# 1AC

### Plan

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

### Adv 1 – Preemption

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

**Gjelten 13**

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

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

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

**Walsh 11**

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

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

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

**Fritz 9**

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

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

**3rd party actors takes out their defense- undermines attribution, repair, deterrence, and escalation control**

**Libicki 09**

Matthew Libicki, Ph.D, senior management scientist at RAND, “CYBERDETERRENCE AND CYBERWAR,” 2009, <http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf> SJE

**An exchange of cyberattacks** between states **may** also **excite the general interest of superpatriot hackers or those who like a dog pile**— particularly if the victim of the attack or the victim of retaliation, or both, are unpopular in certain circles. The very nature of the attacks is likely to reveal the victim’s general vulnerabilities (X is not impregnable) and perhaps even specific vulnerabilities (this is how to get into X). They put certain assets “in play” in the same sense that a takeover bid for a corporation makes it a feasible target for others. Both attacker and retaliator may have to face the possibility that **third-party hackers may continue to plague the target even after the original attacker has pulled back**. Outside participation matters because **hacking is one of the activities in which third parties can play in the same league as states**.30 Software, after all, comes from the commercial world; it is broken by individual hackers and repaired by other individual hackers. It is not unknown for single individuals to break copyright locks that corporations put into the market.31 States may have a larger panoply of attack methods than individuals do, but that is of little help in determining whether a state or an individual carried out a single particular attack. **The emergence of third-party hackers could further complicate attribution and make it difficult to understand the relationships among attack, retaliation, and counterretaliation. The prospect that attacks may continue after the attacker and the target have found out how to live with one another will complicate efforts to restore status quo conditions or even promise as much as a condition to cease hostilities**.**32 All this weakens an implied promise of deterrence: If you stop, we stop. With the existence of third-party hackers, the “we” loses its strength. What attackers want to hear—if you stop, it stops—may not be something the retaliator can promise**. Fortunately, third-party attackers may strengthen an implied threat of deterrence: Do not even start because who knows where it will lead

#### We control the uniqueness- terrorists lack the capacity for large scale attacks now, but could acquire it from states

Powers 9-2

Sam Powers, Institute of Terrorism Research and Response, “The Threat of Cyberterrorism to Critical Infrastructure,” 9/2/13, <http://www.e-ir.info/2013/09/02/the-threat-of-cyberterrorism-to-critical-infrastructure/> SJE

Terrorist organizations have demonstrated their expertize on the web in various forms for over a decade. As the recent attacks by the Tsarnaev brothers in Boston highlights, video broadcasts over social media, for example, serve as one of the many ways by which terrorist groups can recruit members and spur “lone wolf” actors to commit terrible atrocities.[26] While dissemination of propaganda and other such activity is malicious and may eventually lead to an act of terrorism taking place, acts such as small scale hacking for financial gain, temporarily paralyzing non critical websites and spreading of propaganda, do not constitute cyberterrorism.[27] What is worrisome, however, is that over the past 10 years in particular, trends have emerged that illustrate that al-Qaeda and other terrorists have taken an interest in directing their cyber capabilities towards directly hitting US infrastructure and causing mass damage. We have also learned, and have seen from example, that attacks can be orchestrated without massive funding, by single actors, who are not even affiliated with a terrorist group.[28] In her book Computer Forensics: Cybercriminals, Laws and Evidence, Marie-Helen Maras provides various examples of such instances where “lone wolves” were able to break into SCADA systems, and if they so desired, could have created massive damage. For example, in 2000, a Russian man hacked into an ICS that ran a natural gas pipeline and was able to control the flow of LNG. “Hypothetically, this hacker could have easily increased the gas pressure until the valves broke, causing an explosion to occur.”[29] Although many of these actors have been “lone wolves,” terrorist organizations have not sat on the sidelines idly. Rather, since the new millennium, terrorist groups such as al-Qaeda, and groups supported by Iran like Hamas and Hezbollah, have been actively working towards developing a capacity to strike at the heart of the industrialized world’s critical infrastructure to cause terror and havoc. [30] Former Presidential Adviser for Cyberspace Security, Richard Clarke expresses his concern on the terrorist entrée into the world of cyberwar in a PBS Frontline special. Clarke comments: We also found indications that members of al-Qaeda were from outside of the Unites States doing reconnaissance in the United States on our critical infrastructure. Where were railroad crossings? Where were the big natural gas depositories? Where were the bridges over rivers that also carried the fiber for the backbone on the Internet? It’s possible now to do that kind of targeting, which would have, in the past, required lots of people and running around the country. It is possible to sit in the cyber café in Peshawar and do that kind of reconnaissance. The sentiment of Clarke and others is quite telling in the sense that it not only drives home the al-Qaeda and other terrorists seek the desire to destroy US infrastructure, but that they are slowly gaining the capacity to carry out such attacks. Al-Qaeda members have been tracked seeking information on SCADA systems in the US including wastewater and water supply facilities. In 2005, the al-Farouq web forum exposed a “hacker library” with information that could aid an individual in debilitating and an electric system with a keystroke.[31] In addition, in 2003 an al-Qaeda affiliate built upon an emerging trend in the US and developed an online university for “Jihad Sciences on the Internet,” to instruct students on proper ways to fight electronic Jihad.[32] This sustained desire to wreak havoc on the infrastructure of western nations has thankfully yet to play out. The sophistication to carry out such a large-scale attack is hard to develop and requires substantial funding. There are, however, nation states that are willing to support such ambitions.

#### 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.**¶ Everyone agrees on the need to curb this race by creating proper norms of network behavior. But like Clinton, U.S. cybersecurity policymakers are in the habit of thinking too much about those who attack us and too little about our attacks on others. Creating norms to curb cyberattacks is difficult enough because the attackers' identities are hard to ascertain. But **a**nother large **hurdle is the federal government's refusal to acknowledge more fully its many offensive cyber activities**, or to propose which such activities it might clamp down on in exchange for reciprocal concessions by our adversaries.

#### C) Norms elicit positive responses from non-state actors- allows 3rd parties to increase influence through compliance

Thomas ‘2

[Daniel C. Thomas, University of Illinois at Chicago. “Boomerangs and Superpowers: International Norms, Transnational Networks and US Foreign Policy.” Cambridge Review of International Affairs, Volume 15, Number 1, 2002. ETB]

This evolution in international relations theory includes growing recognition that the **creation of** formal international **norms by state actors facilitates** (often inadvertently) **the political mobilisation of non-state actor**s.5 **By** **identifying with the** purposes of an international **norm**, **non-state actors legitimate their demands, gain access to state decision makers, and thus gain greater influence over state policy**. In some cases, **they may publicise a state’s non-compliance with its obligations under the norm in question**. In other cases, **they may pressure a state that is already in compliance to exert its in􏰝uence on non-compliant states**. **The ‘boomerang effect’ refers to situations where non-state actors apply this strategy transnationally in order to circumvent blocked domestic opportunities for pro- test**.6 International norms thus help non-state actors to create transnational networks capable of reshaping the conceptions of self-interest driving state behaviour.

#### D) Binding restrictions are key- the mere fear of preemptive cyberattack raises hair triggers and locks in structural instability

**Morgan 2010**

(Patrick M. Morgan, Tierney Chair, Peace & Conflict, Political Science School of Social Sciences PH.D., Yale University, “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,” Proceedings of a Workshop on Deterring Cyber Attacks, http://www.lawfareblog.com/wp-content/uploads/2012/02/morgan.pdf)

On the other hand, since they will likely not be readily visible, **the emergence of capabilities for** ¶ disarming or otherwise **very crippling preemptive cyberattacks will be a real nightmare**, and just the ¶ possibility of this is therefore very disturbing. Indications that this might be happening will cause alarm ¶ not just for the actors involved but also for broader stability in international politics. **Both a potential** ¶ **attacker and the target would have to prepare for the worst.** This could lead governments basing ¶ defensive and retaliatory preparations on the opponent’s hypothetical attack capabilities, with each side ¶ operating from what it infers, on the basis of its own research, cybersystems, and espionage efforts, ¶ about what the opponent has.32 **With cyberattacks more feasible and more readily mounted** (given the ¶ right secret preparations) **with little transparency, this could sharply escalate the hair trigger nature of** ¶ **serious confrontations via the reciprocal fear of surprise attack. Mutual cyber first-strike capabilities** ¶ **would set up the severe structural instability once again** (the crisis stability problem) of states racing to ¶ use them first before they could be lost in an enemy attack, the instability exacerbated if each opponent ¶ was uncertain how advanced the other side’s capabilities were and turned to a worst-case analysis.

