# 1AC

### Plan

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

### Adv 1 - Preemption

#### Advantage 1 is Preemption

**Status quo offensive cyber operations by the US has set a precedent that is being modeled by other countries – leads to prolif and diffusion of cyber weapons to third parties**

**Gjelten 13**

(Tom Gjelten, correspondent for NPR, “Pentagon Goes On The Offensive Against Cyberattacks” February 11, 2013, <http://www.npr.org/2013/02/11/171677247/pentagon-goes-on-the-offensive-against-cyber-attacks>, KB)

With the Pentagon now officially recognizing cyberspace as a domain of warfare, **U.S. military commanders** are emphasizing their readiness to defend the nation against cyberthreats from abroad. What they do not say is that they **are** equally **prepared to launch their own cyberattacks against U.S. adversaries.**¶ The importance of plans for offensive cyberwar operations is obscured by the reluctance of the government to acknowledge them. When the Pentagon announced its "Strategy for Operating in Cyberspace" in July 2011, for example, it appeared the military was focused only on protecting its own computer networks, not on attacking anyone else's.¶ "The thrust of the strategy is defensive," declared William Lynn, the deputy secretary of defense at the time. Neither he nor other Pentagon officials had one word to say about possible offensive cyberattacks. The Pentagon would not favor the use of cyberspace "for hostile purposes," according to the strategy. "Establishing robust cyberdefenses no more militarizes cyberspace," Lynn said, "than having a navy militarizes the ocean."¶ Those assurances are deceptive. Behind the scenes, **U.S. commanders are committing vast resources and large numbers of military personnel to planning offensive cyberattacks** and, in at least some cases, actually carrying them out. But the secrecy surrounding offensive cyberwar planning means there has been almost no public discussion or debate over the legal, ethical and practical issues raised by waging war in cyberspace.¶ **Offensive cyberattacks carried out by the United States could set precedents other countries would follow.** **The rules of engagement for cyberwar are not** yet **clearly defined.** And **the lack of regulation concerning the development of cyberweapons could lead to a proliferation of lethal attack tools** — **and** even to the possibility that such **weapons could fall into the hands of unfriendly states, criminal organizations and** even **terrorist groups.**¶In some cases, offensive cyberattacks are being conducted within the parameters of conventional military operations. In Afghanistan, soldiers and Marines depend heavily on video and data links when they go into combat. As part of the process of "prepping the battlefield," commanders may want to launch pre-emptive attacks on the adversary's cybercapabilities in order to make sure their data networks do not get interrupted.¶ Marine Lt. Gen. Richard Mills, in a rare acknowledgment that the military engages in offensive cyber operations, discussed just such a situation during a military conference in August 2012.¶ "I can tell you that as a commander in Afghanistan in the year 2010, I was able to use my cyber operations against my adversary with great impact," Mills declared. "I was able to get inside his nets, infect his command and control, and in fact defend myself against his almost constant incursions to get inside my wire."¶ Another reference to the military's use of cyberattacks as part of a traditional combat operation came in 2009, during a presentation at the Brookings Institution by Air Force Gen. Norton Schwartz. Now retired, Schwartz at the time was serving as Air Force chief of staff. He told his audience that his airmen were prepared to carry out cyberattacks on another country's radar and missile installations before launching airstrikes against that country.¶ "Traditionally, we take down integrated air defenses via kinetic [physical] means," Schwartz said. "But if it were possible to interrupt radar systems or surface-to-air missile systems via cyber, that would be another very powerful tool in our tool kit." Schwartz hinted that the Air Force already had that capability, and in the nearly four years since he gave that speech, such a capability has certainly matured.¶ Cyberattacks, however, are also being used independently of traditional or kinetic operations, according to Jason Healey, a former Air Force officer who now directs the Cyber Statecraft Initiative at the Atlantic Council.¶ "It might happen that we will use them as an adjunct to kinetic," Healey says, "but it's quite clear that we're using [cyber] quite a bit more freely."¶ The best example of an offensive cyberattack independent of a kinetic operation would be Stuxnet, the cyberweapon secretly used to damage nuclear installations in Iran. A U.S. official has privately confirmed to NPR what the New York Times reported last summer — that the United States had a role in developing Stuxnet.¶ Because the operation has been shrouded in secrecy, however, there has been no public discussion about the pros and cons of using a cyberweapon in the way Stuxnet was used.¶ Among the top concerns is that other countries, seeing Stuxnet apparently used by the United States and Israel, might conclude that they would also be justified in carrying out a cyberattack. The British author Misha Glenny, writing in the Financial Times, argued that the deployment of Stuxnet may be seen "as a starting gun; countries around the world can now argue that it is legitimate to use malware pre-emptively against their enemies."¶ Another concern is that **the malicious software code in Stuxnet**, instructing computers to order Iranian centrifuges to spin out of control, **could be modified and used against U.S. infrastructure assets.**¶ **"Now that technology is out there,"** cautions Michigan Rep. Mike Rogers, the Republican chairman of the House Permanent Select Committee on Intelligence. **"People are taking a look at it.** **We are just a few lines of code away from someone else getting closer to a very sophisticated piece of malware that they either wittingly or unwittingly unleash across the world [and cause] huge, huge damage."**¶ The absence of debate over the pros and cons of using cyberweapons is in sharp contrast to the discussion of nuclear weapons. The United States has adopted a "declaratory policy" regarding why it has nuclear weapons and when it would be justified to use them. There is nothing comparable for the cyberweapon arsenal.¶ Rep. Rogers says such gaps in military doctrine and strategy indicate that developments on the cyberwar front are getting ahead of U.S. thinking about cyberwar.¶ "The capabilities, I think, are keeping pace with technology," Rogers said in an interview with NPR. "It's the policy that I worry about. We have not fully rounded out what our [cyber] policies are."¶ The advantages of using cyberweapons are clear. They are more precise than bombs or missiles, and because they damage data rather than physical installations, they are far less likely to hurt innocent civilians. But they are new weapons, and critics say their use should be given careful consideration.¶ **"If we are allowing ourselves to go on the offense without thinking about it, we're likely to militarize cyberspace,"** says the Atlantic Council's Jason Healey. **"We will end up with a cyberspace where everyone is attacking everyone else.** I don't believe we need to go on the offense just yet. The downside is higher than the government acknowledges."¶ White House officials are sensitive to the charge that they should promote more public debate surrounding cybercapabilities. "We understand that there is a view that more discussion is needed about how the United States operates in cyberspace," says National Security Council spokeswoman Caitlin Hayden. "That's why we've published numerous strategies, testified before Congress dozens of times, and [it is why] senior officials ... have given speeches and spoken at conferences and other public events."

**Cyber prolif will be rapid- low barriers of entry and use of proxies**

**Walsh 11**

(Eddie Walsh, The Diplomat's Pentagon (accredited) correspondent and a WSD-Handa Fellow at Pacific Forum CSIS, “The Cyber Proliferation Threat” October 6, 2011, <http://thediplomat.com/new-leaders-forum/2011/10/06/the-cyber-proliferation-threat/>, KB)

**The United States might not be quite as far ahead of other nations in terms of cyber capabilities as many people think** – including potential rivals in the Asia-Pacific, analysts say. It should be a sobering thought for US policymakers at a time when national security analysts around the world have grown increasingly vocal over the proliferation of offensive cyber capabilities by state and non-state actors.¶ **‘There are definitely concerns about cyber warfare proliferation**,’ says Kristin Lord, vice president at the Center for a New American Security, who says she believes that Americans need to take the threat seriously. **‘This isn’t like missiles, which require transporting large materials that can be detected. We are talking about knowledge and code.’**¶ **China, Iran, North Korea and Russia are all seen as likely possessing offensive cyber capabilities that can inflict serious damage on the United States and its allies.** The question is whether they also have the intent to proliferate these capabilities on the black and grey markets.¶ According to Lord, the United States is particularly concerned about scenarios involving collaboration between criminal groups (motivated by financial gain) and state adversaries (wanting to advance their national security interests). **‘We’ve already seen indications of states using criminal groups as proxies for attacks. We** also **know that countries like North Korea are aggressively trying to develop their cyber capabilities,**’ she says. ‘**The open black market, which already exists** in the criminal world, **is** therefore **a big concern**. It provides a place for states and criminals to find each other.’¶ Robert Giesler, a senior vice president and cyber security director at technology applications company SAIC, says **the threat of proliferation is exacerbated by the fact that the technical gap between the United States and its potential adversaries may not be as wide as Americans often like to think.** ‘It’s a dangerous assumption to believe that the US is far ahead in cyber capabilities,’ he says. **‘There’s a low barrier of entry in this market.** We should never use the term dominance in cyber when a 16 year-old can still launch an effective cyber attack.’¶ Faced with such a complex domain, what can the United States do to mitigate the risks posed by foreign cyber capabilities?¶ One answer would be to significantly ramp up US investments in defensive capabilities. According to Giesler, the United States is certainly already further along in defensive cyber security practices and capabilities than the rest of the world. However, Lord cautions that the **United States ‘can’t put a protective wall around every possible target.** Unlike terrorism, **the number of potential targets is almost infinite and not limited by geography.**’

