# 1AC

## 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.**

**No defense- deterrence fails vs 3rd parties, making escalation likely**

**Owens et al 9**

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

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

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

**Clarke 2009**

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

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

**Plan solves-**

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

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

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

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

**Goldsmith 10**

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

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

## Adv 2- Trade-off

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

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

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

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

**Healey ‘13**

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

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

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

**Rid 2/4**/13

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

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

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

**Gjelten, 13**

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

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

#### 2 impacts:

#### First, cyberwar:

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

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

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

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

**Clark and Andreasen 13**

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

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

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

**Gjelten, 13**

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

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

#### Second, cyber crime

**Defense solves it**

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

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

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

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

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

## 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**

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

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

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

**Dycus 10**

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

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

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

**Unfettered presidential powers cause nuclear war; ev is gender modified**

**Forrester 89** - Professor, Hastings College of the Law (Ray, August 1989, ESSAY: Presidential Wars in the Nuclear Age: An Unresolved Problem, 57 Geo. Wash. L. Rev. 1636)

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

## Plans

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

## Solvency

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

**Dycus ‘10**

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

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

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

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

**Huston ‘11**

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

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

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

**Owens et al. ‘9**

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

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

#### Military will adhere to the law- fear the consequences

Dunlap ‘12

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

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

# 2AC

### Yes Cyber War

#### 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.

#### D) Signaling failures

Mulvenon et al. 10

[Edited by Dr. James C. Mulvenon and ¶ Dr. Gregory J. Rattray ¶ Authors: Matt Devost, Maeve Dion, Jason Healey, ¶ Bob Gourley, Samuel Liles, James C. Mulvenon, Hannah Pitts, Gregory J. Rattray. Addressing Cyber Instability. Cyber Conflict Studies Association. ETB]

Signaling, whether prior to the initiation of conflict or during its ¶ various escalatory and de-escalatory phases, is critical to understanding the dynamics of strategic conflict. In the nuclear era, ¶ Schelling argued: ¶ ...violence is most successful when held in reserve and ¶ made contingent upon the adversary’s behavior. Nuclear ¶ diplomacy is the manipulation of latent violence – ¶ violence that can be withheld or inflicted in the future. It ¶ is also understood, however, that the power to hurt and the credibility of threats to do so may be communicated ¶ by some actual violence.60¶ Most nuclear strategists concentrated their attention on ¶ signaling of intent below the nuclear threshold, primarily through ¶ words or conventional forces. Here again Jervis’ work on ¶ perception and misperception as well as Mearsheimer’s work on ¶ conventional deterrence are dispositive.61 Edgier strategists, such ¶ as Herman Kahn, believed that intra-nuclear war was not only ¶ possible but desirable, and laid out highly detailed escalation ¶ control theories based on the ability to communicate to the ¶ adversary with both words and weapons at every stage of nuclear ¶ conflict. ¶ While signaling in nuclear conflict was hardly easy, cyber conflict contains additional complexities. On the level of deterrence ¶ signaling, Libicki identifies “three sources of confusion”: (1) ¶ attribution; (2) BDA [battle damage assessment], and (3) third-party ¶ interference.62 The first and last of these have been touched on ¶ earlier in this chapter, and BDA is discussed below in the sections ¶ on “uncertainty” and “repeatability” of cyber-based effects. For his ¶ part, Libicki recommends full disclosure of cyber attack, at least to ¶ bolster the credibility of retaliation. For once, Schelling supports ¶ Libicki when the former argues: ¶ In the case of a planned, deliberate, surprise attack, the ¶ aggressor has every reason to disguise the truth. But in ¶ the case of ‘inadvertent war,’ both sides have a strong ¶ interest in conveying the truth if the truth can in fact be ¶ conveyed in a believable way in time to prevent the ¶ other side’s mistaken decision.63¶ Yet this view is strongly contested by those unwilling to ¶ sacrifice sources and methods for a single iterative move in a ¶ longer game.64 ¶ Perhaps the more interesting signaling issue is cyber’s ¶ possible use as sub-nuclear signaling. Cyber, for example, could be ¶ used as a vector to establish the credibility of future violence. ¶ However, the plausible deniability of cyber attacks cuts both ways ¶ in this situation. On the positive side a cyber signal could ¶ communicate the credible threat of escalatory violence, but the ¶ deniability could give the adversary necessary relief from an ¶ automatic or mechanistic escalatory response. On the negative ¶ side, a deniable cyber signal could simply complicate the signaling by introducing more ambiguity about the attacker’s identity, ¶ intentions, and thresholds. Indeed, it is difficult to distinguish ¶ between cyber attacks meant to influence decisions and cyber ¶ attacks geared to limit the victims’ options for retaliation. Worse yet, a cyber signaling attack could unintentionally damage ¶ communications infrastructure and therefore undermine its very utility as a means to signal. Finally, cyber signaling runs into major ¶ problems with respect to adversaries with underdeveloped cyber ¶ capabilities or those who use cyber proxies, since the target of the ¶ signal may be too unintelligent to comprehend it or too weak to enforce his will on those he represents.65 Perversely, the important ¶ role of these wild-card proxies, such as those pro-Russian hackers ¶ who were allegedly involved in the 2007 Estonia attacks and the ¶ 2008 Georgia attacks, may in fact lend more credence to ¶ Schelling’s notion of the “threat that leaves something to chance,” ¶ which requires participants to credibly communicate threats in ¶ which “the final decision is not altogether under the control of the ¶ entity making the threat.”66

