**1AC**

### 1AC — Cyber War

#### Contention one is Cyber War:

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

**Goldman 13**, CNN Writer, Nations Prepare for Cyberwar, <http://money.cnn.com/2013/01/07/technology/security/cyber-war/index.html>

Security analysts are predicting that 2013 is when nation-sponsored cyberwarfare goes mainstream -- and some think such attacks will lead to actual deaths. In 2012, large-scale cyberattacks targeted at the Iranian government were uncovered, and in return, Iran is believed to have launched [massive attacks aimed at U.S. banks](http://money.cnn.com/2012/11/05/technology/security/iran-cyberattack/index.html?iid=EL) and Saudi oil companies. At least 12 of the **world's** 15 largest military powers are **currently** building cyberwarfare programs, according to James Lewis, a cybersecurity expert at the Center for Strategic and International Studies. So a [cyber Cold War](http://money.cnn.com/2011/07/28/technology/government_hackers/index.htm?iid=EL) is already in progress. But some security companies believe that battle will become even more heated this year. "Nation states and armies will be more frequent actors and victims of cyberthreats," a team of researchers at McAfee Labs, an Intel ([INTC](http://money.cnn.com/quote/quote.html?symb=INTC&source=story_quote_link), [Fortune 500](http://money.cnn.com/magazines/fortune/fortune500/2012/snapshots/642.html?iid=EL))subsidiary, wrote in a [recent report](http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf" \t "_blank). Michael Sutton, head of security research at cloud security company [Zscaler](http://www.zscaler.com/" \t "_blank), said he expects governments to spend furiously on building up their cyber arsenals. Some may even outsource attacks to online hackers. The Obama administration and many in Congress have been [more vocal](http://money.cnn.com/2012/04/27/technology/cispa-cybersecurity/index.htm?iid=EL) about how an enemy nation or a terrorist cell could target the country's critical infrastructure in a cyberattack. Banks, stock exchanges, nuclear power plants and water purification systems are particularly vulnerable, according to numerous assessments delivered to Congress last year.

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

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

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

#### Cyber arms race causes world war — there are no checks on escalation, deterrence doesn’t apply, and only a certain commitment to the plan solves

CSM 11, Christian Science Monitor

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

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

#### Congressional OCO oversight is key to stop the arms race — otherwise nuclear war is inevitable from arms-racing, command and control hacking, crisis instability, and fracturing nuclear agreements

**Austin, 8/6, Director of Policy Innovation at the EastWest Institute**, Costs of American Cyber Superiority, <http://www.chinausfocus.com/peace-security/costs-of-american-cyber-superiority/>

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

#### The mere perception of Presidential control of OCOs fuels foreign uncertainty – that causes extinction

**Rothschild 13**, Editor of Progressive Magazine, Matthew Rothschild is the editor of The Progressive magazine, which is one of the leading voices for peace and social justice in this country. Rothschild has appeared on Nightline, C-SPAN, The O'Reilly Factor, and NPR, and his newspaper commentaries have run in the Chicago Tribune, the L.A. Times, the Miami Herald, and a host of other newspapers. Rothschild is the host of "[Progressive Radio](http://www.progressive.org/progressive_radio)," a syndicated half-hour weekly interview program. And he does a two-minute daily radio commentary, entitled "[Progressive Point of View](http://www.progressive.org/progressive_pov)," which is also syndicated around the country. Rothschild is the author of You Have No Rights: Stories of America in an Age of Repression (New Press, 2007). He also is the editor ofDemocracy in Print: The Best of The Progressive, 1909-2009(University of Wisconsin Press, 2009)., The Dangers of Obama’s Cyber War Power Grab, <http://progressive.org/dangers-of-obama-cyber-war-power-grab>

There are no checks or balances when the President, alone, decides when to engage in an act of war. And this new aggressive stance will lead to a cyber arms race. The United States has evidently already used cyber weapons against Iran, and so many other countries will assume that cyber warfare is an acceptable tool and will try to use it themselves. Most troubling, U.S. cybersupremacy—and that is Pentagon doctrine—will also raise fears among nuclear powers like Russia, China, and North Korea that the United States may use a cyberattack as the opening move in a nuclear attack. For if the United States can knock out the command and control structure of an enemy’s nuclear arsenal, it can then launch an all-out nuclear attack on that enemy with impunity. This would make such nuclear powers more ready to launch their nuclear weapons preemptively for fear that they would be rendered useless. So we’ve just moved a little closer to midnight. Now, I don’t think Obama would use cyberwarfare as a first strike in a nuclear war. But our adversaries may not be so sure, either about Obama or his successors. They, too, worry about the temptations of a President.

#### **Guaranteed to escalate –**

#### **Misperceptions**

Rosenzweig 9, Professor at Georgetown Law

(Paul, founder of Reid Branch Consulting, specializing in homeland security, senior advisor to the Chertoff Group, Carnegie Fellow at Northwestern, professor at National Defense University, Editorial board at the Journal of National Security Law & Policy, deputy assistant secretary for policy at the US Department of Homeland Security, "National Security Threatsin Cyberspace" merican Bar Association Standing Committee on Law andNational Security And National Strategy Forum, September 2009, [www.utexas.edu/law/journals/tlr/sources/Issue%2088.7/Jensen/fn137.Rosenwieg.pdf](http://www.utexas.edu/law/journals/tlr/sources/Issue%2088.7/Jensen/fn137.Rosenwieg.pdf))

Offensive dominance creates a great risk of cyber arms races. State and non-state actors are likely to view the prevalence of offensive cyber threats as a legitimate rationale for bolstering their own capabilities, both defensive and offensive, thus fueling an action-reaction dynamic of iterative arming. Experts believe that at least 20 nations are engaged in a cyber arms competition and possess the type of advanced capabilities needed to wage cyber war against the United States.121 As Michael Nacht, Former Assistant Secretary of Defense for Global Strategic Affairs, told us, “An arms race is already going on in cyberspace and it is very intense.”122 Conflict in cyberspace is uniquely predisposed to escalation given uncertainties about what constitutes an act of war and the growing number of state and non-state actors seeking offensive capabilities. Actors are more likely to misperceive or miscalculate actions in cyberspace, where there is no widely understood strategic language for signaling intent, capability and resolve.123 Uncertainty will encourage states to prepare for worst-case contingencies, a condition that could fuel escalation. Furthermore, “false flag” attacks, in which an actor purposefully makes an attack look like it came from a third party, could also ignite a conflict.124

#### **Disproportionality**

Sanger 9

(David E., “U.S. Steps Up Effort on Digital Defenses” April 27, 2009, <http://www.nytimes.com/2009/04/28/us/28cyber.html?pagewanted=all&_r=0>)

In the rare case where the preparations for an attack are detected in a foreign computer system, there is continuing debate about whether to embrace the concept of pre-emption, with all of its Bush-era connotations. The questions range from whether an online attack should be mounted on that system to, in an extreme case, blowing those computers up. Some officials argue that if the United States engaged in such pre-emption — and demonstrated that it was watching the development of hostile cyberweapons — it could begin to deter some attacks. Others believe it will only justify pre-emptive attacks on the United States. “Russia and China have lots of nationalistic hackers,” one senior military officer said. “They seem very, very willing to take action on their own.” Senior Pentagon and military officials also express deep concern that the laws and understanding of armed conflict have not kept current with the challenges of offensive cyberwarfare. Over the decades, a number of limits on action have been accepted — if not always practiced. One is the prohibition against assassinating government leaders. Another is avoiding attacks aimed at civilians. Yet in the cyberworld, where the most vulnerable targets are civilian, there are no such rules or understandings. If a military base is attacked, would it be a proportional, legitimate response to bring down the attacker’s power grid if that would also shut down its hospital systems, its air traffic control system or its banking system? “We don’t have that for cyber yet,” one senior Defense Department official said, “and that’s a little bit dangerous.”

#### c) Instant timeframe

**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 other ways, cyber weapons are critically different from their nuclear counterparts. For one thing, the time frame for response to a cyber attack might be much narrower. A nuclear weapon delivered by a land-based ICBM could take 30 minutes to reach its target. An electronic attack would arrive instantaneously, and leave no time to consult with or even inform anyone outside the executive branch before launching a counterstrike, if that were U.S. policy.

### 1AC – Alliances

**Contention 2 is alliances**

#### **Congressional oversight necessary for allied credibility— restoring legitimacy to OCOs is key to cyber coalitions**

Dunlap 12, **Major General and Former Deputy Judge Advocate General**

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

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

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

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

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

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

#### 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 United States 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 catastrophicmistake. 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 — it’s the most probable

**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 Chinese Communist Party 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.

