which discomforts you will seem to match the pattern of at least one psychological error. Robert Pirsig said: “The world’s biggest fool can say the sun is shining, but that doesn’t make it dark out.” If you believe someone is guilty of a psychological error, then demonstrate your competence by first demolishing their consequential factual errors. If there are no factual errors, then what matters the psychology? The temptation of psychology is that, knowing a little psychology, we can meddle in arguments where we have no technical expertise – instead sagely analyzing the psychology of the disputants. If someone wrote a novel about an asteroid strike destroying modern civilization, then someone might criticize that novel as extreme, dystopian, apocalyptic; symptomatic of the author’s naive inability to deal with a complex technological society. We should recognize this as a literary criticism, not a scientific one; it is about good or bad novels, not good or bad hypotheses. To quantify the annual probability of an asteroid strike in real life, one must study astronomy and the historical record: no amount of literary criticism can put a number on it. Garreau (2005) seems to hold that a scenario of a mind slowly increasing in capability, is more mature and sophisticated than a scenario of extremely rapid intelligence increase. But that’s a technical question, not a matter of taste; no amount of psychologizing can tell you the exact slope of that curve. It’s harder to abuse heuristics and biases than psychoanalysis. Accusing someone of conjunction fallacy leads naturally into listing the specific details that you think are burdensome and drive down the joint probability. Even so, do not lose track of the real- world facts of primary interest; do not let the argument become about psychology. Despite all dangers and temptations, it is better to know about psychological biases than to not know. Otherwise we will walk directly into the whirling helicopter blades of life. But be very careful not to have too much fun accusing others of biases. That is the road that leads to becoming a sophisticated arguer – someone who, faced with any discomforting argument, finds at once a bias in it. The one whom you must watch above all is yourself. Jerry Cleaver said: “What does you in is not failure to apply some high-level, intricate, complicated technique. It’s overlooking the basics. Not keeping your eye on the ball.” Analyses should finally center on testable real-world assertions. Do not take your eye off the ball.

#### 6. Even if predictions in the abstract are wrong, policy debates is productive, improves predictive accuracy, and solves cession of the debate to cloistered experts

Tetlock and Gardner 2011 (Philip Tetlock is a professor of organizational behavior at the Haas Business School at the University of California-Berkeley, AND Dan Gardner is a columnist and senior writer for the Ottawa Citizen and the author of The Science of Fear, received numerous awards for his writing, including the Michener Award, M.A. History from York, "OVERCOMING OUR AVERSION TO ACKNOWLEDGING OUR IGNORANCE" July 11 www.cato-unbound.org/2011/07/11/dan-gardner-and-philip-tetlock/overcoming-our-aversion-to-acknowledging-our-ignorance/)

The optimists are right that there is much we can do at a cost that is quite modest relative to what is often at stake. For example, why not build on the IARPA tournament? Imagine a system for recording and judging forecasts. Imagine running tallies of forecasters’ accuracy rates. Imagine advocates on either side of a policy debate specifying in advance precisely what outcomes their desired approach is expected to produce, the evidence that will settle whether it has done so, and the conditions under which participants would agree to say “I was wrong.” Imagine pundits being held to account. Of course arbitration only works if the arbiter is universally respected and it would be an enormous challenge to create an analytical center whose judgments were not only fair, but perceived to be fair even by partisans dead sure they are right and the other guys are wrong. But think of the potential of such a system to improve the signal-to-noise ratio, to sharpen public debate, to shift attention from blowhards to experts worthy of an audience, and to improve public policy. At a minimum, it would highlight how often our forecasts and expectations fail, and if that were to deflate the bloated confidence of experts and leaders, and give pause to those preparing some “great leap forward,” it would be money well spent. But the pessimists are right, too, that fallibility, error, and tragedy are permanent conditions of our existence. Humility is in order, or, as Socrates said, the beginning of wisdom is the admission of ignorance. The Socratic message has always been a hard sell, and it still is—especially among practical people in business and politics, who expect every presentation to end with a single slide consisting of five bullet points labeled “The Solution.” We have no such slide, unfortunately. But in defense of Socrates, humility is the foundation of the fox style of thinking and much research suggests it is an essential component of good judgment in our uncertain world. It is practical. Over the long term, it yields better calibrated probability judgments, which should help you affix more realistic odds than your competitors on policy bets panning out.

## Offcase

### 2AC - Anthro

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

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

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

c. Vague alts are a voting issue – skews 2AC offense and creates a form of sandbagging which unfairly privileges the time benefits of the block

#### 2. There is no coherent link to this argument – the impact claims of the 1AC are against nuclear war. Two arguments

A. Their link argument is survivalism, survival is not a 1AC argument, we just think that mass death is bad

B. Nuclear war would kill other species as well, the fact that we didn’t say humans in the 1AC means the link of omission makes no sense

#### 3. Reject systematic or all-encompassing “root cause” claims for human action

Bleiker, 3 (Roland, 2003, “Discourse and Human Agency,” Contemporary Political Theory, No. 2, Professor at School of Political Science, University of Queensland, pg. 25, JPL)