### Adv 2 - Trade off

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

Francis ‘13

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

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

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

**Healey ‘13**

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

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

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

**Rid 2/4**

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

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

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

**Gjelten, 13**

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

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

#### 2 impacts:

#### First, cyberwar:

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

**McGraw 13**

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

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

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

**Clark and Andreasen 13**

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

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

#### Escalation is rapid and global

VOA News ‘12

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

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

#### Second, cyber crime

**Defense solves it**

**McGraw 13**

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

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

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

Sani et al 12

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

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

#### Economic collapse causes nuclear conflicts

Burrows and Harris 9

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

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

### Adv 3 - SOP

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

**Lorber 13**

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

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

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

**Strong separation of powers key to heg**

**Ikenberry 1**

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

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

**Heg solves great power wars**

**Barnett 11**

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

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

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

**Taylor- Robinson and Ura 12**

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

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

**Interbranch conflict causes extinction**

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**

Forrester 89

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

\*evidence is gendered modified

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

### Solvency

#### 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.**

#### Obama will adhere to the plan- fear of political consequences

**Bradley and Morrison ‘13**

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

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

# 2AC

**Preemption**

**Threats are not socially constructed- decision makers use the most objective, rational, and accurate assessments possible- there are no bureaucratic or ideological motivations to invent threats.**

**Ravenal ‘9**

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

Quite expectedly, the more doctrinaire of the non-interventionists take pains to deny any straightforward, and therefore legitimate, security motive in American foreign and military policy. In fact, this denial leads to a more sweeping rejection of any recognizably rational basis for American foreign policy, and, even, sometimes (among the more theoretical of the non-interventionists), a preference for non-rational accounts, or “models,” of virtually any nation’s foreign policy-making.4 One could call this tendency among anti-imperialists “motive displacement.” More specifically, in the cases under review here, one notes a receptivity to any reworking of history, and any current analysis of geopolitics, that denigrates “the threat”; and, along with this, a positing of “imperialism” (the almost self-referential and primitive impulse) as a sufficient explanation for the often strenuous and risky actions of great powers such as the United States. Thus, not only is “empire” taken to be a sufficient and, in some cases, a necessary condition in bringing about foreign “threats”; but, by minimizing the extent and seriousness of these threats, the anti-imperialists put themselves into the position of lacking a rational explanation for the derivation of the (pointless at best, counter-productive at worst) policies that they designate as imperialistic. A pungent example of this threat denigration and motive displacement is Eland’s account of American intervention in the Korean and Vietnam wars:

After North Korea invaded, the Truman administration intervened merely for the purpose of a demonstration to friends and foes alike. Likewise, according to eminent cold war historians, the United States did not inter- vene in Vietnam because it feared communism, which was fragmented, or the Soviet Union, which wanted détente with the West, or China, which was weak, but because it did not want to appear timid to the world. The behavior of the United States in both Korea and Vietnam is typical of imperial powers, which are always concerned about their reputation, pres- tige, and perceived resolve. (Eland 2004, 64)

Of course, the motive of “reputation,” to the extent that it exists in any particular instance, is a part of the complex of motives that characterize a great power that is drawn toward the role of hegemon (not the same thing as “empire”). Reputation is also a component of the power projec- tion that is designed to serve the interest of national security. Rummaging through the concomitants of “imperialism,” Eland (2004, 65) discovers the thesis of “threat inflation” (in this case, virtual threat invention): Obviously, much higher spending for the military, homeland security, and foreign aid are required for a policy of global intervention than for a policy of merely defending the republic. For example, after the cold war, the security bureaucracies began looking for new enemies to justify keeping defense and intelligence budgets high. Similarly, Eland (ibid., 183), in a section entitled “Imperial Wars Spike Corporate Welfare,” attributes a large portion of the U.S. defense budget—particularly the procurement of major weapons systems, such as “Virginia-class submarines . . . aircraft carriers . . . F-22 fighters . . . [and] Osprey tilt-rotor transport aircraft”—not to the systemically derived requirement for certain kinds of military capabilities, but, rather, to the imperatives of corporate pork. He opines that such weapons have no stra- tegic or operational justification; that “the American empire, militarily more dominant than any empire in world history, can fight brushfire wars against terrorists and their ‘rogue’ state sponsors without those gold- plated white elephants.”

The underlying notion of “the security bureaucracies . . . looking for new enemies” is a threadbare concept that has somehow taken hold across the political spectrum, from the radical left (viz. Michael Klare [1981], who refers to a “threat bank”), to the liberal center (viz. Robert H. Johnson [1997], who dismisses most alleged “threats” as “improbable dangers”), to libertarians (viz. Ted Galen Carpenter [1992], Vice President for Foreign and Defense Policy of the Cato Institute, who wrote a book entitled A Search for Enemies). What is missing from most analysts’ claims of “threat inflation,” however, is a convincing theory of why, say, the American government significantly (not merely in excusable rhetoric) might magnify and even invent threats (and, more seriously, act on such inflated threat estimates). In a few places, Eland (2004, 185) suggests that such behavior might stem from military or national security bureaucrats’ attempts to enhance their personal status and organizational budgets, or even from the influence and dominance of “the military-industrial complex”; viz.: “Maintaining the empire and retaliating for the blowback from that empire keeps what President Eisenhower called the military-industrial complex fat and happy.” Or, in the same section:

In the nation’s capital, vested interests, such as the law enforcement bureaucracies . . . routinely take advantage of “crises”to satisfy parochial desires. Similarly, many corporations use crises to get pet projects— a.k.a. pork—funded by the government. And national security crises, because of people’s fears, are especially ripe opportunities to grab largesse. (Ibid., 182)

Thus, “bureaucratic-politics” theory, which once made several reputa- tions (such as those of Richard Neustadt, Morton Halperin, and Graham Allison) in defense-intellectual circles, and spawned an entire sub-industry within the field of international relations,5 is put into the service of dismissing putative security threats as imaginary. So, too, can a surprisingly cognate theory, “public choice,”6 which can be considered the right-wing analog of the “bureaucratic-politics” model, and is a preferred interpretation of governmental decision- making among libertarian observers. As Eland (2004, 203) summarizes:

Public-choice theory argues [that] the government itself can develop sepa- rate interests from its citizens. The government reflects the interests of powerful pressure groups and the interests of the bureaucracies and the bureaucrats in them. Although this problem occurs in both foreign and domestic policy, it may be more severe in foreign policy because citizens pay less attention to policies that affect them less directly.

There is, in this statement of public-choice theory, a certain ambiguity, and a certain degree of contradiction: Bureaucrats are supposedly, at the same time, subservient to societal interest groups and autonomous from society in general.

This journal has pioneered the argument that state autonomy is a likely consequence of the public’s ignorance of most areas of state activity (e.g., Somin 1998; DeCanio 2000a, 2000b, 2006, 2007; Ravenal 2000a). But state autonomy does not necessarily mean that bureaucrats substitute their own interests for those of what could be called the “national society” that they ostensibly serve. I have argued (Ravenal 2000a) that, precisely because of the public-ignorance and elite-expertise factors, and especially because the opportunities—at least for bureaucrats (a few notable post-government lobbyist cases nonwithstanding)—for lucrative self-dealing are stringently fewer in the defense and diplomatic areas of government than they are in some of the contract-dispensing and more under-the-radar-screen agencies of government, the “public-choice” imputation of self-dealing, rather than working toward the national interest (which, however may not be synonymous with the interests, perceived or expressed, of citizens!) is less likely to hold. In short, state autonomy is likely to mean, in the derivation of foreign policy, that “state elites” are using rational judgment, in insulation from self-promoting interest groups—about what strategies, forces, and weapons are required for national defense.

Ironically, “public choice”—not even a species of economics, but rather a kind of political interpretation—is not even about “public” choice, since, like the bureaucratic-politics model, it repudiates the very notion that bureaucrats make truly “public” choices; rather, they are held, axiomatically, to exhibit “rent-seeking” behavior, wherein they abuse their public positions in order to amass private gains, or at least to build personal empires within their ostensibly official niches. Such sub- rational models actually explain very little of what they purport to observe. Of course, there is some truth in them, regarding the “behavior” of some people, at some times, in some circumstances, under some conditions of incentive and motivation. But the factors that they posit operate mostly as constraints on the otherwise rational optimization of objectives that, if for no other reason than the playing out of official roles, transcends merely personal or parochial imperatives.

My treatment of “role” differs from that of the bureaucratic-politics theorists, whose model of the derivation of foreign policy depends heavily, and acknowledgedly, on a narrow and specific identification of the role- playing of organizationally situated individuals in a partly conflictual “pulling and hauling” process that “results in” some policy outcome. Even here, bureaucratic-politics theorists Graham Allison and Philip Zelikow (1999, 311) allow that “some players are not able to articulate [sic] the governmental politics game because their conception of their job does not legitimate such activity.” This is a crucial admission, and one that points— empirically—to the need for a broader and generic treatment of role.

Roles (all theorists state) give rise to “expectations” of performance. My point is that virtually every governmental role, and especially national-security roles, and particularly the roles of the uniformed mili- tary, embody expectations of devotion to the “national interest”; rational- ity in the derivation of policy at every functional level; and objectivity in the treatment of parameters, especially external parameters such as “threats” and the power and capabilities of other nations.