#### North Korea collapse inevitable – causes global nuclear war

Gompert 13, Senior Fellow at the RAND Corporation and Distinguished Visiting Professor at the United States Naval Academy

(David C., He was Principal Deputy Director of National Intelligence in the first Obama administration, and has served as a senior official in several prior administrations and as a senior business executive, “North Korea: Preparing for the End” Survival, Vol. 55 No. 3, July 2013, http://dx.doi.org/10.1080/00396338.2013.802849)

In considering scenarios for collapse, one place to start is with food – or rather, the lack of it. One possibility is of widespread starvation, owing to further failure of harvests and distribution (fuel also being scarce). This could lead to a meltdown of social order that the regime is incapable of addressing, with or without its standard brutality.6 Even military units are said to be underfed, suggesting that the armed forces would not be spared starvation and might be more concerned with eating than fighting in the event of a breakdown of order.7 If the North Korean food situation worsens, the military as a whole or units of it might move against the regime or else fragment, leaving vulnerable a state that depends vitally on a monopoly of armed force. Even now, North Korean President Kim Jong Un probably cannot fully count on military leaders, which helps explain his attempts to retain their loyalty by looking tough.8 Another possibility, not exclusive of the first, is that the state’s institutions become overwhelmed by the mounting problems they face, and that the political leadership is incapable of issuing useful, realistic direction. Key economic, administrative, judicial and security personnel – perhaps scapegoated and in danger – could flee the country, leaving a shrinking regime effectively ~~paralysed~~ and what is left of North Korean society dissolving, as individuals and bands fare for themselves. Such governmental organ failure would be especially catastrophic for a country that has known only central command. In either scenario (or others one can imagine), an accelerating and compounding deterioration of material and human conditions, declining capacity of the state to cope, and splintering of military and security forces and discipline would combine in a downward spiral. Although most North Koreans already live in wretched conditions, their remarkable resilience, or docility, is no guarantee of future stability. Growing scarcities of food, shelter, sanitation, basic medical care and public safety could cause violence, especially if military cohesion gives way.9 In the event of such a breakdown, the North Korean state’s isolation, intransigence and incompetence would impede large-scale international relief, just as violence would endanger those who would deliver such relief.10 Even if the outside world chose to mount large-scale emergency relief, the state itself, while collapsing, might remain dangerous and opposed to intrusion, especially involving foreign troops. In such dynamics, the North would descend into chaos: people foraging, fighting and fleeing; military and other security forces uncontrolled and scrambling for spoils; chemical, biological and nuclear stockpiles insecure; what’s left of the government – the Kim family and the generals and civilians around them – fractured and panicked. The premise of such scenarios is that North Korea is in important respects a failing state, which might seem to be at odds with its obsessively tight control. One model to predict state failure consists of three conditions: a poor and contracting economy, incompetent and corrupt government, and internal violence.11 North Korea meets the first two conditions: apart from its brutality, the regime is ineffective; the decline in its economy is evidenced in the steady erosion of GDP per capita (which resembles that of Somalia, Liberia or Haiti in comparable periods). At the same time, violence is not rampant, apart from abuse by security forces. But in circumstances like those described here, further economic and political deterioration could lead to disorder and bloodshed by and against the government. At that point, the regime’s control of the country’s territory and population – the last stop before state failure – would give way. We tend not to equate failing states with aggressive ones. But in the North Korean case, paradoxically, the regime could get more dangerous as its prospects worsen and its grip weakens. Given that the latest round of North Korean external misconduct can be traced to internal anxiety, it is not unreasonable to project even more menacing behaviour if the regime loses control. Assuming that a badly wounded North Korean state would merely bark is false comfort that ignores its core nature and instinct to bite. If facing extinction, the regime and whatever forces it still commanded might resort to violence against their enemies. As material and political conditions grow even more dire, attempts to divert attention and buck up the population, elites and the military by provoking external conflict – Kim-family stockin-trade – should be expected. Moreover, the regime’s impulse to blame others for its failures and predicaments could become stronger under the conditions described here. North Korean attacks when cornered would also fit the pattern of trying to frighten others into concessions, be it aid from China, compromise from Seoul, security assurances from the United States, or international acceptance of North Korea’s nuclear-weapons status. Unlike failing states that implode, North Korea could explode. Even if North Korean armed forces fragment, the regime might still be able to order the use of its arsenal of offensive weapons. Violence could be directed against suspected traitors, the North Korean people, South Korea, Japan and the United States. Although it could not sustain an invasion of the South, the North Korean military could be expected to launch devastating artillery attacks, possibly with chemical weapons. In addition, North Korea is thought to have as many as 200,000 ‘special forces’: trained and dedicated irregulars who could be dispatched to infiltrate and cause havoc in South Korea.12 In the worst case, the regime might even detonate one or more nuclear weapons to show resolve, seek to strike a deal for survival or just visit final destruction on the hated Southern state.13 Short of detonating nuclear weapons if faced with extinction, the regime could launch non-nuclear ballistic missiles in large numbers. Depending on when the crisis comes, South Korea, Japan and US bases in the region would fall within the North’s missile-strike radius. Although it will be some years before North Korea is capable of targeting US territory with ballistic-missile re-entry vehicles, let alone nuclear-armed ones, fitting nuclear weapons into missiles is a high priority.14 Although our knowledge of North Korean biological-weapons capabilities is limited, their use in the regime’s last days cannot be excluded. The strong possibility of the Kim regime striking out while going down is what could make plausible Korean contingencies so complex and so demanding for US military forces. Responding to such a dangerous and volatile mix of regular, irregular and human challenges implies requirements that could severely test the United States and South Korea, forcing them to move promptly to gain control of much of North Korea. That North Korea borders and concerns China could make its violent end even more risky and consequential for Northeast Asia and the United States. Under conditions like those described here, China is unlikely to remain idle. The Chinese can be expected to try to keep the regime afloat until they know it is going under. In the event, they would be forced into action to prevent or, failing that, channel a tsunami of refugees and to provide food and shelter, which could require a deployment of large Chinese ground forces to or across the Yalu River.15 Securing North Korean nuclear, chemical and biological weapons could also be a high Chinese priority. For strategic reasons, China might not wait for South Korea and the United States to occupy the North, unify the country and bring their alliance to its frontier. The Chinese would therefore feel pressure to act either if North Korea were becoming a security vacuum or if it appeared that South Korea and its US ally were moving to fill the vacuum. On top of the challenge of dealing with the debris of a Northern collapse, the United States and South Korea could face an assertive or unpredictable Chinese reaction and military moves. The dual dangers of collapse and attack are the products of decades of North Korean decay, rationalisation and conditioned behaviour, accompanied by the acquisition of and growing reliance on nuclear weapons. These parallel developments are linked: with the crumbling of other pillars of power, such as industry and conventional military strength, the North Korean state has come to count on the threat to use nuclear weapons if its existence is in jeopardy. The regime has lately all but said that nuclear weapons are its best hope of survival and last line of defence, stating that they are non-negotiable under any circumstances. Because it would blame and aim to punish its mortal enemies for its ruin, resort to nuclear weapons would fit the pathology of its reasoning. Repeatedly and reflexively, the regime’s paranoia has led to escalation in the face of peril, real or imagined. Whether US nuclear deterrence would work against such ‘rationality’ is unknown.16 The prospect of US retaliation could be discounted by North Korean leaders if they calculate – rather, miscalculate – that their only chance of survival is to resort to their ultimate option, all measures short of that having failed.17 It would not be suicidal, clinically speaking, if the regime believed it could shock its enemies into negotiation. If improbable, North Korean use of nuclear weapons is not implausible in the event that US and South Korean military intervention is thought by Pyongyang to be impending – a prospect that underscores how explosive a collapse could be and how skilful the response must be. So ingrained is the North Korean mindset that neither reversing the state’s destructive behaviour nor loosening its hold on nuclear weapons can be expected. At first, Kim Jong Un’s instalment brought hopes that he would abandon the bellicosity of his father and grandfather, if not of his own will then because political handlers and economic elites surrounding him, fearing for their futures, demanded a different course. These hopes have been shattered, leaving South Korea, the United States and China all unsure how to deal with the latest Kim. Since 2010 the stiffening of the alliance between South Korea and the United States, the rise in international opprobrium and the tightening of sanctions (specifically designed to penalise the regime and its supporters) have produced no fundamental North Korean retreat – a further indication of the strength of the reflex both to dig in and lash out. Yet, rewarding the North’s misconduct by aid, a rush to the conference table, acceptance of its nuclear status or other accommodations would only confirm and reinforce the North’s conviction that hostility pays (as it paid in the past). At this stage, it is not clear that a tough stance by South Korea and the United States would work any better than a compromising one.