A conceptualization of human agency cannot be based on a parsimonious proposition, a one-sentence statement that captures something like an authentic nature of human agency. There is no essence to human agency, no core that can be brought down to a lowest common denominator, that will crystallize one day in a long sought after magic formula. A search for such an elusive centre would freeze a specific image of human agency to the detriment of all others. The dangers of such a totalizing position have been well rehearsed. Foucault (1982, 209), for instance, believes that a theory of power is unable to provide the basis for analytical work, for it assumes a prior objectification of the very power dynamics the theory is trying to assess. Bourdieu (1998, 25) speaks of the ‘imperialism of the universal’ and List (1993, 11) warns us of an approach that ‘subsumes, or, rather, pretends to be able to subsume everything into one concept, one theory, one position.’ Such a master discourse, she claims, inevitably oppresses everything that does not fit into its particular view of the world. What, then, is the alternative to anchoring an understanding of human agency in a foundationalist master narrative? How to ground critique, actions, norms and life itself if there are no universal values that can enable such a process of grounding? Various authors have advanced convincing suggestions. Consider the following three examples: (1) de Certeau (1990, 51) attempts to avoid totalitarian thought by grounding his position not in a systematic theory, but in ‘operational schemes.’ A theory is a method of delineation. It freezes what should be understood in its fluidity. An understanding of operational schemes, by contrast, recognizes that events should be assessed in their changing dimensions. Rather than trying to determine what an event is, such an approach maps the contours within which events are incessantly constituted and reconstituted. Or, expressed in de Certeau’s terminology, one must comprehend forms of action in the context of their regulatory environment. (2) Butler (1992, 3–7) speaks of contingent foundations. Like de Certeau, she too believes that the Foucaultean recognition that power pervades all aspects of society, including the position of the critic, does not necessarily lead into a nihilistic abyss. It merely shows that political closure occurs through attempts to establish foundational norms that lie beyond power. Likewise, to reopen this political domain is not to do away with foundations as such, but to acknowledge their contingent character, to illuminate what they authorize, exclude and foreclose. One must come to terms with how the subject and its agency are constituted and framed by specific regimes of power. However, this is not the end of human agency. Quite to the contrary. Butler (1992, 12–14) argues persuasively that ‘the constituted character of the subject is the very precondition of its agency.’ To appreciate the practical relevance of this claim, one must investigate the possibilities for agency that arise out of existing webs of power and discourse. One must scrutinize how social change can be brought about by a reworking of the power regimes that constitute our subjectivity (Butler, 1992, 13). (3) Deleuze and Guattari (1996, 3–25, 377) go a step further. Opting for the rhizome, they reject all forms of foundations, structures, roots or trees. The latter three, they say, has dominated much of the Western thought. A tree is a hierarchical system in which ones becomes two, in which everything can be traced back to the same origin. Roots and radicles may shatter the linear unity of knowledge, but they hold on to a contrived system of thought, to an image of the world in which the multiple always goes back to a centred and higher unity. The brain, by contrast, is not rooted, does not strive for a central point. It functions like a subterranean rhizome. It grows sideways, has multiple entryways and exits. It has no beginning or end, only a middle, from where it expands and overspills. Any point of the rhizome, Deleuze and Guattari emphasize, is connected to any other. It is a multiplicity without hierarchies, units or fix points to anchor thought. There are only lines, magnitudes, dimensions, plateaus, and they are always in motion. To travel along these lines and dimensions is to engage in nomad thought, to travel along axis of difference, rather than identity. Nomad thought, says one of Deleuze’s feminist interpreters, ‘combines coherence with mobility,’ it is ‘a creative sort of becoming, a performative metaphor that allows for otherwise unlikely encounters and unsuspected sources of interaction of experience and of knowledge’ (Braidotti, 1994, 21). The extent to which this form of thinking constitutes a grounding process may be left open to question. Judging from Deleuze’s own work it is clear, however, that the exploration of difference and multiplicities does not prevent him from taking positions for or against specific political issues. What he does forgo, however, is a central authorial voice F to the benefit of a polyphonic array of whispers and shouts.

#### 4. Perm– Do both. At best their link is one of omission, the permutation resolves it

#### 5. The critique is anthropocentric – it assumes knowledge for nature

Bobertz 97 Bobertz Ass’t Prof of Law, Nebraska College of Law, 1997, Bradley Columbia Journal of Environmental Law,Lexis

Apart from the political dangers Ferry associates with deep ecology, he believes the philosophy suffers from a fundamental self-contradiction. The argument that natural objects can possess their own interests strikes Ferry as "one of the mostabsurd forms of anthropomorphism." n100 We cannot "think like a mountain," to use Aldo Leopold's famous phrase, n101 because, quite obviously, we are not mountains. Recalling Sierra Club v. Morton, n102 the famous standing case involving a proposal to construct a ski resort in California's Mineral King valley, Ferry claims that environmentalists "always suppose that the interests of objects (mountains, lakes and other natural things) are opposed to development. But how do we know? After all, isn't it possible that Mineral King would be inclined to welcome a ski slope after having remained idlefor millions of years?" n103 Yet few people, including the writers Ferry labels as deep ecologists, would disagree with the fact that recognizing value in natural objects is an act of human cognition. Perhaps a person suffering from profound psychosis might claim the ability to understand how a mountain "thinks," but the writers Ferry criticizes do not advance such bizarre claims. n104 For deep ecologists and environmental ethicists, phrases such as "think like a mountain" are metaphorical and heuristic, not literal and agenda-setting.

#### 6. Their impact claims are anthropocentric – belief that humans can cause such harm replicates the problem

Fox, 5 (Russel, 11/22/5, “The Real Anthropocentrism,” In Medias Res, Ph.D, Assistant Professor of Political Science Division of Social and Behavioral Sciences Friends University, JPL)

In the end, I think the attempt to purge the human, to reduce the everyday productive place of actual human beings from one's picture of the natural world (an attempt that can lead ultimately to rather bizarre conclusions), rests on a perverse kind of anthropocentrism. Isn't anthropocentrism exactly what deep ecologists have long said is the root of our problem--the way in which our economies and societies assume that human beings are the center of creation? Yes. But isn't the belief that human beings are utterly and uniquely destructive of the natural world, that in our ordinary consumptive lives we cannot help but be a "foreign" presence on the earth, equally anthropocentric? In fact, it might be an even worse anthropocentrism: in the real world, farmers and gardeners and all those who care about the earth take seriously their stewardship of it, a stewardship which makes them, in my experience at least, humble and careful, aware of the fragility of their relationship with nature. Whereas radical environmentalism too often allows for no such complexity; there is humanity and there is nature, and the further the two are kept tightly separate from each other (close enough for the former to look at and "commune with" the latter, but nothing more), the better for both. For any who find themselves agreeing with this position, I strongly recommend 1491--a wonderful, provocative new book which argues that "pristine" New World which European explorers "discovered" and invaded in the from 15th to the 17th centuries, and which many today consider today to have been a kind of paradise lost, was to a great extent the creation of prolonged human interaction. The Amazon basin, the buffalo herds--all a result of generations of indigenous "species maintenance" and "land planning" (though tragic accidents played a part as well). Real environmentalists know that human technology and society, for better and for worse, are as much a part of the geography of the planet as the life patterns of any other species. Only a truly anthropocentric thinker would think that you can take humans--like either the Gwich'in or the Inupiat--out of the equation, and call what remains to be conserved truly "natural."

