# 1AC

**Adv 1 – Arms Race**

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

Jackson 11-8

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

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

#### US posture invites escalating cycles of attacks

Moss 13

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

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

#### Cyber arms race causes world war

CSM 11

Christian Science Monitor

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

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

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

Austin, 8/6

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

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

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

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

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

#### That independently escalates

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

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

### Adv 2 - Alliances

#### Congressional restrictions necessary for allied cooperation

Dunlap 12

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

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

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

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

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

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

Lawson ‘10

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

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

#### Coalition building key to solve 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.**

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

Bradley and Morrison ‘13

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

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

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

Mellor 13

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

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

# 2AC

#### 1. Framework – The affirmative is a normative statement. Vote aff if the plan is a good idea, neg if it is not.

#### A. Aff Choice - Without a negative strategy that engages the aff, we are robbed on 9 minutes of speech time and given no chance to engage the negative.

#### B. Limits – Their discussion explodes the limits in which we are able to debate – response to individualized events in the debate community means that literally every single debate, discussion, and event that has ever happened in the debate community suddenly becomes something the aff is expected to defend.

#### C. Even if fiat is illusory, we believe our discussion about the impacts of cyberwarfare is good. Debate about the repercussions of cyber preemption are key to generating literature on dangers of cyber war, which checks its use

**Magnuson ‘9**

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

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

#### Let’s be clear – WE DO NOT REJECT A DISCUSSION OF STRUCTURAL VIOLENCE and/or RACISM. We just believe that it must respond directly to the affirmative. We don’t say you have to read a DA or a CP. We don’t say that your discussion is inherently bad, we just believe that the affirmative had the plan and the 1AC and some of that should be relevant in the debate

#### 2. Permutation – do both. The lack of a link to the affirmative means that their discussion is not exclusive with the plan. We can respond to the events of the Harvard debate tournament and enact the affirmative plan.

#### 3. WE PROBLEMATIZE THEIR CONCEPT OF the debate COMMUNITY AS A GIVEN TRUTH, AN UNDERSTOOD SITE OF THE POLITICAL. THIS IS THE SAME CONCEPTUALIZATION THAT GIVES WAY TO THE CLOSING OF THE COMMUNITY WE BOTH CRITICIZE. BY GIVING THE COMMUNITY MEANING AND PURPOSE, THEY REPLACE ONE FORM OF VIOLENCE WITH ANOTHER. THE VIOLENCE OF IMMANENCE, OF GOAL-ORIENTED POLITICS, OF PERFERCTION, REPLICATES THE EXCLUSION THEY CITE. THEIR UNWILLINGNESS TO CONFRONT OUR ARGUMENTS IS TESTAMENT TO THE ESSENTIAL NATURE OF OUR ARGUMENT TO THE VERY IDEA OF COMMUNITY.

**noys 2k0**

[benjamin, “georges bataille”, p. 53-56]

He does not offer us a distanced ‘safe’ Nietzsche, but offers us a community with Nietzsche which places us in the greatest danger. Bataille’s generosity is to make Nietzsche a gift to us outside of the appropriations that marked, and still mark, our understanding of Nietzsche. After Bataille Nietzsche’s ‘Grand politics’ are no longer a Nazi or fascist politics but instead new chances for political thought. Bataille’s luck is to have found some of his best readers after his death, readers who can open some of these chances for a thought of ‘Grand politics’. He still catches readers today ‘in sweet, shared slime’ as he failed to catch them during his lifetime. Jean-Luc Nancy is one of these readers, and he has brought out the depth of Bataille’s thought of community and the way that his thought responds to the exigency of community. In *The Inoperative Community (La communauté désceuvrée),24* Nancy has proposed community as a demand that demands to be thought through Bataille. Nancy has also elicited a response from Bataille’s old friend, Maurice Blanchot, and the exchange between them helps to raise the question of community in its most demanding form. Community is not treated by them only as a matter of intellectual debate but as a practical question, a question of how we live and how we die. Bataille is an essential figure in the thinking of community, which is never restricted to a theory opposed to praxis, because as Nancy remarks, ‘No doubt Bataille has gone furthest into the crucial experience of the modem destiny of community.’ Community has been regularly invoked in contemporary politics, and a rhetoric of community has developed: of the decline of community, of the need to renew community, of community standards, and of the rights of communities for self-expression. This rhetoric of community has given rise to strategies for revitalising communities and to the political theory of ‘communitarianism’.26 The tendency in this politics of community is to suppose that we already know what community is and that all that needs to be applied are certain measures to save or restore it. Bataille’s thought of community is a practical interrogation of what is at stake in community, a rethinking of community itself. Therefore, it is perhaps not surprising that neither his work nor that of Nancy is referenced by these contemporary debates, because they would call into question any politics of community which supposes a knowledge of community. It also suggests that the war and the subsequent Cold War did not settle the political debates initiated during the 1930s. Rather than the war violently resolving the political debates between proponents of fascism, democracy and communism, it violently put an end to those debates. The 1930s are not in fact over, in the sense that what was at stake, not least in relation to the question of community, is still to be thought. The continuing turning towards political thinkers of the 1930s, or thinkers who called the political into question, like Carl Schmitt, Martin Heidegger and Georges Bataille, are all indications that we are still living in the long 1930s. Nancy reopens these debates, where community is both a signifier and practice that was powerfully contested, by refusing to read Bataille as something belonging to the past. Instead Nancy finds in Bataille an opening of the thought of community. Not only is it the opening of community but it is also a thinking of community as open, in contrast to contemporary readings of community as relatively closed and static forms. In this way Nancy is maintaining Bataille’s resistance to the unitary conception of community which underpins fascism and, disturbingly enough, which continues to dominate the thought of community (even in some of the most ‘democratic’ or ‘progressive’ thinking of community). Nancy uses Bataille against models of community for which community is closed, where community is thought of as fusion or communion. This is what he calls a immanentism’ because it thinks of community as immanent, present to itself, and so as closed to the outside.27 To think community as immanent has two effects: firstly, it blocks a thinking of the opening that makes communities possible; and secondly, it tries to bring about a purely immanent community and this is an impossibility which leads to the destruction of community: ‘Immanence, communal fusion, contains no other logic than that of the suicide of the community that is governed by it.’28 The Nazi ‘community’ lived out this logic in the suicide of the Führer and the destruction of Germany, but it is implicit in any immanent model of community. In Bataille can be found a thought of community as open: ‘Bataille is without doubt the one who experienced first, or most acutely, the modern experience of community as neither a work to be produced, nor a lost communion, but rather as space itself, and the spacing of the experience of the outside, of the outside-of-self.’ 2’ Bataille does not reduce community to a work to be produced, and he resisted the idea of the ‘labour of the negative’ which is at work in Hegel, Marx and Kojève. Community is not reduced either to a nostalgia for communion, although we have seen how that desire persists in Bataille. In some sense the impossibility of communion animates Bataille’s critical thinking of community, while still remaining in it as a dream. Bataille’s resistance to communion is not only a resistance against fascism but also against contemporary revivals of community, because these revivals suppose that community can be produced rather than being an impossible possibility of an ‘undefined throng of possible existences’ (IE, 61). The lack of a thought of community as open is evident in how these ‘revivals’ of community are all too often accompanied by a resistance to ‘immigrants’ which, it is claimed, would ‘destroy’ or ‘contaminate’ community. Bataille absolutely resists this thought through his rethinking of community. But he also too faces difficulty in conceiving of an open community, and Nancy is a careful enough reader to note the problems of some of Bataille’s formulations of community as communication. Although communication is an act of opening, Bataille’s description of ‘a place of communication, of fusion of the subject and the object’ (lB. 9) can reduce the communication of community. As Nancy notes, ‘The “place of communication” can in the last analysis still be determined as presence-to-self: for example, as the presence-to-self of communication itself, something that would find an echo in certain ideologies of communication.’ 30 Bataille is in danger of taking communication as a moment of fusion where community is produced as present, whereas his own reading of communication is of communication as the interruption and opening of community. This is the impossibility of community as what makes community possible and as that which makes it impossible to achieve communion.