#### **Allied cyber operations with South Korea key to prevent escalation**

Gompert 13, Senior Fellow at the RAND Corporation and Distinguished Visiting Professor at the United States Naval Academy

(David C., He was Principal Deputy Director of National Intelligence in the first Obama administration, and has served as a senior official in several prior administrations and as a senior business executive, “North Korea: Preparing for the End” Survival, Vol. 55 No. 3, July 2013, http://dx.doi.org/10.1080/00396338.2013.802849)

As already noted, the political aims that US military action should serve are to defuse nuclear, chemical and biological threats; protect allies; ease human suffering; create conditions for favourable unification and avoid conflict with China. With this in mind, US forces could be given any of the following operational missions by policymakers: 1. Secure nuclear, chemical and biological weapons materials, facilities, personnel and delivery systems. 2. Provide command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) for South Korean forces and combined operations. 3. Carry out air- and naval strikes in support of South Korean forces. 4. Seize Northern locations of critical military, political or economic significance. 5. Augment South Korean forces in case North Korea attacks, including ballistic-missile defence. 6. Defeat or control North Korean forces. 7. Create conditions for safe and effective human relief, and provide such relief. 8. Rescue prisoners from North Korean gulags.29 9. Deter, check or shape Chinese military moves. 10. Establish pervasive intelligence, surveillance and reconnaissance (ISR).30 11. Establish ‘information dominance’ (using techniques such as propaganda and cyber operations). Some of these missions could take longer than others to accomplish. In particular, securing nuclear, chemical and biological weapons; ending armed resistance; facilitating humanitarian relief and shaping Chinese moves could require protracted US military operations and presence. Significantly, these are the missions that tend to drive up US force requirements (as we will see). What is asked of US forces would, as noted, depend heavily on the roles and capabilities of South Korean forces in tasks such as overcoming residual North Korean resistance and establishing conditions for humanitarian relief. However, the effectiveness of South Korean forces for such missions would depend on the availability of US support, augmentation and C4ISR. As for securing nuclear weapons, seizing critical locations, defeating large and heavily-armed North Korean forces, and shaping Chinese moves, US forces might have to bear chief responsibility.31 Obviously, such missions would require a closely coordinated US military response, probably involving all services. US commanders can readily call on ample air and naval forces’ capabilities for missions two and three; with the commitment of American intelligence agencies and US Army Cyber Command, it could also meet the needs for ISR and information dominance (missions nine and ten). While relying to the extent possible on joint support, US ground forces would presumably bear or share principal responsibilities for missions one, four, five, six, seven and eight. In contrast to air, naval and cyber capabilities, US ground forces and associated support could be in scarce supply, depending on the nature of the missions, the scale of requirements for these missions and the worldwide availability of such forces.32 The very limited US ground forces stationed in South Korea and Japan would almost certainly be insufficient. For conditions described here, information dominance (mission 11) is not just a buzzword. The ability to influence the North Korean military and other security forces; population; nuclear, chemical and biological weapons custodians and scientists; regime opponents and regime supporters could prove indispensable in shaping views and simply spreading useful information. Because North Korea is known for its lack of information infrastructure, US forces would need to bring much of the technology that permits access to US messaging. As important, their efforts need to fit with those of the South Koreans, whose knowledge, rapport and influence matter more, at the end of the day. Securing nuclear, chemical and biological weapons; seizing critical locations; defeating North Korean attacks and armed opposition; safeguarding or providing emergency relief and deterring or containing Chinese forcesimply a very wide range of heavy demands on US ground forces, further complicated by uncertain and fluid conditions. Missions one, four, six, seven and eight could each require substantial US ground forces in North Korea; to the extent that such missions are concurrent, the demands would be largely additive. Additional requirements to oppose a hostile Chinese move deep into North Korea (addressed below) are hard to contemplate. US ground forces would need to be mobile and agile enough to respond to dynamic conditions and changing demands. Assuming that there is insufficient warning of North Korean collapse to augment US troops in South Korea in advance – or that doing so could trigger Chinese intervention – fast expeditionary ground forces would be crucial. Because time could be critical and short, sizeable ground forces might have to be delivered by air. This presents a dilemma in that the forces that could be inserted most swiftly would be relatively light, whereas the missions and conditions described above could require at least some heavier forces. From the midst of the Cold War on, the US Army has swung episodically between organising, training and equipping for regular warfare, on the one hand, and for irregular or ‘stability’ operations, such as counterinsurgency, on the other. Because the doctrines, operating concepts, skills and gear required differ greatly between the former and the latter, it is not easy to optimise for both at the same time. During Vietnam, the US Army was forced to shift towards irregular operations, including counter-insurgency. Then it shifted back toward preparations for combat with Soviet forces, only to have to ‘re-learn’ counter-insurgency during the post-9/11 decade. Mistakes following the conquest of Iraq remind us how difficult it can be for forces prepared for one mode to perform the other. However, because the missions associated with the sort of Korean contingency described here encompass both of these two basic modes, the US Army cannot choose to prepare for one but not the other, despite how different they are. It is hard to be precise about the scale of US ground forces needed for a crisis that could take several forms and move in several directions.For the purpose of analysis, we can treat conditions in the North (involving degraded human conditions and concern with nuclear, chemical and biological weapons) as constant and the conduct and capabilities of other actors and forces (South Korea, China and, of course, North Korea) as variable.

### 1AC — Solvency

#### The plan solves –

#### **Establishes** Congressional notifications – it’s the perfect middle ground

Lorber 13, JD candidate at UPenn and PhD candidate at Duke

(Eric, EXECUTIVE WARMAKING AUTHORITY AND OFFENSIVE CYBER OPERATIONS: CAN EXISTING LEGISLATION SUCCESSFULLY CONSTRAIN PRESIDENTIAL POWER?, www.law.upenn.edu/live/files/1773-lorber15upajconstl9612013)

Should these statutes be adjusted (or new ones created) that give Congress additional oversight in this area? Two competing desiderata suggest that oversight should be increased, but only to a limited extent. On the one hand, policymakers have suggested that developing strict rules and limitations on the use of offensive cyber operations will handicap the military’s ability to quickly and effectively employ these tools in critical situations, such as cyber warfare against adversarial states. According to these arguments, developing red lines that proscribe the use of these capabilities will create reluctance and trepidation among strategists and will lead to disadvantages in combat situations. On the other hand, developing some legal rules is necessary to ensure that, as these cyber capabilities continue to develop, the President does not gain sufficient leverage to substantially tilt the balance between the President and Congress. Moreover, because these capabilities are still developing at a fast rate, understanding how they should and should not be employed is an important goal and having senior members of Congress and their staffs— professional staff members on the intelligence committees, who likely have substantial experience in these areas—provide input would be useful in developing this understanding. These competing arguments—one for limiting any oversight and one for increasing it—suggest a middle ground that will avoid drawing red lines but will still provide useful congressional insight into the doctrinal and legal development of offensive cyber operations. Such an approach would include new legislation, similar to the Intelligence Authorization Act, explicitly requiring the President to report its use of covert cyber activities to the heads of Senate and House intelligence committees (i.e. the Gang of Eight). Congress would not have the ability to veto such actions, however it would be able to raise potential legal issues with the executive branch, as well as provide policy advice as to the wisdom of employing these capabilities in such circumstances. As a result, while the heads of these committees would not have the ability to draw red lines themselves, they would be able to consult with the executive branch—as the branch employs these capabilities—to determine their likely legality and wisdom. While the President could ignore this advice, such an approach would at the very least keep Congress informed of the developing capabilities and their employment. With such an approach, Congress could play a meaningful role in the shifting and uncertain legal and policy realms of offensive cyber operations, which will undoubtedly become increasingly important as the United States and other nations develop and employ these capabilities with ever-greater frequency.

#### This is key –

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

Bradbury 11**, Assistant Attorney General for the Office of Legal Counsel**

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

Evolving customary law. This approach also accommodates the reality that how the U.S. chooses to use its armed forces will significantly influence the development of customary international law. As the label 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 United States 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 United States. 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 United States 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 United States 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 information technology experts from critical infrastructure firms around the world expressed concern about the United States as a source of computer network attacks than about any other country. This awareness, along with our vulnerability to cyberattacks, fuels a dangerous public and private cyber arms race in an arena where the offense already has a natural advantage.

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

Lewis 11, Senior Fellow at CSIS (James Andrew, Confidence-building and international agreement in cybersecurity, citizenlab.org/cybernorms2012/Lewis2011.pdf)

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

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

**Dycus 10, Professor of National Security Law** Stephen is a Professor of national security law at Vermont Law School, former member of the National Academies committee on cyber warfare, LLM, Harvard University, LLB, BA, Southern Methodist University, “Congress’ Role in Cyber Warfare,” Journal of National Security Law & Policy, 4(1), 2010, p.161-164, <http://www.jnslp.com/read/vol4no1/11_Dycus.pdf>

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

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

Bastby 12, Chairwoman of the American Bar Association’s Privacy and Computer Crime Committee (Judy, CEO of Global Cyber Risk, “U.S. Administration's Reckless Cyber Policy Puts Nation at Risk” June 4, 2012, <http://www.forbes.com/sites/jodywestby/2012/06/04/u-s-administrations-reckless-cyber-policy-puts-nation-at-risk/2/>)

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

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

**Hansen & Friedman 9**, **Professors at the New England School of Law**,(Victor and Lawrence, The Case for Congress: Separation of Powers and the War on Terror, p.130)

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

### 1AC — Plan

#### Plan: The legislative branch of the United States federal government should prohibit offensive cyber operations about which Congress has not been notified.

