# 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

**Cyberwar is probable- multiple IR theories prove**

**Junio ‘13**

[Timothy J. Junio (Tim)is a doctoral candidate of political science at the¶ University of Pennsylvania and a predoctoral fellow at the Center for¶ International Security and Cooperation (CISAC) at Stanford University.¶ He also develops new cyber capabilities at the Defense Advanced¶ Research Projects Agency (DARPA). How Probable is Cyber War? Bringing¶ IR Theory Back In to the Cyber Conflict Debate, Journal of Strategic Studies, 36:1,¶ 125-133. ETB]

Two recent articles in the pages of this journal contribute to an¶ important debate about how information technology (IT) inﬂuences¶ international politics.1¶ Thomas **Rid and** Adam **Liff argue that** **cyber**¶ **‘war’** has never happened and probably **will not happen. A fundamental**¶ **problem** with these articles **is that Rid and Liff do not commit to a**¶ **theoretical framework regarding the causes of war.** **Doing so yields an**¶ **opposite conclusion: international relations theory identiﬁes many**¶ **mechanisms that may cause violent escalation with cyber weapons**.¶ This brief response article explains why **cyber war is sufﬁciently**¶ **probable to merit serious attention from scholars and practitioners**,¶ and proposes a theoretical research agenda. **First, domestic political**¶ **factors** – such as states’ command and control over cyber operations –¶ **must be problematized**. **The principal-agent approach demonstrates**¶ **how variation in incentives and preferences may make militaries more**¶ **likely to favor cyber attack than other kinds of bureaucracies.** This¶ matters in societies with poor civilian control over the military. Second,¶ **the unique material qualities of IT must be evaluated alongside**¶ **traditional mechanisms that cause war**. For instance, **the attribution**¶ **problem and computational complexity in modeling cyber operations**¶ **may increase the odds of inadvertent cyber war by causing states to**¶ **retaliate against the wrong targets or miscalculate the potential costs**¶ **and gains of attacking.**

**Cyberwar escalates:**

**A) Speed, scope, and spoofing**

**Clarke and Knake ‘12**

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

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

**b) Pressure to retaliate**

**Owens et al 9**

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

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

**c) interconnectedness, pace of tech development and info flow, and decreasing legal constraints**

**Farwell and Rohozinski ‘12**

[James Farwell is an expert in strategic communication and has advised the Department of Defense on strategic and political issues in the Middle East. He is author of The Pakistan Cauldron: Conspiracy, Assassination & Instability (Washington: Potomac Books, 2011) and the forthcoming Persuasion & Power (Washington: Georgetown University Press, 2012.¶ Rafal Rohozinski is a principal and CEO of the SecDev Group. He is a cofounder and principal investigator of the Information Warfare Monitor and OpenNet initiative, and author of numerous papers and studies addressing risk and the nexus between conflict, development, and the emerging global cyberspace domain. He was previously the director of the Advanced Network Research Group, Cambridge Security Programme, University of Cambridge. “The New Reality of Cyber War.” *Survival: Global Politics and Strategy*, vol. 54, no. 4, August–September 2012, pp. 107-120. ETB]

These developments put the spotlight on a new era of international engagement. Israeli sources have long boasted about Israel’s involvement in Stuxnet. The US/Israeli use of Stuxnet as reported in detail by Sanger has arguably created a new de facto norm for the conduct of cyber engagements other nations can follow or imitate. **Previously, a key constraint on the use of software as a weapon has been the potential for legal liability arising out of collateral damage inflicted upon innocent parties not targeted**. In practice, **software can be narrowly targeted to surmount that challenge.**¶What Stuxnet shows is that it is possible to have the specific intended effect while avoiding or minimising unplanned side effects by clearly differentiating between the propagator, or boost-phase code that disseminates the program, and the actual payload code that creates the physical effect on a target (the distinction between the gift wrapping and the gift). The reported operation did apparently limit the scope of damage. Stuxnet shows that one can surmount concerns that malware would take down the global network, not just a specific target. The lesson is that **cyber weapons are in a different category from nuclear devices, which have little practical use except as a deterrent.**¶ **The rules of conduct for the use of code are evolving. As parties develop more sophisticated capabilities and acquire experience in their use, the picture will grow more complicated and nuanced. The strategic situation contains echoes of the period between the two world wars, when rapid developments in new technologies and domains of war-fighting preceded an understanding of how effectively to employ them operationally**. Tanks changed the way armies engaged in battle. But despite British and German experimentation with armour in the inter-war period, armoured tactics could only be proven and fully developed on the battlefield from 1939 onwards. There are, moreover, significant differences of view about whether the Germans, renowned for their blitzkrieg tactics, properly understood the strategic use of armour for manoeuvre warfare.¶ **Reports that two states have employed code against another state against which war has not been declared undercuts the common view that risks of escalation render state-to-state cyber war implausible**. Sanger reported that President George W. Bush, under whom Olympic Games was apparently initiated, desired that use of Stuxnet not violate the rules of armed conflict.(4) The Law of Armed Conflict does not prohibit damage to such critical infrastructure. But a strength of using code is that the targeting process can manage the risks.¶ **Stuxnet may appear as embryonic as the British Mk.1 tanks that made their debut at the Battle of the Somme** in 1916. **But technology moves quickly.** **Modern states rightly fear cyber war. Evolving technology is accelerating the flow of information, placing unique pressures on decision-making. Responding to cyber attack may require making decisions at network speed using systems that are themselves targeted. The potential for cascading effects is amplified by the interconnectedness of cyberspace.** Stuxnet worked leisurely. **Future combat in cyberspace may be more akin to the global trading system than existing forms of kinetic engagement, and present a different strategic calculus.**

### SOP

**Constraining a militarized cyberwar policy is key to soft power.**

**Belk and Noyes ‘12**

(Robert (Naval aviator and Politico-Military Fellow, studying international and global affairs at the Harvard Kennedy School) and Matthew (studies international security policy and is a senior associate with the cybersecurity practice at Good Harbor Consulting), “On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy”, 3-20-12, Office of Naval Research, RSR)

