# 1AC GSU

### 1AC LOAC Advantage

#### Squo OCO policy violates the Law of Armed conflict

#### First – Lack of congressional checks make Jus in Bellum impossible to establish

Dycus 10(Professor Stephen Dycus is an internationally recognized authority on national security law and environmental law. The courses he has taught at Vermont Law School include Public International Law, National Security Law, Estates, Property, and Water Law. He was founding chair of the National Security Law Section of the Association of American Law Schools. He is the lead author of "National Security Law" (the field's leading casebook) and "Counterterrorism Law", and he was founding co-editor in chief of the Journal of National Security Law & Policy. (Stephen, "Congress' Role in Cyber Warfare," National Security Journal, Volume 4, Issue 155, 2010 <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>)

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 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.

#### Second – Clandestine nature of Obama’s policies

Loon 12 (Collin Engelbert Peter van Loon Royal Netherlands Army , “Offensive Cyber What are the possibilities of the use of offensive cyber as an offensive capability within the existing international legal framework?”, https://cyberwar.nl/d/MSc-thesis\_Offensive-Cyber\_Collin-van-Loon\_June-2012.pdf)

Offensive cyber operations are not covered by an international agreed legal framework. The consequence is that it is hard to distinguish between the different kind of cyber attacks, their purpose, their origin and under which existing law the attacks fall. LoAC only covers the jus i bello kind of attacks. When the LoAC were first drafted, only nation-states had the legal ability to wage war and to execute operations. Since cyber attack weapons are easy available for everyone, non-state actors and even individuals are capable getting involved in cyber incidents, cyber operations or cyber conflict. Thus, the lines between state, non-state, and individual attackers are unclear in a legal regime that discriminates between LoAC on the one hand and national criminal laws and law enforcement on the other (Dam et al., 2009, s. 22).

The lack of a decent legal framework also endangers a decent distinction between cyber attacks conducted in the cause of warfare, or cyber attacks as a simple hacker’s activity in the cause of law enforcement. The means and methods used by a nation-state to conduct cyber attacks can vary greatly and can also be classified in a number of ways. However, although this variety, these attacks can be similar if not identical to those used by hackers in the context of cyber crimes. Moreover, cyber attacks can occur both in times of peace and war (Palojärvi, 2009). The blurring in these different types of cyber attack makes the need for a general international accepted cyber legal framework even more necessary

#### Third - Definition of ambiguous attack posture

Adkisson et al. 12 Carnagie Mellon University (CDR James Adkisson, Mr. Tokunbo Davies, LT Brian Evans,¶ Mr. Rick Lanchantin, Ms. Patty Walters, “Law of Armed Conflict:¶ Implications for Navy Cyber Strategy¶ Masters of Information Technology Strategy¶ Practicum – 2012”, <http://www.cmu.edu/mits/files/random/mits-cohort1-practicumfinal-lawarmedconflict-implications-aug-2012.pdf>)

The uncertain definition of the ‘use of force’ is increasingly problematic when analyzing cyber attacks. Although cyber attacks do not utilize lethal effects, cyber attacks present a clear danger due to their ability to inflict both intended and unintended damage to critical infrastructure, financial markets, banks and the overall welfare of a nation. Such attacks could lead to the paralysis of a nation due to an inability to support its population, resulting in significant suffering and/or death of non-combatants. As a result, there is a strong argument that the threat of cyber attack is itself a violation of the U.N. Charter and LOAC. In contrast, there is also an argument that cyber should be used in preference to conventional weapons in order to comply with LOAC. This argument is based on the assertion that cyber attacks are more humanitarian because they have less potential to create collateral damage than conventional weapons. These are the issues that commanders and military planners must balance when

conducting operations in cyberspace.

In a February 2012 testimony to Congress, the Director of National Intelligence (DNI), Director of the Central Intelligence Agency (CIA), and Director of the Federal Bureau of Investigations (FBI) stated that cyber security ranks among the top national security concerns. They also indicated that current policy requires revision to address how the use of force in cyberspace conforms to national and international law, including LOAC.

The previous section reviewed the applicability of LOAC to cyber operations. This section builds on that understanding and reviews national policy that impact DoD operations in cyberspace.

B. Defining Policy

The DoD does not expressly define the term ‘policy’. A standard dictionary definition implies that policy provides guidance for solving problems without explicitly defining the solution.2 Accordingly, policy for cyber operations should offer a means to arrive at solutions for achieving the established operational objectives within cyberspace.

While DoD policy is designed to guide the decision-making process, the policies must conform to LOAC. Accordingly, the DoD has stated that current policy and legal regimes that govern actions in traditional warfare domains also apply to cyberspace operations.3¶ The U.S. Navy has in turn stated that Navy cyberspace operations will conform to DoD and national efforts.4 Despite these efforts, cyber policy across the U.S. Government remains severely underdeveloped. Many of the policy documents from the Executive Branch, DoD, individual military services, and Department of Homeland Security (DHS) were written more than ten years ago. Despite their age, these documents continue to influence decisions about cyber operations that result in “legally acceptable plans and orders that support national security objectives.”**¶** 5

While there is significant debate regarding cyber operations amongst the international community, the U.S. Government (USG) is moving forward to try and establish domestic strategies and policies. These policies can generally be examined from the perspectives of offense and defense. Due to lack of international consensus regarding the characteristics of an ‘armed attack’ in cyberspace, there is minimal policy regarding Offensive Cyber Operations (OCO) or Exploitation Cyber Operations (ECO). Policy concerning OCO continues to suffer from a lack of authorities concerning its use. ECO is conducted under U.S. Title 50 authorities that govern the operations of the Intelligence Community (IC).

#### This uniquely antagonizes china and make mutual drawdown impossible

Sanger 9/1/13 (David, A 1982 graduate of Harvard College, Sanger has been writing for the Times for 30 years covering foreign policy, globalization, nuclear proliferation, and the presidency., He has been a member of two teams that won the Pulitzer Prize, and has been awarded numerous honors for national security and foreign policy coverage. “Documents detail U.S. cyber-espionage plans”, <http://www.thehindu.com/news/international/documents-detail-us-cyberespionage-plans/article5083012.ece>)

231 operations planned for 2011 – both small scale and large scale

Newly disclosed budget documents for America’s intelligence agencies show how aggressively the United States is conducting offensive cyber-operations against other states, even while the Obama administration protests attacks on U.S. computer networks by China, Iran and Russia.

The documents, obtained by The Washington Post from Edward J. Snowden, the former National Security Agency contractor, indicate 231 such operations in 2011, a year after the first evidence emerged of a U.S.-and Israeli-led cyberattack against Iran’s nuclear-enrichment centre.

It suggests that President Barack Obama was not deterred by the disclosure of the Iranian operation, which became evident because of a technological error, and is pressing ahead on using cyber-weapons against a variety of targets.

The Post had said it has withheld most of the 178 pages of documents at the request of government officials because of the sensitivities of the spying operations they describe.

Unlike drone attacks, which the administration has begun to acknowledge publicly and provide legal justifications for, cyberattacks are still regarded as part of a secret arsenal.