#### 7. Perm, do the plan and all non-mutually exclusive parts of the alt. We can recognize the need for environmentally sustainable practices without resorting to dangerous biocentrism

Hwang, 3 (Kyung-Sig, 2003, “Apology for Environmental Anthropocentrism,” Eubios Ethics Institute, Professor in Department of Philosophy at Seoul National University, JPL) \*Gender modified

While our ability to affect the future is immense, our ability to foresee the results of our environmental interventions is not. I think that our moral responsibility grows with foresight. And yet, paradoxically in some cases grave moral responsibility is entailed by the fact of one's ignorance. If the planetary life-support system appears to be complex and mysterious, humble ignorance should indicate respect and restraint. However, as many life scientists have complained, these virtues have not been apparent in these generations. Instead they point out, we have boldly marched ahead, shredding delicate ecosystems and obliterating countless species, and with them the unique genetic codes that evolved through millions of years; we have altered the climate and even the chemistry of the atmosphere, and as a result of all this-what?[18] A few results are immediately to our benefit; more energy, more mineral resources, more cropland, convenient waste disposal. Indeed, these short-term payoffs motivated us to alter our natural environment. But by far the larger and more significant results, the permanent results, are unknown and perhaps unknowable. Nature, says poet, Nancy Newhall, "holds answers to more questions than we know how to ask." And we have scarcely bothered to ask.[19] Year and year, the natural habitants diminish and the species disappear, and thus our planetary ecosystem (our household) is forever impoverished. It is awareness of ecological crisis that has led to the now common claim that we need transvaluation of value, new values, a new ethic, and an ethic that is essentially and not simply contingently new and ecological. Closer inspection usually reveals that the writer who states this does not really mean to advance such a radical thesis, that all they are arguing for is the application of old, recognized, ethical values of the kind noted under the characterization of respect for persons, justice, honesty, promotion of good, where pleasure and happiness are seen as goods. Thus, although W. T. Blackstone writes; "we do not need the kind of transvaluation that Nietzsche wanted, but we do need that for which ecologists are calling, that is, basic changes in man's attitude toward nature and man's place in nature, toward population growth, toward the use of technology, and toward the production and distribution of goods and services." We need to develop what I call the ecological attitude. The transvaluation of values, which is needed, will require fundamental changes in the social, legal, political and economic institutions that embody our values. He concludes his article by explicitly noting that he does not really demand a new ethic, or a transvaluation of values. A human being is a hierarchical system and a component of super-individual, hierarchical system of sets. What is needed is not the denial of anthropocentrism, the placing of the highest value on humans and their ends and the conceiving of the rest of the nature as an instrument for those ends. Rather what is needed is the explicit recognition of these hierarchical systems and an ecological approach to science and the accumulation of scientific knowledge in which the myriad casual relationships between different hierarchical systems are recognized and put to the use of humanity. The freedom to use the environment must be restricted to rational and human use. If there is irrational use - pollution, overpopulation, crowding, a growth in poverty, and so on - people may wipe out hierarchies of life related to their own survival and to the quality of their own lives. This sort of anthropocentrism is essential even to human survival and a radical biotic egalitarianism would undermine conditions for that survival.[20] Rational anthropocentrism, one that recognizes the value of human life "transcends our individual life" and one in which we form a collective bond of identity with the future generations is essential in the process of human evolution.

#### 8. Preventing human extinction is necessary in an eco-centric framework

Baum 9 – PhD @ Penn State University Sean Baum, PhD @ Penn State University, 2009, “Costebenefit analysis of space exploration: Some ethical considerations,” Space Policy, Vol. 25, Science Direct

It is of note that the priority of reducing the risk of human extinction persists in forms of CBA which value nature in an ecocentric fashion, i.e. independently of any consideration of human interests. The basic reason is that without humanity leading long-term survival efforts (which would most likely include space colonization), the rest of Earth life would perish as a result of the astronomical processes described above. This point is elaborated by futurist Bruce Tonn, who argues on ecocentric grounds for reorienting society to focus on avoiding human extinction through both immediate avoidance of catastrophe and long-term space colonization [40]. Tonn dubs this process of surviving beyond Earth’s eventual demise ‘‘transcending oblivion’’ [41]. There is thus some convergence in the recommendations of the common anthropocentric, money-based CBA and the ecocentric CBA described here. This convergence results from the fact that (in all likelihood) only humans are capable of colonizing space, and thus human survival is necessary for Earth life to transcend oblivion.

#### 9. Alt fails – people will inevitably be ethnocentric

Lee, 9, Philosophy Professor at Bloomsburg, ‘9 (Wendy, Spring, “Restoring Human-Centerednes to Environmental Conscience: The Ecocentrist's Dilemma, the Role of Heterosexualized Anthropomorphizing, and the Significance of Language to Ecological Feminism” Ethics and the Environment, Vol 14 No 1, Project Muse)

