# 1AC

## Plan

#### 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.

## 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 on 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.**

**No defense- 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.

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

**Clarke 2009**

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

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

#### 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.**

## Advantage 2 is Defense

**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 K**iller **A**pps. 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 backfires – creates priority confusion and drains cyber-defense resources**

**Healey ‘13**

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

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

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

**Rid 2/4**/13

[Thomas Rid is a reader at the Department of War Studies, King's College London. [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**](http://www.tandfonline.com.proxy.library.cornell.edu/doi/pdf/10.1080/01402390.2012.742013%3e#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**

**Clarke 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** nuclear weapons **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.

#### Air gapping empirically fails

Cobos ‘12

[Major Mark A. Cobos, United States Army, School of Advanced Military Studies

United States Army Command and General Staff College Fort Leavenworth, Kansas. “Nodes and Codes: The Reality of Cyber Warfare.” ETB]

In the fall of 2010, at the same time the Symantec Trio and Ralph Langner described Stuxnet’s systematic progress from infected flash drive to centrifuge destruction in the blogosphere, William Lynn published an eye-opening article in *Foreign Affairs* entitled “Defending a New Domain.” The Deputy US Secretary of Defense opened the article by describing a previously classified incident in which a flash drive infected with malicious code established a “digital beachhead” on a US military laptop in the Middle East that it used to send data from classified military networks to servers under foreign control. Lynn emphasized the vulnerability of data in supposedly secure networks that utilize an “air gap,” physically separating secure and unsecure networks like the public internet. The article’s timing, discussion of infection methods, and revelation of an attack on an “air gapped” US network echoed the Stuxnet themes concurrently debated in the Symantec and Langner blogs. Lynn concluded the article by declaring

**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, cybercrime – defense solves it

McGraw 13

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

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

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

Sani et al 12

<Hemraj, Associate Professor & Head, Department of Computer Science & Engineering, Alwar Institute of Engineering & Technology, Yerra Shankar, PhD Student, Department of Mathematics Shiksha ‗O‘ Anusandhan University, T.C. Principal, Orissa Engineering College, “Cyber-Crimes and their Impacts: A Review,” Vol. 2, Issue 2,Mar-Apr 2012, [http://www.ijera.com/papers/Vol2\_issue2/AG22202209.pdf>#SPS](http://www.ijera.com/papers/Vol2_issue2/AG22202209.pdf%3e#SPS)

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

#### Economic collapse causes nuclear conflicts

Burrows and Harris 9

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

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 groupsinheriting¶ organizational structures, command and control processes, and training¶ procedures necessary to conduct sophisticated attacksand 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.¶

#### The best and most qualified studies agree

Royal 2010

(Jedediah Royal, Director of Cooperative Threat Reduction at the U.S. Department of Defense, 2010, “Economic Integration, Economic Signaling and the Problem of Economic Crises,” in Economics of War and Peace: Economic, Legal and Political Perspectives, ed. Goldsmith and Brauer, p. 213-214)

Less intuitive is how periods of economic decline may increase the likelihood of external conflict**.** Political science literature has contributed a moderate degree of attention to the impact of economic decline and the security and defence behaviour of interdependent states. Research in this vein has been considered at systemic, dyadic and national levels. Several notable contributions follow. First, on the systemic level, Pollins (2008) advances Modelski and Thompson's (1996) work on leadership cycle theory, finding that **rhythms in the** global **economy are associated with the** rise and **fall of a** pre-eminent **power and** the often **bloody transition** from one pre-eminent leader to the next. As such, exogenous shocks such as economic crises could usher in a redistribution of relative power (see also Gilpin. 1981) that leads to uncertainty about power balances, **increasing** the **risk of miscalculation** (Feaver, 1995). Alternatively, even a relatively certain redistribution of power could lead to a permissive environment for conflict as a rising power may seek to challenge a declining power (Werner. 1999). Separately, Pollins (1996) also shows that global economic cycles combined with parallel leadership cycles impact the likelihood of conflict among major, medium and small powers, although he suggests that the causes and connections between global economic conditions and security conditions remain unknown. Second, on a dyadic level, Copeland's (1996, 2000) theory of trade expectations suggests that 'future expectation of trade' is a significant variable in understanding economic conditions and security behaviour of states. He argues that interdependent states are likely to gain pacific benefits from trade so long as they have an optimistic view of future trade relations. However, if the expectations of future trade decline, particularly for difficult to replace items such as energy resources, the **likelihood for conflict increases,** as **states will be inclined to use force to gain** access to those **resources.** Crises could potentially be the trigger for decreased trade expectations either on its own or because it triggers protectionist moves by interdependent states.4 Third, others have considered the link between economic decline and external armed conflict at a national level. Blomberg and Hess (2002) **find a strong correlation between internal** conflict **and external conflict**, particularly **during periods of** economic **downturn**. They write: The linkages between internal and external conflict and prosperity are strong and mutually reinforcing. Economic conflict tends to spawn internal conflict, which in turn returns the favour. Moreover, the presence of a recession tends to amplify the extent to which international and external conflicts self-reinforce each other. (Blomberg & Hess, 2002. p. 89) Economic decline has also been linked with an increase in the likelihood of terrorism (Blomberg, Hess, & Weerapana, 2004), which has the capacity to spill across borders and lead to external tensions. Furthermore, crises generally reduce the popularity of a sitting government. "Diversionary theory" suggests that, when facing unpopularity arising from economic decline**,** sitting **governments have increased incentives to fabricate** external military **conflicts to create a 'rally** around the flag' **effect.** Wang (1996), DeRouen (1995). and Blomberg, Hess, and Thacker (2006) find supporting evidence showing that economic decline and use of force are at least indirectly correlated. Gelpi (1997), Miller (1999), and Kisangani and Pickering (2009) suggest that the tendency towards diversionary tactics are greater for democratic states than autocratic states, due to the fact that democratic leaders are generally more susceptible to being removed from office due to lack of domestic support. DeRouen (2000) has provided evidence showing that periods of weak economic performance in the United States, and thus weak Presidential popularity, are statistically linked to an increase in the use of force. In summary, recent economic scholarship positively correlates economic integration with an increase in the frequency of economic crises, whereas political science **scholarship links** economic **decline with** external **conflict** at systemic, dyadic and national levels.5 This implied connection between integration, crises and armed conflict has not featured prominently in the economic-security debate and deserves more attention.

