## 1NC

### 3

#### Immigration reform is up—Obama has leverage—that’s key to overcome GOP obstructionism

Jeff Mason, Reuters, 10/19/13, Analysis: Despite budget win, Obama has weak hand with Congress , health.yahoo.net/news/s/nm/analysis-despite-budget-win-obama-has-weak-hand-with-congress

Democrats believe, however, that Obama's bargaining hand may be strengthened by the thrashing Republicans took in opinion polls over their handling of the shutdown.

"This shutdown re-emphasized the overwhelming public demand for compromise and negotiation. And that may open up a window," said Ben LaBolt, Obama's 2012 campaign spokesman and a former White House aide.

"There's no doubt that some Republican members (of Congress) are going to oppose policies just because the president's for it. But the hand of those members was significantly weakened."

If he does have an upper hand, Obama is likely to apply it to immigration reform. The White House had hoped to have a bill concluded by the end of the summer. A Senate version passed with bipartisan support earlier this year but has languished in the Republican-controlled House.

"It will be hard to move anything forward, unless the Republicans find the political pain of obstructionism too much to bear," said Doug Hattaway, a Democratic strategist and an adviser to Hillary Clinton's 2008 presidential campaign.

"That may be the case with immigration - they'll face pressure from business and Latinos to advance immigration reform," he said.

#### The plan reverses these dynamics—sparks an inter-branch fight derailing the agenda

Douglas Kriner, Assistant Profess of Political Science at Boston University, 2010, After the Rubicon: Congress, Presidents, and the Politics of Waging War, p. 67-69

Raising or Lowering Political Costs by Affecting Presidential Political Capital

Shaping both real and anticipated public opinion are two important ways in which Congress can raise or lower the political costs of a military action for the president. However, focusing exclusively on opinion dynamics threatens to obscure the much broader political consequences of domestic reaction—particularly congressional opposition—to presidential foreign policies. At least since Richard Neustadt's seminal work Presidential Power, presidency scholars have warned that **costly political battles in one policy arena frequently have significant ramifications for presidential power in other realms**. Indeed, two of Neustadt's three "cases of command"—Truman's seizure of the steel mills and firing of General Douglas MacArthur—explicitly discussed the broader political consequences of stiff domestic resistance to presidential assertions of commander-in-chief powers. In both cases, Truman emerged victorious in the case at hand—yet, Neustadt argues, each victory cost Truman dearly in terms of his future power prospects and leeway in other policy areas, many of which were more important to the president than achieving unconditional victory over North Korea."

While congressional support leaves the president's reserve of political capital intact, congressional criticism saps energy from other initiatives on the home front by forcing the president to expend energy and effort defending his international agenda. **Political capital spent shoring up support for a president's foreign policies is capital that is unavailable for his future policy initiatives**. Moreover, any weakening in the president's political clout may have immediate ramifications for his reelection prospects, as well as indirect consequences for congressional races." Indeed, Democratic efforts to tie congressional Republican incumbents to President George W. Bush and his war policies paid immediate political dividends in the 2006 midterms, particularly in states, districts, and counties that had suffered the highest casualty rates in the Iraq War.6°

In addition to boding ill for the president's perceived political capital and reputation, such partisan losses in Congress only further imperil his programmatic agenda, both international and domestic. Scholars have long noted that President Lyndon Johnson's dream of a Great Society also perished in the rice paddies of Vietnam. Lacking both the requisite funds in a war-depleted treasury and the political capital needed to sustain his legislative vision, Johnson gradually let his domestic goals slip away as he hunkered down in an effort first to win and then to end the Vietnam War. In the same way, many of President Bush's **highest second-term domestic priorities**, such as Social Security and immigration reform, **failed** perhaps in large part **because the administration had to expend so much energy** and effort **waging a rear-guard action against congressional critics** of the war in Iraq.

When making their cost-benefit calculations, presidents surely consider these wider political costs of congressional opposition to their military policies. If **congressional opposition in the military arena stands to** derail other elements of his agenda, all else being equal, the president will be more likely to judge the benefits of military action insufficient to its costs than if Congress stood behind him in the international arena

#### Immigration key to ag

Abou-Diwan 1/28

(Antoine, “Bipartisan immigration proposal acknowledges agriculture's needs” January 28, 2013, Imperial Valley Press)

Bipartisan immigration proposal acknowledges agriculture's needs

The bipartisan proposal unveiled Monday paves the way to legalization of the nation’s 11 million undocumented immigrants with a program described as “tough but fair.”

It also addresses the concerns of the agricultural industry, whose labor pool by some estimates is composed of some 50 to 70 percent unauthorized workers.

“Agricultural workers who commit to the long-term stability of our nation’s agricultural industries will be treated differently than the rest of the undocumented population because of the role they play in ensuring that Americans have safe and secure agricultural products to sell and consume,” states the proposal.

Total farmworkers in Imperial County fluctuated between 8,000 and 11,000 in 2012, according to data from the Employment Development Department.

“There’s definitely recognition that agriculture will be taken care of,” said Steve Scaroni, a Heber farmer who has lobbied Washington extensively on immigration reform.

The proposal is based on four broad principles: a path to citizenship for unauthorized immigrants living in the United States, reform of the system to capitalize on characteristics that strengthen the economy, the creation of an effective employment verification system and improving the immigration process for future workers.

The principles are broad and many details need to be worked out.

“The principles acknowledge that the situation in agriculture is distinct and requires different treatment,” said Craig Regelbrugge, chairman of the Agricultural Coalition for Immigration Reform, a group that represents the landscape and nursery industry.

Access to a legal and stable work force is vital, Regelbrugge said, as is a workable program that eliminates or reduces hurdles for a future work force.

“We would like to see the agriculture legalization program attractive so there are incentives for them to work in the sector,” Regelbrugge noted.

The proposals also acknowledge that the United States immigration system is broken, and address criticism that not enough is being done to enforce existing immigration laws. To that end, Monday’s proposals are contingent on secure borders.

But, the acknowledgement of the agriculture sector’s needs allows for some optimism.

“As long as the labor supply solutions are there, we can support the enforcement solutions,” Regelbrugge said.

**Extinction**

**Lugar 2k**

(Richard, a US Senator from Indiana, is Chairman of the Senate Foreign Relations Committee, and a member and former chairman of the Senate Agriculture Committee. “calls for a new green revolution to combat global warming and reduce world instability,” pg online @ <http://www.unep.org/OurPlanet/imgversn/143/lugar.html>)

In a world confronted by global terrorism, turmoil in the Middle East, burgeoning nuclear threats and other crises, it is easy to lose sight of the long-range challenges. **But we do so at our peril.** One of the most daunting of them is meeting the world’s need for food and energy in this century. At stake is not only preventing starvation and saving the environment, but also world peace and security. History tells us that states may go to war over access to resources, and that poverty and famine have often bred fanaticism and terrorism. Working to feed the world will minimize factors that contribute to global instability and the proliferation of weapons of mass destruction. With the world population expected to grow from 6 billion people today to 9 billion by mid-century, the demand for affordable food will increase well beyond current international production levels. People in rapidly developing nations will have the means greatly to improve their standard of living and caloric intake. Inevitably, that means eating more meat. This will raise demand for feed grain at the same time that the growing world population will need vastly more basic food to eat. Complicating a solution to this problem is a dynamic that must be better understood in the West: developing countries often use limited arable land to expand cities to house their growing populations. As good land disappears, people destroy timber resources and even rainforests as they try to create more arable land to feed themselves. The long-term environmental consequences could be disastrous for the entire globe. Productivity revolution To meet the expected demand for food over the next 50 years, we in the United States will have to grow roughly three times more food on the land we have. That’s a tall order. My farm in Marion County, Indiana, for example, yields on average 8.3 to 8.6 tonnes of corn per hectare – typical for a farm in central Indiana. To triple our production by 2050, we will have to produce an annual average of 25 tonnes per hectare. Can we possibly boost output that much? Well, it’s been done before. Advances in the use of fertilizer and water, improved machinery and better tilling techniques combined to generate a threefold increase in yields since 1935 – on our farm back then, my dad produced 2.8 to 3 tonnes per hectare. Much US agriculture has seen similar increases. But of course there is no guarantee that we can achieve those results again. Given the urgency of expanding food production to meet world demand, we must invest much more in scientific research and target that money toward projects that promise to have significant national and global impact. For the United States, that will mean a major shift in the way we conduct and fund agricultural science. Fundamental research will generate the innovations that will be necessary to feed the world. The United States can take a leading position in a productivity revolution. And our success at increasing food production may **play a decisive** humanitarian **role in the survival of** billions of people and the health of **our planet.**

### 2

The President of the United States should give a prompt and full account to Congress of every significant use of cyber weapons, begin an interagency process of doctrine-formation for the offensive use of cyber weapons, and publish the results.

Interagency development of cyber warfare doctrine solves the case – the U.S. is a leader, and the CP incorporates international partners

Mark Young, Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence, 2010, National Cyber Doctrine: The Missing Link in the Application of American Cyber Power, http://jnslp.com/2010/09/29/national-cyber-doctrine-the-missing-link-in-the-application-of-american-cyber-power/

In the development of doctrine**,** foreign partners arealmostas important as the intelligence community in offering particular knowledge, expertise, and intelligence capabilities. **It is unlikely that any future crisis will be met solely by the U**nited **S**tates. **Foreign countries and the U**nited **S**tates are **together on battlefield** of Iraq and Afghanistan, **and they will be in cyber space as well.**

Joint Publication 3-13 states:

**Allies and coalition partners recognize various** [information operations] **concepts and some have thorough and sophisticated doctrine**, procedures, and capabilities for **planning and conducting IO.** The multinational force commander (**MNFC**) **is responsible to resolve potential conflicts between each nation’s IO programs** and the IO objectives and programs of the multinational force. . . . It is vital to integrate allies and coalition partners into IO planning as early as possible so that an integrated and achievable IO strategy can be developed early in the planning process.73

**Foreign partners are critical to the success of U.S. military operations** in all the domains. A new cyber doctrine will clarify the U.S. policy in cyberspace for all allies.

IV. OTHER CONSIDERATIONS

**The most significant policy issues facing any cyberpower projection is the applicability of the Law of War** (LOW). The legal questions must be examined and resolved in detail.74 **The relationship between the laws of war and cyber operations will evolve, but a baseline policy position must involve the entire U.S. government.**

Scrutiny should focus on the definitions of “armed attack,” as well as “distinction” and “proportionality” as applied to cyber operations.75 The U.N. Charter provides guidance for responses to armed attacks. The proper classification of cyber activity as an armed attack is much more difficult than the drafters of the U.N. Charter ever envisioned. These issues are ripe for debate and could be addressed in drafting the guiding principles for a national cyber doctrine.

There is a presumption that the rules of engagement in cyber doctrine “will follow the [L]aw of Armed Conflict, meaning a response taken after receiving an electronic or cyber attack will be scaled in proportion to the attack received, and distinctions will be maintained between combatants and civilians.”76 This presumption may be significant because adversaries using cyber attacks may not distinguish between civilian and military targets. “Security experts warn that all U.S. federal agencies should now be aware that in cyberspace some malicious actors consider that no boundaries exist between military and civilian targets.”77

**The law frequently lags behind technology, but the consequences of adversarial actions against the U**nited **S**tates **and the responses of** the **Cyber Command illustrate the importance of establishing legitimate legal bases for defensive and offensive cyber operations**. “**The potentially nonlethal nature of cyber weapons may cloud the assessment of an attack’s legality, leading to more frequent violations of the principle of distinction** in this new form of warfare than in conventional warfare.”78

**For these reasons, legal experts in the national security sector must engage in the development of the new cyber doctrine.** Now is the time for the UnitedStatesto demonstrate its leadership in establishing the proper doctrine for a governmental approach in accordance with the civil and military principles that have led to U.S. freedom of action.

CONCLUSION

**The U.S. Cyber Command was established** to defend DoD networks against cyber attacks and to develop offensive cyber capabilities. The creation of this command is a legitimate response to the growing capabilities of nations such as China and Russia as well as non-state actors such as al Qaeda and Hamas. The command was established **without an adequate cyber doctrine** to guide the application of joint forces in protecting U.S. freedom of action in cyberspace. **Only by adopting a comprehensive government approach can the U**nited **S**tates **bring its full intellectual might to bear** on the challenging domain of cyberspace.

The joint doctrine development process will allow interagency elements to resolvemanyissues that currently complicate the U.S. approach to cyberpower. The joint doctrine must distinguish computer network operations from their current framework and embrace cyberspace as a war fighting domain. The process will allow debate and resolution of issues such as the training required for a cyber force, the proper classification of U.S. cyber capabilities, the authorities under which computer network attacks may be executed**,** and **actions in cyberspace that** implicate the laws of war**. This new doctrine will enhance U.S. national security by normalizing cyberspace as a domain through which the U**nited **S**tates **can express national values and protect national interests**.

### 1

Restrictions are limitations imposed on action–not reporting and monitoring

**Schiedler-Brown ‘12**

Jean, Attorney, Jean Schiedler-Brown & Associates, Appellant Brief of Randall Kinchloe v. States Dept of Health, Washington, The Court of Appeals of the State of Washington, Division 1, <http://www.courts.wa.gov/content/Briefs/A01/686429%20Appellant%20Randall%20Kincheloe%27s.pdf>

3. The ordinary definition of the term "restrictions" also does not include the reporting and monitoring or supervising terms and conditions that are included in the 2001 Stipulation. Black's Law Dictionary, 'fifth edition,(1979) defines "restriction" as; A limitation often imposed in a deed or lease respecting the use to which the property may be put. The term "restrict' is also cross referenced with the term "restrain." Restrain is defined as; To limit, confine, abridge, narrow down, restrict, obstruct, impede, hinder, stay, destroy. To prohibit from action; to put compulsion on; to restrict; to hold or press back. To keep in check; to hold back from acting, proceeding, or advancing, either by physical or moral force, or by interposing obstacle, to repress or suppress, to curb. In contrast, the terms "supervise" and "supervisor" are defined as; To have general oversight over, to superintend or to inspect. See Supervisor. A surveyor or overseer. . . In a broad sense, one having authority over others, to superintend and direct. The term "supervisor" means an individual having authority, in the interest of the employer, to hire, transfer, suspend, layoff, recall, promote, discharge, assign, reward, or discipline other employees, or responsibility to direct them, or to adjust their grievances, or effectively to recommend such action, if in connection with the foregoing the exercise of such authority is not of a merely routine or clerical nature, but required the use of independent judgment. Comparing the above definitions, it is clear that the definition of "restriction" is very different from the definition of "supervision"-very few of the same words are used to explain or define the different terms. In his 2001 stipulation, Mr. Kincheloe essentially agreed to some supervision conditions, but he did not agree to restrict his license.

That means they must limit presidential discretion

**Lobel, 8** - Professor of Law, University of Pittsburgh Law School (Jules, “Conflicts Between the Commander in Chief and Congress: Concurrent Power over the Conduct of War” 392 OHIO STATE LAW JOURNAL [Vol. 69:391, <http://moritzlaw.osu.edu/students/groups/oslj/files/2012/04/69.3.lobel_.pdf>)

So  too, the congressional power to declare or authorize war has been long held to permit Congress to authorize and wage a limited war—“limited in place, in objects, and in time.” 63 When Congress places such restrictions on the President’s authority to wage war, it limits the President’s discretion to conduct battlefield operations. For example, Congress authorized President George H. W. Bush to attack Iraq in response to Iraq’s 1990 invasion of Kuwait, but it confined the President’s authority to the use of U.S. armed forces pursuant to U.N. Security Council resolutions directed to force Iraqi troops to leave Kuwait. That restriction would not have permitted the President to march into Baghdad after the Iraqi army had been decisively ejected from Kuwait, a limitation recognized by President Bush himself.64

Limits–hundreds of policies raise the costs of Presidential authority – they allow all of them

Ground-consultation allows all the exact same attacks to occur, mixes burdens and kills DA uq

### 4

#### Plan collapses CMR—the military will ignore the aff—kills heg

Mackubin Thomas Owens, professor of national security affairs in the National Security Affairs Department of the Naval War College, Spring 2012, WHAT MILITARY OFFICERS NEED TO KNOW ABOUT CIVIL-MILITARY RELATIONS, http://www.usnwc.edu/getattachment/1ef74daf-ebff-4aa4-866e-e1dd201d780e/What-Military-Officers-Need-to-Know-about-Civil-Mi.aspx

CIVILIAN CONTROL INVOLVES NOT ONLY THE EXECUTIVE BRANCH

It involves Congress as well. As the constitutional scholar Edward Corwin once famously observed, the Constitution is an “invitation to struggle for the privilege of directing American foreign policy” between Congress and the president.13 But **there is a similar tension at work with** regard to **civil-military relations**. Those who neglect the congressional role in American civil-military relations are missing an important element.14

The military has two civilian masters, and this has implications for civil-military relations that officers must understand. For instance, while the president and secretary of defense control the military when it comes to the use of force, including strategy and rules of engagement, Congress controls the military directly with regard to force size, equipment, and organization, and indirectly regarding doctrine and personnel. Indeed, Congress is the “force planner” of last resort.

The U.S. military accepts civilian control by both Congress and the president but offers advice intended to maintain its own institutional and professional autonomy. **On use of force, the military is usually granted a good deal of leeway regarding the terms and conditions** for such use.

By not dissenting from executive-branch policy, American military officers implicitly agree to support presidential decisions on the budget and the use of force, but they also must recognize an obligation to provide their alternative personal views in response to Congress. However, officers must recognize that Congress exerts its control with less regard for military preferences than for the political considerations of its individual members and committees. Thus congressional control of the military is strongly influenced by political considerations, by what Samuel Huntington called “structural,” or domestic, imperatives as opposed to strategic ones.

When the president and Congress are in agreement, the military complies. **When the two branches are in disagreement, the military tends to side with the branch that** most **favors its own views**, but **never to** the point of direct **disobedience to** orders of **the commander in chief**. Military officers are obligated to share their views with Congress. Doing so should not be treated as an “end run” undermining civilian control of the military.15

THE ABSENCE OF A COUP

The absence of a coup does not indicate that civil-military relations are healthy or that civilian control has not eroded. All too often, officers seem to believe that if the United States does not face the prospect of a Latin American– or African-style military coup d’état, all is well in the realm of civil-military relations. But this is a straw man. A number of scholars, including Richard Kohn, Peter Feaver, the late Russell Weigley, Michael Desch, and Eliot Cohen, have argued that although there is no threat of a coup on the part of the military, American civil-military relations have nonetheless deteriorated over the past two decades.16

Their concern is that the American military “has grown in influence to the point of being able to impose its own perspective on many policies and decisions,” which manifests itself in “repeated efforts on the part of the armed forces to frustrate or evade civilian authority when that opposition seems likely to preclude outcomes the military dislikes.” **The result is an unhealthy civil-military pattern that “**could alter the character of American government and **undermine national defense**.”

#### Nuclear war

Frederick Kagan and Michael O’Hanlon 7, Fred’s a resident scholar at AEI, Michael is a senior fellow in foreign policy at Brookings, “The Case for Larger Ground Forces”, April, <http://www.aei.org/files/2007/04/24/20070424_Kagan20070424.pdf>

We live at a time when wars not only rage in nearly every region but threaten to erupt in many places where the current relative calm is tenuous. To view this as a strategic military challenge for the United States is not to espouse a specific theory of America’s role in the world or a certain political philosophy. Such an assessment flows directly from the basic bipartisan view of American foreign policy makers since World War II that overseas threats must be countered before they can directly threaten this country’s shores, that the basic stability of the international system is essential to American peace and prosperity, and that no country besides the United States is in a position to lead the way in countering major challenges to the global order. Let us highlight the threats and their consequences with a few concrete examples, emphasizing those that involve key strategic regions of the world such as the Persian Gulf and East Asia, or key potential threats to American security, such as the spread of nuclear weapons and the strengthening of the global Al Qaeda/jihadist movement. The Iranian government has rejected a series of international demands to halt its efforts at enriching uranium and submit to international inspections. What will happen if the US—or Israeli—government becomes convinced that Tehran is on the verge of fielding a nuclear weapon? North Korea, of course, has already done so, and the ripple effects are beginning to spread. Japan’s recent election to supreme power of a leader who has promised to rewrite that country’s constitution to support increased armed forces—and, possibly, even nuclear weapons— may well alter the delicate balance of fear in Northeast Asia fundamentally and rapidly. Also, in the background, at least for now, SinoTaiwanese tensions continue to flare, as do tensions between India and Pakistan, Pakistan and Afghanistan, Venezuela and the United States, and so on. Meanwhile, the world’s nonintervention in Darfur troubles consciences from Europe to America’s Bible Belt to its bastions of liberalism, yet with no serious international forces on offer, the bloodletting will probably, tragically, continue unabated. And as bad as things are in Iraq today, they could get worse. What would happen if the key Shiite figure, Ali al Sistani, were to die? If another major attack on the scale of the Golden Mosque bombing hit either side (or, perhaps, both sides at the same time)? Such deterioration might convince many Americans that the war there truly was lost—but the costs of reaching such a conclusion would be enormous. Afghanistan is somewhat more stable for the moment, although a major Taliban offensive appears to be in the offing. Sound US grand strategy must proceed from the recognition that, over the next few years and decades, the world is going to be a very unsettled and quite dangerous place, with Al Qaeda and its associated groups as a subset of a much larger set of worries. The only serious response to this international environment is to develop armed forces capable of protecting America’s vital interests throughout this dangerous time. Doing so requires a military capable of a wide range of missions—including not only deterrence of great power conflict in dealing with potential hotspots in Korea, the Taiwan Strait, and the Persian Gulf but also associated with a variety of Special Forces activities and stabilization operations. For today’s US military, which already excels at high technology and is increasingly focused on re-learning the lost art of counterinsurgency, this is first and foremost a question of finding the resources to field a large-enough standing Army and Marine Corps to handle personnel intensive missions such as the ones now under way in Iraq and Afghanistan. Let us hope there will be no such large-scale missions for a while. But preparing for the possibility, while doing whatever we can at this late hour to relieve the pressure on our soldiers and Marines in ongoing operations, is prudent. At worst, the only potential downside to a major program to strengthen the military is the possibility of spending a bit too much money. Recent history shows no link between having a larger military and its overuse; indeed, Ronald Reagan’s time in office was characterized by higher defense budgets and yet much less use of the military, an outcome for which we can hope in the coming years, but hardly guarantee. While the authors disagree between ourselves about proper increases in the size and cost of the military (with O’Hanlon preferring to hold defense to roughly 4 percent of GDP and seeing ground forces increase by a total of perhaps 100,000, and Kagan willing to devote at least 5 percent of GDP to defense as in the Reagan years and increase the Army by at least 250,000), we agree on the need to start expanding ground force capabilities by at least 25,000 a year immediately. Such a measure is not only prudent, it is also badly overdue.

### 5

The United States federal government should require consultation with congress prior to every use of cyber attacks and cyberexploitation operations not targeted at Iran’s nuclear program by the President of the United States and require a prompt and full account of every significant use of cyber weapons by the President of the United States.

The counterplan is functionally and textually competitive – it PICs out of prior consultation for cyber exploitation targeted at Iran

Lin, Chief Scientist, Computer Science and Telecommunications Board, National Research Council of the National Academies, 2010

(Herbert S., former staff member and scientist for the House Armed Services Committee, “Offensive Cyber Operations and the Use of Force,” *Journal of National Security Law and Policy*, <http://jnslp.com/2010/08/13/offensive-cyber-operations-and-the-use-of-force/>)

Hostile actions against a computer system or network can take two forms.1 One form – a cyber attack – is destructive in nature. An example of such a hostile action is erasure by a computer virus resident on the hard disk of any infected computer. In this article, “cyber attack” refers to the use of deliberate actions and operations – perhaps over an extended period of time – to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and (or) programs resident in or transiting these systems or networks.2 Such effects on adversary systems and networks may also have indirect effects on entities coupled to or reliant on them. A cyber attack seeks to cause the adversary’s computer systems and networks to be unavailable or untrustworthy and therefore less useful to the adversary.

