# 1AC

## Adv 1 - Arms Race

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

Goldman 13

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

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

#### Specifically, cyber attacks risk retaliatory cycles and arms races

Moss 13

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

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

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

CSM 11

Christian Science Monitor

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

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

#### Congressional constraints of OCOs are key to solve — otherwise nuclear war is inevitable from arms-racing, command and control hacking, crisis instability, and fracturing nuclear agreements

Austin, 8/6

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

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

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

Clarke 2009

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

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

#### Cyberwar escalates:

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

Clarke and Knake ‘12

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

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

#### b) Pressure to retaliate

Owens et al 9

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

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

#### C) Signaling failures

Mulvenon et al. 10

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

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

## Adv 2 - Trade off

#### Cyber-attack is likely in the squo - actors are mapping out vulnerable infrastructure

Francis ‘13

[David Francis is a reporter based in Berlin and Washington, DC. In addition to repoting for the Fiscal Times, David is a correspondent of the Christian Science Monitor, Financial Times Deutschland, and Deutsche Welle. He is a contributing writer to World Politics Review, SportsIllustrated.com, and the Pittsburgh Post-Gazette, among others. He has reported from all over the world on a number of topics, from transatlantic relations, to sports, to border security, to local news, to finance.In 2010, David was named to the prestigious Atlantik-Brueke association, created to promote transatlantic relations. In 2009, he was awarded the Arthur Burns Fellowship from the International Center for Journalists. He has been a John McCloy Fellow, awarded by the American Council of Germany, and an Arizona State Media Fellow. David has spoken about his reporting at the Georgetown University School of Foreign Service, the Johns Hopkins School for Advanced International Studies, and the World Affairs Council of Pittsburgh. He an undergraduate degree from the University of Chicago, and a master’s degree from Georgetown University. <http://www.thefiscaltimes.com/Articles/2013/03/11/The-Coming-Cyber-Attack-that-Could-Ruin-Your-Life#sthash.UO07zhTu.dpuf> ETB]

But experts warn these kinds of service breaks are just a small symptom of the serious damage cyber terrorists and hackers can cause. Officials have said that hackers could cause a cyber 9/11 – an attack could cause widespread turmoil, including the disappearance of money, electrical failure, and even death. And America could be the battlefield in which these new techniques of war are tested. ¶ “An adversary looking to cause chaos could pick any part of critical infrastructure, from banking to power to health care,” said Jeffrey Carr, chief executive officer of Taia Global, a cyber security firm. “All of those are vulnerable to cyber attack.”¶ The most harmful cyber attacks have the ability to impact nearly every part of American life, putting lives and essential privacy at risk. Without increased vigilance, experts say it’s only a matter of time before a worst-case scenario becomes a reality.¶ ATTACKS ON U.S. INFRASTRUCTURE ¶ Hackers have attempted to infiltrate critical infrastructure components like mass transit and power grids, although few Americans are aware of it. Former Defense Secretary Leon Panetta says they have had limited success. But all it takes it one breach to cause chaos.¶ “We know of specific instances where intruders have successfully gained access to these [critical infrastructure] systems," Panetta said last October in New York. "We also know that they are seeking to create advanced tools to attack these systems and cause panic and destruction and even the loss of life. ”¶ Attacks like the one Panetta described could turn off the power to large parts of the country. Public transportation systems could malfunction and operators to lose control of systems that prevent crashes. Attackers could also take down communication systems and Internet access.¶ According to Tom Kellermann, vice president of cyber security for Trend Micro, attacks on infrastructure could also provide false information to people making life and death decisions. For instance, hackers could target air traffic control systems, providing false information that could cause planes to crash.¶ “Everyone implicitly trusts his or her computer,” he said. “A cyber attack can corrupt this information.”¶ ATTACKS ON BANKING AND HEALTHCARE SYSTEMS ¶ So far, cyber attacks have had limited access to bank accounts for short periods of time, and some personal information has been stolen. But according to Larry Ponemon, founder of the Ponemon Institute, a think tank that studies data privacy, hackers want to do more than disrupt: they want to make money disappear. ¶ “In a successful attack against a bank, credentials and passwords are gone,” he said. “Hackers are trying to go into accounts to steal large sums of money.” Maybe, but imagine, for example, that cyber thieves were able to steal just 1 percent or less from JP Morgan’s $2 trillion in assets. ¶ Health care systems are also vulnerable to these kinds of attacks. Many doctors and hospitals are now keeping electronic medical records. Hackers can get access to this information, making changes that could potentially lead to deadly instances where doctors prescribe unnecessary drugs or order irrelevant procedures for the patient.¶ “I have never seen an industry with more gaping security holes,” Avi Rubin, a computer scientist and technical director of the Information Security Institute at Johns Hopkins University, told the Washington Post last year. “If our financial industry regarded security the way the health-care sector does, I would stuff my cash in a mattress under my bed."

**Current preemptive OCO policy backfires- creates priority confusion and drains cyber-defense resources**

**Healey ‘13**

[Jason Healey is director of the Cyber Statecraft Initiative at the Atlantic Council. <http://www.usnews.com/opinion/blogs/world-report/2013/03/08/clandestine-american-strategy-on-cyberwarfare-will-backfire> ETB]

**America's** generals and **spymasters have decided they can secure a better future in cyberspace through,** what else, covert warfare, **preemptive attacks**, and clandestine intelligence. Our rivals are indeed seeking to harm U.S. interests and it is perfectly within the president's purview to use these tools in response. Yet **this** is an unwise **policy** that **will ultimately backfire**. **The** undoubted, immediate national **security advantages will be at the expense of America's longer-term goals in cyberspace.** ¶ The latest headlines on covert and **preemptive cyberplans highlight just the latest phase of a cyber "cult of offense" dating back to the 1990s.** Unclassified details are scarce, but the Atlantic Council's study of cyber history reveals covert plans, apparently never acted upon, to drain the bank accounts of Slobodan Milosevic and Saddam Hussein. More recent press accounts detail cyber assaults on terrorist networks (including one that backfired onto U.S. servers) and Stuxnet, which destroyed Iranian centrifuges. American spy chiefs say U.S. cyber capabilities are so prolific that this is the "golden age" of espionage, apparently including the Flame and Duqu malware against Iran and Gauss, which sought financial information (perhaps also about Iran) in Lebanese computers.¶ **Offensive cyber capabilities do belong in the U.S. military arsenal. But the continuing obsession with** covert, **preemptive**, and clandestine **offensive cyber capabilities not only reduces resources dedicated for defense but overtakes other priorities as well.**

#### Focus on preemptive cyber-attack capability trades off with fixing critical cyber vulnerabilities

**Rid 2/4**

[Thomas Rid is a reader at the Department of War Studies, King's College London. 2013, [http://www.newrepublic.com/article/112314/obama-administrations-lousy-record-cyber-security#](http://www.newrepublic.com/article/112314/obama-administrations-lousy-record-cyber-security) ETB]

But the rhetoric of war doesn't accurately describe much of what happened. There was no attack that damaged anything beyond data, and even that was the exception; the Obama administration's rhetoric notwithstanding, there was nothing that bore any resemblance to World War II in the Pacific. Indeed, the **Obama** administration **has been** so intent on **responding to the cyber threat with martial aggression** that it hasn't paused to consider the true nature of the threat. And **that has lead to two crucial mistakes: first, failing to realize** (or choosing to ignore) **that offensive capabilities in cyber security don’t translate easily into defensive capabilities. And second, failing to realize** (or choosing to ignore) **that it is far more urgent for the United States to concentrate on developing the latter**, rather than the former.¶ At present, the United States government is one of the most aggressive actors when it comes to offensive cyber operations, excluding commercial espionage. The administration has anonymously admitted that it designed Stuxnet (codenamed Olympic Games) a large-scale and protracted sabotage campaign against Iran’s nuclear enrichment facility in Natanz that was unprecedented in scale and sophistication. Close expert observers assume that America also designed Flame, a major and mysterious espionage operation against several Middle Eastern targets mostly in the energy sector. The same goes for Gauss, a targeted and sophisticated spying operation designed to steal information from Lebanese financial institutions.¶ Developing sophisticated, code-borne sabotage tools requires skills and expertise; they also require detailed intelligence about the input and output parameters of the targeted control system. The **Obama** administration seems to have **decided** **to prioritize** such **high-end offensive operations.** Indeed, the Pentagon's bolstered Cyber Command seems designed primarily for such purposes. **But these kinds of narrowly-targeted offensive investments have no defensive value.** ¶ **So** amid all the activity, **little has been done to address the country's major vulnerabilities**. The software that controls **America's most critical infrastructure**—from pipeline valves to elevators to sluices, trains, and the electricity grid—**is** often **highly insecure** by design, as the work of groups like Digital Bond illustrates. **Worse**, **these systems are** often **connected** **to the internet** **for maintenance** reasons, **which means they are always vulnerable to attack**. Shodan, a search engine dubbed the Google for hackers, has already made these networked devices searchable. Recently a group of computer scientists at the Freie Universität in Berlin began to develop their own crawlers to geo-locate these vulnerable devices and display them on a map. Although the data are still incomplete and anonymized, **parts of America's most vulnerable infrastructure are now visible for anyone to see.**¶ **Defending these areas ought to be the government's top priority, not** the creation of a larger Cyber Command capable of **going on the offense.** Yet the White House has hardly complained that the piece of legislation that would have made some progress towards that goal, the Cybersecurity Act of 2012, has stalled indefinitely in the Senate.

**Military focus on offense spills over the private sector**

**Gjelten, 13**

(Tom, correspondent for NPR, "First Strike: US Cyber Warriors Seize the Offensive", Jan/Feb, [www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive](http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive) NL)

**When the Pentagon launched its much-anticipated “Strategy for Operating in Cyberspace” in July 2011, it appeared the US military was interested only in protecting its own computer networks**, not in attacking anyone else’s. “The thrust of the strategy is defensive,” declared Deputy Secretary of Defense William Lynn. The Pentagon would not favor the use of cyberspace “for hostile purposes.” Cyber war was a distant thought. “Establishing robust cyber defenses,” Lynn said, “no more militarizes cyberspace than having a navy militarizes the ocean.”¶ **That was then. Much of the cyber talk around the Pentagon these days is about offensive operations.** **It is no longer enough for cyber troops to be deployed along network perimeters, desperately trying to block the constant attempts by adversaries to penetrate front lines. The US military’s geek warriors are now prepared to go on the attack, armed with potent cyberweapons that can break into enemy computers with pinpoint precision**.¶ The new emphasis is evident in a program launched in October 2012 by the Defense Advanced Research Projects Agency (DARPA), the Pentagon’s experimental research arm. **DARPA funding enabled the invention of the Internet, stealth aircraft, GPS, and voice-recognition software, and the new program, dubbed Plan X, is equally ambitious.** DARPA managers said **the Plan X goal was “to create revolutionary technologies for understanding, planning, and managing cyberwarfare.”** The US Air Force was also signaling its readiness to go into cyber attack mode, announcing in August that it was looking for ideas on how “to destroy, deny, degrade, disrupt, deceive, corrupt, or usurp the adversaries [sic] ability to use the cyberspace domain for his advantage. **The new interest in attacking enemies rather than simply defending against them has even spread to the business community**. Like their military counterparts, **cybersecurity experts in the private sector have become increasingly frustrated by their inability to stop intruders from penetrating critical computer networks to steal valuable data or even sabotage network operations. The new idea is to pursue the perpetrators back into their own networks**. “We’re following a failed security strategy in cyber,” says Steven Chabinsky, formerly the head of the FBI’s cyber intelligence section and now chief risk officer at CrowdStrike, a startup company that promotes aggressive action against its clients’ cyber adversaries. “There’s no way that we are going to win the cybersecurity effort on defense. We have to go on offense.”¶ **The growing interest in offensive operations is bringing changes in the cybersecurity industry.** Expertise in patching security flaws in one’s own computer network is out; expertise in finding those flaws in the other guy’s network is in. Among the “hot jobs” listed on the career page at the National Security Agency are openings for computer scientists who specialize in “vulnerability discovery.” **Demand is growing in both government and industry circles for technologists with the skills to develop ever more sophisticated cyber tools,** including malicious software—malware—with such destructive potential as to qualify as cyberweapons when implanted in an enemy’s network. “**Offense is the biggest growth sector in the cyber industry right now,”** says Jeffrey Carr, a cybersecurity analyst and author of Inside Cyber Warfare. But have we given sufficient thought to what we are doing? Offensive operations in the cyber domain raise a host of legal, ethical, and political issues, and governments, courts, and business groups have barely begun to consider them.

