# 1AC

## Adv 1: Arms Race

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

Goldman 13

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

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

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

Moss 13

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

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

#### Cyber arms race causes world war

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

CSM 11

Christian Science Monitor

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

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

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

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

Austin, 8/6

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

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

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

Clarke and Knake ‘12

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

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

## Adv 2: Alliances

#### Congressional restrictions necessary for allied cooperation

Dunlap 12

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

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

#### The plan is key to secure cyberspace

Lord et al 11

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

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

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

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

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

Lawson ‘10

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

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

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

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

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

#### Legitimacy is key to band-wagon

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

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

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

Kazianis 12

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

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

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

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

RTT 13

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

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

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

Yoshihara 10

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

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

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

Colby et al 13

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

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

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

Rehman 13

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

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

## Plan

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

## Solvency

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

Bradbury 11

Assistant Attorney General for the Office of Legal Counsel

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

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

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

Goldsmith 10

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

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

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

Lewis 11

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

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

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

Dycus 10

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

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

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

Bastby 12

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

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

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

Hansen & Friedman 9

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

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

# 2AC

## Case

#### Uncontained disease leads to extinction

**Toolis**, the director of a major television series on the history of plagues, **09**

(Kevin, The Express, April 28, 2009 U.K. 1st Edition “Pandemic Pandemonium” lexis)

 It destroyed the Roman Empire, wiped out most of the New World and killed millions in Europe. How disease - not just Mexico's swine fever - has shaped the planet SCIENTISTS call it the Big Die Off, when a terrifying new virus rips through a species and kills up to a third of the entire population. And we all now could be facing a new apocalypse, though no one yet knows how potent the new strain of Mexican swine fever will be, or how many millions could die. Yet if history teaches us anything it tells us that the greatest danger the human race faces is not some crackpot North Korean dictator but a six-gene virus that could wipe out one third of the global population. Our real enemy, a new plague virus, is so small you can barely see it even with an advanced electron microscope. It has no morality, no thought or no plan. All it wants to do is reproduce itself inside another human body. We are just another biological opportunity, a nice warm place to feed and replicate. Viruses are as old as life itself. What is startling though is how vulnerable our globalised societies are to the threat of a new deadly plague. Before World Health Organisation scientists could identify this new H1N1 virus it had travelled halfway across the world via international flights.

#### Warming causes Extinction

**Tickell, 2008**

(Oliver, Climate Researcher, The Gaurdian, “On a planet 4C hotter, all we can prepare for is extinction”, <http://www.guardian.co.uk/commentisfree/2008/aug/11/climatechange>)

We need to get prepared for four degrees of global warming, Bob Watson told the Guardian last week. At first sight this looks like wise counsel from the climate science adviser to Defra. But the idea that we could adapt to a 4C rise is absurd and dangerous. Global warming on this scale would be a catastrophe that would mean, in the immortal words that Chief Seattle probably never spoke, "the end of living and the beginning of survival" for humankind. Or perhaps the beginning of our extinction. The collapse of the polar ice caps would become inevitable, bringing long-term sea level rises of 70-80 metres. All the world's coastal plains would be lost, complete with ports, cities, transport and industrial infrastructure, and much of the world's most productive farmland. The world's geography would be transformed much as it was at the end of the last ice age, when sea levels rose by about 120 metres to create the Channel, the North Sea and Cardigan Bay out of dry land. Weather would become extreme and unpredictable, with more frequent and severe droughts, floods and hurricanes. The Earth's carrying capacity would be hugely reduced. Billions would undoubtedly die. Watson's call was supported by the government's former chief scientific adviser, Sir David King, who warned that "if we get to a four-degree rise it is quite possible that we would begin to see a runaway increase". This is a remarkable understatement. The climate system is already experiencing significant feedbacks, notably the summer melting of the Arctic sea ice. The more the ice melts, the more sunshine is absorbed by the sea, and the more the Arctic warms. And as the Arctic warms, the release of billions of tonnes of methane – a greenhouse gas 70 times stronger than carbon dioxide over 20 years – captured under melting permafrost is already under way. To see how far this process could go, look 55.5m years to the Palaeocene-Eocene Thermal Maximum, when a global temperature increase of 6C coincided with the release of about 5,000 gigatonnes of carbon into the atmosphere, both as CO2 and as methane from bogs and seabed sediments. Lush subtropical forests grew in polar regions, and sea levels rose to 100m higher than today. It appears that an initial warming pulse triggered other warming processes. Many scientists warn that this historical event may be analogous to the present: the warming caused by human emissions could propel us towards a similar hothouse Earth.

#### Warming is real and anthropogenic–best climate data and models

Mueller 12

(The New York Times, Richard A. Mueller, July 28, 2012, “The Conversion of a Climate Change Skeptic” Richard A. Muller, a professor of physics at the University of California, Berkeley, and a former MacArthur Foundation fellow, is the author, most recently, of “Energy for Future Presidents: The Science Behind the Headlines.” <http://www.nytimes.com/2012/07/30/opinion/the-conversion-of-a-climate-change-skeptic.html?_r=1&pagewanted=all>)

CALL me a converted skeptic. Three years ago I identified problems in previous climate studies that, in my mind, threw doubt on the very existence of global warming. Last year, following an intensive research effort involving a dozen scientists, I concluded that global warming was real and that the prior estimates of the rate of warming were correct. I’m now going a step further: Humans are almost entirely the cause. My total turnaround, in such a short time, is the result of careful and objective analysis by the Berkeley Earth Surface Temperature project, which I founded with my daughter Elizabeth. Our results show that the average temperature of the earth’s land has risen by two and a half degrees Fahrenheit over the past 250 years, including an increase of one and a half degrees over the most recent 50 years. Moreover, it appears likely that essentially all of this increase results from the human emission of greenhouse gases. These findings are stronger than those of the Intergovernmental Panel on Climate Change, the United Nations group that defines the scientific and diplomatic consensus on global warming. In its 2007 report, the I.P.C.C. concluded only that most of the warming of the prior 50 years could be attributed to humans. It was possible, according to the I.P.C.C. consensus statement, that the warming before 1956 could be because of changes in solar activity, and that even a substantial part of the more recent warming could be natural. Our Berkeley Earth approach used sophisticated statistical methods developed largely by our lead scientist, Robert Rohde, which allowed us to determine earth land temperature much further back in time. We carefully studied issues raised by skeptics: biases from urban heating (we duplicated our results using rural data alone), from data selection (prior groups selected fewer than 20 percent of the available temperature stations; we used virtually 100 percent), from poor station quality (we separately analyzed good stations and poor ones) and from human intervention and data adjustment (our work is completely automated and hands-off). In our papers we demonstrate that none of these potentially troublesome effects unduly biased our conclusions. The historic temperature pattern we observed has abrupt dips that match the emissions of known explosive volcanic eruptions; the particulates from such events reflect sunlight, make for beautiful sunsets and cool the earth’s surface for a few years. There are small, rapid variations attributable to El Niño and other ocean currents such as the Gulf Stream; because of such oscillations, the “flattening” of the recent temperature rise that some people claim is not, in our view, statistically significant. What has caused the gradual but systematic rise of two and a half degrees? We tried fitting the shape to simple math functions (exponentials, polynomials), to solar activity and even to rising functions like world population. By far the best match was to the record of atmospheric carbon dioxide, measured from atmospheric samples and air trapped in polar ice. Just as important, our record is long enough that we could search for the fingerprint of solar variability, based on the historical record of sunspots. That fingerprint is absent. Although the I.P.C.C. allowed for the possibility that variations in sunlight could have ended the “Little Ice Age,” a period of cooling from the 14th century to about 1850, our data argues strongly that the temperature rise of the past 250 years cannot be attributed to solar changes. This conclusion is, in retrospect, not too surprising; we’ve learned from satellite measurements that solar activity changes the brightness of the sun very little. How definite is the attribution to humans? The carbon dioxide curve gives a better match than anything else we’ve tried. Its magnitude is consistent with the calculated greenhouse effect — extra warming from trapped heat radiation. These facts don’t prove causality and they shouldn’t end skepticism, but they raise the bar: to be considered seriously, an alternative explanation must match the data at least as well as carbon dioxide does. Adding methane, a second greenhouse gas, to our analysis doesn’t change the results. Moreover, our analysis does not depend on large, complex global climate models, the huge computer programs that are notorious for their hidden assumptions and adjustable parameters. Our result is based simply on the close agreement between the shape of the observed temperature rise and the known greenhouse gas increase.