The second form – cyberexploitation – is nondestructive. An example is a computer virus that searches the hard disk of any infected computer and emails to the hostile party all files containing a credit card number. “Cyberexploitation” refers to the use of actions and operations – perhaps over an extended period of time – to obtain information that would otherwise be kept confidential and is resident on or transiting through an adversary’s computer systems or networks. Cyberexploitations are usually clandestine and conducted with the smallest possible intervention that still allows extraction of the information sought.3 They do not seek to disturb the normal functioning of a computer system or network from the user’s point of view, and the best cyberexploitation is one that a user never notices.

For purposes of this article, **the term** “**offensive cyber operations**” **will include military operations and activities in cyberspace for cyber attack against and** (**or**) **cyberexploitation of adversary information systems and networks**. When greater specificity is needed, the terms “cyber attack” and “cyberexploitation” will be used.4

Although the objectives and the legal and policy constructs relevant to cyber attack and cyberexploitation are quite different (see the table in the Appendix to this article), **the technological underpinnings and associated operational considerations of both are quite similar**.

Cyber attacks and cyberexploitation require a vulnerability, access to that vulnerability, and a payload to be executed.5 In a noncyber context, a vulnerability might be a lock to a file cabinet that could be easily picked. Access would be an available path for reaching the file cabinet. From an intruder’s perspective, access to a file cabinet located on the International Space Station would pose a very different problem from that posed by the same cabinet located in an office in Washington, D.C. The payload is responsible for executing the action taken by the intruder after the lock is picked. For example, the intruder can destroy the papers inside, or alter some of the information in those papers.

Plan makes espionage ineffective and un-credible

Lorber ’13

Eric, J.D. Candidate, University of Pennsylvania Law School, Ph.D Candidate, Duke University Department of Political Science, “Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?,” 15 U. Pa. J. Const. L. 961

Yet a surprising amount of uncertainty exists as to which - if any - domestic laws constrain the use of OCOs and how they fit into the congressional-executive balance. As policymakers, scholars, and journalists have lamented, a coherent policy framework governing the use of OCOs does not exist and many questions remain unanswered. n8 Would an attack [\*963] using cyber weapons trigger the requirements of the War Powers Resolution? n9 Would OCOs be subject to reporting requirements under the Intelligence Authorization Act? n10 Conversely, do cyber operations grant the executive branch another tool with which it can prosecute attacks but avoid reporting and responding to congressional inquiries? These questions are largely unanswered both because the rise of OCOs is a relatively recent phenomenon and because much of the information about U.S. technical capability in this field is highly classified. n11 Yet addressing these questions is increasingly important for two reasons. First, as states such as China, Israel, Russia, and the United States 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. n12 Second, the possible employment of these tools adds yet another wrinkle to the battle between the executive and legislative branches over war-making authority. n13 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. n14 As a result, the employment of these tools [\*964] implicates - and perhaps problematically shifts - the balance between the executive's commander-in-chief power n15 and Congress's war-making authority. n16 This Comment provides an initial answer to the question of whether current U.S. law can effectively govern the Executive's use of OCOs. n17 It explores the interaction between this new tool and the current statutory limits on presidential war-making authority, with a particular focus on whether the two current federal laws meant to restrict executive power in this field - the War Powers Resolution n18 and the Intelligence Authorization Act n19 - apply to a wide range of potential offensive cyber operations undertaken by the executive branch. Beyond suggesting that neither the War Powers Resolution nor the Intelligence Authorization Act can effectively regulate most types of offensive cyber operations, this Comment suggests that while marginally problematic for a proper balance of war-making power between the executive and legislative branches, this lack of oversight does not fundamentally shift the current alignment. It does argue, however, that - given this lack of regulatory oversight - **the President now has another powerful war-making tool to use at his discretion**. Finally, the Comment suggests that this lack of limitation may be positive in some ways, as laying down clear legal markers before having a developed understanding of these capabilities may problematically limit their effective use.

Credible threat of espionage is the only way to solve Iran prolif – stuxnet proves fear is high now

Albright et al. 12 [David Albright, chairperson of ISIS, Paul Brannan, senior analyst at ISIS who has done extensive research and analysis on the international nuclear black market, Andrea Stricker, research analyst, Christina Walrond, and Houston Wood, “PREVENTING IRAN FROM GETTING NUCLEAR WEAPONS: CONSTRAINING ITS FUTURE NUCLEAR OPTIONS,” The Institute for Science and International Security, March 5, http://w.isis-online.org/uploads/isis-reports/documents/USIP\_Template\_5March2012-1.pdf]

Iran’s efforts to build covert nuclear sites, which it could operate out of sight of IAEA inspectors, have¶ time and again failed either through good IAEA detective work or Western intelligence agency¶ discoveries. The most recent case is¶ the confirmation by Western intelligence in mid¶ -¶ 2009 that Iran was¶ building a clandestine centrifuge plant near the city of Qom. Senior officials close to the IAEA suspect¶ that this enrichment site was intended to be part of a parallel, secret program to¶ produce weapon¶ -¶ grade¶ uranium under the control of the Iranian military. That facility, now called the Fordow Fuel Enrichment¶ Plant (FFEP), is currently under IAEA safeguards, and Iran declared that it is dedicated to the production¶ of 3.5 percent and 19.7¶ 5 percent uranium. The November 2011 IAEA safeguards report on Iran¶ contains numerous other examples of secret military related nuclear activities and facilities in Iran¶ discovered by about ten IAEA member states, including the United States, Britain, Fra¶ nce, Germany, and¶ Israel.¶ In order to deter Iran from constructing covert nuclear sites, intelligence options aimed at their¶ detection remain vitally important. Known methods used by intelligence agencies include human¶ spying, cyber snooping, aerial surve¶ illance, and bugging of equipment procured by Iran overseas.¶ Intelligence agencies are also encouraging more defectors from the nuclear program with some notable¶ successes.¶ As a result, **Iran must be increasingly anxious that its nuclear program is highly**¶ **penetrated by foreign**¶ **intelligence** agencies. It may hesitate in making decisions to construct parallel, clandestine facilities to¶ make weapon grade uranium; currently, **there is no evidence of a secret enrichment site** able to¶ produce weapon¶ -¶ grade uranium.¶ The 2009/2010 cyber attack by the Stuxnet malware on the Natanz¶ enrichment plant likely worsened Iran’s paranoia. Whichever nation launched that attack had a¶ surprising amount of confidential detail a¶ bout operations at the facility¶ -¶ far more inside information¶ than could be acquired from IAEA reporting. Intelligence agencies needed to penetrate both the inner¶ workings of that plant and a collection of Iranian companies, which illicitly obtained Siemens computer¶ control equipment and software and prepared¶ it for delivery to the centrifuge program, leading to the¶ Stuxnet attack. Moreover, Stuxnet also functioned to gather information about operations at Iran’s¶ centrifuge sites and broadcast them through the Internet to command and control servers located¶ out¶ side Iran.¶ Stuxnet is an example of a covert effort that seeks to actively damage Iranian nuclear equipment¶ subject to U.N. Security Council resolutions. It destroyed at least 1,000 IR¶ -¶ 1 centrifuges at the Natanz¶ Fuel Enrichment Plant and set the progra¶ m back by about a year. **It may have caused lingering effects**¶ that contribute to centrifuge problems at the Natanz plant today. Despite their controversy, more cyber¶ attacks may yet occur. **A Stuxnet 2.0** or 3.0 **may sorely test Iran’s claim that it improved i**¶ **ts cyber**¶ **security** and its ability to significantly mitigate the effects of another cyber attack on the centrifuges at¶ Natanz.¶ The discovery in the fall of 2011 of the ―Duqu‖ malware heightened expectations of additional attacks.¶ This malware, according¶ to the computer security firm Symantec, which analyzed the code, has nearly¶ identical components to the original Stuxnet malware and appears to be the precursor to a future¶ Stuxnet¶ -¶ like attack. Symantec found that ―Duqu’s purpose is to gather intelligence¶ data and assets from¶ entities, such as industrial control system manufacturers, in order to more easily conduct a future¶ attack against another third party. The attackers are looking for information such as design documents¶ that could help them mount a fut¶ ure attack on an industrial control facility.‖¶ 11¶ Despite the downsides¶ and risks associated with cyber attacks against Iranian nuclear facilities, **the tactic is becoming more**¶widely accepted **as a means to slow down Iran’s nuclear progress and stymie progr**¶ **ams which violate**¶ **UNSC resolutions, particularly the uranium enrichment program**.¶ 16¶ Broader sabotage of Iran’s imported equipment is another well¶ -¶ known tactic of Western intelligence¶ agencies. Intelligence agencies first infiltrate an Iranian smuggling networ¶ k and provide the goods the¶ network seeks, but not before they first modify the goods so they will not work, perhaps in a way that¶ will damage adjacent equipment. Sometimes bugging devices are placed in the equipment and send¶ information about operations a¶ fter the equipment is installed at a site. This technique has likely¶ revealed at least one of Iran’s **secret nuclear sites** and, according to official Iranian statements, to have¶ caused centrifuges to break. Undoubtedly, the tactic is being pursued more dili¶ gently today by a range¶ of countries.¶ There are several riskier strategies that are being pursued against Iran that have serious downsides¶ and implications. Assassinations of Iranian nuclear scientists and engineers have occurred with greater¶ frequency b¶ ut should be stopped because they carry too high a risk of retaliation and involve terrorism¶ against civilians. Moreover, **assassinations are unlikely to be effective** in setting back the nuclear¶ program, which involves thousands of specialists and ingrained know - how. Furthermore, Iran could¶ argue that assassinations are equivalent to a military attack and use this as justification for further¶ provocations. An under¶ -¶ siege mentality created by use of such tactics could motivate Iran to further¶ degrade its cooperation with the IAEA and resist offers of negotiation.¶ Recent major accidents at Iranian facilities have led to speculation that countries are conducting¶ sabotage against significant Iranian missile and nuclear¶ -¶ related sites. An explosion late last yea¶ r at a¶ major missile production facility outside Tehran is being called sabotage by some.¶ 12¶ In December 2012,¶ there was an explosion at the newly opened¶ Ghadir steelworks¶ in Yazd that reportedly could have been¶ making maraging steel. Despite Iranian denial¶ s of sabotage and a lack of clear evidence of sabotage,¶ these cases have ignited a debate into the risks, feasibility, and desirability of sabotaging major¶ facilities via covert operations that go beyond cyber attacks.

Nuclear war

Edelman, distinguished fellow – Center for Strategic and Budgetary Assessments, ‘11

(Eric S, “The Dangers of a Nuclear Iran,” *Foreign Affairs*, January/February)

The reports of the Congressional Commission on the Strategic Posture of the United States and the Commission on the Prevention Of Weapons of Mass Destruction Proliferation and Terrorism, as well as other analyses, have highlighted the risk that a nuclear-armed Iran could trigger additional nuclear proliferation in the Middle East, even if Israel does not declare its own nuclear arsenal. Notably, Algeria, Bahrain, Egypt, Jordan, Saudi Arabia,Turkey, and the United Arab Emirates— all signatories to the Nuclear Nonproliferation Treaty (npt)—have recently announced or initiated nuclear energy programs. Although some of these states have legitimate economic rationales for pursuing nuclear power and although the low-enriched fuel used for power reactors cannot be used in nuclear weapons, these moves have been widely interpreted as hedges against a nuclear-armed Iran. The npt does not bar states from developing the sensitive technology required to produce nuclear fuel on their own, that is, the capability to enrich natural uranium and separate plutonium from spent nuclear fuel. Yet enrichment and reprocessing can also be used to accumulate weapons-grade enriched uranium and plutonium—the very loophole that Iran has apparently exploited in pursuing a nuclear weapons capability. Developing nuclear weapons remains a slow, expensive, and di⁄cult process, even for states with considerable economic resources, and especially if other nations try to constrain aspiring nuclear states’ access to critical materials and technology. Without external support, it is unlikely that any of these aspirants could develop a nuclear weapons capability within a decade.

There is, however, at least one state that could receive significant outside support: Saudi Arabia. And if it did, proliferation could accelerate throughout the region. Iran and Saudi Arabia have long been geopolitical and ideological rivals. Riyadh would face tremendous pressure to respond in some form to a nuclear-armed Iran, not only to deter Iranian coercion and subversion but also to preserve its sense that Saudi Arabia is the leading nation in the Muslim world. The Saudi government is already pursuing a nuclear power capability, which could be the first step along a slow road to nuclear weapons development. And concerns persist that it might be able to accelerate its progress by exploiting its close ties to Pakistan. During the 1980s, in response to the use of missiles during the Iran-Iraq War and their growing proliferation throughout the region, Saudi Arabia acquired several dozen css-2 intermediate-range ballistic missiles from China. The Pakistani government reportedly brokered the deal, and it may have also oªered to sell Saudi Arabia nuclear warheads for the css-2s, which are not accurate enough to deliver conventional warheads eªectively. There are still rumors that Riyadh and Islamabad have had discussions involving nuclear weapons, nuclear technology, or security guarantees. This “Islamabad option” could develop in one of several diªerent ways. Pakistan could sell operational nuclear weapons and delivery systems to Saudi Arabia, or it could provide the Saudis with the infrastructure, material, and technical support they need to produce nuclear weapons themselves within a matter of years, as opposed to a decade or longer. Not only has Pakistan provided such support in the past, but it is currently building two more heavy-water reactors for plutonium production and a second chemical reprocessing facility to extract plutonium from spent nuclear fuel. In other words, it might accumulate more fissile material than it needs to maintain even a substantially expanded arsenal of its own. Alternatively, Pakistan might oªer an extended deterrent guarantee to Saudi Arabia and deploy nuclear weapons, delivery systems, and troops on Saudi territory, a practice that the United States has employed for decades with its allies. This arrangement could be particularly appealing to both Saudi Arabia and Pakistan. It would allow the Saudis to argue that they are not violating the npt since they would not be acquiring their own nuclear weapons. And an extended deterrent from Pakistan might be preferable to one from the United States because stationing foreign Muslim forces on Saudi territory would not trigger the kind of popular opposition that would accompany the deployment of U.S. troops. Pakistan, for its part, would gain financial benefits and international clout by deploying nuclear weapons in Saudi Arabia, as well as strategic depth against its chief rival, India. The Islamabad option raises a host of difficult issues, perhaps the most worrisome being how India would respond. Would it target Pakistan’s weapons in Saudi Arabia with its own conventional or nuclear weapons? How would this expanded nuclear competition influence stability during a crisis in either the Middle East or South Asia? Regardless of India’s reaction, any decision by the Saudi government to seek out nuclear weapons, by whatever means, would be highly destabilizing. It would increase the incentives of other nations in the Middle East to pursue nuclear weapons of their own. And it could increase their ability to do so by eroding the remaining barriers to nuclear proliferation: each additional state that acquires nuclear weapons weakens the nonproliferation regime, even if its particular method of acquisition only circumvents, rather than violates, the NPT.

n-player competition

Were Saudi Arabia to acquire nuclear weapons, the Middle East would count three nuclear-armed states, and perhaps more before long. It is unclear how such an n-player competition would unfold because most analyses of nuclear deterrence are based on the U.S.- Soviet rivalry during the Cold War. It seems likely, however, that the interaction among three or more nuclear-armed powers would be more prone to miscalculation and escalation than a bipolar competition. During the Cold War, the United States and the Soviet Union only needed to concern themselves with an attack from the other. Multipolar systems are generally considered to be less stable than bipolar systems because coalitions can shift quickly, upsetting the balance of power and creating incentives for an attack. More important, emerging nuclear powers in the Middle East might not take the costly steps necessary to preserve regional stability and avoid a nuclear exchange. For nuclear-armed states, the bedrock of deterrence is the knowledge that each side has a secure second-strike capability, so that no state can launch an attack with the expectation that it can wipe out its opponents’ forces and avoid a devastating retaliation. However, emerging nuclear powers might not invest in expensive but survivable capabilities such as hardened missile silos or submarinebased nuclear forces. Given this likely vulnerability, the close proximity of states in the Middle East, and the very short flight times of ballistic missiles in the region, any new nuclear powers might be compelled to “launch on warning” of an attack or even, during a crisis, to use their nuclear forces preemptively. Their governments might also delegate launch authority to lower-level commanders, heightening the possibility of miscalculation and escalation. Moreover, if early warning systems were not integrated into robust command-and-control systems, the risk of an unauthorized or accidental launch would increase further still. And without sophisticated early warning systems, a nuclear attack might be unattributable or attributed incorrectly. That is, assuming that the leadership of a targeted state survived a first strike, it might not be able to accurately determine which nation was responsible. And this uncertainty, when combined with the pressure to respond quickly,would create a significant risk that it would retaliate against the wrong party, potentially triggering a regional nuclear war.

### Adv 1

Congress cant check use of force

Douglas Kriner, Assistant Profess of Political Science at Boston University, 2010, After the Rubicon: Congress, Presidents, and the Politics of Waging War, p. 6-8

The role that Congress plays in deciding whether a war is continued or concluded is of intrinsic interest to academics, policymakers, and casual observers of contemporary American politics alike. Yet the belief that Congress retains some capacity to shape the conduct of military affairs after a venture is launched is also a critically important and untested proposition underlying most theories asserting congressional influence over the initiation of military action. Why, according to this emerging literature, do presidents facing a strong opposition party in Congress use force less frequently than do their peers with strong partisan majorities in Congress? The most commonly offered answer is that presidents anticipate Congress's likely reaction to a prospective use of force and respond accordingly.14 Presidents who confront an opposition-led Congress anticipate that it is more willing and able to challenge the administration's conduct of military action than a Congress controlled by their partisan allies. Therefore, the frequency with which presidents use force abroad covaries with the strength of their party in Congress. However, this anticipatory logic requires that Congress has the ability to raise the costs of military action for the president, once that action has begun. If Congress lacks this capacity, presidents have little reason to adjust their willingness to initiate the use of force in anticipation of an adverse congressional response." As a result, determining whether and how Congress can influence the scope and duration of ongoing military operations is critically important even to evaluating prior research that asserts congressional influence over the initiation of military actions. Without it, such analyses rest on shaky ground. Unfortunately, because the dynamics change dramatically once American troops are deployed abroad, simply drawing lessons from existing studies of interbranch dynamics in military policymaking at the conflict initiation phase and applying them to the conflict conduct phase is unlikely to offer much insight." The decision-making environment at the conflict conduct phase differs from that at the conflict initiation phase along at least three key dimensions: the incentives and constraints governing congressional willingness to challenge presidential discretion; the relative institutional capacities of the executive and legislative branches to affect military policymaking; and finally, the ability of unfolding conflict events to change further the political and strategic environment in which the two branches vie for power. With regard to the political constraints that limit would-be adversaries in Congress, the president may **be in an even stronger position** after American troops are deployed in the field. Ordering troops abroad is akin to other unilateral presidential actions; by seizing his office's capacity for independent action, a president can dramatically **change the status quo** and fundamentally alter the political playing field on which Congress and other actors must act to challenge his policies.17 Once the troops are overseas, the political stakes for any congressional challenge to the president's policies are inexorably raised; any such effort is subject to potentially ruinous charges of failing to support the troops. Georgia Senator Richard Russell's conversion from opposition to U.S. intervention in Vietnam in the early 196os to stalwart support for staying the course after Lyndon Johnson's escalation of the American commitment there illustrates this change: "We are there now, and the time for debate has passed. Our flag is committed, and—more importantly—American boys are under fire."" Russell's sentiment was loudly echoed forty years later in the allegations by the Bush administration and its partisan allies in Congress that any legislative efforts to curtail the war in Iraq undermined the troops. As a result of these potentially **intense political costs**, there are reasons to question whether Congress can mount an effective challenge to the policies of the commander in chief. If it cannot, this would compel a reassessment of prior theories asserting congressional influence over the initiation of military actions through the logic of anticipated response. Certainly, more empirical analysis is needed to answer this question.

Cyber war infeasible

Clark, MA candidate – Intelligence Studies @ American Military University, senior analyst – Chenega Federal Systems, 4/28/’12

(Paul, “The Risk of Disruption or Destruction of Critical U.S. Infrastructure by an Offensive Cyber Attack,” American Military University)