### 2AC PTX

#### Won’t pass – Negotiation dead-lock

CNN 9-12**,** 13, <http://money.cnn.com/2013/09/12/news/economy/budget-showdown/>

It also must [approve a debt ceiling increase](http://money.cnn.com/2013/09/12/news/economy/debt-ceiling/index.html?iid=EL) by mid-October. If it doesn't, an independent think tank now estimates that the Treasury Department would not have enough cash coming in to pay all the country's bills in full sometime between Oct. 18 and Nov. 5. After the so-called "X" date, barring a higher debt ceiling, the country would default on some of its obligations. In both cases, many conservatives in the House want to make the defunding or delay of [Obamacare](http://money.cnn.com/2013/07/30/news/economy/government-shutdown-obamacare/index.html?iid=EL) a condition for their support to fund the government and raise the debt limit. That's a non-starter for Democrats and President Obama. What's more the administration has insisted it won't negotiate over the raising the debt limit.

#### Syria THUMPS your DA

**Rothkopf 9/3/13**

[David, <http://www.centredaily.com/2013/09/03/3768415/obama-decision-to-ask-congressional.html>, mg]

**This president just** dialed back the power of his own office**.**¶ **Obama has** reversed decades of precedent **regarding the nature of** presidential war powers— and whether you prefer this change in the balance of power or not**, as a matter of** quantifiable fact **he is transferring greater responsibility for U.S. foreign policy to** a **Congress** that is more divided, more incapable of reasoned debate or action, and more dysfunctional than any in modern American history. Just wait for the Rand Paul filibuster or similar congressional gamesmanship.¶ The president’s own action in Libya was undertaken without such approval. So, too, was his expansion of America’s drone and cyber programs. Will future offensive actions require Congress to weigh in? How will Congress react if the president tries to pick and choose when this precedent should be applied? ¶ **At best,** the door is open to further acrimony**.** At worst, the paralysis of the U.S. Congress that has given us the current budget crisis and almost no meaningful recent legislation will soon be coming to a foreign policy decision near you. Consider House Speaker John Boehner’s statement that Congress will not reconvene before its scheduled Sept. 9 return to Washington.¶ Perhaps more importantly, what will future Congresses expect of future presidents? If Obama abides by this new approach for the next three years, will his successors lack the ability to act quickly and on their own? While past presidents have no doubt abused their War Powers authority to take action and ask for congressional approval within 60 days, we live in a volatile world; sometimes security requires swift action. The president still legally has that right, but **Obama’s decision may have done more** — for better or worse — **to** dial back the imperial presidency **than** anything his predecessors or Congress have done for decades.¶

#### Congress opposed to offensive Cyber ops--- they like the plan, AND Obama will issue other controversial XOs that drain PC

**Russia Times 13**

[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.”¶

#### Syria thumps the debt ceiling

Frenzel 9-6

(Bill Frenzel, contributor, “By Dropping Syria In Congress' Lap, Obama Creates The Worst Of The Bad Old Days” 9/06/2013, <http://www.forbes.com/sites/billfrenzel/2013/09/06/by-dropping-syria-in-congress-lap-obama-creates-the-worst-of-the-bad-old-days/>, KB)

Unfortunately, there is much more to this vote than a President forcing the Congress to ratify his decision. The Syria question is also consuming the President’s political capital at a time when he may be running a bit short anyway. He’s not a lame duck yet, but in a year he will be. Capital spent on Syria is capital not available for looming domestic problems. Worse, the decision comes at a time when Congressional energies ought to be focused on the FY14 CR, the sequester repair, and the Debt Ceiling extension. Congress is already a polarized battleground. Syria, because it is different, may relieve tensions. More likely, it will crank up animosities and resentments between parties, branches and houses. Surely, it will burn valuable negotiating time. Syria is an important foreign policy/national security issue. But it’s a mouse compared to the elephantine domestic fiscal problem. It now seems probable that the Syria vote may delay and confuse settlement of the budget question, and exacerbate existing budget tensions.