#### 4. THEIR ATTEMPT TO OPERATE WITHIN A SINGULAR POLITICAL SITE (THEIR UNIQUE EXPERIENCES WITH COMMUNITY, YOUR PARTICULAR BALLOT, ETC.) ONLY MIRRORS THE SACRIFICAL LOGIC OF EXCLUSIONARY PRACTICES.

**Isseks 2K3**

[fred, european graduate school candidate for the degree of doctorate of philosophy, “media courage: impossible pedagogy in an artificial community, a dissertation submitted to the division of media and communications, june 2003]

Wernick traces Bataille’s history through the Surrealists and his quest for an “experience of community,” one which he realized was impossible. However, he believed that it was possible to simulate the experience of community through the frenzy that would accompany the sacrifice of one of its members. What he and the members of the Acephale society imagined was a link to the notion of sacrifice that Bataille later developed in his theory of a general economy in The Accursed Share. Sacrifice removes the victim from the “real order of things,” and bestows upon him an “intimacy and anguish,” as he is about to lose his thing-ness, and be consumed profitlessly. It is the sacrifice that removes him - if only for an evening as the feast before the ritual sacrifice takes place – from the degraded world of positivist, utilitarian relationships, and enters him into an exalted state. “It is always the purpose of sacrifice to give destruction its due, to save the rest from a mortal danger of contagion. All those who have to do with sacrifice are in danger, but its limited ritual form regularly has the effect of protecting those who offer it.” The point of sacrifice was to remove something from the chain of thing-ness and profitability, and to share in a communal bond. “Sacrifice is heat, in which the intimacy of those who make up the system of common works is rediscovered. Violence is its principle, but the works limit it in time and space; it is subordinated to the concern for uniting and preserving the commonality. The individuals break loose, but a breaking-loose that melts them and blends them indiscriminately with their fellow beings helps to connect them together in the operations of secular time” (Bataille 59) In this way, sacrifice serves the effect of bringing the sacrificers together in a spirit of commonality, or community, in that it reveals to them their intimate connections with each other. Bataille and the Acephale group plotted such a sacrifice – never realized – as an example of this quest for community, or at least the experience of such a community. “In its ecstatic signs and forms, and above all by living in the imminence of a voluntary human sacrifice, the group would try to realize in itself 140 - non-fusionally, and non-hierarchically - a fully headless, i.e. acephalic, condition” (Wernick). It was in this way that Bataille hoped to bridge that impossible gap between the lone individual on the one hand, and any sense of community with “primal bonds of association,” on the other. Bataille, along with Nancy and others, realized community’s impossibility. Bataille’s contribution to this understanding was to seek the community without a head. As Nancy pointed out, there is no “community of essence,” for such an essence would imply a sacrifice of something. Concrete singularity is usually sacrificed in the name of an abstraction that supposedly pulls community together; or the Other is sacrificed in the name of the One, excluded because it does not fit in. In the case of the Acephale sacrifice, the head is offered up, so that headless, the group is unified without a principle, without a logos, or the imposition of any abstraction or essence on their primal sense of community. In this way, the individual partakes in community, without having his or her freedom negated.