Sub-rational models (such as “public choice”) fail to take into account even a partial dedication to the “national” interest (or even the possibility that the national interest may be honestly misconceived in more paro- chial terms). In contrast, an official’s role connects the individual to the (state-level) process, and moderates the (perhaps otherwise) self-seeking impulses of the individual. Role-derived behavior tends to be formalized and codified; relatively transparent and at least peer-reviewed, so as to be consistent with expectations; surviving the particular individual and trans- mitted to successors and ancillaries; measured against a standard and thus corrigible; defined in terms of the performed function and therefore derived from the state function; and uncorrrupt, because personal cheating and even egregious aggrandizement are conspicuously discouraged.

My own direct observation suggests that defense decision-makers attempt to “frame” the structure of the problems that they try to solve on the basis of the most accurate intelligence. They make it their business to know where the threats come from. Thus, threats are not “socially constructed” (even though, of course, some values are).

A major reason for the rationality, and the objectivity, of the process is that much security planning is done, not in vaguely undefined circum- stances that offer scope for idiosyncratic, subjective behavior, but rather in structured and reviewed organizational frameworks. Non-rationalities (which are bad for understanding and prediction) tend to get filtered out. People are fired for presenting skewed analysis and for making bad predictions. This is because something important is riding on the causal analysis and the contingent prediction. For these reasons, “public choice” does not have the “feel” of reality to many critics who have participated in the structure of defense decision-making. In that structure, obvious, and even not-so-obvious, “rent-seeking” would not only be shameful; it would present a severe risk of career termination. And, as mentioned, the defense bureaucracy is hardly a productive place for truly talented rent-seekers to operate, compared to opportunities for personal profit in the commercial world. A bureaucrat’s very self-placement in these reaches of government testi- fies either to a sincere commitment to the national interest or to a lack of sufficient imagination to exploit opportunities for personal profit.

### Syria DA

#### Deal already happened and Obama not pushing

Chu 9-14

Henry Chu, “U.S., Russia agree on a disposal plan for Syria's chemical weapons” September 14, 2013, <http://www.latimes.com/world/worldnow/la-fg-wn-kerry-lavrov-syria-20130914,0,4340460.story>, KB)

Secretary of State John F. Kerry announced Saturday that the U.S. and Russia had agreed on a framework for impounding and destroying Syria’s stockpile of chemical weapons by the middle of next year.¶ Damascus will be given one week from now to give an inventory of its chemical arsenal and will have to allow international inspectors into Syria “no later than November,” Kerry said after a third day of intense negotiations with Russian Foreign Minister Sergei Lavrov in Geneva.

#### PC fails – only our evidence assumes recent developments

Cillizza 6/25

(Chris Cillizza, “Is the presidential bully pulpit dead?; Driving a narrative is almost impossible these days -- even for the president of the United States.” June 25, 2013, Washington Post Blogs, LexisNexis, KB)

While you can debate the relative bad-ness of each of the stories for the White House, what's not debatable is that everyone in the administration from President Obama on down has been driven by the news rather than driving it over these last weeks. That inability of even the President of the United States to push his preferred message on a given day/week/month points to a fundamental new reality of politics: The bully pulpit just ain't what it used to be.¶ "There is no such thing as one storyline per news cycle -- there are a thousand news cycles in any given day, and not all of them can be completely controlled," said Stephanie Cutter, a senior adviser to President Obama's 2012 campaign. "But, you have to understand which of them are breaking through to average Americans, and which of them are just Washington fodder or blogosphere chatter."¶ To be clear: President Obama is still able to push an issue into the public consciousness if he really wants to. Tomorrow's speech on climate change is an example of that fact. But, a president is no longer able to ensure that his preferred daily narrative will be THE daily narrative or what the shelf life of it will be.¶ Take Obama's speech on counterterrorism which he delivered on May 23. The speech provided the clearest vision -- and rationale -- for his use of drones, the prison at Guantanamo Bay and any number of other subjects. But, despite the fact that the speech was viewed as a major landmark in his administration by those who follow counterterrorism policy closely, it quickly disappeared from the news.¶ Why is the bully pulpit less bully these days? Lots and lots of reasons but three seem most salient to us.¶ 1. The ubiquity of news. When Ronald Reagan was president -- or even when Bill Clinton was president -- the White House had to deal with the three major broadcast television networks and a handful of newspapers and wire services. If the White House wanted a certain story pushed, they pushed it to those outlets and there was a damn good chance that they wind up with what they wanted on the evening news and in the morning papers.¶ The splintering of the media into a million smaller shards makes that sort of agenda-driving incredibly difficult. The White House can still sit down with a handful of what it believes to be the most important news outlets in the country to push a message. But, if a blog happens to pop up a semi-controversial item on, say Michelle Obama, then the White House can say goodbye to their preferred message of the day.¶ Every White House needs to learn to roll with the punches that come with being the top elected official in the U.S.. But the punches are non-stop nowadays -- we tend to think of it as a pitching machine that just keeps firing fastballs at you -- and that makes it very, very difficult to roll with them and then pivot to your desired message.¶ 2. The pace of news. Pre-Internet, a White House might have 12-24 hours to respond to the whereabouts of Edward Snowden and what it meant to U.S. foreign policy. Heck, it's uniquely possible that in the pre-Internet era, which wasn't all that long ago, the White House might be the only organization able to track Snowden's whereabouts. Now, his plane is tracked from the time it takes off to the time it lands; reporters are buying seats on a plane from Moscow to Cuba that Snowden was supposedly on.¶ Michael beschloss, the renowned historian, notes that when the Berlin Wall went up in August 1961President John F. Kennedy was on vacation and "went for a week without being successfully pressed to respond or explain why the U.S. had let it happen." Added Beschloss: "There is now an expectation that Presidents (or their aides) respond to developments almost immediately. Thus as Lincoln would have put it, Presidents are very vulnerable to being overtaken by events."¶ Beschloss' point means that as president in today's age, you spend most of your time being reactive, rather than pro-active. And the bully pulpit tends to work far better as an offensive rhetorical weapon than a defensive one.¶ 3. The polarization of the country. Of the 10 most polarized political years on record -- defined as the delta between Republicans and Democrats on the question of presidential job approval -- nine are sometime during the presidencies of Barack Obama and George W. Bush. That's no coincidence.¶ Using the bully pulpit as a persuasion tool only works if there are people who can be persuaded. At the moment, that's a shrinking constituency. "There are at least 40 percent of the voters in this country who don't give a fig for a word [Obama] says, and the same is true of Bush 43 and Clinton," said Jan van Lohuizen, who handled polling for Bush.¶ Regardless of the reason(s) -- and we'd love to hear your reasons in the comments section below -- it's hard to argue with the idea that the bully pulpit has grown less powerful over the last decade and almost certainly will continue to diminish as a dominating message delivery system in the years to come.

#### Plan’s popular - Obama will issue unpopular XOs on cyber – triggers their link

Russia Times 13

“Obama to 'bypass Congress' on CISPA with cybersecurity executive order”¶ [http://rt.com/usa/congress-executive-actions-president-958/,Feb. 11, mg]

**Unable to reach a deal with Congress,** President **Obama plans to use his power to exert executive actions against the will of lawmakers. The president will issue orders addressing controversial topics including cybersecurity**.¶ Although President Obama has issued fewer executive orders than any president in over 100 years, he is making extensive plans to change that, Washington Post reports quoting people outside the White House involved in discussions on the issues. **Due to conflicts with a Congress that too often disagrees on proposed legislation, Obama plans to act alone and is likely "to rely heavily" on his executive powers in future,** according to the newspaper.¶ Obama’s first executive order is expected to be issued this week when the president calls for the creation of new standards on what private-sector companies must do to protect their computer systems from a cybersecurity breach.¶ The order is a direct response to Congress’ refusal to pass the Cyber Intelligence Sharing and Protection Act (CISPA) last year, which the administration deemed crucial to prevent crippling attacks on the nation’s infrastructure. But members of Congress who opposed the legislation cited serious privacy concerns with giving the government greater access to Americans’ personal information that only private companies and servers might have access to.¶ **Despite opposition from lawmakers, the president will use his executive powers** to issue an order **addressing cybersecurity** initiatives.¶ “It is a very dangerous road he’s going down contrary to the spirit of the Constitution,” Sen. Charles E. Grassley (R-Iowa) told the Washington Post. “Just because Congress doesn’t act doesn’t mean the president has a right to act.”¶

#### Perm do both

Lee 9-9

(ESTHER YU-HSI LEE, immigration Reporter/Blogger for ThinkProgress, “House Republicans Stall On Immigration Reform, Blaming Other Priorities” SEPTEMBER 9, 2013, <http://thinkprogress.org/immigration/2013/09/09/2588011/immigration-reform-burner/>, KB)

As much as House Republicans are aiming to push immigration reform off the slate for another year, there is no clear reason as to why reform cannot be taken up simultaneously with any of the other issues. House Judiciary Committee Chairman Bob Goodlatte (R-VA), who has called the 2010 DREAM Act “unfair” and “ripe for fraud,” recently called the Senate immigration bill, “unconstitutional” and would allow “dangerous criminals to be released back onto our streets.”