#### Winners win

Marshall and Prins ‘11

Bryan W. MARSHALL AND PRINS 11, Miami University, Department of Political Science AND Brandon C. PRINS, University of Tennessee & Howard H. Baker, Jr. Center for Public Policy, September 2011 “Power or Posturing? Policy Availability and Congressional Inﬂuence on U.S. Presidential Decisions to Use Force”, Presidential Studies Quarterly, http://onlinelibrary.wiley.com/doi/10.1111/j.1741-5705.2011.03885.x/pdf, [Stolarski]

Presidents rely heavily on Congress in converting their political capital into real policy success. Policy success not only shapes the reelection prospects of presidents, but it also builds the president’s reputation for political effectiveness and fuels the prospect for subsequent gains in political capital (Light 1982). Moreover, the president’s legislative success in foreign policy is correlated with success on the domestic front. On this point, some have largely disavowed the two-presidencies distinction while others have even argued that foreign policy has become a mere extension of domestic policy (Fleisher et al. 2000; Oldﬁeld and Wildavsky 1989) Presidents implicitly understand that there exists a linkage between their actions in one policy area and their ability to affect another. The use of force is no exception; in promoting and protecting U.S. interests abroad, presidential decisions are made with an eye toward managing political capital at home (Fordham 2002).

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

Cillizza 6/25

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

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

**No proliferation**

**Cook 12** 4/2, \*Steven A. Cook is the Hasib J. Sabbagh Senior Fellow for Middle Eastern Studies at the Council on Foreign Relations, “Don't Fear a Nuclear Arms Race in the Middle East,” http://www.foreignpolicy.com/articles/2012/04/02/don\_t\_fear\_a\_nuclear\_arms\_race?page=0,0, AJ