The attacks described in the budget documents appear to be on a far smaller scale than the series of attacks on Iran, which were part of a classified operation called “Olympic Games”.

The Post talked of a parallel effort, code-named GENIE, which it described as an effort by U.S. intelligence officials working for the NSA and the military’s Cyber Command to insert surreptitious controls into foreign computer networks. That computer code, a form of malware, allows U.S. officials to hijack the computers or route some of their data to servers that enable U.S. espionage.

It is unclear how many, if any, of those 231 operations are merely for espionage or data manipulation, and how many may be intended to destroy or disable infrastructure. Mr. Obama, in an executive order signed last year, has reserved the right to decide when the United States should conduct such operations. It is not clear how many of the 231 he approved.

Diplomatically, the disclosure of the latest Snowden documents poses a new challenge to Mr. Obama. He has pressed China to cease its own cyber-operations in the United States, many of which are aimed at the theft of intellectual property — including corporate secrets and plans for the F-35 Joint Strike Fighter, the country’s most expensive new weapons system.

The Chinese have responded that America also conducts extensive cyber-operations — including against China — and will doubtless use the most recent disclosures to press that case. So far, Mr. Obama’s effort to get the Chinese engaged in a deeper dialogue on cyberissues has yielded discussions, but little fruit.

#### Impacts –

#### A) China doesn’t have a model for LOAC in cyberspace – that escalates ANY SKIRMISH.

VornDick 6/30/13 (Wilson VornDick is a lieutenant commander in the U.S. Navy, where he is assigned to the Pentagon. Previously, he worked at the Chinese Maritime Studies Institute at the U.S. Naval War College. , “The Real U.S.-Chinese Cyber Problem”, <http://nationalinterest.org/commentary/the-real-us-chinese-cyber-problem-8796?page=2>)

Recent waves of cyber attacks emanated from China despite their vehement denial that they possess “cyber warfare troops.” Meanwhile, the United States, sensing its own security vulnerabilities, stood up its newest military Combatant Command, USCYBERCOM, in 2009. This enabled a coordinated defensive and offensive capability in an increasingly digitized world as evident in the U.S.-led Stuxnet and Flame malware operations against Iran in 2010. As a result, both of the prominent digital players in the international community can bring forth debilitating and warlike capabilities. Washington and Beijing even agreed to a spontaneous two-day summit in June to stem the increasingly dangerous game of digital cat and mouse. Unfortunately, the norms guiding the use of cyber forces have yet to be established.

One crucial point lost amid the backdrop of the new digitized battlefield is the lack of Chinese leadership experience both military and political in utilizing key principles of the laws of armed conflict (LOAC). LOAC principles are becoming the foundation and framework for the emerging rules on cyber warfare. Some in China are slowly recognizing this shift. Given the increasingly interconnected, globalized and legally ill-defined nature of cyber technologies, one false move by either the United States or China could steer them into a cyber collision with horrendous conventional consequences.

General Escalation of Force, Proportionality and Rules of Engagement Concepts in War

Jus in bello (just conduct in war) is the set of general laws and principles that govern the way war is fought. It also incorporates the principles of escalation of force (EOF), proportionality, and the rules of engagement (ROE). This was created to promote humane standards in warfare despite the overreaching, destructive nature inherent in war. With the end of WWII, these principles now have been codified with international and customary laws into the Geneva Convention. These embody the modern concept of the law of armed conflict.

U.S. Experience with the LOAC

The U.S. Department of Defense leadership has a vast experience with these principles as they apply to the doctrine of jus in bello. They presently use various rules, approaches, and protocols to abide by the LOAC. Prior to the start of hostilities, military planners will delineate three key principles taken from the LOAC noted earlier: escalation of force (EOF), proportionality, and rules of engagement (ROE). This is to avoid confusion and miscalculation before, during and after hostilities.

The Army’s Escalation of Force Handbook defines EOF as “sequential actions that begin with nonlethal force measures (visual signals to include flags, spotlights, lasers and pyrotechnics) and may graduate to lethal measures (direct action) to include warning, disabling or deadly shots to defeat a threat and protect the force.” Meanwhile, proportionality is military action that is not excessive in relation to the concrete and direct military advantage anticipated. The Army has a uniform Standard Rules of Engagement dictating engagement of force.

Since September 11, U.S. policy makers and military strategists have been provided a tremendous opportunity to finesse those LOAC concepts based on first-hand experience gained in Iraq, Afghanistan, Libya, Guantanamo Bay, on the Korean peninsula and off the Horn of Africa. Each of these situations has spanned a wide range of possibilities in utilizing both cyber and conventional forces. U.S. commanders were required to tailor and adjust these forces to the realities on the ground. This resulted in the integral inclusion of cyber and information warfare training across all military services and senior leaderships. The significance of these experiences has pushed U.S. policy makers to shape frameworks to govern the nebulous and proliferating world of cyber warfare.

The Tallinn Manual and Emerging Cyber Norms

The law-of-armed-conflict principles already established are guiding the discussion and implementation of the emerging rules, doctrines and frameworks that may one day govern the future of cyber warfare. Realizing the need for a LOAC as it applied to the cyber domain, various states, NGOs and individuals have begun to provide their own precepts. Last year, tremendous work and energy by scholars, policymakers and digital leaders from around the world was poured into the Tallinn Manual on the International Law Applicable to Cyber Warfare. This collaborative document provides a starting point to cover the use of force in cyber warfare by state and nonstate actors. However, this document is merely a guiding post and lacks enforcement mechanisms. There is still no globally recognized norm. China has not provided transparency or information regarding their cyber intentions. Despite this, China’s previous views on conventional use of force may offer some clues on future cyber warfare strategies.

The Chinese have not had practical, hands-on experience with escalation of force, proportionality or rules of engagement. The Chinese military has not conducted significant operations since its shellacking in the 1979 border war with Vietnam. Their military has a dearth of expertise in applying these concepts in a real-time threat environment. This inexperience is compounded by the fact that the PRC and PLA leadership define the concepts differently from the United States and others. Because LOAC principles gained from battlefield experience are finding their way into the norms of the cyber domain, the Chinese authorities may be ill-prepared to deal with the pandora’s box of cyber warfare. This mismatch of LOAC experience potentially could cause a miscalculation in any cyber encounter.

Lonnie Henley conducted a study on Chinese escalation management in 2006. He found that Chinese military strategists and theorists segregate EOF and proportionality under their concepts of containment of war (遏制战争 ezhi zhanzheng) and war control (战争控制 zhanzheng kongzhi). Further, he pointed out that Chinese perceptions on war containment and control can be described as the “deliberate actions of war leaders to limit or restrain the outbreak, development, scale, intensity, and aftermath of war” as well as controlling its vertical and horizontal escalation. The Chinese concept of war control is unique in that it seeks a united and focused national effort to maintain the political and military initiative at all cost. The concept of seizing the initiative is not new, and it was even an integral part of Mao Zedong’s war strategy. A recent article in Xinhua by Li Duaguang, a professor at the National Defense University, expounded further on war control by stating that “by preparing for war, one can curb war.” This pull towards seizing the initiative could make Chinese leadership lean too far forward on the side of miscalculation and error. Regrettably, there also has been a dearth of current Chinese discussion on these two principles, so it is difficult to assess Chinese intent in the cyber realm.