#### 2 impacts:

#### First, cyberwar:

**Overconcentration on offense is destabilizing- makes cyberwar inevitable**

**McGraw 13**

<[Gary McGraw](http://www.tandfonline.com/action/doSearch?action=runSearch&type=advanced&searchType=journal&result=true&prevSearch=%2Bauthorsfield%3A(McGraw%2C+G)), PhD is Chief Technology Ofﬁcer of Cigital, and author of¶ Software Security (AWL 2006) along with ten other software security¶ books. He also produces the monthly Silver Bullet Security Podcast for¶ IEEE Security & Privacy Magazine (syndicated by SearchSecurity), Cyber War is Inevitable (Unless We Build Security In), Journal of Strategic Studies - Volume 36, Issue 1, 2013, pages 109-119, <http://www.tandfonline.com.proxy.library.cornell.edu/doi/pdf/10.1080/01402390.2012.742013>>#**SPS**

**Also of note is the balancing effect that extreme cyber vulnerability**¶ **has on power when it comes to cyber war.** In the case of the Stuxnet¶ attack, the balance of power was clearly stacked high against Iran.¶ Subsequently, however, Iran responded with the (alleged) hijacking of a¶ US drone being used for surveillance in Iranian airspace.10 **Ironically, it**¶ **may be that the most highly developed countries are more vulnerable to**¶ **cyber warfare because they are more dependent on modern high-tech**¶ **systems.** **In any case, failure to build security into the modern systems**¶ **we depend on can backlash, lowering the already low barrier to entry**¶ **for geopolitically motivated cyber conﬂict.** **Defending against cyber**¶ **attack (by building security in) is just as important as developing**¶ **offensive measures. Indeed it is more so.**¶ War has both defensive and offensive aspects, and understanding this¶ is central to understanding cyber war. **Over-concentrating on offense**¶ **can be very dangerous and destabilizing because it encourages actors to**¶ **attack ﬁrst and ferociously, before an adversary can.** **Conversely, when**¶ **defenses are equal or even superior to offensive forces, actors have less**¶ **incentive to strike ﬁrst because the expected advantages of doing so are**¶ **far lower.** **The United States is supposedly very good at cyber offense**¶ **today, but from a cyber defense perspective it lives in the same glass**¶ **houses as everyone else.** The root of the problem is that the systems we¶ depend on – the lifeblood of the modern world – are not built to be¶ secure.11¶ This notion of offense and defense in cyber security is worth teasing¶ out. Offense involves exploiting systems, penetrating systems with¶ cyber attacks and generally leveraging broken software to compromise¶ entire systems and systems of systems.12 Conversely, defense means¶ building secure software, designing and engineering systems to be¶ secure in the ﬁrst place, and creating incentives and rewards for systems¶ that are built to be secure.13 What sometimes passes for cyber defense¶ today – actively watching for intrusions, blocking attacks with network¶ technologies such as ﬁrewalls, law enforcement activities, and protecting against malicious software with anti-virus technology – is little more than a cardboard shield.14 **If we do not focus more attention on**¶ **real cyber defense by building security in, cyber war will be inevitable.**¶

**That causes nuclear miscalc due to hair-trigger response**

**Clark and Andreasen 13**

(Richard A. Clarke, the chairman of Good Harbor Security Risk Management, was special adviser to the president for cybersecurity in the George W. Bush administration. Steve Andreasen, a consultant to the Nuclear Threat Initiative, was the National Security Council’s staff director for defense policy and arms control from 1993 to 2001, “Cyberwar’s threat does not justify a new policy of nuclear deterrence” June 14, 2013, <http://articles.washingtonpost.com/2013-06-14/opinions/39977598_1_nuclear-weapons-cyber-attack-cyberattacks>, KB)

President Obama is expected to unveil a new nuclear policy initiative this week in Berlin. Whether he can make good on his first-term commitments to end outdated Cold War nuclear policies may depend on a firm presidential directive to the Pentagon rejecting any new missions for nuclear weapons — in particular, their use in response to cyberattacks.¶ The Pentagon’s Defense Science Board concluded this year that **China and Russia could develop capabilities to launch an “existential cyber attack” against the United States** — that is, **an attack causing sufficient damage that our government would lose control of the country.** “**While the manifestation of a nuclear and cyber attack are** very **different**,” the board concluded, “in the end, **the existential impact to the United States is the same.”**¶ Because it will be impossible to fully defend our systems against existential cyberthreats, the board argued, the United States must be prepared to threaten the use of nuclear weapons to deter cyberattacks. In other words: I’ll see your cyberwar and raise you a nuclear response.¶ Some would argue that Obama made clear in his 2010 Nuclear Posture Reviewthat the United States has adopted the objective of making deterrence of nuclear attacks the “sole purpose” of our nuclear weapons. Well, the board effectively reviewed the fine print and concluded that the Nuclear Posture Review was “essentially silent” on the relationship between U.S. nuclear weapons and cyberthreats, so connecting the two “is not precluded in the stated policy.”¶ As the board noted, cyberattacks can occur very quickly and without warning, requiring rapid decision-making by those responsible for protecting our country. **Integrating the nuclear threat into the equation means making clear to any potential adversary that the United States is prepared to use nuc**lear weapon**s very early in response to a major cyberattack — and is maintaining nuclear forces on “prompt launch” status to do so.**¶ **Russia and China would** certainly take note — and presumably **follow suit**. Moreover, **if the United States, Russia and China adopted policies threatening an early nuclear response to cyber­attacks, more countries would surely take the same approach.**¶ It’s hard to see how this cyber-nuclear action-reaction dynamic would improve U.S. or global security. It’s more likely to lead to a new focus by Pentagon planners on generating an expanding list of cyber-related targets and the operational deployment of nuclear forces to strike those targets in minutes.¶ Against that backdrop, maintaining momentum toward reducing the role of nuclear weapons in the United States’ national security strategy (and that of other nations) — a general policy course pursued by the past five presidents — would become far more difficult. **Further reductions in nuclear forces and changes in “hair-trigger” postures, designed to lessen the risk of an accidental or unauthorized nuclear launch, would** also probably **stall**.¶ Fortunately, Obama has both the authority and the opportunity to make clear that he meant what he said when he laid out his nuclear policy in Prague in 2009. For decades, presidential decision directives have made clear the purpose of nuclear weapons in U.S. national security strategy and provided broad guidance for military planners who prepare the operations and targeting plans for our nuclear forces. An update to existing presidential guidance is one of the homework items tasked by the 2010 Nuclear Posture Review.¶ Cyberthreats are very real, and **there is** much we ne**ed to do to defend our military and critical civilian infrastructure against** what former defense secretary Leon E. Panetta referred to as **a “cyber Pearl Harbor”** — including enhancing the ability to take action, when directed by the president, against those who would attack us. We also need more diplomacy such as that practiced by Obama with his Chinese counterpart, Xi Jinping, at their recent summit. Multinational cooperation centers could ultimately lead to shared approaches to cybersecurity, including agreements related to limiting cyberwar.

#### Second, cyber crime

**Defense solves it**

**McGraw 13**

<[Gary McGraw](http://www.tandfonline.com/action/doSearch?action=runSearch&type=advanced&searchType=journal&result=true&prevSearch=%2Bauthorsfield%3A(McGraw%2C+G)), PhD is Chief Technology Ofﬁcer of Cigital, and author of¶ Software Security (AWL 2006) along with ten other software security¶ books. He also produces the monthly Silver Bullet Security Podcast for¶ IEEE Security & Privacy Magazine (syndicated by SearchSecurity), Cyber War is Inevitable (Unless We Build Security In), Journal of Strategic Studies - Volume 36, Issue 1, 2013, pages 109-119, <http://www.tandfonline.com.proxy.library.cornell.edu/doi/pdf/10.1080/01402390.2012.742013>>#**SPS**

**The conceptual conﬂation of cyber war, cyber espionage, and cyber**¶ **crime into a three-headed cyber Cerberus perpetuates fear, uncertainty**¶ **and doubt. This has made the already gaping policy vacuum on cyber**¶ **security more obvious than ever before.**¶ Of the three major cyber security concerns in the public eye, cyber¶ crime is far more pervasive than cyber war or espionage. And yet it is¶ the least commonly discussed among policymakers. Cyber crime is¶ already commonplace and is growing: 285 million digital records were¶ breached in 2008 and 2011 boasted the second-highest data loss total¶ since 2004.2¶ Though economic calculations vary widely and are difﬁcult to make,¶ cyber crime and data loss have been estimated to cost the global¶ economy at least $1.0 trillion dollars annually.3¶ Even if this estimate is¶ an order of magnitude too high, cyber crime is still an important problem that needs addressing. Just as consumers ﬂock to the Internet,¶ so do criminals. Why did Willie Sutton, the notorious Depression-era¶ gangster, rob banks? As he famously (and perhaps apocryphally) put it:¶ ‘That’s where the money is.’ Criminals ﬂock to the Internet for the same¶ reason.¶ Cyber espionage is another prominent problem that captivates the¶ imagination, and is much more common than cyber war. The highly¶ distributed, massively interconnected nature of modern information¶ systems makes keeping secrets difﬁcult. It is easier than ever before to¶ transfer, store and hide information, while more information than ever¶ before is stored and manipulated on networked machines. A pen drive¶ the size of a little ﬁnger can store more information than the super¶ computers of a decade ago.¶ **Cyber war, cyber espionage, and cyber crime all share the same root**¶ **cause: our dependence on insecure networked computer systems.** The¶ bad news about this dependency is that cyber war appears to be¶ dominating the conversation among policy-makers even though cyber¶ crime is the largest and most pervasive problem. **When pundits and**¶ **policymakers focus only on cyber war, the most threats emanating from**¶ **cyber crime and espionage are relegated to the background.** **Interestingly, building systems properly from a security perspective will address**¶ **the cyber crime and espionage problems just as effectively as it will**¶ **address cyber war.** **By building security into our systems in the ﬁrst**¶ **place we can lessen the possibility of cyber war, take a bite out of cyber**¶ **crime, and deter cyber espionage all at the same time.**

#### Major cyber-crime crushes the global economy via ripple effects

Sani et al 12

<Hemraj, Associate Professor & Head, Department of Computer Science & Engineering, Alwar Institute of Engineering & Technology, Yerra Shankar, PhD Student, Department of Mathematics Shiksha ‗O‘ Anusandhan University, T.C. Principal, Orissa Engineering College, “Cyber-Crimes and their Impacts: A Review,” Vol. 2, Issue 2,Mar-Apr 2012, <http://www.ijera.com/papers/Vol2_issue2/AG22202209.pdf>>#SPS

.1. Potential Economic Impact ¶ The 2011 Norton Cyber crime disclosed that over 74 million people in the United States were victims of cyber crime ¶ in 2010. These criminal acts resulted in $32 billion in direct financial losses. Further analysis of this growing ¶ problem found that 69 percent of adults that are online have been victims of cyber crime resulting in 1 million cyber ¶ crime victims a day. Many people have the attitude that cyber crime is a fact of doing business online! [18]. ¶ As today‘s consumer has become increasingly dependent on computers, networks, and the information these ¶ are used to store and preserve, the risk of being subjected to cyber-crime is high. Some of the surveys conducted ¶ in the past have indicated as many as 80% of the companies‘ surveyed acknowledged financial losses due to ¶ computer breaches. The approximate number impacted was $450 million. Almost 10% reported financial fraud ¶ [14]. Each week we hear of new attacks on the confidentiality, integrity, and availability of computer systems. This ¶ could range from the theft of personally identifiable information to denial of service attacks. ¶ As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks ¶ are traded via internet, bank transactions are performed via internet, purchases are made using credit card via ¶ internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the ¶ economy. ¶ The disruption of international financial markets could be one of the big impacts and remains a serious ¶ concern. The modern economy spans multiple countries and time zones. Such interdependence of the world's ¶ economic system means that a disruption in one region of the world will have ripple effects in other regions. ¶ Hence any disruption of these systems would send shock waves outside of the market which is the source of the ¶ problem. ¶ Productivity is also at risk. Attacks from worms, viruses, etc take productive time away from the user. Machines ¶ could perform more slowly; servers might be in accessible, networks might be jammed, and so on. Such ¶ instances of attacks affect the overall productivity of the user and the organization. It has customer service impacts ¶ as well, where the external customer sees it as a negative aspect of the organization. ¶ In addition, user concern over potential fraud prevents a substantial cross-section of online shoppers from ¶ transacting business. It is clear that a considerable portion of e-commerce revenue is lost due to shopper hesitation, ¶ doubt, and worry. These types of consumer trust issues could have serious repercussions and bear going into more ¶ detail

#### Economic collapse causes nuclear conflicts

Burrows and Harris 9

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

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

## Plan

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

## Solvency

#### The plan solves –

#### First, norm-setting - other countries model our use of OCOs — clear restrictions on use are essential

Bradbury 11

Assistant Attorney General for the Office of Legal Counsel

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

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

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

Goldsmith 10

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

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

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

Lewis 11

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

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

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

Dycus 10

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

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

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

Bastby 12

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

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

**Criticizing the probability of our impacts is meaningless – all war is low probability but examining policies around cyber warfare operations is critical to prevent miscalculation. Our roleplaying in this space has long term effects on the political and changes the way we orient cyber policies**