The conventional wisdom has it wrong: Iran’s development of a nuclear weapon won’t spur its neighbors to get the bomb. On March 21, Haaretz correspondent Ari Shavit wrote a powerful op-ed in the New York Times that began with this stark and stunning claim: "An Iranian atom bomb will force Saudi Arabia, Turkey, and Egypt to acquire their own atom bombs." Indeed, it has become axiomatic among Middle East watchers, nonproliferation experts, Israel's national security establishment, and a wide array of U.S. government officials that Iranian proliferation will lead to a nuclear arms race in the Middle East. President Barack Obama himself, in a speech to the American Israel Public Affairs Committee (AIPAC) last month, said that if Iran went nuclear, it was "almost certain that others in the region would feel compelled to get their own nuclear weapon." Multiple nuclear powers on a hair trigger in the Middle East -- the most volatile region on earth, and one that is undergoing massive political change -- is a nightmare scenario for U.S. and other security planners, who have never before confronted a challenge of such magnitude. But thankfully, all the dire warnings about uncontrolled proliferation are -- **if not exactly science fiction -- further from reality** than Shavit and Obama indicate. There are very good reasons for the international community to meet the challenge that Iran represents, but Middle Eastern nuclear dominoes are not one of them. Theorists of international politics, when pondering the decision-making process of states confronted by nuclear-armed neighbors, have long raised the fears of asymmetric power relations and potential for nuclear blackmail to explain why these states would be forced to proliferate themselves. This logic was undoubtedly at work when Pakistan embarked on a nuclear program in 1972 to match India's nuclear development program. Yet for all its tribulations, **the present-day Middle East is not the tinderbox that South Asia was in the middle of the 20th century**. Pakistan's perception of the threat posed by India -- a state with which it has fought four wars since 1947 -- is **far more acute than how either Egypt or Turkey perceive the Iranian challenge**. And while Iran is closer to home for the Saudis, the security situation in the Persian Gulf is not as severe as the one along the 1,800-mile Indo-Pakistani border. Most important to understanding why the Middle East will **not be a zone of unrestrained proliferation is the significant difference between desiring nukes and the actual capacity to acquire them**. Of all three states that Shavit mentioned, the one on virtually everyone's list for possible nuclear proliferation in response to Iran is Turkey. But the Turkish Republic is already under a nuclear umbrella: Ankara safeguards roughly 90 of the United States' finest B61 gravity bombs at Incirlik airbase, near the city of Adana. These weapons are there because Turkey is a NATO member, and Washington's extended deterrence can be expected to at least partially mitigate Turkey's incentives for proliferation. But even if the Turks wanted their own bomb, they have almost no capacity to develop nuclear weapons technology. Indeed, Turkey does not even possess the capability to deliver the 40 B61 bombs at Incirlik that are allocated to Turkish forces in the event of an attack, according to a report released by the Carnegie Endowment for International Peace. Given the changes in Turkey's foreign policy and its drive for global influence, it is conceivable that it will want to develop a Turkish version of France's force de frappe. However, Ankara would literally be starting from scratch: Turkey has no fissile material, cannot mine or enrich uranium, and does not possess the technology to reprocess spent fuel, all of which are required for nuclear weapons development. This does not mean that Turkey is not interested in nuclear technology. Yet Ankara's efforts, to the extent that they exist beyond the two small-scale facilities in Ankara and Kucukcekmece, are directly related to the country's predicted energy shortfall resulting from the combination of a booming economy and growing population. The Turkish government has announced plans for civilian nuclear power to provide a quarter of Turkey's electricity needs by 2040. But even this three-decade timeline seems overly optimistic given the inchoate nature of Turkey's nuclear research. The Egyptians are way ahead of the Turks in developing nuclear infrastructure, but don't expect to see the rise of a nuclear power on the Nile anytime soon. Egypt's nuclear program is actually older than India's, and was established only three years after Israel founded its Atomic Energy Commission. The Egyptian Atomic Energy Commission, which Gamal Abdel Nasser established in 1955, was exclusively dedicated to the development of peaceful atomic energy, though there were suspicions to the contrary. The 1956 nuclear cooperation agreement with the Soviet Union transferred to Egypt a 2-megawatt light water reactor that only produced small amounts of plutonium. Even after Mubarak's son Gamal triumphantly declared at the ruling party's 2006 convention that Egypt was going to ramp up its nuclear development program, it is hard to believe that Egyptians ever really took him seriously. Mubarak spent $160 million on consultants to tell him where to build 10 planned nuclear power plants, and selected a location along the Mediterranean for the first one. But each of the power plants comes with a price tag of $1.5 billion -- and this is a country that in the last 15 months has spent approximately $26 billion of its $36 billion foreign currency reserves just to stay afloat. One has to wonder about the pundits' warning of an Egyptian bomb: Have they even been to Egypt lately? If so, they might have a better grasp of Egypt's ramshackle infrastructure and the dire state of its economy, neither of which can support a nuclear program. What about Saudi Arabia, then, the Sunni power that is on the tip of most analysts' tongues when it comes to Shiite Iran getting the bomb? Saudi Arabia has the cash to make large-scale investments in nuclear technology. Indeed, the only factor that makes warnings about Saudi proliferation -- such as that delivered by former Ambassador the United States Prince Turki al-Faisal last year -- even remotely credible is the resources the Saudis can muster to buy a nuclear program. Yet, while Riyadh can outfit itself with nuclear facilities with ease, it does not have the capacity to manage them. Mohamed Khilewi, a former Saudi diplomat, claims that the kingdom has been developing a nuclear arsenal to counter Israel since the mid-1970s -- but he offers no substantiated evidence to support these claims. In fact, the country has no nuclear facilities and no scientific infrastructure to support them. It's possible that Saudi Arabia could import Pakistanis to do the work for them. But while Saudis feel comfortable with Pakistanis piloting some of their warplanes and joining their ground forces, setting up a nuclear program subcontracted with Pakistani know-how -- or even acquiring a nuclear device directly from Islamabad -- poses a range of political risks for the House of Saud. No doubt there would be considerable international opprobrium. Certainly Washington, which implicitly extends its nuclear umbrella to Saudi Arabia, would have a jaundiced view of a nuclear deal between Riyadh and Islamabad. Moreover, it's one thing to hand the keys to an F-15 over to a foreigner, but letting them run your nuclear program is another matter altogether. The concern about Saudi proliferation stems from fears that the kingdom would be forced to act if both Iran and Israel possessed a nuclear arsenal. "We cannot live in a situation where Iran has nuclear weapons and we don't," an unnamed Saudi official declared to the Guardian on the sidelines of a meeting between Prince Turki al Faisal and NATO officials in June 2011. "It's as simple as that. If Iran develops a nuclear weapon, that will be unacceptable to us and we will have to follow suit." Yet given the fact that the Saudis have very little nuclear infrastructure to speak of, this kind of statement is little more than posturing designed to force the U.S. hand on Iran. Unlike similar warnings by Israel, which has the capacity to follow through on its threat to attack Iran's nuclear sites, Riyadh's rhetoric about acquiring nuclear weapons is empty. What is amazing is how many people take the Saudis seriously. If Khilewi had been telling the truth, now would seem like a good time for the Riyadh to give Tehran a look at what the royal family has been hiding in the palace basement all these years -- but so far, we have only heard crickets. Despite its flimsiness, it is hard to ignore the utility of the Middle East's nuclear dominoes theory. For those who advocate a preventive military strike on Iran, **it provides a sweeping geopolitical rationale for a dangerous operation**. But the evidence doesn't bear this argument out: If Washington decides it has no other option than an attack, it should do so because Iran is a threat in its own right, and not because it belives it will thwart inevitable proliferation in places like Turkey, Egypt, and Saudi Arabia. It won't, for the simple reason that there is **no reason to believe these countries represent a proliferation risk** in the first place.