**2AC**

### China

#### The threat is real:

#### Modernization — they’re massively expanding military capabilities — that’s Kazianis and RTT

#### Bellicosity — RTT says they’re increasingly assertive in territorial disputes

#### Internal documents prove — none of their epistemology args apply — Kazianis and Yoshihara cite official PLA doctrine — anti-access attacks are a crucial part of their strategy and it’s a key objective to expand to Taiwan and the South China Sea

#### China’s expansion to South China Sea is rooted in historical national identity — the alternative is naiive

**Prabhakar 11** Dr.W.Lawrence S., Associate Professor, Department of Political Science, Madras Christian College, Chennai, India; Adjunct Senior Fellow, Centre for Asian Strategic Studies, New Delhi, India; Guest Professor, Department of Humanities and Social Sciences, Indian Institute of Technology-Madras., “ The Evolving Geopolitics in the South China Sea”, PDF

Sovereignty Concerns and the apprehension of sovereignty violations by contending states both regional and extra-regional is a dominant factor in the region. Sovereignty concerns are derivative of the historical and colonial factors that have shaped the national identities and resistance to external domination. Territorial and maritime disputes and contentions over unresolved border and boundary issues have been emerged as vital points of assertion of national sovereignty. Regional responses to territorial disputes have been in the form of modernization of naval forces and air forces that are viewed as viable instruments to secure the islands and protect the maritime areas **The South China Sea is yet another source of national identity for China.** The “recovery” of the area for the Chinese leaders provides a means to erase a century of national humiliation of colonialism and “unjust treaties” that China was subjected to. **China views the issue as a part of the domestic issue** and hence the Law of the People’s Republic of China on the Territorial Waters and Contiguous Areas was passed by the National People’s Assembly as a means to recover the area to Chinese suzerainty. China reiterated claims in the South China Sea and stipulated the right to use force to protect islands-- the Spratlys and their surrounding waters. The law questioned the peaceful management of the territorial dispute and was regarded by the Association as a political provocation. **The PLA tends to view the South China Sea as a domestic issue-- a derivative of China’s national identity.** Superimposed on the patterns of power rivalry from the ancient period that had witnessed several power transitions between China, Japan, Korea and India, thus **the South China Sea** and the East China Sea **have been flash points that have intermittently triggered in different periods of history**. With the Cold war overlay since 1945-1991, the region was relatively calm thanks to the large measure of the strategic balancing of the United States and the Soviet Union—although the Cold war had witnessed the worst Indo-China conflict that raged for several years. In the post-cold war period and into the midway of the Globalization period, the South China Sea had emerged as vital hub for contending maritime access between China and most of the Southeast Asian states of Malaysia, Singapore, Vietnam, Philippines, Taiwan, Brunei, Thailand, Cambodia with most of the contentions over Spratlys and Paracels archipelago besides the other islands with contenders like the Woody Island (China) Layang Layang (Malaysia), Truong Sa Lon(Vietnam), Taipingdao (Taiwan), Pagasa (Rancudo) Airfield) (Philippines). These islands offer mid-sea access that could serve for amphibious and aerial staging points in a sea of contending territorial and resources disputes.

### 2AC — Mutual Threat Con

**Mutual threat construction is an institutional reality — we should engage it**

**Gries 7** (Peter Hayes, Harold J. & Ruth Newman Chair in U.S.-China Issues and Director of the Institute for U.S.- China Issues at the University of Oklahoma, “Harmony, Hegemony & U.S.-China Relations”, *World Literature Today*, July 2007 issue)

Furthermore, the new Chinese Occidentalism depicts Americans as an aggressive, militaristic, and threatening people. It certainly does not help that the current Bush administration’s embrace of military and unilateral means to resolve international disputes in Iraq and elsewhere has provided ample fodder for Chinese nationalist arguments. The danger is that heightened Chinese perceptions of U.S. threat could promote the emergence of an acute “security dilemma” in U.S.-China relations. Feeling threatened by a “hegemonic” U.S., Chinese could decide to step up their military modernization for defensive reasons. Americans would likely respond to increased Chinese arms acquisitions with heightened threat perception of their own, leading the U.S. to embrace its own defensive arms buildup. The unintended result: a possible U.S.-China arms race in East Asia. Absent feelings of mutual trust, and given the deep animosities that have led to the recent deterioration of Sino-Japanese relations and the always volatile situation in the Taiwan Strait, **there is a real possibility that the U**nited **S**tates **will get drawn into** yet another **conflict with China** in the first decades of the twenty-first century.¶ What can be done? While American and Chinese nationalists produce Orientalist and Occidentalist discourses based on similar epistemologies of difference, other Americans and Chinese can construct discourses of similarity. At its best, American and Chinese cultural products, like the special section on contemporary Chinese literature in this issue of World Literature Today, celebrate our common humanity. Translation and cultural exchange can reveal our shared challenges: modernization, globalization—indeed, the human condition. In the end, cultural products that raise awareness of our common humanity can serve as a vital counterweight to the discourses of difference and threat that undermine U.S.-China relations.

### 2AC D&G K

**The role of the ballot is to decide between a plan or a competitive policy option**

**It creates relevant strategies for change that are predictable and allow the aff to get offense against**

**The alternative isn’t a relevant consideration to whether the plan’s action should occur — voting issue, only opportunity costs should be evaluated to teach cost-benefit analysis**

**Our discussion raises awareness of cyber militarism and spills over to policy**

**NRC 9**, WILLIAM A. OWENS, AEA Holdings, Inc., Co-chair KENNETH W. DAM, University of Chicago, Co-chair THOMAS A. BERSON, Anagram Laboratories GERHARD CASPER, Stanford University DAVID D. CLARK, Massachusetts Institute of Technology RICHARD L. GARWIN, IBM Fellow Emeritus JACK L. GOLDSMITH III, Harvard Law School CARL G. O’BERRY, The Boeing Company JEROME H. SALTZER, Massachusetts Institute of Technology (retired) MARK SEIDEN, MSB Associates SARAH SEWALL, Harvard University WALTER B. SLOCOMBE, Caplin & Drysdale WILLIAM O. STUDEMAN, U.S. Navy (retired) MICHAEL A. VATIS, Steptoe & Johnson LLP Staff HERBERT S. LIN, Study Director KRISTEN BATCH, Associate Staff Officer (through August 2008) TED SCHMITT, Consultant JANICE SABUDA, Senior Project Assistant (through March 2008) ERIC WHITAKER, Senior Project Assistant JOSEPH F. TRAUB, Columbia University, Chair PRITHVIRAJ BANERJEE, Hewlett Packard Company FREDERICK R. CHANG, University of Texas, Austin WILLIAM DALLY, Stanford University MARK E. DEAN, IBM Almaden Research Center DEBORAH L. ESTRIN, University of California, Los Angeles KEVIN C. KAHN, Intel Corporation JAMES KAJIYA, Microsoft Corporation RANDY H. KATZ, University of California, Berkeley JOHN E. KELLY III, IBM Research SARA KIESLER, Carnegie Mellon University JON KLEINBERG, Cornell University PETER LEE, Carnegie Mellon University TERESA H. MENG, Stanford University WILLIAM H. PRESS, University of Texas, Austin PRABHAKAR RAGHAVAN, Yahoo! Research DAVID E. SHAW, D.E. Shaw Research ALFRED Z. SPECTOR, Google, Inc. ROBERT F. SPROULL, Sun Microsystems, Inc. PETER SZOLOVITS, Massachusetts Institute of Technology ANDREW J. VITERBI, Viterbi Group, LLC PETER WEINBERGER, Google, Inc. JON EISENBERG, Director RENEE HAWKINS, Financial and Administrative Manager HERBERT S. LIN, Chief Scientist, CSTB LYNETTE I. MILLETT, Senior Program Officer NANCY GILLIS, Program Officer

ENITAA. WILLIAMS, Associate Program Officer MORGAN R. MOTTO, Program Associate SHENAE BRADLEY, Senior Program Assistant ERIC WHITAKER, Senior Program Assistant, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of CYBERATTACK CAPABILITIES, <http://www.anagram.com/berson/nrcoiw.pdf>

A historical analogy might be drawn to the study of nuclear issues. In many ways, today’s state of affairs regarding public discourse on cyberattack is analogous to the nuclear debate of 50 years ago. At that time, nuclear policy issues were veiled in secrecy, and there was little public debate about them. Herman Kahn’s books (On Thermonuclear War, Thinking the Unthinkable) were the first that addressed in the open literature what it might mean to fight a nuclear war. These seminal pieces did much to raise the public profile of these issues and stimulated an enormous amount of subsequent work outside government that has had a **real impact on nuclear policy**. From our perspective as the co-chairs of this study, the topic of cyberattack is so important across a multitude of national interests—not just defense or even just national security—that it **deserves robust and open discussion and debate**, both among thoughtful professionals in the policy, military, intelligence, law enforcement, and legal fields and among security practitioners in the private sector. But for such discussion and debate to be productive, they must be based on some **common foundation of information about the topic at hand.** Thus, **the report’s role in providing education and background is in our view its most important function**.