## Advantage 3 is Separation of Powers

#### Congressional restrictions on executive 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.

**Even small violations of separation of powers must be avoided like nuclear war risks**

**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.”

**Interbranch conflict causes war**

Jamison 93

Linda S. Jamison, Deputy Director of Governmental Relations @ CSIS, Spring 1993, 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; ev is gender modified**

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)

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

#### 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.**

**NFU for 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 – fear the consequences

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.

# 2AC

## Modernity K

**3. Prefer pragmatic reform over the utopianism of the alt**

Erik Olin **Wright 2007**, Vilas Distinguished Professor of Sociology at the University of Wisconsin, “Guidelines for Envisioning Real Utopias”, Soundings, April, www.ssc.wisc.edu/~wright/Published%20writing/Guidelines-soundings.pdf

5. Waystations

The final guideline for discussions of envisioning real utopias concerns the importance of waystations. **The central problem of envisioning real utopias concerns the viability of institutional alternatives that embody emancipatory values**, **but the practical achievability of such institutional designs often depends upon the existence of smaller steps, intermediate institutional innovations that move us in the right direction but only partially embody these values.** **Institutional proposals which have an all-or-nothing quality to them are both less likely to be adopted in the first place, and may pose more difficult transition-cost problems if implemented**. **The catastrophic experience of Russia in the “shock therapy” approach to market reform is historical testimony to this problem.** Waystations are a difficult theoretical and practical problem because **there are many instances in which partial reforms may have very different consequences than full- bodied changes**. Consider the example of unconditional basic income. Suppose that a very limited, below-subsistence basic income was instituted: not enough to survive on, but a grant of income unconditionally given to everyone. One possibility is that this kind of basic income would act mainly as a subsidy to employers who pay very low wages, since now they could attract more workers even if they offered below poverty level earnings. There may be good reasons to institute such wage subsidies, but they would not generate the positive effects of a UBI, and therefore might not function as a stepping stone.

**What we ideally want**, therefore, **are intermediate reforms that have two main properties:** first, **they concretely demonstrate the virtues of the fuller program of transformation, so they contribute to the ideological battle of convincing people that the alternative is credible and desirable;** and second, **they enhance the capacity for action of people, increasing their ability to push further in the future**. **Waystations that increase popular participation and bring people together in problem-solving deliberations for collective purposes are particularly salient in this regard**. **This is what in the 1970s was called “nonreformist reforms”**: **reforms that are possible within existing institutions and that pragmatically solve real problems while at the same time empowering people in ways which enlarge their scope of action in the future.**

#### 4. Policy focused debates are necessary to promote more accountable policymaking and increase the educational value of debate – radical activism results in social disengagement and failed intervention

David Chandler. 2007. Professor of International Relations at the Department of Politics and International Relations, University of Westminster –

“The Attraction of Post-Territorial Politics: Ethics and Activism in the International Sphere” – Inaugural Lecture – May – available at: http://www.davidchandler.org/pdf/short\_articles/Inaugural%20lecture.pdf)