Yet, Chinese media reports have filled some of the void with regards to ROE(交战规则 jiaozhan guize). Despite a lack of battle-tested ROE experience, China has linked ROE with cyber warfare and basically has asserted that the United States lacks a legal basis for any unilateral cyber rules of engagement of its own. This is because the Chinese fear that unilateral action by the United States, such as establishing a cyber ROE, would set the stage for future U.S. preemptive action in anticipation of a cyber attack that could target China.

Cyber in China’s Recent Defense White Paper

These pronouncements come at the heels of China’s recently published defense white paper that publicly promulgates its military’s intentions. “Cyber” is mentioned only twice in the entire paper. China did recognize however, that “changes in the form of war from mechanization to informationization are accelerating,” while “major powers are vigorously developing new and more sophisticated military technologies so as to ensure that they can maintain strategic superiorities in international competition in such areas as . . . cyber space.” China also unequivocally stated in the document that it would “counterattack” if attacked.

Troubling Prospects for U.S.-Chinese Cyber Operations

This is particularly troubling for Chinese and American authorities because it is unclear whether or not they could manage their cyber responses in a measured and proportional way if an unofficial or official outbreak of digital force, intentional or not, were to occur. The severity of this issue is intensified by the lack of official Chinese pronouncements or transparency on their cyber operations. Clandestine cyber units, such as the PLA-sponsored Unit 61398 in Shanghai, operate with destructive global reach, adding a layer of uncertainty to an illicit cyber response.

After a thorough analysis of the defense white paper, it is clear that the Chinese leadership is reticent to articulate their intentions in cyber warfare. For defense purposes, this is troublesome for Washington. There is a variety of political and military reasons for this course of action. Perhaps this Chinese reluctance in setting the guidelines of response stems from the lack of pressure from the United States and other nations. In any case, it is doubtful that the leadership would state a different course of action than its professed desire to conduct only defensive and nonaggressive operations.

Despite this, there is a distinct possibility that if push came to shove, Chinese leadership may be ill-equipped to bring its digital forces to bear or reign in these forces in a responsive, proportional manner once they are released. This is precisely because the Chinese lack LOAC doctrine, training and first-hand experience. The Chinese leadership could make a disastrous miscalculation if it were to mismatch capability or response with the objective or threat at hand, thus risking more confusion and escalation. The recent summit in June may be step toward some sort of digital détente or cyberwar norm. The two states should work to form one sooner rather than later, lest they push each other over the digital edge.

#### China perceives US policy – lack of CLARITY makes Chinese invasion of Taiwan inevitable.

Austin & Gady 12 (Greg Austin – phD in International Relations, Vice President for the Worldwide Security Initiative, including a leadership role in the institute's work on cybersecurity, is now a Professorial Fellow. Greg has a 30-year career in international affairs, including senior posts in academia and government., Franz Stefan Gady -- M.A. in Strategic Studies/International Economics from the School of Advanced International Studies, Johns Hopkins University., “CYBER DETENTE BETWEEN THE U.S. AND CHINA: Shaping the Agenda, <http://www.ewi.info/system/files/detente.pdf>)

In sum, China is probably engaged in cyber warfare planning for operations against the United States on a very serious level, and possibly more so than for naval or air combat operations against it. At least in relative terms, China’s cyber warfare capability is probably far more powerful but less lethal than its conventional military capabilities. That suits China enormously in both respects. China’s military strategy is highly defensive, but to defend against U.S. operations against China over Taiwan, China has to rely mainly on unconventional operations, and these include cyber operations as well as psy-ops of the classic kind, including through fifth- column policies.

The scale and intensity of United States offensive cyber operations aimed at China on a day-to–day basis may be lower than vice versa, but without access to classified material it would be hard to characterize the difference between the potential disruptive effects of American and Chinese capabilities. This lack of clarity, in an environment of exceedingly low transparency peculiar to cyberspace compared with land, air, sea and space operations, aggravates insecurities on both sides.

The two most urgent tasks for bilateral discussions would therefore appear to be clarifying the relationship between offensive and defensive cyber operations at the strategic and operational levels of war (the thresholds of response), and clarifying the link between these thresholds and traditional notions of strategic nuclear and conventional force deterrence.

#### Cyber attacks are a prelude to all out kinetic war

Moss 4/19/13 (Trefor, covers Asian politics, defence and security, and was Asia-Pacific Editor at Jane’s Defence Weekly until 2009 The Diplomat- - “Is Cyber War the New Cold War?”, <http://thediplomat.com/2013/04/19/is-cyber-war-the-new-cold-war/3/>)

Cyberspace matters. We know this because governments and militaries around the world are scrambling to control the digital space even as they slash defense spending in other areas, rapidly building up cyber forces with which to defend their own virtual territories and attack those of their rivals.

But we do not yet know how much cyberspace matters, at least in security terms. Is it merely warfare’s new periphery, the theatre for a 21st century Cold War that will be waged unseen, and with practically no real-world consequences? Or is it emerging as the most important battle-space of the information age, the critical domain in which future wars will be won and lost?

For the time being, some states appear quite content to err on the side of boldness when it comes to cyber. This brazen approach to cyber operations – repeated attacks followed by often flimsy denials – almost suggests a view of cyberspace as a parallel universe in which actions do not carry real-world consequences. This would be a risky assumption. The victims of cyber attacks are becoming increasingly sensitive about what they perceive as acts of aggression, and are growing more inclined to retaliate, either legally, virtually, or perhaps even kinetically.

The United States, in particular, appears to have run out of patience with the stream of cyber attacks targeting it from China – Google and The New York Times being just two of the most high-profile victims – and which President Obama has now insisted are at least partly state-sponsored.

Although setting up a cybersecurity working group with China, Washington has also signaled it intends to escalate. U.S. Cyber Command and NSA chief General Keith Alexander signaled this shift of policy gears earlier this month when he told Congress that of 40 new CYBERCOM teams currently being assembled, 13 would be focused on offensive operations. Gen Alexander also gave new insight into CYBERCOM’s operational structure. The command will consist of three groups, he said: one to protect critical infrastructure; a second to support the military’s regional commands; and a third to conduct national offensive operations.

As cyber competition intensifies between the U.S. and China in particular, the international community approaches a crossroads. States might begin to rein in their cyber operations before things get further out of hand, adopt a rules-based system governing cyberspace, and start respecting one another’s virtual sovereignty much as they do one another’s physical sovereignty. Or, if attacks and counter-attacks are left unchecked, cyberspace may become the venue for a new Cold War for the Internet generation. Much as the old Cold War was characterized by indirect conflict involving proxy forces in third-party states, its 21st century reboot might become a story of virtual conflict prosecuted by shadowy actors in the digital realm. And as this undeclared conflict poisons bilateral relations over time, the risk of it spilling over into kinetic hostilities will only grow.