#### 5. Our discussions are good even in their role of the ballot - role playing overcomes preconceived ideological notions and breaks out of traditional pedagogical frameworks by positing students as agents of decision-making

Esberg & Sagan 12

\*Jane Esberg is special assistant to the director at New York University's Center on. International Cooperation. She was the winner of 2009 Firestone Medal, AND \*\*Scott Sagan is a professor of political science and director of Stanford's Center for International Security and Cooperation “NEGOTIATING NONPROLIFERATION: Scholarship, Pedagogy, and Nuclear Weapons Policy,” 2/17 The Nonproliferation Review, 19:1, 95-108

These government or quasi-government think tank simulations often provide very similar lessons for high-level players as are learned by students in educational simulations. Government participants learn about the importance of understanding foreign perspectives, the need to practice internal coordination, and the necessity to compromise and coordinate with other governments in negotiations and crises. During the Cold War, political scientist Robert Mandel noted how crisis exercises and war games forced government officials to overcome ‘‘bureaucratic myopia,’’ moving beyond their normal organizational roles and thinking more creatively about how others might react in a crisis or conflict.6 The skills of imagination and the subsequent ability to predict foreign interests and reactions remain critical for real-world foreign policy makers. For example, simulations of the Iranian nuclear crisis\*held in 2009 and 2010 at the Brookings Institution’s Saban Center and at Harvard University’s Belfer Center, and involving former US senior officials and regional experts\*highlighted the dangers of misunderstanding foreign governments’ preferences and misinterpreting their subsequent behavior. In both simulations, the primary criticism of the US negotiating team lay in a failure to predict accurately how other states, both allies and adversaries, would behave in response to US policy initiatives.7 By university age, students often have a pre-defined view of international affairs, and the literature on simulations in education has long emphasized how such exercises force students to challenge their assumptions about how other governments behave and how their own government works.8 Since simulations became more common as a teaching tool in the late 1950s, educational literature has expounded on their benefits, from encouraging engagement by breaking from the typical lecture format, to improving communication skills, to promoting teamwork.9 More broadly, simulations can deepen understanding by asking students to link fact and theory, providing a context for facts while bringing theory into the realm of practice.10 These exercises are particularly valuable in teaching international affairs for many of the same reasons they are useful for policy makers: they force participants to ‘‘grapple with the issues arising from a world in flux.’’11 Simulations have been used successfully to teach students about such disparate topics as European politics, the Kashmir crisis, and US response to the mass killings in Darfur.12 Role-playing exercises certainly encourage students to learn political and technical facts\* but they learn them in a more active style. Rather than sitting in a classroom and merely receiving knowledge, students actively research ‘‘their’’ government’s positions and actively argue, brief, and negotiate with others.13 Facts can change quickly; simulations teach students how to contextualize and act on information.14

#### 6. The call for the judge to evaluate the debate with a specific “role of the ballot” ignores the complexity of decision-making and demands the judge ignore his/her life experiences and agency

Wordlaw 10 (Wardlaw, Kim McLane, Circuit Judge, United States Court of Appeals for the Ninth Circuit, 2010, “Umpires, Empathy, and Activism: Lessons from Judge Cardozo”, Notre Dame Law Review) FS

Judge Cardozo recognized that the law is not always a strike zone; that the facts of life are not always pitches; and that judges are not always umpires making objective calls between balls and strikes. He acknowledged that there are some areas in which the law is unclear or undeveloped and others in which reasonable jurists will disagree about its proper application to the facts.12 In these areas of the law, where much appellate litigation and most Supreme Court litigation takes place, judges must exercise judgment and discretion. Yet the judge-as-umpire construct, as recently deployed in political debate, fails to recognize the existence of either judgment or discretion. Only after we acknowledge that complications do exist within the law—that the act of judging defies simple metaphors and labels—may we engage in a serious discussion about what should be expected of our judges. Time and again, Judge Cardozo acknowledged that judges should be true to their sense of justice, shaped as it is by their own life experiences. It is as unrealistic as it is unwise to expect our judges to shed their humanity when they don their robes. Life experiences facilitate judges’ ability to appreciate the problems of the people on whose behalf they administer justice. The questions before our courts are too important and too complex to be addressed from a singular vantage point, and it is incumbent upon the judge to understand the views of others. Judge Cardozo’s recognition that one’s life experiences and sentiments of justice come to bear on the act of judging did not, by any means, render him an “activist.” To the contrary, he emphasized that our judges should be modest, ever vigilant of their role as public servants operating within the confines of the constitutional structure of which they share stewardship. He was as honest and candid in discussing his approach to judging as he was restrained in his view of the judge’s role in our democracy. His example undermines the politically popular assertion that empathy and activism are one and the same. “There has been a certain lack of candor,” Judge Cardozo wrote, “in much of the discussion of the theme [of judges’ humanity], or rather perhaps in the refusal to discuss it, as if judges must lose respect and confidence by the reminder that they are subject to human limitations.”13 That a judge is a fellow citizen, whose sense of justice is informed by his life experiences, should be embraced, not ignored—or, worse, chastised—especially when those life experiences facilitate one’s ability to understand the circumstances of others.

#### 7. Removing the judge’s personal agency prevents empathy so perspective-taking becomes impossible

Nielson and Weinberg 12 (Nielson, Laura Beth, Associate Professor of Sociology and Law & Director of Legal Studies at Northwestern, and Weinberg, Jill D., MA from U. Chicago and PhD candidate at Northwestern, 2012, “EXAMINING EMPATHY: DISCRIMINATION, EXPERIENCE, AND JUDICIAL DECISIONMAKING”, Southern California Law Review, Vol. 85:313, <http://weblaw.usc.edu/why/students/orgs/lawreview/documents/SCalLRev85_Weinberg.pdf>) FS