Over the past decade, **hard power has dominated U.S. foreign policy often** ¶ **to the detriment of U.S. influence and national security**. **To avoid such missteps** in cyberspace, **policy-makers should analyze the way the international** ¶ **community will interpret American use of cyber force**. While this may seem selfevident, especially in light of the fact that we have often equated cyber force with ¶ other uses of force, there are relevant distinctions for force executed through ¶ cyberspace.¶ First, **the history of cyberspace** (and particularly the Internet) **has** ¶ **overwhelmingly been driven by non-military use**. The inherent insecurity with ¶ current global networks stems predominantly from the fact that the Internet was ¶ originally designed for openness and flexibility.138 **Security has always been a** ¶ **secondary concern**. For this reason, **the overwhelming majority of users of** ¶ **cyberspace place a premium on the nature of the Internet as an open**, ¶ empowering **medium**. **Use of cyber force may alter foreign perception of the U.S.** ¶ **as trying to militarize cyberspace**. **The Chinese have already asserted that**, by ¶ creating CYBERCOM, **the U.S. has indeed done exactly that**.**139 An actual use of** ¶ **cyber force might convince others that the Chinese argument has merit.**¶ For that reason, **cyber force**, as the sole aspect of an operation, **may be** ¶ **counterproductive to U.S. interests if the destructive effect were large enough, if** ¶ **there were significant collateral damage, or if the targets were non-state actors**.¶ Drone strikes against Tehrik-i-Talibani (TTP) in the tribal areas of Pakistan are ¶ contentious enough (and certainly have a cost in terms of U.S. soft power).¶ **Targeting any insurgent or terrorist group through cyber means may prove even** ¶ **more costly.**¶ As described in the “Strategic” section above, **cyber force** as an aspect of a ¶ coordinated (and legitimized) military operation **may appear to the international public as new U.S. military technology and not civilian technology co-opted by** ¶ **the world’s remaining hegemon for military purposes**. **This is a critical** ¶ **distinction, and the context of using cyber force may drive the way it is perceived** ¶ **abroad and hence the way such an operation affects American soft power.**

**Soft power prevents extinction – disease, climate change, terrorism, and great power war**

Joseph **Nye 8** is professor of international relations at Harvard University, “American Power After the Financial Crises,” <http://www.foresightproject.net/publications/articles/article.asp?p=3533>, DOA: 7-23-13, y2k

Power always depends on context, and in today's world, it is distributed in a pattern that resembles a complex three-dimensional chess game. On the top chessboard, military power is largely unipolar and likely to remain so for some time. But on the middle chessboard, economic power is already multi-polar, with the US, Europe, Japan and China as the major players, and others gaining in importance. **The bottom chessboard is the realm of transnational relations that cross borders outside of government control,** and **it includes actors as** **diverse as bankers** electronically **transferring sums larger than most national budgets** at one extreme, **and terrorists transferring weapons** **or hackers disrupting Internet operations** at the other. **It** also **includes new challenges like pandemics and climate change**. On this bottom board, power is widely dispersed, and it makes no sense to speak of unipolarity, multi-polarity or hegemony. **Even in the aftermath of the financial crisis, the giddy pace of technological change is likely to continue to drive globalisation, but the political effects will be quite different for the world of nation states and the world of non-state actors**. In inter-state politics, the most important factor will be the continuing "return of Asia". In 1750, Asia had three-fifths of the world population and three-fifths of the world's product. By 1900, after the industrial revolution in Europe and America, Asia's share shrank to one-fifth of the world product. By 2040, Asia will be well on its way back to its historical share. **The "rise" in the power of China and India may create instability**, but it is a problem with precedents, and we can learn from history about how our policies can affect the outcome. **A century ago, Britain managed the rise of American power without conflict, but the world's failure to manage the rise of German power led to two devastating world wars.** In transnational politics, **the information revolution is dramatically reducing the costs of computing and communication. Forty years ago, instantaneous global communication was possible but costly, and restricted to governments and corporations**. Today it is virtually free to anyone with the means to enter an internet café. **The barriers to entry into world politics have been lowered, and non-state actors now crowd the stag**e. In 2001, **a non-state group killed more Americans than the government of Japan killed at Pearl Harbor**. **A pandemic** spread by birds or travelers on jet aircraft **could kill more people than perished in the first or second world wars**. This is a new world politics with which we have less experience. The problems of power diffusion (away from states) may turn out to be more difficult than power transition among states. **The problem for American power in the 21st century is that there are more and more things outside the control of even the most powerful state**. Although the United States does well on the traditional measures, there is increasingly more going on in the world that those measures fail to capture. **Under the influence of the information revolution and globalisation, world politics is changing in a way that means Americans cannot achieve all their international goals acting alone**. For example, **international financial stability** **is vital to the prosperity of Americans, but the United States needs the cooperation of others to ensure it**. **Global climate change too will affect the quality of life, but the United States cannot manage the problem alone**. **And in a world where borders are becoming more porous than ever to everything from drugs to infectious diseases to terrorism, America must mobilise international coalitions to address shared threats and challenges.** As the largest country, American leadership will remain crucial. The problem of American power after this crisis is not one of decline, but realisation that **even the largest country cannot achieve its aims without the help of others.**

### T

#### OCO’s includes cyber attacks and cyber exploitations

Lin ‘10

[Herbert S., Chief Scientist, Computer Science and Telecommunications Board, National ¶ Research Council (NRC) of the National Academies. At the NRC, Dr. Herbert Lin has been ¶ study director of major projects on public policy and information technology. Prior to his ¶ NRC service, he was a staff member and scientist for the House Armed Services Committee ¶ (1986-1990), where his portfolio included defense policy and arms control issues. OFFENSIVE CYBER OPERATIONS AND THE USE OF FORCE . JOURNAL OF NATIONAL SECURITY LAW &POLICY 4.63. ETB]