#### Controversial fights ensure agenda success.

Dickerson 1/18

(John, Chief Political Correspondent at the Slate, Political Director of CBS News, Covered Politics for Time Magazine for 12 Years, Previous White House Correspondent, Go for the Throat!, http://tinyurl.com/b7zvv4d)

On Monday, President Obama will preside over the grand reopening of his administration. It would be altogether fitting if he stepped to the microphone, looked down the mall, and let out a sigh: so many people expecting so much from a government that appears capable of so little. A second inaugural suggests new beginnings, but this one is being bookended by dead-end debates. Gridlock over the fiscal cliff preceded it and gridlock over the debt limit, sequester, and budget will follow. After the election, the same people are in power in all the branches of government and they don't get along. There's no indication that the president's clashes with House Republicans will end soon.¶ Inaugural speeches are supposed to be huge and stirring. Presidents haul our heroes onstage, from George Washington to Martin Luther King Jr. George W. Bush brought the Liberty Bell. They use history to make greatness and achievements seem like something you can just take down from the shelf. Americans are not stuck in the rut of the day.¶ But this might be too much for Obama’s second inaugural address: After the last four years, how do you call the nation and its elected representatives to common action while standing on the steps of a building where collective action goes to die? That **bipartisan** bag of tricks has been tried and it didn’t work. People don’t believe it. Congress' approval rating is 14 percent, the lowest in history. In a December Gallup poll, 77 percent of those asked said the way Washington works is doing “serious harm” to the country.¶ The challenge for President Obama’s speech is the challenge of his second term: how to be great when the **environment stinks**. Enhancing the president’s legacy requires something more than simply the clever application of predictable stratagems. Washington’s **partisan rancor**, the size of the problems facing government, and the limited amount of **time** before Obama is a lame duck all point to a single conclusion: The president who came into office speaking in lofty terms about **bipartisanship** and cooperation can only cement his legacy if he **destroys the GOP**. If he wants to transform American politics, he must **go for the throat**.¶ President Obama could, of course, resign himself to tending to the achievements of his first term. He'd make sure health care reform is implemented, nurse the economy back to health, and put the military on a new footing after two wars. But he's more ambitious than that. He ran for president as a one-term senator with no executive experience. In his first term, he pushed for the biggest overhaul of health care possible because, as he told his aides, he wanted to make history. He may already have made it. There's no question that he is already a president of consequence. But there's no sign he's content to ride out the second half of the game in the Barcalounger. He is approaching gun control, climate change, and immigration with wide and excited eyes. He's not going for caretaker.¶ How should the president proceed then, if he wants to be bold? The Barack Obama of the first administration might have approached the task by finding some Republicans to deal with and then start agreeing to some of their demands in hope that he would win some of their votes. It's the traditional approach. Perhaps he could add a good deal more schmoozing with lawmakers, too. ¶ That's the old way. **He has abandoned that**. He doesn't think it will work and he doesn't have the time. As Obama explained in his last press conference, he thinks the Republicans are dead set on opposing him. They cannot be unchained by schmoozing. Even if Obama were wrong about Republican intransigence, other constraints will limit the chance for cooperation. Republican lawmakers worried about primary challenges in 2014 are not going to be willing partners. He probably has at most 18 months before people start dropping the lame-duck label in close proximity to his name. ¶ Obama’s **only remaining option is to pulverize**. Whether he succeeds in passing legislation or not, given his ambitions, his goal should be to delegitimize his opponents. Through a series of **clarifying fights over controversial issues**, he can force Republicans to either side with their coalition's most extreme elements or cause a rift in the party that will leave it, at least temporarily, in disarray. ¶ This theory of political transformation rests on the weaponization (and slight bastardization) of the work by Yale political scientist Stephen Skowronek. Skowronek has written extensively about what distinguishes transformational presidents from caretaker presidents. In order for a president to be transformational, the old order has to fall as the orthodoxies that kept it in power exhaust themselves. Obama's gambit in 2009 was to build a new post-partisan consensus. That didn't work, but by exploiting the weaknesses of today’s Republican Party, Obama has an opportunity to hasten the demise of the old order by increasing the political cost of having the GOP coalition defined by Second Amendment absolutists, **climate science deniers**, supporters of “self-deportation” and the pure no-tax wing.

#### Water infrastructure thumps – it will trigger huge partisan fights

Tate 9-11

(CURTIS TATE, McClatchy Washington Bureau, “House adds water infrastructure bill to pile of unfinished business” September 11, <http://www.kansascity.com/2013/09/11/4474921/house-adds-water-infrastructure.html>, KB)

Lawmakers in the House of Representatives introduced their version of a bill Wednesday to move forward work on an array of water projects across the country, legislation that traditionally sails through Congress on a bipartisan basis.¶ The Water Resources Reform and Development Act, the first such bill in six years, would authorize repair and improvements to dams and levees, the deepening of harbors and navigation channels, and flood control and coastal protection projects.¶ With the Atlantic and Gulf coasts reeling from the impact of hurricanes, locks and dams deteriorating on Midwestern rivers, East Coast ports needing to accommodate bigger ships and the threat of catastrophic floods in major cities, the legislation serves many critical needs.¶ “It’s not a regional issue, it’s a national priority,” Rep. Bill Shuster, R-Pa., chairman of the House Transportation and Infrastructure Committee, told a news conference at the Capitol.¶ The Senate overwhelmingly approved its version of the bill in May by 83-14, and Shuster and his House colleagues expressed confidence Wednesday that their legislation would succeed.¶ “The bill has been a bipartisan bill from day one,” he said.¶ But with the capital consumed by sharp divisions over fiscal policy, foreign policy and immigration, passage of the latest bill is no guarantee. A farm bill, for example, cleared the Senate on a bipartisan vote earlier this summer but went down to defeat in the House, embarrassing leaders on both sides of the aisle.¶ The House is adding the water legislation to a pile of unfinished business, including the farm bill, immigration reform and the debt limit.

**2ac- Israel Relations DA**

**Relations low- Palestine settlements**

**Ben-David & Gauoette 13**

Calev Ben-David & Nicole Gaouette, Bloomberg, “Obama-Netanyahu Odd Couple Testing U.S.-Israel Ties,” 1/24/13, <http://www.bloomberg.com/news/2013-01-23/obama-netanyahu-odd-couple-tests-u-s-israel-alliance-resilience.html> SJE

**Obama**, 51, has **aired his unhappiness about the construction of Jewish settlements in the West Bank**, which Israel captured from Jordan in the 1967 Mideast War. According to Peace Now, an Israeli group that favors negotiations with the Palestinians, **Netanyahu’s previous coalition government issued a record number of tenders for West Bank housing** during the past 47 months. **Increased settlement construction makes the resumption of the peace process and the possibility of negotiating a two-state solution more remote**, said Philip Wilcox, a former State Department Mideast expert who’s now president of the Foundation for Middle East Peace, a Washington policy group. **The issue poses a “huge dilemma” for the U.S., which has built its relationship with Israel on the basis of shared values and interests,** Wilcox said. **If Israel moves toward a situation where Jews are a ruling minority in a unitary state, the country will be neither Jewish nor democratic, and that “removes the moral underpinnings of the U.S.-Israeli relationship,”** he said.

**Relations resilient - empirics**

**Miller 10**

Aaron David Miller, public policy scholar at the Woodrow Wilson Center for Scholars and former adviser to six secretaries of state on Arab-Israeli negotiations, June 2010, “Obama, Israel & American Jews: The Challenge—A Symposium,” <http://www.commentarymagazine.com/viewarticle.cfm/obama--israel---american-jews--the-challenge-a-symposium-15449?page=all>

It’s true that the United States is going through **a tough patch in the U.S.-Israeli relationship**. Of the three worst periods of tension in that relationship, the current crisis still **doesn’t approach 1956** (over Suez), **1975** (the reassessment of the second Sinai disengagement agreement), **or 1991** (over housing loan guarantees and settlements). **In these three cases, sanctions against Israel were either threatened or used.** And while the current tensions are not just a bump in the road (and could even worsen), **the U.S.-Israeli bond has proved remarkably resilient over the course of the last 60-plus years. The marriage of interests and ideology creates a powerful and enduring bond that links Israel and the United States together.**

### Prez Powers

#### Asian war is unlikely - all potential conflicts are solved by regional stability initiatives

Bitzinger & Desker ‘8

senior fellow and dean of S. Rajaratnam School of International Studies respectively (Richard A. Bitzinger, Barry Desker, “Why East Asian War is Unlikely,” Survival, December 2008, <http://pdfserve.informaworld.com-/678328_731200556_906256449.pdf>)