However, politics is no less important to many of us today. Politics still gives us a sense of social connection and social rootedness and gives meaning to many of our lives. It is just that the nature and practices of this politics are different. We are less likely to engage in the formal politics of representation - of elections and governments - but in post-territorial politics, a politics where there is much less division between the private sphere and the public one and much less division between national, territorial, concerns and global ones. This type of politics is on the one hand ‘global’ but, on the other, highly individualised: it is very much the politics of our everyday lives – the sense of meaning we get from thinking about global warming when we turn off the taps when we brush our teeth, take our rubbish out for recycling or cut back on our car use - we might also do global politics in deriving meaning from the ethical or social value of our work, or in our subscription or support for good causes from Oxfam to Greenpeace and Christian Aid. I want to suggest that when we do ‘politics’ nowadays it is less the ‘old’ politics, of self-interest, political parties, and concern for governmental power, than the ‘new’ politics of global ethical concerns. I further want to suggest that the forms and content of this new global approach to the political are more akin to religious beliefs and practices than to the forms of our social political engagement in the past. Global politics is similar to religious approaches in three vital respects: 1) global post-territorial politics are no longer concerned with power, its’ concerns are free-floating and in many ways, existential, about how we live our lives; 2) global politics revolve around practices with are private and individualised, they are about us as individuals and our ethical choices; 3) the practice of global politics tends to be non-instrumental, we do not subordinate ourselves to collective associations or parties and are more likely to give value to our aspirations, acts, or the fact of our awareness of an issue, as an end in-itself. It is as if we are upholding our goodness or ethicality in the face of an increasingly confusing, problematic and alienating world – our politics in this sense are an expression or voice, in Marx’s words, of ‘the heart in a heartless world’ or ‘the soul of a soulless condition’. The practice of ‘doing politics’ as a form of religiosity is a highly conservative one. As Marx argued, religion was the ‘opium of the people’ - this is politics as a sedative or pacifier: it feeds an illusory view of change at the expense of genuine social engagement and transformation. I want to argue that global ethical politics reflects and institutionalises our sense of disconnection and social atomisation and results in irrational and unaccountable government policy making. I want to illustrate my points by briefly looking at the practices of global ethics in three spheres, those of radical political activism, government policy making and academia. Radical activism People often argue that there is nothing passive or conservative about radical political activist protests, such as the 2003 anti-war march, anti-capitalism and anti-globalisation protests, the huge march to Make Poverty History at the end of 2005, involvement in the World Social Forums or the radical jihad of Al-Qaeda. I disagree; these new forms of protest are highly individualised and personal ones - there is no attempt to build a social or collective movement. It appears that theatrical suicide, demonstrating, badge and bracelet wearing are ethical acts in themselves: personal statements of awareness, rather than attempts to engage politically with society. This is illustrated by the ‘celebration of differences’ at marches, protests and social forums. It is as if people are more concerned with the creation of a sense of community through differences than with any political debate, shared agreement or collective purpose. It seems to me that if someone was really concerned with ending war or with ending poverty or with overthrowing capitalism, that political views and political differences would be quite important. Is war caused by capitalism, by human nature, or by the existence of guns and other weapons? It would seem important to debate reasons, causes and solutions, it would also seem necessary to give those political differences an organisational expression if there was a serious project of social change. Rather than a political engagement with the world, it seems that radical political activism today is a form of social disengagement – expressed in the anti-war marchers’ slogan of ‘Not in My Name’, or the assumption that wearing a plastic bracelet or setting up an internet blog diary is the same as engaging in political debate. In fact, it seems that political activism is a practice which isolates individuals who think that demonstrating a personal commitment or awareness of problems is preferable to engaging with other people who are often dismissed as uncaring or brain-washed by consumerism. The narcissistic aspects of the practice of this type of global politics are expressed clearly by individuals who are obsessed with reducing their carbon footprint, deriving their idealised sense of social connection from an ever increasing awareness of themselves and by giving ‘political’ meaning to every personal action. Global ethics appear to be in demand because they offer us a sense of social connection and meaning while at the same time giving us the freedom to construct the meaning for ourselves, to pick our causes of concern, and enabling us to be free of responsibilities for acting as part of a collective association, for winning an argument or for success at the ballot-box. While the appeal of global ethical politics is an individualistic one, the lack of success or impact of radical activism is also reflected in its rejection of any form of social movement or organisation. Strange as it may seem, the only people who are keener on global ethics than radical activists are political elites. Since the end of the Cold War, global ethics have formed the core of foreign policy and foreign policy has tended to dominate domestic politics. Global ethics are at the centre of debates and discussion over humanitarian intervention, ‘healing the scar of Africa’, the war