Offensive cyber operations (cyber attacks and cyber exploitations) pose ¶ many challenges for the interpretation of jus ad bellum and the U.N. ¶ Charter, some of which have been addressed in this article. In the long run, ¶ it is inevitable that some future conflict will have a cyber component to it, ¶ and it behooves policy makers to understand the legal landscape before ¶ such a conflict occurs. A central recommendation of the NRC Report is ¶ that analysts develop the requisite knowledge and expertise now so that ¶ they are prepared to help policy makers if and when such conflict occurs. ¶ By exploring some of the relevant questions, this article takes one modest ¶ step on that path of exploration

#### Cyber attacks must have physical effects outside of the affected system

Brown and Tullos ‘12

[Colonel Gary D. Brown, USAF, has been the Staff Judge Advocate at U.S. Cyber Command since its inception in May 2010. He holds a J.D. and an LL.M. in International Law, and is a Nebraska attorney. Lieutenant Colonel Owen W. Tullos, USAF, was the Deputy Staff Judge Advocate for Operations Law at U.S. Cyber Command, Ft. Meade, Maryland until July 2012. He holds a J.D. and an LL.M. with a dual specialty in International Law and Operations Law. He is a member of the South Dakota bar. <http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations> ETB]

Cyber Attack

Cyber attack falls on the right of the spectrum and moves farther to the right depending on the severity of the attack. In contrast to the way the term “computer network attack” is used by DoD, “cyber attack” as used here means cyber activity that has effects in the real world beyond the cyber system itself. Mere degradation or denial of a system, for example, are not cyber attacks. The definition of cyber attack used here is actions in cyberspace whose foreseeable results include damage or destruction of property, or death or injury to persons.¶ To date, the best real-world example of a cyber attack is Stuxnet, an operation reportedly carried out by Israel and the US to slow Iran’s development of nuclear weapons. Reports of Stuxnet estimate 1,000 Iranian centrifuges were damaged beyond repair when stealthy malware caused machines to spin at certain high and low ranges. The result of the Stuxnet activity – destruction of equipment – would make it a cyber attack under the cyber spectrum proposed here. Stuxnet falls in the red category, and illustrates how physical destruction may occur via cyberspace and constitute a use of force – an attack equivalent to one conducted using traditional means of warfare.¶ A tragic accident that occurred in Russia in 2009 provides a hypothetical example of what a cyber attack at the far right end of the spectrum could look like. A damaged turbine at the Sayano-Shushenskaya hydroelectric power plant had been shut down for maintenance. A computer operator at a control facility, located far from the dam, seeking to correct for a loss in available power, brought the damaged turbine back on line. The operator’s electronically delivered command for increased activity caused the damaged turbine to spin out of control, killing 75 people and causing over $1 billion damage. While the official investigation of the dam failure blamed poor management and technical flaws, this tragedy demonstrates how wrongdoers might theoretically take control of a computer system and cause horrific damage by manipulating it.¶ Had the event at Sayano-Shushenskaya been caused by malicious cyber actors, it would have crossed the line to attack. Like Stuxnet, it would have served as an example of the kind of physical effects that define a genuine attack. Aligning the meaning of “attack” in the cyber context with the way the term is used in other domains allows for a more precise analysis of cyber activities under international law. Specifically, it would leave the operating space in the middle of the spectrum, the disruptive activities, to be analyzed separately.

### CP 1

#### No solvency- Congress CANNOT prohibit

Colella ‘88

Frank SPRING, 1988 54 Brooklyn L. Rev. 131

Because the subsequent versions of the amendment sought to deny the executive any latitude in supporting the Contras, they seem to be examples of congressional overreaching. Congress may regulate aspects of "foreign covert action," but it cannot totally bar the president from carrying them out. n151 One commentator incisively observes, "[C]ongress cannot deny the President the capacity to function effectively in this area any more than it could deny the courts the capacity to carry out their independent constitutional duties." n152 The restrictions contained in later versions of the amendments n153 make it apparent that Congress prevented effective execution of the president's policy objectives.

**Distrust of the president and fear of rollback means no modeling- impact is cyber war**

**Rothschild** **13** (Matthew, Feb 4, "The Danger's of Obama's Cyber War Power Grab," www.progressive.org/dangers-of-obama-cyber-war-power-grab)

When our **founders** were drafting the Constitution, they **went out of their way to give warmaking powers to Congress, not the President.**¶ **They understood that if the President could make war on his own, he’d be no different than a king.**¶ And they also understood, as James Madison said, that such power “would be too much temptation” for one man.¶ And so they vested that power in Congress.¶ But since World War II, one President after another has usurped that power.¶ The latest usurper is President Obama, who did so in Libya, and with drones, and now is prepared to do so in cyberspace.¶ According to The New York Times, **the Obama Administration has concluded that the President has the authority to launch preemptive cyberattacks.**¶ **This is a** very **dangerous**, and very undemocratic **power grab.**¶ **There are no checks** or balances **when the President, alone, decides when to engage in an act of war.**¶ And **this** new aggressive stance **will lead to a cyber arms race.** The United States has evidently already used cyber weapons against Iran, and so many **other countries will assume** that **cyber warfare is** an **acceptable** tool **and** will try to **use it themselves.**¶ **Most troubling, U.S. cybersupremacy—and that is Pentagon doctrine—will also raise fears among nuclear powers like Russia, China, and North Korea that the United States may use a cyberattack as the opening move in a nuclear attack.**¶ For **if the United States can knock out the command and control structure of an enemy’s nuclear arsenal, it can then launch an all-out nuclear attack on that enemy with impunity. This would make such nuclear powers more ready to launch their nuc**lear weapon**s preemptively for fear that they would be rendered useless.** So **we’ve just moved a little closer to midnight**.¶ Now, I don’t think Obama would use cyberwafare as a first strike in a nuclear war. But **our adversaries may not be so sure, either about Obama or his successors.**¶ **They, too, worry about the temptations of a President**.