Although judges may decide cases mechanically or politically, the empathetic perspective suggests that judges do not completely abandon their experiences when deciding cases. There are instances in which an individual’s personal background influences how she perceives social situations. As Justice Sotomayor suggests, living in the United States as a Latina tends to include different life experiences, resultant attitudes, and world views. Perhaps as proponents and critics suggest, judges acknowledge the importance of law, yet add life experience resulting from shared kinds of experiences.32 Given this, we contend “empathy” (by which we mean the world views of judges that are formed, at least in part, by the social location they occupy), plays a crucial role in cases that are more emotionally charged and morally consequential, as viewed differently from controversies that are not (e.g., federalism and takings clause matters).33 We believe that empathy and politically motivated decisionmaking are not synonymous, but scholars are quick to conflate the two. The empathethic perspective also comes from the Critical Race Theory tradition, which suggests that a diverse judiciary greatly shapes judicial decisionmaking, legal analysis, and, by extension, the law itself.34 Specifically, judges who hail from different social or cultural backgrounds may provide a more nuanced understanding of facts, evidence, and credibility determinations than judges who lack such experience. While the jurisprudential discourse in this area is significant,35 there has been little empirical work to move beyond the anecdotal or doctrinal accounts. To support this claim, we draw from the extensive literature in psychology that examines the influence of individual background on how individuals respond to questions about the presence or absence of discrimination. While psychologists define empathy in a variety of ways, the general definition suggests that empathy is an emotion that becomes activated by imagining or observing another person’s particular situation.36 Often (but not always), by observing or imagining the other person’s emotions in a particular context, an empathetic response is generated because of “perspective taking.”37 In other words, empathy is a stand-alone emotion, but there can be an element of vicarious emotion as well. Empathy is different from sympathy, in which a person merely imagines the experiences of another. In contrast, a person experiencing empathy is aware and actually sensitive to the state or condition of another.38 Empathy has been shown to have a substantial impact on decisionmaking. For example, previous research shows that individuals who empathize with victims have a greater willingness to help that individual.39 Whether a person is more or less empathetic depends on common membership in a social category or group.40 Often these differences are based on race41 and gender42 categories.

#### 8. Permutation – do the kritik as a first response and then enact the plan. There must come a time where the first response is done, at which point our discussions can continue.

#### 9. Our model of debate is still good - effective deliberation is crucial to the activation of personal agency and is only possible in a switch-side debate format where debaters divorce themselves from ideology to engage in political contestation

Roberts-Miller 3

Patricia Roberts-Miller 3 is Associate Professor of Rhetoric at the University of Texas "Fighting Without Hatred:Hannah Ar endt ' s Agonistic Rhetoric" JAC 22.2 2003