**Proliferation of cyber weapons to terrorists causes nuclear great power wars**

**Fritz 9**

Researcher for International Commission o n Nuclear Nonproliferation and Disarmament [Jason, researcher for International Commission on Nuclear Nonproliferation and Disarmament, former Army officer and consultant, and has a master of international relations at Bond University, “Hacking Nuclear Command and Control,” July, <http://www.icnnd.org/latest/research/Jason_Fritz_Hacking_NC2.pdf>]

This paper will analyse the threat of cyber terrorism in regard to nuclear weapons. Specifically, this research will use open source knowledge to identify the structure of nuclear command and control centres, how those structures might be compromised through computer network operations, and how doing so would fit within established cyber terrorists’ capabilities, strategies, and tactics. If access to command and control centres is obtained, **terrorists could** fake or actually **cause one nuclear-armed state to attack another**, thus **provoking a nuclear response** from another nuclear power. **This may be an easier alternative for terrorist groups than building or acquiring a nuclear weapon or dirty bomb** themselves. **This would also act as a force equaliser, and provide terrorists with the asymmetric benefits of high speed, removal of geographical distance, and a** relatively **low cost.** Continuing **difficulties in** developing **computer tracking technologies** which could trace the identity of intruders, and difficulties in establishing an internationally agreed upon legal framework to guide responses to computer network operations, **point towards an inherent weakness in using computer networks to manage nuclear weaponry. This is** particularly **relevant to reducing the hair trigger posture of existing nuclear arsenals.** **All computers** which are connected to the internet **are susceptible to infiltration and remote control. Computers** which operate on a closed network **may** also **be compromised by various hacker methods, such as privilege escalation, roaming notebooks, wireless access points, embedded exploits in software and hardware, and maintenance entry points.** For example, **e-mail spoofing** targeted at individuals who have access to a closed network, **could lead to the installation of a virus on an open network. This virus could then be** carelessly **transported on removable data storage** between the open and closed network. Information found on the internet may also reveal how to access these closed networks directly. **Efforts by militaries to place increasing reliance on computer networks**, including experimental technology such as autonomous systems, **and their desire to have multiple launch options, such as nuclear triad capability, enables multiple entry points for terrorists.** For example, if a terrestrial command centre is impenetrable, perhaps isolating one nuclear armed submarine would prove an easier task. There is evidence to suggest **multiple attempts have been made by hackers to compromise the extremely low radio frequency once used by the US Navy to send nuclear launch approval to submerged submarines.** Additionally, **the alleged Soviet system known as Perimetr was designed to automatically launch nuclear weapons if it was unable to establish communications with Soviet leadership. This was intended as a retaliatory response in the event that nuclear weapons had decapitated Soviet leadership; however it did not account for the possibility of cyber terrorists blocking communications** through computer network operations in an attempt to engage the system. **Should a warhead be launched, damage could be further enhanced through additional computer network operations. By using proxies, multi-layered attacks could be engineered. Terrorists could** remotely **commandeer computers in China and use them to launch a US nuclear attack against Russia.** Thus **Russia would believe it was under attack from the US and the US would believe China was responsible.** Further, **emergency response communications could be disrupted, transportation could be shut down, and disinformation, such as misdirection, could be planted**, thereby **hindering the disaster relief effort and maximizing destruction. Disruptions in communication and the use of disinformation could** also **be used to provoke uninformed responses.** For example, a nuclear strike between India and Pakis**tan could be** coordinated **with Distributed Denial of Service attacks against key networks,** so theywould have further difficulty in identifying what happened and beforced to respond quickl**y. Terrorists could** also **knock out communications between** these **states** so they cannot discuss the situation. Alternatively, amidst the confusion of a traditional large-scale terrorist attack, **claims of responsibility and declarations of war could be falsified in an attempt to instigate a hasty military response. These false claims could be posted directly on Presidential, military, and government websites. E-mails could also be sent to the media and foreign governments using the IP addresses and e-mail accounts of government officials. A sophisticated** and all encompassing **combination of traditional terrorism and cyber terrorism could be enough to launch nuclear weapons on its own, without the need for compromising command and control centres directly.**

#### And independently, cyber preemption escalates to 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.”**

**Plan solves-**

#### A) It provides international credibility that creates stables norms for deterring preemptive use

**Clarke and Knake ‘12** (Richard (former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States) and Robert (Cybersecurity and homeland security expert at the Council on Foreign Relations), Cyber War: The Next Threat to National Security and What to Do About It, Harper Collins Books, 2012, RSR)

**Balancing our desire for military flexibility** **with the need to address the fact that cyber war could**¶ **damage the U.S. significantly, it may be possible to craft international constraints short of a complete ban.**¶ An international agreement that banned, under any circumstances, the use of cyber weapons is the most¶ extreme form of a ban. In the previous chapter, we looked briefly at the proposal of a no-first-use¶ agreement, which is a lesser option. **A no-first-use agreement could simply be a series of mutual**¶ **declarations**, or it could be a detailed international agreement. **The focus could be on keeping cyber**¶ **attacks from starting wars**, not on limiting their use once a conflict has started. We could apply the pledge¶ to all nations, or only to those nations that made a similar declaration or signed an agreement.¶ **Saying we won’t be the first ones to use cyber weapons may in fact have more than just diplomatic**¶ **appeal in the international arena**. **The existence of the pledge might make it less likely that another nation**¶ **would initiate cyber weapons use because to do so would violate an international norm that employing**¶ **cyber weapons crosses a line, is escalatory, and potentially destabilizing**. **The nation that goes first and**¶ **violates an agreement has added a degree of international opprobrium to its actions and created** in the¶ global community **a presumption of misconduct. International support for that nation’s** underlying **position**¶ in the conflict **might** thus **be undermined and the potential for international sanctions increased.**

**B) US norms against preemptive cyberattacks reverses cyber weapons prolif**

**Goldsmith 10**

Jack Goldsmith, teaches at Harvard Law School and is on the Hoover Institution's Task Force on National Security and Law. He was a member of a 2009 National Academies committee, “Can we stop the cyber arms race?” February 01, 2010, <http://articles.washingtonpost.com/2010-02-01/opinions/36895669_1_botnets-cyber-attacks-computer-attacks>, KB)

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

### Adv 2 - Tradeoff

#### Advantage 2 is Tradeoff

**Cyber attack is highly like in the squo- actors are probing grid weaknesses**

**Reed ‘12** John, Reports on the frontiers of cyber war and the latest in military technology for Killer Apps at Foreign Policy, "U.S. energy companies victims of potentially destructive cyber intrusions", 2012, killerapps.foreignpolicy.com/posts/2012/10/11/us\_energy\_companies\_victims\_of\_potentially\_destructive\_cyber\_attacks

Foreign actors are probing the networks of key American companies in an attempt to gain control of industrial facilities and transportation systems, Defense Secretary Leon Panetta revealed tonight.¶ "We know that foreign **cyber actors are probing America's critical infrastructure networks**," said Panetta, disclosing previously classified information during a speech in New York laying out the Pentagon's role in protecting the U.S. from cyber attacks. "They are targeting the computer control systems that operate chemical, **electricity** and water plants, and those that guide transportation thorough the country."¶ He went on to say that the U.S. government knows of "specific instances where intruders have gained access" to these systems -- frequently known as Supervisory Control and Data Acquisition (or SCADA) systems -- and that "they are seeking to create advanced tools to attack these systems and cause panic, destruction and even the loss of life," according to an advance copy of his prepared remarks.¶ The secretary said that **a coordinated attack on enough critical infrastructure could be a "cyber Pearl Harbor" that would "cause physical destruction and loss of life, paralyze and shock the nation, and create a profound new sense of vulnerability.**"¶ While there have been reports of criminals using 'spear phishing' email attacks aimed at stealing information about American utilties, Panetta's remarks seemed to suggest more sophisticated, nation-state backed attempts to actually gain control of and damage power-generating equipment. ¶ Panetta's comments regarding the penetration of American utilities echo those of a private sector cyber security expert Killer Apps spoke with last week **who said that the networks of American electric companies were penetrated, perhaps in preparation for a Stuxnet-style attack**.¶ Stuxnet is the famous cyber weapon that infected Iran's uranium-enrichment centrifuges in 2009 and 2010. Stuxnet is believed to have caused some of the machines to spin erratically, thereby destroying them.¶ "**There is hard evidence** that there has been penetration of our power companies, and given Stuxnet, that is a staging step before destruction" of electricity-generating equipment, the expert told Killer Apps. Because uranium centrifuges and power turbines are both spinning machines, "**the attack is identical -- the one to take out the centrifuges and the one to take out our power systems is the same attack**."¶ "If a centrifuge running at the wrong speed can blow apart" so can a power generator, said the expert. "If you do, in fact, spin them at the wrong speeds, you can blow up any rotating device."¶ Cyber security expert Eugene Kaspersky said two weeks ago that one of his greatest fears is someone reverse-engineering a sophisticated cyber weapon like Stuxnet **-- a relatively easy task** -- and he noted that Stuxnet itself passed through power plants on its way to Iran. "Stuxnet infected thousands of computer systems all around the globe, I know there were power plants infected by Stuxnet very far away from Iran," Kaspersky said.