The Asia-Pacific region can be regarded as a zone of both relative insecurity and strategic stability. It contains some of the world’s most significant flashpoints – the Korean peninsula, the Taiwan Strait, the Siachen Glacier – where tensions between nations could escalate to the point of major war. It is replete with unresolved border issues; is a breeding ground for transnationa terrorism and the site of many terrorist activities (the Bali bombings, the Manila superferry bombing); and contains overlapping claims for maritime territories (the Spratly Islands, the Senkaku/Diaoyu Islands) with considerable actual or potential wealth in resources such as oil, gas and fisheries. Finally, the Asia-Pacific is an area of strategic significance with many key sea lines of communication and important chokepoints. Yet despite all these potential crucibles of conflict, the Asia-Pacific, if not an area of serenity and calm, is certainly more stable than one might expect. To be sure, there are separatist movements and internal struggles, particularly with insurgencies, as in Thailand, the Philippines and Tibet. Since the resolution of the East Timor crisis, however, the region has been relatively free of open armed warfare. Separatism remains a challenge, but the break-up of states is unlikely. Terrorism is a nuisance, but its impact is contained. The North Korean nuclear issue, while not fully resolved, is at least moving toward a conclusion with the likely denuclearisation of the peninsula. Tensions between China and Taiwan, while always just beneath the surface, seem unlikely to erupt in open conflict any time soon, especially given recent Kuomintang Party victories in Taiwan and efforts by Taiwan and China to re-open informal channels of consultation as well as institutional relationships between organisations responsible for cross-strait relations. And while in Asia there is no strong supranational political entity like the European Union, there are many multilateral organisations and international initiatives dedicated to enhancing peace and stability, including the Asia-Pacific Economic Cooperation (APEC) forum, the Proliferation Security Initiative and the Shanghai Co-operation Organisation. In Southeast Asia, countries are united in a common geopolitical and economic organisation – the Association of Southeast Asian Nations (ASEAN) – which is dedicated to peaceful economic, social and cultural development, and to the promotion of regional peace and stability. ASEAN has played a key role in conceiving and establishing broader regional institutions such as the East Asian Summit, ASEAN+3 (China, Japan and South Korea) and the ASEAN Regional Forum. All this suggests that war in Asia – while not inconceivable – is unlikely.

**Enemies good**

**Reinhard 4** – Kenneth Reinhard, Professor of Jewish Studies at UCLA, 2004, “Towards a Political Theology- Of the Neighbor,” online: http://www.cjs.ucla.edu/Mellon/Towards\_Political\_Theology.pdf

**If the concept of the political is defined, as** Carl Schmitt does, **in terms of the Enemy/Friend opposition**, the world we find ourselves in today is one from which the political may have already disappeared, or at least has mutated into some strange new shape. **A world not anchored by the “us” and “them” binarisms** that flourished as recently as the Cold War **is** one **subject to radical instability**, **both subjectively and politically**, as Jacques Derrida points out in The Politics of Friendship: **The effects of this destructuration would be countless**: **the ‘subject’** in question **would be looking for new reconstitutive enmities**; **it would multiply ‘little wars’ between nation-states**; **it would sustain** at any price so-called ethnic or **genocidal struggles**; **it would seek to pose itself**, to find repose, **through opposing still identifiable adversaries – China, Islam?** **Enemies without which** … **it would lose its political** **being** … without an enemy, and therefore without friends, where does one then find oneself, qua a self? (PF 77) **If one accepts Schmitt’s account of the political**, **the disappearance of the enemy results in** something like **global psychosis**: **since the mirroring relationship between Us and Them provides a form of stability**, **albeit one based on projective identifications and repudiations**, **the loss of the enemy threatens to destroy** what Lacan calls **the “imaginary tripod” that props up the psychotic with a sort of pseudo-subjectivity, until something causes it to collapse, resulting in full-blown delusions, hallucinations, and paranoia.**  Hence, for Schmitt, **a world without enemies is much more dangerous than one where one is surrounded by enemies**; as Derrida writes, **the disappearance of the enemy** **opens the door for** “an **unheard-of violence**, **the evil of a malice knowing neither measure nor ground,** **an unleashing** **incommensurable in its unprecedented –** therefore **monstrous** –forms; a **violence** **in the face of which what is called hostility, war, conflict, enmity, cruelty,** even hatred, **would regain reassuring and ultimately appeasing contours, because they would be identifiable**” (PF 83).

**AT Endless War**

**FRAMEWORK—The aff is a normative statement. Vote aff if plan is a good idea, neg if it isn’t.**

**A. Solves their offense –the impact of the K is a reason the aff is bad.**

B. **Aff choice – they arbitrarily steal 9 minutes of offense, destroys the aff’s only advantage.**

**VVA**

**FP**

**perm- NME**

**P- alt**

**No risk of continual war making – institutional safeguards check**

Allen **Buchanan 7**, Professor of Philosophy and Public Policy at Duke, 2007 (Preemption: military action and moral justification, pg. 128)

The intuitively plausible idea behind the 'irresponsible act' argument is that, other things being equal, the higher the stakes in acting and in particular the greater the moral risk, the higher are the *epistemic requirements* for justified action. The decision to go to war is generally a high stakes decision par excellence and the moral risks are especially great, for two reasons. First, unless one is justified in going to war, one's deliberate killing of enemy combatants will he murder, indeed mass murder. Secondly, at least in large-scale modem war, it is a virtual certainty that one will kill innocent people even if one is justified in going to war and conducts the war in such a way as to try to minimize harm to innocents. Given these grave moral risks of going to war, quite apart from often substantial prudential concerns, some types of justifications for going to war may simply be too subject to abuse and error to make it justifiable to invoke them. The 'irresponsible act' objection is not a consequentialist objection in any interesting sense. It does not depend upon the assumption that every particular act of going to war preventively has unacceptably bad consequences (whether in itself or by virtue of contributing lo the general acceptance of a principle allowing preventive war); nor does it assume that it is always wrong lo rely on a justification which, if generally accepted, would produce unacceptable consequences. Instead, the "irresponsible act' objection is more accurately described as an agent-centered argument and more particularly an argument from moral epistemic responsibility. The 'irresponsible act' objection to preventive war is highly plausible if— but only if—one assumes that the agents who would invoke the preventive-war justification are, as it were, *on their own* in making the decision to go to war preventively. In other words, the objection is incomplete unless the context of decision-making is further specified. Whether the special risks of relying on the preventive-war justification are unacceptably high will depend, *inter alia,* upon whether the decision-making process includes effective provisions for redu­cing those special risks. Because the special risks are at least in significant part epistemic—due to the inherently speculative character of the preventive war-justification—the epistemic context of the decision is crucial. Because institutions can improve the epistemic performance of agents, it is critical to know what the institutional context of the preventive-war decision is, before we can regard the 'irresponsible agent' objection as conclusive. Like the 'bad practice' argument, this second objection to preventive war is inconclusive because it does not consider— and rule out—the possibility that well-designed institutions for decision-making could address the problems that would otherwise make it irresponsible for a leader to invoke the preventive-war justification.

**No impact**

**Gray 7**—Director of the Centre for Strategic Studies and Professor of International Relations and Strategic Studies at the University of Reading, graduate of the Universities of Manchester and Oxford, Founder and Senior Associate to the National Institute for Public Policy, formerly with the International Institute for Strategic Studies and the Hudson Institute (Colin, July, “The Implications of Preemptive and Preventive War Doctrines: A Reconsideration”, <http://www.ciaonet.org/wps/ssi10561/ssi10561.pdf>)

7. A policy that favors preventive warfare expresses a futile quest for absolute security. It could do so. Most controversial policies contain within them the possibility of misuse. In the hands of a paranoid or boundlessly ambitious political leader, prevention could be a policy for endless warfare. However, the American political system, with its checks and balances, was designed explicitly for the purpose of constraining the executive from excessive folly. Both the Vietnam and the contemporary Iraqi experiences reveal clearly that although the conduct of war is an executive prerogative, in practice that authority is disciplined by public attitudes. Clausewitz made this point superbly with his designation of the passion, the sentiments, of the people as a vital component of his trinitarian theory of war. 51 It is true to claim that power can be, and indeed is often, abused, both personally and nationally. It is possible that a state could acquire a taste for the apparent swift decisiveness of preventive warfare and overuse the option. One might argue that the easy success achieved against Taliban Afghanistan in 2001, provided fuel for the urge to seek a similarly rapid success against Saddam Hussein’s Iraq. In other words, the delights of military success can be habit forming. On balance, claim seven is not persuasive, though it certainly contains a germ of truth. A country with unmatched wealth and power, unused to physical insecurity at home—notwithstanding 42 years of nuclear danger, and a high level of gun crime—is vulnerable to demands for policies that supposedly can restore security. But we ought not to endorse the argument that the United States should eschew the preventive war option because it could lead to a futile, endless search for absolute security. One might as well argue that the United States should adopt a defense policy and develop capabilities shaped strictly for homeland security approached in a narrowly geographical sense. Since a president might misuse a military instrument that had a global reach, why not deny the White House even the possibility of such misuse? In other words, constrain policy ends by limiting policy’s military means. This argument has circulated for many decades and, it must be admitted, it does have a certain elementary logic. It is the opinion of this enquiry, however, that the claim that a policy which includes the preventive option might lead to a search for total security is **not at all convincing**. Of course, folly in high places is always possible, which is one of the many reasons why popular democracy is the superior form of government. It would be absurd to permit the fear of a futile and dangerous quest for absolute security to preclude prevention as a policy option. Despite its absurdity, this rhetorical charge against prevention is a stock favorite among prevention’s critics. It should be recognized and dismissed for what it is, a debating point with little pragmatic merit. And strategy, though not always policy, **must be nothing if not pragmatic**.