**Doesn’t solve SOP- CP retains preemptive capability at presidential discretion, which means the president has still usurped the power- cementing congressional authority means it stays balanced- and if congress stays silent it’ll lead to massive expansion of aggressive presidential powers- that’s Huston, Lorber, and Dycus**

#### Links to politics – congress wants to be involved

Sasso 2012

(Brandon Sasso, December 21, 2012, “House Republicans urge Obama not to issue cybersecurity order,” The Hill, http://thehill.com/blogs/hillicon-valley/technology/274391-house-republicans-urge-obama-not-to-issue-cybersecurity-order)

A group of 46 House Republicans, led by Reps. Marsha Blackburn (Tenn.) and Steve Scalise (La.), sent President Obama a letter on Friday urging him not to issue an executive order on cybersecurity.¶ "Instead of preempting Congress' will and pushing a top-down regulatory framework, your administration should engage Congress in an open and constructive manner to help address the serious cybersecurity challenges facing our country," the lawmakers wrote. ¶ The White House is currently drafting an executive order that would encourage operators of critical infrastructure, such as banks and electric grids, to meet cybersecurity standards. ¶ The administration says the order, which could come as early as January, is necessary to protect vital systems from hackers.¶ The White House began working on the order after Senate Republicans blocked the Democrats' preferred cybersecurity bill.¶ But in their letter, the House Republicans urged the administration to continue working with Congress.

### CP 2

**2ac- Put Under Cover Action Statute CP**

**Links to politics**

**Goldsmith ‘13**

[Jack, Washington Post, <http://articles.washingtonpost.com/2013-02-05/opinions/36757699_1_government-lawyers-secret-warfare-al-qaeda> ETB]

**A new** legal and political **foundation** for stealth warfare **cannot succeed without** **the** initiative and **support of the president. The chances of such support**, however, **are dim**. The **Obama** administration **prefers to act based on old authorities and not to engage Congress in establishing new authorities for new wartime challenges.** This is unfortunate for U.S. constitutional traditions and for the stability of our long-term counterterrorism strategy. And **it is unfortunate for the president, not only because he increasingly acts without political cover, and because his secret wars are increasingly criticized and scrutinized abroad, but also because he alone will be bear the legacy of any negative consequences** — at home and globally — **of unilateral,** lethal, **secret warfare.**

### Politics

#### PC low and fails for fiscal fights

Greg Sargent 9-12, September 12th, 2013, "The Morning Plum: Senate conservatives stick the knife in House GOP leaders," Washington Post, factiva

All of this underscores a basic fact about this fall's fiscal fights: Far and away the dominant factor shaping how they play out will be the divisions among Republicans. There's a great deal of chatter (see Senator Bob Corker for one of the most absurd examples yet) to the effect that Obama's mishandling of Syria has diminished his standing on Capitol Hill and will weaken him in coming fights. But those battles at bottom will be about whether the Republican Party can resolve its internal differences. Obama's "standing" with Republicans -- if it even could sink any lower -- is utterly irrelevant to that question.¶ The bottom line is that, when it comes to how aggressively to prosecute the war against Obamacare, internal GOP differences may be unbridgeable. Conservatives have adopted a deliberate strategy of deceiving untold numbers of base voters into believing Obamacare will be stopped outside normal electoral channels. Central to maintaining this fantasy is the idea that any Republican leader who breaks with this sacred mission can only be doing so because he or she is too weak and cowardly to endure the slings and arrows that persevering against the law must entail. GOP leaders, having themselves spent years feeding the base all sorts of lies and distortions about the law, are now desperately trying to inject a does of reality into the debate by pointing out that the defund-Obamacare crusade is, in political and practical terms alike, insane. But it may be too late. The time for injecting reality into the debate has long since passed.

#### Energy floor debates pound the DA

Amy Harder 9/12, and Clare Foran, National Journal, "The Energy Debate That Wasn't", 2013, www.nationaljournal.com/daily/the-energy-debate-that-wasn-t-20130912?mrefid=mostViewed

The second day of the Senate's first floor debate on an energy bill in six years was marked by obstruction, opposition, and frustration.¶ Sen. David Vitter, R-La., held firm in his refusal to allow debate to move forward to an energy-efficiency bill until Senate leaders agree on a time to vote on his amendment related to President Obama's health care law. Vitter first interfered with the energy debate Wednesday afternoon, shortly after Senate Majority Leader Harry Reid, D-Nev., moved to the bill in place of the Syria resolution that was put on hold.¶ Vitter's stance put an uncontroversial measure with broad support on a difficult legislative obstacle course.¶ "Senators who have talked about energy policy for years and years now say they want to have their issues that are unrelated to energy advance today, even though they have the potential to undermine this bill," Senate Energy and Natural Resources Chairman Ron Wyden, D-Ore., said on the floor, showing clear frustration. "I don't know how that adds up, if you give a lot of speeches at home about sensible energy policy and then take steps to undermine it."¶ Wyden didn't name any names, but he didn't have to.¶ "Since they were all directed at my activity, I want to respond," said Vitter just moments after Wyden concluded his comments. "I have nothing against this bill, I applaud that work. I did hear a lot this summer—quite frankly, I didn't hear about this bill or any provision of this bill. But I'm not denigrating it."¶ Vitter isn't the only Republican seeking to pivot the debate. Senate Minority Leader Mitch McConnell, R-Ky., also filed an amendment to the energy bill seeking to delay a key part of Obamacare. He spoke about the amendment Thursday morning but didn't mention the energy bill at all.¶ A number of other Republican senators also used floor time to voice opposition to the health care law, including John Barrasso of Wyoming, Dan Coats of Indiana, and Jeff Flake of Arizona.¶ Among the GOP voices, Vitter's was the loudest. Whether senators will actually get to debate energy—even controversial issues like the Keystone XL pipeline and climate-change regulations—now hinges on whether Vitter either backs down from his amendment or comes to an agreement with Senate leaders on another path to vote on it down the road.¶ Even if a deal is reached with Vitter, more obstacles await. Sens. John Hoeven, R-N.D., and Mary Landrieu, D-La., introduced an amendment Thursday that would declare the Keystone pipeline to be in the national interest. A decision on a permit for the controversial project is still pending at the State Department.¶ On another thorny issue, Sens. Joe Donnelly, D-Ind., and Roy Blunt, R-Mo., introduced an amendment that would ban the Environmental Protection Agency from requiring costly carbon-capture and sequestration technology to be used in order to comply with climate-change regulations. The amendment would instead require the EPA to develop technology standards for different fuels and different sources of emissions.¶ Barrasso is also pushing an amendment to block the agency's upcoming climate rules unless they are approved by Congress. The EPA is expected to issue regulations limiting carbon emissions for new power plants very soon.