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

**Healey ‘13**

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

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

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

**Rid 2/4**

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

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

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

**Gjelten, 13**

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

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

#### 2 impacts:

#### First, cyberwar:

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

**McGraw 13** <[Gary McGraw](http://www.tandfonline.com/action/doSearch?action=runSearch&type=advanced&searchType=journal&result=true&prevSearch=%2Bauthorsfield%3A(McGraw%2C+G)), PhD is Chief Technology Ofﬁcer of Cigital, and author of¶ Software Security (AWL 2006) along with ten other software security¶ books. He also produces the monthly Silver Bullet Security Podcast for¶ IEEE Security & Privacy Magazine (syndicated by SearchSecurity), Cyber War is Inevitable (Unless We Build Security In), Journal of Strategic Studies - Volume 36, Issue 1, 2013, pages 109-119, <http://www.tandfonline.com.proxy.library.cornell.edu/doi/pdf/10.1080/01402390.2012.742013>>#**SPS**

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

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

**Clark and Andreasen 13**

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

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

**Link is linear- every investment in offensive capabilities fuels a cyber-arms race that risks escalation**

**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)

In addition, **there are policy questions raised by the escalating government investment in offensive cyber war capabilities.** One fear is that **each new offensive cyberweapon introduced into use will prompt the development of an even more lethal weapon by an adversary and trigger a fierce cyber arms race. A hint of such an escalatory cycle may be seen in the confrontation with Iran over its nuclear program.** US officials suspect the Iranian government was responsible for the recent wave of cyber attacks directed against Aramco, the Saudi oil company, and may also have been behind a series of denial-of-service attacks on US financial institutions. **Such attacks could be in retaliation for the Stuxnet worm.**¶ Some writers foresee a dangerous new world, created by the United States and Israel with the deployment of Stuxnet. Misha Glenny, writing in the Financial Times, argued that the tacit US admission of responsibility for Stuxnet will act “as a starting gun; countries around the world can now argue that it is legitimate to use malware pre-emptively against their enemies.” One danger is that US adversaries, notably including Russia and China, may now cite the use of Stuxnet to support their argument that an international treaty regulating the use of cyberweapons may be needed. The United States has long opposed such a treaty on the grounds that it would undermine its own technological advantages in cyberspace and could also lead to efforts to regulate the Internet in ways that would harm freedom of expression and information.

#### Second, cyber crime

**Defense solves it**

**McGraw 13** <[Gary McGraw](http://www.tandfonline.com/action/doSearch?action=runSearch&type=advanced&searchType=journal&result=true&prevSearch=%2Bauthorsfield%3A(McGraw%2C+G)), PhD is Chief Technology Ofﬁcer of Cigital, and author of¶ Software Security (AWL 2006) along with ten other software security¶ books. He also produces the monthly Silver Bullet Security Podcast for¶ IEEE Security & Privacy Magazine (syndicated by SearchSecurity), Cyber War is Inevitable (Unless We Build Security In), Journal of Strategic Studies - Volume 36, Issue 1, 2013, pages 109-119, <http://www.tandfonline.com.proxy.library.cornell.edu/doi/pdf/10.1080/01402390.2012.742013>>#**SPS**

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

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

Panda, Sani, Rao, 12 <Hemraj, Associate Professor & Head, Department of Computer Science & Engineering, Alwar Institute of Engineering & Technology, Yerra Shankar, PhD Student, Department of Mathematics Shiksha ‗O‘ Anusandhan University, T.C. Principal, Orissa Engineering College, “Cyber-Crimes and their Impacts: A Review,” Vol. 2, Issue 2,Mar-Apr 2012, <http://www.ijera.com/papers/Vol2_issue2/AG22202209.pdf>>#SPS

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

#### Decline trigger multiple nuclear conflicts

Harris and Burrows, 9

\*counselor in the National Intelligence Council, the principal drafter of Global Trends 2025, \*\*member of the NIC’s Long Range Analysis Unit “Revisiting the Future: Geopolitical Effects of the Financial Crisis”, Washington Quarterly, http://www.twq.com/09april/docs/09apr\_burrows.pdf)

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

### Adv 3 – Separation of Powers

#### Advantage 3 is Seperation of Powers

#### Congressional restrictions on executive cyberwar power is critical to maintain SOP

**Lorber 13**

[Eric, J.D. Candidate, University of Pennsylvania Law School, Ph.D Candidate, Duke University

Department of Political Science. Journal Of Constitutional Law 15.3 <https://www.law.upenn.edu/live/files/1773-lorber15upajconstl9612013>. ETB]

Yet addressing these questions is increasingly important for two reasons. ¶ First, **as states such as China, Israel, Russia, and the U**nited **S**tates **use these weapons now and likely will do so more in future conflicts, determining the domestic legal strictures governing their use would provide policymakers and military planners a better sense of how to operate in cyberspace**.12¶ Second**, the possible employment of these tools adds yet another wrinkle to the battle between the executive and legislative branches over war-making authority**.13 In particular, if neither the War Powers Resolution nor the ¶ Intelligence Authorization Act governs OCOs**, the executive may be allowed** ¶ **to employ U.S. military power** in a manner largely **unchecked by congressional authority**.**14 As a result, the employment of these tools i**mplicates—and perhaps **problematically shifts—the balance between the executive**’s commander-in-chief power15 **and Congress’**s war-making ¶ authority.16

**Strong separation of powers key to heg**

**Ikenberry 1** (G. John, Professor @ Georgetown University, Spring, The National Interest)

First, **America's mature political institutions organized around the rule of law have made it a relatively predictable and cooperative hegemon. The pluralistic and regularized way in which U.S. foreign and security policy is made reduces surprises and allows other states to build long-term, mutually beneficial relations. The governmental separation of powers creates a shared decision-making system that opens up the process and reduces the ability of any one leader to make abrupt or aggressive moves toward other states**. An active press and competitive party system also provide a service to outside states by generating information about U.S. policy and determining its seriousness of purpose. **The messiness of a democracy can**, indeed, **frustrate American diplomats and confuse foreign observers. But over the long term, democratic institutions produce more consistent and credible policies--policies that do not reflect the capricious and idiosyncratic whims of an autocrat**. Think of the United States as a giant corporation that seeks foreign investors. It is more likely to attract investors if it can demonstrate that it operates according to accepted accounting and fiduciary principles. The rule of law and the institutions of policymaking in a democracy are the political equivalent of corporate transparency and accountability. Sharp shifts in policy must ultimately be vetted within the policy process and pass muster by an array of investigatory and decision-making bodies. **Because it is a constitutional, rule-based democracy, outside states are more willing to work with the U**nited **S**tates-or, to return to the corporate metaphor, to invest in ongoing partnerships.

**Heg solves great power wars**

**Barnett 11**

(Thomas P.M. Former Senior Strategic Researcher and Professor in the Warfare Analysis & Research Department, Center for Naval Warfare Studies, U.S. Naval War College American military geostrategist and Chief Analyst at Wikistrat., worked as the Assistant for Strategic Futures in the Office of Force Transformation in the Department of Defense, “The New Rules: Leadership Fatigue Puts U.S., and Globalization, at Crossroads,” March 7 http://www.worldpoliticsreview.com/articles/8099/the-new-rules-leadership-fatigue-puts-u-s-and-globalization-at-crossroads)