#### Nuclear war

**Glaser, 11** — Professor of Political Science and International Affairs and Director of the Institute for Security and Conflict Studies at the Elliott School of International Affairs at George Washington University (Charles, “Will China's Rise Lead to War?: Why Realism Does Not Mean Pessimism”, Foreign Affairs, March/April 2011, lexis)

ACCOMMODATION ON TAIWAN? THE PROSPECTS for avoiding intense military competition and war may be good, but growth in China's power may nevertheless require some changes in U.S. foreign policy that Washington will find disagreeable--particularly regarding Taiwan. Although it lost control of Taiwan during the Chinese Civil War more than six decades ago, China still considers Taiwan to be part of its homeland, and unification remains a key political goal for Beijing. China has made clear that it will use force if Taiwan declares independence, and much of China's conventional military buildup has been dedicated to increasing its ability to coerce Taiwan and reducing the United States' ability to intervene. Because China places such high value on Taiwan and because the United States and China--whatever they might formally agree to--have such different attitudes regarding the legitimacy of the status quo, the issue poses special dangers and challenges for the U.S.-Chinese relationship, placing it in a different category than Japan or South Korea. **A crisis** over Taiwan **could** fairly **easily escalate to nuclear war**, because each step along the way might well seem rational to the actors involved. Current U.S. policy is designed to reduce the probability that Taiwan will declare independence and to make clear that the United States will not come to Taiwan's aid if it does. Nevertheless, the United States would find itself under pressure to protect Taiwan against any sort of attack, no matter how it originated. Given the different interests and perceptions of the various parties and the limited control Washington has over Taipei's behavior, a crisis could unfold in which the United States found itself following events rather than leading them. Such dangers have been around for decades, but ongoing improvements in China's military capabilities may make Beijing more willing to escalate a Taiwan crisis. In addition to its improved conventional capabilities, China is modernizing its nuclear forces to increase their ability to survive and retaliate following a large-scale U.S. attack. Standard deterrence theory holds that Washington's current ability to destroy most or all of China's nuclear force enhances its bargaining position. China's nuclear modernization might remove that check on Chinese action, leading Beijing to behave more boldly in future crises than it has in past ones. A U.S. attempt to preserve its ability to defend Taiwan, meanwhile, could fuel a conventional and nuclear arms race. Enhancements to U.S. offensive targeting capabilities and strategic ballistic missile defenses might be interpreted by China as a signal of malign U.S. motives, leading to further Chinese military efforts and a general poisoning of U.S.-Chinese relations.

#### LOAC adherence is key --- human survival hangs in the balance

**Weston 91** – Chair of the International and Comparative Law Program @ The University of Iowa [Weston, Burns H., “Logic and Utility of a Lawful United States Foreign Policy,” Transnational Law & Contemporary Problems, Vol. 1, Issue 1 (Spring 1991), pp. 1-14

George Will and others like him are right, of course, that the rhetoric of **international law can be used**, like a double-edged sword, **against the** **U**nited **S**tates **as well as by it**. They are wrong, however, to bemoan this fact-unless, of course, they bemoan the nature of law itself, a process of legitimized politics that, in Benjamin Cardozo's unforgettable words, seeks the "reconciliation of the irreconcilable," the "merger of antitheses," the "synthesis of opposites," in "one unending paradox."12 Though the "real world" often is not a very nice place and though for this reason it sometimes may seem that the responsible pursuit of national interests requires realpolitik policies and practices, **a foreign policy that corresponds with** what most people have in mind when they think of "**The Rule of Law**" (i.e., notions of equality, mutuality, reciprocity, cooperation, and third-party procedure) **is more likely to find itself on the winning side of most political and strategic** **battles than one that does not. Legality**, like honesty**, is generally the best** **policy. It enhances power used under its aegis.**

In the pages following, I suggest six concrete reasons why **the U**nited **S**tates-indeed, all nations- **should take international law seriously**, even¶ when others do not. Viewed in isolation, they may not persuade the hardened realpolitiker. Viewed together, however, they should.

1. Respect for International Law Assists Human Survival

To begin with, **it is not healthy** for people (and for other living things) **to resist** principles of **international law in a world that is bristling with** **more than 50,000 nuclear weapons and other greatly expanded technologies** **of war and mass destruction**. **If** the **history** of the last half century **has** **taught us anything, it is that our present militarily competitive international** **order cannot be expected to prevent large-scale war for very long** (e.g.,Kuwait). **There is**, therefore, **little hope for genuine security**, national or global, **without** a strengthening of the **legal foundations**, bilateral and multilateral, **for** the **nonmilitary**-preferably democratic-**resolution of** **international disputes.** These would include, but not be limited to, the improvement of U.N. peacekeeping and peacemaking opportunities and capabilities, and the improvement of both national and international opportunities and capabilities for legal challenges to coercive foreign policies. 13 Even if other countries do not always follow suit, surely **our** **country and our children's future will be better served if we strive** hard **to build as peaceful and just** a world **society** as we can, and **while we still** **have the chance**. 14 The Soviet Union, home to more than 25,000 nuclear weapons and many newly-awakened nationalisms, faces a world history that demonstrates little support for the proposition that collapsing empires fade quietly. And **in our increasingly "high-tech" world, with military** **research and development fast at work on** atomic guns**,** particle-beam cannons**, and** other space age deviltries **that divert attention from the perils** **of nuclear proliferation, many** regimes in Western Asia and elsewhere **have** **been acquiring** nuclear and other weapons of mass destruction**-and the** **means to deliver them, with frightening ease and speed, to almost anywhere** **on earth.**

In sum, **it is respect** (or lack of respect) **for international law that**, in the end, **will** determine the fate of the Earth. As the late Bill Bishop counseled pithily over two decades ago, "under present conditions **all [States]**¶ **need international law in order to continue to exist together on this planet.**"15 **Rededication to the world rule of law and cooperation in this Age of Nuclear** **Anxiety is not a matter of choice. It is**, quite simply, **a** matter of survival.

2. Respect for International Law Enhances International Stability

Living as we do in the twilight years of the global Middle Ages, characterized by more than 160 separate fiefdoms, each with a monopoly control over the military instrument and each only barely accountable in any formal sense either to each other or to the larger arena in which each operates, it is easy to be seduced by the popular claim that ours is an anarchical world. Such an outlook does not, however, comport with reality. Every hour of every day, ships ply the sea, planes pierce the clouds, and artificial satellites probe outer space. Every hour of every day, communications are transmitted, goods and services traded, and people andthings transported from one country to another. Every hour of every day, transactions are negotiated, resources exploited, and institutions established across national and equivalent frontiers. And in all these respects, the many processes of authoritative and controlling decision that help to regulate such endeavors-what we call international law-are observed rather well on the whole.

On the other hand, **when States bend, twist, or** otherwise show **disrespect** for this ordering force to suit their special interests, **international law**, because **it** is an essentially voluntarist process of decision that is seriously lacking in centralized command and enforcement structures, **quickly loses** **its otherwise stabilizing influence**. The kidnapping of sixty-two Americans at the U.S. Embassy in Teheran in 1979, for example, demonstrates well the fundamental instability that can flow from a failure or refusal to abide by international law. Without, in this instance, a commitment to the basic rules of diplomatic protection, diplomacy ceased to exist and respectable discourse became impossible. Without a commitment to the world rule of law there could be no assurance of inter-governmental stability.