**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:** i**nternational** r**elations 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.**¶What is Cyber War? (Again. . .)¶ Rid and Liff do not deﬁne cyber war the same way, and there is no¶ disciplinary consensus. Rid, Liff, and this author at least agree on the¶ following: **cyber war is a coercive act involving computer network**¶ **attack. Network attack means information is disrupted, degraded, or**¶ **destroyed**. **‘Coercive’ means using force to change or preserve a political**¶ **status quo**. A point of contention is lethality, which Rid believes is¶ necessary for cyber ‘war’.2¶ This is an extreme and undesirable¶ requirement, particularly because (as Rid himself points out) non-lethal¶ cyber attacks may be more costly than conventional warfare.3¶ It is¶ important to note that Rid focuses on network attack, whereas Liff¶ considers a broader conﬂict process. This response addresses both.¶ The central point of Rid’s article is that it is difﬁcult to cause lethal¶ effects with cyber weapons, and that politically motivated, instrumental cyber attack has never killed anyone.4¶ While the empirics of his¶ article are sound – he describes recent cyber attacks accurately – **Rid**¶ **never explains what causes war or makes war more or less likely. The**¶ **arguments in his article are exclusively deﬁnitional, and do not directly**¶ **support his title’s assertion that ‘Cyber War Will Not Take Place**.’¶ Liff does better from a theoretical point of view; he links his article to¶ the bargaining approach to war.5¶ He does an excellent job of offering¶ counterpoints to four arguments about why cyber attack may increase¶ the probability of war. However, **Liff** never establishes why his¶ reasonable views are more plausible than their alternatives. This is¶ because he **is not explicit about assumptions that are necessary for his**¶ **arguments to hold, nor about the circumstances under which those**¶ **assumptions break down**. For example, Liff argues that private¶ information may make war less likely because states poorly estimate he gains from cyber attack.6¶ Although Liff is right to point out that¶ ambiguity in cyber operations is important, he is wrong to assume the¶ causal arrow points in one direction. Ambiguity can make war more or¶ less likely, because it may lead states to overestimate their potential¶ gains, overestimate their stealth, and/or underestimate their adversary’s¶ skill.¶ Finally, **it must be recognized that any future war is a low probability event. Crafting claims that particular conﬂict scenarios are improbable** is rather unimpressive**; what is important to understand is the potential cost and probability of cyber war relative to other kinds of conﬂict.**¶Causes of Cyber War¶ **The noted problems in the Rid and Liff articles could have been**¶ **avoided by drawing on structured theoretical approaches that are**¶ **common to the study of the causes of all kinds of warfare**. What would¶ such an approach look like? This response lacks the space to fully¶ develop one, but recommends a way forward. Literally **dozens of**¶ **arguments have been advanced in the political science discipline**¶ **regarding the causes of war, and very many of these offer reasons to**¶ **believe cyber war is** plausible or even **probable**.7¶ An approach,¶ advanced in James Fearon’s modern classic ‘Rationalist Explanations¶ for War,’ is to list assumptions that create an ideal condition in which¶ war should never happen.8¶ One way to structure scientiﬁc inquiry¶ regarding the probability of cyber war is to examine how **the unique**¶ **material qualities of IT affect each of the assumptions**. Table 1 offers a¶ cursory version of such an analysis to identify priority areas for further¶ study. Among a large number of revealed paths to cyber war, one –¶ principal-agent problems involving the bureaucracies that conduct¶ cyber operations – is detailed here to demonstrate the plausibility of¶ speciﬁc mechanisms and what follow-on empirical work should look¶ like.¶ Principal-Agent Problems¶ Rid and Liff appear to assume that states are unitary rational actors¶ (URAs), and do not explain the domestic political processes whereby¶ states make foreign policy choices. **Empirically and theoretically, it is important to relax the URA assumption and problematize who has**¶ **formal and actual release authority over cyber weapons.** **The principal agent approach**, for instance, **works from the premise that** individuals and **organizations often vary in their incentives and preferences, which could make war beneﬁcial for some at the cost of others**.9¶ **This** and¶ related **thinking inform how scholars study other military technologies,**¶ **such as nuclear weapons**. Scott Sagan points out **that although unauthorized nuclear war is improbable, it is sufﬁciently probable that people should worry a great deal about command and control (C2)** **issues**.10 Many anecdotes echo Sagan’s work. For example, a Russian¶ general was asked during the Cold War about his backup plan in the¶ event he could not open the safe containing his nuclear launch codes.¶ His answer was that he would bash the safe open with a sledgehammer¶ he kept nearby!11¶ Consideration of how bureaucracies do what they do – like keeping¶ emergency nuclear war sledgehammers – is of critical importance to the¶ cyber C2 question. Although controlling large organizations is a core¶ function of militaries, **the conduct of cyber operations is different from**¶ **other kinds of activity in a way that greatly magniﬁes the ‘strategic corporal’ problem. This is because constant cyber operations** other than¶ war **decrease the bureaucratic friction that normally alerts superiors to**¶ **aberrant behavior.** In the case of nuclear weapons, a long chain of¶ events is required before unauthorized activities occur. Someone¶ probably would notice a crazed general using his sledgehammer on¶ the launch codes safe, turning keys, fueling missiles, and so on. In¶ contrast, **it is a core function of cyber bureaucrats to access adversary**¶ **networks constantly, and to develop push-button solutions to minimize**¶ **lags during war**. Furthermore**, if the perception that cyber weapons are**¶ **non-lethal comes to be widely perceived** (as Rid would prefer), **it is**¶ **reasonable to conclude that** the threshold for their use will be lower¶ **than other kinds of weapons – even if the cost of cyber attacks is**¶ **greater.**¶While weak C2 is a necessary condition for a war caused by¶ principal-agent problems, it is not sufﬁcient, because bureaucracies¶ (agents) must also have different incentives or preferences from their¶ populations or leaders (the ‘principals’). A deep political science literature argues that militaries are more prone to favor offensive operations than other kinds of bureaucracies.12 Early evidence suggests that¶ **this ‘cult of the offensive’ operates regarding cyber warfare**. James¶ **Cartwright**, the former Vice Chairman of the US Joint Chiefs of Staff,¶ **calls for the United States to engage in more offensive cyber operations,**¶ **and reportedly created a bureaucracy to that end.**13 **This perspective exists in other countries; ofﬁcials with** South Korea’s Cyber Command¶ believe that ‘the best defense is a good offense’**, and that they should**¶ **preemptively disable menacing foreign servers.14** Chinese military¶ textbooks recommend ‘information offensive through computer network attack’in advance of conventional warfare.15 In contrast, nearly¶ all other bureaucracies – such as those responsible for diplomacy, law¶ enforcement, and homeland security – appear oriented toward cyber¶ defense.¶ **If this offensive mindset is observed in countries where civilians have**¶ **ﬁrm control over military organizations, then what is the risk from**¶ **countries with different civil-military relations?16 The thought of weak**¶ **or military-dominated states possessing advanced cyber capabilities is**¶ **troubling,** to say the least, **and offers highly plausible paths to cyber**¶ **wa**r. An example, **North Korea, already has demonstrated offensive**¶ **tendencies, as that government appears to have conducted disruptive**¶ **and destructive cyber attacks**.17¶ **Many potential paths to war result from a combination of ‘cult of the**¶ **offensive’ reasoning and weak C2. One is for militaries to justify cyber**¶ **attack as acts of self-defense or preemption. Another is for militaries to**¶ **conduct offensive cyber operations without informing their superiors.**¶ **Yet another is the potential for offensive biases to make them more**¶ **easily fall bait to ‘false ﬂag’ operations**. These are merely derivatives of¶ principal-agent problems that arise among politically motivated actors;¶ the outlook worsens when considering other incentives, such as proﬁt,¶ that may lead corrupt bureaucrats to sell lethal skills or software to the¶ highest bidder.¶ **So, how much should scholars and practitioners care about cyber wa**r?¶ A belief that cyber war is hyped appears to have motivated Rid and Liff¶ to pen their pieces. **A satisfying answer must explain at least two things:**¶ **the destructive potential of cyber war, and the probability that it will**¶ **happen. It appears uncontroversial that,** if **cyber war** happens, it **will be** ¶ **highly costly** even if not lethal. Few contest the idea that a successful¶ and sustained degradation of military capabilities, deprivation of¶ civilian services, destruction of ﬁnancial records, or other such ‘digital¶ Pearl Harbor’ scenarios, would be pretty bad.¶ On the other hand, there is little agreement in academic or policy¶ circles regarding whether or not cyber war will happen. **This response**¶ **offers an important corrective to narratives that cyber war is**¶ **improbable. A small number of premises lead to a conclusion that**¶cyber war is, at a minimum, plausible enough to merit serious¶ attention. Further research would do well to commit to theoretical¶ paradigms, such as the approach recommended in Table 1. This kind of¶ rigorous scholarship is a prerequisite to reducing the incidence of cyber¶ conﬂict and avoiding cyber war.

#### Arguing against the practices of the USFG in the context of war powers allows for an engaged public that can expose the hypocrisy of the federal government – only focus on specific policy questions can actualize change by making it relevant to policy-makers –

Mellor 13

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

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

# 2AC

## Kritik

#### There is likely a near-zero chance of nuclear war, but protective and defensive counter-measures like the aff are still necessary

**Matheny, ‘7** [Jason G. Matheny, “Reducing the Risk of Human Extinction” Risk Analysis, Vol. 27, No. 5, 2007]

It is possible for humanity (or its descendents) to survive a million years or more, but we could succumb to extinction as soon as this century. During the Cuban Missile Crisis, U.S. President Kennedy estimated the probability of a nuclear holocaust as “somewhere be- tween one out of three and even” (Kennedy, 1969, p. 110). John von Neumann, as Chairman of the U.S. Air Force Strategic Missiles Evaluation Committee, pre- dicted that it was “absolutely certain (1) that there would be a nuclear war; and (2) that everyone would die in it” (Leslie, 1996, p. 26). More recent predictions of human extinction are little more optimistic. In their catalogs of extinction risks, Britain’s Astronomer Royal, Sir Martin Rees (2003), gives humanity 50-50 odds on surviving the 21st century; philosopher Nick Bostrom argues that it would be “misguided” to assume that the probability of extinction is less than 25%; and philosopher John Leslie (1996) assigns a 30% probability to extinction during the next five centuries. The “Stern Review” for the U.K. Treasury (2006) assumes that the probability of human extinction during the next century is 10%. And some explanations of the “Fermi Paradox” imply a high probability (close to 100%) of extinction among technological civilizations (Pisani, 2006).4 **Estimating the probabilities of unprecedented events is subjective**, so we should treat these numbers skeptically. Still, even if the probability of extinction is several orders lower, because the stakes are high, it could be wise to invest in extinction countermeasures.

#### Thinking about worst-case cyber scenarios is good- key to preparedness and reduces chances of cyber war

**Clarke and Knake ‘10**

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

In the seminal 1983 movie about computers and war, War Games, ¶ starring a young Matthew Broderick, the tinny computer voice ¶ asked haltingly, “Do you want to play a game of thermonuclear war?” ¶ Why don’t we play a game of cyber war in order to elucidate some of ¶ the policy choices that shape a strategy. DoD runs such exercises, ¶ called Cyber Storm, annually. The CIA’s annual cyber war exercise, ¶ Silent Horizon, has been happening since 2007. For the purposes of ¶ this analysis, I’ll make the same request of you that I made of students ¶ at Harvard’s Kennedy School and national security bureaucrats sitting ¶ around the White House Situation Room conference table: “Don’t ¶ fight the scenario.” By that I mean, **do not spend a lot of time rejecting** ¶ **the premise that circumstances could happen someday that would** ¶ **result in the U.S. being on the edge of conflict with Russia or China. When U.S. cyber warriors talk about the “big one,” they usually** ¶ **have in mind a conflict in cyberspace with Russia or China**, the two ¶ nations with the most sophisticated offensive capability other than ¶ the U.S. **No one wants hostilities with those countries to happen.** ¶ **Thinking about it, for the purposes of understanding what cyber** ¶ **war would look like, does not make it more likely**. In fact, **by under­**¶ **standing the risks of our current cyber war posture, we might reduce** ¶ **the chances of a real cyber war.** **And if, despite our intentions, a** ¶ **cyber war does happen, it would be best to have thought in advance** ¶ **about how it could unravel.**¶ **Certainly, I did not want to see the attack of 9/11 happen, but I** ¶ **had chaired countless** “tabletop exercises,” or **war game scenarios,** **to** ¶ **get myself and the bureaucracy ready in case something like it did** ¶ **happen**. **When it came, we had already thought through how to re­**¶ **spond on the day of an attack and the few days thereafter**. We spent ¶ enormous effort to try to prevent attacks, but we also devoted some ¶ time to thinking about what we would do if one succeeded. **Had we** ¶ **not done so, that awful day would have been even worse**. **So**, **in that** ¶ **spirit of learning by visualizing, let’s think about a period of rising** ¶ **tensions** between the U.S. and China.

#### 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.

#### Risk framing motivates new social movements and re-democratizes politics

**Borraz, ‘7** [Olivier Borraz, Centre de Sociologie des Organisations, Sciences Po-CNRS, Paris, Risk and Public Problems, Journal of Risk Research Vol. 10, No. 7, 941–957, October 2007, p. 951]

**These studies** seem to **suggest** that **risk is a way of framing a public problem in such a way as to politicize the search for solutions. This politicization entails**, in particular, **a widening of** the range of **stakeholders, a reference to broader political issues** and debates, **the search for new decision- making processes** (either **in terms of democratization**, or renewed scientific expertise), and the explicit mobilization of non-scientific arguments in these processes. But if this is the case, then it could also be true that risk is simply one way of framing public problems. Studies in the 1990s, in particular, showed that a whole range of social problems (e.g., poverty, housing, unemployment) had been reframed as health issues, with the result that their management was transferred from social workers to health professionals, and in the process was described in neutral, depoliticized terms (Fassin, 1998). **Studies of risk**, on the contrary, seem to **suggest that similar social problems could well be re-politicized**, i.e., **taken up by new social movements**, producing and using alternative scientific data, calling for more deliberative decision-making procedures, and clearly intended to promote change in the manner in which the state protects the population against various risks (health and environment, but also social and economic). In other words, **framing public problems as risks could afford an opportunity for a transformation in the political debate**, from more traditional cleavages around social and economic issues, to rifts stemming from antagonistic views of science, democracy and the world order.