**The impact is super easy to contain and it won’t be that bad.**

**Barnett, ‘11**

[Thomas, World Politics Review, 11-14, “The New Rules: How to Stop Worrying and Live with the Iranian Bomb,” http://www.worldpoliticsreview.com/articles/10652/the-new-rules-how-to-stop-worrying-and-live-with-the-iranian-bomb]

The International Atomic Energy Agency’s latest report on Iran’s nuclear program surprised no one, even as it created the usual flurry of op-eds championing preventative “next steps.” As I’ve been saying for the past half-decade, there are none. Once the U.S. went into both Iraq and Afghanistan, the question went from being, “How do we prevent Iran from getting the Bomb?” to “How do we handle Iran’s Bomb?” That shift represents neither defeatism nor appeasement. Rather, it reflects a realistic analysis of America’s strategic options. With that in mind, here are 20 reasons why Iran’s successful pursuit of the Bomb is not the system-changing event so many analysts are keen to portray. 1. Iran’s efforts are not irrational. America invaded Iran’s western and eastern neighbors in quick succession, while putting Iran on notice that it, too, was on the list of George W. Bush’s “Axis of Evil.” Decades of history tell Tehran: Get the Bomb, and the U.S. will never invade. Iran’s logic here is unassailable. 2. The world’s rising powers are not on board with the West. Brazil and Turkey made their diplomatic play last spring, and the West vilified them in response. Russia has already dismissed more sanctions as a clear “instrument of regime change.” China and India, along with Russia, have their own energy interests in Iran. In sum, Tehran’s workaround options are considerable. 3. More Western sanctions will have no impact. See above. Also, though the economic costs to date have been substantial, Tehran is willing to endure any amount of economic pain to ensure regime survival. The Arab Spring and the dangers it poses to the mullahs’ rule only sharpen this instinct. 4. Iran will not accept any deal that doesn’t include maintaining at least the pathway to the Bomb. The Bomb not only ensures regime survival, it is Tehran’s ticket to the great powers’ club. Without it, Iran is simply a failed revolution, a moribund economy and a sullen, checked-out society. With it, Iran is a focus of global attention and remains in the race for regional leadership. 5. Iran’s Bomb will offer the regime no significant new regional influence. Iran is already losing the Arab Spring -- and Iraq -- to Turkey and will likely lose influence to a revived Cairo as well. Iran’s Bomb is a desperate pan-Islamism card vis-à-vis Israel that will only engender a vigorous anti-Shiite response from the Saudis. 6. The strategic balance of power in the region will not dissolve. Iran’s Bomb means closing the door on a U.S. invasion, but nothing else. Iran’s limited proxy wars are neither enhanced nor inhibited by possessing the Bomb, as America will stand by both Israel and the Saudis. 7. America’s regional military presence will not be threatened. The U.S. military has a long and well-established record of serving as a tripwire presence in regional hotspots. That won’t change with Iran’s Bomb. If anything, Tehran’s achievement will reverse America’s growing fixation on building up its military in Asia vis-à-vis China. 8. The terror threat is overblown. Persian Iran isn’t pursuing the Bomb to put it in the hands of extremist Arab nonstate actors. Even Israel is a red herring for the Bomb’s ultimate purposes, which are clearly anti-U.S. and anti-Saudi. 9. The right historical analogy is not late-1930s Europe, but South Asia once both Pakistan and India got their Bomb. Israel is no Czechoslovakia. Rather, it is armed to the teeth with nuclear weapons and can wipe Iran off the map far more feasibly than vice versa. Yes, the early stages of a mutually assured destruction dyad between Israel and Iran would be scary, but the world has managed this scenario before -- with a perfect record to date. 10. The MAD situation between Israel and Iran is manageable. Israel owns a state-of-the-art multilayered missile defense system, which means it can survive a direct exchange far better than Iran ever could. It also means Israel could retaliate with confidence in any suitcase bomb scenario. 11. An Israeli attack will not work. It will slow down Iran’s pursuit of the Bomb, but as the -- presumably -- joint Israeli-U.S. Stuxnet cyberattack on Iran showed, Tehran can simply respond by ramping up its effort all the more. 12. A U.S. attack is not feasible any time soon. President Barack Obama doesn’t want to be a one-term president that badly, nor is he willing to tarnish his Nobel Peace Prize that decisively. More importantly, attacking Iran would torpedo Obama’s entire effort to get out of Iraq and Afghanistan with some sense of honor. 13. Iran has already achieved a crude but effective asymmetrical deterrence capability. There is no derailing the Bomb pursuit without regime change, and the U.S. is simply unwilling to take on that massive effort. The quick-and-dirty route is to nuke Iran’s facilities, sending the double signal of “No nukes for you!” and “See what we’re capable of?” But once you start talking about using nukes to destroy nukes, you realize that Iran has already achieved a sloppy deterrence. 14. A pre-emptive war works primarily to Iran’s advantage. The political infighting in Tehran is at an all-time high. Meanwhile, the Arab Spring is going badly for Iran. Thus an attack by either Israel or the U.S. would be a godsend to the decaying theocratic regime, changing those narratives and unifying the country. 15. We can easily arm Iran’s rivals. America has been selling arms like crazy throughout the region for a while now, and nothing will keep Washington from further enhancing the defensive -- and offensive -- capabilities of Iran’s many enemies. 16. The danger of wider proliferation is overblown. Yes, Riyadh and possibly Ankara will follow suit, but arguing that anti-Western regimes the world over will now seek a nuclear deterrent is fanciful. After all these years of freaking out about nuclear proliferation, we’re still talking about just the two remaining “Axis of Evil” members. To date, North Korea’s achievement has triggered no such regional nuclear race in East Asia. Iran’s effort likely will in the Middle East, but that is still a unique dynamic with limited legs. 17. The follow-on regional proliferation can be played to our advantage. Nothing clarifies the strategic mind like nukes. Once the Saudis join in, the world’s great powers will force a regional strategic dialogue. When that happens, Israel’s diplomatic existence will finally be recognized across the region. 18. The soft-kill option has worked before. In 1972, America gave the Soviets a signed piece of paper that declared them a legitimate nuclear power. Deprived of its own version of the “great Satan,” the USSR collapsed from within -- in the space of a generation. The Iranian mullahs’ self-destruction will come far faster.