Of course, States-especially the major powers-are perfectly capable of unilaterally resisting the doctrines, principles, and rules of international law without necessarily feeling directly the destabilizing impact that their noncompliance ultimately has on the wider structure of international law and order itself. The probability of being formally punished for violating international law is usually so slim that foreign policy strategists commonly give little or no weight to the cost of decision-making marked by dubious legality.

However, the increasingly interdependent and interpenetrating character of today's world is of such magnitude and complexity that no nation, least of all the United States, can sensibly afford to insist upon its own independence of action without simultaneously threatening its own ultimate good and the ultimate good of others, and potentially in very fundamental ways. Though not understood by most Americans, it is in fact the United States "which stands to lose the most in a state of world anarchy." 16 Because the United States and its citizens have such wide-ranging and far-flung international interests, we urgently need a stable, predictable environment of international legal rules and procedures that can help to secure those interests on a cooperative basis worldwide. It is not in the first instance our freedom of action that should be our concern when we refuse to commit to the world rule of law, but rather, the stability of our world public order itself.

3. Respect for International Law Advances Our Geopolitical Interests

Allowing principles of international law and multilateral cooperation to inform our foreign policy also serves our geopolitical interests, especially our long-term geopolitical interests. For example, in contrast to our recent hegemonic warmongering in Grenada, Nicaragua, and Panama, a record of faithful adherence to the principle of nonintervention and to the right to self-determination would have helped, politically at least, to neutralize the Israelis in southern Lebanon and the Occupied Territories, the Soviets in the Baltics, and the Iraqis in Kuwait. As the late L.F.E. Goldie observed a number of years ago: "Obedience to law... is not only a categorical value but also a prudential one." 1'7 My colleague and former Prime Minister of New Zealand Sir Geoffrey W. R. Palmer, referring to the need for strict compliance with arms control and disarmament treaties, once put it this way: "[I]s it possible on the one hand to look to international law to provide essential security guarantees, while on the other hand, in other areas, the right is quietly being reserved to undermine, ignore and indeed walk away from the rule of law in international affairs?"18

In recent years, however, during the Reagan presidency especially, the United States has come before the world community more to bury international law than to praise it. Selectively displaying its military strength to the general disregard of international law, it has chosen, at least when the risks have been low, to advance several broadly defined but narrowly determined national interests:

(1) demonstrating American will to act with decisiveness and reinforcing deterrence against the Soviet Union in the Third World; (2) displaying the ability of U.S. armed forces to defend American and allied interests; (3) inducing countries that challenge the U.S. to cease and desist; and (4) enhancing in the broadest terms an international perception of the U.S. as the great world power. 19

But to favor such special interests over the common interest of a world rule of law is to shoot ourselves in the geopolitical foot-perhaps not always, but more often than is commonly realized. It gets us into quagmires from which it is hard to extricate ourselves and it subverts our ability to ensure in other settings that other governments, especially our adversaries, will fulfill their obligations under international law that are in our interest for them to fulfill.

The point is depressingly simple to illustrate. If we can unilaterally reinterpret and abrogate an arms control treaty with the Soviet Union,20 why cannot the Soviets do the same with us? If we can excuse the kidnapping and killing of innocent civilians by the Nicaraguan Contras because they were "freedom fighters,"21 what right do we have to condemn the Palestinians or Shiites for doing the same thing in Lebanon? If we can ignore a World Court decision relative to the human rights violations we encouraged in Nicaragua,2 how can we complain when Iran ignores a World Court decision relative to the taking of U.S. hostages in Teheran?2 If we can claim the right to seize fugitives from abroad,2 what logic compels our right to object when the Iranian Majlis (parliament) approves legislation authorizing Iranian officials to arrest Americans anywhere in the world for violations of Iranian law?25 If we can intercept a civilian aircraft over the Mediterranean on the grounds that it appears to threaten our national security interests, 26 what is to stop the Soviet Union from doing the same thing over the Pacific for the same reason?27 If we can condone a U.S. military raid upon an ambassadorial residence in Panama despite our obligations under the 1961 Vienna Convention on Diplomatic Relations, how can we complain when Iranian students seize a U.S. embassy protected by the 1961 Vienna Convention on Diplomatic Relations? 28 And so forth.

Such partisan uses of international law are illustrative of what, during the 1980s, has been referred to as the "Reagan Corollary" of international law-which is to claim a right "to pressure the international legal system into changing in a manner beneficial to United States interests."9 However, such uses do not, in the end, correspond to our long-term national interest of ensuring that other governments in other settings fulfill their obligations under international law. Were every nation to adopt this Reagan Corollary, a perverted interpretation of international doctrines, principles, and rules would become the standard practice and the international legal system would quickly disintegrate into a system of retributive justice extremely unsafe for the geopolitical interests of even the most powerful States.

Thus, if the United States wants to insist upon compliance with international law to protect American interests, it will be to its advantage to obey international law, even when its application proves inconvenient. If we want meaningful international law to be available when we find it useful, we must respect it even when we do not.

4. Respect for International Law Promotes Policy Efficacy

**A failure to adhere to international law-in particular the prohibitions** **against the threat and use of nondefensive force** and the admonitions to¶ promote and safeguard human rights**-tends** also **to be counterproductive**, hence not very efficacious. **While militarism** and support of repressive regimes to the disregard of international law **may sometimes yield tactical victories that are viscerally pleasing in the short-run, they rarely achieve** **strategically satisfying gains, to say nothing of justice, over the long-run**. Consider, for example, the Reagan administration's decision, pursuant to what came to be known as the "Schultz Doctrine," to fight terrorism with American-sponsored counterterrorism, 30 the ultimate denouement of which was the sordid Iran-Contra affair. In keeping with this decision, the United States provided Israel with diplomatic, financial, and material support of Israel's illegal invasion of southern Lebanon in 1982,31 in violation of common Article 1 of the four Geneva Conventions on the laws of war of 194932 and involving the killing of more than 20,000 people (at a time when, ironically, Palestinian terrorist attacks against American persons and property had been in decline). Not surprisingly, the victims of the invasion and their sympathizers held Washington responsible, in conjunction with Israel, for the atrocities committed by the Israeli army and the Lebanese Phalange militia against Palestinian civilians in the Sabra and Shatilla refugee camps in southern Lebanon.33 American interests immediately began to experience a pronounced increase in terrorist attacks-via airplane hijackings, kidnappings, assassinations, bombings, and other paramilitary activitiesfrom Palestinian, Shiite, and other groups throughout the Middle East.