#### Ignoring the threat causes panic – worse than fear, stops solvency, turns their state power arguments

**Sandman and Lanard, 2003**

Peter M. PhD in Communications and Professor at Rutgers specializing in crisis communication; Jody, Psychiatrist, 28 April, “Fear Is Spreading Faster than SARS — And So It Should!”

China is universally condemned for covering up SARS and putting the world at risk. **Covering up an epidemic is about as bad a communication strategy as we can imagine**. Among its outcomes: **China actually does face a panic problem, as its people confront not just a raging epidemic but a government that lies to them about it. The West’s “soft cover-up” is much gentler and less dishonest** — a cover-up of over-reassurance and minimization rather than of lies. **But if SARS does keep getting worse in the West**, as it has in China, **the soft cover-up will also fail ... and may also provoke panic. Public anxiety can lead to genuine panic or to astonishing resilience**. The paradox is that efforts **to squelch the anxiety** (“allay the public’s fear” is the usual phrase) **can actually induce the panic it aims to prevent. Resilience is likelier when authorities ally with the anxiety, harness it,** and steer it instead of trying to prevent it. Of course even superb handling of the public’s fears may not prevent panic if the epidemic gets bad enough. There has often been some panic during the great epidemics of the past. But **panic will be likelier and more widespread if the authorities have been minimizing the risk than if they have been acknowledging it candidly** and compassionately.

#### There’s no one root cause of war

**Sharp 8** – senior associate deputy general counsel for intelligence at the US Department of Defense, Dr. Walter, “Democracy and Deterrence”, Air Force University Press, May, http://aupress.maxwell.af.mil/Books/sharp/Sharp.pdf

**While classical liberals focused on political structures, socialists analyzed the socioeconomic system** of states as the primary factor in determining the propensity of states to engage in war. Socialists such as Karl Marx attributed war to the class structure of society; Marx believed that war resulted from a clash of social forces created by a capitalist mode of production that develops two antagonistic classes, rather than being an instrument of state policy. Thus capitalist states would engage in war because of their growing needs for raw materials, markets, and cheap labor. **Socialists believed replacing capitalism with socialism could prevent war, but world events have proven socialists wrong as well**.32 **These** two **schools of thought**—war is caused by innate biological drives or social institutions—**do not demonstrate any meaningful correlation with the occurrence or nonoccurrence of war. There are many variables not considered** by these two schools: for example, the influence of **national special interest groups such as the military or defense contractors** that **may seek glory through victory, greater resources, greater domestic political power, or justification for their existence.** Legal scholar Quincy **Wright** has conducted one of the “most thorough studies of the nature of war”33 and **concludes that there “is no single cause of war**.”34 In *A Study of War*, he concludes that **peace is an equilibrium of four complex factors: military and industrial technology, international law governing the resort to war, social and political organization at the domestic and international level, and the distribution of attitudes and opinions concerning basic values.** War is likely when controls on any one level are disturbed or changed.35 Similarly, **the 1997 US National Military Strategy identifies the root causes of conflict as political, economic, social, and legal conditions.**36 **Moore** has **compiled the following list of conventional explanations for war: specific disputes; absence of dispute settlement mechanisms; ideological disputes; ethnic and religious differences; communication failures; proliferation of weapons and arms races; social and economic injustice; imbalance of power; competition for resources; incidents, accidents, and miscalculation; violence in the nature of man; aggressive national leaders; and economic determination**. He has concluded, however, that these causes or motives for war explain specific conflicts but fail to serve as a central paradigm for explaining the cause of war.37

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

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

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

**Privileging ontology and epistemology guarantees policy failure because of theoretical reductionism, and isn’t relevant to the truth value of our arguments.**

Owen 2 **(**university of Southampton, David Owen, Reader of Political Theory at the Univ. of Southampton, Millennium Vol 31 No 3 2002 p. 655-7)

Commenting on the ‘philosophical turn’ in IR, Wæver remarks that ‘[a] frenzy for words like “epistemology” and “ontology” often signals this philosophical turn’, although he goes on to comment that these terms are often used loosely.4 However, loosely deployed or not, it is clear that debates concerning ontology and epistemology play a central role in the contemporary IR theory wars. In one respect, this is unsurprising since it is a characteristic feature of the social sciences that periods of disciplinary disorientation involve recourse to reflection on the philosophical commitments of different theoretical approaches, and there is no doubt that such reflection can play a valuable role in making explicit the commitments that characterise (and help individuate) diverse theoretical positions. Yet, such a philosophical turn is not without its dangers and I will briefly mention three before turning to consider a confusion that has, I will suggest, helped to promote the IR theory wars by motivating this philosophical turn. The first danger with the philosophical turn is that it has an inbuilt tendency to prioritise issues of ontology and epistemology over explanatory and/or interpretive power as if the latter two were merely a simple function of the former. But **while the** explanatory and/or interpretive **power of a theoretical account is not** wholly **independent of its ontological and**/or **epistemological commitments** (otherwise criticism of these features would not be a criticism that had any value), **it is by no means clear that it is**, in contrast, **wholly dependent on these** philosophical **commitments**. Thus, for example, **one need not be sympathetic to rational choice theory to recognise** that **it can provide powerful accounts of certain** kinds of **problems**, such as the tragedy of the commons in which dilemmas of collective action are foregrounded. It may, of course, be the case that the advocates of rational choice theory cannot give a good account of why this type of theory is powerful in accounting for this class of problems (i.e., how it is that the relevant actors come to exhibit features in these circumstances that approximate the assumptions of rational choice theory) and, if this is the case, it is a philosophical weakness—but this does not undermine the point that, for a certain class of problems, rational choice theory may provide the best account available to us. In other words, while the critical judgement of theoretical accounts in terms of their ontological and/or epistemological sophistication is one kind of critical judgement, it is not the only or even necessarily the most important kind. The second danger run by the philosophical turn is that because **prioritisation of ontology and epistemology** promotes theory-construction from philosophical first principles, it **cultivates a theory-driven rather than problem-driven approach to IR**. Paraphrasing Ian Shapiro, the point can be put like this: **since** it is the case that **there is always a plurality of possible true descriptions of a given action**, event or phenomenon, **the challenge is to decide which is the most apt** in terms of getting a perspicuous grip on the action, event or phenomenon in question given the purposes of the inquiry; yet, from this standpoint, **‘theory-driven work is** part of a **reductionist** program’ **in that it ‘dictates always opting for the description** that calls for the explanation that **flows from the preferred model** or theory’.5 The justification offered for this strategy rests on the mistaken belief that it is necessary for social science because general explanations are required to characterise the classes of phenomena studied in similar terms. However, as Shapiro points out, this is to misunderstand the enterprise of science since ‘**whether there are general explanations** for classes of phenomena **is a question for** social-scientific **inquiry, not to be prejudged** before conducting that inquiry’.6 Moreover, **this** strategy easily **slips into** the promotion of the pursuit of **generality over** that of **empirical validity**. The third danger is that the preceding two combine to encourage the formation of a particular image of disciplinary debate in IR—what might be called (only slightly tongue in cheek) ‘the Highlander view’—namely, an image of warring theoretical approaches with each, despite occasional temporary tactical alliances, dedicated to the strategic achievement of sovereignty over the disciplinary field. It encourages this view because the turn to, and prioritisation of, ontology and epistemology stimulates the idea that there can only be one theoretical approach which gets things right, namely, the theoretical approach that gets its ontology and epistemology right. This image feeds back into IR exacerbating the first and second dangers, and so a potentially vicious circle arises.

#### Value to life should be individually determined – their impact claims invalidate personal autonomy

SCHWARTZ, HENDRY, & PREECE 2004 Professional Metaphysician, Senior Lecturer, General Practicianer Professor, Academic Surgeon [“Medical Ethics: A case based approach,” Lisa, Paul, and Robert]

Those who choose to reason on this basis hope that if the quality of a life can be measured then the answer to whether that life has value to the individual can be determined easily. This raises special problems, however, because the idea of quality involves a value judgement, and value judgements are, by their essence, subject to indeterminate relative factors such as preferences and dislikes. Hence, **quality of life is difficult to measure and will vary according to individual tastes, preferences and aspirations**. As a result, **no general rules or principles can be asserted that would simplify decisions about the value of a life based on its quality**. Nevertheless, **quality is still an essential criterion in making such decisions because it gives legitimacy to the possibility that rational, autonomous persons can decide for themselves that their own lives either are worth, or are no longer worth, living. To disregard this possibility would be to imply that no individuals can legitimately make such value judgements about their own lives** and, if nothing else, that would be counterintuitive. 2 In our case, Katherine Lewis had spent 10 months considering her decision before concluding that her life was no longer of a tolerable quality. She put a great deal of effort into the decision and she was competent when she made it. Who would be better placed to make this judgement for her than Katherine herself? And yet, a doctor faced with her request would most likely be uncertain about whether Katherine's choice is truly in her best interest, and feel trepidation about assisting her. We need to know which considerations can be used to protect the patient's interests. The quality of life criterion asserts that there is a difference between the type of life and the fact of life. This is the primary difference between it and the sanctity criterion discussed on page 115. Among quality of life considerations rest three assertions: 1. there is relative value to life 2. the value of a life is determined subjectively 3. not all lives are of equal value. Relative value The first assertion, that life is of relative value, could be taken in two ways. In one sense, it could mean that the value of a given life can be placed on a scale and measured against other lives. The scale could be a social scale, for example, where the contributions or potential for contribution of individuals are measured against those of fellow citizens. **Critics of quality of life criteria frequently name this as a potential slippery slope where lives would be deemed worthy of saving, or even not saving, based on the relative social value of the individual concerned.** So, for example, a mother of four children who is a practising doctor could be regarded of greater value to the community than an unmarried accountant. The concern is that the potential for discrimination is too high. **Because of the possibility of prejudice and injustice, supporters of the quality of life criterion reject this interpersonal construction in favour of a second, more personalized, option.** According to this interpretation, the notion of relative value is relevant not between individuals but within the context of one person's life and is measured against that person's needs and aspirations. So Katherine would base her decision on a comparison between her life before and after her illness. The value placed on the quality of a life would be determined by the individual depending on whether he or she believes the current state to be relatively preferable to previous or future states and whether he or she can foresee controlling the circumstances that make it that way. Thus, the life of an athlete who aspires to participate in the Olympics can be changed in relative value by an accident that leaves that person a quadriplegic. The athlete might decide that the relative value of her life is diminished after the accident, because she perceives her desires and aspirations to be reduced or beyond her capacity to control. However, if she receives treatment and counselling her aspirations could change and, with the adjustment, she could learn to value her life as a quadriplegic as much or more than her previous life. This illustrates how it is possible for a person to adjust the values by which they appraise their lives. For Katherine Lewis, the decision went the opposite way and she decided that a life of incapacity and constant pain was of relatively low value to her. It is not surprising that the most vociferous protesters against permitting people in Katherine's position to be assisted in terminating their lives are people who themselves are disabled. Organizations run by, and that represent, persons with disabilities make two assertions in this light. First, they claim that accepting that Katherine Lewis has a right to die based on her determination that her life is of relatively little value is demeaning to all disabled people, and implies that any life with a severe disability is not worth living. Their second assertion is that with proper help, over time Katherine would be able to transform her personal outlook and find satisfaction in her life that would increase its relative value for her. The first assertion can be addressed by clarifying that the case of Katherine Lewis must not be taken as a general rule. Deontologists, who are interested in knowing general principles and duties that can be applied across all cases would not be very satisfied with this; they would prefer to be able to look to duties that would apply in all cases. Here, a case-based, context-sensitive approach is better suited. Contextualizing would permit freedom to act within a particular context, without the implication that the decision must hold in general. So, in this case, Katherine might decide that her life is relatively valueless. In another case, for example that of actor Christopher Reeve, the decision to seek other ways of valuing this major life change led to him perceiving his life as highly valuable, even if different in value from before the accident that made him a paraplegic. This invokes the second assertion, that Katherine could change her view over time. Although we recognize this is possible in some cases, it is not clear how it applies to Katherine. Here we have a case in which a rational and competent person has had time to consider her options and has chosen to end her life of suffering beyond what she believes she can endure. Ten months is a long time and it will have given her plenty of opportunity to consult with family and professionals about the possibilities open to her in the future. Given all this, it is reasonable to assume that Katherine has made a well-reasoned decision. It might not be a decision that everyone can agree with but if her reasoning process can be called into question then at what point can we say that a decision is sound? She meets all the criteria for competence and she is aware of the consequences of her decision. It would be very difficult to determine what arguments could truly justify interfering with her choice. Subjective determination The second assertion made by supporters of the quality of life as a criterion for decisionmaking is closely related to the first, but with an added dimension. This assertion suggests that the **determination of the value of the quality of a given life is a subjective determination to be made by the person experiencing that life.** The important addition here is that **the decision is a personal one that, ideally, ought not to be made externally by another person but internally by the individual involved.** Katherine Lewis made this decision for herself based on a comparison between two stages of her life. So did James Brady. Without this element**, decisions based on quality of life criteria lack salient information and the patients concerned cannot give informed consent. Patients must be given the opportunity to decide for themselves whether they think their lives are worth living or not. To ignore or overlook patients' judgement in this matter is to violate their autonomy and their freedom to decide for themselves on the basis of relevant information about their future, and comparative consideration of their past.** As the deontological position puts it so well, **to do so is to violate the imperative that we must treat persons as rational and as ends in themselves**.