Bender undertakes this task in the course of promoting his specific version of ecocen trism that he calls "nondualism" but it is telling that, instead of offering an argument that provides grounds for rejecting the "dualism" of experiencing subject and experienced object, he resorts to an experience of "nonduality": I start out…in ordinary, dualistic, waking consciousness, feeling myself a subject amidst myriad objects around me, each experienced as other. I discover I do not exist independently, but am like a node in a web, through which diverse kinds of energy flow. For example, I [End Page 35] take in the Sun's warmth, the in-breath, food, water, human speech, and so on. Meanwhile, I expel many kinds of energy. Like the out-breath, speech, bodily movements, and excreta. The energy I take in and expel circulates everywhere on Earth, passing through others as through myself. Thus I discover my connectedness to all other beings, such that I, like they, am but one manifestation of this energy flow, of planet Earth…. Nonduality emerges as I realize further that natural phenomena are Earth transiently manifest, empty of substantive selfhood (objectivity), since everything is dependently co-originated. Thus, though I am precisely emptiness of substantive or independent selfhood; even so, as one particular manifold of relations, I am unique. (2003, 435) The difficulties here are three-fold: First, this isn't an argument, but rather an experiential narrative, hence it would be folly to think it could establish anything other than that someone can have such an experience. But since such could be motivated by, say, exhaustion, illness, or the use of narcotics, it hardly establishes any metaphysical claim about the nature of identity or being—much less about any capacity to dissociate oneself from "substantive selfhood." Second, however much he may feel himself to be "empty of substantive selfhood" Bender's use of "I' suggests that he confuses the capacity to conceive with the capacity to actually be so emptied. It's one thing to conceive of myself as connected to all other beings—indeed I do so conceive myself, I know this in the abstract to be true and I know of no evidence that contradicts it. It is, however, quite another thing to experience myself as emptied of selfhood. Moreover, it is simply false that what I can conceive, imagine, think, or even describe is necessarily something I can experience per se. Third, although Bender's appeals to intuition, mystical insight, Spinoza's notion of particulars as manifestations of nature (2003, 434–5), or Buddhist inspired meditation (2003, 436–7) might be compelling for someone already convinced that so-called nondualist identification with nonhuman nature is possible, these hardly suffice as an argument convincing to the skeptic who may not share the necessary presuppositions or traditions. Here too, then, Bender's account is unconvincing—the ethical norm he derives from it (among others), "Form one body with all beings!" is likely to be mystifying to anyone unconvinced we can make this leap of faith from centeredness to "one body" or (as the moral dictum requires) from the "I" of subject-object dualism to the disavowal of my body. [End Page 36] Moreover, if I am right that there are good reasons to take the specifically embodied configuration of capacities and limitations that describe human being seriously, no such dissociation from "I" is possible—in fact, it intimates precisely the dualism Bender rejects. However deep my feelings (spiritual sensibilities, affectionate sentiments, desires to connect) go with respect to my appreciation of natural objects and phenomena, I nonetheless remain at the center of my embodied consciousness—and cannot be/do otherwise. Hence, one more version of the ecocentrist's dilemma: the dissociation of self demanded by the moral maxim "form one body with all things" assumes that I can dissociate my consciousness from my body—what else to call this but dualism? The notion that I could dissociate myself without dissociating myself from my situated body to be "one with all things" is comprehensible only if I am not (at least essentially) my body, but rather a consciousness that, even if not fully independent, is capable of not merely conceiving but experiencing "my" body as something other than bound by my own skin, that is, as not my body. Hence I must be dual—a "mind" that, in virtue of its capacity to empty itself of its "substantive selfhood," is merely in a dissociable body. No doubt, Bender would find this objection to his view onerous. However, when he advises us to try to expand our selves through, for example, meditation or to encompass an ever-wider set of relations with and to human and nonhuman others (2003, 423–4), it is hard to see how his view does not fit the dualist shoe. He writes that "[s]uch a practice, over time, should transform your sense of who you are as you discover you are not the separate skin-encapsulated individual you once thought you were, but that you belong to all other living beings, and that other beings are not really other, and that you yourself are not really the center of concern." (2003, 424, my emphasis) Again, Bender confuses what I can conceive with what I can experience—I can conceive myself as "not the center of concern," but not an iota of this moral recognition either requires or makes possible an experience of myself as anything other than "skin encapsulated." Bender hasn't, moreover, the luxury of trading in his metaphysical commitments for the option that he's speaking "merely" phenomenologically or metaphorically. For neither the environmental pragmatist, who would likely deny the need to undertake such a practice in order to have a stake in the future of human [End Page 37] consciousness, nor those who engage in such practices without a smidgeon of the environmental activism Bender hopes will follow, are likely to be moved by anything but an argument for nondualism—and this Bender does not provide.

#### 10. Given that inevitability, the attempt of the alternative causes us to give up and abandon all ethical engagement with the environment

Lee, 9, Philosophy Professor at Bloomsburg, ‘9 (Wendy, Spring, “Restoring Human-Centerednes to Environmental Conscience: The Ecocentrist's Dilemma, the Role of Heterosexualized Anthropomorphizing, and the Significance of Language to Ecological Feminism” Ethics and the Environment, Vol 14 No 1, Project Muse)

A second difficulty is that if Bender is correct that the centeredness of human consciousness predisposes (or just is) chauvinistic, then either we really are doomed to continue the ecocidal trajectory of our history or, as Bender argues, we must disavow our human-centeredness in favor of an ecocentric ("non-dualist") perspective and practice (2003, 397–404, 445–9). Hence a first version of the ecocentrist's dilemma: If the ecocentrist is wrong, and it turns out that human-centeredness (qua chauvinistic) is an ineradicable feature of human consciousness (at least short of suicide), then we're doomed to precisely the environmental destruction Bender chronicles in impressive (if however despairing) detail in The Culture of Extinction. We are, in other words determined to "dominate the earth!" in which case we may as well just "hang it up," head out to buy Hummers, and buy stock in Shell. This, of course, is not a conclusion Bender (or any of us) would find acceptable. But if, alternatively, the ecocentrist is right, he/she must show how it is possible—at the level of conscious experience—to dissociate that experience from the centered "I" of the subject who, in other words, has it in mind to accomplish the disavowal of the presumably egoistic self and permanently redirect consciousness towards the eco-centric.3

**11. Rejecting anthropocentrism prevents the environmental movement from effectuating political change**

Martin W. **Lewis, 1992**. Associate Research Professor of Geography, Duke University. Green Delusions: An Environmentalist Critique of Radical Environmentalism, 22]

**It is widely accepted that environmental thinkers can be divided into two camps: those who favor the preservation of nature for nature's sake, and those who wish only to maintain the environment as the necessary habitat of humankind** (see Pepper 1989; O'Riordan 1989; W. Fox 1990). In the first group stand the green radicals, while the second supposedly consists of environmental reformers, also labeled "shallow ecologists." Radicals often pull no punches in assailing the members of the latter camp for their anthropocentrism, managerialism, and gutless accommodationism--to some, "shallow ecology" is "just a more efficient form of exploitation and oppression" (quoted in Nash 1989:202). While **this dichotomy** may accurately depict some of the major approaches of the past, **it** **is remarkably unhelpful for devising the kind of framework required for a truly effective environmental movement. It incorrectly assumes that those who adopt an anti-anthropocentric view** (that is, one that accords intrinsic worth to nonhuman beings) **will also embrace the larger political programs of radical environmentalism**. Similarly**, it portrays those who favor reforms within the political and economic structures of representative democracies as thereby excluding all nonhumans from the realm of moral consideration**. Yet **no convincing reasons are ever provided to show why these beliefs should necessarily be aligned in such a manner**. (For an instructive discussion of the pitfalls of the anthropocentric versus nonanthropocentric dichotomy, see Norton 1987, chapter II.)

### 2AC – Legalism (Posner and Vermule)

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

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

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

c. Vague alts are a voting issue – skews 2AC offense and creates a form of sandbagging which unfairly privileges the time benefits of the block

#### 2. Posner and Vermeule are wrong---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

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.