#### Debt ceiling will inevitably be raised, despite fights

Fisher 8-28

Fisher Investments, independent investment advisor with offices in Washington and California, “The Return of the Debt Ceiling,” 8/28/13, <http://www.marketminder.com/a/fisher-investments-the-return-of-the-debt-ceiling-part-108/5df0e3a8-cdac-4718-a17f-1c98aa75bdf0> SJE

That said, chances are the Treasury doesn’t stay in this pickle for long, if it even gets there. It’s a virtual certainty Congress will up the debt ceiling—as it has 107 times before—whether in the 11th hour or a little after. Yes, Congress is gridlocked. Yes, both sides have drawn lines in the sand: The Obama administration will not negotiate over the debt limit, while some in Congress promise a “whale of a fight” if their demands aren’t met. But this political posturing, maddening as it may be, is part of the negotiation process. Since the debt ceiling was born, legislators have used it as leverage to get what they want from the opposing party. But they always raise it, and Congress has every incentive to do it again. Congress is full of hundreds of politicians who want to be re-elected—they know their chances are slim if they do anything voters might perceive as putting the US in a precarious fiscal position. Expect plenty of political chest puffing and finger pointing, but ultimately, some sort of resolution to the debt ceiling despite the gridlock. After all, that’s pretty much Congress’s M.O. these days. Remember the fiscal cliff? Congress reached a “compromise” on New Year’s Day after months of grandstanding. Heck, this past May Congress raised the debt ceiling with a temporary waiver! Congress’ favorite pastime seems to be kicking the can down the road—and it’s no different with this iteration of the debt ceiling. Sometimes, like in the recent student loan legislation, they break out the Congressional time machine and retroactively kick the can. Now sure, we may see some day-to-day market volatility as politicians politick. But that shouldn’t alter stocks’ longer-term trajectory. Just like the debt ceiling, we expect this bull market to continue to rise.

#### 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.”

#### Obama won’t push the plan – no PC loss

**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.”¶

#### No food wars – empirics go aff – tech solves

#### Alt causes to food prices - warming

Carrington 11

Damian Carrington 11, head environment reporter at the Guardian, “Food prices driven up by global warming, study shows”, May 5, <http://www.guardian.co.uk/environment/2011/may/05/food-prices-global-warming>

Global warming has already harmed the world's food production and has driven up food prices by as much as 20% over recent decades, new research has revealed. The drop in the productivity of crop plants around the world was not caused by changes in rainfall but was because higher temperatures can cause dehydration, prevent pollination and lead to slowed photosynthesis. Lester Brown, president of the Earth Policy Institute, Washington DC, said the findings indicate a turning point: "Agriculture as it exists today evolved over 11,000 years of reasonably stable climate, but that climate system is no more." Adaptation is difficult because our knowledge of the future is not strong enough to drive new investments, he said, "so we just keep going, hoping for the best." The scientists say their work shows how crucial it is to find ways to adapt farming to a warmer world, to ensure that rises in global population are matched by rising food production. "It is vital," said Wolfram Schlenker, at Columbia University in New York and one of the research team. "If we continue to have the same seed varieties and temperatures continue to rise, then food prices will rise further. [Addressing] that is the big question." The new research joins a small number of studies in which the fingerprint of climate change has been separated from natural variations in weather and other factors, demonstrating that the effects of warming have already been felt in the world. Scientists have shown that the chance of the severe heatwave that killed thousands in Europe in 2003 was made twice as likely by global warming, while other work showed that the floods that caused £3.5bn of damage in England in 2000 were made two to three times more likely.

#### New tech and adaption solve food shortages

Michaels 11

Patrick Michaels is senior fellow in environmental studies at the CATO Institute. " Global Warming and Global Food Security," June 30, CATO, <http://www.cato.org/publications/commentary/global-warming-global-food-security>

While doing my dissertation I learned a few things about world crops. Serial adoption of new technologies produces a nearly constant increase in yields. Greater fertilizer application, improved response to fertilizer, better tractor technology, better tillage practices, old-fashioned genetic selection, and new-fashioned genetic engineering all conspire to raise yields, year after year.¶ Weather and climate have something to do with yields, too. Seasonal rainfall can vary a lot from year-to-year. That's "weather." If dry years become dry decades (that's "climate") farmers will switch from corn to grain sorghum, or, where possible, wheat. Breeders and scientists will continue to develop more water-efficient plants and agricultural technologies, such as no-till production.¶ Adaptation even applies to the home garden. The tomato variety "heat wave" sets fruit at higher temperatures than traditional cultivars.¶ However, Gillis claims that "[t]he rapid growth in farm output that defined the late 20th century has slowed" because of global warming.¶ His own figures show this is wrong. The increasing trend in world crop yields from 1960 to 1980 is exactly the same as from 1980 to 2010. And per capita grain production is rising, not falling.

#### PC fails

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.