**Events in Libya are a further reminder for Americans** that we **stand at a crossroads in our continuing evolution as the world's sole full-service superpower**. **Unfortunately**, **we are increasingly seeking change without cost, and shirking from risk because we are tired of the responsibility**. We don't know who we are anymore, and our president is a big part of that problem. Instead of leading us, he explains to us. Barack Obama would have us believe that he is practicing strategic patience. But many experts and ordinary citizens alike have concluded that he is actually beset by strategic incoherence -- in effect, a man overmatched by the job. It is worth first examining the larger picture: **We live in a time of arguably the greatest structural change in the global order yet endured**, **with this historical moment's most amazing feature being its** relative and absolute **lack of mass violence**. That is something to consider when Americans contemplate military intervention in Libya, because if we do take the step to prevent larger-scale killing by engaging in some killing of our own, we will not be adding to some fantastically imagined global death count stemming from the ongoing "megalomania" and "evil" of American "empire." We'll be engaging in the same sort of system-administering activity that has marked our stunningly successful stewardship of global order since World War II. Let me be more blunt: **As the guardian of globalization**, **the U.S. military has been the greatest force for peace the world has ever known**. **Had America been removed from the global dynamics that governed the 20th century**, the **mass murder never would have ended**. Indeed, it's entirely conceivable **there would now be no identifiable human civilization left, once nuclear weapons entered the killing equation.**  But **the world did not keep sliding down that path of perpetual war**. **Instead, America stepped up and changed everything by ushering in our now-perpetual great-power peace**. **We introduced the international liberal trade order known as globalization** and played loyal Leviathan over its spread. **What resulted was the collapse of empires, an explosion of democracy**, the **persistent spread of human rights**, the liberation of women, **the doubling of life expectancy**, a roughly **10-fold increase in adjusted global GDP** **and a profound and persistent reduction in battle deaths from state-based conflicts.** That is what American "hubris" actually delivered. Please remember that the next time some TV pundit sells you the image of "unbridled" American military power as the cause of global disorder instead of its cure. With self-deprecation bordering on self-loathing, we now imagine a post-American world that is anything but. Just watch who scatters and who steps up as the Facebook revolutions erupt across the Arab world. While we might imagine ourselves the status quo power, we remain the world's most vigorously revisionist force. As for the sheer "evil" that is our military-industrial complex, again, let's examine what the world looked like before that establishment reared its ugly head. The last great period of global structural change was the first half of the 20th century, a period that saw a death toll of about 100 million across two world wars. That comes to an average of 2 million deaths a year in a world of approximately 2 billion souls. Today, with far more comprehensive worldwide reporting, researchers report an average of less than 100,000 battle deaths annually in a world fast approaching 7 billion people. Though admittedly crude, these **calculations suggest a 90 percent absolute drop and a 99 percent relative drop in deaths due to war. We are clearly headed for a world order characterized by multipolarity, something the American-birthed system was designed to both encourage and accommodate. But given how things turned out the last time we collectively faced such a fluid structure, we would do well to keep U.S. power, in all of its forms**, deeply embedded in the geometry to come. To continue the historical survey, after salvaging Western Europe from its half-century of civil war, the U.S. emerged as the progenitor of a new, far more just form of globalization -- one based on actual free trade rather than colonialism. America then successfully replicated globalization further in East Asia over the second half of the 20th century, setting the stage for the Pacific Century now unfolding.

**Keeping strong SoP is a drule**

**Redish and Cisar 91** professor of law at Northwestern and Law Clerk to Chief Judge William Bauer, United States Court of Appeals, Seventh Circuit

Martin H. and Elizabeth J., December 1991, IF ANGELS WERE TO GOVERN" \*: THE NEED FOR PRAGMATIC FORMALISM IN SEPARATION OF POWERS THEORY ,1992 Duke Law Journal, 41 Duke L.J. 449, p. 474

In summary, **no defender of separation of powers can prove with certitude that**, but for the existence of separation of powers, **tyranny would be the inevitable outcome. But the question is whether we wish to take that risk, given the obvious severity of the harm that might result**. **Given both the relatively limited cost imposed by use of separation of powers and the great severity of the harm sought to be avoided, one should not demand a great showing of the likelihood that the feared harm would result**. For **just as in the case of the threat of nuclear war**, no one wants to be forced into the position of saying, “I told you so.”

**Early SOP key to prevent escalation of prez powers and massive inter-branch conflict**

**Taylor- Robinson and Ura 12** (Michelle M, Joseph, "Public opinion and conflict in the separation of powers: Understanding the Honduran coup of 2009," Journal of Theoretical Politics, Oct 9, jtp.sagepub.com/content/early/2012/10/07/0951629812453216.full.pdf)

Finally, our model shows that **once inter-institutional conﬂict has emerged within the**¶ **separation of powers, it is likely** to continue inexorably **until it is resolved by authoritative**¶ **public action**. **An institution that** rationally **seeks to expand its authority in a separation**¶ **of powers system will also have incentives to continue and**, indeed, **escalate the conﬂict**¶ **rather than abandon its effort to aggrandize its authority in the face of opposition**. Likewise, **an attacked institution that rationally combats an attempted expansion of another**¶ **institution’s authority will not fold if the aggressor subsequently raises the stakes.** In the¶ case of Honduras, this dynamic is visible in the mutual escalation of the conﬂict between¶ President Zelaya and the nation’s Congress and Supreme Court. More generally, **this**¶ **result indicates dim prospects for hopes that inter-branch conﬂicts may be resolved by processes that are entirely endogenous to the institutions in question. Rather, intervention by the public or some other exogenous force may be critical to resolving a conﬂict**¶ **once it has emerged.**

**Interbranch conflict causes extinction**

Linda S. **Jamison**, Deputy Director of Governmental Relations @ CSIS, Spring 19**93**, Executive-Legislative Relations after the Cold War, Washington Quarterly, v.16, n.2, p. 189

Indeed there are very few domestic issues that do not have strong international implications, and likewise there are numerous transnational issues in which all nations have a stake. Environmental degradation, the proliferationof weapons of mass destruction, population control, migration, international narcotics trafficking, the spread of AIDS, andthe deterioration of the human condition in the less developed world are circumstancesaffecting all corners ofthe globe. Neither political isolation nor policy bifurcation is an option for the United States. Global circumstances have drastically changed with the end of the Cold War and the political and policy conditions that sustained bipartisan consensus are not applicable to the post-war era. The formulation of a new foreign policy must be grounded in broad-based principles that reflect domestic economic, political and social concerns while providing practical solutions to new situations. Toward a cooperative US Foreign Policy for the 1990s: Ifthe federalgovernment is to meetthenewinternational policychallengesof the post-cold war era, institutional dissension caused by partisan competition and executive-legislative friction must give way to a new way of business**.** Policy flexibility must be the watchword of the 1990s in the foreign policy domainif the United States is to have any hope of securing its interests in theuncertainyears ahead**.** One former policymaker, noting the historical tendency of the United States to make fixed “attachments,” has argued that a changing world dictates policy flexibility, where practical solutions can be developed on principles of broad-based policy objectives (Fulbright 1979). Flexibility, however, will not be possible without interbranch cooperation. The end of the Cold War and the new single-party control of the White House and Congress provide a unique opportunity to reestablish foreign policy cooperation. Reconfiguring post cold war objectives requires comprehension of the remarkable transformations in world affairs and demands an intense political dialogue that goes beyond the executive branch (Mann 1990, 28-29).

**Congressional failure to act leads to massive expansion in prez power- now key**

**Dycus 10**

[Stephen, Professor, Vermont Law School. JOURNAL OF NATIONAL SECURITY LAW &POLICY 4.155.

<http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf> ETB]

**If Congress now fails to enact guidelines for cyber warfare, it might** ¶ **be perceived as inviting “measures on independent presidential** ¶ **responsibility.**”21 Chief Justice **Marshall suggested in Little v. Barreme that** ¶if Congress had remained silent, the President might have been free to ¶ conduct the Quasi-War with France as he saw fit.22 But **the national interest** ¶ **in electronic warfare**, just as in that early maritime conflict, **is so great that** ¶ **the planning and conduct of such a war should not be left entirely to the** ¶ **Executive. And because a cyber war might be fought under circumstances** ¶ **that make it impossible for Congress to play a meaningful contemporaneous** ¶ **role, Congress ought to get out in front of events now in order to be able to** ¶ **participate in the formulation of national policy.**

**Unfettered presidential powers cause nuclear war**

Forrester 89

Professor, Hastings College of the Law (Ray, August 1989, ESSAY: Presidential Wars in the Nuclear Age: An Unresolved Problem, 57 Geo. Wash. L. Rev. 1636)