The Department of Homeland Security worries that our critical infrastructure and key resources (CIKR) may be exposed, both directly and indirectly, to multiple threats because of CIKR reliance on the global cyber infrastructure, an infrastructure that is under routine cyberattack by a “spectrum of malicious actors” (National Infrastructure Protection Plan 2009). CIKR in the extremely large and complex U.S. economy spans multiple sectors including agricultural, finance and banking, dams and water resources, public health and emergency services, military and defense, transportation and shipping, and energy (National Infrastructure Protection Plan 2009). The disruption and destruction of public and private infrastructure is part of warfare, without this infrastructure conflict cannot be sustained (Geers 2011). Cyber-attacks are desirable because they are considered to be a relatively “low cost and long range” weapon (Lewis 2010), but prior to the creation of Stuxnet, the first cyber-weapon, the ability to disrupt and destroy critical infrastructure through cyber-attack was theoretical. The movement of an offensive cyber-weapon from conceptual to actual has forced the United States to question whether offensive cyber-attacks are a significant threat that are able to disrupt or destroy CIKR to the level that national security is seriously degraded. It is important to understand the risk posed to national security by cyber-attacks to ensure that government responses are appropriate to the threat and balance security with privacy and civil liberty concerns. The risk posed to CIKR from cyber-attack can be evaluated by measuring the threat from cyber-attack against the vulnerability of a CIKR target and the consequences of CIKR disruption. As the only known cyber-weapon, Stuxnet has been **thoroughly analyzed** and **used as a model** for predicting future cyber-weapons. The U.S. electrical grid, a key component in the CIKR energy sector, is a target that has been analyzed for vulnerabilities and the consequences of disruption predicted – the electrical grid has been used in multiple attack scenarios including a classified scenario provided to the U.S. Congress in 2012 (Rohde 2012). Stuxnet will serve as the weapon and the U.S. electrical grid will serve as the target in this risk analysis that concludes that there is a low risk of disruption or destruction of critical infrastructure from a an offensive cyber-weapon because of the complexity of the attack path, the limited capability of non-state adversaries to develop cyber-weapons, and the existence of multiple methods of mitigating the cyber-attacks. To evaluate the threat posed by a Stuxnet-like cyber-weapon, the complexity of the weapon, the available attack vectors for the weapon, and the resilience of the weapon must be understood. The complexity – how difficult and expensive it was to create the weapon – identifies the relative cost and availability of the weapon; inexpensive and simple to build will be more prevalent than expensive and difficult to build. Attack vectors are the available methods of attack; the larger the number, the more severe the threat. For example, attack vectors for a cyberweapon may be email attachments, peer-to-peer applications, websites, and infected USB devices or compact discs. Finally, the resilience of the weapon determines its availability and affects its usefulness. A useful weapon is one that is resistant to disruption (resilient) and is therefore available and reliable. These concepts are seen in the AK-47 assault rifle – a simple, inexpensive, reliable and effective weapon – and carry over to information technology structures (Weitz 2012). The evaluation of Stuxnet identified malware that is “unusually complex and large” and required code written in multiple languages (Chen 2010) in order to complete a variety of specific functions contained in a “vast array” of components – **it is one of the most complex threats ever analyzed by Symantec** (Falliere, Murchu and Chien 2011). To be successful, Stuxnet required a **high** **level of technical knowledge across multiple disciplines**, a laboratory with the target equipment configured for testing, and a foreign intelligence capability to collect information on the target network and attack vectors (Kerr, Rollins and Theohary 2010). The malware also needed careful monitoring and maintenance because it could be easily disrupted; as a result Stuxnet was developed with a high degree of configurability and was upgraded multiple times in less than one year (Falliere, Murchu and Chien 2011). Once introduced into the network, the cyber-weapon then had to utilize four known vulnerabilities and four unknown vulnerabilities, known as zero-day exploits, in order to install itself and propagate across the target network (Falliere, Murchu and Chien 2011). Zero-day exploits are **incredibly difficult to find** and fewer than twelve out of the 12,000,000 pieces of malware discovered each year utilize zero-day exploits and this rarity makes them valuable, zero-days can fetch $50,000 to $500,000 each on the black market (Zetter 2011). The use of four rare exploits in a single piece of malware is “unprecedented” (Chen 2010). Along with the use of four unpublished exploits, Stuxnet also used the “first ever” programmable logic controller rootkit, a Windows rootkit, antivirus evasion techniques, intricate process injection routines, and other complex interfaces (Falliere, Murchu and Chien 2011) all **wrapped up in “layers of encryption** like Russian nesting dolls” (Zetter 2011) – including custom encryption algorithms (Karnouskos 2011). As the malware spread across the now-infected network it had to utilize additional vulnerabilities in proprietary Siemens industrial control software (ICS) and hardware used to control the equipment it was designed to sabotage. Some of these ICS vulnerabilities were published but some were unknown and **required such a high degree of inside knowledge** that there was speculation that a Siemens employee had been involved in the malware design (Kerr, Rollins and Theohary 2010). The unprecedented technical complexity of the Stuxnet cyber-weapon, along with the extensive technical and financial resources and foreign intelligence capabilities required for its development and deployment, indicates that the malware was likely developed by a nation-state (Kerr, Rollins and Theohary 2010). Stuxnet had very limited attack vectors. When a computer system is connected to the public Internet a host of attack vectors are available to the cyber-attacker (Institute for Security Technology Studies 2002). Web browser and browser plug-in vulnerabilities, cross-site scripting attacks, compromised email attachments, peer-to-peer applications, operating system and other application vulnerabilities are all vectors for the introduction of malware into an Internetconnected computer system. Networks that are not connected to the public internet are “air gapped,” a technical colloquialism to identify a physical separation between networks. Physical separation from the public Internet is a common safeguard for sensitive networks including classified U.S. government networks. If the target network is air gapped, infection can only occur through physical means – an infected disk or USB device that **must be physically introduced** into a possibly access controlled environment and connected to the air gapped network. The first step of the Stuxnet cyber-attack was to initially infect the target networks, a difficult task given the probable disconnected and well secured nature of the Iranian nuclear facilities. Stuxnet was introduced via a USB device to the target network, a method that suggests that the attackers were familiar with the configuration of the network and knew it was not connected to the public Internet (Chen 2010). This assessment is supported by two rare features in Stuxnet – having all necessary functionality for industrial sabotage fully embedded in the malware executable along with the ability to self-propagate and upgrade through a peer-to-peer method (Falliere, Murchu and Chien 2011). Developing an understanding of the target network configuration was a significant and daunting task based on Symantec’s assessment that Stuxnet repeatedly targeted a total of five different organizations over nearly one year (Falliere, Murchu and Chien 2011) with physical introduction via USB drive being the only available attack vector. The final factor in assessing the threat of a cyber-weapon is the resilience of the weapon. There are two primary factors that make Stuxnet **non-resilient**: the complexity of the weapon and the complexity of the target. Stuxnet was highly customized for sabotaging specific industrial systems (Karnouskos 2011) and needed a large number of very complex components and routines in order to increase its chance of success (Falliere, Murchu and Chien 2011). The **malware required eight vulnerabilities** in the Windows operating system **to succeed** and therefore would have failed if those vulnerabilities had been properly patched; four of the eight vulnerabilities were known to Microsoft and subject to elimination (Falliere, Murchu and Chien 2011). Stuxnet also required that two drivers be installed and required two stolen security certificates for installation (Falliere, Murchu and Chien 2011); driver installation would have failed if the stolen certificates had been revoked and marked as invalid. Finally, the configuration of systems is ever-changing as components are upgraded or replaced. There is no guarantee that the network that was mapped for vulnerabilities had not changed in the months, or years, it took to craft Stuxnet and successfully infect the target network. Had specific components of the target hardware changed – the targeted Siemens software or programmable logic controller – the attack would have failed. Threats are less of a threat when identified; this is why zero-day exploits are so valuable. Stuxnet went to great lengths to hide its existence from the target and utilized multiple rootkits, data manipulation routines, and virus avoidance techniques to stay undetected. The malware’s actions occurred only in memory to avoid leaving traces on disk, it masked its activities by running under legal programs, employed layers of encryption and code obfuscation, and uninstalled itself after a set period of time, all efforts to avoid detection because its authors knew that detection meant failure. As a result of the complexity of the malware, the changeable nature of the target network, and the chance of discovery, Stuxnet is not a resilient system. It is a fragile weapon that required an investment of time and money to constantly monitor, reconfigure, test and deploy over the course of a year. There is concern, with Stuxnet developed and available publicly, that the world is on the brink of a storm of highly sophisticated Stuxnet-derived cyber-weapons which can be used by hackers, organized criminals and terrorists (Chen 2010). As former counterterrorism advisor Richard Clarke describes it, there is concern that the technical brilliance of the United States “has created millions of potential monsters all over the world” (Rosenbaum 2012). Hyperbole aside, technical knowledge spreads. The techniques behind cyber-attacks are “constantly evolving and making use of lessons learned over time” (Institute for Security Technology Studies 2002) and the publication of the Stuxnet code may make it easier to copy the weapon (Kerr, Rollins and Theohary 2010). **However**, this is something of a zero-sum game because knowledge works both ways and cyber-security techniques are also evolving, and “understanding attack techniques more clearly is the first step toward increasing security” (Institute for Security Technology Studies 2002). Vulnerabilities are discovered and patched, intrusion detection and malware signatures are expanded and updated, and monitoring and analysis processes and methodologies are expanded and honed. Once the element of surprise is lost, weapons and tactics are less useful, this is the core of the argument that “uniquely surprising” **stratagems like Stuxnet are single-use**, like Pearl Harbor and the Trojan Horse, the “very success [of these attacks] precludes their repetition” (Mueller 2012). This paradigm has already been seen in the “son of Stuxnet” malware – named Duqu by its discoverers – that is based on the same modular code platform that created Stuxnet (Ragan 2011). With the techniques used by Stuxnet now known, other variants such as Duqu are being discovered and countered by security researchers (Laboratory of Cryptography and System Security 2011). It is obvious that the effort required to create, deploy, and maintain Stuxnet and its variants is massive and it is not clear that the rewards are worth the risk and effort. Given the location of initial infection and the number of infected systems in Iran (Falliere, Murchu and Chien 2011) it is believed that Iranian nuclear facilities were the target of the Stuxnet weapon. A significant amount of money and effort was invested in creating Stuxnet but yet the expected result – assuming that this was an attack that expected to damage production – was minimal at best. Iran claimed that Stuxnet caused only minor damage, probably at the Natanz enrichment facility, the Russian contractor Atomstroyeksport reported that no damage had occurred at the Bushehr facility, and an unidentified “senior diplomat” suggested that Iran was forced to shut down its centrifuge facility “for a few days” (Kerr, Rollins and Theohary 2010). Even the most optimistic estimates believe that Iran’s nuclear enrichment program was only delayed by months, or perhaps years (Rosenbaum 2012). The actual damage done by Stuxnet is not clear (Kerr, Rollins and Theohary 2010) and the primary damage appears to be to a higher number than average replacement of centrifuges at the Iran enrichment facility (Zetter 2011). Different targets may produce different results. The Iranian nuclear facility was a difficult target with limited attack vectors because of its isolation from the public Internet and restricted access to its facilities. What is the probability of a successful attack against the U.S. electrical grid and what are the potential consequences should this critical infrastructure be disrupted or destroyed? An attack against the electrical grid is a reasonable threat scenario since power systems are “a high priority target for military and insurgents” and there has been a trend towards utilizing commercial software and integrating utilities into the public Internet that has “increased vulnerability across the board” (Lewis 2010). Yet the increased vulnerabilities are mitigated by an increased detection and deterrent capability that has been “honed over many years of practical application” now that power systems are using standard, rather than proprietary and specialized, applications and components (Leita and Dacier 2012). The security of the electrical grid is also enhanced by increased awareness after a smart-grid hacking demonstration in 2009 and the identification of the Stuxnet malware in 2010; as a result the public and private sector are working together in an “unprecedented effort” to establish robust security guidelines and cyber security measures (Gohn and Wheelock 2010).

Networks are safe—nobody has the means

Gray 13

COLIN S. GRAY is Professor of International Politics and Strategic Studies at the University of Reading, England, worked at the International Institute for Strategic Studies and at the Hudson Institute before founding the National Institute for Public Policy, Author of 25 books, Strategic Studies Institute, April 2013, "MAKING STRATEGIC SENSE OF CYBER POWER: WHY THE SKY IS NOT FALLING", http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf

It is one thing to be able to be an electronic nuisance, to annoy, disrupt, and perhaps delay. But it is quite another to be capable of inflicting real persisting harm on the fighting power of an enemy. Critically important military computer networks are, of course, accessible neither to the inspired amateur outsider, nor to the malignant political enemy. Easy passing reference to a hypothetical “cyber Pearl Harbor” reflects both poor history and ignorance of contemporary military common sense. Critical potential military (and other) targets for cyber attack are extremely hard to access and influence (I believe and certainly hope), and the technical knowledge, skills, and effort required to do serious harm to national security is forbiddingly high. This is not to claim, foolishly, that cyber means absolutely could not secure near-catastrophic results. However, it is to say that such a scenario is extremely improbable. Cyber defense is advancing all the time, as is cyber offense, of course. But so discretionary in vital detail can one be in the making of cyberspace, that confidence—real confidence—in cyber attack could not plausibly be high. It should be noted that I am confining this particular discussion to what rather idly tends to be called cyber war. In political and strategic practice, it is unlikely that war would or, more importantly, ever could be restricted to the EMS. Somewhat rhetorically, one should pose the question: Is it likely (almost anything, strictly, is possible) that cyber war with the potential to inflict catastrophic damage would be allowed to stand unsupported in and by action in the other four geographical domains of war? I believe not.

Defense is dominant

**Rid 12** (Thomas Rid, reader in war studies at King's College London, is author of "Cyber War Will Not Take Place" and co-author of "Cyber-Weapons.", March/April 2012, “Think Again: Cyberwar”, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full)

"Cyberweapons Can Create Massive Collateral Damage." Very unlikely. When news of Stuxnet broke, the New York Times reported that the most striking aspect of the new weapon was the "collateral damage" it created. The malicious program was "splattered on thousands of computer systems around the world, and much of its impact has been on those systems, rather than on what appears to have been its intended target, Iranian equipment," the Times reported. Such descriptions encouraged the view that computer viruses are akin to highly contagious biological viruses that, once unleashed from the lab, will turn against all vulnerable systems, not just their intended targets. But this metaphor is deeply flawed. As the destructive potential of a cyberweapon grows, the likelihood that it could do far-reaching damage across many systems shrinks. Stuxnet did infect more than 100,000 computers -- mainly in Iran, Indonesia, and India, though also in Europe and the United States. But it was so specifically programmed that it didn't actually damage those machines, afflicting only Iran's centrifuges at Natanz. The worm's aggressive infection strategy was designed to maximize the likelihood that it would reach its intended target. Because that final target was not networked, "all the functionality required to sabotage a system was embedded directly in the Stuxnet executable," the security software company Symantec observed in its analysis of the worm's code. So yes, Stuxnet was "splattered" far and wide, but it only executed its damaging payload where it was supposed to. Collateral infection, in short, is not necessarily collateral damage. A sophisticated piece of malware may aggressively infect many systems, but if there is an intended target, the infection will likely have a distinct payload that will be harmless to most computers. Especially in the context of more sophisticated cyberweapons, the image of inadvertent collateral damage doesn't hold up. They're more like a flu virus that only makes one family sick. "In Cyberspace, Offense Dominates Defense." Wrong again. The information age has "offense-dominant attributes," Arquilla and Ronfeldt wrote in their influential 1996 book, The Advent of Netwar. This view has spread through the American defense establishment like, well, a virus. A 2011 Pentagon report on cyberspace stressed "the advantage currently enjoyed by the offense in cyberwarfare." The intelligence community stressed the same point in its annual threat report to Congress last year, arguing that offensive tactics -- known as vulnerability discovery and exploitation -- are evolving more rapidly than the federal government and industry can adapt their defensive best practices. The conclusion seemed obvious: Cyberattackers have the advantage over cyberdefenders, "with the trend likely getting worse over the next five years." A closer examination of the record, however, reveals three factors that put the offense at a disadvantage. First is the high cost of developing a cyberweapon, in terms of time, talent, and target intelligence needed. Stuxnet, experts speculate, took a superb team and a lot of time. Second, the potential for generic offensive weapons may be far smaller than assumed for the same reasons, and significant investments in highly specific attack programs may be deployable only against a very limited target set. Third, once developed, an offensive tool is likely to have a far shorter half-life than the defensive measures put in place against it. Even worse, a weapon may only be able to strike a single time; once the exploits of a specialized piece of malware are discovered, the most critical systems will likely be patched and fixed quickly. And a weapon, even a potent one, is not much of a weapon if an attack cannot be repeated. Any political threat relies on the credible threat to attack or to replicate a successful attack. If that were in doubt, the coercive power of a cyberattack would be drastically reduced.

Reject their ev - it's exaggerated and financially biased

Rid 13

Thomas Rid, Reader in War Studies at King's College London, His most recent book is Cyber War Will Not Take Place, also a non-resident fellow at the Center for Transatlantic Relations in the School for Advanced International Studies, Johns Hopkins University, PhD in political science from Humboldt University of Berlin, OC Register, March 15, 2013, "Thomas Rid: Hype, fear-mongering hurts cyberwar", http://www.ocregister.com/articles/systems-499977-cyber-control.html

LONDON – The White House likes a bit of threat. In his State of the Union address, Barack Obama wanted to nudge Congress yet again into passing meaningful legislation. The president emphasized that America's enemies are "seeking the ability to sabotage our power grid, our financial institutions and our air traffic control systems." After two failed attempts to pass a cybersecurity act in the past two years, he added swiftly: "We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."

Fair enough. A bit of threat to prompt needed action is one thing. Fear-mongering is something else: counterproductive. Yet too many a participant in the cybersecurity debate reckon that puffery pays off.

The Pentagon, no doubt, is the master of razzmatazz. Leon Panetta set the tone by warning again and again of an impending "cyber Pearl Harbor." Just before he left the Pentagon, the Defense Science Board delivered a remarkable report, "Resilient Military Systems and the Advanced Cyber Threat." The paper seemed obsessed with making yet more drastic historical comparisons: "The cyber threat is serious," the task force wrote, "with potential consequences similar to the nuclear threat of the Cold War." The manifestations of an all-out nuclear war would be different from cyberattack, the Pentagon scientists helpfully acknowledged. But then they added, gravely, that "in the end, the existential impact on the United States is the same."A reminder is in order: The world has yet to witness a single casualty, let alone fatality, as a result of a computer attack. Such statements are a plain insult to survivors of Hiroshima. After all, a bit of fear helps to claim – or keep – scarce resources when austerity and cutting seems out-of-control. The report recommended allocating the stout sum of $2.5 billion for its top two priorities alone, protecting nuclear weapons against cyberattacks and determining the mix of weapons necessary to punish all-out cyber-aggressors.

Then there are private computer security companies. Such firms, naturally, are keen to pocket some of the government's money earmarked for cybersecurity. And hype is the means to that end. Which leads to the next point: The media want to sell copy through threat inflation. "In Cyberspace, New Cold War," the headline writers at the Times intoned in late February. "The U.S. is not ready for a cyberwar," shrieked the Washington Post earlier this week. Instead of calling out the above-mentioned Pentagon report, the paper actually published two supportive articles on it and pointed out that a major offensive cyber capability now seemed essential "in a world awash in cyber-espionage, theft and disruption."

The Post should have reminded its readers that the only military-style cyberattack that has actually created physical damage – Stuxnet – was actually executed by the United States government.

Finally, the intelligence community tags along with the hype because the NSA and CIA are still traumatized by missing 9/11. Missing a "cyber 9/11" would be truly catastrophic for America's spies, so erring on the side of caution seems the rational choice.

This means that the quality of the public debate suffers, as experts as well as journalists have no choice but to rely on industry reports of sometimes questionable quality or anonymous informants whose veracity is hard to assess.

Accidental launch lands in the ocean

**Slocombe 9**

Frmr Under Secretary of Defense for Policy; Caplin & Drysdale Attorneys (Walter, De-Alerting: Diagnoses, Prescriptions, and Side-Effects, <http://www.ewi.info/system/files/Slocombe.pdf>,)

Moreover, in recent years, both the US and Russia, as well as Britain and China, have modified their procedures so that even if a nuclear-armed missile were launched, it would go not to a “real” target in another country but – at least in the US case - to empty ocean. In addition to the basic advantage of insuring against a nuclear detonation in a populated area, the fact that a missile launched in error would be on flight path that diverged from a plausible attacking trajectory should be detectable by either the US or the Russian warning systems, reducing the possibility of the accident being perceived as a deliberate attack. De-targeting, therefore, provides a significant protection against technical error. These arrangements – PALs and their equivalents coupled with continued observance of the agreement made in the mid-90s on “de-targeting” – do not eliminate the possibility of technical or operator-level failures, but they come very close to providing absolute assurance that such errors cannot lead to a nuclear explosion or be interpreted as the start of a deliberate nuclear attack.6 The advantage of such requirements for external information to activate weapons is of course that the weapons remain available for authorized use but not susceptible of appropriation or mistaken use. The drawback from a deterrence and operational point of view is, of course, that the system for transmitting the information must not be susceptible of interruption – that is, there must be assurance that an authorized decision maker will be able to act and have the decision – and the accompanying authenticated orders and unlock combinations – communicated to and received by the operators of the weapon systems. Accordingly, a system of combination-locked safeties requires a highly survivable network for decision and communication with the operators. Otherwise there would be pressures for early transmission of the codes, with their insertion subject to a later execute order or even more dangerous, pre-delegation of authority to issue the execute orders. In this, as in other aspects of measures to meet the “never” requirement, a highly capable and highly survivable command and control system is essential.

#### Cyberwar doesn’t go kinetic

Thomas Rid, Kings College London War Studies, Nov/Dec 2013, Cyberwar and Peace, Foreign Affairs, Ebsco

If cyberattacks reduce the amount of violence inherent in conflict, and if they often take the form of sabotage or espionage, then many officials and commentators who have been warning about the dawn of cyberwar have been ringing false alarms. Digital violence does have implications for ethics and for national security strategy, however. Weaponized code, or **cyberattacks** more generally, can **achieve goals that used to require conventional force**. The most sophisticated cyberattacks are highly targeted, and cyberweapons are unlikely to cause collateral damage in the same way conventional weapons do. **Therefore**, in many situations, the use **of computers would be ethically preferable to the use of conventional weapons: a cyberattack might be less violent**, less traumatizing, **and more limited**.

A comparable dynamic applies to the ethics of cyber-espionage. Intelligence might be gained by infiltrating computer systems and intercepting digital signals, or it might be acquired by sneaking human spies, sometimes armed, into hostile territory at personal risk, or it might be got by interrogating suspects under harsh conditions. Depending on the case, computer espionage might be ethically preferable to any of the other options.

A cyberattack will not always be the strategically sound option, however. Indeed, even the celebrated Stuxnet operation was not necessarily a strategic success. The attack was designed to slow and delay Iran's nuclear enrichment program and undermine the Iranian government's trust in its ability to develop a nuclear weapon. The attack might well have achieved those goals in the short term. But as soon as the malfunctions and delays were traced to sabotage, the psychological effect of the operation likely changed, as the Iranians could reassure themselves that they were not "stupid" and that they were faced with aggressive foreign adversaries. They now knew that the problem was not their own ineptitude; somebody else was doing this to them.

In an ongoing confrontation, such as the one over Iran's nuclear program, cyberattacks might yield valuable intelligence, but they likely possess very little coercive value. Consider that during the Cold War, the United States stationed hundreds of thousands of ground forces in West Germany and other areas bordering the Soviet bloc to communicate that Washington was alert and technically sophisticated, as well as serious about attacking if Moscow crossed a redline. A contemporary counterproliferation approach that relied on cyberattacks, by contrast, might send an altogether different message to the Iranians: that Washington is alert and technically sophisticated, but not really serious about attacking, even if Tehran does cross a redline. After all, a standalone **cyberattack would not** likely **put the lives of U.S. personnel in peril, a fact that could signal a lower level of commitment**.

### Adv 2

Unrestrained use deters cyber war – legal norms increase risk of conflict

Crosston 12 (Dr. Matthew Crosston is the Miller Endowed Chair for Industrial and International Security and founder and director of the International Security and Intelligence Studies (ISIS) program at Bellevue University. He has authored two books, several book chapters, and nearly a dozen peer-reviewed articles on counterterrorism, corruption, democratization, radical Islam, and cyber deterrence, “Virtual Patriots and a New American Cyber Strategy” Winter 2012, Strategic Studies Quarterly, p. 100-118)

These proposed behavioral rules about jus in cyber bello are paradoxical: with so many constraints on allowable action, the underlying motivational framework of fear—so essential in the original Cold War in moderating behavior—becomes nonexistent. Indeed, if the above parameters were ob served, then a state could arguably be more motivated to attack. Remove the civilian population and domestic infrastructure from cyber attack, and you have sanitized cyber war to a point where **there is no fear of engagement**.

A Cyber Cold War would be multilateral rather than bilateral: it would involve many nations, with different interests and not allied by treaty. Furthermore, the parties would include major non-governmental players such as private compa nies or even individuals or groups of individual hackers, perhaps with political interests. It is unlikely, in the more capitalistic and constitutionally free countries, which national governments can easily rein in these potential corporate and indi vidual cyber attackers. 20

The problem with this formulation is that it envisions a so-called cyber cold war beholden to apparently voluntary parameters of constraint. The parameters elaborated, however, do not honor but corrupt the true deterring force that existed in the Cold War. If an overt strategy of credible cyber debilitation were allowed to openly develop, then most of the problems mentioned above would be inconsequential to the proper functioning of the virtual global commons—multilateral or bilateral, individuals or groups, national governments or private corporations, clearly defined adversaries or anonymous, nonattributable attacks. A system that does not rely on arbitrary good behavior and instead proactively establishes overt cyber-weaponization strategies alongside continued covert capabili ties creates an environment where the futility of first-strike efficacy and perceived retaliatory devastation reigns in behavior globally.

The United States tends to be obsessive about keeping its technological capabilities classified. This is partially explained by the need to maintain effective surprise in retaliation to an attack rather than striving to prevent an attack initially. Yet, it is also explained by the US attempt to be the leading voice for liberally idealistic global cyber norms. This was confirmed in 2008 when former intelligence official Suzanne Spaulding testified before the House Cybersecurity Subcommittee.

My concern is that (the Department of Defense) has been so vocal about the development and deployment of [classified] cyber-warfare capabilities that it will be very difficult for that department to develop and sustain the trust necessary to undertake essential collaboration on defensive cybersecurity efforts with the private sector and with international stakeholders. . . . There is significant risk that these vital partners will suspect that the collaboration is really aimed at strengthening our offensive arsenal (emphasis added). 21

There are two problems with the above quote. On the one hand, policymakers continue to focus on apparent voluntary trust in a domain that is not typified by such behavior. On the other hand, the DoD remains stead fast in its worship of clandestine capability and thus loses the preemptive deterrence of overt strategy which can compel cooperation as opposed to just hoping for it. These are not small problems, as trust and collaboration between dangerous actors work when there is an element of consequence to poor action. An overt strategy of offensive cyber capability—revealing some cards while not revealing all, with no nod to ethical considerations that demand targeting constraints and a focus purely on the efficacy of preemptive deterrence—arguably has a chance to shine a light of consequence into the shadowy anarchy of cyber. This is how the United States, as men tioned at the beginning of this article, could be inspired by the essence of Chinese cyber strategy, but it must ultimately elevate to a higher capability and competence.