#### 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.

### AT Fight Back

#### No fight back

Bannon 13

(Brad Bannon runs Bannon Communications Research, a political polling and consulting firm which helps labor unions, progressive issue groups, and Democratic candidates win public affairs and political campaigns, May 28, 2013, <http://www.usnews.com/opinion/blogs/brad-bannon/2013/05/28/obama-wants-us-to-take-away-his-war-powers--we-should>, “An Offer We Can’t Refuse”, AB)

President Obama kicked off the long Memorial Day weekend with a speech which had a request that you hardly get from a president or anybody else in Washington. The president asked Congress to take away some of his power. This is not the kind of offer that comes along very often, so Congress should snap it up while it's still on the table. President Obama asked Congress to replace or refine the Authorization for the Use of Military Force that Congress passed after the al-Qaida attack on the World Trade Center on 9/11. President George W. Bush used the authorization as a blank check to justify illegal renditions, drone attacks, indefinite detention and just about anything else he and Vice President Dick Cheney wanted to do. Reduction in presidential authority with the repeal of authorization would mean more power for the federal legislative branch to review and restrain the president's actions.

### Prez Powers

### 2ac- Flex DA

#### No link- plan preserves presidential flexibility by allowing retaliation during crisis- falling short of a complete ban preserves flex- that’s Clarke and Knake, and Dycus

#### Obama weak now- Syria deal

Maloof 9/13

F. Michael Maloof, senior staff writer for WND and the G2Bulletin, is a former security policy analyst in the Office of the Secretary of Defense¶ Read more at <http://www.wnd.com/2013/09/putin-makes-obama-look-indecisive-weak/#JFIueVqdjRHQa1GD.99> ETB

If Kerry and Lavrov come up with a plan, it will further consolidate Putin’s efforts in the Middle East, at U.S. expense.¶ “If the U.S. administration were to ignore Russian protests and proceed with a (military) strike with at least rhetorical coalition support, Russia would have little to show for its claimed influence in the Middle East,” according to the open intelligence group Stratfor.¶ “However, if Russia could effectively stunt the U.S.-led military campaign through an airy diplomatic proposal, then Russia will have played a hand in directly showcasing U.S. unreliability to its allies,” it said.¶ A proposal could make the U.S. look weak and indecisive while Moscow comes off “as the voice of reason” in a war that no one wants, and it will be all the Obama administration’s doing.

#### It’s impossible for the president to remain adequately flexible on cyber

Waxman ‘11

[Associate Professor, Columbia Law School; Adjunct Senior Fellow, Council on Foreign

Relations; Member of the Hoover Institution Task Force on National Security and Law. THE YALE JOURNAL OF INTERNATIONAL LAW 36:421. <http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf> ETB]

Such interpretive reorientation raises subsidiary doctrinal issues that¶ might not sit comfortably with extant U.S. legal positions about the resort to¶ force more generally. For example, in recent years the U.S. government has pushed an interpretation of anticipatory self-defense—the doctrinal notion that¶ a state may resort to self-defensive force in advance of an imminent attack,¶ rather than having to wait to suffer the first blow—that permits flexibility in¶ assessing the “imminence” of a threat so as to take account of the difficulty of¶ assessing when contemporary security threats are temporally immediate.72 If cyber-attacks with certain effects give rise to rights of self-defense, could an impending one give rise to such a right in advance as well? Moreover, how would a state even assess imminence in this context?73 Anticipatory selfdefense is especially difficult to evaluate in this context because even if hostile¶ cyber-attack capabilities and intentions are identified, there may be little or no¶ indication of their future timing. It may also be impossible to assess their likely consequences in advance, because modern society’s heavy reliance on¶ interconnected information systems means that the indirect secondary or¶ tertiary effects of cyber-attacks may be much more consequential than the¶ direct and immediate ones.74

**Massive alt causes**

**Rozell 12**

(Mark Rozell, Professor of Public Policy, George Mason University, “From Idealism to Power: The Presidency in the Age of Obama” 2012, <http://www.libertylawsite.org/book-review/from-idealism-to-power-the-presidency-in-the-age-of-obama/>, KB)

A substantial portion of Goldsmith’s book presents in detail his case that **various forces** outside of government, and some within, **are responsible for hamstringing the president** in unprecedented fashion: **Aggressive**, often intrusive, **journalism, that at times endangers national security; human rights and other advocacy groups**, some **domestic and** other **cross-national, teamed with big resources and talented, aggressive lawyers, using every legal category and technicality possible to complicate executive action**; **courts** thrust into the mix, **having to decide critical national security law controversies**, even when the judges themselves have little direct knowledge or expertise on the topics brought before them; **attorneys within the executive branch** itself **advising against actions** based on often narrow legal interpretations and with little understanding of the broader implications of tying down the president with legalisms.

# 1AR

## CP

## Prez Powers

### UQ

#### Syia sent international signal of weakness – cant reverse what he asked for – nobody trusts that - that’s Karabell

#### Obama is sending global signals of weakness and uncertainty

Forbes 9/1

<http://www.forbes.com/sites/dougschoen/2013/09/01/weak-on-syria-weak-in-the-world/> ETB