\*evidence is gendered modified

On the basis of this report, the startling fact is that **one** man **[person] alone has the ability to start a nuclear war**. A basic theory--if not the basic theory of our Constitution--is that **concentration of power** in any one person, or one group, **is dangerous to** mankind **[humanity]. The Constitution**, therefore, **contains a strong system of checks and balances, starting** **with the separation of powers** between the President, Congress, and the Supreme Court. The message is that no one of them is safe with unchecked power. Yet, in what is probably the most dangerous governmental power ever possessed, we find the potential for world destruction lodged in the discretion of one person. As a result of public indignation aroused by the Vietnam disaster, in which tens of thousands lost their lives in military actions initiated by a succession of Presidents, Congress in 1973 adopted, despite presidential veto, the War Powers Resolution. Congress finally asserted its checking and balancing duties in relation to the making of presidential wars. Congress declared in section 2(a) that its purpose was to fulfill the intent of the framers of the Constitution of the United States and insure that the collective judgment of both the Congress and the President will apply to the introduction of United States Armed Forces into hostilities, or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and to the continued use of such forces in hostilities or in such situations. The law also stated in section 3 that [t]he President in every possible instance shall consult with Congress before introducing United States Armed Forces into hostilities or into situations where imminent involvement in hostilities is clearly indicated. . . . Other limitations not essential to this discussion are also provided. The intent of the law is clear. Congress undertook to check the President, at least by prior consultation, in any executive action that might lead to hostilities and war.  [\*1638]  President Nixon, who initially vetoed the resolution, claimed that it was an unconstitutional restriction on his powers as Executive and Commander in Chief of the military. His successors have taken a similar view. Even so, some of them have at times complied with the law by prior consultation with representatives of Congress, but obedience to the law has been uncertain and a subject of continuing controversy between Congress and the President. Ordinarily, the issue of the constitutionality of a law would be decided by the Supreme Court. But, despite a series of cases in which such a decision has been sought, the Supreme Court has refused to settle the controversy. The usual ground for such a refusal is that a "political question" is involved. The rule is well established that the federal judiciary will decide only "justiciable" controversies. "Political questions" are not "justiciable." However, the standards established by the Supreme Court in 1962 in [Baker v. Carr, 369 U.S. 186,](http://www.lexisnexis.com/us/lnacademic/mungo/lexseestat.do?bct=A&risb=21_T9842011382&homeCsi=7338&A=0.48452774259109876&urlEnc=ISO-8859-1&&citeString=369%20U.S.%20186&countryCode=USA) to determine the distinction between "justiciable controversies" and "political questions" are far from clear. One writer observed that the term "political question" [a]pplies to all those matters of which the court, at a given time, will be of the opinion that it is impolitic or inexpedient to take jurisdiction. Sometimes this idea of inexpediency will result from the fear of the vastness of the consequences that a decision on the merits might entail. Finkelstein, Judicial Self-Limitation, 37 HARV. L. REV. 338, 344 (1924)(footnote omitted). It is difficult to defend the Court's refusal to assume the responsibility of decisionmaking on this most critical issue. The Court has been fearless in deciding other issues of "vast consequences" in many historic disputes, some involving executive war power. It is to be hoped that the Justices will finally do their duty here. But **in the meantime the spectre of single-minded power persists, fraught with all of the frailties** of human nature **that each human possesses, including the President**. World history is filled with tragic examples. Even if the Court assumed its responsibility to tell us whether the Constitution gives Congress the necessary power to check the President, the War Powers Resolution itself is unclear. Does the Resolution require the President to consult with Congress before launching a nuclear attack? It has been asserted that "introducing United States Armed Forces into hostilities" refers only to military personnel and does not include the launching of nuclear missiles alone. In support of this interpretation, it has been argued that Congress was concerned about the human losses in Vietnam and in other presidential wars, rather than about the weaponry. Congress, of course, can amend the Resolution to state explicitly that "the introduction of Armed Forces" includes missiles as well as personnel. However, the President could continue to act without prior consultation by renewing the claim first made by President  [\*1639]  Nixon that the Resolution is an unconstitutional invasion of the executive power. Therefore, the real solution, in the absence of a Supreme Court decision, would appear to be a constitutional amendment. All must obey a clear rule in the Constitution. The adoption of an amendment is very difficult. Wisely, Article V requires that an amendment may be proposed only by the vote of two-thirds of both houses of Congress or by the application of the legislatures of two-thirds of the states, and the proposal must be ratified by the legislatures or conventions of three-fourths of the states. Despite the difficulty, the Constitution has been amended twenty-six times. Amendment can be done when a problem is so important that it arouses the attention and concern of a preponderant majority of the American people. But the people must be made aware of the problem. It is hardly necessary to belabor the relative importance of the control of nuclear warfare. A constitutional amendment may be, indeed, the appropriate method. But the most difficult issue remains. What should the amendment provide? How can the problem be solved specifically? The Constitution in section 8 of Article I stipulates that "[t]he Congress shall have power . . . To declare War. . . ." The idea seems to be that only these many representatives of the people, reflecting the public will, should possess the power to commit the lives and the fortunes of the nation to warfare. This approach makes much more sense in a democratic republic than entrusting the decision to one person, even though he may be designated the "Commander in Chief" of the military forces. His power is to command the war after the people, through their representatives, have made the basic choice to submit themselves and their children to war. **There is a recurring relevation of a paranoia of power**throughout human history **that has impelled one leader after another** to draw their people **into wars** which, in hindsight, were foolish, unnecessary, and, in some instances, downright insane. Whatever may be the psychological influences that drive the single decisionmaker to these irrational commitments of the lives and fortunes of others, the fact remains that the **behavior is** a **predictable** one **in any government that does not provide an effective check and balance against uncontrolled power in the hands of one human**. We, naturally, like to think that our leaders are above such irrational behavior. Eventually, however, human nature, with all its weakness, asserts itself whatever the setting. At least that is the evidence that experience and history give us, even in our own relatively benign society, where the Executive is subject to the rule of law.  [\*1640]  Vietnam and other more recent engagements show that it can happen and has happened here. But the "nuclear football"--the ominous "black bag" --remains in the sole possession of the President. And, most important, his **[the] decision to launch a nuclear missile would be**, in fact if not in law, a **declaration of nuclear war, one which** the nation and, indeed, **humanity** in general, probably **would be unable to survive**.

### Solvency

#### Next is Solvency

#### Congressional action is critical to cyber expertise and preserves presidential flexibility

**Dycus ‘10**

[Stephen, Professor, Vermont Law School. JOURNAL OF NATIONAL SECURITY LAW &POLICY 4.155.

<http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf> ETB]

Congress’s active role in the development and implementation of cyber ¶ warfare policy is no guarantee of national security. The policy might be ¶ flawed in various ways. There is also a risk that whatever policy is adopted ¶ will not be properly executed or that its execution will have unintended ¶ results. The policy might be misunderstood or might not provide clear or ¶ appropriate guidance in the urgent circumstances facing its interpreter. The ¶ person charged with implementing the policy might make a mistake – for ¶ example, by interpreting a potential enemy’s electronic espionage as an ¶ attack. Available cyber weaponry might not work as planned. Or a purely ¶ defensive move by U.S. operators might be construed by another nation as ¶ offensive, and provoke an attack. Nor can the clearest policy, statutory or ¶ executive, guarantee compliance by an Executive determined to ignore it.71¶ The rules might be construed by the President in a way that reduces the ¶ importance of Congress’s role. Or they might be challenged in court. ¶ **Congress should not**, however, **hesitate to take the steps outlined here** ¶ **merely because they might produce unintended results or because they** ¶ **could be difficult to enforce. Exactly the same criticisms could be leveled** ¶ **at almost any reorganization or legislative initiative. The high stakes in this** ¶ **instance, and Congress’s constitutional responsibility for formulation of** ¶ **national security policy, mean that Congress cannot sit this one out**. ¶ It might be suggested that these proposed measures would dangerously ¶ tie the President’s hands, thereby limiting her freedom to respond to ¶ unpredictable future national security threats. The very point of the ¶ recommendations, however, is that **Congress should place limits on the** ¶ **President’s actions** – to require her to share the responsibility for deciding ¶ to go to war. **Even then, if the nation comes under sudden cyber or kinetic** ¶ **attack the President will remain free to respond as she sees fit.** ¶ **The United States faces unprecedented challenges from enemies** ¶ **equipped with new weaponry possessing vast, evolving destructive** ¶ **potential. The two political branches must draw on their respective** ¶ **expertise and experiences to work together to meet these challenges,** as the ¶ Framers intended.

#### XO can’t solve- binding precedent is key to norm building and check expansion of prez powers

**Huston ‘11**

[Warner Todd Huston is a Chicago based freelance writer, has been writing opinion editorials and social criticism since early 2001, <http://www.conservativecrusader.com/articles/we-need-rules-for-cyberwarfare-before-a-president-steals-that-power-too> ETB]

**Presidents have had certain restrictions for war**-making ever since because the founders wanted to make sure that war was something duly considered not easily engaged.¶ **This should hold as much for use of computer-based warfare** as it does for any other type of military attack. **Currently** computer-based war, or **cyberwarfare**, presents a new field of military application and we **have no legal precedent to govern its use.**¶ **Despite the last 200 years of presidents slowly stealing away power from Congress to initiate military actions, we should really think long and hard about allowing any president to unleash cyberwarfare at his discretion**. In fact, **we should set a precedent immediately to prevent any president from using cyberwarfare without the consent of Congress.**¶ Why? Because cyberwarfare is a far, far different animal than use of conventional military forces and indiscriminate use of it **would endanger** our way of **life** in harsh and immediate terms if used against us. For that reason, **we should be very careful when we use it against others**. We should have solid legal definitions behind its use **so as not to give enemies the excuse to resort to it quickly themselves.**¶ You see, cyberwarfare is a relatively cheap war power, easier to implement, and requires far fewer in personnel and facilities than launching an invasion using conventional military forces. This is not to say that cyberwarfare is easy -- far from it. But it is cheaper and easier than deploying regular military forces.¶ So, we should casually resort to cyberwarfare no more easily than we would to using conventional forces. But **if we do not set down** specific and **binding rules for its use we risk giving this power over to a president which could cause less considered use of this** sort of **warfare**. **That** in turn, **would give enemies an excuse to do the same**. Further, remember that setting legally binding reasons for warfare is a long and proud American tradition, one that legitimizes our nation and one we should not casually toss aside simply under the assumption that enemies will not be as thoughtful as we.¶ **We should lead the world in** **considered** **use of cyberwarfare** **and we should do so now**. Any of those that felt we illicitly launched into the war on terror should no less worry about indiscriminate use of cyberwarfare. But illicit use or no, **we should be** deadly **certain of what powers our president can have,** **when and how he can use them, and where the line should be drawn, even in cyberspace.**