Totalitarianism and the Competitive Space of Agonism¶ Arendt is probably most famous for her analysis of totalitarianism (especially her The Origins of Totalitarianism andEichmann in Jerusa¬lem), but the recent attention has been on her criticism of mass culture (The Human Condition). Arendt's main criticism of the current human condition is that the common world of deliberate and joint action is fragmented into solipsistic and unreflective behavior. In an especially lovely passage, she says that in mass society people are all imprisoned in the subjectivity of their own singular experience, which does not cease to be singular if the same experience is multiplied innumerable times. The end of the common world has come when it is seen only under one aspect and is permitted to present itself in only one perspective. (Human 58)¶ What Arendt so beautifully describes is that isolation and individualism are not corollaries, and may even be antithetical because obsession with one's own self and the particularities of one's life prevents one from engaging in conscious, deliberate, collective action. Individuality, unlike isolation, depends upon a collective with whom one argues in order to direct the common life. Self-obsession, even (especially?) when coupled with isolation from one' s community is far from apolitical; it has political consequences. Perhaps a better way to put it is that it is political precisely because it aspires to be apolitical. This fragmented world in which many people live simultaneously and even similarly but not exactly together is what Arendt calls the "social."¶ Arendt does not mean that group behavior is impossible in the realm of the social, but that social behavior consists "in some way of isolated individuals, incapable of solidarity or mutuality, who abdicate their human capacities and responsibilities to a projected 'they' or 'it,' with disastrous consequences, both for other people and eventually for themselves" (Pitkin 79). One can behave, butnot act. For someone like Arendt, a German-assimilated Jew, one of the most frightening aspects of the Holocaust was the ease with which a people who had not been extraordinarily anti-Semitic could be put to work industriously and efficiently on the genocide of the Jews. And what was striking about the perpetrators of the genocide, ranging from minor functionaries who facilitated the murder transports up to major figures on trial at Nuremberg, was their constant and apparently sincere insistence that they were not responsible. For Arendt, this was not a peculiarity of the German people, but of the current human and heavily bureaucratic condition of twentieth-century culture: we do not consciously choose to engage in life's activities; we drift into them, or we do them out of a desire to conform. Even while we do them, we do not acknowledge an active, willed choice to do them; instead, we attribute our behavior to necessity, and we perceive ourselves as determined—determined by circumstance, by accident, by what "they" tell us to do. We do something from within the anonymity of a mob that we would never do as an individual; we do things for which we will not take responsibility. Yet, whether or not people acknowledge responsibil¬ity for the consequences of their actions, those consequences exist. Refusing to accept responsibility can even make those consequences worse, in that the people who enact the actions in question, because they do not admit their own agency, cannot be persuaded to stop those actions. They are simply doing their jobs. In a totalitarian system, however, everyone is simply doing his or her job; there never seems to be anyone who can explain, defend, and change the policies. Thus, it is, as Arendt says, rule by nobody.¶ It is illustrative to contrast Arendt's attitude toward discourse to Habermas'. While both are critical of modern bureaucratic and totalitar¬ian systems, Arendt's solution is the playful and competitive space of agonism; it is not the rational-critical public sphere. The "actual content of political life" is "the joy and the gratification that arise out of being in company with our peers, out of acting together and appearing in public, out of inserting ourselves into the world by word and deed, thus acquiring and sustaining our personal identity and beginning something entirely new" ("Truth" 263). According to Seyla Benhabib, Arendt's public realm emphasizes the assumption of competition, and it "represents that space of appearances in which moral and political greatness, heroism, and preeminence are revealed, displayed, shared with others. This is a competitive space in which one competes for recognition, precedence, and acclaim" (78). These qualities are displayed, but not entirely for purposes of acclamation; they are not displays of one's self, but of ideas and arguments, of one's thought. When Arendt discusses Socrates' thinking in public, she emphasizes his performance: "He performed in the marketplace the way the flute-player performed at a banquet. It is sheer performance, sheer activity"; nevertheless, it was thinking: "What he actually did was to make public, in discourse, the thinking process" {Lectures 37). Pitkin summarizes this point: "Arendt says that the heroism associated with politics is not the mythical machismo of ancient Greece but something more like the existential leap into action and public exposure" (175-76). Just as it is not machismo, although it does have considerable ego involved, so it is not instrumental rationality; Arendt's discussion of the kinds of discourse involved in public action include myths, stories, and personal narratives.¶ Furthermore, the competition is not ruthless; it does not imply a willingness to triumph at all costs. Instead, it involves something like having such a passion for ideas and politics that one is willing to take risks. One tries to articulate the best argument, propose the best policy, design the best laws, make the best response. This is a risk in that one might lose; advancing an argument means that one must be open to the criticisms others will make of it. The situation is agonistic not because the participants manufacture or seek conflict, but because conflict is a necessary consequence of difference. This attitude is reminiscent of Kenneth Burke, who did not try to find a language free of domination but who instead theorized a way that the very tendency toward hierarchy in language might be used against itself (for more on this argument, see Kastely). Similarly, Arendt does not propose a public realm of neutral, rational beings who escape differences to live in the discourse of universals; she envisions one of different people who argue with passion, vehemence, and integrity.¶ Continued…¶ Eichmann perfectly exemplified what Arendt famously called the "banal¬ity of evil" but that might be better thought of as the bureaucratization of evil (or, as a friend once aptly put it, the evil of banality). That is, he was able to engage in mass murder because he was able not to think about it, especially not from the perspective of the victims, and he was able to exempt himself from personal responsibility by telling himself (and anyone else who would listen) that he was just following orders. It was the bureaucratic system that enabled him to do both. He was not exactly passive; he was, on the contrary, very aggressive in trying to do his duty. He behaved with the "ruthless, competitive exploitation" and "inauthen-tic, self-disparaging conformism" that characterizes those who people totalitarian systems (Pitkin 87).¶ Arendt's theorizing of totalitarianism has been justly noted as one of her strongest contributions to philosophy. She saw that a situation like Nazi Germany is different from the conventional understanding of a tyranny. Pitkin writes,¶ Totalitarianism cannot be understood, like earlier forms of domination, as the ruthless exploitation of some people by others, whether the motive be selfish calculation, irrational passion, or devotion to some cause. Understanding totalitarianism's essential nature requires solving the central mystery of the holocaust—the objectively useless and indeed dysfunctional, fanatical pursuit of a purely ideological policy, a pointless process to which the people enacting it have fallen captive. (87)¶ Totalitarianism is closely connected to bureaucracy; it is oppression by rules, rather than by people who have willfully chosen to establish certain rules. It is the triumph of the social.¶ Critics (both friendly and hostile) have paid considerable attention to Arendt's category of the "social," largely because, despite spending so much time on the notion, Arendt remains vague on certain aspects of it. Pitkin appropriately compares Arendt's concept of the social to the Blob, the type of monster that figured in so many post-war horror movies. That Blob was "an evil monster from outer space, entirely external to and separate from us [that] had fallen upon us intent on debilitating, absorb¬ing, and ultimately destroying us, gobbling up our distinct individuality and turning us into robots that mechanically serve its purposes" (4).