Put another way, the President made it clear a year ago that there was a red line that the Syrians should not cross. All evidence suggests that they have surely crossed it and instead of striking, the President lectures the American people, and indeed the world, on American democracy.¶ Indeed, just this morning, a Syrian state state-run newspaper called Obama’s decision to seek Congressional approval before taking military action “the start of the historic American retreat.” It doesn’t get clearer than that.¶ This is not a president who shies away from using his executive power. He has altered ObamaCare, pushed his gun control agenda to strengthen national background checks, delayed the deportation of illegal immigrants when Congress wouldn’t agree amongst many other examples. But he has now suddenly decided that before he takes action, action that is within his purview, he is going to seek Congressional approval that is almost impossible to predict as to whether it will be granted or not.¶ If Obama really wanted to go ahead he would have brought congress back into session immediately and not waited more than 10 days thereby giving the Syrians time to plan for an attack – should one ultimately come. And even then, Obama has made it clear any such attack will be limited in nature and scope and will not involve regime change.¶ It follows that the message Obama’s speech yesterday sends is a muddled one at best.¶ It said to the mullahs in Iran and their Supreme Leader Ali Khamenei that they can continue to pursue their nuclear program by enriching uranium and refining plutonium without having to fear that they will be precipitously attacked by the US.¶ And to Russia’s President Putin, who has been an unbendable ally of Assad, providing him with arms and anti-aircraft weaponry, Obama has shown that the balance of power in the Middle East has almost certainly shifted away from the US. This is all the more alarming as Putin said just yesterday that the idea that the Syrian regime used chemical weapons is “absolute nonsense.”¶ What’s more, with a totally incoherent American policy on Egypt wherein it is unclear who and what we support, the US’s approach to the Syria further paints a bleak picture of American power and potency. Indeed, with our only real achievement in the region being the recent appearance of convincing the Arabs and Israelis to come to the peace table, an image of American uncertainty is radiating across the globe.¶ And although this would be a serious accomplishment if progress is made, our inaction on Syria signals to Israel, one of our strongest allies, that we are not willing to stick our neck out for them, their safety and way of life.¶ To our allies around the world who have said that if we do not stand firm we will send the wrong message to the Syrians, Obama offered not much of a response other than to tell them, in so many words, that they may well have to go it alone.¶ The US has not been sending clear messages. And though it may be apparent to me that the President’s move was calculated to force responsibility on a reluctant Congress and to play to 80% of the American people who have said in polls that they are against intervention in Syria, that does not mean that the US is offering anything but a confused image of our mission in the world to both our allies and foes.¶ Thus, in the short term the President may have managed to escape from the political quandary he faces. But in the longer term, America looks weaker, feckless and more uncertain.¶ President Obama has, if nothing else, compounded the view of a weak leader heading an unsure nation. This is an image we can ill afford to project.

#### Obama weak now- Syria deal

Maloof 9/13

F. Michael Maloof, senior staff writer for WND and the G2Bulletin, is a former security policy analyst in the Office of the Secretary of Defense¶ Read more at <http://www.wnd.com/2013/09/putin-makes-obama-look-indecisive-weak/#JFIueVqdjRHQa1GD.99> ETB

If Kerry and Lavrov come up with a plan, it will further consolidate Putin’s efforts in the Middle East, at U.S. expense.¶ “If the U.S. administration were to ignore Russian protests and proceed with a (military) strike with at least rhetorical coalition support, Russia would have little to show for its claimed influence in the Middle East,” according to the open intelligence group Stratfor.¶ “However, if Russia could effectively stunt the U.S.-led military campaign through an airy diplomatic proposal, then Russia will have played a hand in directly showcasing U.S. unreliability to its allies,” it said.¶ A proposal could make the U.S. look weak and indecisive while Moscow comes off “as the voice of reason” in a war that no one wants, and it will be all the Obama administration’s doing.

### 2AC- Cyber Deterrence DA

**Cyber deterrence is low now and fails**

**Clarke and Knake ‘10**

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

‘

**With a nuclear detonation, one could be fairly certain about** ¶ **what would happen to the target. I**f the target was a military base, ¶ it would become unusable for years, if not forever. On my first day ¶ of graduate school at MIT in the 1970s, I was given a circular slide ¶ rule, which was a nuclear­effect calculator. Spin one circle and you ¶ picked the nuclear yield, say 200 kilotons. Spin another circle and ¶ you could choose an airburst or a groundburst. Throw in how far ¶ away from the target you might be in a worst case and your handy ¶ little spinning device told you how many pounds of explosive pres­¶ sure per square inch would be created and how many would be ¶ needed to collapse a hardened underground missile silo in on itself, ¶ before becoming little radioactive pieces of dust thrown way up ¶ in the atmosphere. **A cyber warrior may possibly have similar certainty that were he to hit some system** with a sophisticated cyber ¶ weapon, **that system**, say a modern freight railroad, **would likely** ¶ **stop cold. What he may not know is whether the railroad has a reliable resiliency plan, a backup command­and­control network that** ¶ **he does not know about because the enemy is keeping it secret and** ¶ **not using it until it’s needed**. Just as a secret intrusion­prevention ¶ system might surprise us when it’s suddenly turned on in a crisis, ¶ a secret continuity­of­operations system that could quickly get the target back up and running is also a form of defense against cyber ¶ attack.¶ **The potential surprise capability of an opponent’s defense makes** ¶ **deterrence in cyber war theory fundamentally different from deterrence theory in nuclear strategy**. **It was abundantly clear in nuclear** ¶ **strategy that there was an overwhelming case of what was called** ¶ **“offensive preference,”** that is to say, any defense deployed or even ¶ devised could easily be overwhelmed by a well­timed surprise attack. ¶ It costs far less to modify one’s missile offense to deal with defensive ¶ measures than the huge costs necessary to achieve even minimally ¶ effective missile protection. **Whatever the defense did, the offense** ¶ **won with little additional effort.** **In addition, no one thought for a** ¶ **moment that the Soviet Union or the United States could secretly** ¶ **develop and deploy an effective missile­defense system.** Ronald Rea­¶ gan hoped that by spending billions of dollars on research, the U.S. ¶ could change the equation and make strategic nuclear missile de­¶ fense possible. Decades later it has not worked, and today the U.S. ¶ hopes, at best, to be able to stop a small missile attack launched by ¶ accident or a minor power’s attack with primitive missiles. Even that ¶ remains doubtful.¶ **In** strategic **nuclear war theory, the destructive power of the of­**¶ **fense was well known, no defense could do much to stop it, the** ¶ **offense was feared, and nations were thereby deterred from using** ¶ **their own nuclear weapons or taking other provocative steps that** ¶ **might trigger a nuclear response.** **Deterrence derived from suffi cient certainty. In the case of cyber war, the power of the offense** ¶ **is largely secret; defenses of some efficacy could possibly be created** ¶ **and might even appear suddenly in a crisis, but it is unlikely any** ¶ **nation is effectively deterred today from using its own cyber weap­**¶ **ons in a crisis; and the potential of retaliation with cyber weapons** ¶ **probably does not yet deter any nation from pursuing whatever** ¶ **policy it has in mind.** Assume for the sake of discussion that the United States (or some ¶ other nation) had such powerful offensive cyber weapons that it ¶ could overcome any defense and inflict significant disruption and ¶ damage on some nation’s military and economy. If the U.S. sim­¶ ply announced that it had that capability, but disclosed no details, ¶ many opponents would think that we were bluffing. Without de­¶ tails, without ever having seen U.S. cyber weapons in action, few ¶ would so fear what we could do as to be deterred from anything.¶ The U.S. could theoretically look for an opportunity to punish ¶ some bad actor nation with a cyber attack just to create a demon­¶ stration effect. (The U.S. used the F­117 Stealth fighter­bomber in ¶ the 1989 invasion of Panama not because it feared Panamanian ¶ air defenses, but because the Pentagon wanted to show off its new ¶ weapon to deter others. The invasion was code­named Operation ¶ Just Cause, and many in the Pentagon quipped that the F­117 was ¶ sent in “just cause we could.”) **The problem with the idea of using** ¶ **cyber weapons in the next crisis that comes up is that many sophisticated cyber attack techniques may be similar to the cryptologist’s** ¶ **“onetime pad” in that they are designed for use only once**. **When** ¶ **the cyber attack weapons are used, potential opponents are likely** ¶ **to detect them and apply all of their research capability in coming** ¶ **up with a defense.**¶If the U.S. cannot deter others with its secret cyber weapons, is it ¶ possible that the U.S. itself may be deterred by the threat from other ¶ nations’ cyber warriors? In other words, are we today self­deterred ¶ from conventional military operations because of our cyber war vul­¶ nerabilities? If a crisis developed in the South China Sea, as in the ¶ exercise described above, I doubt that today anyone around the table ¶ in the Situation Room would say to the President, “You better not ¶ send those aircraft carriers to get China to back down in that oil dis­¶ pute. If you do that, Mr. President, Beijing could launch a cyber at­¶ tack to crash our stock market, ground our airlines, halt our trains, and plunge our cities into a sustained blackout. There is nothing we ¶ have today that could stop them, sir.”¶ Somebody should say that, because, of course, it’s true. But would ¶ they? Very unlikely. The most senior American military officer just ¶ learned less than two years ago that his operational network could ¶ probably be taken down by a cyber attack. The Obama White ¶ House did not get around for a year to appointing a “cyber czar.” ¶ America’s warriors think of technology as the ace up their sleeves, ¶ something that lets their aircraft and ships and tanks operate better ¶ than any in the world. It comes hard to most of the U.S. military ¶ to think of technology as something that another nation could use ¶ effectively against us, especially when that technology is some geek’s ¶ computer code and not a stealthy fighter­bomber.¶ So, **we cannot deter other nations with our cyber weapons**. **In** ¶ **fact, other nations are so undeterred that they are regularly hack­**¶ **ing into our networks. Nor are we likely to be deterred from doing** ¶ **things that might provoke others into making a major cyber attack**. ¶ Deterrence is only a potential, something that we might create in the ¶ mind of possible cyber attackers if (and it is a huge if) we got serious ¶ about deploying effective defenses for some key networks. Since we ¶ have not even started to do that, **deterrence theory**, the sine qua non ¶ of strategic nuclear war prevention, **plays no significant role in stop­**¶ **ping cyber war today.**