Further hindering this evolution, **the academic community has re mained too enamored with trying to connect ethical theories into the cyber domain to create a liberal, idealistic governing code.** Many scholars have acknowledged that these theories, whether utilitarianism, Kantian theory, or natural rights theory, have cast relatively little new light into the cyber domain. 22 Despite such sincere if misguided efforts, **the best possibility for preemptive cyber deterrence might be** old-school strategic realism **and not new-school ethical liberalism.**

As awkward as it may be to admit publicly, the Chinese might have something for the United States to truly consider. A fusion of Sun Tzu’s pragmatism with Machiavelli’s overt strategic amorality carries the potential to deter negative cyber action before it ever begins. As Sun Tzu as serted, the highest realization of warfare is to attack the enemy’s plans; next is to attack its alliances; next to attack the army; and the lowest is to attack its fortified cities. Machiavelli made it clear that if an injury has to be done to a man, it should be so severe that his vengeance need not be feared. This overt, amoral offensive fusion has one purpose: not to logistically conduct war but to strategically avoid it. At the present time there is no current discussion of US cyber strategy broaching these subjects, and subsequently, the zero-sum cyber game remains unchanged.

Cyber attack key to deter future Chinese cyber aggression

Schmitt 13 (Gary, co-directs the Marilyn War Center for Security Studies at the American Enterprise Institute, “How to meet the threat from China's army of cyber guerrillas” June 06, 2013, Fox News)

When President Obama meets woth Chinese President Xi Jinping Friday and Saturday in Southern California, a major topic of conversation between the two will be Chinese cyber-attacks and cyber-espionage against American commercial and government targets.

According to U.S. counterintelligence officials, billions upon billions of dollars worth of information has been “lifted” out of American computers and servers in recent years.

In fact, only last week, newspapers were reporting that an internal Defense Department review had concluded that China had used cyber attacks to gather data on more than three dozen key U.S. military programs, including the country’s most advanced missile defense systems, naval warships and even the F-35 Joint Strike Fighter—the stealthy, fifth-generation jet **that will be the backbone of the American military’s ability to sustain air superiority in the decades ahead.**

As one might expect, the Chinese government has denied any complicity in these attacks. And it is doubtful, given how successful Chinese efforts have been, that even “blunt” talk by the president to the new Chinese leader, will have much effect on Chinese practices.

The reality is, the Chinese government is engaged in a form of warfare—new to be sure in its technological aspects but not new in the sense that cyber attacks harm our relative military strength and damage the property (intellectual and proprietary) of citizens and companies alike.

So far, the American government’s response has largely been defensive, either talking to the Chinese about establishing new, agreed-upon “rules of road” for cyberspace or working assiduously to perfect new security walls to protect government and key private sector computer systems.

Although neither effort should be abandoned, they are no more likely to work than, say, before World War II, the Kellogg-Briand Pact could outlaw war and the Maginot Line could protect France from an invading Germany.

This last point is especially important. When it comes to cyberspace, according to Cyber Command head and director of the National Security Agency, General Keith Alexander, those on the offensive side of the computer screen–that is, those hacking into or compromising computer systems–have the advantage over those on the defensive side who are trying to keep systems secure. Walls have always been breached and codes broken.

Moreover, attempts to beef up security are complicated by the fact that our own cyber warriors are undoubtedly reluctant to provide those charged with protecting systems here at home with the latest in their own capabilities.

In addition to increasing the chance such information might leak by expanding the number of persons in the know, efforts to use that information to plug our own vulnerabilities can inadvertently alert a potential adversary on the very backdoors American would want to save for using in a future crisis or conflict.

All of which leads to the conclusion that to stem the tide of harmful cyber attacks by the Chinese (or, for that matter, Iran, Russia or North Korea), **there has to be a cyber response on America’s part that** deters continued cyber aggression**.**

Reprisals that are proportionate, in self-defense and designed to stop others from such behavior falls well within the bounds of international law as traditionally understood.

Nor is it the case that such reprisals should be limited to responding to government-on-government cyber attacks. The U.S. government has always understood that it has an affirmative duty to protect the lives and property of its citizens from foreign aggression and, in times both past and current, this has meant using American military might.

That need not be the case here, however. Indeed, one advantage of the cyber realm is the wide variety of options it offers up for reprisal that can inflict economic harm without causing loss of life or limb.

The good news is that the U.S. government has been gradually beefing up its offensive cyber capabilities.

Indeed, a little over a month ago in open testimony before the House Armed Services Committee, Gen. Alexander said that he created thirteen new teams that would go on the offensive if the nation were hit by a major cyber attack. And new reports coming out of the Pentagon indicate that the Joint Chiefs would like to empower geographic combatant commanders to counter cyber attacks with offensive cyber operations of their own.

These are necessary steps if we hope to create a deterrent to Chinese cyber aggression; however, they are not sufficient.

The threat posed by China’s army of cyber “guerrillas” is constant, is directed at both the U.S. government and the private sector, and ranges from the annoying to the deadly serious.

**A truly adequate response would require meeting the Chinese challenge on all these fronts**. And **no amount of summitry between the American and Chinese leaders** is likely to **substitute for the cold, hard fact that, when it comes to Chinese misbehavior,** upping the cost to Beijing is a necessary first step **to reclaiming the peaceful potential of the newest of the “great commons,” cyberspace.**

No modeling - strategic incentive to maintain legal ambiguity

Waxman 11

Matthew C. Waxman, Associate Professor, Columbia Law School; Adjunct Senior Fellow, Council on Foreign Relations; Member of the Hoover Institution Task Force on National Security and Law, Yale Journal of International Law, March 16, 2011, “Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," vol 36, http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1674565

B. Technology, Power Shifts, and the Strategic Logic of Legal Interpretation

With these relationships between law and power in mind, the United States has an interest in regulating cyber-attacks, but it will be difficult to achieve such regulation through international use-of-force law or through new international agreements to outlaw types of cyber-attacks.143 That is because the distribution of emerging cyber-capabilities and vulnerabilities— vulnerabilities defined not only by the defensive capacity to block actions but also by the ability to tolerate and withstand attacks—is unlikely to correspond to the status quo distribution of power built on traditional measures like military and economic might.

It is not surprising that the United States seems inclined toward an interpretation of Articles 2(4) and 51 that allows it to classify some offensive cyber-attacks as prohibited “force” or an “armed attack” but does not otherwise move previously drawn lines to encompass economic coercion or other means of subversion in that classification. Nor is it surprising to see the United States out in front of other states on this issue. The power and vulnerability distribution that accompanies reliance on networked information technology is not the same as past distributions of military and economic power, and perhaps not to the United States’s advantage relative to rivals. Moreover, some U.S. strengths are heavily built on digital interconnectedness and infrastructure that is global, mostly private, and rapidly changing; these strengths are therefore inextricably linked to new and emerging vulnerabilities.144

Although some experts assess that the United States is currently strong relative to others in terms of offensive capabilities,145 several factors make the United States especially vulnerable to cyber-attack, including the informational and electronic interconnectedness of its military and public and private sectors, and political obstacles to curing some of these vulnerabilities through regulation.146 As the Obama administration’s 2010 National Security Strategy acknowledged:

The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority . . . . Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale.147

In other words, U.S. technological strengths create corresponding exposures to threats. The U.S. government is especially constrained politically and legally in securing its information infrastructure—which is largely privately held or privately supplied—against cyber-threats, and these constraints shape its international strategy. Proposals to improve cyber-security through regulation include promulgating industry standards to enhance the security of information technology products and protect networks and computers from intrusion, and, more invasively, expanding the government’s authority to monitor information systems and communications.148 Such proposals invariably face powerful antiregulatory industry pressures and heightened civil liberties sensitivities.149 Information technology industry groups and privacy organizations have together pushed back against moves to impose government security mandates and against more intrusive government cyber-security activities, arguing that they would stifle innovation, erode civil liberties, and fail to keep up with rapidly evolving threats amid a globalized economy.150 A reluctance to secure information systems domestically through government regulation then elevates U.S. government reliance on other elements of a defensive strategy.

In that light, U.S. legal interpretations and declaratory postures that define prohibited force in ways that extend narrow Charter interpretations to take account of cyber-warfare may be seen as part of an effort to sustain a legal order in which anticipated U.S. military and economic moves and countermoves against potential adversaries fit quite comfortably—that is, a legal order that preserves U.S. comparative advantages. In extending the foundational U.N. Charter prohibition on force to cyber-attacks by emphasizing their comparable effects to conventional military attacks, such interpretations help deny that arsenal to others by raising the costs of its use. At the same time, by casting that prohibition and complementary self-defense authority in terms that help justify military force in response, this interpretation reduces the costs to the United States of using or threatening to use its vast military edge (and it helps signal a willingness to do so).

Put another way, the United States appears to be placing hedged bets about what the future strategic environment will look like and how best to position itself to operate and compete in it. On balance, for example, the United States may prefer relatively clear standards with respect to cyber-actions that have immediate destructive effects—at least clear enough to justify armed response or deterrence to activities or scenarios deemed threatening—while at the same time preferring some permissive haziness with respect to intelligence collection and its own countermeasures in cyberspace. Such a posture allows the United States to protect itself from hostile penetrations while also preserving some latitude for those activities in which it may be relatively strong.151 Internally, that clarity facilitates planning for contingencies and deliberation about options;152 externally, it may help articulate and deter the crossing of red lines.153

In trying to explain what may be driving the U.S. interpretation, this Article is neither affirming nor denying this strategic logic, which is contingent on future capabilities and vulnerabilities that are both highly uncertain and shrouded in secrecy. Rather, it is trying to uncover and scrutinize some of the underlying assumptions.

There are several strategic reasons for the United States to be cautious in considering interpretations that expand narrow definitions of “force” and “attack” so that they include potentially broad categories of cyber-attacks— risks that are often not acknowledged or addressed in discussions of the U.S. interpretive trajectory. For one thing, the United States has generally defeated efforts by other states to interpret Articles 2(4) and 51 expansively to include economic coercion and other forms of political subversion.154 In thinking about the Charter regime as a whole, therefore, the United States may not want to reopen those debates. Cyber-attacks can allow state and nonstate actors to inflict massive harm without resort to arms, but that has long been true of many other instruments, including economic and financial means, covert subterfuge, and other widely used instruments. In that regard, one advantage of promoting legal regulation of cyber-attacks through a new treaty or international agreement instead of through Charter interpretation is that such efforts would have little if any effect on broader Charter law. An advantage, however, to working through Charter interpretation rather than new agreements is that Charter law can evolve incrementally and begin shaping international actors’ expectations through unilaterally initiated state practice without having to reach consensus (the difficulties of which are discussed in the next Section).

Depending on the relative risk of different types of future cyber-attack scenarios, it might also be in the United States’s strategic interest to legally delink cyber-activities from armed force instead of defining force by reference to effects, or at least to impose extremely high legal thresholds for treating cyberattacks equivalent to force or armed attack, in order to reduce the chances of military escalation from cyber-activities.155 As capabilities proliferate among state and nonstate actors to conduct various sorts of malicious, hostile, or intelligence-gathering activities in cyberspace, any normative constraints that come from treating some cyber-attacks as force prohibited by Article 2(4) and any deterrence value of treating them as armed attacks triggering self-defense rights under Article 51 might be outweighed by the dangers of lowering legal barriers to military force in a wider range of circumstances.156 That is, the value of promoting a right of armed self-defense against cyber-attacks may turn out to be quite low—since, among other things, it may be difficult to sufficiently prove one’s case publicly in justifying military responses—while doing so may introduce greater security instability to the international system by eroding normative constraints on military responses to nonmilitary harms.157

As the following Section explores, it is very difficult to assess these risk balances because the global security environment is shifting dramatically and unpredictably. Moreover, even if the United States could assess the risks accurately, other states may be operating under different sets of strategic assumptions about that future.

C. Divergent Interests and Implications for Charter Interpretation

Assuming the United States decides firmly on a legal interpretation going forward, the redrawing of legal lines on a map of inequitably distributed power and vulnerabilities would create winners and losers and would make it difficult to reach agreement on new legal boundaries, whether through interpretive evolution of the U.N. Charter or new conventions.158 In thinking about legal interpretations of Articles 2(4) and 51, success therefore depends on the ability of proponents to articulate and defend their legal lines using combinations of traditional and new forms of power for deterrence, self-defense, enforcement, and influence.

Again, one should not divorce analysis of any proposed content of Articles 2(4) and 51 from the processes by which it is interpreted, reinterpreted, enforced, and reinforced.159 The likely factual ambiguity surrounding cyberattacks and the pressures to take aggressive responsive or escalatory measures more quickly than those facts can be resolved may sometimes require strategic and military decisionmaking amid legal gray zones. Moreover, as involved states marshal their arguments amid these moves and countermoves, and as they consider their long-term interests, they may also calculate differently what Stone calls “the expected value . . . of built-in [legal] ambiguities as future political weapons.”160

That is, even if states widely share a common, minimum interest in restricting some cyber-attacks, states may have divergent interests regarding specific substantive content as well as the desired degree of clarity in the law. Salient differences will likely stem from asymmetries of geostrategic ambitions, internal and external commitment to legal norms generally, and the nature and extent of public-private institutional relationships.161

In contrast to the United States, some states that are developing offensive cyber-warfare capabilities (such as North Korea, according to many experts) are non-status-quo powers or aspiring regional powers,162 and they may prefer legal ambiguity as to cyber-attacks or narrow interpretations of Article 51 that would allow them—if they resort to cyber-attacks—to portray themselves as victims of any responsive military strikes.163 Offensive cyber-capabilities have the potential to shift or upset international balances of power, because some states are more vulnerable than others to cyber-attack (in terms of capacity to block actions as well as to tolerate or withstand them), and attacks could have a disproportionately large impact on countries or militaries that have a higher reliance on networked information systems.164 Developing an offensive cyberwarfare capability is likely to be less expensive in resources and diplomatic costs than competing economically or militarily with much stronger states, though legal flexibility or constraints could alter that calculus.165 On the other hand, some small states that are unlikely to develop sophisticated offensive or defensive systems may advocate international legal interpretations or new agreements that are very restrictive of cyber-attacks and define attacks broadly, seeing themselves as highly reliant on protective norms.166 Individually, though, they will have little power to promote those principles.

Like the United States, other major actors may have much to lose from cyber-attacks. However, they may calculate their short- and long-term strategic interests with respect to cyber-warfare and its regulation differently than the United States, in light of their own matrix of offensive and defensive capabilities, public-private institutional relationships, and asymmetries in the ways international law constrains different actors.167 Russia, for example, has proposed to the United Nations a draft statement of principles that would prohibit the development, creation, and use of cyber-attack tools. Meanwhile, though, Russia is engaged in developing cyber-attack capabilities,168 and some analysts are skeptical of Russia’s sincerity in proposing cyber-arms control agreements, especially given the difficulties of verifying them.169 China likely sees cyber-warfare capabilities as a way of equalizing the conventional military superiority of the United States,170 so it may be reluctant to concede legally “disarming” interpretations, at least without some reciprocal benefit or legal concession. Russia and China, which, as mentioned earlier, both reportedly exploit informal relationships with private actors (i.e., “citizen hackers”) to conduct attacks and collect intelligence in cyberspace, may also incline toward legal doctrine that makes it difficult to impute private cyber-actions to governments.171 Meanwhile, some European states have approached the legal relationship between cyber-attacks and force cautiously, perhaps because of general concerns about military escalation of crises and divergent strategic assessments among themselves.172

Differences in internal politics, ideology, and government control over information will also shape state interests in competing interpretations of Charter norms. With echoes of debates from prior eras,173 various types of states are likely to view cyber-threats differently and to distinguish offensive attacks from defensive measures differently. For instance, some states that tightly control information, including major powers like China, are especially concerned about internal political dissent and might therefore define what the United States sees as “Internet freedom” as a threat to vital security interests. Efforts to crack down on what they (or other states that exercise strong state control over Internet content) may view as defensive measures against hostile subversion may be viewed by the United States (or other states that value and promote free speech) as hostile, offensive measures.174 It is hard to envision a state in China’s position strongly endorsing or standing behind U.S. visions for international legal regulation of cyber-attacks without some unlikely concessions by the United States.175

From a policy standpoint, this should sound another cautionary note about efforts to build international legal consensus about cyber-attacks and the use of force, whether through Charter interpretation or new agreements. Emergent U.S. government inclinations toward effects-based interpretations of the Charter may be legally reasonable and protective of some core U.S. interests, as well as widely shared foreign interests. But even if they help in the short term to manage competing risks of too much or too little authority to employ cyberattacks, or too much or too little leeway to resort to armed self-defense in response, a coherent legal strategy can only be forged and advanced in the long term if it is integrated effectively with broader diplomacy and security strategy, including efforts to build and sustain offensive, defensive, deterrent, and intelligence capabilities—while others do the same based on a different set of objectives, capabilities, vulnerabilities, and constraints.

Stuxnet kills credibility of any US cyber-restraint norm—try or die for deterrence through offensive cyber capabilities

Tim Stevens, associate of the Centre for Science and Security Studies at King’s College, London, 2012, A Cyberwar of Ideas? Deterrence and Norms in Cyberspace, Contemporary Security Policy 33. 1

Even as states attempt to regulate the use of cyberspace for, inter alia, military first strikes, they will retain significant military and intelligence cyber capabilities to be exercised below the level of an as-yet unascertained cyber conflict threshold. The latter may require legal definition at the global level, or it may yet fall to unilateral declarations of tolerance, or displays of force posture or operational capacity, most likely in conjunction with strategic allies. It may be that the norm that emerges from this situation is not of non-use but of ‘acceptable’ use, which serves to demonstrate where the ‘red lines’ of cyber operations are. **It is unlikely, therefore, that a ‘cyber taboo’ analogous to nuclear and chemical weapons taboos will be constructed**.129 In the absence of any firm notion of what, for example, a ‘cyberwar’ might actually look like, there may be little immediate societal pressure to avoid one, and plenty of latitude afforded to states to develop capabilities that might conceivably be used in one, if such a thing even exists.130 Nevertheless, as Nina Tannenwald argues with respect to the nuclear taboo, a norm of non-use may stand a greater chance of being adopted by alliances of democracies than by authoritarian states.131 However, given the possible US-Israeli involvement in the Stuxnet sabotage of Iranian nuclear technology, we must wonder if we are already past this point.132 The lure of a voluntary framework banning the offensive use of cyberspace may prove irresistible to many ‘like-minded nations’, even if its actual applicability is strictly limited. Importantly, an international **normative regime not backed with** coordinated and **credible force will serve** no deterrent function against exactly those ‘rogue’ and non-state actors most likely to conduct disruptive cyber operations.

Yet the question remains: how effective is a norms-based approach to cyber deterrence likely to be? How can we tell what aspects of a deterrence strategy are working, or which aren't? In truth, it is much too early to know. Even if it were possible to get all parties to comply with a set of norms hammered out through diplomacy and other forms of negotiation, what guarantees are there that these would be adhered to? Again, **there are no** such **guarantees**. It may be that states can be persuaded to comply with international normative frameworks through a mix of inducement, coercion and moral pressure. So too might industry and civil society be persuaded to do their part through a gradual process of cultural learning, and all parties work together to achieve the ‘global culture of cybersecurity’ currently aspired to. Even were these norms to operate strongly and bind together these actors such that norms of non-use or acceptable use became institutionalized, **they are never likely to persuade all who might have the capabilities to prosecute actions in cyberspace that constitute strategic threats**. For this reason alone, states and their militaries and security services will, even whilst pursuing denial strategies and improving defensive cybersecurity, be loath to abandon the search for effective punitive measures through which deterrence might be achieved. In turn, the norm of retaliatory punishment may prove to be a powerful deterrent in itself.

#### No Chinese attack on Taiwan

Bush, 10

[Richard C Bush III, Director, Center for Northeast Asian Policy Studies at the Brookings Institution, “China-Taiwan: Recent Economic, Political, and Military Developments Across the Strait, and Implications for the United States,” 3/18/10, Brookings, http://www.brookings.edu/testimony/2010/0318\_china\_economy\_bush.aspx]

What is the trajectory of the current process? Conceptually, there are at least two possibilities. On the one hand, and more consequential, what we are watching might reflect movement toward the resolution of the fundamental dispute between the two sides. One type of resolution would be unification according to the PRC’s one-county, two-systems formula, but there are others. On the other hand, what we are seeing could be the stabilization of cross-Strait relations. That term implies several things: increasing two-way contact, reducing mutual fear, increasing mutual trust and predictability, expanding areas of cooperation, institutionalizing interaction, and so on. It constitutes a shift from the conflicted coexistence of the 1995-2008 period to a more relaxed coexistence. Examples of this process at work are the array of economic agreements that the two sides have concluded, removing obstacles to closer interchange; China’s approval for Taiwan to attend the 2009 meeting of the World Health Assembly; and the two sides’ tacit agreement that neither will steal the other’s diplomatic partners.

In and of itself, stabilization does not lead ineluctably to a resolution of the China-Taiwan dispute—however much Beijing prefers inevitability and however much some in Taiwan fear it. President Ma has been quite explicit that unification will not be discussed during his term of office, whether that is four or eight years. The Chinese leadership at least realizes that the current situation is better than the previous one and understands that resolution will be a long-term process.

Certainly, however, stabilization can create a better climate for resolution. It’s easier to address the tough conceptual issues that are at the heart of this dispute in an environment of greater mutual trust. But I don’t see that happening anytime soon. Stabilization can also evolve very incrementally toward resolution, either through better mutual understanding or because one side, knowingly or unknowingly, makes concessions to the other. How stabilization might migrate to resolution brings me to the Commission’s questions.

China’s Initiatives

Since 2005, and in contrast to past periods, China’s approach to Taiwan has been rather skillful. President Hu Jintao shifted the priority from achieving unification in the near or medium term to opposing Taiwan independence (unification remains the long-term goal). Although he speaks about the need for the two sides to “scrupulously abide by the one-China principle,” he has been prepared, for the sake of achieving substantive progress, to tolerate so far the Ma administration’s quite ambiguous approach to that issue. The Beijing leadership recognizes the importance of building mutual trust through dialogue and exchanges after a decade-plus of mutual fear. It is emphasizing what the two sides have in common—economic cooperation and Chinese culture—and agreed to reduce somewhat the zero-sum competition in the international arena. Through its policies and interactions, it is trying to build up support for a PRC-friendly public on Taiwan. It sees the value of institutionalizing a more stable cross-Strait relationship.

The exception to this trend is the continuation of the People’s Liberation Army’s acquisition of capabilities that are relevant to a Taiwan contingency. Why this build-up continues, in spite of the decline in tensions since President Ma took office, is puzzling. After all, Ma’s policies reduce significantly what Beijing regarded as a serious national security problem. China is more secure today than two years ago, yet it continues to make Taiwan more vulnerable. Possible explanations are rigid procurement schedules; the inability of civilian leaders to impose a change even when it makes policy sense; and a decision to fill out its capacity to coerce and intimidate Taiwan, in case a future Taiwan government challenges China’s fundamental interests. The answer is not clear. I am inclined to believe that it is a combination of the second and third reasons.

What is clear is that this trend is in no one's interests – Taiwan's, China's or the United States'. Taiwan's leaders are unlikely to negotiate seriously on the issues on Beijing's agenda under a darkening cloud of possible coercion and intimidation. The Taiwanese people will not continue to support pro-engagement leaders if they conclude that this policy has made Taiwan less secure. The U.S. will not benefit if mutual fear again pervades the Taiwan Strait.

Where do Current Trends Lead?