on terror and the ‘war against climate insecurity’. Tony Blair argued in the Guardian last week that ‘foreign policy is no longer foreign policy’ (Timothy Garten Ash, ‘Like it or Loath it, after 10 years Blair knows exactly what he stands for’, 26 April 2007), this is certainly true. Traditional foreign policy, based on strategic geo-political interests with a clear framework for policy-making, no longer seems so important. The government is down-sizing the old Foreign and Commonwealth Office where people were regional experts, spoke the languages and were engaged for the long-term, and provides more resources to the Department for International Development where its staff are experts in good causes. This shift was clear in the UK’s attempt to develop an Ethical Foreign Policy in the 1990s – an approach which openly claimed to have rejected strategic interests for values and the promotion of Britain’s caring and sharing ‘identity’. Clearly, the projection of foreign policy on the basis of demonstrations of values and identity, rather than an understanding of the needs and interests of people on the ground, leads to ill thought-through and short-termist policy-making, as was seen in the ‘value-based’ interventions from Bosnia to Iraq (see Blair’s recent Foreign Affairs article, ‘A Battle for Global Values’, 86:1 (2007), pp.79–90). Governments have been more than happy to put global ethics at the top of the political agenda for - the same reasons that radical activists have been eager to shift to the global sphere – the freedom from political responsibility that it affords them. Every government and international institution has shifted from strategic and instrumental policy-making based on a clear political programme to the ambitious assertion of global causes – saving the planet, ending poverty, saving Africa, not just ending war but solving the causes of conflict etc – of course, the more ambitious the aim the less anyone can be held to account for success and failure. In fact, the more global the problem is, the more responsibility can be shifted to blame the US or the UN for the failure to translate ethical claims into concrete results. Ethical global questions, where the alleged values of the UN, the UK, the ‘civilised world’, NATO or the EU are on the line in ‘wars of choice’ from the war on terror to the war on global warming lack traditional instrumentality because they are driven less by the traditional interests of Realpolitik than the narcissistic search for meaning or identity. Governments feel the consequences of their lack of social connection, even more than we do as individuals; it undermines any attempt to represent shared interests or cohere political programmes. As Baudrillard suggests, without a connection to the ‘represented’ masses, political leaders are as open to ridicule and exposure as the ‘Emperor with no clothes’ (In the Shadow of the Silent Majorities, New York: Semiotext(e), 1983, for example). It is this lack of shared social goals which makes instrumental policy-making increasingly problematic. As Donald Rumsfeld stated about the war on terror, ‘there are no metrics’ to help assess whether the war is being won or lost. These wars and campaigns, often alleged to be based on the altruistic claim of the needs and interests of others, are demonstrations and performances, based on ethical claims rather than responsible practices and policies. Max Weber once counterposed this type of politics – the ‘ethics of conviction’ – to the ‘ethics of responsibility’ in his lecture on ‘Politics as a Vocation’. The desire to act on the international scene without a clear strategy or purpose has led to highly destabilising interventions from the Balkans to Iraq and to the moralisation of a wide range of issues from war crimes to EU membership requirements. Today more and more people are ‘doing politics’ in their academic work. This is the reason for the boom in International Relations study and the attraction of other social sciences to the global sphere. I would argue that the attraction of IR for many people has not been IR theory but the desire to practice global ethics. The boom in the IR discipline has coincided with a rejection of Realist theoretical frameworks of power and interests and the sovereignty/anarchy problematic. However, I would argue that this rejection has not been a product of theoretical engagement with Realism but an ethical act of rejection of Realism’s ontological focus. It seems that our ideas and our theories say much more about us than the world we live in. Normative theorists and Constructivists tend to support the global ethical turn arguing that we should not be as concerned with ‘what is’ as with the potential for the emergence of global ethical community. Constructivists, in particular, focus upon the ethical language which political elites espouse rather than the practices of power. But the most dangerous trends in the discipline today are those frameworks which have taken up Critical theory and argue that focusing on the world as it exists is conservative ‘problem-solving’ while the task for critical theorists is to focus on emancipatory alternative forms of living or of thinking about the world. Critical thought then becomes a process of wishful thinking rather than one of engagement, with its advocates arguing that we need to focus on clarifying our own ethical frameworks and biases and positionality before thinking about or teaching on world affairs; in the process this becomes ‘me-search’ rather than research. We have moved a long way from Hedley Bull’s perspective that, for academic research to be truly radical, we had to put our values to the side to follow where the question or inquiry might lead. The inward-looking and narcissistic trends in academia, where we are more concerned with our ‘reflectivity’ – the awareness of our own ethics and values - than with engaging with the world, was brought home to me when I asked my IR students which theoretical frameworks they agreed with most and they replied mostly Critical theory and Constructivism despite the fact that they thought that states operated on the basis of power and self-interest in a world of anarchy. Their theoretical preferences were based more on what their choices said about them as ethical individuals than about how theory might be used to understand and engage with the world.