¶ Pitkin is critical of this version of the "social" and suggests that Arendt meant (or perhaps should have meant) something much more complicated. The simplistic version of the social-as-Blob can itself be an instance of Blob thinking; Pitkin's criticism is that Arendt talks at times as though the social comes from outside of us and has fallen upon us, turning us into robots. Yet, Arendt's major criticism of the social is that it involves seeing ourselves as victimized by something that comes from outside our own behavior. I agree with Pitkin that Arendt's most powerful descriptions of the social (and the other concepts similar to it, such as her discussion of totalitarianism, imperialism, Eichmann, and parvenus) emphasize that these processes are not entirely out of our control but that they happen to us when, and because, we keep refusing to make active choices. We create the social through negligence. It is not the sort of force in a Sorcerer's Apprentice, which once let loose cannot be stopped; on the contrary, it continues to exist because we structure our world to reward social behavior. Pitkin writes, "From childhood on, in virtually all our institutions, we reward euphemism, salesmanship, slo¬gans, and we punish and suppress truth-telling, originality, thoughtful-ness. So we continually cultivate ways of (not) thinking that induce the social" (274). I want to emphasize this point, as it is important for thinking about criticisms of some forms of the social construction of knowledge: denying our own agency is what enables the social to thrive. To put it another way, theories of powerlessness are self-fulfilling prophecies.¶ Arendt grants that there are people who willed the Holocaust, but she insists that totalitarian systems result not so much from the Hitlers or Stalins as from the bureaucrats who may or may not agree with the established ideology but who enforce the rules for no stronger motive than a desire to avoid trouble with their superiors (see Eichmann and Life). They do not think about what they do. One might prevent such occurrences—or, at least, resist the modern tendency toward totalitarian¬ism—by thought: "critical thought is in principle anti-authoritarian" (Lectures 38).¶ By "thought" Arendt does not mean eremitic contemplation; in fact, she has great contempt for what she calls "professional thinkers," refusing herself to become a philosopher or to call her work philosophy. Young-Bruehl, Benhabib, and Pitkin have each said that Heidegger represented just such a professional thinker for Arendt, and his embrace of Nazism epitomized the genuine dangers such "thinking" can pose (see Arendt's "Heidegger"). "Thinking" is not typified by the isolated con¬templation of philosophers; it requires the arguments of others and close attention to the truth. It is easy to overstate either part of that harmony. One must consider carefully the arguments and viewpoints of others:¶ Political thought is representative. I form an opinion by considering a given issue from different viewpoints, by making present to my mind the standpoints of those who are absent; that is, I represent them. This process of representation does not blindly adopt the actual views of those who stand somewhere else, and hence look upon the world from a different perspective; this is a question neither of empathy, as though I tried to be or to feel like somebody else, nor of counting noses and joining a majority but of being and thinking in my own identity where actually I am not. The more people's standpoints I have present in my mind while I am ponder¬ing a given issue, and the better I can imagine how I would feel and think if I were in their place, the stronger will be my capacity for represen¬tative thinking and the more valid my final conclusions, my opinion. ("Truth" 241)¶ There are two points to emphasize in this wonderful passage. First, one does not get these standpoints in one's mind through imagining them, but through listening to them; thus, good thinking requires that one hear the arguments of other people. Hence, as Arendt says, "critical thinking, while still a solitary business, does not cut itself off from' all others.'" Thinking is, in this view, necessarily public discourse: critical thinking is possible "only where the standpoints of all others are open to inspection" (Lectures 43). Yet, it is not a discourse in which one simply announces one's stance; participants are interlocutors and not just speakers; they must listen. Unlike many current versions of public discourse, this view presumes that speech matters. It is not asymmetric manipulation of others, nor merely an economic exchange; it must be a world into which one enters and by which one might be changed.¶ Second, passages like the above make some readers think that Arendt puts too much faith in discourse and too little in truth (see Habermas). But Arendt is no crude relativist; she believes in truth, and she believes that there are facts that can be more or less distorted. She does not believe that reality is constructed by discourse, or that truth is indistinguishable from falsehood. She insists tha^ the truth has a different pull on us and, consequently, that it has a difficult place in the world of the political. Facts are different from falsehood because, while they can be distorted or denied, especially when they are inconvenient for the powerful, they also have a certain positive force that falsehood lacks: "Truth, though powerless and always defe ated in a head-on clash with the powers that be, possesses a strength of its own: whatever those in power may contrive, they are unable to discover or invent a viable substitute for it. Persuasion and violence can destroy truth, but they cannot replace it" ("Truth" 259).¶ Facts have a strangely resilient quality partially because a lie "tears, as it were, a hole in the fabric of factuality. As every historian knows, one can spot a lie by noticing incongruities, holes, or the j unctures of patched-up places" ("Truth" 253). While she is sometimes discouraging about our ability to see the tears in the fabric, citing the capacity of totalitarian governments to create the whole cloth (see "Truth" 252-54), she is also sometimes optimistic. InEichmann in Jerusalem, she repeats the story of Anton Schmidt—a man who saved the lives of Jews—and concludes that such stories cannot be silenced (230-32). For facts to exert power in the common world, however, these stories must be told. Rational truth (such as principles of mathematics) might be perceptible and demonstrable through individual contemplation, but "factual truth, on the contrary, is always related to other people: it concerns events and circumstances in which many are involved; it is established by witnesses and depends upon testimony; it exists only to the extent that it is spoken about, even if it occurs in the domain of privacy. It is political by nature" (23 8). Arendt is neither a positivist who posits an autonomous individual who can correctly perceive truth, nor a relativist who positively asserts the inherent relativism of all perception. Her description of how truth functions does not fall anywhere in the three-part expeditio so prevalent in bothrhetoric and philosophy: it is not expressivist, positivist, or social constructivist. Good thinking depends upon good public argument, and good public argument depends upon access to facts: "Freedom of opinion is a farce unless factual information is guaranteed" (238).¶ The sort of thinking that Arendt propounds takes the form of action only when it is public argument, and, as such, it is particularly precious: "For if no other test but the experience of being active, no other measure but the extent of sheer activity were to be applied to the various activities within the vita activa, it might well be that thinking as such would surpass them all" (Human 325). Arendt insists that it is "the same general rule— Do not contradict yourself (not your self but your thinking ego)—that determines both thinking and acting" (Lectures 3 7). In place of the mildly resentful conformism that fuels totalitarianism, Arendt proposes what Pitkin calls "a tough-minded, open-eyed readiness to perceive and judge reality for oneself, in terms of concrete experience and independent, critical theorizing" (274). The paradoxical nature of agonism (that it must involve both individuality and commonality) makes it difficult to maintain, as the temptation is great either to think one's own thoughts without reference to anyone else or to let others do one's thinking.¶ Arendt's Polemical Agonism¶ As I said, agonism does have its advocates within rhetoric—Burke, Ong, Sloane, Gage, and Jarratt, for instance—but while each of these theorists proposes a form of conflictual argument, not one of these is as adversarial as Arendt's. Agonism can emphasize persuasion, as does John Gage's textbook The Shape of Reason or William Brandt et al.'s The Craft of Writing. That is, the goal of the argument is to identify the disagreement and then construct a text that gains the assent of the audience. This is not the same as what Gage (citing Thomas Conley) calls "asymmetrical theories of rhetoric": theories that "presuppose an active speaker and a passive audience, a speaker whose rhetorical task is therefore to do something to that audience" ("Reasoned" 6). Asymmetric rhetoric is not and cannot be agonistic. Persuasive agonism still values conflict, disagreement, and equality among interlocutors, but it has the goal of reaching agreement, as when Gage says that the process of argument should enable one's reasons to be "understood and believed" by others (Shape 5; emphasis added).