Consider also the refusal of the United States to accept the jurisdiction of the International Court of Justice in the case brought by Nicaragua in April 1985 in protest of Washington's illegal assistance to, and support of, the Contra guerrillas against Nicaragua's democratically elected Sandinista government.34 Instead of making its substantive case before the Court, the United States contended that what it considered to be an issue of Western Hemispheric security was not properly for the World Court to decide and that, in any event, there was no reason for the United States to submit to the Court's jurisdiction when, over the years, the Soviet Union had consistently refused to do so. 35 As one sensitive observer put it, "[this] argument was politically attractive domestically, but it eroded the stature of the World Court that American values had once tried to build up."36 More such examples could easily be recounted. It might be asked, for example, whether our aiding and abetting the assassination of Chile's Allende or our legally dubious support of the Shah of Iran really did serve our long-term national interest. And the same might be asked, as well, of the Iran-Contra affair and of our legally questionable assistance to Saddam Hussein during and after the Iran-Iraq war.

But the efficacy argument is perhaps best demonstrated by noting the large-scale political support that was extended to Washington, internationally as well as nationally, during at least the early months of the 1990-91 Persian Gulf crisis when the United States pressed hard for economic sanctions against Iraq that were, it can be said, not only timely and measured but in keeping with the collective security system authorized in San Francisco in 1945.37 Adherence to the principles and procedures of international law, President Bush discovered, was essential to gaining the world's support to force Iraq's hand. Lawful foreign policies are consensusbuilding policies-politically pragmatic or efficient policies-and they are useful even to a superpower.

To put it all another way, **we abandoned lynching parties on the western** **frontier not only because they turned into orgies of wasteful bloodlust but** **also because they simply did not stop horse thieves. International law** **violations, like violations of law in general, have a dubious pragmatic record** **at best.**

5. Respect for International Law Safeguards Domestic Society

Disregard of international law and institutions tends to be self destructive as well as destructive of international order. The consequences of our unilateral and disproportionate uses of force in Vietnam should be proof enough. Over a decade and a half later, as such movies as Platoon, Born on the Fourth of July, and Casualties of War alone bear witness, we are still licking the socioeconomic, political, and ethical wounds. Though not always immediately apparent or discernible, international law violations and "go-it- alone" policies that fail to show a decent respect for the rights and opinions of others invariably corrode our core essence, diminishing our national integrity and threatening even our individual liberties. As Professor Bilder has asked, can we legitimately expect to separate the standards that govern the way our government operates internationally from those that govern it internally? 8 If we tell our elected officials that it's okay to act illegally, corruptly, or brutally abroad, can we be completely sure that they will really listen when we tell them that they should not act that way at home? If we say to the Secretary of State, the CIA, or the National Security Council that it's okay to bend the law a little because we do not like another country's ideology, can we rightfully expect that the Attorney General or the FBI will not bend the law a little when it comes to those of our citizens who do not share the government's ideology in domestic affairs?

In other words, when we show contempt for international law and cooperation, we badly damage our sense of national self-respect and purpose and, in so doing, invite civil unrest. In addition to the widespread civil disobedience that characterized the era of the legally problematic Vietnam War, we may note the popular protests that, more recently, accompanied Washington's extraordinary build-up of offensive nuclear weapons, its policy of "constructive engagement" with apartheid South Africa, and its military adventurism in Central America.3 9 One of the wondrous things about our country-deep-rooted in our ideology even if not always borne out in practice-is our commitment to decent behavior and the rule of law. From our very beginnings, we have officially embraced the notion of a Higher Law based upon "principles of right and justice that prevail because of their own obvious merit:"40 liberty, equality, participation, and due process. And since at least the turn of the century, cognate international principles have been added: the self-determination of peoples, the sovereign equality of States, respect for international law and organization, and the peaceful settlement of international disputes. So, when our government resorts to¶ foreign policy plots and maneuvers of a Machiavellian sort that sacrifice or otherwise diminish these principles, the spillover into the domestic arena is predictable. The government soon loses the support of the people.

Our Founding Fathers established that ours is a society of laws, not of men. To most of us, therefore, "standing tall" in the global community does not mean being the toughest kid on the block, pushing other countries around and breaking our promises as we once accused the Soviet Union of doing, but acting humanely and honorably. Intuitively we know that it is necessary for us to uphold the rule of law abroad in order to uphold it at home. Intuitively we know that "[t]he two are inextricably connected." 41 Intuitively we know that a double standard erodes our claim to moral leadership in the international community.42

6. Respect for International Law Ennobles Our National Rectitude

As evidenced by the U.N. General Assembly's declaration of the 1990s as the "Decade of International Law,"43 there is a growing realization that an effective system of international law is fundamental to the achievement¶ of a world public order of human dignity. It is essential to peace and security, and it is indispensable for just solutions to the many complex and urgent problems that otherwise currently make up the human agenda.

International law provides, potentially, the most durable framework for undertaking cooperative action toward the abolition of war, the promotion of human rights, the ending of mass poverty, and the creation of a sustainable global environment. Its progressive evolution, in keeping with Article 28 of the Universal Declaration of Human Rights ("Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized"),4 is the key to all that is right and good.

To insist upon respect for international law and cooperation is, thus, the morally correct thing to do, and for this reason alone it is in our longterm best interest. Rather than throw our weight around as if at some shootout at the OK Corral, the United States should reaffirm its commitment to a law-oriented foreign policy and, from this posture, through carefully planned and diligently executed diplomatic strategy, regain a once assumed (even if not always demonstrated) moral stature among the family of nations-the "American difference," as President Reagan used to call it. Along the way, discovering that it would thus gain the upper hand in the global competition for hearts and minds, including the enthusiastic support of otherwise doubting allies, the United States would also discover that commitment to international law and cooperation is fundamentally a matter of self-interest. Our reputation as a law-abiding nation, one that genuinely honors the world rule of law in practice, is a vital asset, strongly affecting our ability to win friends and influence people. It is a reputation that cannot-must not-be squandered.

Most importantly, however, the United States has an especial obligation in this regard. Quite simply, the size of our economy, the sophistication of our technology, the ubiquity of our investments, and the power of our arsenals make us so globally consequential that the acts and omissions of our government transmit a powerful and usually lasting message. Like it or not, our words and our deeds count heavily in the normative, institutional, and procedural development of world affairs. 45 And this establishes for us, a professedly democratic and peace-loving country, an historically unique moral responsibility. Pg. 4-13 // AT: K

#### The plan solves --- eyes are on the US – our adherence to LOAC is modeled globally. OCO ambiguity is the biggest internal link

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>)

Evolving customary law. This approach also accommodates the reality that how the U.S. chooses to use its armed forces will significantly influence the development of customary international law.

As the label implies, customary law can evolve depending on the accepted conduct of major nations like the United States. The real-world practice of the United States in adapting the use of its military to the new challenges raised by computer warfare will (and should) help clarify the accepted customs of war in areas where the limits are not clearly established today.

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.

But there will be gray areas in the middle. Thus, it’s far less clear that a computer assault that’s limited to deleting or corrupting data or temporarily disabling or disrupting a computer network or some specific equipment associated with the network in a way that’s not life threatening or widely destructive should be considered a use of force justifying military retaliation, even if the network belongs to the military or another government agency.