#### 5. Debating about specific policies is essential to promote more ethical and accountable policymaking – their abstract politics promotes disengagement and poor argumentation skills

David Chandler. 2007. Centre for the Study of Democracy, Westminster, Area, Vol. 39, No. 1, p. 118-119

This disjunction between the human/ethical/global causes of post-territorial political activism and the capacity to 'make a difference' is what makes these individuated claims immediately abstract and metaphysical – there is no specific demand or programme or attempt to build a collective project. This is the politics of symbolism. The rise of symbolic activism is highlighted in the increasingly popular framework of 'raising awareness'– here there is no longer even a formal connection between ethical activity and intended outcomes (Pupavac 2 006). Raising awareness about issues has replaced even the pretense of taking responsibility for engaging with the world – the act is ethical in-itself. Probably the most high profile example of awareness raising is the shift from Live Aid, which at least attempted to measure its consequences in fund-raising terms, to Live 8 whose goal was solely that of raising an 'awareness of poverty'. The struggle for 'awareness' makes it clear that the focus of symbolic politics is the individual and their desire to elaborate upon their identity – to make us aware of their 'awareness', rather than to engage us in an instrumental project of changing or engaging with the outside world. It would appear that in freeing politics from the constraints of territorial political community there is a danger that political activity is freed from any constraints of social mediation (see further, Chandler 2004a). Without being forced to test and hone our arguments, or even to clearly articulate them, we can rest on the radical 'incommunicability' of our personal identities and claims – you are 'either with us or against us'; engaging with those who disagree is no longer possible or even desirable. It is this lack of desire to engage which most distinguishes the unmediated activism of post-territorial political actors from the old politics of territorial communities, founded on struggles of collective interests (Chandler 2004b). The clearest example is old representational politics – this forced engagement in order to win the votes of people necessary for political parties to assume political power. Individuals with a belief in a collective programme knocked on strangers' doors and were willing to engage with them, not on the basis of personal feelings but on what they understood were their potential shared interests. Few people would engage in this type of campaigning today; engaging with people who do not share our views, in an attempt to change their minds, is increasingly anathema and most people would rather share their individual vulnerabilities or express their identities in protest than attempt to argue with a peer.This paper is not intended to be a nostalgic paean to the old world of collective subjects and national interests or a call for a revival of territorial state-based politics or even to reject global aspirations: quite the reverse. Today, politics has been 'freed' from the constraints of territorial political community – governments without coherent policy programmes do not face the constraints of failure or the constraints of the electorate in any meaningful way; activists, without any collective opposition to relate to, are free to choose their causes and ethical identities; protest, from Al Qaeda, to anti-war demonstrations, to the riots in France, is inchoate and atomized. When attempts are made to formally organize opposition, the ephemeral and incoherent character of protest is immediately apparent.

**b. Ontology has no political impact**

**Srnicek 09** [Nick, Ph.D Candidate in International Relations @ the London School of Economics, “Notes on Ontology and Politics,” http://accursedshare.blogspot.com/2009/01/some-notes-on-ontology-and-politics.html]

It seems to me that one of the most contentious and unremarked upon effects of speculative realism has to do with its attack on a piece of continental dogma – namely **the presupposition that ontology is necessarily political**. This idea **is seen in any number of** continental **works**, **from Deleuze’s** constructivism, **to Derrida**’s deconstructions of presence, **to the social constructivists, gender and identity theorists**, among others. The basic idea being that ontology is always constructed through a political battle, a conflict over what exists. In this regards, the contribution of continental work was to undermine the notion that what exists can be definitively determined in an essential way. The problem was that **they went too far** with this line of thought **and tended** (I say tended, because there are almost always exceptions) **to deny the independence of ontology from politics**. In many cases, ontology even became passé, a mere relic of classical philosophy. These ideas, unsurprisingly, came along necessarily with the general acceptance of correlationism – if we can’t speak or know of anything independent of its manifestation to us, then every thing is necessarily already wrapped up in our political relations. With speculative realism, however, this situation changes. The turn towards objects, towards the absolute, and towards the real as indifferent, all imply that **ontology must be independent of politics**. We can see this most clearly in Brassier’s work, I believe (although it is implicit in all of them). The relative absence of politics in Nihil Unbound stems partly from the belief that we can study ontology without having to be concerned about its political effects. The results of such a study, as in Brassier’s work, can be rather disconcerting for politics – what if there is no such thing as agency? – but this alone fails to discredit the arguments for such a position. So what does the separation of politics and ontology entail? A few hesitant and suggestive remarks might begin to make clear what precisely is at stake for any speculative realist politics**... The separation entails**, first of all, that **an ontology cannot be validated in terms of its political effects**. Part of Badiou’s greatness is undoubtedly to have rejuvenated the concept of the subject, but when judging his ontology, we have to do so while bracketing these political effects. Similarly, when studying the results of neuroscience and their political implications, we must be careful not to reject them simply because they don't accord with our fundamental beliefs about ourselves. If it turns out that we are no more than patterns of neurons firing, this is a reality whose effective truth holds sway regardless of our political desires. (As an aside, I think that such an idea needs to reject Levi's 'Principle of Irreduction', as there are scientific examples of entities being reduced to other entities. The basic argument against such a principle being that we can be mistaken about how the difference an entity makes, makes that difference.) The second effect is that **we can no longer construct an ontology in order to achieve some political goal. We may wish to privilege difference as a counter to constricting identity formations, but we cannot justify this privileging with political arguments.** Rather, properly philosophical arguments need to be marshaled in support of these ideas. (This raises the important question of whether philosophy can ever be distinguished from politics completely, but the linguistic intermingling of the two need not entail their necessary correlation outside of language.) A third and similar point is that **an ontology cannot dictate a political program. Difference may be privileged**, for example, **but this can be taken in the direction of a capitalist individualism or the direction of undermining traditional power relations** - a realist ontology will allow for a multitude of political projects to be spawned from it, without necessarily being liberating or progressive (or constraining or conservative). The fourth effect is a little more radical, I think. This is a renunciation of the tendency among continental theorists to place their political arguments in terms of ontology – I’m thinking here of things like Badiou and the uncounted, Rancière and the people, Deleuze and the minor, etc. The common thread being that the collective agency for political change is always determined in terms of its ontological status – what is inexistent, or uncounted, or unactualized. But political change need not require that something fundamentally new come into being. **There can be real political progress made without having to generate ontological novelty**. (I’ll also mention too that the faith in the New tends to be another continental political dogma. As though the New was necessarily progressive. While the New may be considered an ontological category, its political content is entirely underdetermined by ontological reasoning.)