To be honest, I do not know. I cannot rule out the possibility that gradually and over time the Taiwan public and political leaders will abandon decades of opposition to one-country, two systems and choose to let Taiwan become a special administrative region of the PRC. But I doubt it. Despite the consciousness on the island of China’s growing power and leverage, there is still a broad consensus that the Republic of China (or Taiwan) is a sovereign state, a position that is inconsistent with China’s formula. Moreover, because of the provisions of the ROC constitution, fundamental change of the sort that Beijing wants would require constitutional amendments and therefore a broad and strong political consensus, which does not exist at this time.

So if political integration is to occur in the next couple of decades, it will occur not because of the cumulative impact of economic integration but because Beijing has decided to make Taiwan an offer that is better than one-country, two systems. So far, I see no sign it will do so.

The more likely future is the continued creation and consolidation of a stabilized order, one in which economic interdependence deepens, social and cultural interaction grows, competition in the international community is muted, and all these arrangements will be institutionalized to one degree or another. But none of this will be automatic. Issues relevant to the resolution of the dispute (e.g. whether Taiwan is a sovereign entity) may come up in the process of stabilization and dealt with in ways that do not hurt either side’s interests And the issue of China’s growing military power—and what it reflects about PLA intentions—remains.

## 2NC

### DA

### 2nc ov—ops

India-Pakistan—

**GSN 10** (Global Security Newswire, “Regional Nuclear War Could Devastate World Population, Report Warns,” <http://www.globalsecuritynewswire.org/gsn/nw_20100315_4193.php>)

Computer modeling suggests a nuclear exchange between India and Pakistan would **block out the sun with large amounts of airborne debris, disrupting global agriculture and leading to the starvation of around 1 billion people**, *Scientific American* reported in its January issue (see *GSN*, March 4). The nuclear winter scenario assumes that cities and industrial zones in each nation would be hit by 50 bombs the size of the atomic bomb dropped on Hiroshima, Japan, in World War II. Although some analysts have suggested a nuclear exchange would involve fewer weapons, researchers who created the computer models contended that **the panic from an initial nuclear exchange could cause a conflict to quickly escalate**. Pakistan, especially, might attempt to fire all of its nuclear weapons in case India's conventional forces overtake the country's military sites, according to Peter Lavoy, an analyst with the Naval Postgraduate School. The nuclear blasts and subsequent blazes and radiation could kill more than 20 million people in India and Pakistan, according to the article. Assuming that each of the 100 bombs would burn an area equivalent to that seen at Hiroshima, U.S. researchers determined that the weapons used against Pakistan would generate 3 million metric tons of smoke and the bombs dropped on India would produce 4 million metric tons of smoke. Winds would blow the material around the world, **covering the atmosphere over all continents within two weeks.** The reduction in sunlight would cause temperatures to drop by 2.3 degrees Fahrenheit for several years and precipitation to drop by one-tenth. The climate changes and other environmental effects of the nuclear war would have a **devastating affect on crop yields** unless farmers prepared for such an occurrence in advance. The observed effects of volcano eruptions, smoke from forest fires and other events support the findings of the computer modeling, the researchers said. "A nuclear war could trigger declines in yield nearly everywhere at once, and a worldwide panic could bring the global agricultural trading system to a halt, with severe shortages in many places. Around 1 billion people worldwide who now live on marginal food supplies would be directly threatened with starvation by a nuclear war between India and Pakistan or between other regional nuclear powers," wrote Alan Robock, a climatology professor at Rutgers University in New Jersey, and Owen Brian Toon, head of the Atmospheric and Oceanic Sciences Department at the University of Colorado at Boulder.

Asia—

**Campbell et al 8**

(Kurt M, Assistant Secretary of State for East Asian and Pacific Affairs, Dr. Campbell served in several capacities in government, including as Deputy Assistant Secretary of Defense for Asia and the Pacific, Director on theNational Security Council Staff, previously the Chief Executive Officer and co-founder of the Center for a New American Security (CNAS), served as Director of the Aspen Strategy Group and the Chairman of the Editorial Board of the Washington Quarterly, and was the founder and Principal of StratAsia, a strategic advisory company focused on Asia, rior to co-founding CNAS, he served as Senior Vice President, Director of the International Security Program, and the Henry A. Kissinger Chair in National Security Policy at the Center for Strategic and International Studies, doctorate in International Relation Theory from Oxford, former associate professor of public policy and international relations at the John F. Kennedy School of Government and Assistant Director of the Center for Science and International Affairs at Harvard University, member of Council on Foreign Relations and  International Institute for Strategic Studies, “The Power of Balance: America in iAsia” June 2008, <http://www.cnas.org/files/documents/publications/CampbellPatelSingh_iAsia_June08.pdf>)

Asian *investment* is also at record levels. Asian countries lead the world with unprecedented infra­structure projects. With over $3 trillion in foreign currency reserves, Asian nations and businesses are starting to shape global economic activity. Indian firms are purchasing industrial giants such as Arcelor Steel, as well as iconic brands of its once-colonial ruler, such as Jaguar and Range Rover. China’s Lenovo bought IBM’s personal computer We call the transformations across the Asia-Pacific the emergence of “iAsia” to reflect the adoption by countries across Asia of fundamentally new stra­tegic approaches to their neighbors and the world. Asian nations are pursuing their interests with real power in a period of both tremendous potential and great uncertainty. iAsia is: *Integrating:* iAsia includes increasing economic interdependence and a flowering of multinational forums to deal with trade, cultural exchange, and, to some degree, security. *Innovating:* iAsia boasts the world’s most successful manufacturing and technology sectors and could start taking the lead in everything from finance to nanotech to green tech. *Investing:* Asian nations are developing infrastruc­ture and human capital at unprecedented rates. But the continent remains plagued by: Insecurity: Great-power rivalry is alive in Asia. Massive military investments along with historic suspicions and contemporary territorial and other conflicts make war in Asia plausible. Instability: From environmental degradation to violent extremism to trafficking in drugs, people, and weapons, Asian nations have much to worry about. *Inequality:* Within nations and between them, inequality in Asia is more stark than anywhere else in the world. Impoverished minorities in countries like India and China, and the gap in governance and capacity within countries, whether as back­ward as Burma or as advanced as Singapore, present unique challenges. A traditional approach to Asia will not suffice if the United States is to both protect American interests and help iAsia realize its potential and avoid pitfalls. business and the Chinese government, along with other Asian financial players, injected billions in capital to help steady U.S. investment banks such as Merrill Lynch as the American subprime mortgage collapse unfolded. Chinese investment funds regional industrialization, which in turn creates new markets for global products. Asia now accounts for over 40 percent of global consumption of steel 4 and China is consuming almost half of world’s available concrete. 5 Natural resources from soy to copper to oil are being used by China and India at astonishing rates, driving up commodity prices and setting off alarm bells in Washington and other Western capitals. Yet Asia is not a theater at peace. On average, between 15 and 50 people die every day from causes tied to conflict, and suspicions rooted in rivalry and nationalism run deep. The continent harbors every traditional and non-traditional challenge of our age: it is a cauldron of religious and ethnic tension; a source of terror and extrem­ism; an accelerating driver of the insatiable global appetite for energy; the place where the most people will suffer the adverse effects of global climate change; the primary source of nuclear proliferation; and the most likely theater on Earth for a major conventional confrontation and even a nuclear conflict. Coexisting with the optimism of iAsia are the ingredients for internal strife, non-traditional threats like terrorism, and traditional interstate conflict, which are all magnified by the risk of miscalculation or poor decision-making.

### Uniqueness

#### CMR strong now

Andrew Exum, CNAS Senior Fellow, 7/4/12, No Crisis in Wartime U.S. Civil-Military Relations, EBSCO

Last week, I noted one of the ironies of the U.S. effort in Afghanistan since 2009: From the perspective of civil-military relations, the process worked. Regardless of one's opinion of the Obama administration's strategy in Afghanistan and despite the high degree to which the U.S. government and its allies have struggled to implement that strategy, the division of labor between civilian officials and military officers in formulating the strategy itself functioned more or less according to design.

In light of the reaction the column generated, I'd like to examine civil-military relations in the United States more broadly. Today, I will discuss some of the literature that informs our thinking on civil-military relations, and next week, I will offer my thoughts on the state of civil-military relations in the United States today and offer policy recommendations to improve them.

I should say from the start that I do not believe there to be any "crisis" in civil-military relations in the United States. Several wise scholars -most notably Andrew Bacevich and Richard Kohn -have argued there is such a crisis. And I share many of the concerns both of them raise, from the fetishization of military service to the active involvement of retired general officers in political campaigns.

But either because I am writing from France -which does have a history of toxic and even mutinous civil-military relations in its recent democratic past -or because I remember historical accounts of the days when Douglas MacArthur used his military staff to plot his political career, **I consider contemporary civil-military relations in the U**nited **S**tates **to be quite healthy**.

In addressing the issue, I will consider civil-military relations only as they pertain to the prosecution of war itself. I am less concerned by civil-military relations in peacetime, though for many of the reasons Bacevich and Kohn raise, this subject is also worth considering.

The canonical text on civil-military relations in the United States remains Samuel Huntington's "The Soldier and the State" (1957). If we start with the belief that war takes place on four levels -the political, the strategic, the operational and the tactical -Huntington's model reserves the role of defining the political ends of a war for elected civilian leaders, while assigning the operational and tactical levels of war to the professional military officers. As for the strategic aims of a conflict as well as the resources the nation will devote to its prosecution, civilians and military officers decide on them together in Huntington's model.

It is not clear whether or not Huntington entirely intended for his scholarly work to be normative. Regardless, successive generations of U.S. military officers have been raised in the belief that Huntington's model is the way in which the division of labor in war is supposed to be organized. Military officers thus resent it when civilian officials stick their noses into tactical and operational affairs.

As Eliot Cohen ably demonstrates in "Supreme Command" (2002), however, civilians do sometimes stick their noses into the tactical and operational affairs of the military -and often to positive effect. Choosing historical examples ranging from Abraham Lincoln to David Ben-Gurion, Cohen demonstrates why it is sometimes necessary for politicians to get their hands dirty running a war. After all, war is fundamentally a political affair -and it really is sometimes too important to be left to the generals. A statesman who ignores military affairs can be as much of a menace as a statesman who fancies himself a better tactician than his generals.

U.S. military officers, as a whole, dislike Cohen's arguments for reasons that should be obvious to all. These officers reflexively resent what they see as "interference" in their affairs. What those officers perhaps miss is that among Cohen's intended audience was a certain former governor of Texas who Cohen feared was not as interested in military affairs as he needed to be having become president. Indeed, George W. Bush learned the hard way -and at the cost of much U.S. blood and treasure -that even though the U.S. military will insist as an institution that its general officers are equally able, that is not always the case. Some officers are better than others, and one of the more important decisions a president can make is in his selection of commander.

To the chagrin of military officers, then, the division of labor between civilian officials and military officers in wartime is not fixed. Civilians have long reserved the right to interfere in military affairs. Lincoln and Ben-Gurion did this to positive effect. Adolf Hitler, among others, did so in such a way that his meddling hamstrung his generals.

What is rigidly fixed in the U.S. system of government, however, is civilian supremacy over the military. Article I of the U.S. Constitution gives the U.S. Congress the sole right to declare war, while Article II establishes the president as the commander-in-chief. Remarkably, the civilian leadership of the United States has never faced a serious threat by the military to usurp powers reserved for civilian authorities. Only MacArthur mounted a serious challenge -a series of challenges, really -to civilian authorities, and even he was eventually put in his place.

Those who fear that civil-military relations in the United States are in crisis -and these fears reached an apex in 2009 -lack both comparative and historical perspective. The 82nd Airborne Division might not have done the best job in Iraq's al-Anbar province in 2003, but unlike its French counterparts, it has never threatened to jump onto the Washington mall and overthrow the government. And despite the fears of many pundits in 2009 that high-profile general officers such as David Petraeus and Stanley McChrystal harbored secret ambitions to undermine a young Democratic president, both men now happily and humbly serve as civilians in that same president's administration.

#### Hagel revived CMR—but military backlash to the plan would sour CMR

James Carafano, Vice president of Foreign and Defense policy studies at The Heritage Foundation, 3/6/13, Uncivil Military Relations, nationalinterest.org/commentary/uncivil-military-relations-8186

So while Hagel has settled in at the Pentagon, **he cannot sit easy**. He is a marked man. His critics will be looking for the first misstep to call for his head. The new secretary also faces a new problem—a possible half-trillion dollars in defense cuts on top of the approximately half-trillion dollars in cuts he inherited. Hagel may be efficient, smart and prudent in making the Pentagon’s ends meet. But he will still have to run a Walmart-size company on a 7 Eleven-size budget in a world that is not much safer than it was four years ago.

Still, neither budgets nor headhunters may prove to be Hagel’s biggest headache. He should be most worried about the dark shadow of sour civil-military relations.

The best take on American civil-military relations remains the introduction to Eliot Cohen’s masterful book, Supreme Command. Cohen makes the point that the realms of political and military decision-making are not distinctly separate spheres. Rather, they do and should overlap. **Generals** should make decisions that win battles. They **shouldn’t meddle in politics**, but their military advice always ought to be suitable, feasible and acceptable. During World War II, for example, the U.S. Army estimated that about 10 percent of the nation’s manpower could be put in uniform without creating a worker shortage that would undermine the capacity of industry to sustain the armed forces. It would have made no sense for the military to ask for a bigger force than the nation could sensibly field.

### Middle East

#### The Mid East models US CMR

William Perry, Former Secretary of State, 5/23/1996, Fulfilling the Role of Preventive Defense, http://www.defense.gov/speeches/speech.aspx?speechid=974

America has long understood that the spread of democracy to more nations is good for America's national security. It has been heartening this past decade to see so many nations around the world come to agree with us that democracy is the best system of government. But as the nations of the world attempt to act on this consensus, we are seeing that there are important steps between a worldwide consensus and a worldwide reality. Democracy is learned behavior. Many nations today have democracies that exist on paper, but in fact are extremely fragile. Elections are a necessary but insufficient condition for a free society. It is also necessary to embed democratic values in the key institutions of nations.

The Defense Department has a key role to play in this effort. **It is a simple fact that virtually every country in the world has a military. In virtually every new democracy** -- in Russia, in the newly free nations of the former Soviet Union, in Central and Eastern Europe, in South America, in the "Asian Tigers" -- **the military represents a major force**. In many cases, it is the most cohesive institution. It often contains a large percentage of the educated elite and controls key resources. In short, it is an institution that can help support democracy or subvert it.

We must recognize that each society moving from totalitarianism to democracy will be tested at some point by a crisis. It could be an economic crisis, a backslide on human fights and freedoms, or a border or ethnic dispute with a neighboring country. When such a crisis occurs, we want the military to play a positive role in resolving the crisis, not a negative role by fanning the flames of the crisis -- or even using the crisis as a pretext for a military coup.

In these new democracies, we can choose to ignore this important institution or we can try to exert a positive influence. We do have the ability to influence; indeed, every military in the world looks to the U.S. armed forces as the model to be emulated. That is a valuable bit of leverage that we can put to use creatively in our preventive defense strategy.

#### Key to stability

Alan Richards, California University Santa Cruz Economics and Environmental Studies Professor, 2004, The Future Security Environment in the Middle East, http://www.rand.org/pubs/monograph\_reports/MR1640/MR1640.pdf

Military establishments are among the most—if not the most— important domestic constituencies in the states of the Middle East. Despite periodic experiments with political and economic liberaliza-tion, the region’s Arab states in particular remain solidly nondemocratic.1 Political leaders rely ultimately on coercive power to maintain their positions and depend upon their armed forces to defend against challengers and opponents. For this reason, military organi- zations are constituencies no authoritarian leader can afford to ignore. In fact, political leaders have proven quite successful in man- aging relations with their armed forces. Throughout the Middle East, leaders have attained and retained political control over their militaries, even as they continue to depend on their officers’ loyalty to maintain office. Analyzing the bases of this political control provides crucial insight into the internal logic of the region’s authoritarian regimes. Civil-military relations are essential for evaluating the past and future stability of the key U.S. adversaries and allies in the region.

Assessing civil-military relations is also significant for regional relations and broader U.S. security interests. Civil-military relations often compromise their military effectiveness and consequently the capacity of allies and adversaries in the region to project conventional military power. Military establishments play a dual role in the authoritarian regimes of the Middle East. They act as defenders of state and sovereignty against external adversaries. Yet they also defend the regime from internal opponents and challengers. This dual mandate creates particular pressures for leaders. They must ensure the support and quiescence of military leaders, which as final guar- antors of the regime are imbued with substantial political influence, while arming themselves against external threats in the region. In fact, the dual mandate of these militaries contains an inherent con- tradiction: Maintaining political control often compromises the po- tential effectiveness of military forces in conventional war. Rarely have authoritarian leaders proved capable of securing both their regimes and their states, a fact underscored by the pervasive ineffectiveness of their armed forces in the region’s many wars.

Nuclear war

James A. **Russell,** Senior Lecturer, National Security Affairs, Naval Postgraduate School, ‘9 (Spring) “Strategic Stability Reconsidered: Prospects for Escalation and Nuclear War in the Middle East” IFRI, Proliferation Papers, #26, http://www.ifri.org/downloads/PP26\_Russell\_2009.pdf

Strategic stability in the region is thus undermined by various factors: (1) asymmetric interests in the bargaining framework that can introduce unpredictable behavior from actors; (2) the presence of non-state actors that introduce unpredictability into relationships between the antagonists; (3) incompatible assumptions about the structure of the deterrent relationship that makes the bargaining framework strategically unstable; (4) perceptions by Israel and the United States that its window of opportunity for military action is closing, which could prompt a preventive attack; (5) the prospect that Iran’s response to pre-emptive attacks could involve unconventional weapons, which could prompt escalation by Israel and/or the United States; (6) the lack of a communications framework to build trust and cooperation among framework participants. These systemic weaknesses in the coercive bargaining framework all suggest that escalation by any the parties could happen either on purpose or as a result of miscalculation or the pressures of wartime circumstance. Given these factors, it is disturbingly easy to imagine scenarios under which a conflict could quickly escalate in which the regional antagonists would consider the use of chemical, biological, or nuclear weapons. It would be a mistake to believe the nuclear taboo can somehow magically keep nuclear weapons from being used in the context of an unstable strategic framework. Systemic asymmetries between actors in fact suggest a certain increase in the probability of war – a war in which escalation could happen quickly and from a variety of participants. Once such a war starts, events would likely develop a momentum all their own and decision-making would consequently be shaped in unpredictable ways. The international community must take this possibility seriously, and muster every tool at its disposal to prevent such an outcome, which would be an unprecedented disaster for the peoples of the region, with substantial risk for the entire world.

### CP

### Solvency—1

We solve preemption---ppl know when we use them

#### Need clarity about attacks

Walker 8/2/13 (Richard, Pen Name for New York News Producer, American free Press, “OBAMA EXPANDS WAR POWERS; CAN UNLEASH CYBERWAR ANY TIME <http://americanfreepress.net/?p=11966#sthash.GqeI03l8.dpuf>)

The very moment United States President Barack Obama authorized the “dropping” of an electronic bomb on Iran’s nuclear industry he crossed a line into a new kind of warfare that could have global consequences today and far into the future. The weapon used against Iran was built with the cooperation of Israel and was named Stuxnet. It was a “worm” that infected the computers running Iran’s nuclear industry. German systems control expert, Ralph Langer, who told the world about Stuxnet, remarked Stuxnet represented a dangerous capability and that its code could be used by hackers and others. In other words, Obama had unleashed a weapon that could be re-engineered by anyone to attack computer networks controlling American infrastructure.

Perhaps the most significant aspect of the Stuxnet attack was it demonstrated how Obama had given to himself new powers to launch a cyberwar against any country without Congressional approval. Unlike conventional war in which soldiers are sent to the front and bombs are dropped from the skies, cyberweapons silently and stealthily attack information systems, as well as financial and power centers. We do not know how many times Obama has used his new Cyber Command unit to attack nations other than Iran.

Obama’s Presidential Policy Directive 20, known as PPD 20, which he signed in October 2012, was a stark example of a power grab to accord to him special powers to launch a cyber war at a moment of his choosing. The Guardian newspaper, which first revealed the existence of the directive, claimed it sought a larger target list for cyber attacks and contemplated the use of cyber weapons within the U.S. if the president gave the green light and only in an emergency. But what kind of emergency remains unclear, as does the list of nations he might target in the future.

### Solvency—2

All their Cong key ev is about creating doctrine—need ot resolve ambiguity to negotiate with China—that’s their Adkisson card AND Austin

Their solvency card is from Bradbury—we solve

Steven Bradbury, Former head of the Office of Legal Counsel in the Department of Justice, 4/18/2011, The Developing Legal Framework for Defensive and Offensive Cyber Operations, harvardnsj.org/wp-content/uploads/2011/04/Vol.-2\_Bradbury\_Final.pdf

Conclusion. So here’s my thesis: To my view, **the lack of clarity on certain of** these **issues** under international law **means that with respect to those issues,** the President is free to decide, as a policy matter, where and how the lines should be drawn on the limits of traditional military power in the sphere of cyberspace. For example, that means that within certain parameters, **the President could decide when and to what extent military cyber operations may target computers located outside areas of hot fighting** that the enemy is using for military advantage. And **when a cyber attack is directed at us, the President can decide, as a matter of national policy, whether and when to treat it as an act of war.**

The corollary to all this is that in situations where the customs of war, in fact, are not crystallized, the lawyers at the State Department and the Justice Department shouldn’t make up new red lines — out of some aspirational sense of what they think international law ought to be — that end up putting dangerous limitations on the options available to the United States. Certainly, the advice of lawyers is always important, especially so where the legal lines are established or firmly suggested. No one would contend that the laws of war have no application to cyber operations or that cyberspace is a law-free zone. But it’s not the role of the lawyers to make up new lines that don’t yet exist in a way that preempts the development of policy.14

**In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention** on cyberwarfare — perhaps a kind of arms control agreement for cyber weapons. I believe **there is no foreseeable prospect that that will happen**. **Instead**, the outlines of accepted norms and limitations in this area will develop through the practice of leading nations. And the policy decisions made by the United States in response to particular events will have great influence in shaping those international norms**.** I think that’s the way we should want it to work.

One final admonition I’ll offer on the topic of offensive cyber operations: **In cases where the President shapes new policy** by choosing military action over covert action for a cyber operation, or vice versa, I would strongly urge that the President fully brief both sets of committees in Congress — the Intelligence Committees and the Armed Services Committees — and explain the basis for the choice. It’s inevitable the committees will find out anyway when a jurisdictional marker is crossed, and **it will help smooth the development of consistent policies and standards for the committee members and staff to understand and appreciate the choices made on both sides of the question.**

### Norms – 2NC

#### The CP’s declaratory policy creates international norms – the executive drives change

Segal 11 (Adam, Maurice R. Greenberg Senior Fellow for China Studies, “Cyberspace Governance: The Next Step” Policy Innovation Memorandum No. 2, March 2011, Council on Foreign Relations)

After years of dismissing the utility of international negotiations on cyberspace, U.S. officials now say that they will participate in talks to develop rules for the virtual world. But which norms should be pursued first and through which venues? As a start, the United States should issue two "cyber declaratory statements," one about the thresholds of attacks that constitute an act of war and a second that promotes "digital safe havens"--civilian targets that the United States will consider off-limits when it conducts offensive operations. These substantive statements should emerge from a process of informal multilateralism rather than formal negotiations. **Washington should engage allies and close partners such as India first and then reach out to other powers such as China and Russia with the goal that they also issue similar statements. Washington should also reach out to the private corporations that operate the Internet and nongovernmental organizations responsible for its maintenance and security.**

Declaratory statements play an important role in the definition, diffusion, and adoption of international norms. The discussions that precede the statements encourage actors to identify desirable and realistically attainable norms; the statements themselves set the behaviors that states will be held to. They are also likely to increase strategic stability. Explicit statements give potential attackers a more concrete picture of what type of attacks the United States will respond to and how, making signaling easier and improving stability.