#### Ontology is a DESTRUCTIVE HISTORICAL FICTION – any GATEWAY claims are just TRICKS based on how we SHELVE BOOKS

**Shirky 5**

Clay Shirky, teacher of NYU's graduate Interactive Telecommunications Program, 03/15/05¶ <http://www.itconversations.com/shows/detail470.html>¶ I hold a joint appointment at NYU, as an Associate Arts Professor at the Interactive Telecommunications Program (ITP) and as a Distinguished Writer in Residence in the Journalism Department. I am also a Fellow at the Berkman Center for Internet and Society, and was the Edward R. Murrow Visiting Lecturer at Harvard's Joan Shorenstein Center on the Press, Politics, and Public Policy in 2010.

**There are many ways to organize data:** labels, lists, categories, taxonomies, **ontologies.** Of these, **ontology -- assertions about essence and relations among a group of items -- seems to be the highest-order method of organization**. Indeed, the predicted value of the Semantic Web assumes that ontological successes such as the Library of Congress's classification scheme are easily replicable. Those successes are not easily replicable. **Ontology, far from being an ideal high-order tool, is a 300-year-old hack, now nearing the end of its useful life. The problem ontology solves is not how to organize ideas but how to organize things** -- **the Library of Congress's classification scheme exists not because concepts require consistent hierarchical placement, but because books do**. The LC scheme, when examined closely, is riddled with inconsistencies, bias, and gaps. Top level geographic categories, for example, include "The Balkan Penninsula" and "Asia." The primary medical categories don't include oncology, defaulting to the older and now discredited notion that cancers were more related to specific organs than to common processes. And the list of such oddities goes on. The reason the LC scheme is accumulating these errors faster than they can correct them is the physical fact of the book, which makes a card catalog scheme necessary, and constant re-shelving impossible. Likewise**, it enforces cookie-cutter categorization** **that doesn't reflect the polyphony of its contents--there is a literature of creativity, for example, made up of books about art, science, engineering, and so on, and yet those books are not categorized** (which is to say shelved) **together, because the LC scheme doesn't recognize creativity** as an organizing principle. For a reader interested in creativity, the LC **ontology destroys value rather than creating it.** ¶ As we have learned from the Web**, when data is decoupled from physical presence, it is fluid enough to be grouped differently by different readers, and on different days**. The Web's main virtue, in handling data, is to transmute organization from an a priori, content-based judgment to one that can be ad hoc, context-based, socially embedded, and constantly altered. **The Web frees us from needing to argue about whether The Book of 5 Rings "is" a business book or a primer on war -- it is plainly both, and not only are we freed from making that judgment firmly or in advance, we are freed from needing to make it explicit at all.** ¶ This talk begins by exploring **the rise of ontological classification**. In the period after the invention of the printing press but before the invention of the search engine, intellectual production **was vested in books,** objects that were numerous but opaque. When you have more than a few hundred books, **categorization becomes a forced move**, even if the categories are somewhat **arbitrary,** **because** without categories, you can no longer locate individual **books**.

#### Problem-solution impact is backwards---acting with a flawed epistemology allows us to change that epistemology.

Harris 7 (Graham, Adjunct Prf. @ Centre for Environment University of Tasmania, Seeking Sustainability in an age of complexity p. 9-10)

1 am not going to address the global 'litany' at length here. The arguments have been well made by others, especially and most elegantly by E. O. Wilson. What 1 wish to address here is the question: 'Can we grasp the complexity of it all and, if so, what do we do about it?' Given the fundamental nature of the problem the destruction of the biosphere and its ecosystem ser- vices together with the huge changes going on in human societies and cultures driven by globalisation and technological change the precautionary principle would suggest that even if the epistemology is flawed, the data are partial and the evidence is shaky, we should pay attention to the little we know and do whatever is possible to mitigate the situation even if we fundamentally disagree about the means and the ends. The only ethical course of action is, as John Ral- ston Saul writes," based on 'a sense of the other and of inclusive responsibility'. We know enough to act. Ethics is about uncertainty, doubt, system thinking and balancing difficult choices. It is about confronting the evidence**.** Over the past two or three decades, as there has been an increasing appre- ciation of the importance of good environmental management, and as western societies have become more open and the ICT revolution has made informa- tion much more widely available there has been a growing debate between the worlds of science, industry, government and the community around environ- mental ethics and environmental issues and their management. During this period new knowledge has been gained, ideas have changed (sometimes quite fundamentally) and there have been huge changes in government and social institutions and policies. We are all on a recursive journey together: we are lit- erally 'making it up as we go along'. This is not easy and there are no optimal solutions. This is an adaptive process requiring feedback from all parts of the system. Yes, there will be surprises. This is why it is so important that when we act we constantly reflect on what we know and what we are doing about it and where it is all going. As we reach the physical limits of the global biosphere the values we place on things are changing and must change further. A new environmental ethic is required, one that is less instrumental and more embracing. Traditionally there has tended to be a schism between those who take an anthropocentric view (that the world is there for us to use) and those who take the non-anthropocentric view (those who value nature in its own right). Orthodox anthropocentrisni dictates that non-human value is instrumental to human needs and interests. In contrast, non-anthropocentrics take an objectivist view and value nature intrinsically; some may consider the source of value in non-human nature to be independent of human consciousness.45 What is required is a more complex and systems view of ethics which finds a middle ground between the instrumentalist and objectivist views. Norton '46 for example, proposes an alternative and more complex theory of value - a universal Earth ethic - which values processes and dynamics as well as entities and takes an adaptive management view of changing system properties. For sustainable development to occur, choices about values will remain within the human sphere but we should no longer regard human preferences as the only criterion of moral significance. 'Humans and the planet have entwined destinies"' and this will be increasingly true in many and complex ways as we move forward. There are calls for an Earth ethic beyond the land ethic of Aldo Leopold.45 The science of ecology is being drawn into the web .49 Ecologists are becoming more socially and culturally aware and engaged" and the 'very doing' of ecology is becoming more ethical.tm' Some scientists are beginning to see themselves more as agents in relationships with society and less as observers.

#### Reps don’t shape reality—focusing on them obscures material and political analysis which turns the criticism

Tuathail 96(Gearoid, Department of Georgraphy at Virginia Polytechnic Institute, Political Geography, 15(6-7), p. 664, science direct)

While theoretical debates at academic conferences are important to academics, the discourse and concerns of foreign-policy decision- makers are quite different, so different that they constitute a distinctive problem- solving, theory-averse, policy-making subculture. **There is a danger that academics assume that the discourses they engage are more significant** in the practice of foreign policy and **the exercise of power than they really are**. This is not, however, to minimize the obvious importance of academia as a general institutional structure among many that sustain certain epistemic communities in particular states. In general, I do not disagree with Dalby’s fourth point about politics and discourse except to note that his statement-‘Precisely because reality could be represented in particular ways political decisions could be taken, troops and material moved and war fought’-evades the important question of agency that I noted in my review essay. **The assumption that it is representations that make action possible is inadequate by itself.** **Political, military and economic structures, institutions, discursive networks and leadership are all crucial in explaining social action and should be theorized together with representational practices**. Both here and earlier, Dalby’s reasoning inclines towards a form of idealism. In response to Dalby’s fifth point (with its three subpoints), it is worth noting, first, that his book is about the CPD, not the Reagan administration. He analyzes certain CPD discourses, root the geographical reasoning practices of the Reagan administration nor its public-policy reasoning on national security. Dalby’s book is narrowly textual; the general contextuality of the Reagan administration is not dealt with. Second, let me simply note that I find that the distinction between critical theorists and post- structuralists is a little too rigidly and heroically drawn by Dalby and others. Third, Dalby’s interpretation of the reconceptualization of national security in Moscow as heavily influenced by dissident peace researchers in Europe is highly idealist, an interpretation that ignores the structural and ideological crises facing the Soviet elite at that time. Gorbachev’s reforms and his new security discourse were also strongly self- interested, an ultimately futile attempt to save the Communist Party and a discredited regime of power from disintegration. The issues raised by Simon Dalby in his comment are important ones for all those interested in the practice of critical geopolitics. While I agree with Dalby that questions of discourse are extremely important ones for political geographers to engage**there is a danger of fetishizing this concern with discourse so that we neglect the institutional and the sociological, the materialist and the cultural, the political and the geographical contexts within which particular discursive strategies become significant**,. Critical geopolitics, in other words, should not be a prisoner of the sweeping ahistorical cant that sometimes accompanies ‘poststructuralism nor convenient reading strategies like the identity politics narrative; it needs to always be open to the patterned mess that is human history.

#### Discursive focus trades off with focus on structural change—it becomes a psychological substitute for action.

Kidner 2k – psychology professor, David, Nature and Psyche, p 66-7

Noam Chomsky has noted that if "it's too hard to deal with real problems,' some academics tend to "go off on wild goose chases that don't matter ... [or] get involved in academic cults that are very divorced from any reality and that provide a defense against dealing with the world as it actually is." An emphasis on language can serve this sort of defensive function; for the **study of discourse enables one to stand aside** from issues **and avoid** any **commitment to a cause** or ideal, **simply** presenting all sides of a debate and **pointing out** the **discursive strategies** involved. **As the physical world** appears to **fade into** mere **discourse**, so **it comes to seem less real** than the language used to describe it; and environmental **issues lose** the dimensions of **urgency** and tragedy and become instead the proving grounds for ideas and attitudes. Rather than walking in what Aldo Leopold described as a "world of wounds," the discursive theorist can study this world dispassionately, safely insulated from the emotional and ecological havoc that is taking place elsewhere. Like experimentalism, this is a schizoid stance that exemplifies rather than challenges the characteristic social pathology of our time; and it is one that supports Melanie Klein's thesis that **the internal object world can serve as a psychotic substitute for an external "real" world that is** either absent or **unsatisfying**." Ian Craib's description of **social constructionism as a "social psychosis"** therefore **seems** entirely **apt**. But what object relations theorists such as Klein fail to point out is the other side of this dialectic that withdrawing from the external world and substituting an internal world of words or fantasies, because of the actions that follow from this state of affairs, makes the former even less satisfying and more psychologically distant, so contributing to the vicious spiral that severs the "human" from the "natural" and abandons nature to industrialism.

**Prefer specific scenarios – even if we invoke some security logic, the fact that others will securitize means that we have to make worst-case assessments to avoid escalation**

Ole **Waever**, Senior Research Fellow – Copenhagen Peace Research Inst., **2K**

(I. R. Theory & the Politics of European Integration, ed Kelstrup/Williams p. 282-285)

The other main possibility is to stress responsibility. Particularly **in a field like security one has to make choices and deal with the challenges and risks that one confronts** – and not shy away into long-range or principled transformations. The meta-political line risks (despite the theoretical commitment to the concrete other) implying that politics can be contained within large ‘systemic’ questions. In line with the classical revolutionary tradition, after the change (now no longer the revolution but the meta-physical transformation), there will be no more problems whereas in our situation (until the change) we should not deal with the ‘small questions’ of politics, only with the large one (cf. Rorty 1996). However, the ethical demand in post-structuralism (e.g. Derrida’s ‘justice’) is of a kind that can never be instantiated in any concrete political order – it is an experience of the undecidable that exceeds any concrete solution and re-inserts politics. Therefore, politics can never be reduced to meta-questions; there is no way to erase the small, particular, banal conflicts and controversies. In contrast to the quasi-institutionalist formula of radical democracy which one finds in the ‘opening’ oriented version of deconstruction, we could with Derrida stress the singularity of the event. To take a position, take part, and ‘produce events’ (Derrida 1994: 89) means to get involved in specific struggles. Politics takes place ‘in the singular event of engagement’ (Derrida 1996: 83). Derrida’s politics is focused on the calls that demand response/responsibility in words like justice, Europe and emancipation. Should we treat security in this manner? No, security is not that kind of call. ‘Security’ is not a way to open (or keep open) an ethical horizon. **Security** is a much more situational concept oriented to the handling of specifics. It **belongs to the sphere of how to handle challenges – and avoid ‘the worst’** (Derrida 1991). Here enters again the possible pessimism hich for the security analyst might be occupational or structural. The infinitude of responsibility (Derrida 1996: 86) or the tragic nature of politics (Morgenthau 1946, Chapter 7) means that one can never feel reassured that by some ‘good deed’, ‘I have assumed my responsibilities’ (Derrida 1996: 86). If I conduct myself particularly well with regard to someone, I know that it is to the detriment of an other; of one nation to the detriment of another nation, of one family to the detriment of another family, of my friends to the detriment of other friends or non-friends, etc. This is the infinitude that inscribes itself within responsibility; otherwise there would be no ethical problems or decisions. (ibid.; and parallel argumentation in Morgenthau 1946; Chapters 6 and 7) Because of this there will remain conflicts and risks – and the question of how to handle them. Should developments be securitized (and if so, in what terms)? Often our reply will be to aim for de-securitization and then politics meet meta-politics; but **occasionally** the underlying **pessimism** regarding the prospects for orderliness and compatibility among human aspirations **will point to** **scenarios sufficiently worrisome that** **responsibility will entail securitization in order to block the worst. As a security/securitization analyst, this means accepting the task of trying to manage and avoid spirals and accelerating security concerns, to try to assist in shaping the continent in a way that creates the least insecurity and violence – even if this occasionally means invoking/producing ‘structures’ or even using the dubious instrument of securitization**. In the case of current European configuration, the above analysis suggests the use of securitization at the level of European scenarios with the aim of preempting and avoiding numerous instances of local securitization that could lead to security dilemmas and escalations, violence and mutual vilification.