### 2AC Flex

#### 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.

### 2AC

**International distrust of the president dooms the signal and solvency**

**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**.

#### Links to politics – immense opposition to bypassing debate

Hallowell 13

(Billy Hallowell, writer for The Blaze, B.A. in journalism and broadcasting from the College of Mount Saint Vincent in Riverdale, New York and an M.S. in social research from Hunter College in Manhattan, “HERE’S HOW OBAMA IS USING EXECUTIVE POWER TO BYPASS LEGISLATIVE PROCESS” Feb. 11, 2013, <http://www.theblaze.com/stories/2013/02/11/heres-how-obamas-using-executive-power-to-bylass-legislative-process-plus-a-brief-history-of-executive-orders/>, KB)

“In an era of polarized parties and a fragmented Congress, the opportunities to legislate are few and far between,” Howell said. “So presidents have powerful incentive to go it alone. And they do.”¶ And the political opposition howls.¶ Sen. Marco Rubio, R-Fla., a possible contender for the Republican presidential nomination in 2016, said that on the gun-control front in particular, Obama is “abusing his power by imposing his policies via executive fiat instead of allowing them to be debated in Congress.”¶ The Republican reaction is to be expected, said John Woolley, co-director of the American Presidency Project at the University of California in Santa Barbara.¶ “For years there has been a growing concern about unchecked executive power,” Woolley said. “It tends to have a partisan content, with contemporary complaints coming from the incumbent president’s opponents.”

### 2AC K

**Cyber threats are real – they facilitate dangerous armed social movements**

**Deibert and Rohozinski 2010**

(Ronald J, professor of Political Science and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto, and Rafal, Canadian expert and practitioner active in the fields of information security, cyber warfare, and the globalization of armed violence at the University of Toronto, 2010, International Studies Association, “Risking Security: Policies and Paradoxes of Cyberspace Security,” International Political Sociology, vol. 4, p. 22, BS)