Norms elicit positive responses from non-state actors- allows 3rd parties to increase influence through compliance

Thomas ‘2

[Daniel C. Thomas, University of Illinois at Chicago. “Boomerangs and Superpowers: International Norms, Transnational Networks and US Foreign Policy.” Cambridge Review of International Affairs, Volume 15, Number 1, 2002. ETB]

This evolution in international relations theory includes growing recognition that the **creation of** formal international **norms by state actors facilitates** (often inadvertently) **the political mobilisation of non-state actor**s.5 **By** **identifying with the** purposes of an international **norm**, **non-state actors legitimate their demands, gain access to state decision makers, and thus gain greater influence over state policy**. In some cases, **they may publicise a state’s non-compliance with its obligations under the norm in question**. In other cases, **they may pressure a state that is already in compliance to exert its in􏰝uence on non-compliant states**. **The ‘boomerang effect’ refers to situations where non-state actors apply this strategy transnationally in order to circumvent blocked domestic opportunities for pro- test**.6 International norms thus help non-state actors to create transnational networks capable of reshaping the conceptions of self-interest driving state behaviour.

**Rejection of sovereign exception fails and results in more violence**

**Moreiras, 2004**. professor, romance studies and literature – Duke University. Alberto, CR: The New Centennial Review, 4.3.

But Rasch remains a Schmittian, not a Benjaminian. For him, **no interruption of the political principle of reason—the ultimate principle of political order, the nomos of the nomos, the principle of sovereign exception**, which he persuasively shows to be a case of the logical law of the excluded middle (Rasch 2002, 38–42)—**is possible without risking the collapse of the political into an eschatology of the end of the world, which is the same as an eschatology of radical origin: “to be liberated from the structure of sovereignty is to be returned to a natural state of innocence**” (48). **Rasch is suspicious of** Benjamin’s—and **Agamben’s**—**pure violence as the harbinger of a “completely new politics” that might in fact accomplish nothing but an exclusion of the political** (38). As he says in a different essay**, “the political does not exist to usher in the good life by eliminating social antagonism; rather, it exists to serve as the medium for an acceptably limited and therefore productive conflict in the inevitable absence of any final, universally accepted vision of the good life”** (Rasch n.d., 30–31). **Rasch opposes a politics of the katechon—a properly Schmittian politics of the containment of evil—to the messianic politics of the reestablishment of natural innocence that he detects in Agamben’s Homo Sacer**.12 Is there, in fact, in Agamben’s State of Exception, an “appeal to the ontological hope” of “infinite perfectibility” (Rasch n.d., 29)? And, a fortiori, is that also what is behind Derrida’s Voyous? The crucial question here concerns the determination of a practical understanding of the political beyond every messianic delusion. **Messianic delusion turns every politics into a kind of ultrapolitics whose political effectivity then wavers between the inane and the catastrophic**. An alternative question is: are onto-theological politics the only possible politics for our age? R E A S O N B E YOND R E A S O N Autoimmunity is said to refer to “this strange illogical logic through which a living being can spontaneously destroy, in an autonomous fashion, that which, in it, is destined to protect it against the other, to immunize it against the intrusive aggression of the other” (Derrida 2003, 173). Autoimmunity is therefore a kind of “death drive” (215) that can be related to the structure of betrayal as self-betrayal, which, as we saw, Lacan considers a radical structure of the human relationship to being. For Lacan, the abandonment of the ethical imperative not to give ground on one’s desire is ultimately an accommodation to the real from which there is no return; the path back of the “ordinary man” into his own business is blocked once he has paid the price of accommodation to the service of goods and has betrayed the structure of his desire: “once one has crossed that boundary . . . there is no way back. It might be possible to do some repair work, but not to undo it” (Lacan 1992, 321). This betrayal formalizes politics—just as it formalizes religion—for Lacan. Lacanian politics, to the extent that they are understood to be a politics of the subject, are framed by a postrevolutionary service of goods, in which a sublimated jouissance waits infinitely, and uselessly, for the formation of the universal State. Is an alternative frame for contemporary politics available? Both Derrida and Agamben radicalize Schmitt’s intuition regarding the necessity of a transformation in the concept of the political given the exhaustion of the political order of modernity. The political order of modernity has exhausted itself through autoimmunitary developments— something that Schmitt anticipated both in his partisan theory, through the projection of the figure of the total counterpartisan that follows “the inevitability of a moral compulsion,” and in his investigation of the notion of a nomos of the earth, which reaches an unexpected arrest in the notion of the Kantian unjust enemy. If both Derrida and Agamben can be said to be Schmittian to a certain extent, in spite of their fundamental antagonism to the German thinker, it is precisely insofar as both of them take as point of departure for their investigations of political sovereignty some of Schmitt’s crucial theories. Derrida makes it very clear through a sort of disavowing avowal: “One did not have to wait for Schmitt to know that the sovereign is he who decides exceptionally and performatively on the exception, he who guards or gives himself the right to suspend the law; or to know that this juridico-political concept, like all the others, secularizes a theological heritage” (2003, 211–12). And Agamben of course makes Schmitt a crucial reference in both Homo Sacer and State of Exception.13 Both of them are interested, not, like Rasch, in a reassertion of sovereignty as the only possible pragmatic framing for a conceptualization of the political today, but rather in a dismantling of the claims of sovereignty as ultimate political claims, or as the ultimate claims of the political. They want to explore the contemporary troubles of sovereignty, troubles in sovereignty—what Derrida can and does call in French mal de souveraineté (196). These troubles are autoimmunity troubles: sovereignty ultimately suffers from itself, as it is its action that ultimately dooms it to face, in a certain far-from-reassuring impotence, the absolute threat or the anomic terror of the real. Can we then think of politics not beyond sovereignty, but rather as not exhausted by the sovereign frame? Is there a position—a properly political position—that can establish a distance from sovereignty without dreaming, like the Lacanian ordinary man, of the messianic fulfillment of the universal State, when desire will coincide absolutely with itself (and when, therefore, there will be nothing but the sovereign, as sovereign desire)? If there is a position, if it is possible to work out a position that can think of sovereignty without being absolutely circumscribed by sovereignty, that position will have accomplished a derangement of onto-theology. It will not have gotten rid of it, just as it will not have gotten rid of sovereignty, but it will have displaced onto-theology, and its political translation as sovereignty theory, from the horizon of the political. Derrida uses the shorthand “nonsovereign god” for this possibility, echoing Heidegger but also displacing Heidegger.14 And **Agamben talks about the liberation of anomy, as a solicitation of the deep historical compromise of violence and the law. If violence becomes the “thing” of politics for Agamben, this is so to the extent that “human action” must “rescind the link between violence and the law” in order to expose the violence of the law, rather than the lawfulness of violence** (which is the Schmittian project). But the reference to human action is already revealing of a limit in **Agamben’s project**. Certainly human action is an unavoidable referent for politics. But Agamben is still under the Lacanian determination, if on the side of the hero. His project**, a liberation of pure violence, is a tragic project to the extent that it leads the hero towards** what Sophocles calls **até.** Of até Lacan says: “It is an irreplaceable little word. It designates the limit that human life can only briefly cross. The text of the Chorus is significant and insistent—ektos atas. Beyond this até, one can only spend a brief period of time, and that’s where Antigone wants to go. . . . One learns from Antigone’s own mouth testimony on the point she has reached: she literally cannot stand it any more. . . . She lives with the memory of the intolerable drama of the one whose descendence has just been destroyed in the figure of her two brothers. She lives in the house of Creon; she is subject to his law; and that is something she cannot bear” (Lacan 1992, 262–63). **Agamben, like the tragic hero, situates himself “with relation to the goal of desire”** (265), **namely, in the relentless pursuit of a liberation from the sovereign law that has created a permanent state of exception: the ineluctable violence of the state as the house of Creon. To liberate pure violence in order to destroy the law**: of this one could say what Lacan says of the tragic hero, namely, “he knows what he is doing. He always manages to cause things to come crashing down on his head” (275). Agamben defines the contemporary state as one in which “the norm rules, but it is not applied (it does not have force) and . . . acts that have no legal value acquire the force. . . . The state of exception is an anomic space, where what is set in place is a force of law without law . . . , where act and power are radically separated” (52). If the contemporary state, the contemporary embodiment of the law, is absolute exception, understood as absolute oppression, and if only a liberation of violence from its lawful capture can release an appropriate politics, this politics’ human action, like Antigone, stands in “as a pure and simple relationship of the human being to that of which he miraculously happens to be the bearer, namely, the signifying cut that confers on him the indomitable power of being what he is in the face of everything that may oppose him. Anything at all may be invoked in connection with this, and that’s what the Chorus does in the fifth act when it evokes the god that saves. Dionysos is this god; otherwise why would he appear here? There is nothing Dionysiac about the act and the countenance of Antigone. Yet she pushes to the limit the realization of something that might be called the pure and simple desire of death as such. She incarnates that desire” (282). **A politics of heroic desire, in the ineluctable fulfillment of the ethical imperative, might be conceived to be an antisovereign politics, but it is still a subjective politics of catastrophe. At the limit, the hero does not abandon the horizon of sovereignty: the hero simply inverts it, and puts it at the service of an intensely mystical jouissance**, “the passage that allows access to the justice that one of Benjamin’s posthumous fragments defines as a state of the world in which it appears as an absolutely inappropriatable and unjuridifiable good” (Agamben 2003, 83).