**Renouncing use of large-scale attacks reduces the risk of cyberattack**

**Owens et al. ‘9**

[William A. Owens, Kenneth W. Dam, and Herbert S. Lin, editors, ¶ Committee on Offensive Information Warfare, National Research Council. <http://www.lawfareblog.com/wp-content/uploads/2013/01/NRC-Report.pdf> ETB]

**No first use of large-scale cyberattacks**. Although weapons for cyberattack are valid and legitimate military weapons to be deployed and ¶ used in support of U.S. interests, **the U**nited **S**tates **will not be the** ¶ **first nation in a conflict to conduct against nations cyberattacks that** ¶ **would have the potential of causing widespread societal devastation and chaos.** Nevertheless, the United States reserves the right ¶ to conduct such attacks should it be subject to such attacks itself.¶ **Such a policy would** seek to **discourage the use of large-scale cyberattacks as an instrument of** national **policy by any nation.** However, the U.S. ¶ stance on the use of large-scale cyberattacks would be based primarily ¶ on threatening in-kind retaliation rather than setting an example. As in ¶ the previous case, **the benefit to the United States** if such stigmatization ¶ occurred **would be a lower likelihood that it would experience such an** ¶ **attack.**

#### Military will adhere to the law

Dunlap ‘12

[Maj. Gen. Charles J. Dunlap Jr. (Ret.), Professor of the Practice of Law¶ Executive Director, Center on Law, Ethics and National Security @ Duke. In Patriot Debates: Contemporary Issues in National Security Law. <http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch9/ch9_ess2.html> ETB]

This raises an important question: Should America wage war— cyber or otherwise—without legal “limits”? Military commanders have seen the no-legal-limits movie before and they do not like it. In the aftermath of 9/11, civilian lawyers moved in exactly that direction. Former Attorney General Alberto Gonzales, for example, rejected parts of the Geneva Conventions as “quaint.” He then aligned himself with other civilian government lawyers who seemed to believe that the President’s war-making power knew virtually no limits. The most egregious example of this mindset was their endorsement of interrogation techniques now widely labeled as torture.25 The results of the no-legal-limits approach were disastrous. The ill-conceived civilian-sourced interrogation, detention, and military tribunal policies, implemented over the persistent objections of America’s military lawyers, caused an international uproar that profoundly injured critical relations with indispensable allies.26 Even more damaging, they put the armed forces on the road to Abu Ghraib, a catastrophic explosion of criminality that produced what military leaders like then U.S. commander in Iraq Lieutenant General Ricardo Sanchez labeled as a “clear defeat.”27 Infused with illegalities, Abu Ghraib became the greatest reversal America has suffered since 9/11. In fact, in purely military terms, it continues to hobble counterterrorism efforts. General David Petraeus observed that “Abu Ghraib and other situations like that are non-biodegradable. They don’t go away.” “The enemy,” Petraeus says, “continues to beat you with them like a stick.”28 In short, military commanders want to adhere to the law because they have hard experience with the consequences of failing to do so.

**deterrence fails vs 3rd parties, making escalation likely**

**Owens et al 9**

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

**Catalytic conflict refers to the phenomenon in which a third party** ¶ **instigates conflict between two other parties.** These parties could be ¶ nation-states or subnational groups, such as terrorist groups. The canonical scenario is one in which the instigator attacks either Zendia or Ruritania in such a way that Zendia attributes the attack to Ruritania, or vice ¶ versa. **To increase confidence in the success of initiating a catalytic war,** ¶ **the instigator might attack both parties, seeking to fool each party into** ¶ **thinking that the other party was responsible**. ¶ As also noted in Section 2.4.2, **high-confidence attribution of a cyberattack under all circumstances is** arguably very **problematic, and an instigator would find it by comparison very easy to deceive each party about** ¶ **the attacker’s identity.** Thus, **a catalytic attack could be very plausibly** ¶ **executed**. In addition, **if a state of tension already exists** between the ¶ United States and Zendia, **both** U.S. and Zendian **leaders will be predisposed toward thinking the worst about each other—and thus may be** ¶ **less likely to exercise due diligence in carefully attributing a cyberattack.** ¶ A Ruritanian might thus choose just such a time to conduct a catalytic ¶ cyberattack.

# 2AC

## 2AC Feminism K

#### The alternative does nothing to question patriarchy – voting negative is simply a negation of a policy, no change occurs

#### The plan is a step in the right direction of decreasing offensive operations

#### Ethier alternative can’t overcome all the patriarchy in the status quo which means it fails OR the permutation can overcome any tiny link to the aff

#### Case outweighs - EVERYBODY is effected by nuclear war

#### 4. Perm – do both – that solves

Zizek 89, Senior Researcher in the Department of Philosophy at the University of Ljubljana, Slovenia, Codirector of the Center for Humanities at Birkbeck College, University of London, and Distinguished Fashion Expert for Abercrombie and Fitch Quarterly, ’89 (Slavoj, Autumn, “Looking Awry” October, Vol 50 p 30-55, JSTOR)

By means of a metaphor of the way anamorphosis functions in painting, Bushy tries to convince the queen that her sorrow has no foundation, that its reasons are null, but the crucial point is the way his metaphor splits, redoubles itself, i.e., the way he entangles himself in contradiction. First ("sorrow's eye, glazed with blinding tears, / Divides one thing entire to many objects"), he refers to the simple, commonsense opposition between a thing as it is "in itself," in reality, and its "shadows," reflections in our eyes, subjective impressions multiplied because of our anxieties and sorrows. When we are worried, a small difficulty assumes giant proportions; we see the thing as far worse than it really is. The metaphor at work here is that of a glass surface sharpened, cut in such a way that it reflects a multitude of images; instead of the tiny substance, we see its "twenty shadows." In the following verses, however, things become complicated. At first sight it seems that Shakespeare only illustrates the fact that "sorrow's eye . . . divides one thing entire to many objects" with a metaphor from the domain of painting ("Like perspectives, which rightly gaz'd upon/Show nothing but confusion; ey'd awry/Distinguish form"), but what he really accomplishes is a radical change of terrain. From the metaphor of a sharpened glass surface he passes to the metaphor of anamorphosis, the logic of which is quite different. A detail of a picture that "rightly gaz'd," i.e., from a straightforward, frontal view, appears a blurred spot, assumes clear, distinct shapes once we look at it "awry," from aside. The verses which apply this metaphor back to the queen's anxiety and sorrow are thus profoundly ambivalent: "so your sweet majesty, / Looking awry upon your lord's departure, / Finds shapes of grief more than himself to wail; / Which, look'd on as it is, is nought but shadows / Of what is not." That is to say, if we take the comparison between the queen's look and the anamorphic look literally, we would be obliged to state that precisely by "looking awry," i.e., from aside, she sees the thing in its clear and distinct form, in opposition to the "straightforward," frontal view which sees only an indistinct confusion (and, incidentally, the further development of the drama fully justifies the queen's most sinister presentiments), But, of course, Bushy did not "want to say" this. His intention was to say quite the opposite: by means of an imperceptible subreption, he returned to the first metaphor (that of a sharpened glass) and "wanted to say" that, because her view is distorted by sorrow and anxiety, the queen sees causes for alarm where a closer, matter-of-fact look attests that there is next to nothing in it. What we have here are thus two realities, two "substances." On the level of the first metaphor, we have the commonsense reality as "substance with twenty shadows," as a thing split into twenty reflections by our subjective view; in short, as a substantial "reality" distorted by our subjective perspective (inflated by our anxiety, etc.). If we look at a thing straight on, from a matter-of-fact perspective, we see it "as it really is," while the look puzzled by our desires and anxieties ("looking awry") gives us a distorted, blurred image of the thing. On the level of the second metaphor (anamorphosis), however, the relation is exactly the opposite: if we look at a thing straight on, i.e., from a matter-of-fact, disinterested, "objective" perspective, we see nothing but a formless spot. The object assumes clear and distinctive features only if we look at it "from aside," i.e., with an "interested" look, with a look supported, permeated, and "distorted" by a desire. This is precisely the Lacanian objet petit a, the object-cause of desire, an object which is, in a way, posited by the desire itself. The paradox of desire is that it posits retroactively its own cause, i.e., an object that can be perceived only by the look "distorted" by desire, an object that does not exist for an "objective" look. In other words, the objet petit a is always, by definition, perceived in a distorted way, because, outside this distortion, "in itself," it does not exist, i.e., because it is nothing but the embodiment, the materialization of this distortion, of this surplus of confusion and perturbation introduced by desire into so-called "objective reality." Objet petit a is "objectively" nothing, it is nothing at all, nothing of the desire itself which, viewed from a certain perspective, assumes the shape of "something." It is, as is formulated in an extremely precise manner by the queen in her response to Bushy, her "something grief" begot by "nothing" ("For nothing hath begot my something grief "). Desire "takes off" when "something" (its object-cause) embodies, gives positive existence to its "nothing," to its void. This "something" is the anamorphic object, a pure semblance that we can perceive clearly only by "looking awry." It is precisely (and only) the logic of desire that belies the notorious wisdom that "nothing comes from nothing." In the movement of desire, "something comes from nothing." It is true that the object-cause of desire is a pure semblance, but this does not prevent it from triggering off a whole chain of consequences which regulate our "material," "effective" life and deeds.

