### Plan

**The United States federal government should substantially increase statutory restrictions on the war powers authority of the president of the United States by statutorily removing the President’s authority to authorize the preemptive use of large-scale cyber-attacks.**

### Advantage – Cyber War

#### The first internal link is arms racing ---

#### Squo offensive cyber posture 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.”

#### It goes nuclear due to command and control hacking, crisis instability, and fracturing nuclear agreements - congressional restrictions are key to solve

Austin, 8/6

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

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

#### Plan solves - 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.

#### Second internal link is preemption ---

#### The US preparing to initiate a preemptive cyberwar now

Martin ‘13

[Patrick, Global Research. <http://www.globalresearch.ca/obamas-cyberwarfare-first-strike-using-offensive-cyber-effects-operations-oceo-to-destabilize-countries/5338457> ETB]

The US government is developing detailed plans to attack other countries using cyberwarfare techniques, according to a report Friday in the British daily newspaper Guardian. President Obama gave the orders to plan for cyber attacks, including preemptive strikes by the US, **in** **a**n 18-page **directive** issued last October and **leaked to the newspaper**, which published it on its web site. Presidential Policy Directive 20 defines Offensive Cyber Effects Operations (OCEO), which “can offer unique and unconventional capabilities to advance US national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging.”¶ It continues:¶ “The United States government shall identify potential targets of national importance where OCEO can offer favorable balance of effectiveness and risk as compared with other instruments of national power.”¶ The directive instructs the secretary of defense, the director of national intelligence, and the director of the CIA to “prepare for approval by the president through the National Security Advisor a plan that identifies potential systems, processes and infrastructure against which the United States should establish and maintain OCEO capabilities.” Since the deadline for this action is six months after the approval of the directive, which came in October, this plan has presumably already been developed and submitted to the National Security Council.¶ In relation to foreign targets of cyberwarfare, the directive authorizes actions by US government agencies in circumstances where the identity and nationality of the “adversary” are uncertain. The US government “shall make all reasonable efforts, under circumstances prevailing at the time, to identify the adversary and the ownership and geographic location of the targets and related infrastructure where DCEO or OCEO will be conducted or cyber effects are expected to occur.”¶ Translated into plain language, this means that a US government attack on alleged hackers could target a foreign government or military without definitively identifying them as the source of the hacking. In recent months, the Obama administration and US media, spearheaded by the New York Times, have hyped the threat of Chinese hackers, supposedly organized through a Chinese military office in Shanghai, without providing any actual proof of the linkage.¶ As one of its intelligence sources told the Guardian, US complaints about Chinese cyberwarfare efforts were hypocritical: “We hack everyone everywhere. We like to make a distinction between us and the others. But we are in almost every country in the world.”¶ The directive acknowledges that cyber-warfare efforts by the US government may produce “potential unintended or collateral consequences,” not only within the targeted countries, but worldwide and in the US itself. These consequences could include “loss of life, significant responsive actions against the United States, significant damage to property, serious adverse US foreign policy consequences, or serious economic impact on the United States.” The directiveessentiallyreiterates the doctrine of preventive warfare, enunciated by George W. Bush in 2002 in the run-up to the invasion of Iraq. Bush declared that the United States had the right to attack other countries, not merely to preempt an impending attack, but to prevent any potential attack at any time in the future—a formula for unlimited worldwide aggression.

#### 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.”**

#### Third internal link is defense ---

#### 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.

**Overconcentration on offense is uniquely 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.

#### Escalation is rapid and global

VOA News ‘12

<http://blogs.voanews.com/digital-frontiers/2012/03/20/the-coming-cyberwar-with-iran/> ETB

That said, the battles might actually begin small. Think online skirmishes between angry bands of nationalist hackers, busting into systems and defacing websites, but doing no serious long-term damage. Or perhaps, says Matthew Aid, should Israel decide to strike Iranian targets, it might begin with online operations to knock out crucial defense systems, “…like the artillery barrage before the cavalry goes up the hill.” That, cautions professor Sean Lawson, would probably elicit a response from Iran, and soon after from allies like Hezbollah, Syria and possibly even North Korea. And if that were to happen, hacker havens like Russia, China and those in Europe and North America might soon join the fray. One genuine danger of cyberwar, says Lawson, is how quickly it could spread around the globe.