Method focus causes scholarly paralysis

**Jackson**, associate professor of IR – School of International Service @ American University, **‘11**

(Patrick Thadeus, The Conduct of Inquiry in International Relations, p. 57-59)

Perhaps the greatest irony of this instrumental, decontextualized importation of “falsification” and its critics into IR is the way that an entire line of thought that privileged disconfirmation and refutation—no matter how complicated that disconfirmation and refutation was in practice—has been transformed into a license to **worry endlessly about foundational assumptions.** At the very beginning of the effort to bring terms such as “paradigm” to bear on the study of politics, Albert O. **Hirschman** (1970b, 338) **noted this very danger**, suggesting that without “a little more ‘reverence for life’ and a little less straightjacketing of the future,” the **focus on** producing internally **consistent** packages of **assumptions instead of** actually examining **complex empirical situations would result in scholarly paralysis.** Here as elsewhere, Hirschman appears to have been quite prescient, inasmuch as the major effect of paradigm and research programme language in IR seems to have been a series of debates and discussions about whether the fundamentals of a given school of thought were sufficiently “scientific” in their construction. Thus **we have debates about how to evaluate scientific progress**, and attempts to propose one or another set of research design principles **as uniquely scientific**, and inventive, “reconstructions” of IR schools, such as Patrick James’ “elaborated structural realism,” supposedly for the purpose of placing them on a **firmer scientific footing** by making sure that they have all of the required elements of a basically Lakatosian19 model of science (James 2002, 67, 98–103).

The bet with all of this scholarly activity seems to be that if we can just get the fundamentals right, then scientific progress will inevitably ensue . . . even though this is the precise opposite of what Popper and Kuhn and Lakatos argued! In fact, all of this obsessive interest in foundations and starting-points is, in form if not in content, a lot closer to logical positivism than it is to the concerns of the falsificationist philosophers, despite the prominence of language about “hypothesis testing” and the concern to formulate testable hypotheses among IR scholars engaged in these endeavors. That, above all, is why I have labeled this methodology of scholarship neopositivist. While it takes much of its self justification as a science from criticisms of logical positivism, in overall sensibility it still operates in a visibly positivist way, attempting to construct knowledge from the ground up by getting its foundations in logical order before concentrating on how claims encounter the world in terms of their theoretical implications. This is by no means to say that neopositivism is not interested in hypothesis testing; on the contrary, neopositivists are extremely concerned with testing hypotheses, but **only after the fundamentals have been** soundly **established.** Certainty, not conjectural provisionality, seems to be the goal—a goal that, ironically, Popper and Kuhn and Lakatos would all reject.

# 1AR

### AT Terror Contradiction

#### Norms elicit positive responses from non-state actors- allows 3rd parties to increase influence through compliance

Thomas ‘2

[Daniel C. Thomas, University of Illinois at Chicago. “Boomerangs and Superpowers: International Norms, Transnational Networks and US Foreign Policy.” Cambridge Review of International Affairs, Volume 15, Number 1, 2002. ETB]

This evolution in international relations theory includes growing recognition that the **creation of** formal international **norms by state actors facilitates** (often inadvertently) **the political mobilisation of non-state actor**s.5 **By** **identifying with the** purposes of an international **norm**, **non-state actors legitimate their demands, gain access to state decision makers, and thus gain greater influence over state policy**. In some cases, **they may publicise a state’s non-compliance with its obligations under the norm in question**. In other cases, **they may pressure a state that is already in compliance to exert its in􏰝uence on non-compliant states**. **The ‘boomerang effect’ refers to situations where non-state actors apply this strategy transnationally in order to circumvent blocked domestic opportunities for pro- test**.6 International norms thus help non-state actors to create transnational networks capable of reshaping the conceptions of self-interest driving state behaviour.

### AT Root of Terror

**The alternative locks in the war system – infinite number of non-falsifiable ‘root causes’ means only incentive theory solves**

**Moore ’04** – Dir. Center for Security Law @ University of Virginia, 7-time Presidential appointee, & Honorary Editor of the American Journal of International Law, Solving the War Puzzle: Beyond the Democratic Peace, John Norton Moore, pages 41-2.

**If major interstate war is predominantly a product of a synergy between a potential nondemocratic aggressor and an absence of effective deterrence, what is the role of the many traditional "causes" of war**? Past, and many contemporary, theories of war have focused on the role of specific disputes between nations, ethnic and religious differences, arms races, poverty or social injustice, competition for resources, incidents and accidents, greed, fear, and perceptions of "honor," or many other such factors. **Such factors may well play a role in motivating aggression or in serving as a means for generating fear and manipulating public opinion**. **The reality**, **however**, **is that while some of these may have more potential to contribute to war than others, there may well be an infinite set of motivating factors, or human wants, motivating aggression**. **It is not the independent existence of such motivating factors for war but rather the circumstances permitting or encouraging high risk decisions leading to war that is the key to more effectively controlling war**. **And** **the same may also be true of democide**. The early focus in the Rwanda slaughter on "ethnic conflict," as though Hutus and Tutsis had begun to slaughter each other through spontaneous combustion, distracted our attention from the reality that a nondemocratic Hutu regime had carefully planned and orchestrated a genocide against Rwandan Tutsis as well as its Hutu opponents.I1 **Certainly if we were able to press a button and end poverty, racism, religious intolerance, injustice, and endless disputes, we would want to do so**. Indeed, democratic governments must remain committed to policies that will produce a better world by all measures of human progress. The broader achievement of democracy and the rule of law will itself assist in this progress. **No one**, however, **has yet been able to demonstrate the kind of robust correlation with any of these "traditional" causes of war as is reflected in the "democratic peace."** Further, **given the difficulties in overcoming many of these social problems, an approach to war exclusively dependent on their solution may be to doom us to war for generations to come.** A useful framework in thinking about the war puzzle is provided in the Kenneth Waltz classic Man, the State, and War,12 first published in 1954 for the Institute of War and Peace Studies, in which he notes that previous thinkers about the causes of war have tended to assign responsibility at one of the three levels of individual psychology, the nature of the state, or the nature of the international system. This tripartite level of analysis has subsequently been widely copied in the study of international relations. We might summarize my analysis in this classical construct by suggesting that the most critical variables are the second and third levels, or "images," of analysis. Government structures, at the second level, seem to play a central role in levels of aggressiveness in high risk behavior leading to major war. In this, the "democratic peace" is an essential insight. The third level of analysis, the international system, or totality of external incentives influencing the decision for war, is also critical when government structures do not restrain such high risk behavior on their own. Indeed, nondemocratic systems may not only fail to constrain inappropriate aggressive behavior, they may even massively enable it by placing the resources of the state at the disposal of a ruthless regime elite. It is not that the first level of analysis, the individual, is unimportant. I have already argued that it is important in elite perceptions about the permissibility and feasibility of force and resultant necessary levels of deterrence. It is, instead, that the second level of analysis, government structures, may be a powerful proxy for settings bringing to power those who may be disposed to aggressive military adventures and in creating incentive structures predisposing to high risk behavior. We should keep before us, however, the possibility, indeed probability, that a war/peace model focused on democracy and deterrence might be further usefully refined by adding psychological profiles of particular leaders, and systematically applying other findings of cognitive psychology, as we assess the likelihood of aggression and levels of necessary deterrence in context. A post-Gulf War edition of Gordon Craig and Alexander George's classic, Force and Statecraft,13 presents an important discussion of the inability of the pre-war coercive diplomacy effort to get Saddam Hussein to withdraw from Kuwait without war.14 This discussion, by two of the recognized masters of deterrence theory, reminds us of the many important psychological and other factors operating at the individual level of analysis that may well have been crucial in that failure to get Hussein to withdraw without war. We should also remember that nondemocracies can have differences between leaders as to the necessity or usefulness of force and, as Marcus Aurelius should remind us, not all absolute leaders are Caligulas or Neros. Further, the history of ancient Egypt reminds us that not all Pharaohs were disposed to make war on their neighbors. Despite the importance of individual leaders, however, we should also keep before us that major international war is predominantly and critically an interaction, or synergy, of certain characteristics at levels two and three, specifically an absence of democracy and an absence of effective deterrence. Yet another way to conceptualize the importance of democracy and deterrence in war avoidance is to note that each in its own way internalizes the costs to decision elites of engaging in high risk aggressive behavior. Democracy internalizes these costs in a variety of ways including displeasure of the electorate at having war imposed upon it by its own government. And deterrence either prevents achievement of the objective altogether or imposes punishing costs making the gamble not worth the risk. Testing the Hypothesis Theory without truth is but costly entertainment. **HYPOTHESES, OR PARADIGMS, are useful if they reflect the real world better than previously held paradigms**.