**c.Ontology first is bogus – no warrant**

**Jackson 10**

Patrick Thaddeus Jackson, 2010. Associate Professor of International Relations in the School of International Service at the American University in Washington, DC. “The Conduct of Inquiry in International Relations: Philosophy of Science and its Implications for the Study of World Politics,” p 27-8.

However, I do not think that putting ontology first in the panacea that many seem to think it is. For one thing**, if one puts ontology first then one is, at least provisionally, committed to a particular** (if revisable) **account of what the world is made up of**: co-constituted agents and structures, states interacting under conditions of anarchy, global class relations, or what have you. **This is a rather large leap to make on anyone’s authority**, let alone that of a philosopher of science. Along these lines**, it is unclear what if any *warrant* we could provide for most ontological claims if ontology in this sense were to always “come first.”** **If someone makes an ontological claim about something existing in the world, then we are faced with an intriguing epistemological problem of how possibly to know whether that claim is true, and the equally intriguing problem of selecting the proper methods to use in evaluating that claim** (Chernoff 2009b, 391). **But if epistemology and method are supposed to be fitted to ontology, then we are stuck with techniques and standards designed to respond to the specificity of the object under investigation**. This problem is roughly akin to using state-centric measurements of cross-border transactions to determine whether globalization is eroding state borders, because the very object under investigation—“state borders”—is presupposed by the procedures of data collection, meaning that the answer will always, and necessarily, assert the persistence of the state.

**8. a. Life should be valued as apriori – it precedes the ability to value anything else**

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

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

**b. Existence precedes the ability to ascribe value [and respect the other]**

Paul **Wapner. 2003.** Associate Prof. and Dir. Global Env’t. Policy Prog. – American U., Dissent, “Leftist criticism of “nature””, Winter, 50:1.

All attempts to listen to nature are social constructions--except one. **Even the most radical postmodernist must acknowledge the distinction between physical existence and nonexistence**. As I have said, postmodernists accept that there is a physical substratum to the phenomenal world even if they argue about the different meanings we ascribe to it. This acknowledgment of physical existence is crucial. **We can't ascribe meaning to that which doesn't appear. What doesn't exist can manifest no character**. Put differently, yes, the postmodernist should rightly worry about interpreting nature's expressions. And all of us should be wary of those who claim to speak on nature's behalf (including environmentalists who do that). But we need not doubt the simple idea that **a prerequisite of expression is existence**. This in turn suggests that **preserving the nonhuman world-in all its diverse embodiments-must be seen** by eco-critics **as a fundamental good**. Eco-critics must be supporters, in some fashion, of environmental preservation. Postmodernists reject the idea of a universal good. They rightly acknowledge the difficulty of identifying a common value given the multiple contexts of our value-producing activity. In fact, if there is one thing they vehemently scorn, it is the idea that there can be a value that stands above the individual contexts of human experience. Such a value would present itself as a metanarrative and, as Jean Francois Lyotard has explained, postmodernism is characterized fundamentally by its "incredulity toward meta-narratives." Nonetheless, I can't see how postmodern critics can do otherwise than accept the value of preserving the nonhuman world. The nonhuman is the extreme "other"; it stands in contradistinction to humans as a species. In understanding the constructed quality of human experience and the dangers of reification, postmodernism inherently advances an ethic of respecting the "other." At the very least, **respect must involve ensuring that the "other" actually continues to exist**. In our day and age, **this requires us to take responsibility for protecting the actuality of the nonhuman**. Instead, however, we are running roughshod over the earth's diversity of plants, animals, and ecosystems. Postmodern critics should find this particularly disturbing. If they don't, they deny their own intellectual insights and compromise their fundamental moral commitment.

**c. Give people the choice to live**

**Paterson 3** Craig, Department of Philosophy, Providence College, Rhode Island “A Life Not Worth Living?”, Studies in Christian Ethics, <http://sce.sagepub.com>

In determining whether a life is worth living or not, **attention should be focused upon an array of ‘interests’ of the person**, and these, for the competent patient at least, are going to vary considerably, since they will be informed by the patient’s underlying dispositions, and, for the incompetent, by a minimal quality threshold. It follows that for competent patients, a broad-ranging assessment of quality of life concerns is the trump card as to whether or not life continues to be worthwhile. Different patients may well decide differently. **That is the prerogative of the patient**, for the only unpalatable alternative is to force a patient to stay alive. For Harris, life can be judged valuable or not when the person assessing his or her own life determines it to be so. **If a person values his or her own life, then that life is valuable, precisely to the extent that he or she values it**. Without any real capacity to value, there can be no value. As Harris states, ‘. . . the value of our lives is the value we give to our lives’. It follows that the **primary injustice** done to a person is to **deprive the person of a life he or she may think valuable**. Objectivity in the value of human life, for Harris, essentially becomes one of negative classification (ruling certain people out of consideration for value), allied positively to a broad range of ‘critical interests’; interests worthy of pursuing — **friendships, family, life goals, etc**. — which are subjected to de facto **self-assessment** for the further determination of meaningful value. Suicide, assisted suicide, and voluntary euthanasia, can therefore be justified, on the grounds that once the competent nature of the person making the decision has been established, the thoroughgoing commensuration between different values, in the form of interests or preferences, is essentially left up to the individual to determine for himself or herself.