**2. Permutation do both – resolves the link to the kritik**

#### 3. Debating about specific policies is essential to promote more ethical and accountable policymaking – their abstract politics promotes disengagement and poor argumentation skills

David Chandler. 2007. Centre for the Study of Democracy, Westminster, Area, Vol. 39, No. 1, p. 118-119

This disjunction between the human/ethical/global causes of post-territorial political activism and the capacity to 'make a difference' is what makes these individuated claims immediately abstract and metaphysical – there is no specific demand or programme or attempt to build a collective project. This is the politics of symbolism. The rise of symbolic activism is highlighted in the increasingly popular framework of 'raising awareness'– here there is no longer even a formal connection between ethical activity and intended outcomes (Pupavac 2 006). Raising awareness about issues has replaced even the pretense of taking responsibility for engaging with the world – the act is ethical in-itself. Probably the most high profile example of awareness raising is the shift from Live Aid, which at least attempted to measure its consequences in fund-raising terms, to Live 8 whose goal was solely that of raising an 'awareness of poverty'. The struggle for 'awareness' makes it clear that the focus of symbolic politics is the individual and their desire to elaborate upon their identity – to make us aware of their 'awareness', rather than to engage us in an instrumental project of changing or engaging with the outside world. It would appear that in freeing politics from the constraints of territorial political community there is a danger that political activity is freed from any constraints of social mediation (see further, Chandler 2004a). Without being forced to test and hone our arguments, or even to clearly articulate them, we can rest on the radical 'incommunicability' of our personal identities and claims – you are 'either with us or against us'; engaging with those who disagree is no longer possible or even desirable. It is this lack of desire to engage which most distinguishes the unmediated activism of post-territorial political actors from the old politics of territorial communities, ///founded on struggles of collective interests (Chandler 2004b). The clearest example is old representational politics – this forced engagement in order to win the votes of people necessary for political parties to assume political power. Individuals with a belief in a collective programme knocked on strangers' doors and were willing to engage with them, not on the basis of personal feelings but on what they understood were their potential shared interests. Few people would engage in this type of campaigning today; engaging with people who do not share our views, in an attempt to change their minds, is increasingly anathema and most people would rather share their individual vulnerabilities or express their identities in protest than attempt to argue with a peer.This paper is not intended to be a nostalgic paean to the old world of collective subjects and national interests or a call for a revival of territorial state-based politics or even to reject global aspirations: quite the reverse. Today, politics has been 'freed' from the constraints of territorial political community – governments without coherent policy programmes do not face the constraints of failure or the constraints of the electorate in any meaningful way; activists, without any collective opposition to relate to, are free to choose their causes and ethical identities; protest, from Al Qaeda, to anti-war demonstrations, to the riots in France, is inchoate and atomized. When attempts are made to formally organize opposition, the ephemeral and incoherent character of protest is immediately apparent.

**Legal grey holes not inevitable**

Philip **Alston 11,** John Norton Pomeroy Professor of Law at the NYU School of Law, UN Special Rapporteur on extrajudicial, summary or arbitrary executions from 2004 until 2010, “The CIA and Targeted Killings Beyond Borders,” 2011, 2 Harv. Nat'l Sec. J. 283, lexis nexis

The second problem with Vermeule's approach is the extent to which it **blurs empirical conclusions with normative arguments**. While he never actually states that black or grey holes are normatively desirable, he simply concludes that they are "inevitable" or "unavoidable", and that "decrying their existence is pointless." n558 He situates himself as a realist who is merely observing the reluctance of judges and legislators to scrutinize executive responses to emergencies. The legislators, he says, are "best [\*430] understood as Schmittian lawmakers," n559 while the judges are prudent in not being prepared to shoulder the responsibility of extending the rule of law to emergency situations, even those very broadly defined. n560 Scholars, it seems, are also realists, or at least are equally pusillanimous, since only a handful of them "takes seriously a model of 'global due process.'" n561. But it is done with an air of resignation and pragmatism rather than arguing, as Schmitt would, that it is both inevitable and normatively desirable for the sovereign to enjoy unfettered, dictatorial, powers. It is important to note that the empirical foundation upon which Vermeule bases his analysis is not only rather slight, but also ignores or downplays important examples of cases in which **the courts have in fact pushed back significantly against the executive in relation to conditions of detention and the use of torture**. n562 The results are far from perfect, but they hardly justify the conclusion that black and grey holes are necessarily inevitable.¶ Vermeule seeks to buttress his reliance on this empirical fatalism and his dismissal of "the aspiration to extend legality everywhere . . . [as] hopelessly utopian," n563 by asserting that there is unanimous support among the legal and political elites in the United States that the executive must be able to act illegally:¶ There are too many domains affecting national security in which official opinion holds unanimously, across institutions and partisan lines and throughout the modern era, that executive action must proceed untrammeled by even the threat of legal regulation and judicial review . . . . n564¶ This amounts to a normative argument, but because it is intertwined so carefully with the empirical argument he avoids tackling it head on. Thus, Dyzenhaus's argument for both the importance and feasibility of a common law constitutionalism that upholds the rule of law in the thick sense of vindicating fundamental constitutive principles is never really engaged with directly. Instead, claims of principle are refuted on the basis [\*431] of pragmatic arguments in favor of "hypocritical lip-service" which enables a "veil of decency" n565 to conceal the violations of the law that are being perpetrated and subsequently either overlooked or upheld by the courts. Vermeule concedes that judges could insist upon compliance with the rule of law, but asserts that it is "institutionally impossible for them to do so." n566¶ While Vermeule assiduously avoids any reference to or engagement with either international or foreign law, he invites such engagement when he argues that legal black and grey holes are not a peculiarly American response to the post-9/11 emergency, but rather are "integral to the administrative state," and hence "no legal order governing a massive and massively diverse administrative state can hope to dispense with them." n567 In other words, the United States should not be considered exceptional in this regard. The reality, however, is that almost **all of the principal common law jurisdictions with which the United States can be reasonably be compared (such as Canada, the United Kingdom, and Australia) have, within reasonable limits, respected the rule of law in emergency situations**. Roach has surveyed the extent to which this has been achieved and highlights the crucial role of the right given to states under domestic and international human rights law to derogate from certain rights in the case of emergency. n568 But the difference between Vermeule's approach and the derogation approach is that the latter compels governments to be explicit and open about the derogations, to demonstrate that they fall within specified limits, and to accept that the legality of any derogations is subject to judicial review. The need to spell out the derogation, to notify it publicly, and to be able and prepared to justify it against pre-determined criteria also ensure that the public will be much more involved in the process.