## Risk K

#### We must weigh competing probabilities and dismiss threats to survival if they are very unlikely—the alternative is that we do nothing about any existential risk

POSNER 2004(Richard, US Court of Appeals judge and Senior Lecturer at the University of Chicago Law School, Catastrophe: Risk and Response 19)

The reason for the hedge in “essentially” is that I want to avoid making claims of metaphysical certainty. From a scientific standpoint, anything is possible. But some possibilities really are too remote to be worth worrying about, such as the possibility that my next breath will create a black hole or that the entire human population will be persuaded to commit suicide. To put this differently, we have to be selective in responding to the catastrophic risks because if we allow our imaginations to multiply their number indefinitely we’ll end up doing nothing about any of them.

#### Even if they win the world is getting better, war is still increasingly possible - multiple reasons

Ferguson 8

Laurence A. Tisch Professor of History at Harvard University, William Ziegler Professor of Business Administration at Harvard Business School, senior fellow at the Hoover Institute, graduated from Magdalen College in Oxford, named as one of the 100 most influential people in the world by Time Magazine, writer of many bestselling books, including The War of the World, generally a badass british historian, with a specialty in financial and economic history [9/26, Niall, interviewed by Joanne Myers, “The War of the World: Twentieth-Century Conflict and the Descent of the West”, Carnegie Council for Ethics in International Affairs, [https://www.carnegiecouncil.org/resources/transcripts/5396.html/:pf\_printable](https://www.carnegiecouncil.org/resources/transcripts/5396.html/%3Apf_printable), AL]

So **The War of the World**, singular, **is an attempt to explain why the twentieth century was so astonishingly violent**, not only in absolute terms—after all, the world is more populous than ever—but also in relative terms. **If you work out how many people died violently** in the course of the twentieth century, **it was of the order of 180 million.** One estimate puts it at **one in every twenty-two deaths**; that is to say, one in every twenty-two human deaths in the twentieth century **was violent**, not natural. If you take the most explosive of all the conflicts, the one which is right at the heart of this book, World War II, roughly 60 million people died violently in that war. If you work out what percentage of the population of the world in 1939 that was, it's between 2 and 3 percent. None of the great wars of modern history—I hesitate to go further back than 1600, for reasons I'll explain in a second—had such a terrifyingly high mortality rate as that. So there is a question here about why the twentieth century was so violent. Now, experts on thirteenth-century Asia assure me that Genghis Khan—who I used to call "Genghis" in my ignorance—killed comparable proportions, if not higher proportions, of the world population in his time. And it may even be that if we go back beyond the ancient world to the prehistoric world, that primitive societies were still more violent. Some primitive tribes have astonishingly high mortality rates, according to the anthropologists. But that's not really the point. **The** twentieth **century is astonishing because that kind of violence coincided with unprecedented progress.** So there is a paradox here which makes the twentieth century really unique. **The average human being got maybe four times better off**, possibly five times better off, if you try to work out a figure for per-capita gross domestic product. He or she was more likely to live in democracy at the end of the twentieth century than at the beginning. In all kinds of ways, scientific and cultural, the twentieth century was a time of astonishing progress. So it is really very important for us to try to understand why progress coincided with holocausts of violence, with some sixteen conflicts that claimed a million or more deaths. Seen in these terms, **the world wars become part of a continuum of organized violence.** The book is an attempt to explain why. The best **explanations** are easy to remember. At least one person besides me in this room will be jet-lagged, and that person will be glad of the fact that my explanation is relatively easy to commit to memory. It has four parts, and each of them begins with the letter "E," which I find always helps under exam conditions. **The first is** economic volatility. Now, why is economic volatility important? I know we're uptown, we're not on Wall Street, but give me a couple of minutes on this. It's important because it helps you to identify the dangerous times. You see, it's crucial that **the twentieth century was not evenly violent.** Not every year, not every decade, was equally violent. **There were huge spikes of organized violence**, particularly between 1914 and 1945. I try to show that one reason for this is that the mid-twentieth century was by far the most volatile time. **If you look at fluctuations in growth, inflation, asset prices, the interwar period stands out as being roughly seven times more volatile** than our own time. We have almost forgotten what volatility feels like these days. The last ten years have seen almost unprecedented smoothness in the pattern of economic growth in the world's developed economies. And yet, transport yourself back to the 1920s and 1930s, and you enter a time when economic activity went up and down like some kind of fairground ride. So **economic volatility**, the first of my E's, **helps us narrow down the timeframe**, because we need to understand why, for example, the early 1940s were the most dangerous time of all time. My second E is ethnic disintegration. This **is terribly important**. In many ways, **it's the most important argument**—and, I think, original argument—in the book. It matters because it helps you identify where violence happened, because, once again, it wasn't evenly geographically distributed. It was, in fact, heavily concentrated in certain parts of the world. In a fifty-year period I identify, from 1904-1953, violence in the world was extraordinarily concentrated in two places: Central and Eastern Europe; and at the other end of Eurasia, Manchuria and the Korean Peninsula. If you were born in those parts of the world, your chances of dying violently were much, much higher than if you were born in, say, Canada. That is extremely important. Why? Because **when you look at those places**—look at an ethno-linguistic map of, say, Central Europe in 1900—**what leaps out is what patchworks they were, ethno-linguistic patchworks, extraordinarily heterogeneous societies with enormously interlocked minorities.** Now, the key to understanding what happened in the mid-twentieth century is to realize that it was a process of disintegration. In 1900, **these multiethnic societies looked remarkably stable.** Indeed, in some places, particularly in the German-speaking cities of Central Europe, levels of intermarriage, coeducation, or any of the measures you might take when you were looking for evidence of assimilation and integration, suggested that problems of ethnic conflict were diminishing fast. In a city like Hamburg in the 1920s, one in every two marriages involving at least one Jewish partner was to a non-Jewish partner. Half of these marriages were mixed. Looking at the world in the 1920s, you would have said that Germany was the place that had, in effect, solved what late-nineteenth century racists had called "the Jewish question." **But that would be wrong**, because what happened—and it wasn't only with respect to Jews and Germans—what happened in Central and Eastern Europe in the period after around 1929 was an astonishing ripping apart of multiethnic societies. **I talk about** the city of **Chernovitz as just an example of what a multiethnic city looked like.** It is now Chernivtsi in Ukraine, and very little remains of its identity as Chernovitz. But in 1900 Chernovitz was a great multiethnic Hapsburg city inhabited by German bureaucrats, German-Jewish academics, but also by Ukranians, Poles, Romanians. **It was a kind of melting pot—and yet, it was a melting pot that exploded**, that blew up, as if something went wrong in the recipe. So ethnic disintegration is the key to understanding the location, if you like, of conflict, to understanding why Ukraine was a bad place to be born in and Sweden much less so. 3) My third component in the great equation of disaster also begins with E: it is empires in decline**.** Counterintuitively from some liberal perspectives, **I argue that it is when empires decline and fall that violence is most likely to spike.** It is **at the moment of this dissolution** that **the stakes are suddenly terribly high and local elites do battle** for, as it were, the political succession. Roughly, twelve empires declined and fell in the course of the twentieth century. That's a very large number, indeed. In fact, I think I can safely say that in no previous century had so many empires hit the deck. I think that helps explain again why the middle of the twentieth century was so tremendously violent. These great waves of imperial decline, which began with the collapse of the Qing Dynasty in China, continued through the dissolution of the Romanov, Ottoman, Habsburg, and Hohenzollern empires in Central and Eastern Europe towards the end of the First World War, experienced another great wave of crisis when the Japanese unleashed their extraordinary assault on the European, and indeed American, empires in Asia. These **times of imperial crisis produced great spikes in the level of organized violence.** If you want to go beyond that timeframe, think only of 1947, a date much on our minds. That, after all, saw in many ways the highest level of violence in the history of British India, at its end, at its moment of dissolution. It illustrates the key point. As the imperial authority wanes, those on the ground, in the localities, suddenly have a lot to fight for, and particularly in multiethnic societies. And, since most of the great empires were extraordinarily multiethnic, it's not surprising that in the time of imperial dissolution minorities found themselves vulnerable as never before to what was once called "the tyranny of the majority." 4) **The fourth, and final**, of my E's - just to recap for those of you revising: economic volatility was the first, ethnic disintegration was the second, empires in decline was the third - the fourth **is** Eastern ascendancy**.** You see, **we often misunderstand the twentieth century. We think of it in terms of the triumph of the West**—or even the American century, although I think that was supposed to begin after World War II. I argue that **this is a misunderstanding of the trajectory of modern history.** It was in 1900 that the West truly ruled the world. In 1900, 82 percent of the world's population lived in empires, and most of those empires were controlled by Western powers. By Western powers, I mean principally the European powers, but also the United States. It is an astonishing statistic to my mind. It also illustrates better than anything the sheer dominance of Western power. When a relatively small percentage of mankind—and, after all, if you figure out the West as I do in the book, it was never as much as 20 percent of the world's population - such a small proportion was able to rule over the majority of the world's population, because 50 percent of the world's population lived in Asia in 1900, and only a very few (the Japanese) enjoyed anything resembling political independence. I think the descent of the West—and I use the term advisedly, not to invoke the memory of Oswald Spengler, a man of whom I disapprove; I use the term because I want to connote, not only a crude decline from power, but also perhaps a descent in moral terms—**the descent of the West is the key to understanding the** twentieth **century. It was a violent and painful process.** It was never smooth. That is why the conflict between Japan and the Western powers in Asia and the Pacific was so astonishingly brutal. We should not think of the transfer of power from West to East as a naturally smooth power. **The twentieth century suggests that it has been punctuated by violence.** That's why 1904 is such an important date. That's the moment Japan succeeds in beating a European empire for the first time, sinking the entire Russian expeditionary force sent to fight over Korea/Manchuria in the Russo-Japanese War. I think I just have time to draw some conclusions from this argument for our own time. In some ways, **the problems that bedeviled the first half of the** twentieth **century were solved horribly**; solved by ethnic cleansing, solved by genocide, solved by partition. **The killing fields** at either end of Eurasia—Central and Eastern Europe, Korea/Manchuria—**ceased to be killing fields** after 1953. **And yet, violence didn't stop. I** try to **argue** in the epilogue **that** in many ways **the Cold War wasn't cold at all**; **it was a third world war if you were in Guatemala or Cambodia or Angola.** In fact, I call it the "Third World's war," because **all that had happened was that** violence was relocated **to places that people** in the dominant powers during the Cold War **seldom saw.** So violence didn't stop during the Cold War, and **there is no reason to assume that it has stopped since the Cold War.** There is one part of **the world today** which **already exhibits all the traits that I see as having been** explosive in the mid-twentieth century. Where **economic volatility**, if you just look at growth rates in these countries for the past twenty years, is roughly five times higher than in the United States; where **ethnic disintegration** is already well underway, a region where a multiethnic city is in the process of tearing itself apart as we speak; and a part of the world where in my view—and those of you who know my last book, Colossus, will see what I am driving at—where in my view **an empire is manifestly in decline.** I am talking about the Middle East, and the empire I have in mind is, of course, the American empire. To me **the most troubling thing** about the Middle East today is **this conjunction of extraordinary economic volatility.** Look at growth rates in Iraq and its neighbors since 1986. You are looking at the kind of volatility Central Europe experienced in the 1920s and 1930s. **Look at what is happening in Iraq. Against all expectations**—and I include myself in this—**a war between insurgents and occupiers has morphed** before our very eyes **into** something very like **a civil war** between Sunni and Shiite Muslims, not to forget Kurds. **The process whereby a multiethnic society tears itself apart is all too familiar** to someone like me, who specializes in European history. We have been here before, and we know how it starts, how society's communities that have lived together relatively peacefully despite ethnic and sectarian differences suddenly turn on one another, and neighbor kills neighbor. In The Brookings Institute's recent surveys of Iraq, there are some astonishing findings that leap off the page. **Sectarian violence is an order of magnitude higher this year than last year.** Ninety-two percent of votes in Iraqi elections were cast by sectarian parties. In surveys, **enormous percentages of Sunni Iraqis say that they have** themselves **experienced**, or know people who have experienced, **ethnic cleansing.** All of this is unfolding because it seems to me **the dominant empire in that region**, which certainly exerted extraordinary informal power in the 1970s, **is waning, losing credibility, losing control.** In 1920, it was possible for an English-speaking empire to quell an insurgency and stabilize multiethnic Iraq. But then the ratio of Iraqis to occupying forces was something like 20:1. Today it is 210:1. In other words, the odds of success were an order of magnitude that is smaller this time around. That demographic transition is part of what I mean when I describe the descent of the West. Today the powers that I call the Western powers account for barely 10 percent of the world's population. The populations of the East have grown relatively. That means the prospect of Western power is, from the very word go, significantly diminished. If I am right and the stakes are right here, **this is a somber subject.** If I am right, then **the ingredients for a much higher level of conflict than we have yet seen** in the Middle East **are in place.** That may sound shocking to those of you who think of the Middle East as a terribly violent place. But actually, the amazing thing about the Middle East is how small its wars have generally been, with the sole exception of the Iran-Iraq war. We could see much more violence there. **We could see violence of the sort we saw in Central** and Eastern **Europe** in the early 1940s, because the ingredients are all in place. In other words, ladies and gentlemen, **The War of the World implies**, to my deep alarm, **the possibility of a sequel**—a sequel **played out**, not in the killing fields of Poland/Ukraine, but **in the killing fields** conceivably of Palestine, of Lebanon, of the Persian Gulf.