The Problem

Increased U.S. receptivity to international negotiations reflects a growing sense **that domestic efforts to secure cyberspace are inadequate and that the United States has hurt itself by sitting on the sidelines.** There is real fear that a cyberattack--the use of computer power to attack computer, communication, transportation, and energy networks--could disrupt the economy, destroy critical infrastructure, or degrade military capabilities. The Internet was originally designed for the use and convenience of a small group of researchers in the United States; security was an afterthought. Now the network is global and there has been a proliferation of devices from laptops to smartphones connecting to it. No one agency, either national or multilateral, exerts authority over all parts of the Web.

As the United States has focused on domestic efforts to make cyberspace more secure--appointing a cyber coordinator, standing up Cyber Command, and deploying Einstein 2, an intrusion detection system--other states have challenged the U.S. conception of the web as a global commons open to commerce and the free exchange of information. Moreover, **the United States' refusal to enter into negotiations reinforced the sense that it intended to dominate cyberspace and limit the ability of other countries to maneuver in this new domain**.

The Obama administration's May 2009 Cyberspace Policy Review revealed a shift in U.S. attitudes. "International norms are critical to establishing a secure and thriving digital infrastructure," the report concluded. In December 2009 the United States agreed to talk with Russia and a United Nations arms control committee about Internet security.

International cooperation is necessary, but some fundamental characteristics of cyberspace make traditional arms control agreements unlikely. The technologies used in most attacks are commercial and widely available. Attacks can be masked and routed across several networks, obscuring whether they are the work of independently operating "patriotic hackers," criminal groups, an official security agency, bored teenagers, or some combination of all four. This problem of attribution undermines verification; signatories to any agreement would have little confidence they could identify violators.

Moreover, there is no consensus about what constitutes a cyberattack. The United States talks primarily about defending critical infrastructure like the power grid or financial systems; China, Russia, and others worry about these vulnerabilities but also see the free flow of information as a threat to domestic stability. As a result, in any negotiations, Beijing and Moscow are likely to demand that the United States limit its support for "digital activists" in return for China and Russia controlling "patriotic hackers," a requirement Washington is unlikely to meet.

The Rules of Cyberspace

While a more formal agreement may never be reachable, the United States has a clear interest in defining the rules of interstate behavior in cyberspace. It has a particular interest in identifying the point at which a cyberattack becomes the equivalent of an "armed attack" in international law as well as in defining what constitutes a legitimate target of cyberattack. In the physical world, for example, states are expected to abide by the principle of distinction which requires attacks only be made on legitimate military targets and permits attacks on civilian targets only when "demanded by the necessities of war." This norm was developed through several centuries of war and formalized after World War II in the Geneva Protocols.

At this point, most countries would accept that a cyberattack with "kinetic effects" equivalent to those of a conventional armed attack should be treated in the same manner, allowing for individual and collective self-defense as well as cyber and kinetic responses. But **what about attacks below this threshold that nonetheless threaten critical interests, say, by destroying public data or disrupting financial markets?** After consulting with its allies and friends, **the United States should issue a public "cyber declaratory statement" that reserves the right to respond either through a conventional or computer network attack, but leaves some room for maneuver**. Attacks on data and financial markets could both be covered by this statement as long as the consequences of an attack resulted in real suffering, not simply inconvenience.

**The United States will not renounce the development and use of offensive weapons, but it should still work to develop "digital safe havens" and then in a separate initiative declare these targets off limits.** Again, there is likely to be relatively easy consensus around some areas--hospitals and medical data--and much less agreement around others such as financial systems, power grids, and Internet infrastructure. The United States should also develop methods to mark its digital safe havens. It may have to separate its own network and data systems--data, for example, from the Department of Health and Human Services and the Pentagon should not sit on the same servers. U.S. policy makers should also work with companies and NGOs to address what are likely to be significant technical challenges in disentangling protected and non-protected spaces.

Building International Support

Since communication networks are global and primarily in private hands, an informal multilateralism is a more appropriate approach than a more formal multilateralism. U.S. officials should continue to show flexibility about venue, engaging through bilateral and multilateral meetings such as the United Nations, the G20, and regional groupings. There have been several moves to limit the role of nongovernmental groups in Internet governance--most recently in a December 2010 decision to involve only member states and exclude the Internet Governance Caucus and other organizations from a UN working group. By insisting on their participation in the relevant forum, the United States can continue to strengthen the authority of these groups.

In the case of thresholds and digital safe havens, **the United States should conduct discussions with close allies, friends, private companies, and NGOs over a twelve-to-eighteen month period**. The discussions about thresholds are particularly important for the United States to have with its allies; the large scale distributed denial of service attacks on Estonia in 2007 raised the question of whether the country should, or could, have invoked Article 5 of the NATO charter, in which members agree that an "armed attack against one or more of them . . . shall be considered an attack against them all." At the time and as is still the case today, NATO and international law lacked an accepted definition of what constitutes a cyberattack. These discussions should then be expanded to include other partners such as India and then to potential adversaries. **After all of these consultations, the United States should issue substantive statements about thresholds and response.** Although these statements will be unilateral**,** the goal of the consultative process should be to spur others to issue similar commitments.

This decentralized strategy is particularly important after Stuxnet, the malware that appears to target the Iranian nuclear program. It is now widely assumed that the United States, along with Israel, was behind the code. As a result, many countries will remain skeptical about Washington's intentions. Rules that appear to be the work of the United States alone will have little chance of gaining international support. **But building a coalition of states who will gain from and are willing to push for new rules may give these norms greater legitimacy**.

There has been in the United States' international engagement, however, a tendency to substitute process for strategy. While the decentralized approach to cyberconflict is the right one, it does not help in identifying strategic goals. The White House will have to become actively involved in order to push the process forward. **The National Security Council's** Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC) **subcommittee on international cyberspace policy efforts should** drive action, **not just coordinate and share information about what other agencies are doing**.

An informal multilateralism is best suited to cyberspace, and by focusing on some of the norms of interstate cyberconflict, and on thresholds and legitimate targets in particular, the U**nited** S**tates** will be better able to begin shaping international norms.

### At: dycus

Says oversight fails, and we just need standards

Dycus 10 (Professor Vermont Law School, “Congress’s Role in Cyber Warfare”, 8/11/2010, <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>)

III. ALEGISLATIVE HAND ON THE CYBER WAR MOUSE Cyber warfare, as that term is used here, refers to conflicts that utilize cyber or electronic weapons either offensively or defensively, or both. Cyber weapons are currently employed offensively in kinetic warfare, for example, to suppress an enemy’s air defenses or disrupt its communications, or defensively to track enemy troop movements. These weapons might also be used offensively to disable an enemy’s cyber weaponry or defensively in response to an enemy attack, to prevent further aggression. The term “cybersecurity” might be understood to refer to defense against cyber attacks. “Cyber attack” suggests offensive use, but the label is inexact and might be misleading. A preemptive strike to ward off an imminent enemy attack is considered defensive. Digital espionage might be part of the preparation for an attack, or it might be perceived that way by the target, which might then be provoked to defend itself by responding with a preemptive attack, either cyber or kinetic. The important point here is that any use of cyber weapons, offensive or defensive, could have enormous consequences for the security and other interests of the United States. The effect of such use, actual or potential, matters more than the labels. And if the effect – on human life or property, for example, or diplomatic relations or compliance with the law of armed conflict – is substantial, Congress has a role to play in adopting policy for that use. Congress has not thus far adopted measures suited to the regulation of cyber warfare. The War Powers Resolution, for example, is concerned with sending U.S. troops into harm’s way, rather than with clicking a computer mouse to launch a cyber attack, although the strategic consequences might be similar. And the WPR’s relatively relaxed timetable for executive notice and legislative response is unrealistic for war on a digital battlefield. Similarly, if cyber warfare is regarded as an intelligence activity, the intelligence oversight measures just described cannot, for reasons already indicated, ensure that Congress will be able to play a meaningful role. In the words of the National Research Council study cited above, “Today’s policy and legal framework for guiding and regulating the use of cyberattack is ill-formed, undeveloped, and highly uncertain.”45 Our experience with nuclear weapons may point to needed reforms. Since the beginning of the Cold War, the United States has had a fairly clear nuclear policy (albeit one that deliberately includes an element of ambiguity) – one known generally to Congress, the American public, and potential enemies.46 Congress has approved or disapproved the purchase of the weapons and delivery systems. It has been briefed on the policy, and it has debated that policy vigorously.47 While Congress has not articulated U.S. nuclear policy in any coherent form, it has collaborated closely with the executive branch in the development and execution of that policy. Cyber weapons bear a striking resemblance to nuclear weapons in some important ways. An enemy’s cyber attack would, like a nuclear strike, probably come without a clear warning. There are as yet no reliable defenses against either a cyber attack or a nuclear attack. Collateral damage from a nuclear attack would almost certainly be very extensive and would linger for an extended period.48 The direct and indirect effects of a cyber attack, while different in kind and degree, still could be widespread and indiscriminate.49 In other ways, cyber weapons are critically different from their nuclear counterparts. For one thing, the time frame for response to a cyber attack might be much narrower. A nuclear weapon delivered by a land-based ICBM could take 30 minutes to reach its target. An electronic attack would arrive instantaneously, and leave no time to consult with or even inform anyone outside the executive branch before launching a counterstrike, if that were U.S. policy. What most distinguishes digital warfare, however, is the potential difficulty in identifying the source of a cyber attack. It is always possible, of course, that an enemy might covertly deliver a nuclear device to the U.S. homeland in a shipping container or a Cessna. But the apparent ease with which a cyber attack may be carried out without attribution could make it impossible to fight back at all. If an attacker made it appear that the source was an innocent neutral state or perhaps another enemy of the attacker, a misdirected U.S. response might provoke a wider conflict. The potential difficulty in tracking the source also makes a policy of deterrence based on a threat of retaliation far less credible. Given these characteristics of cyber warfare, and the continuing refinement of cyber weaponry, we approach a state of extreme strategic instability, with each nation on hair-trigger alert. The execution of an illconceived cyber war policy calling for a prompt response – or any response – to an attack or threatened attack could have disastrous, unanticipated consequences. It also might, depending on the circumstances, violate the law of armed conflict. Congress accordingly needs to work closely with the executive branch in the development of a policy for this new kind of conflict. Such a policy ought to reflect the distinctive technology and strategy of digital warfare, and it should be reviewed constantly as the technology evolves. Like other regulations dealing with dynamic subjects, this policy should include general approaches that reflect this nation’s broad strategic concerns and fundamental values. But the policy must also be crafted with enough flexibility to allow those charged with its execution to deal with future developments that cannot now be predicted. And it should set out a procedure for such adaptive use by identifying, for example, who must be consulted under what circumstances, and who will make the final critical decisions. It is at least theoretically possible that Congress could play an active, real-time role in the implementation of whatever cyber warfare policy is adopted. The policy might, for example, like the War Powers Resolution, require consultation “in every possible circumstance.”50 But it seems more likely that a digital war would begin and end before any notice could ever reach Capitol Hill. Congress therefore needs to lay down clear guidelines, with as much flexibility as prudence requires, for executive branch officials to follow if consultation is not reasonably possible. And Congress should require a prompt and full account of every significant use of cyber weapons.

### AT: Object Fiat

#### Internal constraints are key neg ground – it matches the academic debate

Sinnar, assistant professor of law at Stanford Law School, May 2013

(Shirin, “Protecting Rights from Within? Inspectors General and National Security Oversight,” 65 Stan. L. Rev. 1027, Lexis)

More than a decade after September 11, 2001, the debate over which institutions of government are best suited to resolve competing liberty and national security concerns continues unabated. While the Bush Administration's unilateralism in detaining suspected terrorists and authorizing secret surveillance initially raised separation of powers concerns, the Obama Administration's aggressive use of drone strikes to target suspected terrorists, with little oversight, demonstrates how salient these questions remain. Congress frequently lacks the [\*1029] information or incentive to oversee executive national security actions that implicate individual rights. Meanwhile, courts often decline to review counterterrorism practices challenged as violations of constitutional rights out of concern for state secrets or institutional competence. n1

These limitations on traditional external checks on the executive - Congress and the courts - have led to increased academic interest in potential checks within the executive branch. Many legal scholars have argued that executive branch institutions supply, or ought to supply, an alternative constraint on executive national security power. Some argue that these institutions have comparative advantages over courts or Congress in addressing rights concerns; others characterize them as a second-best option necessitated by congressional enfeeblement and judicial abdication.

### Transparency – 2NC

#### A public doctrine ensures transparency – it demystifies our cyber policy

Mark Young, Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence, 2010, National Cyber Doctrine: The Missing Link in the Application of American Cyber Power, http://jnslp.com/2010/09/29/national-cyber-doctrine-the-missing-link-in-the-application-of-american-cyber-power/

A new cyber doctrine will provide guidance on the application of cyberpower in response to a physical attack or as part of a computer network attack **initiated by the U.S. government.** Under the existing doctrine, a computer network attack “is not integrated with overall [warfare] planning because of the highly compartmented classification that cyber activities receive.”51 **A major objective of assembling an interagency team to establish a national cyber doctrine is to improve the integration of** cyber defense and **offense into joint interagency operational planning. Operations in cyberspace must be “synchronized and coordinated with other operation**s, just as land and air operations . . . must be synchronized and coordinated.”52 **With their current classification, network attack capabilities are misunderstood and not widely employed**.

A national cyber doctrine should be unclassified to the maximum extent possible. As with other doctrines, a classified annex may be necessary to delineate sensitive capabilities, operations, or relationships. While it is foolish to disclose all the elements of U.S. cyberpower, the foundational principles that govern the applications of cyberpower should be widely disseminated. The development of this doctrine would de-mystify the domain for the national security community and the American people. **Federal agencies should participate in the debate to establish this doctrine and help institutionalize its principles across the entire government**. This debate can inform the decision on what information must remain classified and what does not need to be classified.

Although the doctrine should include as much unclassified detail as possible, the national cyber doctrine may require a classified annex to document U.S. offensive computer network capabilities. Other unclassified doctrines do not disclose specifications of weapons systems but do include a classified annex for a variety of purposes. Cyber weapons should be viewed as having little distinction from traditional weapons or techniques available to the U.S. Government. “Cyber weapons simply provide the operational planner with another option, in addition to the air-delivered, laser-guided bomb and the Special Operations force with demolition charges.”53 Given the nature of cyberwarfare, it is more important that details of specific weapons or techniques remain classified. As noted in a recent study, “As a general rule, [computer network] tricks exhaust themselves to the extent . . . that their existence and thus the need to protect against their recurrence is obvious and . . . that counters to their recurrence are straightforward to implement.”54

This issue of overclassification must be addressed if U.S. national security organizations are to benefit from cyberpower. According to Andrew Krepinevich, the “cyberwarfare competition is so shrouded in secrecy that it is difficult to determine the United States’ level of vulnerability, let alone options for addressing it.”55 The development of a national cyber doctrine would clarify the nation’s capabilities to those who are responsible for projecting U.S. power. The highly classified nature of computer network operations capabilities has prevented computer networks from being fully integrated into traditional war fighting exercises conducted by combatant commands. “[A]n unclassified and authoritative statement of current joint doctrine for the use of computer network attack is unavailable” and is still evolving.56

**The national security sector needs to debate cyberpower publicly**, rather than just hold classified conversations.57 **An open debate about the application of power and the circumstances that warrant** a doctrinal response would clarify and further develop the general understanding of not only the capabilities but also the limitations of network operations

### Effective Constraint – 2NC

#### Collaborative nature of DoD doctrine guarantees compliance across the executive

Mark Young, Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence, 2010, National Cyber Doctrine: The Missing Link in the Application of American Cyber Power, http://jnslp.com/2010/09/29/national-cyber-doctrine-the-missing-link-in-the-application-of-american-cyber-power/

Whether directed by the Cyber Command or by other government agencies, the employment of U.S. power in the cyber domain requires a rapid paradigm shift uncharacteristic of the DoD. To accelerate this shift, **the national security community needs a new doctrine to provide the fundamental principles by which executive branch** departments and agencies **can ensure** the **freedom of U.S. action in cyberspace**. The DoD controls most of the expertise in computer network operations and is well positioned to lead the national security community in establishing U.S. cyber policies and doctrines. It cannot do this alone, however.

This article argues that a national cyber doctrine is necessary. **It is the link between strategy and the execution of the missions of the national security sector**. Doctrine may traditionally be a military notion, but **agencies are acknowledging the wisdom of establishing guiding principles.** A national cyber doctrine can be a vehicle used to define the roles of departments and agencies for the entire U.S. government. **In contrast to a presidential executive order or a** National Security Council **directive**, a doctrine is developed in an openly collaborative fashion.

Author David Kilcullen’s observations regarding counterinsurgency collaboration are also applicable to the development of a national cyber doctrine: “**To be effective, we must marshal not only all agencies of the [U.S. government], but also all agencies of a host nation, multiple foreign allies and coalition partners, international institutions, nongovernment organizations** . . . international and local media, religious and community groups, and charities and businesses.”5

**The DoD has developed an extensive collection of doctrines that guide military operations, but there is no doctrine to guide** applications of national cyberpower. Cyber Command’s missions are being formulated without an adequate doctrine to define the strategic context, establish the fundamentals of cyberpower, or debate issues concerning computer network operations. The Secretary of Defense memorandum ordering the establishment of the Cyber Command mandates the synchronization of cyberwar effects “across the global security environment as well as providing support to civil authorities and international partners.”6 Coordination of interagency cyber operations and cooperation with civil and foreign partners are the types of activities for which doctrine is well suited. Other DoD doctrines govern similar activities in the sea, air, land, and space domains.7

**While the DoD has no authority to enforce** military **doctrines outside of the Department,** sound principles developed with the full participation of interagency partners will be followed due to their utility and effectiveness, not because of coercion. As has been observed, “You cannot command what you do not control.”8 **Therefore the doctrine should foster a unified effort across the entire U.S. national security community.** Its success will depend “on a shared diagnosis of the problem, platforms for collaboration, information sharing and deconfliction.”9

The current U.S. **counterinsurgency doctrine provides a model of how an inclusive doctrine can gain acceptance throughout the national security community**. The development of the counterinsurgency doctrine was directed by then Lieutenant General David Petraeus after his return from his second tour of duty in Iraq in 2004. Petraeus brought together traditional and nontraditional partners to devise fundamental principles by which to address an extremely difficult set of combat circumstances. Some “military officers questioned the utility of the representatives from nongovernment organizations (NGOs) and the media, but they proved to be the most insightful of commentators.”10

The application of cyberpower is just as complicated as counterinsurgency operations, and in many ways it is more complicated. The success of the counterinsurgency doctrine, produced by a group of collaborators that included those typically excluded from the development of military doctrine, shows the wisdom of an inclusive approach.

By creating a diverse community of interest to draft cyber doctrine, the national security community can more adequately address long-standing questions about U.S. activities in cyberspace**:** How should the government act to protect privacy while undertaking robust efforts to prevent cyber attacks? How will the Cyber Command support the strategic goal of defending the U.S. economy? What are the likely consequences of and who will be responsible for responding to a successful cyber attack that results in loss of life or destruction of property?

### Soft power

Soft power fails - empirics

Drezner 11

Daniel W. Drezner, Professor of International Politics at the Fletcher School of Law and Diplomacy at Tufts University, Foreign Affairs, July/August 2011, "Does Obama Have a Grand Strategy?", <http://www.foreignaffairs.com/print/67869>

What went wrong? The administration, and many others, erred in believing that improved standing would give the United States greater policy leverage. The United States' standing among foreign publics and elites did rebound. But this shift did not translate into an appreciable increase in the United States' soft power. Bargaining in the G-20 and the UN Security Council did not get any easier. Soft power, it turns out, cannot accomplish much in the absence of a willingness to use hard power. The other problem was that China, Russia, and other aspiring great powers did not view themselves as partners of the United States. Even allies saw the Obama administration's supposed modesty as a cover for shifting the burden of providing global public goods from the United States to the rest of the world. The administration's grand strategy was therefore perceived as promoting narrow U.S. interests rather than global public goods.

### Deterrence – 2NC

Declaratory policies solve transparency—the case turns are net benefits

Waxman 13 (Matthew, Professor, Columbia Law School; Adjunct Senior Fellow, Council on Foreign Rela-tions; Member of the Hoover Institution Task Force on National Security and Law, “Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions” 2013, 89 INT’L L. STUD. 109)

III. A STRATEGIC PERSPECTIVE

A strategic perspective on the question of cyber attacks as armed attacks sees the issue as one linking a purported right of armed self-defense to long-term policy interests—both national interests and global ones in the case of the United States—including security and stability. The substance and clarity of any such legal right has the potential to significantly enhance or detract from those strategic ends. Armed self-defense to cyber attacks may be strategically valuable in several respects. First, anticipatory or responsive military actions might be important in some cases to protecting military and critical infrastructure vulnerable to cyber attacks—for example, by striking at facilities or indi-viduals responsible for launching or directing them—though, because the physical infrastructure associated with cyber attacks may be quite small and widely dispersed, this sort of preventive use of force specifically to neutral-ize the possibility of initial or follow-on cyber attacks has not been the sub-ject of much discussion. Second, the credible threat of self-defensive mili-tary actions might help deter cyber attacks by raising the prospective costs of hostile cyber activities in the minds of adversaries (though probably not much so of non-State adversaries, against whom deterrent threats of mili-tary action will not be very potent). Such strategic logic likely underlies the U.S. declaratory postures described in the previous section, putting adver-saries on notice that they should expect a possible military response to some cyber threats.

### Cyber

### 2NC No Cyber War Impact

Err neg - their authors exaggerate and cyber defense tech is improving

Libicki 8/16/13

MARTIN C. LIBICKI is a Senior Management Scientist at the RAND Corporation and a Visiting Professor at the U.S. Naval Academy, Foreign Affairs, August 16, 2013, "Don't Buy the Cyberhype: How to Prevent Cyberwars From Becoming Real Ones", http://www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype

These days, most of Washington seems to believe that a major cyberattack on U.S. critical infrastructure is inevitable. In March, James Clapper, U.S. director of national intelligence, ranked cyberattacks as the greatest short-term threat to U.S. national security. General Keith Alexander, the head of the U.S. Cyber Command, recently characterized “cyber exploitation” of U.S. corporate computer systems as the “greatest transfer of wealth in world history.” And in January, a report by the Pentagon’s Defense Science Board argued that cyber risks should be managed with improved defenses and deterrence, including “a nuclear response in the most extreme case.”

Although the risk of a debilitating cyberattack is real, the perception of that risk is far greater than it actually is. No person has ever died from a cyberattack, and only one alleged cyberattack has ever crippled a piece of critical infrastructure, causing a series of local power outages in Brazil. In fact, a major cyberattack of the kind intelligence officials fear has not taken place in the 21 years since the Internet became accessible to the public.

Thus, while a cyberattack could theoretically disable infrastructure or endanger civilian lives, its effects would unlikely reach the scale U.S. officials have warned of. The immediate and direct damage from a major cyberattack on the United States could range anywhere from zero to tens of billions of dollars, but the latter would require a broad outage of electric power or something of comparable damage. Direct casualties would most likely be limited, and indirect causalities would depend on a variety of factors such as whether the attack disabled emergency 911 dispatch services. Even in that case, there would have to be no alternative means of reaching first responders for such an attack to cause casualties. The indirect effects might be greater if a cyberattack caused a large loss of confidence, particularly in the banking system. Yet scrambled records would probably prove insufficient to incite a run on the banks.

Officials also warn that the United States might not be able to identify the source of a cyberattack as it happens or in its immediate aftermath. Cyberattacks have neither fingerprints nor the smell of gunpowder, and hackers can make an intrusion appear legitimate or as if it came from somewhere else. Iran, for example, may not have known why its centrifuges were breaking down prematurely before its officials read about the covert cyber-sabotage campaign against the country’s nuclear program in The New York Times. Victims of advanced persistent threats -- extended intrusions into organization networks for the purpose of espionage -- are often unaware for months, or even years, that their servers have been penetrated. The reason that such attacks go undetected is because the removal of information does not affect the information in the system, so nothing seems amiss. The exfiltration of information can also be easily hidden, such as in the daily flow of web traffic from an organization.