**d. Life has intrinsic and objective value achieved through subjective pleasures---its preservation should be an a priori goal**

Amien **Kacou 8** WHY EVEN MIND? On The A Priori Value Of “Life”, Cosmos and History: The Journal of Natural and Social Philosophy, Vol 4, No 1-2 (2008) cosmosandhistory.org/index.php/journal/article/view/92/184

Furthermore, **that manner of finding things good that is in pleasure can certainly not exist in any world without consciousness (i.e., without “life,” as we now understand the word)**—slight analogies put aside. In fact, we can begin to develop a more sophisticated definition of the concept of “**pleasure**,” in the broadest possible sense of the word, as follows: it **is the common psychological element in all psychological experience of goodness** (be it in joy, admiration, or whatever else). In this sense, pleasure can always be pictured to “mediate” all awareness or perception or judgment of goodness: **there is pleasure in all consciousness of things good; pleasure is the common element of all conscious satisfaction**. In short, **it is simply the very experience of liking things,** or the liking of experience, in general. In this sense, **pleasure is**, not only uniquely characteristic of life but also, **the core expression of goodness in life—the most general sign or phenomenon for favorable conscious valuation, in other words. This does not mean that “good” is absolutely synonymous with “pleasant”—what we value may well go beyond pleasure**. (The fact that we value things needs not be reduced to the experience of liking things.) **However, what we value beyond pleasure remains a matter of speculation or theory.** Moreover, we note that a variety of things that may seem otherwise unrelated are correlated with pleasure—some more strongly than others. In other words, **there are many things the experience of which we like.** For example: **the admiration of others; sex; or rock-paper-scissors**. But, again, **what they are is irrelevant in an inquiry on a priori value**—what gives us pleasure is a matter for empirical investigation.

**Thus, we can see now that**, in general, **something primitively valuable is attainable in living—that is, pleasure itself. And it seems equally clear that we have a priori logical reason to pay attention to the world in any world where pleasure exists**. **Moreover, we can now also articulate a foundation for a security interest in our life: since the good of pleasure can be found in living (**to the extent pleasure remains attainable),[17] **and only in living, therefore, a priori, life ought to be continuously (and indefinitely) pursued at least for the sake of preserving the possibility of finding that good**.

However, this platitude about the value that can be found in life turns out to be, at this point, insufficient for our purposes. It seems to amount to very little more than recognizing that our subjective desire for life in and of itself shows that **life has some objective value. For what difference is there between saying, “living is unique in benefiting something I value (namely, my pleasure); therefore, I should desire to go on living,” and saying, “I have a unique desire to go on living; therefore I should have a desire to go on living,**” whereas the latter proposition immediately seems senseless? In other words, “life gives me pleasure,” says little more than, “I like life.” Thus, **we seem to have arrived at the conclusion that the fact that we already have some (subjective) desire for life shows life to have some (objective) value**. But, if that is the most we can say, then it seems our enterprise of justification was quite superficial, and the subjective/objective distinction was useless—for all we have really done is highlight the correspondence between value and desire. Perhaps, our inquiry should be a bit more complex.

**f. Extinction outweighs ethics**

**Bok 88** (Sissela Bok, Professor of Philosophy @ Brandeis University, 1988, Applied Ethical Theory, ed. Rosenthal and Shehadi, pg. 203)

The same argument can be made for Kant’s other formulations of the Categorical Imperative: “So act as to use humanity, both in your own person and in the person of every other, always at the same time as an end, never simply as a means”; and “So act as if you were always through your actions a law-making member in a universal kingdom of Ends.” **No one with a concern for humanity** could consistently **will** to **risk eliminating humanity** in the person of himself and every other or to risk the death of all members in a universal Kingdom of Ends **for the sake of justice. To risk** their **collective death for the sake of following one’s conscience would be** as Rawls said, “**irrational, crazy**,” And **to say that one did not intend such a catastrophe**, but that one merely failed to stop other persons from bringing it about **would be beside the point when the end of the world was at stake.** For although it is true that we cannot be held responsible for most of the wrongs that others commit, the Latin maxim presents a case where **we would have to take such a responsibility seriously** – perhaps **to the point of deceiving, bribing, even killing an innocent person, in order that the world not perish**. To avoid self-contradiction, the Categorical imperative would, therefore, have to rule against the Latin maxim on account of its cavalier attitude toward the survival of mankind. But the ruling would then produce a rift in the application of the Categorical Imperative. Most often the Imperative would ask us to disregard all unintended but foreseeable consequences, such as the death of innocent persons, whenever concern for such consequences conflicts with concern for acting according to duty. But, in the extreme case, **we** might **have to go against even the strictest moral duty** precisely **because of the consequences**.