**Threats are real**

**Ravenal ‘9**

[Earl C. Ravenal, distinguished senior fellow in foreign policy studies @ Cato, is professor emeritus of the Georgetown University School of Foreign Service. He is an expert on NATO, defense strategy, and the defense budget. He is the author of *Designing Defense for a New World Order.* What's Empire Got to Do with It? The Derivation of America's Foreign Policy.” *Critical Review: An Interdisciplinary Journal of Politics and Society* 21.1 (2009) 21-75]

Quite expectedly, the more doctrinaire of the non-interventionists take pains to deny any straightforward, and therefore legitimate, security motive in American foreign and military policy. In fact, this denial leads to a more sweeping rejection of any recognizably rational basis for American foreign policy, and, even, sometimes (among the more theoretical of the non-interventionists), a preference for non-rational accounts, or “models,” of virtually any nation’s foreign policy-making.4 One could call this tendency among anti-imperialists “motive displacement.” More specifically, in the cases under review here, one notes a receptivity to any reworking of history, and any current analysis of geopolitics, that denigrates “the threat”; and, along with this, a positing of “imperialism” (the almost self-referential and primitive impulse) as a sufficient explanation for the often strenuous and risky actions of great powers such as the United States. Thus, not only is “empire” taken to be a sufficient and, in some cases, a necessary condition in bringing about foreign “threats”; but, by minimizing the extent and seriousness of these threats, the anti-imperialists put themselves into the position of lacking a rational explanation for the derivation of the (pointless at best, counter-productive at worst) policies that they designate as imperialistic. A pungent example of this threat denigration and motive displacement is Eland’s account of American intervention in the Korean and Vietnam wars:¶ After North Korea invaded, the Truman administration intervened merely for the purpose of a demonstration to friends and foes alike. Likewise, according to eminent cold war historians, the United States did not inter- vene in Vietnam because it feared communism, which was fragmented, or the Soviet Union, which wanted détente with the West, or China, which was weak, but because it did not want to appear timid to the world. The behavior of the United States in both Korea and Vietnam is typical of imperial powers, which are always concerned about their reputation, pres- tige, and perceived resolve. (Eland 2004, 64)¶ Of course, the motive of “reputation,” to the extent that it exists in any particular instance, is a part of the complex of motives that characterize a great power that is drawn toward the role of hegemon (not the same thing as “empire”). Reputation is also a component of the power projec- tion that is designed to serve the interest of national security. Rummaging through the concomitants of “imperialism,” Eland (2004, 65) discovers the thesis of “threat inflation” (in this case, virtual threat invention): Obviously, much higher spending for the military, homeland security, and foreign aid are required for a policy of global intervention than for a policy of merely defending the republic. For example, after the cold war, the security bureaucracies began looking for new enemies to justify keeping defense and intelligence budgets high. Similarly, Eland (ibid., 183), in a section entitled “Imperial Wars Spike Corporate Welfare,” attributes a large portion of the U.S. defense budget—particularly the procurement of major weapons systems, such as “Virginia-class submarines . . . aircraft carriers . . . F-22 fighters . . . [and] Osprey tilt-rotor transport aircraft”—not to the systemically derived requirement for certain kinds of military capabilities, but, rather, to the imperatives of corporate pork. He opines that such weapons have no stra- tegic or operational justification; that “the American empire, militarily more dominant than any empire in world history, can fight brushfire wars against terrorists and their ‘rogue’ state sponsors without those gold- plated white elephants.”¶ **The underlying notion of “the security bureaucracies . . . looking for new enemies” is a threadbare concept** that has somehow taken hold across the political spectrum, from the radical left (viz. Michael Klare [1981], who refers to a “threat bank”), to the liberal center (viz. Robert H. Johnson [1997], who dismisses most alleged “threats” as “improbable dangers”), to libertarians (viz. Ted Galen Carpenter [1992], Vice President for Foreign and Defense Policy of the Cato Institute, who wrote a book entitled A Search for Enemies). **What is missing from most analysts’ claims of “threat inflation,” however, is a convincing theory of why, say, the American government significantly (not merely in excusable rhetoric) might magnify and even invent threats (and, more seriously, act on such inflated threat estimates).** In a few places, Eland (2004, 185) suggests that such behavior might stem from military or national security bureaucrats’ attempts to enhance their personal status and organizational budgets, or even from the influence and dominance of “the military-industrial complex”; viz.: “Maintaining the empire and retaliating for the blowback from that empire keeps what President Eisenhower called the military-industrial complex fat and happy.” Or, in the same section:¶ In the nation’s capital, vested interests, such as the law enforcement bureaucracies . . . routinely take advantage of “crises”to satisfy parochial desires. Similarly, many corporations use crises to get pet projects— a.k.a. pork—funded by the government. And national security crises, because of people’s fears, are especially ripe opportunities to grab largesse. (Ibid., 182)¶ Thus, “bureaucratic-politics” theory, which once made several reputa- tions (such as those of Richard Neustadt, Morton Halperin, and Graham Allison) in defense-intellectual circles, and spawned an entire sub-industry within the field of international relations,5 is put into the service of dismissing putative security threats as imaginary. So, too, can a surprisingly cognate theory, “public choice,”6 which can be considered the right-wing analog of the “bureaucratic-politics” model, and is a preferred interpretation of governmental decision- making among libertarian observers. As Eland (2004, 203) summarizes:¶ Public-choice theory argues [that] the government itself can develop sepa- rate interests from its citizens. The government reflects the interests of powerful pressure groups and the interests of the bureaucracies and the bureaucrats in them. Although this problem occurs in both foreign and domestic policy, it may be more severe in foreign policy because citizens pay less attention to policies that affect them less directly.¶ There is, in this statement of public-choice theory, a certain ambiguity, and a certain degree of contradiction: Bureaucrats are supposedly, at the same time, subservient to societal interest groups and autonomous from society in general.¶ This journal has pioneered the argument that state autonomy is a likely consequence of the public’s ignorance of most areas of state activity (e.g., Somin 1998; DeCanio 2000a, 2000b, 2006, 2007; Ravenal 2000a). But state autonomy does not necessarily mean that bureaucrats substitute their own interests for those of what could be called the “national society” that they ostensibly serve. I have argued (Ravenal 2000a) that, precisely because of the public-ignorance and elite-expertise factors, and especially because the opportunities—at least for bureaucrats (a few notable post-government lobbyist cases nonwithstanding)—for lucrative self-dealing are stringently fewer in the defense and diplomatic areas of government than they are in some of the contract-dispensing and more under-the-radar-screen agencies of government, the “public-choice” imputation of self-dealing, rather than working toward the national interest (which, however may not be synonymous with the interests, perceived or expressed, of citizens!) is less likely to hold. In short, state autonomy is likely to mean, in the derivation of foreign policy, that “state elites” are using rational judgment, in insulation from self-promoting interest groups—about what strategies, forces, and weapons are required for national defense.¶ Ironically, “public choice”—not even a species of economics, but rather a kind of political interpretation—is not even about “public” choice, since, like the bureaucratic-politics model, it repudiates the very notion that bureaucrats make truly “public” choices; rather, they are held, axiomatically, to exhibit “rent-seeking” behavior, wherein they abuse their public positions in order to amass private gains, or at least to build personal empires within their ostensibly official niches. Such sub- rational models actually explain very little of what they purport to observe. Of course, there is some truth in them, regarding the “behavior” of some people, at some times, in some circumstances, under some conditions of incentive and motivation. But the factors that they posit operate mostly as constraints on the otherwise rational optimization of objectives that, if for no other reason than the playing out of official roles, transcends merely personal or parochial imperatives.¶ My treatment of “role” differs from that of the bureaucratic-politics theorists, whose model of the derivation of foreign policy depends heavily, and acknowledgedly, on a narrow and specific identification of the role- playing of organizationally situated individuals in a partly conflictual “pulling and hauling” process that “results in” some policy outcome. Even here, bureaucratic-politics theorists Graham Allison and Philip Zelikow (1999, 311) allow that “some players are not able to articulate [sic] the governmental politics game because their conception of their job does not legitimate such activity.” This is a crucial admission, and one that points— empirically—to the need for a broader and generic treatment of role.¶ Roles (all theorists state) give rise to “expectations” of performance. My point is that **virtually every governmental role, and especially national-security roles**, **and particularly the roles of the uniformed mili- tary, embody** expectations of devotion to the “national interest”; rational- ity in the derivation of policy at every functional level; and **objectivity in the treatment of parameters, especially external parameters such as “threats” and the power and capabilities of other nations.**¶ **Sub-rational models** (such as “public choice”) **fail** **to take into account even a partial dedication to the “national” interest** (**or even the possibility that the national interest may be honestly misconceived in more paro- chial terms). In contrast, an official’s role connects the individual to the (state-level) process, and moderates the** (perhaps otherwise) **self-seeking impulses of the individual. Role-derived behavior tends to be formalized and codified; relatively transparent and at least peer-reviewed, so as to be consistent with expectations; surviving the particular individual and trans- mitted to successors and ancillaries; measured against a standard and thus corrigible; defined in terms of the performed function and therefore derived from the state function; and uncorrrupt, because personal cheating and even egregious aggrandizement are conspicuously discouraged**.¶ My own direct observation suggests that **defense decision-makers attempt to “frame” the structure of the problems that they try to solve on the basis of the most accurate intelligence. They make it their business to know where the threats come from. Thus, threats are not “socially constructed”** (even though, of course, some values are).¶ **A major reason for the rationality, and the objectivity, of the process is that much security planning is done, not in vaguely undefined circum- stances that offer scope for idiosyncratic, subjective behavior, but rather in structured and reviewed organizational frameworks. Non-rationalities (which are bad for understanding and prediction) tend to get filtered out. People are fired for presenting skewed analysis and for making bad predictions. This is because something important is riding on the causal analysis and the contingent prediction.** For these reasons, “**public choice” does not have the “feel” of reality to many critics who have participated in the structure of defense decision-making. In that structure**, obvious, and even not-so-obvious, **“rent-seeking” would not only be shameful; it would present a severe risk of career termination.** And, as mentioned**, the defense bureaucracy is hardly a productive place for truly talented rent-seekers to operate, compared to opportunities for personal profit in the commercial world. A bureaucrat’s very self-placement in these reaches of government testi- fies either to a sincere commitment to the national interest or to a lack of sufficient imagination to exploit opportunities for personal profit.**

#### Science and reason are good – key to progressive politics and stopping oppression – turns the K.

Alan **Sokal**, Professor of Physics at New York University, **1996** (“A Plea for Reason, Evidence and Logic,” Talk Presented at a Forum at New York University, October 26th, Available Online at http://www.physics.nyu.edu/faculty/sokal/nyu\_forum.html, Accessed 07-31-2010)

I didn't write the parody for the reasons you might at first think. My aim wasn't to defend science from the barbarian hordes of lit crit or sociology. I know perfectly well that the main threats to science nowadays come from budget-cutting politicians and corporate executives, not from a handful of postmodernist academics. Rather, **my goal is to defend** what one might call **a scientific worldview -- defined broadly as a respect for evidence and logic, and for the incessant confrontation of theories with the real world**; in short, **for reasoned argument over wishful thinking, superstition and demagoguery**. And my motives for trying to defend these old-fashioned ideas are basically political. I'm worried about **trends in the American Left** -- particularly here in academia -- that at a minimum **divert us from the task of formulating a progressive social critique, by leading smart and committed people into trendy but ultimately empty intellectual fashions**, and **that can in fact undermine the prospects for such a critique, by promoting subjectivist and relativist philosophies that** in my view **are inconsistent with producing a realistic analysis of society** that we and our fellow citizens will find compelling. David Whiteis, in a recent article, said it well: **Too many academics, secure in their ivory towers and insulated from the real-world consequences of the ideas they espouse, seem blind to the fact that non-rationality has historically been among the most powerful weapons in the ideological arsenals of oppressors**. The hypersubjectivity that characterizes postmodernism is a perfect case in point: far from being a legacy of leftist iconoclasm, as some of its advocates so disingenuously claim, it in fact ... plays perfectly into the anti-rationalist -- really, anti-thinking -- bias that currently infects "mainstream" U.S. culture. Along similar lines, the philosopher of science Larry Laudan observed caustically that **the displacement of the idea that facts and evidence matter by the idea that everything boils down to subjective interests and perspectives is** -- second only to American political campaigns -- **the most prominent and pernicious manifestation of anti-intellectualism in our time**.