#### The convergence of hyper-competition and hyper-power status make conflict increasingly likely

Capie 11

Senior Lecturer in International Relations at Victoria University of Wellington, New Zealand, Visiting Scholar at the Weatherhead Center for International Affairs at Harvard University, Research Associate in the ASEAN Studies Centre at American University, co-editor of the journal Political Science, member of the editorial board of Asian Politics and Policy [7/6, David, “Welcome to the dark side? Mittelman's encounter with global insecurity”, Global Change, Peace & Security, Volume 23, Issue 2, Taylor and Francis, AL]

The book's thesis is that **there are two systemic drivers of contemporary security and insecurity. The first is** what Mittelman calls hypercompetition**, the** ‘**intensified competition that agglomerates markets**’. **Accelerated by** ‘new **tech**nologies, **the rise of transnational capital and increasing labour mobility**’, national **production systems are giving way to global firms** with supply chains extending across the world. The language of **war has permeated commerce, with corporations embracing aspects of a Hobbesian** ‘**warre of all against all**’ **as they seek to cut costs, raise efficiency and dominate markets.** Hypercompetition is ‘heavily but not totally American’ in several of its facets, including the long reach of US markets, investment in R&D, the prevalence of neoliberal ideas about the ordering of the economy and society as well as the prevalence of American popular culture. **The second is the** concentration of power **in a**n historically **unprecedented hegemonic actor: the U**nited **S**tates of America. The book puts aside the traditional vocabulary of geopolitics, arguing that the USA is not a superpower or even a great power enjoying a unipolar moment. Rather, ‘**in light of the large distance between the U**nited **S**tates **and the other major powers** in a globalizing world’, **the preferred term is hyperpower.**3 The idea builds on the notion of hyperpuissance coined by French foreign minister Hubert Vedrine in 1998, but, **drawing on Gramscian notions of consensual hegemony** and Foucauldian biopolitics, **Mittelman gives it more precision** and extracts greater analytic leverage from it. Notably, in his vision, **although there can be only one hyperpower, the concept extends beyond the US**A as a state. Instead, **hyperpower is imperial** in character, **a** ‘**weblike structure**, including a net of overseas military bases, a clutch of allies, aspects of ideological appeal, and an educational system that widely propagates values **associated with those at the epicentre of globalization**’.4 **When hypercompetition and hyperpower converge** (or coincide), **the conditions point to** the book's third core concept: hyper**conflict. This arises** ‘**out of the tension between the logic of statecentric and polycentric worlds**’ and when ‘a medley of nonstate actors both accommodates and more assertively resists state initiatives’.5 Although only in a ‘nascent’ phase, **hyperconflict expresses itself as** ‘**heightened coercion and weakening consensus**’, ‘**pervasive uncertainty**’ **and** ‘a **rising** climate of **fear**’.6 Contrasting the ‘old’ order of war with the ‘new’ order of militarized globalization, Mittelman argues that **the old order was** ‘**permeated by wars** between states and within them, as well as partial safeguards with rules to manage them’. **This has been** ‘partly **supplanted by hyperpower enmeshed in various conflicts**, but the most flagrant conflicts deny military solutions. In fact, **the application of more** and more **coercion inflames tensions, emboldens unconventional enemies, and inspires recruits** for their causes.’7 **The three concepts** serve less as a model or formal explanation of contemporary insecurity and **work** more **as a heuristic**, ‘a grammar for thinking about evolving forms of world order’.8 The author seeks to provide a vocabulary through which the links between globalization and insecurity can be understood holistically and critically explored. One of Hyperconflict's most significant contributions is the wide-ranging theoretical discussion that fills its first two chapters, offering a sophisticated distillation of the vast literatures on globalization and peace and conflict to form a compelling and provocative account.