#### 5. Perm do the plan and non-competitive parts of the alt

#### 9. Wars don’t have single causes – consensus of experts

Cashman 2kGreg, Professor of Political Science at Salisbury State University “What Causes war?: An introduction to theories of international conflict” pg. 9

Two warnings need to be issued at this point. First, while we have been using a single variable explanation of war merely for the sake of simplicity, multivariate explanations of war are likely to be much more powerful. Since social and political behaviors are extremely complex, they are almost never explainable through a single factor. Decades of research have led most analysts to reject monocausal explanations of war. For instance, international relations theorist J. David Singer suggests that we ought to move away from the concept of “causality” since it has become associated with the search for a single cause of war; we should instead redirect our activities toward discovering “explanations”—a term that implies multiple causes of war, but also a certain element of randomness or chance in their occurrence.

#### Threats are real – we can’t ignore them

Olav. F. Knudsen, Prof @ Södertörn Univ College, ‘1 [*Security Dialogue* 32.3, “Post-Copenhagen Security Studies: Desecuritizing  Securitization,” p. 360]

In the post-Cold War period, agenda-setting has been much easier to influence than the securitization approach assumes. That change cannot be credited to the concept; the change in security politics was already taking place in defense ministries and parlia- ments before the concept was first launched. Indeed, securitization in my view is more appropriate to the security politics of the Cold War years than to the post-Cold War period. Moreover, I have a problem with the underlying implication that it is unim- portant whether states ‘really’ face dangers from other states or groups. In the Copenhagen school, threats are seen as coming mainly from the actors’ own fears, or from what happens when the fears of individuals turn into paranoid political action. In my view, this emphasis on the subjective is a misleading conception of threat, in that it discounts an independent existence for what- ever is perceived as a threat. Granted, political life is often marked by misper- ceptions, mistakes, pure imaginations, ghosts, or mirages, but such phenom- ena do not occur simultaneously to large numbers of politicians, and hardly most of the time. During the Cold War, threats – in the sense of plausible possibilities of danger – referred to ‘real’ phenomena, and they refer to ‘real’ phenomena now. The objects referred to are often not the same, but that is a different matter. Threats have to be dealt with both in terms of perceptions and in terms of the phenomena which are perceived to be threatening. The point of Wæver’s concept of security is not the potential existence of danger somewhere but the use of the word itself by political elites. In his 1997 PhD dissertation, he writes, ‘One can view “security” as that which is in language theory called a speech act: it is not interesting as a sign referring to something more real – it is the utterance itself that is the act.’ The deliberate disregard of objective factors is even more explicitly stated in Buzan & Wæver’s joint article of the same year. As a consequence, the phenomenon of threat is reduced to a matter of pure domestic politics. It seems to me that the security dilemma, as a central notion in security studies, then loses its founda- tion. Yet I see that Wæver himself has no compunction about referring to the security dilemma in a recent article. This discounting of the objective aspect of threats shifts security studies to insignificant concerns. What has long made ‘threats’ and ‘threat perceptions’ important phenomena in the study of IR is the implication that urgent action may be required. Urgency, of course, is where Wæver first began his argu- ment in favor of an alternative security conception, because a convincing sense of urgency has been the chief culprit behind the abuse of ‘security’ and the consequent ‘politics of panic’, as Wæver aptly calls it. Now, here – in the case of urgency – another baby is thrown out with the Wæverian bathwater. When real situations of urgency arise, those situations are challenges to democracy; they are actually at the core of the problematic arising with the process of making security policy in parliamentary democracy. But in Wæver’s world, threats are merely more or less persuasive, and the claim of urgency is just an- other argument. I hold that instead of ‘abolishing’ threatening phenomena ‘out there’ by reconceptualizing them, as Wæver does, we should continue paying attention to them, because situations with a credible claim to urgency will keep coming back and then we need to know more about how they work in the interrelations of groups and states (such as civil wars, for instance), not least to find adequate democratic procedures for dealing with them.

#### And monocausal focus on root cause justifies violence and tyranny

Achterhuis 2. **[Hans**, Professor of Philosophy @ Twente University, Peace Review, vol. 14, p. 158]

At base, each person who has-or claims to have-a single account for violence is proceeding in an extremely violent manner. Those who claim to know the origin of violence, to know the root of all evil, give themselves at the same stroke the moral right to reach back and root it out-thus providing, via a chain of reasoning with which we are all familiar, the justification for using violence in order to drive violence from the world. If we know where its origin lies, what could be wrong with using violence for the (sole) purpose of obtaining eternal peace and prosperity? This is a violent chain of reasoning. Implicitly or explicitly, it entails the call for a relentless struggle against the discovered origin of evil, whether that be said to lie in a particular class, nation, or ethnic group; a particular social structure such as capitalism or socialism; or a particular condition such as poverty. Whenever or wherever such an origin is posed, violence is alread 'resent for it inevitably sets up the argument that violence is permitted in order to achieve peace. It is a means-ends logic: the noble ends sanctify the violent means. From Valkenberg I learned that we cannot think about violence as a means-ends logic, but only in the form of a dialogue between human beings. If readers sense a strong reaction on my part against monocausal theories, I readily admit that the reaction is first of all directed against myself. For it is a lesson I learned only through trial and error. Once upon a time I too thought that I had located the origin of violence and could thus revolutionize the world. But this, in my opinion, is the greatest temptation for the political thinker. Many political philosophers have proposed totalitarian therapies based on philosophical analyses that attribute the origin of social evil to a single root. But single philosophical answers to the question of violence can never be more than partial. Such answers are but pieces of a dialogue.

#### Turn—Reductionism—their attempt to diagnose the problem of sexual difference ignores other causal factors and reproduces oppression

Butler 1997 ([Pheng Cheah](http://muse.jhu.edu/journals/diacritics/v028/28.1butler.html#top) is an associate professor of English at Northwestern University, [Drucilla Cornell](http://muse.jhu.edu/journals/diacritics/v028/28.1butler.html#top) is a professor of law, women's studies, and political science at Rutgers University, [Elizabeth Grosz](http://muse.jhu.edu/journals/diacritics/v028/28.1butler.html#top) teaches Philosophy and Critical Theory at Monash University in Australia, Judith Butler, “The Future of Sexual Difference: An Interview with [Judith Butler](http://muse.jhu.edu/journals/diacritics/v028/28.1butler.html#authbio1) and [Drucilla Cornell](http://muse.jhu.edu/journals/diacritics/v028/28.1butler.html#authbio2),” Diacritics 28., Project Muse)

PC: I still feel that Irigaray's work facilitates more than you have been allowing. It seems that there is sexual oppression in all societies and that, in neocolonial globalization, the maternal body is the support of the global capitalist system. Women of the South become low-paid workers or unpaid workers or sweated labor largely because of the identifications of woman as good wife, good mother, or good daughter. This seems to confirm Irigaray's point that woman has always been regarded as a (maternal) envelope for man, that the maternal body has been made the substrate of existence in many societies. In a perverse way, this is even more true if one thinks about the role of reproductive engineering (the suppression of the mother) in keeping populations low in the South so that it can be more attractive to foreign direct investment or inflows of multinational capital. Hence if we want to think about political transformation on a global scale, something that is necessitated by the fact that globalization increasingly connects all nations--then [End Page 35] isn't Irigaray's ethics of sexual difference useful because it undermines the basis of this globalized form of superexploitation? If one doesn't want to use the word "universal" because it is a bad word, wouldn't sexual difference be at least generalizable, so that this idea of a sexual ethics can be made practicable in a global political theater? Or do you see the attempt to extend Irigarayan ethics as a form of cultural imperialism that fetishizes the maternal body? JB: But here you are talking about generalizability and usefulness, and here it is a question of whether we can use sexual difference to describe what can be ethnographically substantiated as a prevalent concern in a number of societies. . . . PC: I would say "all societies," but to be cautious one should say "most" . . . JB: Even if we do accept that questions of reproduction, which I gather is not what you mean by the maternal body. . . . PC: But they are conjoined. . . . EG: It's particularly this ideology of being a faithful part of the family, of being a good wife and a good mother--it's precisely that ideology that forces poor women to continue working in appalling conditions. JB: Right. But then the question is whether the use of sexual difference as we have seen it in at least two of its forms that we have talked about, whether that works as a rallying point for politicization or indeed, as something that is descriptively rich for any of these societal situations. . . . PC: . . . or counterproductive, as both of you have claimed in terms of the scenarios that you described above. JB: It seems that you are suggesting that there is a question of the reification of the feminine as the maternal, a way in which the feminine has been cast as the maternal, in a number of societies. And now Irigaray comes along, and does she diagnose this or does she continue that act of fusion? EG: No, is she useful? JB: At which point, we are then asking whether her notion of sexual difference usefully describes these preexisting societies. If that were true, then we would have to go back to square one and ask what we mean by "sexual difference," because as Drucilla has taught me, as Naomi Schor has taught me, it is not supposed to describe the existing and it cannot, it is precisely what is beyond any description of the existing. . . . PC: But Irigaray tries to overcome the essence/existence distinction. This is what makes her idea of sexual difference so interesting. It is the work of the negative that is at the same time extremely real, to speak in Hegelian terms, that she sometimes also uses and reinscribes. There is no split between the ideal and the real. For her, sexual difference is the sensible transcendental. JB: It seems to me that you are having it be all things, and the real question is, To what extent can her framework work as a politicization in a global perspective, or is it in fact globalizing in an imperialist mode that would make it actually quite problematic? [End Page 36] EG: Those are the two operative questions that we want to ask! They are the positive and negative limits, what might be good or bad about what her work entails. JB: Let me just point one thing out to you. We could have an argument: is her notion of sexual difference in fact reactionary? Is it complicit with the very problem that women are facing in these societies that we purport to be describing? EG: Yes, there isn't a simple answer to these questions. But how would one go about answering them? JB: I'm struck by the fact that she's not particularly interested in problems of globalization, is she? She's very interested in universality, though.