#### Neolib’s inevitable and movements are getting smothered out of existence—no alternative economic system

**Jones 11**—Owen, Masters at Oxford, named one of the Daily Telegraph's 'Top 100 Most Influential People on the Left' for 2011, author of "Chavs: The Demonization of the Working Class", The Independent, UK, "Owen Jones: Protest without politics will change nothing", 2011, www.independent.co.uk/opinion/commentators/owen-jones-protest-without-politics-will-change-nothing-2373612.html

My first experience of police kettling was aged 16. It was May Day 2001, and the anti-globalisation movement was at its peak. The turn-of-the-century anti-capitalist movement feels largely forgotten today, but it was a big deal at the time. To a left-wing teenager growing up in an age of unchallenged neo-liberal triumphalism, just to have "anti-capitalism" flash up in the headlines was thrilling. Thousands of apparently unstoppable protesters chased the world's rulers from IMF to World Bank summits – from Seattle to Prague to Genoa – and the authorities were rattled. **Today, as protesters in nearly a thousand cities across the world follow the example set by** the **Occupy** Wall Street protests, **it's worth pondering what happened to the anti-globalisation movement**. Its **activists did not lack passion or determination. But they did lack a coherent alternative to the neo-liberal project.** **With no clear political direction, the movement was easily swept away by** the **jingoism and turmoil that followed 9/11,** just two months after Genoa. Don't get me wrong: the Occupy movement is a glimmer of sanity amid today's economic madness. By descending on the West's financial epicentres, it reminds us of how a crisis caused by the banks (a sentence that needs to be repeated until it becomes a cliché) has been cynically transformed into a crisis of public spending. The founding statement of Occupy London puts it succinctly: "We refuse to pay for the banks' crisis." The Occupiers direct their fire at the top 1 per cent, and rightly so – as US billionaire Warren Buffett confessed: "There's class warfare, all right, but it's my class, the rich class, that's making war, and we're winning." The Occupy movement has provoked fury from senior US Republicans such as Presidential contender Herman Cain who – predictably – labelled it "anti-American". They're right to be worried: those camping outside banks threaten to refocus attention on the real villains, and to act as a catalyst for wider dissent. **But a coherent alternative to the tottering global economic order remains, it seems, as distant as ever. Neo-liberalism crashes around, half-dead, with no-one to administer the killer blow.** There's always a presumption that a crisis of capitalism is good news for the left. Yet in the Great Depression, fascism consumed much of Europe. The economic crisis of the 1970s did lead to a resurgence of radicalism on both left and right. But, spearheaded by Thatcherism and Reaganism, the New Right definitively crushed its opposition in the 1980s.**This time round, there doesn't even seem to be an alternative for the right to defeat**. That's not the fault of the protesters. In truth, **the left has never recovered from being virtually smothered out of existence**. **It was the victim of a perfect storm: the rise of the New Right; neo-liberal globalisation; and the** repeated **defeats suffered by the trade union movement.** But, above all, it was the aftermath of the collapse of Communism that did for the left**. As US neo-conservative** Midge **Decter triumphantly put it: "It's time to say: We've won. Goodbye**." From the British Labour Party to the African National Congress, left-wing movements across the world hurtled to the right in an almost synchronised fashion. **It was as though the left wing of the global political spectrum had been sliced off. That's why**, **although we live in an age of revolt, there remains no left to give it direction and purpose.**

#### Neolib solves war and the alt’s collapse causes it – historical evidence and studies prove

Tures ‘3 – Associate Professor of Political Science @ LaGrange College

John A. Tures, Associate Professor of Political Science at LaGrange College, 2003, “ECONOMIC FREEDOM AND CONFLICT REDUCTION: EVIDENCE FROM THE 1970S, 1980S, AND 1990S”, Cato Journal, Vol. 22, No. 3. http://www.cato.org/pubs/journal/cj22n3/cj22n3-9.pdf

**The last three decades have witnessed an unprecedented expansion of market-based reforms and the profusion of economic freedom in the international system**. This shift in economic policy has sparked a debate about whether free markets are superior to state controls. Numerous studies have compared the neoliberal and statist policies on issues of production capacity, economic growth, commercial vol- umes, and egalitarianism. An overlooked research agenda, however, is the relationship between levels of economic freedom and violence within countries. Proponents of the statist approach might note that a strong gov- ernment can bend the market to its will, directing activity toward policies necessary to achieve greater levels of gross domestic product and growth. By extracting more resources for the economy, a pow- erful state can redistribute benefits to keep the populace happy. Higher taxes can also pay for an army and police force that intimidate people. Such governments range from command economies of totali- tarian systems to autocratic dictators and military juntas. Other eco- nomically unfree systems include some of the authoritarian “Asian tigers.” **A combination of historical evidence, modern theorists, and statis- tical findings, however, has indicated that a reduced role for the state in regulating economic transactions is associated with a decrease in internal conflicts. Countries where the government dominates the commercial realm experience an increase in the level of domestic violence. Scholars have traced the history of revolutions to explain the relationship between statism and internal upheavals. Contemporary authors also posit a relationship between economic liberty and peace. Statistical tests show a strong connection between economic freedom and conflict reduction during the past three decades**.

#### Rejecting security allows private forces to fill in the security vacuum left by the state resulting in more violent forms of securitization

Loader and Walker 07<Ian and Neil, professor of criminology and Director of the center for Criminology at Oxford Professor of European Law European University Institute Florence , *Civilizing Security*, pg 22-25)

**Today it cannot be assumed that the state remains pre-eminent in either authorizing or delivering** policing and **security**. **Other non-state actors now lay claim to authority and competence in this field**. In defence of the contention that what Johnston and Shearing (2003) call the ‘governance of security’ is conducted by a multiplicity of institutions, one can point to the following: • **Private security has become big business across the world.** In Britain, the USA, Canada, South Africa and beyond it has long been acknowledged that those employed by commercial security outfits outstrip the total number of public police officers. Private security operatives are hired by corporations, national and local governments, and private citizens to guard office complexes, airports, universities, housing estates, schools, hospitals, shopping centres, civic buildings, courts, even police stations. People’s access to, and conduct within, large tracts of urban space is regulated by private security guards, employed by commercial companies, enforcing property rather than criminal law. Such guards also, in some settings, engage in ‘front-line’ law enforcement and order maintenance policework (Rigakos 2002). 1 Anxious citizens, in turn, rely on the security market for an array of protective hardware (alarms, gates, locks, CCTV systems), as well as resorting to forms of self-policing — often encouraged by insurance companies and neo-liberal governments. Some have formed ‘private residential associations’ or sought security inside ‘gated communities’, withdrawing their demand and support for public provision (including policing provision) in the process. In response, the public police increasingly act as market players, contracting-out non-core ‘business’, eliciting corporate sponsorship, and marketing or even selling their services to a public disaggregated into individual ‘customers’. • **All this is happening in societies with strong, established states**. In those with weak or failing states, or undergoing political transition, the public police are not the only or main security actor, nor can they lay claim to a monopoly over legitimate force inside their territory. **Across many parts of the globe today** — in Italy, Colombia, Brazil, Northern Ireland, Russia, Afghanistan, the impacted ghettos of US and European cities **one finds alternative power centres contesting state authority, ‘shadow sovereigns’** (Nordstrom 2000) operating their own codes of behaviour and mechanisms of enforcement (Gambetta 1993; Varese 2001). In these contexts, those who can afford to have, once more, fled behind walls, venturing from their residential enclosures only to make passage to other protected work and leisure domains. **The dispossessed by contrast are left at the mercy not only of militarized, partisan police forces, but also criminal gangs, hired ‘rent-a-cops’ and urban vigilantes.** Alternatively, in some isolated pockets parts of South Africa and Argentina for instance — poor communities are striving to put in place non-violent, local capacity-building forms of non-state security governance. • Nor are these developments confined within the borders of modern states. ‘**Security’ has also become a multinational business, one that crosses territorial boundaries and further erodes the internal/external security distinction.** Several private security enterprises now trade their wares across the globe (Johnston 2006). They sell security advice, equipment and personnel to anxious citizens and warring factions in weak and failed states. They claim to be filling the ‘security gaps’ left by the fall of communist rule in the former Soviet Union and eastern Europe. And they offer to serve and protect the interests of multinationals operating in disordered, crime-ridden locations. To this, one can add the ‘privatization of violence’ occurring in many conflict and post-conflict zones around the world, as ‘private military firms’ such as MPRI and Dyncorp — dubbed by Peter Singer (2003) ‘corporate warriors’ — promote and sell military ‘know-how’, equipment and intervention to beleaguered governments and other armed groups (Avant 2005). It is a telling symbol of these trends that one of the fastest-growing industries in post- invasion Iraq is private security. **These examples** too we will flesh out in more detail below. What they serve for the moment to **illustrate** is **the existence of a pluralized — market-driven — environment where the state exists alongside, sponsors and competes against a plethora of non-state actors in a bid to promise security to citizens**. It is a field where the state is not only less and less involved in delivering policing and security on the ground — what Osborne and Gaebler (1992) call ‘rowing’ — but also often lacks the effective regulatory capacity to ‘steer’. It is a field constituted by new sites of rule and authority beyond the state, one where market power or communal ordering escapes from the forms of public will- formation that only the democratic state can supply. **Against this backdrop, the project of civilizing security is faced not only** (or even mainly) **with the task of controlling the arbitrary, discriminatory exercise of sovereign force, or with the excesses of state power. It is confronted, rather more, with a notable absence of political institutions with the capacity and legitimacy required to prevent those with ‘the loudest voices and the largest pockets’** (Johnston and Shearing 2003: 144) **from organizing their own ‘security’ in ways that impose unjustifiable burdens of insecurity upon others**. Or, to put the same point more widely: **These days, the main obstacle to social justice is not the invasive intentions or proclivities of the state, but its growing impotence,** aided and abetted daily by the officially adopted ‘there is no alternative’ creed. I suppose that **the danger we will have to fight back in the coming century won’t be totalitarian coercion, the main preoccupation of the century just ended, but the falling apart of ‘totalities’ capable of securing the autonomy of human society.** (Bauman and Tester 2001: 139)

#### The alt results in more securitization and intervention

Tara McCormack, 2010, is Lecturer in International Politics at the University of Leicester and has a PhD in International Relations from the University of Westminster. 2010, (Critique, Security and Power: The political limits to emancipatory approaches, page 127-129)

The following section will briefly raise some questions about the rejection of the old security framework as it has been taken up by the most powerful institutions and states. Here we can begin to see the political limits to critical and emancipatory frameworks. In an international system which is marked by great power inequalities between states, the **rejection of the** old narrow national interest-based **security framework** by major international institutions, and the adoption of ostensibly emancipatory policies and policy rhetoric, **has the consequence of problematising weak or unstable states and allowing international institutions or major states a more interventionary role, yet without establishing mechanisms by which the citizens of states being intervened in might have any control over the agents or agencies of their emancipation**. Whatever the problems associated with the pluralist security framework **there were at least formal and clear demarcations. This has the consequence of entrenching international power inequalities and allowing for a shift towards a hierarchical international order in which the citizens in weak or unstable states may arguably have even less freedom or power than before**. Radical critics of contemporary security policies, such as human security and humanitarian intervention, argue that we see an assertion of Western power and the creation of liberal subjectivities in the developing world. For example, see Mark Duffield’s important and insightful contribution to the ongoing debates about contemporary international security and development. Duffield attempts to provide a coherent empirical engagement with, and theoretical explanation of, these shifts. Whilst these shifts, away from a focus on state security, and the so-called merging of security and development are often portrayed as positive and progressive shifts that have come about because of the end of the Cold War, Duffield argues convincingly that these shifts are highly problematic and unprogressive. For example, the rejection of sovereignty as formal international equality and a presumption of nonintervention has eroded the division between the international and domestic spheres and led to an international environment in which Western NGOs and powerful states have a major role in the governance of third world states. Whilst for supporters of humanitarian intervention this is a good development, Duffield points out the depoliticising implications, drawing on examples in Mozambique and Afghanistan. Duffield also draws out the problems of the retreat from modernisation that is represented by sustainable development. The Western world has moved away from the development policies of the Cold War, which aimed to develop third world states industrially. Duffield describes this in terms of a new division of human life into uninsured and insured life. Whilst we in the West are ‘insured’ – that is we no longer have to be entirely self-reliant, we have welfare systems, a modern division of labour and so on – sustainable development aims to teach populations in poor states how to survive in the absence of any of this. **Third world populations must be taught to be self-reliant, they will remain uninsured. Self-reliance of course means the condemnation of millions to a barbarous life of inhuman bare survival.** Ironically, although sustainable development is celebrated by many on the left today, by leaving people to fend for themselves rather than developing a society wide system which can support people, sustainable development actually leads to a less human and humane system than that developed in modern capitalist states. Duffield also describes how many of these problematic shifts are embodied in the contemporary concept of human security. For Duffield, we can understand these shifts in terms of Foucauldian biopolitical framework, which can be understood as a regulatory power that seeks to support life through intervening in the biological, social and economic processes that constitute a human population (2007: 16). Sustainable development and human security are for Duffield technologies of security which aim to *create* self-managing and self-reliant subjectivities in the third world, which can then survive in a situation of serious underdevelopment (or being uninsured as Duffield terms it) without causing security problems for the developed world. For Duffield this is all driven by a neoliberal project which seeks to control and manage uninsured populations globally. Radical critic Costas Douzinas (2007) also criticises new forms of cosmopolitanism such as human rights and interventions for human rights as a triumph of American hegemony. Whilst we are in agreement with critics such as Douzinas and Duffield that **these new security frameworks cannot be empowering, and ultimately lead to more power for powerful states,** we need to understand why these frameworks have the effect that they do. We can understand that these frameworks have political limitations without having to look for a specific plan on the part of current powerful states. **In new security frameworks such as human security we can see the political limits of the framework proposed by critical and emancipatory theoretical approaches**.