This was the case with the “distributed denial of service” attacks experienced by Estonia in 2007, which severely disrupted the country’s banking and communications systems. Suspecting that Russia was behind it, Estonia suggested that NATO declare that Estonia’s sovereignty had been attacked, which would have triggered the collective self-defense article of the NATO Treaty, but that suggestion was rebuffed on the ground that a cyber attack is not a clear military action.12

There’s an echo of that reasoning in Article 41 of the U.N. Charter, which says that a “complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications” is not a “measure . . . involving armed force.”

And what about Stuxnet? As I understand it from public reports, Stuxnet was a computer worm that found its way into the systems controlling Iran’s nuclear program and gave faulty commands causing the destruction of the centrifuges used for enriching uranium. Suppose President Ahmadinejad claimed that Israel was behind the Stuxnet worm and claimed that Stuxnet constituted an armed attack on Iran that justified a military response against Israel. I suspect the United States would disagree.

At the same time, when it comes to a cyber attack directed against U.S. computer systems, I certainly want the President to have leeway in determining whether or not to treat the attack as a use of force that supports military retaliation. Making such judgments is a traditional power exercised by the President, and I think he retains that leeway.

Similarly, I submit, it’s not clearly established that a cyber attack aimed at disrupting a server or Web site located in a neutral country or in a country outside a theater of open hostilities would be a violation of that country’s neutrality.

The server might be a valid military target because it’s being used for the communications or command and control of the enemy fighters in the area of hostilities (after all, al Qaeda regularly uses the Internet in planning and ordering operations). The server might have no connection to the host country’s military, government, or critical infrastructure, and it might be readily targeted for a computer attack without inflicting widespread damage on unrelated systems used for civilian purposes.

Such a focused cyber operation — with little physical impact beyond the destruction of data or the crippling of a server — is very different from the kind of physical violation of territory — such as a conventional troop incursion or a kinetic bombing raid — that we ordinarily think of as constituting an affront to neutrality.13

Although every server has a physical location, the Internet is not segmented along national borders, and the enemy may gain greater tactical advantage from a server hosted half way around the world than from one located right in the middle of hostilities.

The targeting of a server in a third country may well raise significant diplomatic difficulties (and I wouldn’t minimize those), but I don’t think the law-of-war principle of neutrality categorically precludes the President from authorizing such an operation by an execute order to Cyber Command.

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.

#### Prior notification is key to check executive action

Healey and Wilson 13- Jason Healey is the director of the Cyber Statecraft Initiative at the Atlantic Council. A.J. Wilson is a visiting fellow at the

Atlantic Council (Jason, and A.J. "Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain," Atlantic Council Cyber Statecraft Initiative, February 2013)

The administration’s interpretation of “hostilities” should go beyond the risk to American lives to have more logical consistency with cyberspace as a warfighting domain, like the land, sea, air, and space. Table 1 shows a more consistent vision of “logical” presence that may be useful in determining when US armed forces have been sufficiently “introduced into foreign territory [etc.]” or “into hostilities” to trigger the WPR’s reporting and/or withdrawal requirements. Involving the legislative branch in cyber conflict decisionmaking in this gradated manner—which, as the table shows, is easily transposed to the physical realm—need be neither unreasonable nor disproportionate. After all, transparency is required of those who govern open societies. Especially in this information age, we as citizens are right to expect it. The United States needs the capacity to carry out offensive operations in cyberspace, but the Executive branch must accept that the same checks and balances that apply to physical hostilities apply also to cyber conflict. Future cyber attacks may have the ability to destroy or degrade an adversary’s critical infrastructure, cripple its economy, and seriously compromise its ability to defend itself. They may cause physical injury or even death. Their strategic consequences—not to mention their fiscal and economic costs—may be just as significant as a physical attack. This is, indeed, why the Pentagon has rightly decided to treat cyberspace as the fifth domain. But it must, by the same token, accept that logical forms of presence matter in cyberspace in the same way that physical forms matter in the kinetic space, and therefore it must apply the War Powers Resolution accordingly. The Founding Fathers could not have imagined a world in which weapons made of information travel around the globe at the speed of light; but they did know how to distribute power to encourage restraint in its application. Even in cyberspace, there is a voice for both branches.

### 1AC Deterrence Advantage

#### Advantage 2 Is deterrence

#### No OCO regulations now that creates a ZONE OF TWILIGHT around inter branch relations.

Healey and Wilson 13- Jason Healey is the director of the Cyber Statecraft Initiative at the Atlantic Council. A.J. Wilson is a visiting fellow at the

Atlantic Council (Jason, and A.J. "Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain," Atlantic Council Cyber Statecraft Initiative, February 2013)