#### Seriously, there will be wars: economics, security dilemma, nationalism

Mearsheimer 99

Mearsheimer, Distinguished Professor of Political Science, 1999. ¶ (John Mearsheimer, “Is Major War Obsolete?” 1999, http://www.ciaonet.org/conf/cfr10/index.html

So what I’m saying here is you can have an absence of war, but it can be for two different sets of reasons; one the obsolescence rationale that Michael laid out, and two the deterrence rationale. Now I think the central claim that’s on the table is wrong-headed, and let me tell you why. First of all, there are a number of good reasons why great powers in the system will think seriously about going to war in the future, and I’ll give you three of them and try and illustrate some cases. First, states oftentimes compete for economic resources. Is it hard to imagine a situation where a reconstituted Russia gets into a war with the United States and the Persian Gulf over Gulf oil? I don’t think that’s implausible. Is it hard to imagine Japan and China getting into a war in the South China Sea over economic resources? I don’t find that hard to imagine. A second reason that states go to war which, of course, is dear to the heart of realists like me, and that’s to enhance their security. Take the United States out of Europe, put the Germans on their own; you got the Germans on one side and the Russians on the other, and in between a huge buffer zone called eastern or central Europe. Call it what you want. Is it impossible to imagine the Russians and the Germans getting into a fight over control of that vacuum? Highly likely, no, but feasible, for sure. Is it hard to imagine Japan and China getting into a war over the South China Sea, not for resource reasons but because Japanese sea-lines of communication run through there and a huge Chinese navy may threaten it? I don’t think it’s impossible to imagine that. What about nationalism, a third reason? China, fighting in the United States over Taiwan? You think that’s impossible? I don’t think that’s impossible. That’s a scenario that makes me very nervous. I can figure out all sorts of ways, none of which are highly likely, that the Chinese and the Americans end up shooting at each other. It doesn’t necessarily have to be World War III, but it is great-power war. Chinese and Russians fighting each other over Siberia? As many of you know, there are huge numbers of Chinese going into Siberia. You start mixing ethnic populations in most areas of the world outside the United States and it’s usually a prescription for big trouble. Again, not highly likely, but possible. I could go on and on, positing a lot of scenarios where great powers have good reasons to go to war against other great powers.

#### Energy competition increases the risk of major power escalation

Klare 8

Klare, A professor of peace and world security studies at Hampshire College, 2008 ¶ (Michael T.,"The End of the World as You Know It,", <http://zmag.org/znet/viewArticle/17176>)

Until very recently, the mature industrial powers of Europe, Asia, and North America consumed the lion's share of energy and left the dregs for the developing world. As recently as 1990, the members of the Organization of Economic Cooperation and Development (OECD), the club of the world's richest nations, consumed approximately 57% of world energy; the Soviet Union/Warsaw Pact bloc, 14% percent; and only 29% was left to the developing world. But that ratio is changing: With strong economic growth in the developing countries, a greater proportion of the world's energy is being consumed by them. By 2010, the developing world's share of energy use is expected to reach 40% and, if current trends persist, 47% by 2030. China plays a critical role in all this. The Chinese alone are projected to consume 17% of world energy by 2015, and 20% by 2025 -- by which time, if trend lines continue, it will have overtaken the United States as the world's leading energy consumer. India, which, in 2004, accounted for 3.4% of world energy use, is projected to reach 4.4% percent by 2025, while consumption in other rapidly industrializing nations like Brazil, Indonesia, Malaysia, Thailand, and Turkey is expected to grow as well.**These rising economic dynamos will have to compete with the mature economic powers for access to remaining untapped reserves of exportable energy** -- in many cases, bought up long ago by the private energy firms of the mature powers like Exxon Mobil, Chevron, BP, Total of France, and Royal Dutch Shell. Of necessity, the new contenders have developed a potent strategy for competing with the Western "majors": they've created state-owned companies of their own and fashioned strategic alliances with the national oil companies that now control oil and gas reserves in many of the major energy-producing nations.

#### Nuclear war causes extinction - prefer the latest studies

Choi 11

writer for National Geographic News [Charles Q., 2/22/2011, National Geographic, “Small Nuclear War Could Reverse Global Warming for Years?,” <http://news.nationalgeographic.com/news/2011/02/110223-nuclear-war-winter-global-warming-environment-science-climate-change/>, DS]

**Even a regional nuclear war could spark "unprecedented" global cooling and reduce rainfall for years, according to U.S. government computer models. Widespread famine and disease would likely follow, experts speculate.** During the Cold War a nuclear exchange between superpowers—such as the one feared for years between the United States and the former Soviet Union—was predicted to cause a "nuclear winter." In that scenario **hundreds of nuclear explosions spark huge fires, whose smoke, dust, and ash blot out the sun for weeks amid a backdrop of dangerous radiation levels.** Much of humanity eventually dies of starvation and disease. Today, with the United States the only standing superpower, nuclear winter is little more than a nightmare. But nuclear war remains a very real threat**—for instance, between developing-world nuclear powers, such as India and Pakistan.** To see what climate effects such a regional nuclear conflict might have, **scientists from NASA and other institutions modeled a war involving a hundred Hiroshima-level bombs, each packing the equivalent of 15,000 tons of TNT—just 0.03 percent of the world's current nuclear arsenal.** (See a National Geographic magazine feature on weapons of mass destruction.) **The researchers predicted the resulting fires would kick up roughly five million metric tons of black carbon into the upper part of the troposphere, the lowest layer of the Earth's atmosphere.** In NASA climate models, **this carbon then absorbed solar heat and, like a hot-air balloon, quickly lofted even higher, where the soot would take much longer to clear from the sky.** (Related: "'Nuclear Archaeologists' Find World War II Plutonium.") Reversing Global Warming? **The global cooling caused by these high carbon clouds wouldn't be as catastrophic as a superpower-versus-superpower nuclear winter, but "the effects would still be regarded as leading to unprecedented climate change,"** **research physical scientist Luke Oman said** during a press briefing Friday at a meeting of the American Association for the Advancement of Science in Washington, D.C. **Earth is currently in a long-term warming trend. After a regional nuclear war, though, average global temperatures would drop by 2.25 degrees F (1.25 degrees C) for two to three years afterward,** the models suggest. At the extreme, **the tropics, Europe, Asia, and Alaska would cool by 5.4 to 7.2 degrees F (3 to 4 degrees C),** according to the models. Parts of the Arctic and Antarctic would actually warm a bit, due to shifted wind and ocean-circulation patterns, the researchers said. After ten years, **average global temperatures would still be 0.9 degree F (0.5 degree C) lower than before the nuclear war**, the models predict. (Pictures: "Red Hot" Nuclear-Waste Train Glows in Infrared.) Years Without Summer **For a time Earth would likely be a colder, hungrier planet. "Our results suggest that agriculture could be severely impacted, especially in areas that are susceptible to late-spring and early-fall frosts**," said Oman, of NASA's Goddard Space Flight Center in Greenbelt, Maryland. **"Examples similar to the crop failures and famines experienced following the Mount Tambora eruption in 1815 could be widespread and last several years**," he added. That Indonesian volcano ushered in "the year without summer," a time of famines and unrest. (See pictures of the Mount Tambora eruption.) **All these changes would also alter circulation patterns in the tropical atmosphere, reducing precipitation by 10 percent globally for one to four years**, the scientists said. **Even after seven years, global average precipitation would be 5 percent lower than it was before the conflict**, according to the model. In addition, researcher Michael Mills, of the National Center for Atmospheric Research in Colorado, found **large decreases in the protective ozone layer, leading to much more ultraviolet [uv] radiation reaching Earth's surface and harming the environment and people.** "The main message from our work," NASA's Oman said, "would be that even a regional nuclear conflict would have global consequences."