¶ Arendt's version is what one might call polemical agonism: it puts less emphasis on gaining assent, and it is exemplified both in Arendt's own writing and in Donald Lazere's "Ground Rules for Polemicists" and "Teaching the Political Conflicts." Both forms of agonism (persuasive and polemical) require substantive debate at two points in a long and recursive process. First, one engages in debate in order to invent one's argument; even silent thinking is a "dialogue of myself with myself (Lectures 40). The difference between the two approaches to agonism is clearest when one presents an argument to an audience assumed to be an opposition. In persuasive agonism, one plays down conflict and moves through reasons to try to persuade one's audience. In polemical agonism, however, one's intention is not necessarily to prove one's case, but to make public one' s thought in order to test it. In this way, communicability serves the same function in philosophy that replicability serves in the sciences; it is how one tests the validity of one's thought. In persuasive agonism, success is achieved through persuasion; in polemical agonism, success may be marked through the quality of subsequent controversy.¶ Arendt quotes from a letter Kant wrote on this point:¶ You know that I do not approach reasonable objections with the intention merely of refuting them, but that in thinking them over I always weave them into my judgments, and afford them the opportunity of overturning all my most cherished beliefs. I entertain the hope that by thus viewing my judgments impartially from the standpoint of others some third view that will improve upon my previous insight may be obtainable. {Lectures 42)¶ Kant's use of "impartial" here is interesting: he is not describing a stance that is free of all perspective; it is impartial only in the sense that it is not his own view. This is the same way that Arendt uses the term; she does not advocate any kind of positivistic rationality, but instead a "universal interdependence" ("Truth" 242). She does not place the origin of the "disinterested pursuit of truth" in science, but at "the moment when Homer chose to sing the deeds of the Trojans no less than those of the Achaeans, and to praise the glory of Hector, the foe and the defeated man, no less than the glory of Achilles, the hero of his kinfolk" ("Truth" 262¬63). It is useful to note that Arendt tends not to use the term "universal," opting more often for "common," by which she means both what is shared and what is ordinary, a usage that evades many of the problems associated with universalism while preserving its virtues (for a brief butprovocative application of Arendt's notion of common, see Hauser 100-03).¶ In polemical agonism, there is a sense in which one' s main goal is not to persuade one's readers; persuading one's readers, if this means that they fail to see errors and flaws in one' s argument, might actually be a sort of failure. It means that one wishes to put forward an argument that makes clear what one's stance is and why one holds it, but with the intention of provoking critique and counterargument. Arendt describes Kant's "hope" for his writings not that the number of people who agree with him would increase but "that the circle of his examiners would gradually be en¬larged" {Lectures 39); he wanted interlocutors, not acolytes.¶ This is not consensus-based argument, nor is it what is sometimes called "consociational argument," nor is this argument as mediation or conflict resolution. Arendt (and her commentators) use the term "fight," and they mean it. When Arendt describes the values that are necessary in our world, she says, "They are a sense of honor, desire for fame and glory, the spirit of fighting without hatred and 'without the spirit of revenge,' and indifference to material advantages" {Crises 167). Pitkin summarizes Arendt's argument: "Free citizenship presupposes the ability to fight— openly, seriously, with commitment, and about things that really mat¬ter—without fanaticism, without seeking to exterminate one's oppo¬nents" (266). My point here is two-fold: first, there is not a simple binary opposition between persuasive discourse and eristic discourse, the conflictual versus the collaborative, or argument as opposed to debate.¶ Second, while polemical agonismrequires diversity among interlocutors, and thus seems an extraordinarily appropriate notion, and while it may be a useful corrective to too much emphasis on persuasion, it seems to me that polemical agonism could easily slide into the kind of wrangling that is simply frustrating. Arendt does not describe just how one is to keep the conflict useful. Although she rejects the notion that politics is "no more than a battlefield of partial, conflicting interests, where nothing countfs] but pleasure and profit, partisanship, and the lust for dominion," she does not say exactly how we are to know when we are engaging in the existential leap of argument versus when we are lusting for dominion ("Truth" 263).¶ Like other proponents of agonism, Arendt argues that rhetoric does not lead individuals or communities to ultimate Truth; it leads to decisions that will necessarily have to be reconsidered. Even Arendt, who tends to express a greater faith than many agonists (such as Burke, Sloane, or Kastely) in the ability of individuals to perceive truth, insists that self-deception is always a danger, so public discourse is necessary as a form of testing (see especially Lectures and "Truth"). She remarks that it is difficult to think beyond one's self-interest and that "nothing, indeed, is more common, even among highly sophisticated people, than the blind obstinacy that becomes manifest in lack of imagination and failure to judge" ("Truth" 242).¶ Agonism demands that one simultaneously trust and doubt one' s own perceptions, rely on one's own judgment and consider the judgments of others, think for oneself and imagine how others think. The question remains whether this is a kind of thought in which everyone can engage. Is the agonistic public sphere (whether political, academic, or scientific) only available to the few? Benhabib puts this criticism in the form of a question: "That is, is the 'recovery of the public space' under conditions of modernity necessarily an elitist and antidemocratic project that can hardly be reconciled with the demand for universal political emancipa¬tion and the universal extension of citizenship rights that have accompa¬nied modernity since the American and French Revolutions?" (75). This is an especially troubling question not only because Arendt's examples of agonistic rhetoric are from elitist cultures, but also because of com¬ments she makes, such as this one from The Human Condition: "As a living experience, thought has always been assumed, perhaps wrongly, to be known only to the few. It may not be presumptuous to believe that these few have not become fewer in our time" {Human 324).¶ Yet, there are important positive political consequences of agonism.¶ Arendt' s own promotion of the agonistic sphere helps to explain how the system could be actively moral. It is not an overstatement to say that a central theme in Arendt's work is the evil of conformity—the fact that the modern bureaucratic state makes possible extraordinary evil carried out by people who do not even have any ill will toward their victims. It does so by "imposing innumerable and various rules, all of which tend to 'normalize' its members, to make them behave, to exclude spontaneous action or outstanding achievement" (Human 40). It keeps people from thinking, and it keeps them behaving. The agonistic model's celebration of achievement and verbal skill undermines the political force of conformity, so it is a force against the bureaucratizing of evil. If people think for themselves, they will resist dogma; if people think of themselves as one of many, they will empathize; if people can do both, they will resist totalitarianism. And if they talk about what they see, tell their stories, argue about their perceptions, and listen to one another—that is, engage in rhetoric—then they are engaging in antitotalitarian action.¶ In post-Ramistic rhetoric, it is a convention to have a thesis, and one might well wonder just what mine is—whether I am arguing for or against Arendt's agonism. Arendt does not lay out a pedagogy for us to follow (although one might argue that, if she had, it would lookmuch like the one Lazere describes in "Teaching"), so I am not claiming that greater attention to Arendt would untangle various pedagogical problems that teachers of writing face. Nor am I claiming that applying Arendt's views will resolve theoretical arguments that occupy scholarly journals. I am saying, on the one hand, that Arendt's connection of argument and thinking, as well as her perception that both serve to thwart totalitarian¬ism, suggest that agonal rhetoric (despite the current preference for collaborative rhetoric) is the best discourse for a diverse and inclusive public sphere. On the other hand, Arendt's advocacy of agonal rhetoric is troubling (and, given her own admiration for Kant, this may be intentional), especially in regard to its potential elitism, masculinism, failure to describe just how to keep argument from collapsing into wrangling, and apparently cheerful acceptance of hierarchy. Even with these flaws, Arendt describes something we would do well to consider thoughtfully: a fact-based but not positivist, communally grounded but not relativist, adversarial but not violent, independent but not expressivist rhetoric.