#### Security sustains a form of democratic citizenship necessary to enhance standards of living and ensure rights

Loader and Walker 07<Ian and Neil, professor of criminology and Director of the center for Criminology at Oxford Professor of European Law European University Institute Florence , *Civilizing Security*, pg 7-8)

By invoking this phrase we have in mind two ideas, both of which we develop in the course of the book. The first, which is relatively familiar if not uncontroversial, is that security needs civilizing. States — even those that claim with some justification to be ‘liberal’ or ‘democratic’ — have a capacity when self-consciously pursuing a condition called ‘security’ to act in a fashion injurious to it. So too do non-state ‘security’ actors, a point we return to below and throughout the book. They proceed in ways that trample over the basic liberties of citizens; that forge security for some groups while imposing illegitimate burdens of insecurity upon others, or that extend the coercive reach of the state — and security discourse — over social and political life. As monopoly holders of the means of legitimate physical and symbolic violence, modern states possess a built-in, paradoxical tendency to undermine the very liberties and security they are constituted to protect. Under conditions of fear such as obtain across many parts of the globe today, states and their police forces are prone to deploying their power in precisely such uncivil, insecurity- instilling ways. If the state is to perform the ordering and solidarity- nourishing work that we argue is vital to the production of secure political communities then it must, consequently, be connected to forms of discursive contestation, democratic scrutiny and constitutional control. The state is a great civilizing force, a necessary and virtuous component of the good society. But if it is to take on this role, the state must itself be civilized — made safe by and for democracy. But our title also has another; less familiar meaning — the idea that **security is civilizing. Individuals who live, objectively or subjectively, in a state of anxiety do not make good democratic citizens**, as European theorists reflecting upon the dark days of the 1930s and 1940s knew well (Neumann 1957). **Fearful citizens tend to be inattentive to, unconcerned about, even enthusiasts for; the erosion of basic freedoms. They often lack openness or sympathy towards others, especially those they apprehend as posing a danger to them.** They privilege the known over the unknown, us over them, here over there. They often retreat from public life, seeking refuge in private security ‘solutions’ while at the same time screaming anxiously and angrily from the sidelines for the firm hand of authority — for tough ‘security’ measures against crime, or disorder, or terror. **Prolonged episodes of violence, in particular, can erode or destroy people’s will and capacity to exercise political judgement and act in solidarity with others** (Keane 2004: 122—3). **Fear, in all these ways, is the breeding ground, as well as the stock-in-trade, of authoritarian, uncivil government.** But there is more to it than that. Security is also civilizing in a further, more positive sense. **Security**, we shall argue, is **in a sociological sense a ‘thick’ public good, one whose production has irreducibly social dimensions, a good that helps to constitute the very idea of ‘public- ness’**. Security, in other words, is simultaneously the producer and product of forms of trust and abstract solidarity between intimates and strangers that are prerequisite to democratic political communities. The state, moreover; performs vital cultural and ordering work in fashioning the good of security conceived of in this sense. **It can**, under the right conditions, **create inclusive communities of practice and attachment, while ensuring that these remain rights-regarding, diversity- respecting entities.** In a world where the state’s pre-eminence in governing security is being questioned by private-sector interests, practices of local communal ordering and transnational policing networks, the constitution of old- and new-fashioned forms of democratic political authority is, we shall argue, indispensable to cultivating and sustaining the civilizing effects of security.

# 1AR

## Kritik

#### Fear can be channeled and productive – suppressing it causes panic

Sandman and Lanard, 2003

Peter M. PhD in Communications and Professor at Rutgers specializing in crisis communication; Jody, Psychiatrist, 28 April, “Fear Is Spreading Faster than SARS — And So It Should!”

8.   **Stop worrying excessively about panic.   Panic is rare**. It is less rare during life-threatening epidemics than in most other sorts of crises, so you can’t afford to ignore the possibility altogether. But remember that **efforts to avert panic** — for example, **by withholding bad news and making over-reassuring statements — tend to backfire**. People often disobey in a crisis, or an impending crisis. But that’s not panic. **Worry more about denial; worry more about apathy; don’t worry just about panic.** 9.   Worry less about the public’s fear.   Of course **excessive fear can paralyze people**, or lead them to unwise, desperate attempts at self-protection. **But insufficient fear provokes insufficient self-protection ... and insufficient efforts to protect the rest of the community,** and insufficient support for the policy changes and public expenditures that may be needed. **So guide people’s fear. Harness it.** Channel it. Titrate it. Don’t try to squelch it. **Somewhere midway between apathy and panic is the level of emotional arousal that’s right for a serious emergency. It’s more than concern, less than terror. Call it “fear” — and welcome it.**

#### Fear is inevitable and productive – when people are afraid, they take steps to protect themselves. Denying fear causes it to turn into denial or panic.

Sandman and Lanard 2003

Peter M. PhD in Communications and Professor at Rutgers specialzing in crisis communication; Jody, Psychiatrist, Sept 7, “Fear of fear”

Let’s start with the obvious. **Any normal person is going to be more anxious than usual while awaiting a biopsy result,** a turbulent airplane landing, or a layoff notice. **Human emotions tend to match the situation.** **The same is true of a more widespread threat.** Of course the public at large will be commensurately alarmed when told that a terrorism attack, an epidemic, or a hurricane may be approaching. Moreover, **fear isn’t just normal in frightening situations; it is functional**. Both the human body and the body politic ultimately benefit from the changes (physiological and sociological ... and inevitably emotional) that accompany preparedness for crisis. Take terrorism as a case in point. Nearly everyone agrees that we need people to be vigilant for indications of terrorist attacks; to prepare themselves and their families to cope with possible attacks; to be supportive of preparedness expenses and tolerant of preparedness inconveniences. And nearly everyone agrees that we need all this to ramp up in an actual attack, so that people put other agendas on hold, follow instructions willingly, and help care for their neighbors. The question is what emotional state, what state of mind, is conducive to this sort of public readiness. We believe the right answer is fear. **We won’t get there if terrorism is merely one of many issues people are “concerned” about, along with West Nile Virus and inflation and rap lyrics. Either** terrorism is different **from most other concerns, or it isn’t. If it is, we need to get used to the idea that people are going to be appropriately frightened,** and we need to help them get used to it too. Not all fear is functional. **Fear that is paralyzing**, fear that verges on panic**, is obviously not functional. Terror is the goal of terrorism, not the goal of preparedness. But fear is not necessarily terror. This is a conceptual mistake officials routinely make**, a mistake they seem terribly attracted to — **the embedded, preconscious, erroneous assumption that all fear is one short step removed from panic**. Some fear is. Most fear is not. When officials express their reluctance about “unduly frightening people,” they are literally right. The key word here is “unduly.” **Unduly frightening people is wrong. Duly frightening people is right,** and important. The problem is telling the two apart. The distinction is partly a matter of degree — “enough” fear versus “excessive” fear. Perhaps in addition there are kinds of fear like the kinds of cholesterol — “good” fear versus “bad” fear. But we suspect **the key difference is neither the amount of fear nor the kind of fear, but rather people’s ability to bear the fear. Much is known about how to enhance that ability**. Among the things that help: **Give people things to do — action binds anxiety. Give people things to decide — decision-making provides more individual control**, which makes fear more tolerable. **Encourage appropriate anger** — the desire to get even often trumps the desire to cower. **Encourage love (and camaraderie**) — soldiers, for example, fight for their friends and for their country. **Provide candid leadership — we get more frightened when our leaders seem to be misleading us. Show your own fear and show you can bear it** — apparently fearless leaders are little help to a fearful public. Most importantly, **treat other people’s fear as legitimate. Fear is likeliest to escalate into terror or panic (or to flip into denial) when it is treated as shameful and wrong**. “It’s natural to be afraid, I’m afraid too” is a much more empathic response to public fear than “there’s nothing to be afraid of.” If we want people to bear their fear, we must assure them that their fear is appropriate. Even fear that is statistically inappropriate can and should be legitimized as normal, understandable, and widespread. **Leaders who are contemptuous of people’s fear have a much tougher time explaining the reasons why they needn’t be afraid.**

#### Meta-analyses of fear literature prove the stronger the fear appeal the stronger likelihood of behavior change

**Witte and Allen ’00**

Department of Communication, Michigan State University. And Department of Communication, University of Wisconsin–Milwaukee, respectively [Kim Witte and Mike Allen, “A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns,” Health Educ Behav 2000, 27: 591 p. 595]

At least **three meta-analyses have been conducted on the fear appeal literature**. **Boster and Mongeau8 and Mongeau9** examined the influence of a fear appeal on perceived fear (the manipulation check; i.e., did the strong vs. weak fear appeals differ significantly in their influence on measures of reported fear), attitudes, and behaviors. They **found** that on average, **fear appeal manipulations** **produced** moderate associations between reported fear and strength of fear appeal (r = .36 in Boster and Mongeau and r = .34 in Mongeau) and modest but reliable **relationships between the strength of a fear appeal and attitude change** (r = .21 in Boster and Mongeau and r = .20 in Mongeau) **and the strength of a fear appeal and behavior change** (r = .10 in Boster and Mongeau and r = .17 in Mongeau). **Sutton**7 used a different meta-analytic statistical method (z scores) and **reported signifi- cant positive effects for strength of fear appeal on intentions and behaviors.** None of the meta-analyses found support for a curvilinear association between fear appeal strength and message acceptance. Overall, the previous meta-analyses suggested that fear appeal manipulations work in producing different levels of fear according to different strengths of fear appeal messages. Furthermore, **the meta-analyses suggest that the stronger the fear appeal, the greater the attitude, intention, and behavior change**.

The present meta-analysis will update and expand on these results by assessing the rel- ative fit of the data to each fear appeal model and examining the influence of fear appeals on both intended (i.e., attitudes, intentions, behaviors) and unintended (i.e., defensive avoidance, reactance) outcomes.

#### A positive, linear relationship between strength of fear appeal persuasion exists

**Witte and Allen ’00**

Department of Communication, Michigan State University. And Department of Communication, University of Wisconsin–Milwaukee, respectively [Kim Witte and Mike Allen, “A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns,” Health Educ Behav 2000, 27: 591 p. 601-2]

**Consistent with previous meta-analyses, this study suggests that the stronger the** fear aroused by a **fear appeal, the more persuasive it is.** For example, the fear manipulation-attitude correlation was .21 in Boster and Mongeau,8 .20 in Mongeau,9 and .14 in this study (Sutton’s study used a different type of analysis with a combined z score that is not comparable to the correlation7). Similarly, **we found a correlation between the fear manipulation and behavior** at .15, compared with Boster and Mongeau’s .10 and Mongeau’s .17. While Boster and Mongeau did not assess the influence of fear manipula- tion on intentions, our study indicates that the relationship is within the range of the other danger control responses at .11. Overall, fear appears to have a relatively weak but reli- able effect on attitudes, intentions, and behaviors. The differences between the findings of our meta-analysis and the previous meta-analyses may be accounted for by the more con- sistent and careful operationalizations of attitudes and behaviors in recent studies. For example, the early studies measured attitudes in a wide variety of ways. These measures may not have been comparable, and some attitude measures may actually have measured intentions. More recent research has consistently defined attitudes as evaluations of cer- tain behaviors, intentions as one’s intentions to perform a certain behavior, and behaviors as self-report indicators of the degree to which one did what the recommended response advocated. It is interesting to note that **in this meta-analysis, the effects of the fear manip- ulation on attitudes, intentions, and behaviors were relatively consistent** (i.e., .14, .11, .15, respectively).

**Destroys the alt**

**Levinas 85**

Emmanuel Levinas, professor of philosophy, and Philippe Nemo, professor of new philosophy, Ethics and Infinity, ‘85, pg. 6-7

Are we not in need of still more precautions**? Must we not step back from this question to raise another, to recognize the obvious circularity of ask­ing what is**the “What is . .?“ question? It seems to beg the question. Is our new suspicion, then, that **Heidegger begs the question of metaphysics when he asks “What is poetry?” or “What is thinking?”? Yet his thought is insistently anti-metaphysical**. **Why, then, does he retain the metaphysical question par excellence?** Aware of just such an objection, he pro­poses, against the vicious circle of the *petitio principi,* an alternative, productive circularity: hermeneutic questioning. **To ask “What is.** . .?“ does not partake of onto-theo-logy if one **acknowledges** (1) **that the answer can never be** fixed absolutely, **but** calls **essen­tially**, **endlessly**, for additional “What is . . .?“ ques­tions. Dialectical refinement here replaces vicious circularity. **Further**, beyond **the** openmindedness called for by dialectical refinement, hermeneutic **questioning** (2) **insists on avoiding subjective impositions**, on avoid­ing reading into rather than harkening to things. **One must harken to the things themselves**, ultimately to being, in a careful attunement to what is. But do the refinement and care of the herme­neutic question — which succeed in avoiding onto­theo-logy succeed in avoiding all viciousness? Certainly they convert a simple fallacy into a produc­tive inquiry, they open a path for thought. **But is it not the case that however much refinement and care one brings to bear, to ask what something is leads to asking what something else is, and so on and so forth, ad infinitum***?* What is disturbing in this is not so much the infinity of interpretive depth, which has the virtue of escaping onto-theo-logy and remaining true to the way things are, to the phenomena, **the coming to be and passing away of being. Rather, the problem lies in the influence the endlessly open horizon of such thinking exerts on the way of such thought. That is, the problem lies in what seems to be the very virtue of hermeneutic thought, namely, the doggedness of the “What is . . .?“ question, in its inability to escape itself, to escape being and essence**.