**Human life has inherent value – arguing otherwise is a slippery slope to slavery and eugenics**

Melinda **Penner** (Director of Operations – STR, Stand To Reason) **2005** “End of Life Ethics: A Primer”, Stand to Reason, http://www.str.org/site/News2?page=NewsArticle&id=5223

Intrinsic value is very different. Things with intrinsic value are valued for their own sake. They don’t have to achieve any other goal to be valuable. They are goods in themselves. Beauty, pleasure, and virtue are likely examples. Family and friendship are examples. Something that’s intrinsically valuable might also be instrumentally valuable, but even if it loses its instrumental value, its intrinsic value remains. **Intrinsic value is what people mean when they use the phrase "the sanctity of life." Now when someone argues that someone doesn’t have "quality of life" they are arguing that life is only valuable as long as it obtains something else with quality, and when it can’t accomplish this, it’s not worth anything anymore. It's only instrumentally valuable. The problem with this view is that it is entirely subjective and changeable with regards to what might give value to life**. Value becomes a completely personal matter, and, as we all know, our personal interests change over time. **There is no grounding for objective human value and human rights if it’s not intrinsic value. Our legal system is built on the notion that humans have intrinsic value**. The Declaration of Independence: "We hold these truths to be self-evident, that all men are created equal, that each person is endowed by his Creator with certain unalienable rights...." **If human beings only have instrumental value, then slavery can be justified because there is nothing objectively valuable that requires our respect. There is nothing other than intrinsic value that can ground the unalienable equal rights we recognize because there is nothing about all human beings that is universal and equal. Intrinsic human value is what binds our social contract of rights. So if human life is intrinsically valuable, then it remains valuable even when our capacities are limited. Human life is valuable even with tremendous limitations. Human life remains valuable because its value is not derived from being able to talk, or walk, or feed yourself, or even reason at a certain level. Human beings don’t have value only in virtue of states of being (e.g., happiness) they can experience. The "quality of life" view is a poison pill because once we swallow it, we’re led down a logical slippery slope**. The exact same principle can be used to take the life of human beings in all kinds of limited conditions because I wouldn't want to live that way. Would you want to live the life of a baby with Down’s Syndrome? No? Then kill her. Would you want to live the life of an infant with cerebral palsy? No? Then kill him. Would you want to live the life of a baby born with a cleft lip? No? Then kill her. (In fact, they did.) **Once we accept this principle, it justifies killing every infant born with a condition that we deem a life we don’t want to live. There’s no reason not to kill every handicapped person who can’t speak for himself — because I wouldn’t want to live that way.** This, in fact, is what has happened in Holland with the Groningen Protocol. Dutch doctors euthanize severely ill newborns and their society has accepted it.

# 1AR

#### Their human rights claims are just a Kantian modification of the Westphalian model of legitimate war which masks the species war in order to achieve its idea of the good life

KOCHI 2K9 [tarik, lecturer in law and international security @ U of Sussex, Doctorate in Law from Griffith, “species war: law, violence, and animals”, ‘law, culture, and the humanities’, 353-359]

Modern international humanitarian law both inherits aspects of the Westphalian system and moves beyond it. While international humanitarian or human rights law still relies upon the sovereignty of nation-states and accepts to a limited degree the state’s right to go to war and its internal monopoly upon the legitimacy of violence, each of these forms of right are re-shaped and limited in accordance with a higher standard of legitimacy located around the ideals of international peace and the cosmopolitan concept of “humanity.” By attempting to place “human rights” as a category that stands above or at least challenges the traditional rights of the state, inter- national humanitarian law morally orders war and sets out a cosmopolitan and global conception of the good life. While the category of peace is held onto, survival is displaced by human rights as the central category for deriving the legitimacy of the international order and the legitimacy of war. Of course, the category of survival is not erased completely as the human-animal dis- tinction of species war continues to operate at a subterranean level. One of the first thinkers to sketch out the theoretical justifications for such a re-ordering of inter-state relations and the legitimacy of global violence was Immanuel Kant.32 In proposing a universal moral theory which attempted to equally value all members of humanity, Kant rejected the way in which previous Western intellectual traditions had legitimated particular forms of violence and killing by valuing the lives of Europeans over non-Europeans. Further, Kant challenged the over-valuation of the “life” of the state against the lives of humans in general. In re-thinking the relation between war and law Kant enunciated a form of sovereignty located around the idea of humanity. On the basis of this higher and universal right of humanity Kant’s approach demanded that state action be guided by moral reasoning and moral duty and in this respect Kant asked that the juridical persona of states adopt a distinctly moral persona – states are conceptualized and expected to act as if they are moral persons.33