#### 10. Permutation – do the plan and then begin our discussion of a first response.

#### 11. We need not address concerns like prescribing a new metaphysics, politics, set of standards, whatever; our flea from their WILL TO ORDER IS PROFICIENT.

**strysick 97**

[michael, “the end of community and the politic of grammar”, cultural critique, p.195-215]

Community gains nothing from attempting to build and rebuild immanent, avowable empires. Violence is at the root of the immanent mentality; its manifest destiny razes what it will, creating endless trails of tears. Incredulity confronts the immanent with itself, mirroring it in order to undo power, not usurp it. But this entails a change in foundation, in what Nietzsche refers to as grammar. Unless foundations change, what arises from them will not change demonstrably. Rather, we must engage a task to expose totalizing gestures within community. This is the approach that community's altered politics (la politique), by virtue of a new orientation of the political (le politique), must engage. And this approach marks not merely incredulity to metanarratives, but more importantly, incredulity toward the lingering shadow of the grammar of metanarratives. How will this grammar be broken? The importance of undoing this mentality arises not out of any search for truth, any metaphysical quest, or any religious pilgrimage; rather, it arises from the need for justice as manifest equality. Unavowability itself defines a horizontal community. In the process, difference-on which avowability and inequality has for so long been based-is not erased but rather becomes the greatest challenge. Thus, it requires a radical shift, an overturning of a prevailing mentality that prefers the one to the many, or even the many as mediated through the one. The challenge is to work to understand the many in terms of the many, mediated only by itself. But how could such radical changes take place? Who would take charge of this? Again, even asking the question in this manner belies the point to which empire is embedded in our very thinking, specifically if we seek to answer it through the concept of leaders and followers. Community need not shrink the world to a handful but enlarge it to the many. Rather than scheming about and theorizing on how to achieve such a horizontal structure, it is best to simply undo those vertical elements when they appear. Rather than describing an end point to be reached, with a specific program to that end, we can describe a point from which we wish to flee. Community has endured codes, laws, and plans promising paradise, redemption, and salvation; now, we must conceive of practical ways to move further away from self-created states of emergency. Such a notion of community will not be achieved by some revisionist undoing of past documents but by a real undoing of past practices- incredulity in its strongest form. After all, we cannot change the past, but we need not be anchored in its mistakes nor chained to its insensitivities. We need go no further in thinking about undoing the grammar of community than Lyotard's first word in defining postmodernism: incredulity. Lyotard's term describes not merely a lack of belief, but even more, a lack of faith: an inability to invest trust in those past creeds and faiths that have preferred the homogeneous and total at the expense of difference and our shared elective affinities. Now, we must be motivated to create new myths in order to reinvest the notion of credibility. The relationship to the past is characterized purely by the necessity of rethinking and restating what has been said. But the post, while commenting on the past by naming a "post”-also relates to the future, saying not only that we have lost faith in the past but also its modus operandi. At once, all three tenses are brought into play: at present, in large part because of the past, we do not know what to do in the future, into which we are forever propelled. Of course, progress is called into question in the process-Walter Benjamin states this so eloquently in his "Theses on the Philosophy of History." Despite the passage of time we are no better equipped to avoid the so-called state of emergency in which we persist nor to repair it nor to quell the storm blowing us further away from paradise. The continued proliferation of voices and visions in society, and concomitant ways of hearing and seeing those imaginings, have engaged the slow death of community by challenging its grammar. New ends-stressing the plural over and against the singular, the total-are emerging, though perhaps very slowly. The degree to which they succeed will depend on the ability to undo totality and its grammar such that our differences alone are held in common, affinities are as important as facts, and our discourse marks this alterity. An altered grammar, thus, directs itself toward nothing less than an expression of the inability to speak for all, an acknowledgment of the unspeakable manner in which we have tried to form and enforce such totalizing narratives, and an awareness of the ultimate demand that we speak and think otherwise. Change can occur but only to the degree that community begins to mark its end as not simply recognizing and allowing "other" voices to speak, and at the point when the grammar of the same and the bias of homogeneity is broken. This will only occur at the moment when we begin to realize that all are "other" and none are the same.

#### 12Now, their argument is that we must discuss our relationship to the events at Harvard. There is no brightline for how much we must do that. Personally, Thayer and I were not at Harvard, we were only able to keep up on what was happening via the NDT/CEDA facebook page. Of course, that doesn’t mean that we weren’t affected by it. Myself, as a freshman, it was the first big thing that I experienced. I was confused, sad, angry, and nervous. I was upset that the community I love so much was so angry.