#### Nuclear war would destroy the environment and the food chain, ensuring extinction of all life

Thompson 2008

Andrea Thompson 2008 LiveScience “Regional Nuclear War would affect entire globe”, <http://www.livescience.com/environment/080407-nuclear-ozonehole.html>

Previous studies ,including a 1985 National Research Council Report, had examined the effects of nuclear war on ozone loss by considering the chemicals the bombs would spew into the atmosphere. But they failed to consider the massive smoke plumes that would rise into the air as the bombed-out cities burned.  The new study considers both, painting a picture of citywide firestorms and ozone destruction.  "It has as much to do with the bombs as it does with the fuels in modern megacities," Mills said. "Pretty much everything will burn in a city."  A previous study conducted by Toon showed that as buildings, cars and other infrastructure burned, the air above would fill with soot. Some of this soot would fall out of the atmosphere in so-called black rains, but the rest would make its way up into the atmosphere within a matter of days, Mills said.  The heat from these firestorms (like those that destroyed Dresden, Germany, in World War II) would push the soot-filled air into the upper troposphere, the bottom-most layer of the Earth's atmosphere. The blackened air would then be warmed by incoming sunlight and would rise further, into the stratosphere, which sits atop the troposphere and is the layer of the atmosphere where the ozone that protects us from the sun's harmful ultraviolet rays is found. The soot could eventually rise 50 miles (80 kilometers) up in the atmosphere, the study found.  The new study found that up in the stratosphere, the soot would continue to absorb incoming sunlight and heat the surrounding air. This heat would jump-start the chemical reactions that destroy ozone.  "So the temperatures go way up and this changes the rates of a number of catalytic cycles that destroy ozone," Mills told LiveScience. As these cycles speed up, they wipe out the ozone molecules much faster than they would at normal temperatures.  The heating of the stratosphere would also alter its circulation, prolonging the time that it normally takes for the air in that layer to turn over, prolonging the soot's effect on ozone destruction.  Global ozone hole  Above the mid-latitudes, where the United States and most of Europe lie, ozone levels would drop by 25 to 40 percent. At higher northern latitudes, ozone losses would reach 50 to 70 percent, the model results show.   "The models show this magnitude of ozone loss would persist for five years, and we would see substantial losses continuing for at least another five years," Mills said.  The 1985 NRC report found only a 17 percent depletion of stratospheric ozone over the Northern Hemisphere, which would recover by half in just three years.  "The big surprise is that this study demonstrates that a small-scale, regional nuclear conflict is capable of triggering ozone losses even larger than losses that were predicted following a full-scale nuclear war," Toon said.  These losses would drop ozone levels below the amount that typically marks the seasonal ozone hole over Antarctica — only this ozone hole would extend from about 20 degrees north and south of the equator, creating a near-global ozone hole.  The loss of this protective "sunscreen" layer could have a terrible impact on the plants and animals living below that would then be susceptible to UV radiation.  Damage to plants and animals at mid-latitudes would likely rise sharply, according to the study, which was funded by the University of Colorado at Boulder. UV rays could also damage the bacteria at the roots of some crops, which the plants depend on for some food.   Previous studies have shown residents of aquatic ecosystems, especially amphibians, are particularly susceptible to UV rays because they can do little to avoid it. Many plankton in the ocean could also be wiped out, endangering the many marine organisms that depend on them for food.

#### Nuclear war causes extinction

Woodwell 1986

George M Woodwell, PhD From Duke, Director of the Ecosystems center at the Marine Biological Laboratory at Woods Hole Mass. , Nuclear Winter, Deterrence, and the Prevention of Nuclear War, Edited by Sederberg, 1986 p. 20

The primary concern, I suppose, is the direct effects on people. Many of the same uncertainties that apply to the induction of climatic changes apply as well to inferences about human mortality. The size and characters of the war are important: Are cities the targets? The analyses from previous studies range widely up to the recent WHO analysis that suggests a total mortality of 1.1 billion for a 10,000 MT war. No estimates in this study dealt with the effects of a climatic crisis. Systematic efforts at estimating the additional mortality due to dark and prolonged cold in the weeks following such a war are beyond the limits of this discussion and, when developed, any estimates will prove as tenuous as virtually all other assumptions concerning the effects of a hypothetical war. Survivors of the immediate effects of the weapons will emerge into a radioactive environment that is likely to be perpetually dark and frozen with 10-20C or more of frost. On first analysis it would seem difficult to exaggerate the difficulties of accumulating the resources required for survival under those conditions. All supplies of fresh water would be frozen. Plants and animals, left unprotected, would be frozen and dead. Agriculture would be paralyzed transportation, normal communications of all types, sources of fuel, power supplies, and the normal machinery of govemment, including normal conventions established in law or in manners will have been destroyed or suspended: under those circumstances mere survival will be a major challenge and it is well within the realm of probability that few or none would survive in areas as large as continents, possibly in the northern hemisphere itself.

**Deterrence doesn’t apply to cyberspace**

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

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

####  War does pay – industrial capacity, raw materials, security

Mearsheimer 99

Mearsheimer, Distinguished Professor of Political Science, 1999. ¶ (John Mearsheimer, “Is Major War Obsolete?” 1999, http://www.ciaonet.org/conf/cfr10/index.html)

Let me make three quick points on that. One is, there’s a book by Peter Liberman, who actually teaches at Queens College, called Does Conquest Pay? which addresses this issue. And it shows very nicely that even though we live in the post-industrial age, conquest does pay, and that you can extract resources when you conquer countries in the modern age. Second point is, even if you don’t buy that argument, you can still make the raw-materials argument, which is the one that I went to because it’s the easier argument to make, involving things like the South China Sea and oil in the Persian Gulf. And my third and final point would be, even if you take the economic arguments off the table-let’s say that they just don’t hold any water-the security arguments remain alive and well. We knocked the Soviet Union down the toilet bowl during the Cold War. It produced no economic benefits for us, but what it did was it eliminated our principal competitor, which, from a realist’s perspective, is a wonderful thing. And I think most people in the audience think it was a wonderful thing. It had no economic benefits, but it had significant strategic benefits, because we wanted no peer competitors in the world because that’s the way we like it.

#### The obsolescence of major war is impossible—states inevitably slip into conflicts

Doran 99

Doran, Professor of International Relations at Johns Hopkins University's School of Advanced International Studies, Summer 1999 (Charles F., Survival, “Is Major War Obsolete? An Exchange: The Structural Turbulence of International Affairs,” June, vol.41 no.2, p.139-142)

Finally, of course, it is important to be clear about the meaning of the word at the heart of this argument. 'Obsolescence', in this context, can have two meanings. One is that something falls out of fashion. The other is that it is no longer in use. The former definition applies, perhaps, to war in general. But it does not apply to major war, because major war was never in fashion. I do not believe that any government since the beginning of the nineteenth century, has purposely sought a major war. Rather, they have slipped into major wars. They may well have been interested in fighting wars, especially if such wars were thought to be quick and not very destructive, or only destructive for the other side. But they did not expect these wars to develop into the kind that took place in the Napoleonic period, or the First and Second World Wars. That leaves the second definition, 'disuse'. Therefore the burden of the argument has to be that major wars are no longer going to happen. And that is a faith that is very difficult to maintain.