**Engaging policy is key**

**McClean**, **Professor – Philosophy, Rutgers**, **1**

**(THE CULTURAL LEFT AND THE LIMITS OF SOCIAL HOPE, http://www.american-philosophy.org/archives/2001%20Conference/Discussion%20papers/david\_mcclean.htm)**

Leftist American culture critics might put their considerable talents to better use if they bury some of their cynicism about America's social and political prospects and help forge public and political possibilities in a spirit of determination to, indeed, achieve our country - the country of Jefferson and King; the country of John Dewey and Malcom X; the country of Franklin Roosevelt and Bayard Rustin, and of the later George Wallace and the later Barry Goldwater. To invoke the words of King, and with reference to the American society, the time is always ripe to seize the opportunity to help create the "beloved community," one woven with the thread of agape into a conceptually single yet diverse tapestry that shoots for nothing less than a true intra-American cosmopolitan ethos, one wherein both same sex unions and faith-based initiatives will be able to be part of the same social reality, one wherein business interests and the university are not seen as belonging to two separate galaxies but as part of the same answer to the threat of social and ethical nihilism. We who fancy ourselves philosophers would do well to create from within ourselves and from within our ranks a new kind of public intellectual who has both a hungry theoretical mind and who is yet capable of seeing the need to move past high theory to other important questions that are less bedazzling and "interesting" but more important to the prospect of our flourishing - questions such as "How is it possible to develop a citizenry that cherishes a certain hexis, one which prizes the character of the Samaritan on the road to Jericho almost more than any other?" or "How can we square the political dogma that undergirds the fantasy of a missile defense system with the need to treat America as but one member in a community of nations under a "law of peoples?"The new public philosopher might seek to understand labor law and military and trade theory and doctrine as much as theories of surplus value; the logic of international markets and trade agreements as much as critiques of commodification, and the politics of complexity as much as the politics of power (all of which can still be done from our arm chairs.) This means going down deep into the guts of our quotidian social institutions, into the **grimy pragmatic details** where intellectuals are loathe to dwell but where the officers and bureaucrats of those institutions take difficult and often unpleasant, imperfect decisions that affect other peoples' lives, and **it means making honest attempts to truly understand how those institutions actually function in the actual world before howling for their overthrow commences. This might help keep us from being slapped down in debates by true policy pros who actually know what they are talking about** but who lack awareness of the dogmatic assumptions from which they proceed, and who have not yet found a good reason to listen to jargon-riddled lectures from philosophers and culture critics with their snobish disrespect for the so-called "managerial class."

#### Arugment about why there are multiple different moves under the table is why this should be brought out in the open

**The plan is a link turn -**

**Cyber war is happening and is offense against the alt**

**Inevitable because the chess game is inevitable**

**Expansion as a reaction to the US**

**The plan brings this out into the open understand**

**2 pieces of offense**

**Miscalculation – Rothschild – countries perceive it as a prerequisite to a nuclear attack so they use their own nukes**

**Centralization of control – combo of NSA and US Cybercom with 0 oversight means decisions can be madea t the will of 1 man – plan k2 break down hierarchy**

**Only the aff changes these actions which happen at the highest level of govenremnt -**

**Warfare is inevitable – should be a form that provides checks and balances which causes the minimum amount of violence**

**Our aff is proof of why the secret is bad ]**

**Turn — discussion of global problems stops crisis-driven responses and fosters empathy**

**Ungar 5,** president – Goucher College, 2005 [Sanford, “compassion fatigue: the next wave?”, winter, www.goucher.edu/x4726.xml]

There is a temptation to worry that before long, we will be hit by one more severe case of what has come to be known as “compassion fatigue”—a deadening of our sensibilities by the unrelenting bombardment of shallow and sensationalist media coverage of disease, famine, death, and war. Susan D. Moeller, a well-traveled observer who now teaches at the University of Maryland, has written tellingly of this phenomenon. “Through a choice of language and images,” she says, “the newest event is represented as more extreme than a similar past situation.” When we use the same extreme words to describe very different events, we undermine our ability to differentiate among them. Our sense of tragedy and cataclysm can be ratcheted only so high before we simply become overwhelmed. Some news organizations try to hold our attention by personalizing the events—pointing out, for example, that U.S. citizens perished in the tsunami, or drawing comparisons between this disaster overseas and others closer to international problems. “Why, to listen to NPR,” he complained, “you would think that there is trouble everywhere. It’s exhausting.” Visitors from across the country—sufferers all from compassion fatigue, I suppose—nodded their heads in agreement. “Well,” I said, as I attempted to confront him later, “there **really is a lot to worry about** in the world, and someone has to call our attention to it.” He was not about to be persuaded, preferring instead to focus on the customary agenda of parochial issues facing Americans. There’s a real danger in that attitude. If we allow our exhaustion to keep us from thinking about global concerns, we risk ignoring some important issues that may deserve a place in our consciousness alongside our domestic debates. By now it should be obvious that events and conditions around the world can have a profound impact on Main Street America. One would think there is plenty of evidence to make the point: the crisis- inspired fluctuation in gasoline prices at the pump; the international shortage of steel and concrete due to the construction boom in China; and the ebb and flow of immigration to the United States on the basis of circumstances in Mexico and Central America, among other places. Not to mention the consequences we have all experienced, in varying ways and to varying degrees, as a result of the Iraq war. The tsunami has ramifications for Americans beyond what might seem immediately apparent. It has been suggested that American generosity toward these countries with large Muslim populations could have an important restorative effect on the United States’ image throughout the Muslim world. It’s a shame it took a catastrophe like this to get us interested in what’s going on there. Perhaps if we **paid closer attention** to the concerns of others over a sustained period of time, we would gain a better understanding of the global disparities that breed problems like terrorism—and, in the process, go a long way toward making the world safer for everyone. In the heat of political battle, in the midst of some of our own legitimate preoccupations, it may have become more difficult to sustain the argument that Americans’ lives are meaningfully affected by poverty, disease, and tragedy in distant, hard-to-pronounce places. But we **must not turn our attention away**, and we must demand that those we entrust to report the news be not only **vigilant, but also responsible**, in their presentation of global events. Otherwise, we will be **doomed to await the tsunamis of history**, literal and figurative, to help us figure out what is really going on.

#### Reform is good – blowing up the board does nothing

**Ferguson 11,** Professor of Anthropology at Stanford

(James, The Uses of Neoliberalism, Antipode, Vol. 41, No. S1, pp 166–184)

If we are seeking, as this special issue of Antipode aspires to do, to link our critical analyses to the world of grounded political struggle—not only to interpret the world in various ways, but also to change it—then there is much to be said for focusing, as I have here, on mundane, real- world debates around policy and politics, even if doing so inevitably puts us on the compromised and reformist terrain of the possible, rather than the seductive high ground of revolutionary ideals and utopian desires. But I would also insist that there is more at stake in the examples I have discussed here than simply a slightly better way to ameliorate the miseries of the chronically poor, or a technically superior method for relieving the suffering of famine victims. My point in discussing the South African BIG campaign, for instance, is not really to argue for its implementation. There is much in the campaign that is appealing, to be sure. But one can just as easily identify a series of worries that would bring the whole proposal into doubt. Does not, for instance, the decoupling of the question of assistance from the issue of labor, and the associated valorization of the “informal”, help provide a kind of alibi for the failures of the South African regime to pursue policies that would do more to create jobs? Would not the creation of a basic income benefit tied to national citizenship simply exacerbate the vicious xenophobia that already divides the South African poor, in a context where many of the poorest are not citizens, and would thus not be eligible for the BIG? Perhaps even more fundamentally, is the idea of basic income really capable of commanding the mass support that alone could make it a central pillar of a new approach to distribution? The record to date gives powerful reasons to doubt it. So far, the technocrats’ dreams of relieving poverty through efficient cash transfers have attracted little support from actual poor people, who seem to find that vision a bit pale and washed out, compared with the vivid (if vague) populist promises of jobs and personalistic social inclusion long offered by the ANC patronage machine, and lately personified by Jacob Zuma (Ferguson forthcoming). My real interest in the policy proposals discussed here, in fact, has little to do with the narrow policy questions to which they seek to provide answers. For what is most significant, for my purposes, is not whether or not these are good policies, but the way that they illustrate a process through which specific governmental devices and modes of reasoning that we have become used to associating with a very particular (and conservative) political agenda (“neoliberalism”) may be in the process of being peeled away from that agenda, and put to very different uses. Any progressive who takes seriously the challenge I pointed to at the start of this essay, the challenge of developing new progressive arts of government, ought to find this turn of events of considerable interest. As Steven Collier (2005) has recently pointed out, it is important to question the assumption that there is, or must be, a neat or automatic fit between a hegemonic “neoliberal” political-economic project (however that might be characterized), on the one hand, and specific “neoliberal” techniques, on the other. Close attention to particular techniques (such as the use of quantitative calculation, free choice, and price driven by supply and demand) in particular settings (in Collier’s case, fiscal and budgetary reform in post-Soviet Russia) shows that the relationship between the technical and the political-economic “is much more polymorphous and unstable than is assumed in much critical geographical work”, and that neoliberal technical mechanisms are in fact “deployed in relation to diverse political projects and social norms” (2005:2). As I suggested in referencing the role of statistics and techniques for pooling risk in the creation of social democratic welfare states, social **technologies need not have any essential** or eternal **loyalty to the political formations within which they were first developed**. Insurance rationality at the end of the nineteenth century had no essential vocation to provide security and solidarity to the working class; it was turned to that purpose (in some substantial measure) because it was available, in the right place at the right time, to be appropriated for that use. Specific ways of solving or posing governmental problems, specific institutional and intellectual mechanisms, can be combined in an almost infinite variety of ways, to accomplish different social ends. With social, as with any other sort of technology, it is not the machines or the mechanisms that decide what they will be used to do. Foucault (2008:94) concluded his discussion of socialist government- ality by insisting that the answers to the Left’s governmental problems require not yet another search through our sacred texts, but a process of conceptual and institutional innovation. “[I]f there is a really socialist governmentality, then it is not hidden within socialism and its texts. It cannot be deduced from them. It must be invented”. But invention in the domain of governmental technique is rarely something worked up out of whole cloth. More often, it involves a kind of bricolage (Le ́vi- Strauss 1966), a piecing together of something new out of scavenged parts originally intended for some other purpose. As we pursue such a process of improvisatory invention, we might begin by making an inventory of the parts available for such tinkering, keeping all the while an open mind about how different mechanisms might be put to work, and what kinds of purposes they might serve. If we can go beyond seeing in “neoliberalism” an evil essence or an automatic unity, and instead learn to see a field of specific governmental techniques, we may be surprised to find that some of them can be repurposed, and put to work in the service of political projects very different from those usually associated with that word. If so, we may find that the cabinet of governmental arts available to us is a bit less bare than first appeared, and that some rather useful little mechanisms may be nearer to hand than we thought.