Even among democratic states, **the explosion of civic networks has presented serious challenges**, though of a slightly different nature. **Just as progressive and social justice groups have made use of the Internet to advance global norms, so too have a wide variety of militant groups, extremists, criminal organizations, and terrorists to serve more ulterior purposes. Cyberspace has facilitated their activities** in much the same way as it has for more benign civil society networks that often get more attention, but **the aims of these groups are often criminal, covert, and sometimes violent. We call these risks through the network dark nets**, of which there are two different sorts (Deibert and Rohozinski 2008). **The most well known of the dark nets are armed social movements, which can represent a multiplicity of local causes, but whose ability to share tactics, contacts, and at times, drink from the same ideological well, make them appear as a uniﬁed global network. In the post-9/11 era, Al Qaeda and the Jihad movements represent the most visible manifestation of this kind of armed social movement. However, they are by no means the ﬁrst and only networks of this kind.** Many of the ‘‘new wars’’ (as Mary Kaldor calls them) that occurred during the 1990s were fought essentially as transnational civil wars where participants pursued both guerilla and conventional warfare against government and rival groups (Kaldor 1999). **In conﬂicts that included Sri Lanka, Somalia, former Yugoslavia, West Africa and Chechnya, ‘‘new wars’’ demonstrated that armed social movements are capable of challenging and at times defeating state actors without the need of state-based patrons or backers. More importantly, this new generation of armed social actors has also increasingly embraced cyberspace** (Rohozinski 2004). **They recognize the capacity afforded by cyberspace to ‘‘effect’’ both their supporters and opponents**. Signiﬁcantly, it was these groups, rather than militaries of the First World War, that were the ﬁrst to leverage cyberspace as means to wage information operations redeﬁning the main battleﬁeld away from the military and towards the political sphere (Weimann 2006b). **Beginning with the ﬁrst Chechen war, the video taping of attacks on the Russian military became more important than the military signiﬁcance of the attacks themselves.** When shown to supporters, as well as the Russian public (via rebroadcast in Russian television, and later on the Internet) their shock value was enough to convey the impression that the Russian military was being defeated. Similar tactics were adopted and further reﬁned by Hezbollah in its resistance against Israeli occupation of Southern Lebanon prior to their withdrawal in 2001, and again in the 2006 summer war. Attacks were documented and produced in the form of music videos, that were both broadcast across Hezbollah’s terrestrial TV station, (al Manar) as well as made available for download from a website, the movement established as part of its strategic communications and information warfare strategy (Pahlavi 2007; Wehrey 2002). **These video shorts proved highly effective**, and have since undergone several signiﬁcant evolutions, paralleling the spread and popularity of such on-line resources as YouTube and Twitter that are used by ‘‘civil’’ networks. **They are now one of the key instruments used by these movements to attract interest in their causes and are a signiﬁcant feature of the more than 4,500+ active jihad websites, chat rooms, and forums** (Weimann 2006a; Kimmage 2008). As the resources necessary for producing multimedia technologies continue to fall, and access to inexpensive digital cameras and computers increases, the threshold and number of video and other multimedia products in circulation has grown exponentially, while the age of the producers has declined. During the early months of the second Intifada, for example, several of the more compelling PowerPoint slides circulating on the Internet depicting the brutality of the Israeli reoccupation of the West bank were produced by a 14-year-old living in a refugee camp in Lebanon.

#### Cyber operates in a realist framework

Dawson ‘13

[Ashley Dawson, M.A. Candidate in Policy Sci @ University of British Columbia. “Addressing Cyber Warfare: Bolstering Deterrence through developing norms.” Master’s Thesis. Etb]

RDT is centered around two central strategies with the goal of dissuading an ¶ adversary from undertaking an action that it has not already started through fear of the ¶ consequences: deterrence by punishment or MAD, a strategy that centres on a credible ¶ threat of offensive retaliation, and deterrence by denial, a defensive strategy in which a¶ potential aggressor is convinced that the offensive and defensive balance is such that an ¶ offensive attack cannot succeed and therefore should be avoided. Moreover, according to ¶ Achen and Snidal, two key components are crucial for the success of RDT: the credibility of the deterrence capabilities, and the rational actor assumption of decisions ¶ rely on a cost-benefit analysis.28 In other words, cyber deterrence is pursued by rational ¶ actors undertaking a cost benefit analysis before making logical decisions,29 where states¶ only engage in conflicts when they expect to win or from which they expect to at least ¶ yield a net gain. Therefore the proliferation of any cyber-technology that lowers a¶ weaker state’s estimation of the power/capabilities gap between it and a stronger ¶ adversary can thus be expected

#### IR theory proves cyberwar is probable- multiple mechanisms

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.

What is Cyber War? (Again. . .)

#### Their engagement in solely theory of cyberwar will never create change – only the permutation can resolve that.

Eriksson and Giacomello ‘6

[Johan Eriksson and Giampiero Giacomello. International Political Science Review 27.3 (Jul., 2006), pp. 221-244. “The Information Revolution, Security, and International Relations: (IR) Relevant Theory?” ETB]

The foregoing analysis has shown that there are two interrelated problems in ¶ past efforts at understanding security in the digital age. First, theory and practice ¶ on this matter are so distant that they hardly ever inform each other. Second, ¶ existing IR theories are plagued by an entrenched dualism, implying great difficulties for theoretical adaptation and application in analyses of the complexities of the emerging new digital world. ¶ One possible way of overcoming these problems is by adopting a more "prag ¶ matic" approach.'9 While there are several strands of pragmatist philosophy, ¶ pragmatism generally advocates bridge building between theory and practice, ¶ methodological pluralism, contingent generalizations, and theoretical comple ¶ mentarities and tolerance rather than entrenched opposition (Bauer and Brighi, ¶ 2002: iii). This seems to be exactly what is needed to bridge the gap between ¶ theory and practice, and to help overcome the dualistic conflicts in academic IR. ¶ There is thus no reason why the scholar trying to understand digital-age security ¶ cannot draw simultaneously on insights from a diverse range of IR theories, ¶ unfortunately often depicted as contending or incompatible, and on insights from ¶ the policy-oriented literature. ¶ The critical reader might wonder whether "pragmatist" is another word for ¶ "empiricist" or, more cynically worded, for "not smart enough for theory" ¶ (Lewontin, 1992). Indeed, pragmatism is more of an orientation, or ethos, than a ¶ theory. This is, however, a necessary first step to overcoming the chasm between ¶ theory and practice, and while a particular theory is not proffered, a fruitful ¶ starting point for the development of theory on security in the digital age is ¶ provided. With such a pragmatic approach applied to case studies and compar ¶ ative analyses, it is possible to build a foundation upon which further theory ¶ building can be done, with an emphasis on middle-range theory and on ¶ conditional rather than universal generalizations.