#### War is always possible – statements of lasting peace have never been correct – Mandelbaum’s exception of Russia and China undermine their entire argument

Kagan 1999

Donald Kagan is Hilihouse Professor of History and Classics at Yale University “Is Major War Obsolete? An Exchange” Survival, vol. 41, no. 2, Summer 1999, pp. 139—52

I agree that the present moment in history provides a better chance than ever for achieving a long period of peace, that the deterrent offered by nuclear weapons works towards that end, and that the growth of trade, democracy and economic interdependence assists that prospect. I do not, however, believe that war is obsolete — not yet, anyway. Nor do I believe that the present situation is unique in history any more than any moment is. As always, the chances for peace in the future depend on the decisions and the actions taken by people and these, as always, provide no guarantee against war — even ‘major’ war as Michael Mandelbaum has defined it. This is not the first time in history that people have thought that they had arrived at such a moment, such an extraordinary turning point. In 29BC, when Augustus closed the doors of the Temple of Janus in Rome for only the third time in the 500 years of Rome’s history, as a demonstration, a propaganda move, but also as a statement of a real expectation that new conditions had arrived that made peace appear to be a lasting peace. He turned out to be wrong. A more interesting year, perhaps, is 1792: a wonderful year for people to be stunningly optimistic about the prospects for the future. William Pitt the Younger, then Prime Minister of England, predicted that there were going to be at least 15 years of peace; never had the horizon looked clearer. And in the same year, two intellectuals of different sorts, Joseph Priestley and Tom Paine, had expectations of the same kind. In fact, they were less limited and more like the optimistic views that Michael Mandelbaum puts forward in his article. They based their future on a major change of conditions in the world. Priestley said:’ The present commercial treaties between England and France and between other nations, formerly hostile to each other, seem to show that mankind begin to be sensible to the folly of war and promise a new and important era in the state of the world in general, at least in Europe. Paine said: ‘If commerce were permitted to act to the universal extent it is capable, it would extirpate the system of war’. And of course, to this view were added the views of Kant and Montesquieu, who thought that the establishment of the political institution of the republic was going to have the same pacifying effect. Monarchies were really what war was about. Now that they were gone, there would be no more war. As Paine put it:2 The instant the form of government was changed in France, the republican principles of peace and domestic prosperity and economy arose with the new government, and the same consequences would follow in the case of other nations. Of course, within a year, France and England were at war, and 20 years or so of terrible, dreadful conflict followed. In 1848, John Stuart Mill also sang the praises of commerce:3 Commerce, which is rapidly rendering war obsolete, by strengthening and multiplying the personal interests which act in natural opposition to it . The great extent and rapid increase of international trade ... [is] the principal guarantee of the peace of the world. And then, of course, at the end of the nineteenth century and early in the twentieth century, two people of note wrote important statements of this thesis. One had a great impact; the other was not much noticed but was perhaps the more perceptive. The former was Norman Angell’s famous work, The Great Illusion. Basically, his message was that war had become so devastating from an economic point of view that nobody would ever fight. The only problem in Angell’s view was to teach people enough to know war was a disaster. Ivan Bloch was the other one, who said that war was so horrible in his day because the incredible means that had become available for fighting meant that no society could survive very long if they ever started such a war. The horror and danger of future war, he felt, would deter these conflicts. Well, of course, within a few years came the First World War. Now having said all this, even if all these men were wrong, this does not mean that Michael Mandelbaum cannot be right. But it should inspire some degree of modesty and caution. In fact Mandelbaum is very cautious in the language that he uses. Major war is not necessarily finished, he concedes. It’s not dead, it’s obsolete. This is a charming term that seems to say more than it does, because that allows Mandelbaum to draw back from the more total claims later on. A major war is unlikely but not unthinkable, which is to say he thinks it can happen. It is obsolete, he writes, in the sense that it is no longer fashionable. To pick up the metaphor is to see some of its limitations as well as its charm. Is war really a matter of fashion? And even if it is, don’t we have to face the fact that there are some people who choose to be unfashionable, and then there are other people who have never heard of fashion in the first place? China and Russia are two cases to which the writer points. He identifies the Taiwan Straits and the Russo-Ukrainian border as places where wars may well break out, should they erupt anywhere. They are the ‘potential Sarajevos of the twenty-first century’. He is right. And, of course, it is this concession, however genuinely and generously and modestly expressed, that gives away the game. Since there are at least two places where major wars between great powers might well break out even today — and two are quite enough — it seems to me that his entire thesis is undermined.

#### Organizations lack full deterrence capabilities—Lack of civilian control means states are more likely to strike preemptively or abandon nuclear discipline

Clark 97

Clark, associate professor of political science and director of the national security studies program at California State University, 97 (Mark T., “Deterrence in the Second Nuclear Age-book reviews: Neorealism versus Organizational Theory,” http://www.findarticles.com/p/articles/mi\_m0365/is\_n1\_v41/ai\_19238111)

Sagan's critique is a healthy antidote to Waltz's optimism. In his view, there are two principal arguments that suggest pessimism about any future with a greater number of nuclear-armed adversaries. From his study of militaries, Sagan finds that their organizational behavior inclines them towards deterrence failure. It is not that militaries want war but that, of all groups in a society, they are the most likely to believe war is probable and are most inclined to adopt preventive or preemptive strategies. Military officers are more skeptical of nonmilitary solutions to conflicts than are their civilian counterparts, according to Sagan. It also makes sense, in classical military terms, to adopt preventive or preemptive strategies, since no military prefers to fight on its adversary's terms. Taking the offensive alleviates some of these problems. Secondly, Sagan argues that newly armed nuclear states will lack the positive mechanisms of civilian control. Here, Sagan's critique is very strong. By examining the history of the U.S. nuclear safety record he is able to document many near accidents and bureaucratic snafus that could have led to catastrophic accidents, and in this way he points out the weakness in Waltz's arguments. Sagan comments: Waltz asked why should we expect new nuclear states to experience greater difficulties than did the old ones? The evidence of the number of near-accidents with U.S. nuclear weapons during the Cold War suggests that there would be reason enough to worry about nuclear accidents in new nuclear states even if their safety difficulties were "only" as great as those experienced by old nuclear powers (p. 80). He adds six reasons why new nuclear powers are unlikely to compile the safety record of the United States. But if the problem is acute for newly emergent nuclear powers that develop their programs indigenously, it will be doubly so for those that inherit or buy their programs. They will lack even the discipline that a new nuclear nation will accrue by investing enormous amounts of time, talent, and treasure into developing its nuclear program.

Predictions are accurate enough and should be used as a basis for political action

Chernoff 2009. Fred, Prof. IR and Dir. IR – Colgate U., European Journal of International Relations, “Conventionalism as an Adequate Basis for Policy-Relevant IR Theory”, 15:1