**Society functions absent the individuals – we cannot solely focus on the relation to eachother**

**Wight – Professor of IR @ University of Sydney – 6**

(Colin, Agents, Structures and International Relations: Politics as Ontology, pgs. 48-50

One important aspect of this relational ontology is that these relations constitute our identity as social actors. According to this relational model of societies, one is what one is, by virtue of the relations within which one is embedded. A worker is only a worker by virtue of his/her relationship to his/her employer and vice versa. ‘Our social being is constituted by relations and our social acts presuppose them.’ At any particular moment in time an individual may be implicated in all manner of relations, each exerting its own peculiar causal effects. This ‘lattice-work’ of relations constitutes the structure of particular societies and endures **despite changes in the individuals occupying them**. Thus, the relations, the structures, are ontologically distinct from the individuals who enter into them. At a minimum, the social sciences are concerned with two distinct, although mutually interdependent, strata. There is an ontological difference between people and structures: ‘people are not relations, societies are not conscious agents’. Any attempt to explain one in terms of the other should be rejected. If there is an ontological difference between society and people, however, we need to elaborate on the relationship between them. Bhaskar argues that we need a system of mediating concepts, encompassing both aspects of the duality of praxis into which active subjects must fit in order to reproduce it: that is, a system of concepts designating the ‘point of contact’ between human agency and social structures. This is known as a ‘positioned practice’ system. In many respects, the idea of ‘positioned practice’ is very similar to Pierre Bourdieu’s notion of *habitus*. Bourdieu is primarily concerned with what individuals do in their daily lives. He is keen to refute the idea that social activity can be understood **solely in terms of individual decision-making**, or as determined by surpa-individual objective structures. Bourdieu’s notion of the *habitus* can be viewed as a bridge-building exercise across the explanatory gap between two extremes. Importantly, the notion of a habitus can only be understood in relation to the concept of a ‘social field’. According to Bourdieu, a social field is ‘a network, or a configuration, of objective relations between positions objectively defined’. A social field, then, refers to a structured system of social positions occupied by individuals and/or institutions – the nature of which defines the situation for their occupants. This is a social field whose form is constituted in terms of the relations which define it as a field of a certain type. A *habitus* (positioned practices) is a mediating link between individuals’ subjective worlds and the socio-cultural world into which they are born and which they share with others. The power of the habitus derives from the thoughtlessness of habit and habituation, rather than consciously learned rules. The habitus is imprinted and encoded in a socializing process that commences during early childhood. It is inculcated more by experience than by explicit teaching. Socially competent performances are produced as a matter of routine, without explicit reference to a body of codified knowledge, and without the actors necessarily knowing what they are doing (in the sense of being able adequately to explain what they are doing). As such, the *habitus* can be seen as the site of ‘internalization of reality and the externalization of internality.’ Thus social practices are produced in, and by, the encounter between: (1) the *habitus* and its dispositions; (2) the constraints and demands of the socio-cultural field to which the habitus is appropriate or within; and (3) the dispositions of the individual agents located within both the socio-cultural field and the *habitus*. When placed within Bhaskar’s stratified complex social ontology the model we have is as depicted in Figure 1. The explanation of practices will require all three levels. Society, as field of relations, exists prior to, and is independent of, individual and collective understandings at any particular moment in time; that is, social action requires the conditions for action. Likewise, given that behavior is seemingly recurrent, patterned, ordered, institutionalised, and displays a degree of stability over time, there must be sets of relations and rules that govern it. Contrary to individualist theory, these relations, rules and roles are not dependent upon either knowledge of them by particular individuals, or the existence of actions by particular individuals; that is, **their explanation cannot be reduced to consciousness** or to the attributes **of individuals**. These emergent social forms must possess emergent powers. This leads on to arguments for the reality of society based on a causal criterion. Society, as opposed to the individuals that constitute it, is, as Foucault has put it, ‘a complex and independent reality that has its own laws and mechanisms of reaction, its regulations as well as its possibility of disturbance. This new reality is society…It becomes necessary to reflect upon it, upon its specific characteristics, its constants and its variables’.

### AT: Death Good

#### Their argument denies the value to our experience because it erases the line between life and death- even if death is valuable and there are great things going on there, simply embracing death denies the possibility of agency for choice and sucks the meaning from our current reality

Kymlicka ‘3

(Will, professor of philosophy @ Queens University. Contemporary Political Thought: A Reader And Guide. Edited by Alan Finlayson, pp. 496-498)

The defining feature of liberalism is that it ascribes certain fundamental freedoms to each individual. In particular, it grants people a very wide freedom of choice in terms of how they lead their lives. It allows people to choose a conception of the good life, and then allows them to reconsider that decision, and adopt a new and hopefully better plan of life. Why should people be free to choose their own plan of life? After all, we know that some people will make imprudent decisions, wasting their time on hopeless or trivial pursuits. Why then should the government not intervene to protect us from making mistakes, and to compel us to lead the truly good life? There are a variety of reasons why this is not a good idea: governments may not be trustworthy; Some individuals have idiosyncratic needs which are difficult for even a well-intentioned government to take into account; supporting controversial conceptions of the good may lead to civil strife. Moreover, paternalistic restrictions on liberty often simply do not work — lives do not go better by being led from the outside, in accordance with values the person does not endorse. Dworkin calls this the ‘endorsement constraint’, and argues that ‘no component contributes to the value of a life without endorsement … it is implausible to think that someone can lead a better life against the grain of his profound ethical convictions than at peace with them’ (Dworkin 1989: 486). However, the fact that we can get it wrong is important, because (paradoxically) it provides another argument for liberty. Since we can be wrong about the worth or value of what we are currently doing, and since no one wants to lead a life based on false beliefs about its worth, it is of fundamental importance that we be able rationally to assess our conceptions of the good in the light of new information or experiences, and to revise them if they are not worthy of our continued allegiance. This assumption that our beliefs about the good life are fallible and revisable is widely endorsed in the liberal tradition — from John Stuart Mill to the most prominent contemporary American liberals, such as John Rawls and Ronald Dworkin. (Because of their prominence, I will rely heavily on the works of Rawls and Dworkin in the rest of this chapter.) As Rawls puts it, individuals ‘do not view themselves as inevitable tied to the pursuit of the particular conception of the good and its final ends which they espouse at any given time’. Instead, they are ‘capable of revising and changing this conception’. They can ‘stand back’ from their current ends to ‘survey and assess’ their worthiness (Rawls 1980: 544; cf. Mill 1912: 122; Dworkin 1913). So we have two preconditions for leading a good life. The first is that we lead our life from the inside, in accordance with our beliefs about what gives value to life. Individuals must therefore have the resources and liberties needed to lead their lives in accordance with their beliefs about value, without fear of discrimination or punishment. Hence the traditional liberal concern with individual privacy, and opposition to ‘the enforcement of morals’. The second precondition is that we be free to question those beliefs, to examine them in light of whatever information, examples, and arguments our culture can provide. Individuals must therefore have the conditions necessary to acquire an awareness of different views about the good life, and an ability to examine these views intelligently. Hence the equally traditional liberal concern for education, and freedom of expression and association. These liberties enable us to judge what is valuable, and to learn about other ways of life.