But since everything is becoming increasingly dependent on computers, could levels of damage impossible today become inevitable tomorrow? As it happens, all of the trend lines -- good and bad -- in cyberspace are rising simultaneously: the sophistication of attackers, but also that of the defenders; the salience of cyberattacks as weapons, but also the awareness of the threat they pose; the bandwidth available for organizing larger attacks, but also the resources to ward them off. It is bad news that Iran is beginning to see cyberwar as a deniable means of exploiting easy targets. And it is good news that software companies are now rethinking the architectural features of their systems that permit such vulnerabilities to exist in the first place.

#### Cyber makes war less likey

Thomas Rid, Kings College London War Studies, Nov/Dec 2013, Cyberwar and Peace, Foreign Affairs, Ebsco

Yet the hype about everything "cyber" has obscured three basic truths: cyberwar has never happened in the past, it is not occurring in the present, and it is highly unlikely that it will disturb the future. Indeed, rather than heralding a new era of violent conflict, so far **the cyber-era has been defined by the opposite trend**: **a computer-enabled assault on political violence.** **Cyberattacks diminish rather than accentuate political violence** by making it easier for states, groups, and individuals to engage in two kinds of aggression that do not rise to the level of war: sabotage and espionage. Weaponized computer code and computer-based sabotage operations make it possible to carry out highly targeted attacks on an adversary's technical systems without directly and physically harming human operators and managers. Computer-assisted attacks make it possible to steal data without placing operatives in dangerous environments, thus reducing the level of personal and political risk.

These developments represent important changes in the nature of political violence, but they also highlight limitations inherent in cyber-weapons that greatly curtail the utility of cyberattacks. Those limitations seem to make it difficult to use cyberweapons for anything other than one-off, hard-to-repeat sabotage operations of questionable strategic value that might even prove counterproductive. And cyber-espionage often requires improving traditional spycraft techniques and relying even more heavily on human intelligence. Taken together, these factors call into question the very idea that computer-assisted attacks will usher in a profoundly new era.

### At: us preemption key

Pre-emptive strikes are categorically defensive cyber operations – they don’t solve their advantage

Dycus 10 (Professor Vermont Law School, “Congress’s Role in Cyber Warfare”, 8/11/2010, http://jnslp.com/wp-content/uploads/2010/08/11\_Dycus.pdf)

Cyber warfare, as that term is used here, refers to conflicts that utilize¶ cyber or electronic weapons either offensively or defensively, or both.¶ Cyber weapons are currently employed offensively in kinetic warfare, for¶ example, to suppress an enemy’s air defenses or disrupt its¶ communications, or defensively to track enemy troop movements. These¶ weapons might also be used offensively to disable an enemy’s cyber¶ weaponry or defensively in response to an enemy attack, to prevent further¶ aggression.¶ The term “cybersecurity” might be understood to refer to defense¶ against cyber attacks. “Cyber attack” suggests offensive use, **but the label¶ is inexact** and might be misleading. A preemptive strike to ward off an¶ imminent enemy attack is considered defensive. Digital espionage might¶ be part of the preparation for an attack, or it might be perceived that way by¶ the target, which might then be provoked to defend itself by responding¶ with a preemptive attack, either cyber or kinetic.

### 2NC Military = Safe

No risk – nukes aren’t connected to the tubes

Green 2

The Washington Monthly. Washington: Nov 2002. Vol. 34, Iss. 11; pg. 8, 6 pgs

JOSHUA GREEN is an editor of the Washington Monthly.

Serious effort and plain good fortune have combined to bring this about. Take nuclear weapons. The biggest fallacy about their vulnerability, promoted in action thrillers like WarGames, is that they're designed for remote operation. "[The movie] is premised on the assumption that there's a modem bank hanging on the side of the computer that controls the missiles," says Martin Libicki, a defense analyst at the RAND Corporation. "I assure you, there isn't." Rather, nuclear weapons and other sensitive military systems enjoy the most basic form of Internet security: they're "air-gapped," meaning that they're not physically connected to the Internet and are therefore inaccessible to outside hackers. (Nuclear weapons also contain "permissive action links," mechanisms to prevent weapons from being armed without inputting codes carried by the president.) A retired military official was somewhat indignant at the mere suggestion: `As a general principle, we've been looking at this thing for 20 years. What cave have you been living in if you haven't considered this [threat]?"

### taiwan

#### Econ ties outweigh everything

Daniel **Lynch 12**, IR prof at USC, “Why Ma Won the Elections and what’s Next for Taiwan and China”, January 15, <http://www.foreignaffairs.com/articles/137029/daniel-lynch/why-ma-won-the-elections-and-whats-next-for-taiwan-and-china?page=show>

During the campaign, most observers insisted that the election was not about cross-strait relations but about socio-economic issues, including rapid economic growth amid worsening inequality, reduced career opportunities for recent college graduates, and unaffordable housing costs. In fact, socio-economic issues are inseparable from cross-strait issues. Ma ran on his record of improving ties between China and Taiwan, claiming that friendship meant stability and prosperity and that a reversion to DPP rule would throw Taiwan back into the dark days of the mid-2000s, when DPP President Chen Shui-bian's avowedly Taiwan-centric policies blocked negotiations even on direct passenger plane flights across the Taiwan Strait. Tsai, no protectionist or isolationist herself, promised not to roll back cooperation with China for the same reason. Her main criticism of Ma was that he is naive about China. According to her, issues of further integration -- such as allowing Chinese professionals and white-collar workers to take jobs in Taiwan -- should be approached cautiously. For their part, voters seem to have accepted Ma's contention that reducing cross-strait tensions improves the country's economic well-being. Indeed, more than ever, Taiwan's economy is dependent on China's. This is partly a result of market dynamics (Taiwanese capital flows across the Taiwan Strait in search of lower production costs) and partly a result of the KMT and Chinese Communist Party's efforts to facilitate integration. By the end of 2011, some 80,000 Taiwanese firms had invested up to $200 billion in mainland factories, research and development centers, stores, and restaurants. And annual trade between the two sides exceeded $150 billion. Meanwhile, out of a total population of 23 million, one million or more Taiwanese live in China. Directly or indirectly, the majority of Taiwanese households depend on Chinese economic dynamism for their livelihood. These are the dynamics that had helped Ma win a landslide victory in the 2008 Taiwan elections to begin with. He had made the campaign promise to pursue something like a Taiwanese-Chinese common market. He delivered on this pledge in 2010 by signing with Beijing the Economic Cooperation Framework Agreement (ECFA), under which the two sides agreed to slash tariffs on a wide variety of goods and services. By December 2011, 16.1 percent of Taiwanese goods exported to China and 10.5 percent of Chinese goods exported to Taiwan were already tariffed at preferential rates. Important services were also covered under ECFA's "early harvest" provisions.

### LOAC

### 2nc – solves arms races

OCO solves their arms race adv—deters cyber escalation

LIEUTENANT COLONEL SCOTT W. BEIDLEMAN, United States Air Force, 2009, Defining and Deterring Cyber War, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA500795

In general, deterrence is a state of mind. It is the concept of one state influencing another state to choose not to do something that would conflict with the interests of the influencing state. Similarly, the central idea of deterrence from the perspective of the Department of Defense is “to decisively influence the adversary’s decision-making calculus in order to prevent hostile actions against U.S. vital interests.”82 Deterred states decide not to take certain actions because they perceive or fear that such actions would produce intolerable consequences.83 The idea of influencing states’ decisions assumes that states are rational actors “willing to weigh the perceived costs of an action against the perceived benefits, and to choose a course of action” logically based on “some reasonable cost-benefit ratio.”84

Thus the efficacy of cyber deterrence relies on the ability to impose or raise costs and to deny or lower benefits related to cyber attack in a state’s decision-making calculus. Credible cyber deterrence is also dependent on a state’s willingness to use these abilities and a potential aggressor’s awareness that these abilities, and the will to use them, exist. While a state’s ability to deter cyber attacks is a subset of its overarching defense strategy comprised of all instruments of national power, this paper focuses on states’ actions to deter cyber attack within the cyberspace domain. Effective cyber deterrence in cyberspace will employ a comprehensive scheme of offensive and defensive cyber capabilities supported by a robust international legal framework.

Offensive capabilities are the primary tools used to impose or raise costs in deterrence. Offensive cyber capabilities and operations provide a state the means and ways for retaliation and enhance the perceived probability that aggressors will pay severely for their actions. A more robust capability translates to a more credible imposition of costs. Until recently, U.S. efforts to develop offensive cyber capabilities have lagged efforts on the defensive side. The daily onslaught of attacks on U.S. networks, coupled with the likelihood that potential U.S. adversaries will be less dependent on electronic networks than the U.S., has prioritized intelligence gathering and defending U.S. capabilities over disrupting enemy capabilities.85 However, the United States has recently gained momentum in the development of offensive cyber capabilities.

In 2006, the U.S. published the National Military Strategy for Cyber Operations with the expressed intent to achieve “military strategic superiority in cyberspace.”86 One of its main goals is to ensure “adversaries are deterred from establishing or employing offensive capabilities against U.S. interests in cyberspace.”87 Unlike the air, land, and sea domains, the U.S. currently lacks dominance in cyberspace.88 In fact, without a significant effort, the U.S. will lose its current technological advantages and “risks parity with adversaries” in cyberspace.89 To this end, the U.S. has taken measures in support of offensive cyber operations. While each military service has some form of cyber footprint, the U.S. Air Force has incorporated operating in cyberspace as part of its core mission on par with flying and space operations. For instance, the commander of the Air Force’s provisional cyber operations command envisions initial offensive cyber operations as subduing or killing data packets that threaten U.S. systems, with the potential to expand in the future to missions normally executed by conventional forces in the past.90 The U.S. continues to modernize its cyber forces, create new hacker units, and conduct cyberwar exercises,91 with the intent to “penetrate and disrupt foreign computer systems.”92 However, the U.S. is not alone in pursuing cyber attack. Over 120 countries already have or are developing computer attack capabilities, reinforcing the need for a strong defense.93

### 1nc congress link

Plan restricts use of cyber ops

Lorber ’13

Eric, J.D. Candidate, University of Pennsylvania Law School, Ph.D Candidate, Duke University Department of Political Science, “Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?,” 15 U. Pa. J. Const. L. 961

Yet a surprising amount of uncertainty exists as to which - if any - domestic laws constrain the use of OCOs and how they fit into the congressional-executive balance. As policymakers, scholars, and journalists have lamented, a coherent policy framework governing the use of OCOs does not exist and many questions remain unanswered. n8 Would an attack [\*963] using cyber weapons trigger the requirements of the War Powers Resolution? n9 Would OCOs be subject to reporting requirements under the Intelligence Authorization Act? n10 Conversely, do cyber operations grant the executive branch another tool with which it can prosecute attacks but avoid reporting and responding to congressional inquiries? These questions are largely unanswered both because the rise of OCOs is a relatively recent phenomenon and because much of the information about U.S. technical capability in this field is highly classified. n11 Yet addressing these questions is increasingly important for two reasons. First, as states such as China, Israel, Russia, and the United States 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. n12 Second, the possible employment of these tools adds yet another wrinkle to the battle between the executive and legislative branches over war-making authority. n13 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. n14 As a result, the employment of these tools [\*964] implicates - and perhaps problematically shifts - the balance between the executive's commander-in-chief power n15 and Congress's war-making authority. n16 This Comment provides an initial answer to the question of whether current U.S. law can effectively govern the Executive's use of OCOs. n17 It explores the interaction between this new tool and the current statutory limits on presidential war-making authority, with a particular focus on whether the two current federal laws meant to restrict executive power in this field - the War Powers Resolution n18 and the Intelligence Authorization Act n19 - apply to a wide range of potential offensive cyber operations undertaken by the executive branch. Beyond suggesting that neither the War Powers Resolution nor the Intelligence Authorization Act can effectively regulate most types of offensive cyber operations, this Comment suggests that while marginally problematic for a proper balance of war-making power between the executive and legislative branches, this lack of oversight does not fundamentally shift the current alignment. It does argue, however, that - given this lack of regulatory oversight - **the President now has another powerful war-making tool to use at his discretion**. Finally, the Comment suggests that this lack of limitation may be positive in some ways, as laying down clear legal markers before having a developed understanding of these capabilities may problematically limit their effective use.

### 1NC Attribution Solves

Deterrence via attribution is effective – actual threats will self report

Charles L. Glaser, Professor of Political Science and International Affairs Elliot School of International Affairs, George Washington University, 11 [“Deterrence of Cyber Attacks and U.S. National Security,” Report GW-CSPRI-2011-5, June 1, http://www.offnews.info/downloads/2011-5CyberDeterrenceGlaser.pdf]

Many experts are quite pessimistic about the feasibility of attribution. For example, William Lynn, the U.S. Deputy Secretary of Defense recently wrote, “The forensic work necessary to identify an attacker may take months, if identification is possible at all.”

Cyber deterrence and the attribution problem

4 Richard Clarke reports that a leading group of cyber experts concluded that it is “fruitless” to try to attribute the source of cyber attacks.5 **This view, however, may exaggerate the attribution problem by overlooking either the purposes of the attacker or the scenario in which the attack occurs**.6

A state that launches a “countervalue” attack against the United States’ economic infrastructure, economy and/or society is likely to have a political purpose. Possible purposes could include compelling the United States to make political concessions during a crisis before a war starts, compelling the United States to stop fighting a war, and reducing the U.S. ability to fight a war by weakening its economy and industrial infrastructure. **For these compelling threats to be effective, the state would have to make demands and spell out its threat.** In addition, it would have to provide the United States with some confidence that attacks would stop if the United States meets that attacker’s demands. **These communication requirements would largely eliminate the attribution problem.** For the scenario of attacking to weaken the U.S. ability to fight, the country the United States was fighting would be immediately identified as the likely suspect; the possibility that the United States would likely come to this conclusion could be sufficient to deter the adversary’s cyber attack. Alternatively, the attacker might not be deterred because the costs of U.S. retaliation were not large compared to the costs of the on-going war; but in this case the failure of deterrence would not result from the attribution problem but instead from the size of the retaliatory costs the United States was threatening.

Of course, actors that lack political objectives are not covered by this argument. Terrorist groups are therefore a natural concern, as they are often viewed as motivated simply by the desire to damage the United States. A very different perspective disagrees, however, arguing that terrorist groups, including al Qaeda, are motivated by political goals and use terror attacks as a means to achieve their political ends.7

The attribution issue for “counterforce” attacks—those directed against U.S. capabilities—is quite different, but may be even less of a problem than with counter value attacks launched by states. This type of attack is most likely to occur during a crisis or war, with the adversary employing the cyber attack to gain a military advantage. Attribution will likely not be a problem, because the United States will know which state it is involved within a conflict. This is not to say that deterring this type of attack will not be difficult; it might be for reasons other than attribution. This is a separate issue that we deal with briefly below. If this is the case, a terrorist group will find itself facing communication requirements that are not unlike those facing states. A terrorist group might be hard to deter by retaliation because there are no good targets to hit in retaliation, and almost certainly no important cyber targets, but again the difficulty of deterrence would not result from attribution problems, but the more familiar problem of threatening attacks that would inflict sufficiently high costs on a terrorist group. Another type of actor that might be of concern here are hackers who are motivated by the technical challenge of undermining U.S. cyber systems and not by political objectives.

All of this said, the difficulty of attribution does create a variety of potential dangers. One possibility is dangerous mischief: a third party—country, terrorist group, or hacker—could launch a cyber attack against the United States while it was involved in a crisis or war with another state. Based on the logic sketched above, this could lead to misattribution, because the United States’ first inclination would likely be to attribute the attack to the country it was already fighting. Consequently, the third party could use such an attack to generate escalation in the on-going conflict, with the goal of increasing the damage that the United States and/or its adversary would suffer. Another problem is that the inability to attribute attacks undermines the U.S. ability to deter (and otherwise respond) to much lower level cyber attacks, including data stealing, espionage, and disruption of commerce. At a minimum, attribution would enable the United States to try to deter these types of attacks by promising to pursue legal actions. **But** for the most part, **these types of attacks do not threaten vital U.S. national security interests**, so from a security perspective the attribution problem does not generate large risks.

### at: china & russia

China and Russia reject US cyber norms

Reed 13

John Reed, reports on the frontiers of cyber war and the latest in military technology for Killer Apps, Foreign Policy, January 24, 2013, "John Kerry: cyber conflict one of world's greatest threats", http://killerapps.foreignpolicy.com/posts/2013/01/24/john\_kerry\_acknowledges\_cyber\_as\_one\_of\_worlds\_greatest\_threats

Here's what Killer Apps reported in September about U.S effort to establish cyber norms based on the laws of armed conflict and the resistance it's met, especially from Russia and China, according to Eric Rosenbach, deputy assistant secretary of defense for cyber policy.

"There are several countries right now that are very aggressive in cyberspace and are likely trying to create norms [of cyberspace behavior] that would be unstable for the international community because they are so aggressive," Rosenbach said. "It's still not completely clear what's acceptable and what's not acceptable and several nations different than the United States have very aggressive notions of what's acceptable."

Russia and China are focused more on controlling citizens' activities on the internet rather than limiting attacks on nations' critical infrastructure, he said.

"There are other countries, the Chinese and Russians in particular, that don't think the law of armed conflict is the best framework to view these things through and they focus much more heavily on control of information than they do on the security of crucial infrastructure or preventing the destruction of networks."

Rosenbach went on to call this a "nonstarter."

"To say that your model of an international law for cybersecurity is based on controlling media content or what people can say about the government isn't something we're interested in at all," he said. "There are other areas -- in particular, the theft of intellectual property -- because that's a major problem for the United States right now, where there are very different ideas about what's acceptable and what's not."

China empirically dodges cyber norms

Inboden 13

Will Inboden is a Distinguished Scholar at the Strauss Center for International Security and Law at the University of Texas-Austin, and a Contributing Editor at Foreign Policy magazine, Foreign Policy, June 3, 2013, "Looking for the strength to negotiate", http://shadow.foreignpolicy.com/posts/2013/06/03/looking\_for\_the\_strength\_to\_negotiate

In the case of China, the White House in recent weeks has at last begun publicly speaking out against China's state-sponsored hacking of American military and commercial targets, but the only real action in response seems to be a call for dialogue because, in the words of a senior administration official "we need to develop some norms and rules." Well, yes, developing norms and rules would be nice, but the immediate issue is much simpler: the Chinese government needs to stop stealing technology from American companies, and needs to stop engaging in low-grade acts of cyberwar against the American military. China will continue this cyberwarfare as long as it can do so without any consequences - and a diplomatic dialogue or even "sternly-worded demarche" from the State Department do not count as consequences. Especially since Beijing has proven very artful at using dialogues as diversionary tactics to resist taking concrete policy steps, with the episodic U.S.-China Human Rights Dialogue being just one example (an especially sad reminder of the failures of U.S. human rights policy as this week marks the anniversary of the Tiananmen Square massacre).

China doesn't care about plan

Segal 11

Adam Segal is the Ira A. Lipman senior fellow for counterterrorism and national security studies at the Council on Foreign Relations, China US Focus, May 26, 2011, "Chinese Responses to the International Strategy for Cyberspace", http://www.chinausfocus.com/peace-security/chinese-responses-to-the-international-strategy-for-cyberspace/

A week after the United States released its International Strategy for Cyberspace, it is possible to gauge some Chinese responses. Not surprisingly, there was a relatively high degree of skepticism about U.S. intentions. Chinese concerns revolved around three issues:

The strategy is really about military capabilities and deterrence. Perhaps following the lead of some U.S. news reports, Chinese press reports focused on the statement that Washington reserved the right “to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law,” to defend itself and its allies. This must be frustrating to the State Department since it was trying to de-emphasize cyberspace as a warfighting “domain” and stress its importance as a public forum, market, and source of innovation. They wanted less talk about Cyber Command and more about international engagement. Certainly it couldn’t have been an accident that Deputy Secretary of Defense William Lynn spoke after Homeland Security Advisor John Brennan, Secretary of State Hillary Clinton, Attorney General Eric Holder, Secretary of Commerce Gary Locke, and Secretary of Homeland Security Janet Napolitano.

Despite the calls for cooperation, the U.S. is trying to maintain its technological lead. In the view of some Chinese analysts, the call for interoperability and global standards mask an effort to lock others into technologies owned by U.S. companies. Global Times quoted one analyst as saying: “The U.S. masters a number of core technologies for cyberspace usage, and it aims to continuously consolidate its advantages.” Similarly, in the area of Internet governance, no matter how often U.S. government officials refer to international cooperation, they still want the United States “to maintain its lead role. At a press conference on the same day, Hillary Clinton made this point very clear.”

US cyber norms don't translate to China

Healey 13

Jason Healey is the director of the Cyber Statecraft Initiative at the Atlantic Council of the United States, Foreign Policy, April 16, 2013, "China Is a Cyber Victim, Too", http://www.foreignpolicy.com/articles/2013/04/16/china\_is\_a\_cyberwar\_victim\_too?page=full

Yet U.S. cyber-operations are extremely different from their Chinese equivalents and cannot be compared in the way the Chinese suggest. When the U.S. military or intelligence community conducts cyber-operations, they are quiet, coordinated, exceptionally well targeted, and under the strict control of senior officers and government executives. Lawyers review every stage. Even Stuxnet, though it was a breathtakingly sophisticated and brazen attack, was so tightly controlled that, when it escaped its target network, it caused no disruption. The White House keeps a close hold on cyber-operations through senior executives, generals, and political appointees throughout the bureaucracy.

Chinese espionage, by comparison, is under no such control. As in other areas of Chinese society, the People's Liberation Army and state-owned enterprises are subject to little oversight and feel little need to coordinate their actions. Recently, one colleague that works for a specialized incident-response firm reported finding as many as seven different Chinese espionage groups operating in the same network, all sending information back to different masters. Few, if any, senior party officials care to rein in activities helping domestic companies (and probably lining their own pockets) by stealing foreign intellectual property.

## 1NR

### at: perm do the cp

Espionage is distinct from cyber attacks within offensive cyber operations

Luke Pelican, J.D., LL.M., August 2011, 12 [“PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT NECESSARY GAME,” 20 CommLaw Conspectus 363]

B. Definitions

This paper addresses cyber-espionage, also known as "cyber-exploitation," defined by Herbert Lin as "the use of actions and operations--perhaps over an extended period of time--to obtain information that would otherwise be kept confidential and is resident on or transiting through an adversary's computer systems or networks." n14¶ Action through cyber-exploitation is **generally covert** and is conducted though the least intrusive means in order to extract the sought-after information. n15 Individuals who engage in cyber-exploitation attempt to leave undisturbed the normal operations of a computer system or network, and an ideal method is one that goes undetected by the user. n16¶ Cyber-espionage can be contrasted with other forms of cyber activities. Such activities include "cyberterrorism" or full-on "cyberwar", both of which could have devastating effects, as compared to others that are less severe in nature, such as low-level "cybercrime" or "cybervandalism." n17 The technical aspects of these activities complicate the determination of whether cyber-espionage is merely espionage or whether it is something more a daunting task for federal regulators and those tasked with defending our networks.¶ One technique that can be utilized is system probing, which consists of gathering valuable intelligence while causing no damage to the network. Dr. Herbert Lin of the National Research Council analogizes such activity to approaching a country's airspace without violating it to engage in observations from the air and to test the countries air defense response. n18 This type of behavior alone, although typically regarded as unfriendly, would not normally raise any use of force concerns. n19 If a method of cyber-espionage is the use of such a payload, even if it is designed not to result in any harm to the host system, the host country will not necessarily have that knowledge and could perceive the payload as a harmful threat. n20¶ Indeed, probing can be a precursor to something far more destructive, [\*366] illustrated by the Russian-Georgian crisis of 2008. n21 While there have been many more examples of pure cyber-espionage activities that have not served as staging for a subsequent attack, government and military officials must nonetheless consider the possibility that a systematic probing and incursion onto sensitive systems could be such a preparatory measure. n22¶ Dr. Lin also provides an example in which an "**offensive cyber operation**" deploys a dual purpose payload into the computer network of an adversary. n23 The payload's first role is merely data observation and collection, activity that falls under the espionage category. The second role is to neutralize the system upon command. n24 Whether the deployment of such a payload amounts to espionage or rises to the level of the threat or use of force is a difficult question to resolve.¶ The Stuxnet worm presents an example of the potential for this type of dual-payload system, **though** the worm **was not employed for espionage purposes**. Stuxnet first gained public attention in June of 2010 by researchers in Belarus, who observed its presence on computers belonging to their Iranian clients. n25 Stuxnet's purpose was to disable centrifuges at the Natanz Fuel Enrichment Plan in Iran by manipulating industrial control equipment developed by Siemens. n26 Stuxnet raises significant questions for policymakers and may represent the future of cyber operations.