In the complex world of foreign affairs and the war puzzle, perfection is unlikely. **No general construct will fit all cases even in the restricted category of "major interstate war"; there are simply too many variables**. **We should insist**, however, **on testing against the real world and on results that suggest enhanced usefulness over other constructs**. In testing the hypothesis, we can test it for consistency with major wars; that is, in looking, for example, at the principal interstate wars in the twentieth century, did they present both a nondemocratic aggressor and an absence of effective deterrence?' And although it is by itself not going to prove causation, we might also want to test the hypothesis against settings of potential wars that did not occur. That is, in nonwar settings, was there an absence of at least one element of the synergy? We might also ask questions about the effect of changes on the international system in either element of the synergy; that is, what, in general, happens when a totalitarian state makes a transition to stable democracy or vice versa? And what, in general, happens when levels of deterrence are dramatically increased or decreased?

### Alt

**The ALT endless mass killings, genocide, and war in the name of state preservation**

**Burke 2007** (Anthony, Senior Lecturer in Politics and International Relations at UNSW, Sydney, Theory and Event 10.2, ontologies of war: violence, existence, and reason, project muse)

Schmitt is important both for understanding the way in which such alienation is seen as a definitive way of imagining and limiting political communities, and for understanding how such a rigid delineation is linked to the inevitability and perpetuation of war. Schmitt argued that the existence of a state 'presupposes the political', which must be understood through 'the specific political distinction...between friend and enemy'. The enemy is 'the other, the stranger; and it sufficient for his nature that he is, in a specially intense way, existentially something different and alien, so that in an extreme case conflicts with him are possible'.[31](http://muse.jhu.edu.ezproxy.mnl.umkc.edu/journals/theory_and_event/v010/10.2burke.html" \l "_edn31" \o ") The figure of the enemy is constitutive of the state as 'the specific entity of a people'.[32](http://muse.jhu.edu.ezproxy.mnl.umkc.edu/journals/theory_and_event/v010/10.2burke.html" \l "_edn32" \o ") Without it society is not political and a people cannot be said to exist: Only the actual participants can correctly recognise, understand and judge the concrete situation and settle the extreme case of conflict...to judge whether the adversary intends to negate his opponent's way of life and therefore must be repulsed or fought in order to preserve one's own form of existence.[33](http://muse.jhu.edu.ezproxy.mnl.umkc.edu/journals/theory_and_event/v010/10.2burke.html" \l "_edn33" \o ") Schmitt links this stark ontology to war when he states that the political is only authentic 'when a fighting collectivity of people confronts a similar collectivity. The enemy is solely the public enemy, because everything that has a relationship to such a collectivity of men, particularly to the whole nation, becomes public by virtue of such a relationship...in its entirety the state as an organised political entity decides for itself the friend-enemy distinction'.[34](http://muse.jhu.edu.ezproxy.mnl.umkc.edu/journals/theory_and_event/v010/10.2burke.html" \l "_edn34" \o ") War, in short, is an existential condition: the entire life of a human being is a struggle and every human being is symbolically a combatant. The friend, enemy and combat concepts receive their real meaning precisely because they refer to the real possibility of physical killing. War follows from enmity. War is the existential negation of the enemy.[35](http://muse.jhu.edu.ezproxy.mnl.umkc.edu/journals/theory_and_event/v010/10.2burke.html" \l "_edn35" \o ") **Schmitt claims that his theory is not biased towards war as a choice** ('It is by no means as though the political signifies nothing but devastating war and every political deed a military action...it neither favours war nor militarism, neither imperialism nor pacifism') **but** it is hard to accept his caveat at face value.[36](http://muse.jhu.edu.ezproxy.mnl.umkc.edu/journals/theory_and_event/v010/10.2burke.html" \l "_edn36" \o ") **When such a theory takes the form of a social discourse** (which it does in a general form) **such an ontology can only support,** as a kind of originary ground, **the basic** Clausewitzian **assumption that war can be a rational way of resolving political conflicts -- because the import of Schmitt's argument is that such 'political' conflicts are ultimately expressed through the possibility of war**. As he says: 'to the enemy concept belongs the ever-present possibility of combat'.[37](http://muse.jhu.edu.ezproxy.mnl.umkc.edu/journals/theory_and_event/v010/10.2burke.html" \l "_edn37" \o ") Where Schmitt meets Clausewitz, as I explain further below, **the existential and rationalistic ontologies of war join into a closed circle of mutual support and justification. This closed circle of existential and strategic reason generates a number of dangers. Firstly, the emergence of conflict can generate military action almost automatically simply because the world is conceived in terms of the distinction between friend and enemy; because the very existence of the other constitutes an unacceptable threat, rather than a chain of actions, judgements and decisions.** (As the Israelis insisted of Hezbollah, they 'deny our right to exist'.) **This effaces agency, causality and responsibility from policy and political discourse: our actions can be conceived as independent of the conflict or quarantined from critical enquiry, as necessities that achieve an instrumental purpose but do not contribute to a new and unpredictable causal chain.** Similarly the Clausewitzian idea of force - which, by transporting a Newtonian category from the natural into the social sciences, assumes the very effect it seeks - further encourages the resort to military violence. **We ignore the complex history of a conflict, and thus the alternative paths to its resolution that such historical analysis might provide, by portraying conflict as fundamental and existential in nature; as possibly containable or exploitable, but always irresolvable**. Dominant portrayals of the war on terror, and the Israeli-Arab conflict, are arguably examples of such ontologies in action. Secondly, the militaristic force of such an ontology is visible, in Schmitt, in the absolute sense of vulnerability whereby a people can judge whether their 'adversary intends to negate his opponent's way of life'.[38](http://muse.jhu.edu.ezproxy.mnl.umkc.edu/journals/theory_and_event/v010/10.2burke.html" \l "_edn38" \o ") Evoking the kind of thinking that would become controversial in the Bush doctrine, Hegel similarly argues that: ...a state may regard its infinity and honour as at stake in each of its concerns, however minute, and it is all the more inclined to susceptibility to injury the more its strong individuality is impelled as a result of long domestic peace to seek and create a sphere of activity abroad. ....the state is in essence mind and therefore cannot be prepared to stop at just taking notice of an injury after it has actually occurred. On the contrary, there arises in addition as a cause of strife the idea of such an injury...[39](http://muse.jhu.edu.ezproxy.mnl.umkc.edu/journals/theory_and_event/v010/10.2burke.html" \l "_edn39" \o ") **Identity, even more than physical security or autonomy, is put at stake in such thinking and can be defended and redeemed through warfare (or,** when taken to a further extreme of an absolute demonisation and dehumanisation of the other, by **mass killing, 'ethnic cleansing' or genocide**).

**The alt fails – states won’t accept transition to true enmity. Schmitt’s theories are no longer practical.**

Kim Lane **Scheppele**, and John J. **O'Brien** Professor of Comparative Law and Professor of Sociology, University of Pennsylvania, May **2004**, University of Pennsylvania Journal of Constitutional Law, 6 U. Pa. J. Const. L. 1001, p.1082-1083

In this Article, I have tried to explain why **the logic of Schmitt's analyses no longer work as a practical matter to justify states of exception, even when it is clear to the international community that something fundamental has changed in the world system since 9/11. The institutional elaboration of a new international system that has occurred since Schmitt's time make his ideas seem all the more dangerous, and** yet all the more **dated**. **There are simply fewer states in the world willing to tolerate either Schmitt's conception of politics or his conception of the defining qualities of sovereignty**. Schmitt's philosophy has, in short, been met with a different sociology. For his ideas to be either persuasive or effective, they must be more than internally coherent or even plausible; they must be loosed in a context in which they can win against other competing ideas. Precisely because of the horrors of the twentieth century, much of the international community that has entrenched both democracy and the rule of law has turned away from these extra-legal justifications for states of exception. Instead, such **states have attempted to embed exceptionality as an instance of the normal, and not as a repudiation of the** [\*1083] **possibility of normality**. Only the United States, with its eighteenth-century constitution and Cold War legacy of exceptionalism, seems to be soldiering on in this new legal space of conflict unaware that the defining aspect of the new sovereignty is that even the new sovereign is bound by rules.