#### 4. No alt to the legal system---causes more abuse

Jerold S. Auerbach 83, Professor of History at Wellesley, “Justice Without Law?”, 1983, p. 144-146

As cynicism about the legal system increases, so does enthusiasm for alternative dispute-settlement institutions. The search for alternatives accelerates, as Richard Abel has suggested, "when some fairly powerful interest is threatened by an increase in the number or magnitude of legal rights.\*'6 Alternatives are designed to provide a safety valve, to siphon discontent from courts. With the danger of political confrontation reduced, the ruling power of legal institutions is preserved, and the stability of the social system reinforced. Not incidentally, alternatives prevent the use of courts for redistributive purposes in the interest of equality, by consigning the rights of disadvantaged citizens to institutions with minimal power to enforce or protect them. It is, therefore, necessary to beware of the seductive appeal of alternative institutions. They may deflect energy from political organization by groups of people with common grievances; or discourage effective litigation strategies that could provide substantial benefits. They may, in the end, create a two-track justice system that dispenses informal "justice" to poor people with "small" claims and "minor" disputes, who cannot afford legal services, and who are denied access to courts. (Bar associations do not recommend that corporate law firms divert their clients to mediation, or that business deductions for legal expenses—a gigantic government subsidy for litigation—be eliminated.) Justice according to law will be reserved for the affluent, hardly a novel development in American history but one that needs little encouragement from the spread of alternative dispute-settlement institutions.¶ It is social context and political choice that determine whether courts, or alternative institutions, can render justice more or less accessible—and to whom. Both can be discretionary, arbitrary, domineering—and unjust. Law can symbolize justice, or conceal repression. It can reduce exploitation, or facilitate it. It can prohibit the abuse of power, or disguise abuse in procedural forms. It can promote equality, or sustain inequality. Despite the resiliency and power of law, it seems unable to eradicate the tension between legality and justice: even in a society of (legal) equals, some still remain more equal than others. But diversion from the legal system is likely to accentuate that inequality. Without legal power the imbalance between aggrieved individuals and corporations, or government agencies, cannot be redressed. In American society, as Laura Nader has observed, "disputing without the force of law ... [is| doomed to fail."7 Instructive examples document the deleterious effect of coerced informality (even if others demonstrate the creative possibilities of indigenous experimentation). Freed slaves after the Civil War and factory workers at the turn of the century, like inner-city poor people now, have all been assigned places in informal proceedings that offer substantially weaker safeguards than law can provide. Legal institutions may not provide equal justice under law, but in a society ruled by law it is their responsibility.¶ It is chimerical to believe that mediation or arbitration can now accomplish what law seems powerless to achieve. The American deification of individual rights requires an accessible legal system/////// for their protection. Understandably, diminished faith in its capacities will encourage the yearning for alternatives. But the rhetoric of "community" and "justice" should not be permitted to conceal the deterioration of community life and the unraveling of substantive notions of justice that has accompanied its demise. There is every reason why the values that historically are associated with informal justice should remain compelling: especially the preference for trust, harmony, and reciprocity within a communal setting. These are not, however, the values that American society encourages or sustains; in their absence there is no effective alternative to legal institutions.¶ The quest for community may indeed be "timeless and universal."8 In this century, however, the communitarian search for justice without law has deteriorated beyond recognition into a stunted off-shoot of the legal system. The historical progression is clear: from community justice without formal legal institutions to the rule of law, all too often without justice. But injustice without law is an even worse possibility, which misguided enthusiasm for alternative dispute settlement now seems likely to encourage. Our legal culture too accurately expresses the individualistic and materialistic values that most Americans deeply cherish to inspire optimism about the imminent restoration of communitarian purpose. For law to be less conspicuous Americans would have to moderate their expansive freedom to compete, to acquire, and to possess, while simultaneously elevating shared responsibilities above individual rights. That is an unlikely prospect unless Americans become, in effect, un-American. Until then, the pursuit of justice without law does incalculable harm to the prospect of equal justice.

5. **Biopower does not result in genocide – it must be combined with racism and sovereign exceptionalism**

Mika **Ojakangas, 2005** - PhD in Social Science and Academy research fellow @ the Helsinki Collegium for Advanced Studies @ University of Helsinki, “The Impossible Dialogue on Biopower: Foucault and Agamben,” May, Foucault Studies, No. 2, http://wlt-studies.com/no2/ojakangas1.pdf

It is the logic of racism, according to Foucault, that makes killing acceptable in modern biopolitical societies. This is not to say, however, that biopolitical societies are necessarily more racist than other societies. It is to say that in the era of biopolitics, only racism, because it is a determination immanent to life, can “justify the murderous function of the State”.89 However, racism can only justify killing – **killing that does not follow from the logic of biopower but from the logic of the sovereign power. Racism is**, in other words, **the only way the sovereign power, the right to kill, can be maintained in biopolitical societies:** “Racism is bound up with workings of a State that is obliged to use race, the elimination of races and the purification of the race, to exercise its sovereign power.”90 Racism is, in other words, a discourse – “quite compatible”91 with biopolitics – through which biopower can be most smoothly transformed into the form of sovereign power. Such transformation, however, changes everything. A biopolitical society that wishes to “exercise the old sovereign right to kill”, even in the name of race, ceases to be a mere biopolitical society, practicing merely biopolitics. It becomes a “demonic combination” of sovereign power and biopower, exercising sovereign means for biopolitical ends. In its most monstrous form, it becomes the Third Reich. For this reason, I cannot subscribe to Agamben’s thesis, according to which biopolitics is absolutized in the Third Reich.93 To be sure, the Third Reich used biopolitical means – it was a state in which “insurance and reassurance were universal”94 – and aimed for biopolitical ends in order to improve the living conditions of the German people -- but so did many other nations in the 1930s. What distinguishes the Third Reich from those other nations is the fact that, alongside its biopolitical apparatus, it erected a massive machinery of death. It became a society that “unleashed murderous power, or in other words, the old sovereign right to take life” throughout the “entire social body”, as Foucault puts it.95 **It is not, therefore, biopolitics that was absolutized in the Third Reic/// – as a matter of fact, biopolitical measures in the Nazi Germany were, although harsh, relatively modest in scale compared to some present day welfare states – but rather the sovereign power: “This power to kill, which ran through the entire social body of Nazi society, was first manifested when the power to take life, the power of life and death, was granted not only to the State but to a whole series of individuals, to a considerable number of people** (such as the SA, the SS, and so on). Ultimately, everyone in the Nazi State had the power of life and death over his or her neighbours, if only because of the practice of informing, which effectively meant doing away with the people next door, or having them done away with.96” **The only thing that the Third Reich actually absolutizes is,** in other words, **the sovereignty of power and therefore, the nakedness of bare life – at least if sovereignty is defined in the Agambenian manner: “The sovereign is the one with respect to whom all men are potentially homines sacri**, and homo sacer is the one with respect to whom all men act as sovereigns.”97