For these and other reasons, many social theorists and social scientists have come to the conclusion that prediction is impossible. Well-known IR reflexivists like Rick Ashley, Robert Cox, Rob Walker and Alex Wendt have attacked naturalism by emphasizing the interpretive nature of social theory. Ashley is explicit in his critique of prediction, as is Cox, who says quite simply, ‘It is impossible to predict the future’ (Ashley, 1986: 283; Cox, 1987: 139, cf. also 1987: 393). More recently, Heikki Patomäki has argued that **‘qualitative changes and emergence are possible, but predictions are not’ defective** and that the latter two presuppose an unjustifiably narrow notion of ‘prediction’.14 **A determined prediction sceptic may continue to hold that there is too great a degree of complexity of social relationships** (which comprise ‘open systems’) **to allow any prediction whatsoever.** Two very **simple examples may circumscribe and help to refute a radical variety of scepticism**. First, **we all make reliable social predictions and do so with great frequency**. We can predict with high probability that a spouse, child or parent will react to certain well-known stimuli that we might supply, based on extensive past experience. More to the point of IR prediction – scepticism, we can imagine a young child in the UK who (perhaps at the cinema) (1) picks up a bit of 19th-century British imperial lore thus gaining a sense of the power of the crown, without knowing anything of current balances of power, (2) hears some stories about the US–UK invasion of Iraq in the context of the aim of advancing democracy, and (3) hears a bit about communist China and democratic Taiwan. Although the specific term ‘preventative strike’ might not enter into her lexicon, it is possible to imagine the child, whose knowledge is thus limited, thinking that if democratic Taiwan were threatened by China, the UK would (possibly or probably) launch a strike on China to protect it, much as the UK had done to help democracy in Iraq. In contrast to the child, readers of this journal and scholars who study the world more thoroughly have factual information (e.g. about the relative military and economic capabilities of the UK and China) and hold some cause-and-effect principles (such as that states do not usually initiate actions that leaders understand will have an extremely high probability of undercutting their power with almost no chances of success). Anyone who has adequate knowledge of world politics would predict that the UK will not launch a preventive attack against China. In the real world, China knows that for the next decade and well beyond the UK will not intervene militarily in its affairs. While Chinese leaders have to plan for many likely — and even a few somewhat unlikely — future possibilities, they do not have to plan for various implausible contingencies: they do not have to structure forces geared to defend against specifically UK forces and do not have to conduct diplomacy with the UK in a way that would be required if such an attack were a real possibility. Any rational decision-maker in China may use some cause-and-effect (probabilistic) principles along with knowledge of specific facts relating to the Sino-British relationship to predict (P2) that the UK will not land its forces on Chinese territory — even in the event of a war over Taiwan (that is, the probability is very close to zero). The statement P2 qualifies as a prediction based on DEF above and counts as knowledge for Chinese political and military decision-makers. A Chinese diplomat or military planner who would deny that theory-based prediction would have no basis to rule out extremely implausible predictions like P2 and would thus have to prepare for such unlikely contingencies as UK action against China. A reflexivist theorist sceptical of ‘prediction’ in IR might argue that the China example distorts the notion by using a trivial prediction and treating it as a meaningful one. But the critic’s temptation to dismiss its value stems precisely from the fact that it is so obviously true. The value to China of knowing that the UK is not a military threat is significant. The fact that, under current conditions, any plausible cause-and-effect understanding of IR that one might adopt would yield P2, that the ‘UK will not attack China’, does not diminish the value to China of knowing the UK does not pose a military threat. A critic might also argue that DEF and the China example allow non-scientific claims to count as predictions. But we note that while physics and chemistry offer precise ‘point predictions’, other natural sciences, such as seismology, genetics or meteorology, produce predictions that are often much less specific; that is, they describe the predicted ‘events’ in broader time frame and typically in probabilistic terms. We often find predictions about the probability, for example, of a seismic event in the form ‘some time in the next three years’ rather than ‘two years from next Monday at 11:17 am’. DEF includes approximate and probabilistic propositions as predictions and is thus able to catagorize as a prediction the former sort of statement, which is of a type that is often of great value to policy-makers. **With the help of these ‘non-point predictions’ coming from the natural and the social sciences, leaders are able to choose the courses of action** (e.g. more stringent earthquake-safety building codes, or procuring an additional carrier battle group) **that are most likely to accomplish the leaders’ desired ends. So while ‘point predictions’ are not what political leaders require in most decision-making situations, critics of IR predictiveness often attack the predictive capacity of IR theory for its inability to deliver them. The critics thus commit the straw man fallacy by requiring a sort of prediction in IR (1) that few, if any, theorists claim to be able to offer, (2) that are not required by policy-makers for theory-based predictions to be valuable, and (3) that are not possible even in some natural sciences.**15 The range of theorists included in ‘reflexivists’ here is very wide and it is possible to dissent from some of the general descriptions. From the point of view of the central argument of this article, there are two important features that should be rendered accurately. One is that reflexivists reject explanation–prediction symmetry, which allows them to pursue causal (or constitutive) explanation without any commitment to prediction. The second is that almost all share clear opposition to predictive social science.16 The reflexivist commitment to both of these conclusions should be evident from the foregoing discussion.

## Baudrillard

#### C. Policy simulation key to creativity and decisionmaking—the detachment that they criticize is key to its revolutionary benefits

Eijkman 12

The role of simulations in the authentic learning for national security policy development: Implications for Practice / Dr. Henk Simon Eijkman. [electronic resource] <http://nsc.anu.edu.au/test/documents/Sims_in_authentic_learning_report.pdf>. Dr Henk Eijkman is currently an independent consultant as well as visiting fellow at the University of New South Wales at the Australian Defence Force Academy and is Visiting Professor of Academic Development, Annasaheb Dange College of Engineering and Technology in India. As a sociologist he developed an active interest in tertiary learning and teaching with a focus on socially inclusive innovation and culture change. He has taught at various institutions in the social sciences and his work as an adult learning specialist has taken him to South Africa, Malaysia, Palestine, and India. He publishes widely in international journals, serves on Conference Committees and editorial boards of edited books and international journal

Policy simulations stimulate Creativity Participation in policy games has proved to be a highly effective way of developing new combinations of experience and creativity, which is precisely what innovation requires (Geurts et al. 2007: 548). Gaming, whether in analog or digital mode, has the power to stimulate creativity, and is one of the most engaging and liberating ways for making group work productive, challenging and enjoyable. Geurts et al. (2007) cite one instance where, in a National Health Care policy change environment, ‘the many parties involved accepted the invitation to participate in what was a revolutionary and politically very sensitive experiment precisely because it was a game’ (Geurts et al. 2007: 547). Data from other policy simulations also indicate the uncovering of issues of which participants were not aware, the emergence of new ideas not anticipated, and a perception that policy simulations are also an enjoyable way to formulate strategy (Geurts et al. 2007). Gaming puts the players in an ‘experiential learning’ situation, where they discover a concrete, realistic and complex initial situation, and the gaming process of going through multiple learning cycles helps them work through the situation as it unfolds. Policy gaming stimulates ‘learning how to learn’, as in a game, and learning by doing alternates with reflection and discussion. The progression through learning cycles can also be much faster than in real-life (Geurts et al. 2007: 548). The bottom line is that problem solving in policy development processes requires creative experimentation. This cannot be primarily taught via ‘camp-fire’ story telling learning mode but demands hands-on ‘veld learning’ that allow for safe creative and productive experimentation. This is exactly what good policy simulations provide (De Geus, 1997; Ringland, 2006). In simulations participants cannot view issues solely from either their own perspective or that of one dominant stakeholder (Geurts et al. 2007). Policy simulations enable the seeking of Consensus Games are popular because historically people seek and enjoy the tension of competition, positive rivalry and the procedural justice of impartiality in safe and regulated environments. As in games, simulations temporarily remove the participants from their daily routines, political pressures, and the restrictions of real-life protocols. In consensus building, participants engage in extensive debate and need to act on a shared set of meanings and beliefs to guide the policy process in the desired direction

#### 2. Even if there is no objective truth, rationality can provide justified belief, and we should still act as if there were.

Sherry 96 – Suzanna, “The Sleep of Reason”, Georgetown Law Journal, Feb, lexis

In order to make even such a limited defense, however, I must first confront [\*473] the broad epistemological challenge: that truth -- or intellectual authority -- does not exist apart from the social and political hierarchies that create and sustain it. If the most radical social constructivists are right, and there is no such thing as truth or objectivity, defending the Enlightenment is like trying to collect water in a sieve. Fortunately, it is not necessary to resolve this philosophical dispute in order to proceed. First, the question I am addressing is not whether the Enlightenment reliance on reason and empiricism is in fact the only epistemology, but whether we ought to proceed as if it were, at least in the public arena. Even **if there are multiple** and contradictory **truths, some may be better suited for public adoption than others.** There is a difference between objective truth and justified beliefs, and **suggesting** that only **beliefs informed by reason are justified does not take any stand on the existence** or accessibility **of** **objective truth**. n110 Further, **neither reason nor truth need be transcendent or objective to inform debate**. As many scholars have recognized, postmodernism has not prevented us from acting as if truth exists. n111 Indeed, we can probably do no less: to act on the postmodern insights would be "like saying that, since philosophers are still debating Descartes' epistemology, one need not take notice of traffic signals in the meantime (since they might not really exist)." n112 Moreover, although it may be less relevant in "soft" disciplines like law, some truth does exist: "**If there were no facts,** surgeons couldn't operate, buildings would collapse, and **airplanes wouldn't get off the ground**." n113 Finally, as William Marshall has pointed out, the search for truth remains an important human enterprise even if objective truth does not exist, because "the human imagination is compelled not only by truth but also by the idea of truth." n114 Similarly, **even if there is no epistemology unconnected to power relationships**, we tend to -- and perhaps **we must -- behave as if there were**. It remains only to give that epistemology content.