#### Their argument leaves us oscillating between life and death- were people in death to embrace the meaning of death, then logically it would create an equally vampiric relationship towards life- establishing a balance between life and death would drain the value from both, which might be even worse

#### Ensuring humanities survival into technological maturity unlocks new modes of experience and understanding we can’t even comprehend right now

Bostrom, 2012 (Mar 6, Nick, director of the Future of Humanity Institute at Oxford, recipient of the 2009 Gannon Award, “We're Underestimating the Risk of Human Extinction,” interview with Ross Andersen, freelance writer in D.C., <http://www.theatlantic.com/technology/archive/2012/03/were-underestimating-the-risk-of-human-extinction/253821/>)

If I wanted some sort of scheme that laid out the stages of civilization, the period before machine super intelligence and the period after super machine intelligence would be a more relevant dichotomy. When you look at what's valuable or interesting in examining these stages, it's going to be what is done with these future resources and technologies, as opposed to their structure. It's possible that the long-term future of humanity, if things go well, would from the outside look very simple. You might have Earth at the center, and then you might have a growing sphere of technological infrastructure that expands in all directions at some significant fraction of the speed of light, occupying larger and larger volumes of the universe---first in our galaxy, and then beyond as far as is physically possible. And then all that ever happens is just this continued increase in the spherical volume of matter colonized by human descendants, a growing bubble of infrastructure. Everything would then depend on what was happening inside this infrastructure, what kinds of lives people were being led there, what kinds of experiences people were having. You couldn't infer that from the large-scale structure, so you'd have to sort of zoom in and see what kind of information processing occurred within this infrastructure. It's hard to know what that might look like, because our human experience might be just a small little crumb of what's possible. If you think of all the different modes of being, different kinds of feeling and experiencing, different ways of thinking and relating, it might be that human nature constrains us to a very narrow little corner of the space of possible modes of being. If we think of the space of possible modes of being as a large cathedral, then humanity in its current stage might be like a little cowering infant sitting in the corner of that cathedral having only the most limited sense of what is possible.

#### Faith is good- while we cannot know for certain the effects of our actions, nor be certain of the cosmology they occur within, we can make reasonable approximations- taking that leap of faith is justified because it allows us to connect positively with others and engage in projects that prevent nihilism

Giman-Olpasky 11

Richard Gilman-Opalsky is Assistant Professor of Political Philosophy in the Department of Political Science at the University of Illinois at Springfield. He is the author of Unbounded Publics: Transgressire Public Spheres, Zapatismo, and Political Theory. Spectacular Capitalism Guy Debord and the Practice of Radical Philosophy

<http://www.scribd.com/doc/58299096/3/Chapter-1-Selectively-Forgetting-Baudrillard>

Simulacra are, by definition, indistinguishable from real events. Nevertheless, the actual existence and constant possibility of simulacra are not sufficient causes for adopting reality agnosticism. It may be impossibleto distinguish the fake holdup and fake sickness from the real holdup andreal sickness, but the child has really been sick, and most criminals are notplaying. Those involved in staging the act of simulation itself do mostly know the difference. But Baudrillard would rightly point out that, fromthe outside – for those confronting simulacra phenomenologically (instead of making them) – our general inability to tell the difference means that we can never be too confident about reality. Reality agnosticism istantamount to treating every event as a possible simulacrum. This is thesame as to treat no events as real. This is precisely what Baudrillard wantsto do, yet I think this is a mistake.Baudrillard presses us to recognize that even suffering and death canbe and have been simulated (i.e. the Timişoara Massacre in 1989 in WesternRomania, where protestors were gunned down by the army. While themassacre was real, it was later disclosed that 27 bodies were exhumed fromthe Timişoara “Paupers’ Cemetery” to exaggerate the massacre for TV effect. This series of events marked the end of Ceauşescu’s Stalinist regimein Romania.). 36 However, despite such manipulation, we do live in a world where suffering and death are real. That even suffering and death couldbe staged, and that we cannot always tell when that is the case, does notmean that we should make such suspicion into an operational logic – thereis always the other side, the side of actual suffering and death. Baudrillardmakes too much out of the fake, and he errs on the wrong side of theequation. What I mean by saying “too much” and “wrong side,” is precisely to raise a normative objection. Wherever we cannot tell the difference (thatis, wherever there are functional simulacra), I contend that we should err on the side of a different obligation. And this is indeed a moral obligation to take human suffering seriously, an obligation that outweighs the integrity of Baudrillard’s skepticism. To put it bluntly, I would rather be fooled intothinking a faked death was real than that a real death was faked, just as I would always prefer the doctor who assumes that my pain is real despite the leap of faith this may entail. We must also ask, from a political point of view, what it means to beagnostic about reality. Can one act with certainty and resolve against human suffering, against inequality, against growing macroeconomic disparity,against misrecognition, etc., if we cannot know anything with any certainty about these things? It is no misuse or abuse of Baudrillard’s work too bserve that his arguments do in fact distance us from a political consideration of the material conditions of poverty, war, repression, and oppression. He explicitly intends for his arguments to be – inasmuch asthis is possible – incompatible with or unusable for moral judgment and political argument. Baudrillard happily argues for the abandonment of moral argument and normative theory altogether (again, much likeNietzsche, who also intended to think beyond good and evil). For example,Baudrillard writes, “It is no longer a matter here of philosophical morality of the sort that says ‘the world isn’t what it ought to be’ or ‘the world isn’t what it was’. No, the world is as it is.” 37 Of course, Baudrillard is right that the world is as it is, but what of the role of human action in making it that way? So much of the world is as it is because of the cumulative effect of collective human action and inaction over time. In light of this, we do have some space within which to consider what ought to be, and what human action can do to move usin that direction. This is a tenuous space indeed, for it promises us nothing and many people already stand in it pushing and pulling in different directions. But, it is in this space of consideration of the impact and the intervening prospects of human action where the possibility for politics remains, and where one hopes that the best heads will enter the fray.

### Threats

#### Threats do exist, and your skepticism is nothing more than a psychological trick that assumes humans are invincible- your willful ignorance allows terrible atrocities to occur

David W. Orr- Professor of Environmental Studies and Politics @ Oberlin College- 4 AUG 2008, The Psychology of Survival, Conservation Biology, Volume 22, Issue 4, pages 819–822, August 2008, http://onlinelibrary.wiley.com/doi/10.1111/j.1523-1739.2008.01008.x/full

Capable of great feats of imagination and invention as well as generating less agreeable behavior, the mind is both the crowning distinction of humankind and our greatest perplexity. Mind reflecting on itself has long been a source of amusement, philosophy, and more recently, science. But it has never been more important to understand the potentials and pathologies of mind relative to the challenges of human survival. It is easier, however, to focus on technology or policy or anything else instead of looking inward to the complexities of human psychology, which is the most difficult and important challenge of building a decent world. The failure to do so explains in large measure why most people underestimate the scope, scale, depth, and causes of the human destruction of nature but, as if caught in a bad dream, we seem powerless to stop it. The rapid destabilization of climate and the destruction of the web of life are symptoms of a prior derangement in our manner of thinking and in our ability to even think clearly about how we think. So what is known about the mind that would usefully to enhance our longer-term prospects? For one thing we know that, whatever the reality, people go to considerable lengths to maintain a favorable self-image and deny unpleasant truths, particularly those that run against deeply ingrained beliefs and world views (Alport 1954). People in the United States, for example, the largest users of Prozac, proudly think of themselves as an optimistic, can-do people not easily given to doubt or despair. That is mostly a useful outlook, until it is not. According to Evan Connell, George Armstrong Custer's last recorded words just before the opening shots at the battle of Little Big Horn, were a stirring: “Hurrah boys, now we have them!” Optimistic bravado in the face of long odds is a much admired trait. Sometimes it works out and sometimes it does not. Unfortunately for Custer that day, Sitting Bull and the Sioux were not much amused and apparently not particularly awed by the chutzpah of the 7th Calvary. In our own time, the 1992 pronouncement by George Herbert Walker Bush that “The American way of life is not negotiable” came only a decade before Osama bin Laden negotiated it downward several trillion dollars depending on how much one cares to include. The end of cheap oil will take it down several more notches. Denial is apparent in the failure to grasp the vulnerabilities of modern society to problems such as climate destabilization. Like Voltaire's Dr. Pangloss, we tend to believe that things always work out for the best. I recently asked a class of U.S. college students, for example, how they would define climatic change. After some discussion, they reached a typically American consensus that it should be defined as “an opportunity.” They were not clear exactly how the opportunity would manifest at various increments of warming for exactly whom and I refrained from asking how the opportunities would work out for those now abandoning their ancestral homes on the coral atoll of Tuvalu, or people living in low-lying areas of Bangladesh, or victims of the larger storms said to be on the way or farmers in the Midwest facing more heat waves and drought, or the 150,000 we are told will die this year in weather events driven by climate change. These are smart students, but they reflect the optimism of youth and the deep tendency to deny unpleasant things now amplified by Western culture moving at warp speed. We, particularly in the West, are inclined to interpret all difficulties and impediments as merely problems that by definition are solvable with enough money, research, and technology. For another thing, we know that people often hold 2 contrary beliefs at the same time and remain happily oblivious to the contradictions. Psychologists call this “cognitive dissonance” (Festinger 1957). The trait manifests among those whose professed creed requires loving one's enemies while zealously bombing the hell out of them, without so much as a flicker of confusion. Humans, perhaps, are not so much rational creatures as very proficient rationalizers.