#### 6. Adopting a legal framework doesn’t entail a commitment to legalism. But it provides a framework which is necessary to solve.

Altman, Professor of Philosophy; Georgia State University, 90 (Andrew, Critical Legal Studies: A Liberal Critique, page 8)

In addition, it would be a distortion of liberal theory to suggest that it has no place for nonlegal modes of social regulation, such as mediation. Liberals can and do acknowledge the value of such nonlegal mechanisms in certain social contexts and can consis that the liberal view requires us to recognize that such procedures and rules have a central role to play in resolving fairly and effectively the conflicts that arise in a society characterized by moral, religious, and political pluralism. Thus, the liberal endorsement of legalism does not necessarily involve a commitment to legalism in the sense that Judith Shldar defines the term: “the ethical attitude that holds moral conduct to be a matter of rule following, and moral relationships to consist of duties and rights determined by rules.” Shldar, Legalism (Cambridge: Harvard University Press, 1986), p. 1. Shlclar understands full weli that a commitment to the liberal rule of law does not entail an acceptance of legalism in her sense of the term. See Legalism, pp. xi-xli. And those who reject the rule of law can argue in the political arena for extending the role of such informal mechanisms. Of course, a liberal state could not allow the antinomians to eradicate legal institutions; in that sense, one might say that the liberal rule of law is not neutral. But the kind of political neutrality which the liberal defends does not aim to guarantee that any normative view has an opportunity to remake society wholly in its vision. It does guarantee an opportunity to negotiate and compromise within a framework of individual rights, and there is no reason why those who defend non- legal modes of social regulation cannot seize the opportunity under a liberal regime to carve out a significant role for nonlegal modes of social regulation within the liberal state. The liberal ver sion of political neutrality demands that antinomians have such an opportunity, but there is nothing remotely inconsistent in liberal thought in making that demand or prohibiting antilegalism from going so far as to destroy all legal institution

#### 7. The success of anti-state and anti-imperialism efforts relies on working with the state and legal institutions, the alternative is war and genocide.

Shaw, Professor of International Relations and Politics at the University of Sussex, ’99 (Martin, November 9, “The unfinished global revolution: Intellectuals and the new politics of international relations”

The new politics of international relations require us, therefore, to go beyond the antiimperialism of the intellectual left as well as of the semi-anarchist traditions of the academic discipline. We need to recognise three fundamental truths: First, in the twenty-first century people struggling for democratic liberties across the non-Western world are likely to make constant demands on our solidarity. Courageous academics, students and other intellectuals will be in the forefront of these movements. They deserve the unstinting support of intellectuals in the West. Second, the old international thinking in which democratic movements are seen as purely internal to states no longer carries conviction – despite the lingering nostalgia for it on both the American right and the anti-American left. The idea that global principles can and should be enforced worldwide is firmly established in the minds of hundreds of millions of people. This consciousness will a powerful force in the coming decades. Third, global state-formation is a fact. International institutions are being extended, and they have a symbiotic relation with the major centre of state power, the increasingly internationalised Western conglomerate. The success of the global-democratic revolutionary wave depends first on how well it is consolidated in each national context – but second, on how thoroughly it is embedded in international networks of power, at the centre of which, inescapably, is the West. From these political fundamentals, strategic propositions can be derived. First, democratic movements cannot regard non-governmental organisations and civil society as ends in themselves. They must aim to civilise local states, rendering them open, accountable and pluralistic, and curtail the arbitrary and violent exercise of power. Second, democratising local states is not a separate task from integrating them into global and often Western-centred networks. Reproducing isolated local centres of power carries with it classic dangers of states as centres of war. Embedding global norms and integrating new state centres with global institutional frameworks are essential to the control of violence. (To put this another way, the proliferation of purely national democracies is not a recipe for peace.) Third, while the global revolution cannot do without the West and the UN, neither can it rely on them unconditionally. We need these power networks, but we need to tame them, too, to make their messy bureaucracies enormously more accountable and sensitive to the needs of society worldwide. This will involve the kind of ‘cosmopolitan democracy’ argued for by David Held80 and campaigned for by the new Charter 9981. It will also require us to advance a global social-democratic agenda, to address the literally catastrophic scale of world social inequalities. Fourth, if we need the global-Western state, if we want to democratise it and make its institutions friendlier to global peace and justice, we cannot be indifferent to its strategic debates. It matters to develop robust peacekeeping as a strategic alternative to bombing our way through zones of crisis. It matters that international intervention supports pluralist structures, rather than ratifying Bosnia-style apartheid. Likewise, the internal politics of Western elites matter. It makes a difference to halt the regression to isolationist nationalism in American politics. It matters that the European Union should develop into a democratic polity with a globally responsible direction. It matters that the British state, still a pivot of the Western system of power, stays in the hands of outward-looking new social democrats rather than inward-looking old conservatives. As political intellectuals in the West, we need to have our eyes on the ball at our feet, but we also need to raise them to the horizon. We need to grasp the historic drama that is transforming worldwide relationships between people and state, as well as between state and state. We need to think about how the turbulence of the global revolution can be consolidated in democratic, pluralist, international networks of both social relations and state authority. We cannot be simply optimistic about this prospect. Sadly, it will require repeated violent political crises to push Western governments towards the required restructuring of world institutions.82 What I have outlined tonight is a huge challenge; but the alternative is to see the global revolution splutter into defeat, degenerate into new genocidal wars, perhaps even nuclear conflicts. The practical challenge for all concerned citizens, and the theoretical and analytical challenges for students of international relations and politics, are intertwined.