**We have an objective definition of war and expanding it causes miscalculation**

Hooker 2005

Commands the XVIII Airborne Corps Combat Support Brigade ("Dragon Brigade") now deployed to Iraq. He commanded an infantry battalion in the 82d Airborne Division and has served as Special Assistant to the Chairman of the Joint Chiefs, with the Office of the Chief of Staff of the Army, as Aide de Camp to the Secretary of the Army, and with the National Security Council. Colonel Hooker holds an M.S. in national security studies from the National Defense University and M.A. and Ph.D. degrees from the University of Virginia in international relations. "Beyond Vom Kriege: the character and conduct of modern war"

Clausewitz described war as "nothing more than a duel on a larger scale ... an act of force to compel the enemy to do our will." (2) Today, "war" is used to mean very different things in very different contexts, **from the war on poverty to** the war on drugs to the war on **terrorism. Because it evokes a call to action** and stimulates national resolve, "**war" is** perhaps **the most used and abused word** in the political lexicon. What does it mean precisely? **War is** surely both a duel and an act of force, but it is perhaps best described as **armed conflict between states**. While not inconsistent with Clausewitz, this usage lends both simplicity and clarity to often-muddied waters. Thus defined, **war can be distinguished from raids, rescue operations, peace-keeping** missions, counter-drug and anti-terror operations, military occupations, shows of force, **and a host of other activities** which involve the use of military forces. **Implicit in this usage is reciprocity**; an unanswered, one-time cruise missile attack is a military operation and a use of force, but hardly a war. However ineffectually, however great the mismatch, both sides must participate in the "duel" for war to exist. **Nor does official sanction particularly matter**. Whether formally declared or not, war is war. Nowadays, even advanced states routinely forego the diplomatic niceties, though all seek and welcome the imprimatur of international support and recognition when they can get it. Here, "**armed conflict" means fighting**--not a show of force or the threat of invasion, but actual combat. The difference is important because the many gradations of the use of "forces" are distinct from the use of "force." Fundamentally, war itself is not about deterrence or dissuasion, although the capability and the will to wage it may be. As Bedford Forrest so pungently put it, "War means fighting. And fighting means killing." **The distinction is crucial. The chance of stumbling into war is too great. All too often, states**men have **used the threat of war as a tool of policy, only to be astounded when it fails and war erupts.**

#### War fuels structural violence

Goldstein 2001

IR professor at American University (Joshua, War and Gender, p. 412, Google Books)

First, peace activists face a dilemma in thinking about causes of war and working for peace. **Many peace scholars and activists support the approach, “if you want peace, work for justice.”** Then, if one believes that sexism contributes to war, one can work for gender justice specifically (perhaps. among others) in order to pursue peace. This approach brings strategic allies to the peace movement (women, labor, minorities), but rests on the assumption that injustices cause war. The evidence in this book suggests that **causality runs at least as strongly the other way. War is not a product of capitalism, imperialism, gender, innate aggression,** or any other single cause, **although all of these influence wars’ outbreaks and outcomes. Rather, war has in part** fueled and sustained **these and other injustices**.9 So, “if you want peace, work for peace.” Indeed, if you want justice (gender and others), work for peace. **Causality does not run just upward through the levels of analysis, from types of individuals, societies, and governments up to war. It runs downward too**. Enloe suggests that changes in attitudes towards war and the military may be the most important way to “reverse women’s oppression.” The dilemma is that peace work focused on justice brings to the peace movement energy, allies, and moral grounding, yet, in light of this book’s evidence, **the emphasis on injustice as the main cause of war seems to be** empirically inadequate.

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

Bradley and Morrison ‘13

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

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

**Criticizing the probability of our impacts is meaningless – all wars are low probability, what matters is that cyberwar is more likely to escalate than other conflicts, which uniquely warrants academic attention**

**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.

**Understanding the risks of current US posture reduces the chances of cyber war escalation - worst case assessments are the best preparation**

**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 timerejecting ¶ thepremise that circumstances couldhappen someday that would ¶result inthe U.S. being on the edgeofconflict 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 understanding 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.

**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**

**Debate about the repercussions of cyber preemption is good - it generates a broader literature base that encourages restraint**

**Magnuson ‘9**

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

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

#### We should talk about cyber even if we don’t have our hands on the levers of power – the alternative is ceding decisionmaking power to elites

Singer 14

Interview with Peter Singer, director of the Center for 21st Century Security and Intelligence and a senior fellow in the Foreign Policy program at the Brookings Institution, 1/14/14, <http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/01/14/cybersecurity-and-cyberwar-a-qa-with-peter-singer/> SJE

Whether you are the president of the United States, of a large corporation, a small business, or your household (when actually your spouse and kids are the true commanders in chief), all of us make cybersecurity decisions that matter. The problem is that we are not well trained and equipped for these new responsibilities. For instance, 70 percent of business executives have made a cybersecurity decision of some sort for their firms, despite the fact that no major MBA program teaches it as part of normal management training. This gap is mirrored at the schools we teach our diplomats, lawyers, generals, journalists and so on. Indeed, handing off a crucial matter for only the “experts” to understand and handle is the best way to be taken advantage of, whether it is by a hacker accessing your bank account or by a spy agency that uses technical and legal doublespeak to haze what they are actually doing. In the book, we argue that it needs to stop being treated as just an area for computer science and better blended into the training for other fields. To put it another way, it is not a book just for the CompSci department, but for people in everything from international relations to law to business, much as cyberissues touch on all these fields.

**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.