**1AR**

**pragmatic policy is the only way to solve — dealing with the nitty gritty details of policy gives us the tool to understand government and effectuate change — that’s McClean — specifically, they’ve conceded lack of detail-oriented policy flips the alt because we won’t be able to effectuate change —this is especially true for cyber operations**

**Keuter 10, President of the George Marshall Institute**, Cybersecurity: Challenging Questions With Incomplete Answers, www.marshall.org/pdf/materials/911.pdf‎

To say that the Internet has transformed society is as obvious as acknowledging its vulnerability. The average American, and consequently, the average American’s congressperson~~man~~ and their staffs, recognize both but lack appreciation, understanding, and insight of the issues involved and the costs and consequences of the available options. Policy makers and the public lack the **detailed knowledge required to critically judge what can or should be done** to address its weaknesses and vulnerabilities. That fact coupled with the immaturity of the policy consensus on what to do explains the intensity of the questioning of General Alexander and the broader concerns about the government’s plans for defending cyberspace.

**We don’t think we’re the state, we endorse something the state should do — this stops extinction**

**Small 6** (Jonathan, former Americorps VISTA for the Human Services Coalition,“Moving Forward,” The Journal for Civic Commitment, Spring, http://www.mc.maricopa.edu/other/engagement/Journal/Issue7/Small.jsp)

What will be the challenges of the new millennium? And how should we equip young people to face these challenges? While we cannot be sure of the exact nature of the challenges, we can say unequivocally that humankind will face them together. If the end of the twentieth century marked the triumph of the capitalists, individualism, and personal responsibility, the new century will present challenges that require collective action, unity, and enlightened self-interest. Confronting global warming, depleted natural resources, global super viruses, global crime syndicates, and multinational corporations with no conscience and no accountability will require cooperation, openness, honesty, compromise, and most of all solidarity – ideals not exactly cultivated in the twentieth century. We can no longer suffer to see life through the tiny lens of our own existence. Never in the history of the world has our collective fate been so intricately interwoven. Our very existence depends upon our ability to adapt to this new paradigm, to envision a more cohesive society. With humankind’s next great challenge comes also great opportunity. Ironically, modern individualism backed us into a corner. We have two choices, work together in solidarity or perish together in alienation. Unlike any other crisis before, the noose is truly around the neck of the whole world at once. Global super viruses will ravage rich and poor alike, developed and developing nations, white and black, woman, man, and child. Global warming and damage to the environment will affect climate change and destroy ecosystems across the globe. Air pollution will force gas masks on our faces, our depleted atmosphere will make a predator of the sun, and chemicals will invade and corrupt our water supplies. Every single day we are presented the opportunity to change our current course, to survive modernity in a manner befitting our better nature. Through zealous cooperation and radical solidarity we can alter the course of human events. Regarding the practical matter of equipping young people to face the challenges of a global, interconnected world, we need to teach cooperation, community, solidarity, balance and tolerance in schools. We need to take a holistic approach to education. Standardized test scores alone will not begin to prepare young people for the world they will inherit. The three staples of traditional education (reading, writing, and arithmetic) need to be supplemented by three cornerstones of a modern education, exposure, exposure, and more exposure. How can we teach solidarity? How can we teach community in the age of rugged individualism? How can we counterbalance crass commercialism and materialism? How can we impart the true meaning of power? These are the educational challenges we face in the new century. It will require a radical transformation of our conception of education. We’ll need to trust a bit more, control a bit less, and put our faith in the potential of youth to make sense of their world. In addition to a declaration of the gauntlet set before educators in the twenty-first century, this paper is a proposal and a case study of sorts toward a new paradigm of social justice and civic engagement education. Unfortunately, the current pedagogical climate of public K-12 education does not lend itself well to an exploratory study and trial of holistic education. Consequently, this proposal and case study targets a higher education model. Specifically, we will look at some possibilities for a large community college in an urban setting with a diverse student body. Our guides through this process are specifically identified by the journal Equity and Excellence in Education. The dynamic interplay between ideas of social justice, civic engagement, and service learning in education will be the lantern in the dark cave of uncertainty. As such, a simple and straightforward explanation of the three terms is helpful to direct this inquiry. Before we look at a proposal and case study and the possible consequences contained therein, this paper will draw out a clear understanding of how we should characterize these ubiquitous terms and how their relationship to each other affects our study. Social Justice, Civic Engagement, Service Learning and Other Commie Crap Social justice is often ascribed long, complicated, and convoluted definitions. In fact, one could fill a good-sized library with treatises on this subject alone. Here we do not wish to belabor the issue or argue over fine points. For our purposes, it will suffice to have a general characterization of the term, focusing instead on the dynamics of its interaction with civic engagement and service learning. Social justice refers quite simply to a community vision and a community conscience that values inclusion, fairness, tolerance, and equality. The idea of social justice in America has been around since the Revolution and is intimately linked to the idea of a social contract. The Declaration of Independence is the best example of the prominence of social contract theory in the US. It states quite emphatically that the government has a contract with its citizens, from which we get the famous lines about life, liberty and the pursuit of happiness. Social contract theory and specifically the Declaration of Independence are concrete expressions of the spirit of social justice. Similar clamor has been made over the appropriate definitions of civic engagement and service learning, respectively. Once again, let’s not get bogged down on subtleties. Civic engagement is a measure or degree of the interest and/or involvement an individual and a community demonstrate around community issues. There is a longstanding dispute over how to properly quantify civic engagement. Some will say that today’s youth are less involved politically and hence demonstrate a lower degree of civic engagement. Others cite high volunteer rates among the youth and claim it demonstrates a high exhibition of civic engagement. And there are about a hundred other theories put forward on the subject of civic engagement and today’s youth. But one thing is for sure; today’s youth no longer see government and politics as an effective or valuable tool for affecting positive change in the world. Instead of criticizing this judgment, perhaps we should come to sympathize and even admire it. Author Kurt Vonnegut said, “There is a tragic flaw in our precious Constitution, and I don’t know what can be done to fix it. This is it: only nut cases want to be president.” Maybe the youth’s rejection of American politics isn’t a shortcoming but rather a rational and appropriate response to their experience. Consequently, the term civic engagement takes on new meaning for us today. In order to foster fundamental change on the systemic level, which we have already said is necessary for our survival in the twenty-first century, we need to fundamentally change our systems. Therefore, part of our challenge becomes convincing the youth that these systems, and by systems we mean government and commerce,have the potential for positive change.Civic engagement consequently takes on a more specific and political meaning in this context. Service learning is a methodology and a tool for teaching social justice, encouraging civic engagement, and deepening practical understanding of a subject. Since it is a relatively new field, at least in the structured sense, service learning is only beginning to define itself. Through service learning students learn by experiencing things firsthand and by exposing themselves to new points of view. Instead of merely reading about government, for instance, a student might experience it by working in a legislative office. Rather than just studying global warming out of a textbook, a student might volunteer time at an environmental group. If service learning develops and evolves into a discipline with the honest goal of making better citizens, teaching social justice, encouraging civic engagement, and most importantly, exposing students to different and alternative experiences, it could be a major feature of a modern education. Service learning is the natural counterbalance to our current overemphasis on standardized testing. Social justice, civic engagement, and service learning are caught in a symbiotic cycle. The more we have of one of them; the more we have of all of them. However, until we get momentum behind them, we are stalled. Service learning may be our best chance to jumpstart our democracy. In the rest of this paper, we will look at the beginning stages of a project that seeks to do just that.

**Our obligation is to make the state ethical – the state is inevitable and the alternative to state ethics is the destruction of the other.**

**Simmons 99** Professor of Political Science @ ASU

(William Paul Simmons, current Associate, formerly at Bethany College in the Department of History and Political Science, “The Third: Levinas' theoretical move from an-archical ethics to the realm of justice and politics,” Philosophy & Social Criticism November 1, 1999 vol. 25 no. 6)

Since ‘it is impossible to escape the State’, 70 Levinas insists that the state be made as ethical as possible. The world of institutions and justice must be held in check by the an-archical responsibility for the Other. Levinas calls for both an-archy and justice. Alongside the an-archical responsibility for the Other there is a place for the realm of the said, which includes ontology, justice and **politics**. Levinas’ thought is not apolitical as many have charged. **His harsh critiques of the political realm refer to a politics unchecked by ethics**. For example, in Totality and Inﬁnity, **Levinas sees politics as antithetical to an ethics based on the Other**. ‘The art of foreseeing war and winning it by every means – politics – is henceforth enjoined as the very exercise of reason. Politics is opposed to morality, as philosophy to naïveté.’ 71 **Politics unrestrained**, by necessity, **totalizes the Other by reducing him or her to abstract categories**. **Levinas will call for a politics that is founded on ethics and not on ontology. The state must be answerable to the an-archical relationship with the Other, it must strive to maintain the exteriority of the Other**. Levinasian heteronomic political thought oscillates between the saying and the said, an-archy and justice, ethics and politics. The liberal state is the concrete manifestation of this oscillation. Levinas calls for a balance between the Greek and the Judaic traditions. **Neither tradition should dominate**. The fundamental contradiction of our situation (and perhaps of our condition) . . . that both the hierarchy taught by Athens and the abstract and slightly anarchical ethical individualism taught by Jerusalem are simultaneously necessary in order to suppress the violence.0020**Each of these principles, left to itself, only hastens the contrary of what it wants to secure.**