### A2- Terrorism Impact

#### 1NC ev is tagged at the military – justifies answering the new 1nr impact

#### Prez flex not key to fight terrorism- Bush proves

**Prakash and Ramsey ‘12**

[Saikrishna B. Prakash and David Lurton Massee, Jr. Professor of Law and Sullivan and Cromwell Professor of Law, University of Virginia School of Law. Thanks to Steve Walt for helpful conversations. Michael D. Ramsey, Professor of Law, University of San Diego School of Law. Book Review: The Goldilocks Executive. 90 Tex. L. Rev. 973. ETB]

Because they do not support their normative claim about the desirability of an executive unbound and because we think well of our Madisonian system, we offer some comments on its recent functioning. As discussed, we think President **Bush**, during the war on terror, **operated within a system of bounded discretion, facing material but not crushing constraints**. **He sought approval from Congress for the attacks against al Qaeda and the Taliban in the AUMF** **and** in repeated **spending authorizations.** **He also sought approval for military action in Iraq**, though initially he hesitated to do so. He had to defend his policies in court; he lost some cases and would have lost others had he pursued his power to its practical limits. **He acted knowing that the courts might second-guess his decisions, a knowledge that affected his decision making. He faced the possibility that Congress would limit his authority on various dimensions, and on occasion Congress did**. **Yet he made a robust**, we would say largely effective, **response to the challenge of terrorism**, at least if we use the substantial disruption of terrorist networks and the absence of a subsequent substantial terror attack on the United States as a yardstick. Facing similar constraints and incentives, President Obama also has acquitted himself well in the war against al Qaeda.¶ To be clear, we concede that substantial, even colossal, mistakes were made in the war on terror. But the leading ones do not seem to have resulted from legal constraints upon executive power. For example, after initial success in Afghanistan in overthrowing Taliban rule, the President failed to consolidate the position of the new Afghan government, allowing the Taliban to regroup as a powerful opposition force. Instead, the President opened a new front in Iraq. Again, after initial success in displacing Saddam Hussein, the Administration failed to deploy enough troops to secure the country (at least until the "surge" in 2007). By some accounts, the distraction of Iraq harmed the fight against al Qaeda, including by delaying the targeting of Osama bin Laden. n121 Whether these are fairly counted as presidential [\*1004] failures, they are not ones attributable to legal constraints on the Executive, meaning that they could have occurred even under an unbound executive. n122¶ Perhaps President Bush would have accomplished more had he not faced a Madisonian system. And perhaps he could have acted with even greater secrecy, dispatch, and success had not Congress and the courts been looking over his shoulder. n123 We are not in a position to evaluate such counterfactuals at a detailed level. But we think there is little case to be made for very substantial costs attributable to executive constraint, even in the context of a crisis such as the war on terror. Of course, one may speculate that in future crises, or future aspects of the continuing war on terror, executive constraint may prove highly detrimental. But we see this as no more than speculation.