#### 8. Alt can’t solve – only legal codification can check the executive.

Kleinerman, Ph.D. in Political Science from Michigan State University, 2009 [Benjamin, The Discretionary President: The Promise and Peril of Executive Power, p. 12-13]

In fact, many of the disputes of the past administration revolve around the rightful place of a wide variety of powers. For instance, to some, the president's authorization of the NSA wiretaps was an egregious violation because he seemed to be literally making new law without any input from the branch whose responsibility it is to make the law. Benjamin Wittes, in a much-lauded book called Law and the Long War, argues that much of the problem in the post-9/11 world is that the Bush administration relied all too much on its inherent executive power and failed to place the U.S. response to terrorism on a proper legal footing. Wittes seeks to begin the steps toward a "viable permanent legal architecture for the struggle."46 The goal, he suggests, should be a "legal architecture that grants the president the powers he needs yet also generates the sort of accountability for the use of those powers that might sustain them with long-term public confidence."47 Wittes's argument is both timely and important. To ground the confrontation with terrorism, a president needs more than merely discretionary executive power. Given the permanent and thus nonextraordinary character of a meaningful "war on terror," U.S. citizens cannot and should not simply call on the powers of a discretionary executive. Wittes writes, "Broad presidential war powers are only defensible insofar as they represent a temporary aggrandizement of executive power to handle a crisis." But this "crisis" seems as though it will be a permanent feature of the modern world. To rely on the description of this war as a crisis "is really to describe a permanent state of emergency with a corresponding growth of executive power and a diminution of checks upon it."48¶ But to remain constitutional in this new ordinary, where vast and unthinkable destruction remains a constant possibility, one should not simply seek to place all foreseeable powers that might be necessary on the kind of legal footing Wittes envisions. Again, although one can imagine scenarios in which torture might be necessary, this does not mean that the United States should legalize torture. Instead, its citizens must think through both what powers they should legalize, and by doing so routinize, and what powers they should leave either outside the laws or simply make illegal, thus forcing the executive power, if it wants to so act, to justify the necessity of its action to Congress and the public. But the public can only do this when it has a proper understanding of discretionary executive power and its relation to the legislature.¶ Much of our problem, as I will suggest in later chapters, is that we no longer have an understanding of the separation of powers model that would be so helpful to us in thinking through the proper governmental arrangements in this confrontation with terrorism. For this reason, Wittes's suggestions, depending as they do on an understanding of the difference between the legislative, executive, and judicial functions, end up falling on deaf ears. Wittes suggests, for instance, "If the goal is a long-term, stable set of legal structures for a conflict of indefinite duration against a novel adversary, neither the judiciary nor the executive can ultimately deliver." He continues, "Only Congress can remove the conflict from the paralyzing war-versus-law-enforcement divide and craft for terrorism new legal rules tailored to terrorism's own peculiarities."44 The problem is that public reception of this argument depends on an understanding of the important functional differences in the separation of powers model between the executive, the legislature, and the judiciary.¶ But this notion of the separation of powers, as the founders understood it, tends to elude us. Describing the founders' understanding, Jeffrey Tulis writes, "The term separation of owers has perhaps obstructed understanding of the extent to which afferent structures were designed to give each branch the special quality needed to secure its governmental objectives."5° Each branch has different objectives. The executive aims, first and foremost, at security, or, as Tulis puts it, "self-preservation." Congress aims, first and foremost, at representing the popular will. The courts aim, first and foremost, at protecting rights. Because of each branch's objective, it is structured so as to achieve the virtue most conducive to achieving this function. The legislature requires deliberation. The executive requires energy, And the judiciary requires judgment. Having lost this perspective is a problem not simply or even primarily because we have lost the founders' original intent. As Tulis shows so well in his book The Rhetorical Presidency, the Constitution remains structured so as to achieve, for each branch, its main objective. And, at the same time, the Constitution stands in the way of each branch achieving functions beyond that to which it is assigned. So, in the case of the presidency, the Constitution is structured so that the president can achieve the energy required to preserve security, but it is also structured to prevent what the founders would have viewed as the type of demagogic leadership envisioned by Woodrow Wilson's transformation of the presidency into a rhetorical mouthpiece for the people. Thus, the new expectations for the presidency constantly grind against its constitutional places. Or, as Wittes unwittingly shows, we have not looked to Congress to provide a legal structure for this confrontation with terrorism because we no longer conceive of Congress as the home of deliberation in the regime.52

#### 9. Perm – do the plan and engage in micro-political resistance against sovereign manipulation of law. 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.

# 1AR

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

**Junio ‘13**

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

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

#### Vote aff – That language ensures the oppression of the disabled

Liat Moshe, PhD Student in Sociology, Disability Studies and Women Studies at Syracuse University, 2005, “’Lame Idea: Disabling Language in the Classroom’”, Building Pedagogical Curb Cuts: Incorporating Disability in the University Classroom and Curriculum

As educators, we must bear in mind that disability labels have a history, and that those labels have been highly contested over the decades. These words were actually created to describe people with different abilities as inferior within particular value systems. For instance, the words “moron,” “idiot” and “imbecile” were used throughout the 20th century as medical classifications to denote different levels of intellectual deficiency. Later on, all these terms were conflated under the umbrella of “mental retardation” (Clark & Marsh, 2002). The category of mental retardation, by itself, is highly contested for its reification of all perceived differences in cognitive abilities into one unified category. The important fact here is that mental retardation is a social construction, not a real condition that is innate in people’s minds. The only requirement for inclusion in this category is deviation from a norm (usually prescribed by the use of IQ test) and perceived incompetence. Mental retardation is by itself a linguistic metaphor that means “cognitively delayed.” When used metaphorically in everyday speech, “retarded” stands for slow or underdeveloped thought processes. When we use terms like “retarded,” “lame” or “blind”— even if we are referring to acts or ideas and not to people at all— we perpetuate the stigma associated with disability. By using a 108 “lame idea” 4105-11\_SU 4/1/05 3:50 PM Page 124 label which is commonly associated with disabled people to denote a deficiency, a lack or an ill-conceived notion, **we reproduce the oppression of people with disabilities.** As educators**, we must be aware of the oppressive power of “everyday” language** and try to change it.