### cyber adv

The CP is transparent, legislative, and lays out clear criteria – those are the requirements in their ev for solving escalatory miscalc

Walker says the ‘list of countries’ we may target is secret – the CP establishes that it’s all but one

Austin says

stronger civilian oversight and subject to more rigorous public scrutiny

That’s a reason we’re sufficient cause we’re better than the squo

Dycus says mainitaining flexible exemptions in our policy is NBD for effectiveness, and is probably better

Dycus 10 (Professor Vermont Law School, “Congress’s Role in Cyber Warfare”, 8/11/2010, <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>)

III. ALEGISLATIVE HAND ON THE CYBER WAR MOUSE Cyber warfare, as that term is used here, refers to conflicts that utilize cyber or electronic weapons either offensively or defensively, or both. Cyber weapons are currently employed offensively in kinetic warfare, for example, to suppress an enemy’s air defenses or disrupt its communications, or defensively to track enemy troop movements. These weapons might also be used offensively to disable an enemy’s cyber weaponry or defensively in response to an enemy attack, to prevent further aggression. The term “cybersecurity” might be understood to refer to defense against cyber attacks. “Cyber attack” suggests offensive use, but the label is inexact and might be misleading. A preemptive strike to ward off an imminent enemy attack is considered defensive. Digital espionage might be part of the preparation for an attack, or it might be perceived that way by the target, which might then be provoked to defend itself by responding with a preemptive attack, either cyber or kinetic. The important point here is that any use of cyber weapons, offensive or defensive, could have enormous consequences for the security and other interests of the United States. The effect of such use, actual or potential, matters more than the labels. And if the effect – on human life or property, for example, or diplomatic relations or compliance with the law of armed conflict – is substantial, Congress has a role to play in adopting policy for that use. Congress has not thus far adopted measures suited to the regulation of cyber warfare. The War Powers Resolution, for example, is concerned with sending U.S. troops into harm’s way, rather than with clicking a computer mouse to launch a cyber attack, although the strategic consequences might be similar. And the WPR’s relatively relaxed timetable for executive notice and legislative response is unrealistic for war on a digital battlefield. Similarly, if cyber warfare is regarded as an intelligence activity, the intelligence oversight measures just described cannot, for reasons already indicated, ensure that Congress will be able to play a meaningful role. In the words of the National Research Council study cited above, “Today’s policy and legal framework for guiding and regulating the use of cyberattack is ill-formed, undeveloped, and highly uncertain.”45 Our experience with nuclear weapons may point to needed reforms. Since the beginning of the Cold War, the United States has had a fairly clear nuclear policy (albeit one that deliberately includes an element of ambiguity) – one known generally to Congress, the American public, and potential enemies.46 Congress has approved or disapproved the purchase of the weapons and delivery systems. It has been briefed on the policy, and it has debated that policy vigorously.47 While Congress has not articulated U.S. nuclear policy in any coherent form, it has collaborated closely with the executive branch in the development and execution of that policy. Cyber weapons bear a striking resemblance to nuclear weapons in some important ways. An enemy’s cyber attack would, like a nuclear strike, probably come without a clear warning. There are as yet no reliable defenses against either a cyber attack or a nuclear attack. Collateral damage from a nuclear attack would almost certainly be very extensive and would linger for an extended period.48 The direct and indirect effects of a cyber attack, while different in kind and degree, still could be widespread and indiscriminate.49 In other ways, cyber weapons are critically different from their nuclear counterparts. For one thing, the time frame for response to a cyber attack might be much narrower. A nuclear weapon delivered by a land-based ICBM could take 30 minutes to reach its target. An electronic attack would arrive instantaneously, and leave no time to consult with or even inform anyone outside the executive branch before launching a counterstrike, if that were U.S. policy. What most distinguishes digital warfare, however, is the potential difficulty in identifying the source of a cyber attack. It is always possible, of course, that an enemy might covertly deliver a nuclear device to the U.S. homeland in a shipping container or a Cessna. But the apparent ease with which a cyber attack may be carried out without attribution could make it impossible to fight back at all. If an attacker made it appear that the source was an innocent neutral state or perhaps another enemy of the attacker, a misdirected U.S. response might provoke a wider conflict. The potential difficulty in tracking the source also makes a policy of deterrence based on a threat of retaliation far less credible. Given these characteristics of cyber warfare, and the continuing refinement of cyber weaponry, we approach a state of extreme strategic instability, with each nation on hair-trigger alert. The execution of an illconceived cyber war policy calling for a prompt response – or any response – to an attack or threatened attack could have disastrous, unanticipated consequences. It also might, depending on the circumstances, violate the law of armed conflict. Congress accordingly needs to work closely with the executive branch in the development of a policy for this new kind of conflict. Such a policy ought to reflect the distinctive technology and strategy of digital warfare, and it should be reviewed constantly as the technology evolves. Like other regulations dealing with dynamic subjects, this policy should include general approaches that reflect this nation’s broad strategic concerns and fundamental values. But the policy must also be crafted with enough flexibility to allow those charged with its execution to deal with future developments that cannot now be predicted. And it should set out a procedure for such adaptive use by identifying, for example, who must be consulted under what circumstances, and who will make the final critical decisions. It is at least theoretically possible that Congress could play an active, real-time role in the implementation of whatever cyber warfare policy is adopted. The policy might, for example, like the War Powers Resolution, require consultation “in every possible circumstance.”50 But it seems more likely that a digital war would begin and end before any notice could ever reach Capitol Hill. Congress therefore needs to lay down clear guidelines, with as much flexibility as prudence requires, for executive branch officials to follow if consultation is not reasonably possible. And Congress should require a prompt and full account of every significant use of cyber weapons.

### loac adv

Ex-post alone is sufficient to solve the loac clarity – their 1ac ev

Bradbury 11 (Steven – partner @ Dechert, LLP, “The Developing Legal Framework for Defensive and Offensive Cyber Operations” March 2011, Cybersecurity: Law, Privacy, and Warfare in a Digital World, Harvard National Security Journal, Vol. 2)

One final admonition I’ll offer on the topic of offensive cyber operations: In cases where the President shapes new policy by choosing military action over covert action for a cyber operation, or vice versa, I would strongly urge that the President fully brief both sets of committees in Congress — the Intelligence Committees and the Armed Services Committe es — and explain the basis for the choice. It’s inevitable the committees will find out anyway when a jurisdictional marker is crossed, **and it will help smooth the development of consistent policies and standards for the committee members and staff to understand and appreciate the choices made** on both sides of the question.

Espionage doesn’t violate the law of armed conflict – same 1ac card

Bradbury 11 (Steven Assistant Attorney General for the Office of Legal Counsel, The Developing Legal Framework for Defensive and Offensive Cyber Operations, http://harvardnsj.org/wp-content/uploads/2011/02/Vol.-2\_Bradbury\_Final1.pdf)

And if you just review the literature on cyber war, you quickly see that that’s where we are: precisely how the laws and customs of war should apply to offensive cyber operations is not yet crystallized in key respects.¶ For example, there aren’t always bright lines to tell us when a cyber attack on computer systems constitutes an “armed attack” or a “use of force” that justifies a nation in launching a responsive military strike under Article 51 of the U.N. Charter.¶ Some questions are easy: Hacking into a sensitive government computer system to steal information is an act of espionage, not an armed attack. **It’s clearly not prohibited by the laws and customs of war**.¶ On the other hand, if the cyber intrusion inflicts significant physical destruction or loss of life by causing the failure of critical infrastructure, like a dam or water supply system, then it obviously would constitute an armed attack under the law of war and would justify a full military response if it could be attributed to a foreign power. Where committed as an offensive act of aggression, such an attack may violate international law.¶ If significant enough, the effect of the attack will determine its treatment, not necessarily whether the attack is delivered through computer lines as opposed to conventional weapons systems. In these cases, the laws and customs of war provide a clear rule to apply.

Seriously, it’s not a violation

Luke Pelican, J.D., LL.M., August 2011, 12 [“PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT NECESSARY GAME,” 20 CommLaw Conspectus 363]

Disagreement abounds as to whether peacetime espionage is permissible [\*370] under international law. n49 Interestingly, international law has not evolved to address the finer aspects of the question--this has been the case during the height of the Cold War and even into the 21st century. n50

**Support for the permissibility of peacetime espionage under international law extends as far back as the 17th century** to the writings of Grotius, n51 a major figure in the development of modern international law. n52 Though espionage conducted in wartime has received attention in international law, in particular the laws governing armed conflict, n53 peacetime espionage has not. n54 According to Roger Scott, **"[e]spionage is not prohibited by international law** as a fundamentally wrongful activity; it does not violate a principle of jus cogens." n55 A jus cogens norm is defined by the Vienna Convention on the Law of Treaties as "a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character." n56 Consequently, a prohibition of or limitation on peacetime espionage is largely governed by the domestic laws of nations. n57

This view most comports with reality given the nature of statecraft and geopolitical necessities. As one scholar observed, "there has never been a war [\*371] without spies, and there never has been a peace in which spies have not engaged in preparations for a future war." n58 Espionage serves a critical purpose in enabling states to acquire information on allies and enemies alike, information that may be difficult to discover through more conventional means. This information in turn allows states to effectively navigate the rough currents of international relations and preserve their individual security.

Despite having its share of supporters, the position that peacetime espionage is illegal under international law is ultimately misguided. Professor Radsan cited Manuel Garcia Mora's claim that "peacetime espionage is regarded as an international delinquency and a violation of international law," n59 though Mora himself acknowledged the point is thoroughly contested. n60 Richard Falk argued espionage is illegal, but noted there is "considerable persuasive policy available to oppose" that conclusion. n61

### impact

They cherry pick history – nuclear states cause the stability-instability paradox – Iran getting the bomb risks nuclear war

Colin H. Kahl, Senior Fellow at the Center for a New American Security focusing on Middle East security and defense policy and Associate Professor at Georgetown SFS, 12 [Response to Iran and the Bomb, “One Step Too Far,” Foreign Affairs, Reviews and Responses, Septempber/October, pp 157-160]

“History shows that when countries acquire the bomb, they feel increasingly vulnerable and become acutely aware that their nuclear weapons make them a potential target in the eyes of major powers,” Waltz argues. “This awareness discourages nuclear states from bold and aggressive action.”¶ In writing this, Waltz ignores a long history of emerging nuclear powers behaving provocatively. In 1950, for example, Soviet leader Joseph Stalin gave North Korea the green light to invade South Korea, thus beginning the Korean War. Stalin apparently assumed (incorrectly) that the United States was unlikely to respond because the Soviets had by then developed their own nuclear weapons. Waltz also claims that China became less aggressive after going nuclear in 1964. But in 1969, Mao Zedong authorized Chinese troops to attack Soviet forces on the Chinese-Soviet border. The attack was meant to warn Moscow against border provocations and to mobilize domestic Chinese support for Mao’s revolution. Like Stalin before him, Mao was probably confident that China’s recently acquired nuclear capabilities would limit the resulting conflict. (In the end, the border clashes produced a larger crisis than Mao had expected, raising the possibility of a Soviet nuclear strike, and China backed down.)¶ Waltz also asserts that “India and Pakistan have both become more cautious since going nuclear.” But Pakistan’s development of nuclear weapons has in fact facilitated its strategy of engaging in low-intensity conflict against India, making the subcontinent more crisis- prone. As the political scientist S. Paul Kapur has shown, as Islamabad’s nuclear capabilities have increased, so has the volatility of the Indian-Pakistani rivalry.¶ Since 1998, when both India and Pakistan openly tested nuclear devices, and to support groups that have conducted terrorist attacks elsewhere in India. Furthermore, in 1999, Pakistan sent conventional forces disguised as insurgents across the Line of Control in the Kargil district of Kashmir, triggering a limited war with India. This move was encouraged by the Pakistanis’ belief that their nuclear deterrent placed clear limits on India’s ability to retaliate with conventional weapons. Additionally, over the past decade, Pakistani-backed militants have engaged in high-profile terrorist attacks inside India itself, including the 2001 attack on the New Delhi parliament complex and the 2008 Mumbai attacks.¶ Waltz writes that “policymakers and citizens in the Arab world, Europe, Israel, and the United States should take comfort from the fact that history has shown that where nuclear capabilities emerge, so, too, does stability.” In fact, the historical record suggests that competition between a nuclear-armed Iran and its principal adversaries would likely follow the pattern known as “the **stability-instability paradox,”** **in which the supposed stability created by mutually assured destruction generates greater instability by making provocations, disputes, and conflict below the nuclear threshold seem safe.¶** During the Cold War, for example, nuclear deterrence prevented large-scale conventional or nuclear war between the United States and the Soviet Union. At the same time, however, the superpowers experienced several direct crises and faced oa in a series of bloody proxy wars in Korea, Vietnam, Afghanistan, Angola, Nicaragua, El Salvador, and elsewhere. A recent statistical analysis by the political scientist Michael Horowitz demonstrated that inexperienced nuclear powers tend to be more crisis-prone than other types of states, and research by another political scientist, Robert Rauchhaus, has found that nuclear states are more likely to engage in low-level militarized disputes with one another, even if they are less likely to engage in full-scale war.¶ If deterrence operates the way Waltz expects it to, a nuclear-armed Iran might reduce the risk of a major conventional war among Middle Eastern states. But history suggests that Tehran’s development of nuclear weapons would encourage Iranian adventurism, **leading to more frequent and intense crises in the Middle East. Such crises would entail some inherent risk of a nuclear exchange resulting from a miscalculation, an accident, or an unauthorized use—a risk that currently does not exist at all.¶** The threat would be particularly high in the initial period after Iran joined the nuclear club. Once the superpowers reached rough nuclear parity during the Cold War, for example, the number of direct crises decreased, and the associated risks of nuclear escalation abated. But during the early years of the Cold War, the superpowers were involved in several crises, and on at least one occasion—the 1962 Cuban missile crisis—they came perilously close to nuclear war. Similarly, a stable deterrent relationship between Iran, on the one hand, and the United States and Israel, on the other, would likely emerge over time, but the initial crisis-prone years would be hair-raising. Although all sides would have a profound interest in not allowing events to spiral¶ out of control, the residual risk of inadvertent escalation stemming from decades of distrust and hostility, the absence of direct lines of communication, and organizational mistakes would be nontrivial—and the consequences of even a low-probability outcome could be devastating.

A nuclear Iran makes an already volatile middle east even more conflict prone – diplomacy and pressure are key

Colin H. Kahl, Senior Fellow at the Center for a New American Security focusing on Middle East security and defense policy and Associate Professor at Georgetown SFS, 12 [Response to Iran and the Bomb, “One Step Too Far,” Foreign Affairs, Reviews and Responses, Septempber/October, pp 157-160]

Because Waltz is sanguine about the effects of Iranian nuclearization, he concludes that “the United States and its allies need not take such pains to prevent the Iranians from developing a nuclear weapon.” Waltz believes that the only utility of continued diplomacy is to maintain “open lines of communication,” which “will make the Western countries feel better able to live with a nuclear Iran,” and he argues that “the current sanctions on Iran can be dropped.”

Waltz is wrong. The threat from a nuclear-armed Iran might not be as grave as some suggest, but it would make an already volatile Middle East even more conflict-prone. Preventing Iran from crossing the nuclear threshold should therefore remain a top U.S. priority. Because a preventive military attack on Iran’s nuclear infrastructure could itself set off a series of unpredictable and destabilizing consequences, the best and most sustainable solution to Iran’s nuclear challenge is to seek a negotiated solution through a combination of economic pressure and diplomacy. It is possible to oppose a rush to war with Iran without arguing, as Waltz does, that a nuclear-armed Iran would make the world a better place.

Iran prolif is a crisis magnifier – draws in great powers to small conflicts

Edelman, Fellow – Center of Strategic and Budgetary Assessments, ‘11

(Eric, “Edelman, Krepinevich, and Montgomery Reply,” *Foreign Affairs* Vol. 9 Iss. 2, March/April)

Ultimately, if Tehran does cross the nuclear threshold and Israel chooses to live with a nuclear-armed Iran, one of the principal objectives of U.S. policy should be convincing Israel to maintain its policy of nuclear opacity for as long as possible. The benefit of a slightly more credible Israeli deterrent would not outweigh the added difficulties the United States would confront in seeking to limit a nuclear Iran's influence, preserve regional stability, and prevent additional proliferation.

A second important issue Adamsky raises is that Iran's acquisition of nuclear weapons would increase the threat that Israel faced from Iranian proxies such as Hamas and Hezbollah, either because Tehran would provide increased assistance and encouragement to these groups or because they would become more reckless once they had a nuclear-armed patron. A premeditated attack by Iran against Israel is not the only scenario that could lead to a nuclear exchange, or even the most plausible one. Instead, a limited conflict in southern Lebanon or the Gaza Strip might spiral out of control. Iranian proxies could escalate their attacks against Israel, assuming that it would be deterred by its fear of a nuclear Iran. Israel could then defy their expectations and conduct major reprisals to demonstrate its resolve, prompting Iran to make nuclear threats in defense of its clients. The results would be unpredictable and potentially disastrous. Although debates over Iran's nuclear program often turn on the issue of Iranian "rationality," it is important to remember that there are many different paths to conflict, and the dynamics of Iranian-Israeli relations could be prone to miscalculation and escalation.

## 2NR

### 2nr card

That’s key – we need to keep it up

Albright et al. 12 [David Albright, chairperson of ISIS, Paul Brannan, senior analyst at ISIS who has done extensive research and analysis on the international nuclear black market, Andrea Stricker, research analyst, Christina Walrond, and Houston Wood, “PREVENTING IRAN FROM GETTING NUCLEAR WEAPONS: CONSTRAINING ITS FUTURE NUCLEAR OPTIONS,” The Institute for Science and International Security, March 5, http://w.isis-online.org/uploads/isis-reports/documents/USIP\_Template\_5March2012-1.pdf]

Intelligence operations aimed at data gathering in¶ Iran through a variety of mea¶ ns, including spying,¶ cyber infiltrations or snooping, aerial surveillance,¶ and bugging of equipment procured by Iran.¶ Intelligence operations aimed at data gathering¶ may provide information and advanced warning¶ about Iran’s nuclear activities and plans¶ . As¶ previously discussed, these measures include¶ operations to gather data through spying, use of¶ cyber infiltrations, aerial surveillance to reveal¶ new activities and nuclear sites, and bugging of¶ equipment destined for the Iranian nuclear¶ program in or¶ der to follow its path and use.¶ Western governments routinely use intelligence¶ operations to increase knowledge about Iran’s¶ activities and should actively expand them and¶ cooperate closely with other governments.¶ Encouraging and seeking information fro¶ m¶ **defectors from Iran’s nuclear program** and¶ providing nucl¶ ear information to the IAEA.¶ The use¶ of spies or domestic informants to obtain data¶ about Iran’s nuclear activities and intentions¶ should be expanded to inform intelligence¶ assessments about Iran’s¶ plans to expand¶ enrichment sites,¶ build covert ones, move toward¶ a dash for nuclear weapons, or experiment with or¶ conduct nuclear weaponization activities.¶ Informants working inside the program with¶ access to the most restricted information and¶ plans ha¶ ve already provided detailed information¶ to Western governments about Iran’s nuclear¶ weaponization projects and other military nuclear¶ efforts. These governments provided a significant¶ amount of this information to the IAEA and should¶ continue to do so.¶ The IAEA plays an important¶ role as a reviewer and synthesizer of such¶ information for its safeguards reporting. It also¶ remains in the best position to attempt to seek¶ answers from Iran.¶ Nations should start programs, if their intelligence¶ agencies do n¶ ot already have them, to encourage¶ and reward defections from Iranian nuclear¶ programs that are in violation of U.N. Security¶ Council resolutions. A whistleblower program¶ should offer asylum for the person and his or her¶ family and a monetary reward for ke¶ y information¶ about secret or banned activities.¶ Stronger mandate to IAEA to investigate Iran’s¶ illicit procurements.¶ The IAEA could also serve a¶ more useful role in investigating Iran’s illicit¶ procurement attempts and should receive a¶ mandate to pursu¶ e this fruitful area. By¶ centralizing available data on Iran’s procurement¶ schemes collected by member states, the IAEA¶ could better understand Iran’s nuclear program¶ and make its analyses available to all member¶ states and their domestic companies. Such¶ an¶ IAEA mandate would support government/industry¶ cooperation programs. Issues of member states¶ sharing confidential information on Iran’s¶ procurement schemes with an international¶ organization would need to be overcome, in¶ addition to some member states¶ ’ concerns about¶ the IAEA potentially communicating directly with¶ private companies.¶ Covert Actions¶ Sabotage of procured goods through infiltration of¶ smuggling networks.¶ As discussed, sabotage of¶ illicitly procured equipment through the¶ infiltration¶ of Iran’s illicit supply lines reportedly has had¶ some success.¶ 30¶ Sabotage efforts can cause damage to enrichment or other nuclear operations. **Such initiatives should¶ be expanded.** Iran’s acquisition of these goods for its nuclear program is in clear viol¶ ation of nations’¶ laws and U.N. Security Council sanctions. Sabotaging the goods is not distinguishable legally from the¶ practices carried out by police forces in enforcing their own national laws.¶ Surveillance and disruption of smuggling networks.¶ Int¶ elligence and law enforcement agencies can¶ seek to survey and disrupt the operations of entire smuggling networks rather than singling out a few¶ key actors. Effective operations require coordination across national boundaries in order to find out¶ what maj¶ or procurement networks are seeking, detect how they operate, and eventually shut them¶ down through intelligence operations or arrests and prosecutions.¶ Cyber attacks meant to inflict physical damage to nuclear facilities.¶ As discussed above,¶ cyber a¶ ttacks¶ against Iran’s nuclear infrastructure are a newer tool first put in use during the 2009/2010 Stuxnet¶ cyber attack against Iran’s Natanz enrichment plant. The attack, launched by unknown governments,¶ resulted in the decommissioning of about 1,000 ce¶ ntrifuges. The malware infected computer systems¶ that controlled centrifuge operations and abruptly spun the centrifuges up to very high and then low¶ speeds in order to destroy their delicate internal machinery. The attack set back Iran’s centrifuge¶ prog¶ ram for about a year, after which it largely recovered. Additional cyber attacks could be considered¶

for use against enrichment plants other than Natanz that pose a greater risk of breakout when they¶ come into operation.¶ The next attack may be more dif¶ ficult to accomplish, since Iran is likely to have taken precautions¶ against this type of attack. These codes also take years to develop. Further, cyber attacks run the risk¶ of being used against an attacker or being manipulated by non¶ -¶ state actors. Yet¶ , the tool has the¶ attractiveness of a lack of signature, psychological impact, and the potential for causing damage.¶ Already a successor to the Stuxnet attack, the **Duqu malware, has shown that cyber attacks are likely to¶ continue against Iran** as long as¶ it remains in violation of Security Council resolutions.