**12. The criticism’s focus on identity creates a politics of exclusion that prevents meaningful critiques and turns the very superior identification they try to solve**

Jarvis 2000[DSL, ‘International Relations and the Challenge of Postmodernism’, February, *University of South Carolina Publishing*, pg. 160-162]

Critical research agendas of this type, however, are not found easily in International Relations. Critics of feminist perspectives run the risk of denouncement as either a misogynist malcontent or an androcentric keeper of the gate. At work in much of this discourse is an unstated political correctness, where the historical marginalization of women bestows intellectual autonomy, excluding those outside the identity group from legitimate participation in its discourse. Only feminist women can do real, legitimate, feminist theory since, in the mantra of identity politics, discourse must emanate from a positional (personal) ontology. Those sensitive or sympathetic to the identity politics of par­ticular groups are, of course, welcome to lend support and encourage­ment, but only on terms delineated by the groups themselves. In this way, they enjoy an uncontested sovereign hegemony oyer their own self-identification, insuring the group discourse is self constituted and that its parameters, operative methodology, *,uu\* standards of argument, appraisal, and evidentiary provisions are self defined. Thus, for example, when Sylvester calls lor a "home.steading" does so "by [a] repetitive feminist insistence that *we be included on our terms"* (my emphasis). Rather than an invitation to engage in dialogue, this is an ultimatum that a sovereign intellectual space be provided and insulated from critics who question the merits of identity-based political discourse. Instead, Sylvester calls upon International Relations to "share space, respect, and trust in a re-formed endeavor," but one otherwise proscribed as committed to demonstrating not only "that the secure homes constructed by IR's many debaters are chimerical," but, as a con­sequence, to ending International Relations and remaking it along lines grounded in feminist postmodernism.93 Such stipulative provisions might be likened to a form of negotiated sovereign territoriality where, as part of the settlement for the historically aggrieved, border incursions are to be allowed but may not be met with resistance or reciprocity. Demands for entry to the discipline are thus predicated on conditions that insure two sets of rules, cocooning postmodern feminist spaces from systematic analyses while "respecting" this discourse as it hastens about the project of deconstructing International Relations as a "male space." Sylvester's impassioned plea for tolerance and "emphatic cooperation" is thus confined to like-minded individuals, those who do not challenge feminist epistemologies but accept them as a necessary means of rein­venting the discipline as a discourse between postmodern identities—the most important of which is gender.94 Intolerance or misogyny thus become the ironic epithets attached to those who question the wisdom of this reinvention or the merits of the return of identity in international theory.'"' Most strategic of all, however, demands for entry to the disci­pline and calls for intellectual spaces betray a self-imposed, politically motivated marginality. After all, where are such calls issued from other than the discipline and the intellectual—and well established—spaces of feminist International Relations? Much like the strategies employed by male dissidents, then, feminist postmodernists too deflect as illegitimate any criticism that derives from skeptics whose vantage points are labeled privileged. And privilege is vari­ously interpreted historically, especially along lines of race, color, and sex where the denotations white and male, to name but two, serve as generational mediums to assess the injustices of past histories. White males, for example, become generic signifiers for historical oppression, indicating anontologicallv privileged group by which the historical experiences of the "other" can then be reclaimed in the context of their related oppression, exploitation, and exclusion. Legitimacy, in this context, can then be claimed in terms of one's group identity and the extent to which the history of that particular group has been "silenced." In this same way, self-identification or "self-situation" establishes one's credentials, allowing admittance to the group and legitimating the "authoritative" vantage point from which one speaks and writes. Thus, for example, Jan Jindy Pettman includes among the introductory pages to her most recent book, *Worldinjj Women,* a section titled "A (personal) politics of location," in which her identity as a woman, a feminist, and an academic, makes appar­ent her particular (marginal) identities and group loyalties.96 Similarly, Christine Sylvester, in the introduction to her book, insists, "It is impor­tant to provide a context for one's work in the often-denied politics of the personal." Accordingly, self-declaration reveals to the reader that she is a feminist, went to a Catholic girls school where she was schooled to "develop your brains and confess something called 'sins' to always male forever priests," and that these provide some pieces to her dynamic objec­tivity.97 Like territorial markers, self-identification permits entry to intel­lectual spaces whose sovereign authority is "policed" as much by marginal subjectivities as they allege of the oppressors who "police" the discourse of realism, or who are said to walk the corridors of the discipline insuring the replication of patriarchy, hierarchical agendas, and "malestream" theory. If Sylvester's version of feminist postmodernism is projected as tolerant, per-spectivist, and encompassing of a multiplicity of approaches, in reality it is as selective, exclusionary, and dismissive of alternative perspectives as mainstream approaches are accused of being.

**14. Associating women with care dangerously limits the ethico-political possibilities for women**

MacGregor 4 – Postdoc Fellows Sherilyn MacGregor is a postdoctoral fellow in the Institute for Environment, Philosophy and Public Policy at Lancaster University, UK. “From Care to Citizenship Calling Ecofeminism Back To Politics,” Ethics & the Environment 9.1 (2004) 56-84

One of the themes in contemporary ecofeminist literature is that women's care-related perspectives on human-nature relations should be adopted as a generalized normative stance, a form of ecological civic virtue or "a universal public caring" (Salleh 1997). This argument is supported by those ecofeminist theorists who portray caring relationships as models for sustainable living and as important sources of political empowerment for women in the larger social sphere. The women who appear in the narratives that inform ecofeminist alternative visions are variously referred to as grassroots women, housewife activists and "re/sisters" (Salleh 1997)) who work voluntarily to sustain life and to fight against the powers that put that life in jeopardy. The vision that their experiences inspire consists of an integration of diverse political struggles into one overarching movement for survival that is grounded in everyday material practices at the local level. So grounded, it is a vision that is fundamentally different from right-wing ideologies that embrace global capitalism as well as from the philosophies of postmodernism that are said to privilege discourse and discourage activism. While there are important aspects to ecofeminist valuations of women's caring—particularly in light of the way non-feminist ecopolitical discourse ignores the work of care—I argue that there are also political risks in celebrating women's association with caring (both as an ethic and a practice) and in reducing women's ethico-political life to care. In view of these risks, to be discussed herein, I think a degree of skepticism is in order. I question whether care is a wise choice of metaphor around which to create a feminist political project for social and ecological change. How can societal expectations that women be caring or the exploitation of women's unpaid caring labor under capitalism be challenged at the same time that the specificity of women's caring stance towards the environment is held up as an answer to the ecological crisis? What does it mean, moreover, for women to enter the realm of the political through a window of care and maternal virtue? How is this feminist? And how, if at all, is it political? It is my position that ecofeminists should see caring through less-than-rosy-glasses, as a paradoxical set of practices, feelings, and moral orientations that are embedded in particular relations and contexts and socially constructed as both feminine and private. Revaluing care in the way many ecofeminists seem to do results in an affirmation of gender roles that are rooted in the patriarchal dualisms that all feminisms, on my definition at least, must aim persistently to resist and disrupt. I support my position by drawing on the work of some of the feminist philosophers, political economists, and political theorists who have argued that the positive identification of women with caring ought to be treated cautiously for it obscures some of the negative implications of feminized care and narrows our understanding of women as political actors. In the first part of the discussion, I cast doubt on ecofeminist ideas about the "feminine principle" by highlighting some of the critiques of care ethics made by feminist moral philosophers. I then subject ecofeminist celebrations of caring labor to questions raised by feminist political economists about its exploitation in globalizing capitalist societies. I also question whether claims that women are empowered through their care-inspired eco-activism have been accompanied by a sufficient consideration of feminist political transformation. That discussion leads into the final part of the paper where I look to feminist theorists of citizenship to develop the argument that ecofeminists would be better served by using the language of citizenship instead of the language of care to understand and theorize women's engagement in ecopolitics.