#### 5. Images of nuclear apocalypse are necessary to problematize their usage

James Foard. 1997. Associate Professor of Religion, Arizona State, “Imagining Nuclear Weapons: Hiroshima, Armageddon, and the Annihilation of the Students of Ichijo School,” Journal of the American Academy of Religion, http://jaar.oxfordjournals.org/cgi/reprint/LXV/1/1.pdf TBC 7/1/10)

**This ambivalence about Hiroshima has been partially ameliorated by displacing it with Armageddon in our imagination of nuclear weapons** In America **the images of the atomic bomb**, particularly after the Soviet Union's successful test in 1949 (Boyer.341), **were pressed into the service of apocalyptic speculations**, both scientific and otherwise, a process which has until recently assigned the horror that Hiroshima represented to a superpower war in an imagined future (cf. Pease'562). Specifically, **images of a nuclear Armageddon have helped us perform two sorts of cultural tasks fundamental for imagining nuclear weapons**: those involving difference and those involving representation. By "difference" I mean both **the articulation of what makes nuclear weapons different from other weapons and the consequent reflection on the different human situation engendered by them**. By "representation" I mean **the expressions which seek to describe the use of nuclear weapons and incorporate that description into structures of meaning Armageddon permits us to define the difference of nuclear weapons by their capacity to destroy the human species** in a war that no one will win. It also has suggested to many, particularly literary critics but also some nuclear strategists, that nuclear war is but an imaginary event, divorced from reality, such that all representations are, to use the most famous phrase, "fabulously textual" (Derrida'23).

#### 7. IR theory proves cyberwar is probable- multiple mechanisms

Junio ‘13

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

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

#### 9. Even if our lives are valueless, there is value in protecting future generations

Nick **Bostrom**, Professor in the Faculty of Philosophy & Oxford Martin School, Director of the Future of Humanity Institute, and Director of the Programme on the Impacts of Future Technology at the University of Oxford, recipient of the 2009 Eugene R. Gannon Award for the Continued Pursuit of Human Advancement, holds a Ph.D. in Philosophy from the London School of Economics, 2011 (“The Concept of Existential Risk,” Draft of a Paper published on ExistentialRisk.com, Available Online at <http://www.existentialrisk.com/concept.html>, Accessed 07-04-2011)

We have thus far considered existential risk from the perspective of utilitarianism (combined with several simplifying assumptions). We may briefly consider how the issue might appear when viewed through the lenses of some other ethical outlooks. For example, the philosopher Robert Adams outlines a different view on these matters. I believe **a better basis for ethical theory** in this area **can be found in** quite a different direction—in **a commitment to the future of humanity as a vast project, or network of overlapping projects, that is generally shared by the human race. The aspiration for a better society**—more just, more rewarding, and more peaceful—**is a part of this project. So are the potentially endless quests for scientific knowledge and philosophical understanding, and the development of artistic and other cultural traditions. This includes** the particular cultural traditions to which we belong, in all their accidental historic and ethnic diversity. It also includes **our interest in the lives of our children and grandchildren, and the hope that they will be able**, in turn, **to have the lives of their children and grandchildren as projects. To the extent that a policy or practice seems likely to be favorable or unfavorable to the carrying out of this complex of projects in the nearer or further future, we have reason to pursue or avoid it**. … **Continuity is as important to our commitment to the project of the future of humanity as it is to our commitment to the projects of our own personal futures. Just as the shape of my whole life, and its connection with my present and past, have an interest that goes beyond that of any isolated experience, so too the shape of human history over an extended period of the future, and its connection with the human present and past, have an interest that goes beyond that of the** (total or average) **quality of life of a population-at-a-time, considered in isolation from how it got that way**. **We owe**, I think, some **loyalty to this project of the human future. We** also **owe it a respect that we would owe it even if we were not of the human race ourselves**, but beings from another planet who had some understanding of it. (28: 472-473) **Since an existential catastrophe would either put an end to the project of the future of humanity or drastically curtail its scope for development, we** would seem to **have a strong prima facie reason to avoid it**, in Adams’ view. We also note that **an existential catastrophe would entail the frustration of many strong preferences**, suggesting that from a preference-satisfactionist perspective it would be a bad thing. In a similar vein, **an ethical view emphasizing that public policy should be determined through informed democratic deliberation by all stakeholders would favor existential-risk mitigation if we suppose**, as is plausible, **that a majority of the world’s population would come to favor such policies upon reasonable deliberation** (even if hypothetical future people are not included as stakeholders). **We might also have custodial duties to preserve the inheritance of humanity passed on to us by our ancestors and convey it safely to our descendants**.[24] **We do not want to be the failing link in the chain of generations, and we ought not to delete or abandon the great epic of human civilization that humankind has been working on for thousands of years, when it is clear that the narrative is far from having reached a natural terminus**. Further, **many theological perspectives deplore naturalistic existential catastrophes, especially ones induced by human activities**: If God created the world and the human species, one would imagine that He might be displeased if we took it upon ourselves to smash His masterpiece (or if, through our negligence or hubris, we allowed it to come to irreparable harm).[25]

#### 10. Abandoning rational epistemology ensures massive violence, destruction of debate, and death of political participation.

Sherry 96 – Suzanna, “The Sleep of Reason”, Georgetown Law Journal, Feb, lexis

Some, however, have suggested that the historical era of the Enlightenment was unique, and that epistemological pluralism would, in the modern world, create little danger of internecine warfare. 139 This optimism overlooks one of the fundamental differences between rational and **antirational epistemologies**: [\*479] because the latter **rest on faith** **rather than reason, they are likely to be impervious to persuasion and** resistant to **compromise**. 140 Moreover, without the skeptical cast of mind fostered by Enlightenment epistemology, antirational epistemologies -- especially religion, with its extrahuman source of authority -- are likely to be conducive to particularly deep conviction. **Deep conviction**, in turn, **is a breeding ground for** exactly **the religious wars of previous centuries**: In Abrams v. United States, Justice Holmes argued that a logical result of deep conviction is intolerance. As Dean Bollinger has added, failing to attempt to silence what one believes to be false might be seen as a sign of weak conviction. . . . To the zealous adherent, **intolerance and persecution become**, in a sense, **the measure of her commitment to** her religious **beliefs**. 141Even in the United States, where religion has largely been domesticated (as Michael Perry puts it), 142 we have not been spared all of the violence associated with pre-Enlightenment religious wars. Although, as Perry points out, "we are not the former Yugoslavia or India," 143 the Branch Davidians, the World Trade Center **bombers**, the abortion clinic killings, **and the growth of** various **organizations -- on the left and the right, not all** of them **religious -- that use irrational arguments to** reject and **resist the authority of government**, by violence if necessary, **should** **give us pause before abandoning the fruits of the Enlightenment**. 144 Indeed, as one historian has pointed out: If we have now entered an era in which those on the right have been joined by some on the left in assailing reason as faulty because it does not correspond to the essential and incontestable truths they have come to know emotionally, or by virtue of their membership in particular groups, the prospects for deliberative democracy are bleak indeed. . . . **If truth resides in difference** and emotion, **then war rather than persuasion is the only possible consequence** **of speaking such a truth to power**. 145

# 1AR

## Risk K

#### Indifference leads to no value to life.

David Johnson. “The Difference Between Winning and Losing: Baudrillardian Reversibility and Chance Versus the World as Stake.” International Journal of Baudrillard Studies 7.1 (January 2010).

If there is no real difference in life between winning and losing, better to just watch others play, but then again, if there is no difference between winning and losing, what is the point of watching?

 Without a difference between winning and losing, even the apathy of the tele-addict is at risk, since without a separation between winning and losing there cannot even be a proper reversal between them, and therefore any drama.

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

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

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