**Cyber threats are real – cyberspace is organized transnationally, not governed centrally, constantly changes, and is difficult to regulate**

**Deibert and Rohozinski 2010**

(Ronald J, professor of Political Science and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto, and Rafal, Canadian expert and practitioner active in the fields of information security, cyber warfare, and the globalization of armed violence at the University of Toronto, 2010, International Studies Association, “Risking Security: Policies and Paradoxes of Cyberspace Security,” International Political Sociology, vol. 4, p. 15-16, BS)

Globalization is generating new security challenges. Modern societies confront a myriad of risks that threaten economic prosperity, undermine the safety and security of citizens, and cause signiﬁcant disruption to society and politics. These risks range from empowered and militant nonstate actors to technological and human-made processes, such as environmental degradation and global warming. **Risk mitigation has become a routine matter of good public policy. Cyberspace represents a special category of risk.**1 A term once found only in science ﬁction novels, cyberspace describes the human-made domain for action that exists as a consequence of an interconnected and interdependent global communications and computing infrastructure. **Cyberspace connects more than half of all humanity and is an indispensable component of political, social, economic, and military power worldwide. In strategic terms, cyberspace is accepted now as a domain equal to land, air, sea, and space. Predictably, in the post-9/11 era, cyberspace is the focus of security concerns as states weigh the risks and beneﬁts of omnipresent global connectivity. However, cyberspace presents special security challenges, for a variety of reasons. First, and most importantly, it is a communication network that is organized transnationally and not through the institutional structures of the state system. Although states and individuals may claim sovereignty or ownership over segments of cyberspace, particularly parts of its material infrastructure, or even opt out of it entirely, once in they are never fully in control. Cyberspace has emergent properties, in other words, that elude state control. Second, and closely related, cyberspace is operated as a mix of public and private networks. Governance of cyberspace, like its architecture, is distributed, and does not take place within a singular forum or point of control** (Dutton and Peltu 2007). Even the Internet Corporation for Assigned Names and Numbers (ICANN), that is most often associated with Internet governance issues, is only narrowly concerned with domain and routing management and not with the full panoply of cyberspace governance issues (Mueller 2002). **There are instead numerous sites of cyberspace governance, from spectrum allocation to copyright and intellectual property regulation to content ﬁltering and cyber-crime (among many others). Each of these sites involves numerous stakeholders, including governments, businesses, and civil society networks. In addition, private sector actors from multiple countries operate most of the core infrastructural components of cyberspace.** What James Der Derian (2003) calls ‘‘heteropolarity’’ perhaps best characterizes the state of cyberspace governance. **Third, unlike other domains, such as the sea, land, air, or space, cyberspace is a human-made domain in constant ﬂux based on the ingenuity and participation of users themselves. One of the core design features of cyberspace is the end-to-end principle, which allows for generative technologies to be introduced into cyberspace by end users as long as they conform to the basic protocols of interconnectivity** (Saltzer, Reed, and Clark 1984). **The latter introduces not only great variation and constant innovation, but also new and unforeseen security risks** (Zittrain 2007). **It also creates major problems for regulation, insofar as regulators are always chasing a moving target. In other words, cyberspace is a domain of constant transformation and a high degree of complexity. Fourth, cyberspace is comprised of both a material and a virtual realm—a space of things and ideas, structure and content.** Theorists and observers of cyberspace often focus on one of these elements to the exclusion or diminution of the other, but both are important and interdependent. Cyberspace is indeed a ‘‘consensual hallucination’’ as Gibson (1984) famously deﬁned it, but one that could not exist without the physical infrastructure that supports it. **Attempts to control and monitor the virtual realm of cyberspace often begin with interventions in the physical infrastructure, at key Internet chokepoints** (Deibert, Palfrey, Rohozinski, and Zittrain 2008). **However, these efforts are never entirely comprehensive; once released into cyberspace, the distributed properties of the network help ideas and information circulate, duplicate and proliferate. Even radical measures, such as disconnecting the Internet entirely as was done recently in Burma and Nepal, can only limit, but not entirely contain the ﬂow of ideas.**