Even as the Obama administration is pushing Congress to pass strong legislation to avert a “Cyber Pearl Harbor,” it is insisting Congress should have little oversight in when the military engages in cyber conflicts. Cyber conflicts are too new and affect the American private sector too much to leave to the administration alone. Despite the administration’s actions to the contrary, if the Department of Defense’s own policies mean what they say, then Congress should have a voice in cyber operations. Since 1973, Congress has claimed the right to terminate military engagements under the War Powers Resolution (WPR). Beginning with Richard Nixon, whose veto had to be overridden to pass the WPR, presidents have typically regarded its provisions as unconstitutional limits on the authority of the commander-in-chief. The Obama administration has taken a slightly different tack, however, accepting “that Congress has powers to regulate and terminate uses of force, and that the [War Powers Resolution] plays an important role in promoting interbranch dialogue and deliberation on these critical matters,” but is seeking nonetheless to limit its application to certain types of conflicts.1 All presidents since Nixon’s successor, Gerald Ford, have submitted reports consistent with the resolution’s terms, although using varying thresholds.2 Under the WPR, the president is obliged to report to Congress within forty-eight hours of: [A]ny case in which United States Armed Forces are introduced—(1) into hostilities or situations where imminent involvement in hostilities is clearly indicated by the circumstances; (2) into the territory, airspace or waters of a foreign nation...; or (3) in numbers which substantially enlarge United States Armed Forces equipped for combat already located in a foreign nation. Situations falling within items (2) or (3) trigger only this reporting requirement. However, in the circumstances contemplated by item (1), the president must, in addition to satisfying the reporting obligation (and absent congressional approval of his actions), terminate the use of United States armed forces within sixty days. A further thirty days are available if the president certifies that only with such an extension can the forces committed be safely withdrawn. In other words, the president, as commander-in-chief, may commit forces for a maximum of ninety days after reporting without the approval of Congress. The text of the War Powers Resolution has four operative terms—none of which is defined—each critical to understanding the requirement set by Congress: “Armed Forces,” “Hostilities,” “Territory,” and “Introduction.” With regard to US operations over Libya, Obama administration officials sought to limit the scope of the WPR by adopting a narrow approach to the definition of “hostilities.” Initially, the president reported the Libyan engagement to Congress within the forty-eight hour window, describing his report as “part of my efforts to keep the Congress fully informed, consistent with the War Powers Resolution.”3 As noted, sixty days after the submission of his initial report the president is required either to pull the forces out or to certify that a thirty-day extension is necessary in order to withdraw them safely. When that deadline arrived with respect to Libya, Obama did neither of these things. Instead, on May 20, 2011, the sixtieth day, he sent another letter soliciting congressional support for the deployment. This second letter did not mention the WPR. 4 Subsequently, a few days before the ninety day outer limit of the WPR, the president provided to Congress a “supplemental consolidated report . . . consistent with the War Powers Resolution,” which reported on a number of ongoing deployments around the world, including the one in Libya.5 At the same time, the Pentagon and State Department sent congressional leaders a report with a legal analysis section justifying the non-application of the WPR, but also calling again for a congressional resolution supporting the war.6 Later, State Department legal adviser Harold Koh expanded upon this analysis in testimony before the Senate Foreign Relations Committee, arguing that operations in Libya should not be considered relevant “hostilities” because there was no chance of US casualties, limited risk of escalation, no “active exchanges of fire,” and only “modest” levels of violence. It is apparent that in defining “hostilities” the administration’s focus is on kinetic operations passing a certain threshold of intensity: while there is no detailed indication in Koh’s testimony of what weight is to be accorded to each of the factors he enumerates, the overriding emphasis is on physical risk to US personnel. As Koh himself said, “we in no way advocate a legal theory that is indifferent to the loss of non-American lives. But . . . the Congress that adopted the War Powers Resolution was principally concerned with the safety of US forces.” The consequences for opposing forces, and for the foreign relations of the United States, matter less—or not at all. Libyan units were decimated by NATO airstrikes; indeed, it was a US strike that initially hit Muammar Gaddafi’s convoy in October 2011, leading directly to his capture and extra-legal execution. Significantly, though, the strike came not from an F-16 but from a pilotless Predator drone flown from a base in Nevada.8 The significance of this for present purposes is that, apparently, even an operation targeting a foreign head of state does not count as “hostilities,” provided there is no involvement of US troops. This is not a new view; indeed, Koh relied heavily on a memorandum from his predecessor in the Ford administration, which defined “hostilities” as “a situation in which units of the US armed forces are actively engaged in exchanges of fire with opposing units of hostile forces.” This formulation would presumably exclude drone attacks and, most importantly for present purposes, remote cyber operations.7As remote war-fighting technology becomes ever more capable, reliable, and ubiquitous, the administration’s restrictive definition of “hostilities” could open up a huge area of unchecked executive power. For example, neither the current administration nor its immediate predecessor has reported under the WPR any of the hundreds of remote drone strikes carried out in Pakistan, Yemen, or Somalia over the past decade. Likewise, the Pentagon has made clear its position that other forms of remote warfare, cyber operations, are also not covered by the WPR.

#### The US has no cyber deterrence strategy. We’re shooting in the dark. INTER-BRANCH CONSENSUS is critical.

Kramer et. al 12 (Franklin D. Kramer is a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He served as the assistant secretary of defense for international security affairs from 1996 to 2001. Stuart H. Starr is also a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He concurrently serves as the president of the Barcroft Research Institute. Larry Wentz is a senior research fellow in the Center for Technology and National Security Policy at the National Defense University., “Cyberpower and National Security”, p. 318)

No cyber deterrence strategy can hope to be airtight to prevent all minorattacks. However, a strategy can increase the chances that major cyber attacks can be prevented; this could protect the United States and its allies not onlyfrom a single major attack but also from serial cyber aggressions and resultingdamage. A worthwhile goal of a cyber deterrence strategy would be to transformmedium-sized attacks into low-probability events and to provide practically 100 percent deterrence of major attacks.

A cyber deterrence strategy could contribute to other key defense activitiesand goals, including assurance of allies, dissuasion, and readiness to defeat adversaries in the event of actual combat. The goal of dissuading adversaries is crucially important. Thus far, the United States has not been noticeably forceful in stating its intentions to deter major cyber attacks and, if necessary, to respond to them with decisive force employing multiple instruments of power. Meanwhile, several countries and terrorist groups are reportedly developing cyber attackcapabilities. Dissuasion of such activities is not an easy task: it requires investment in technical capabilities as well as building an internal consensus to employ these capabilities. If some of these actors can be dissuaded from entering into cybercompetition with the United States and its allies, the dangers of actual cyber aggression will diminish.

How would a cyber deterrence strategy operate, and how can its potentialeffectiveness be judged? Deterrence depends on the capacity of the United States to project an image of resolve, willpower, and capability in sufficient strength to convince a potential adversary to refrain from activities that threaten U.S.and allied interests. As recent experience shows, deterrence can be especiallydifficult in the face of adversaries who are inclined to challenge the United Statesand otherwise take dangerous risks. In cases of failure, deterrence might well have been sound in theory but not carried out effectively enough to work. Theaggressions of Saddam Hussein, Slobodan Milosevic, and al Qaeda might not have been carried out had these actors been convinced that the United Stateswould respond with massive military force. These aggressions resulted because of a failure to communicate U.S. willpower and resolve, not because the attackers were wholly oblivious to any sense of restraint or self-preservation, nor because the logic of deterrence had lost its relevance.

#### Deterrence works by changing the incentive model of adversaries.

Kramer et. al 12 (Franklin D. Kramer is a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He served as the assistant secretary of defense for international security affairs from 1996 to 2001. Stuart H. Starr is also a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He concurrently serves as the president of the Barcroft Research Institute. Larry Wentz is a senior research fellow in the Center for Technology and National Security Policy at the National Defense University., “Cyberpower and National Security”, p. 318)

Ends, Ways, and Means

The goal of a cyber deterrence strategy would be to influence an adversary’sdecisionmaking calculus so decisively that it will not launch cyber attacks againstthe United States, its military forces, or its allies. Coordinated actions reduce thechances for attacker success, so that the dangers, costs, risks, and uncertainties of a cyber attack are perceived to outweigh any expected success, benefits, or rewards. In the case of an adversary who seeks to use threats of cyber attacks, or actual attacks, to coerce the United States into conduct that would serve its larger interests and goals, a cyber deterrence strategy will work if the adversaryjudges that this attempted coercion would not succeed and that the attack would provoke U.S. retaliation, resulting in a net strategic setback for the would-beattacker. For example, if Iran were to contemplate cyber attacks to try to coerce the United States into making political concessions in the Persian Gulf andMiddle East, it might be deterred from this course if its decisionmakers were to judge that the cyber attack would not physically succeed in inflicting the desired damage; that even if the attack succeeded, the United States would not make the desired concessions; or that the United States would be likely to retaliate in ways that inflict unacceptable damage on Iran in return, in the cyber realm or elsewhere.

The same strategic calculus applies to Chinese use of cyber threats andattacks, as well as actions by other plausible adversaries in the cyber domain.Potential U.S. counteractions in such situations are encapsulated in the three principal ways of pursuing deterrence articulated in the JOC model: deterrence by denying benefits, deterrence by imposing costs, and deterrence by offeringincentives for adversary restraint.

Deterrence by denying benefits entails credibly threatening to deprive the attacker of the benefits or gains being sought: convincing it that a cyber attack will not achieve its goals. Deterrence by imposing costs entails credibly threatening to impose costs, losses, and risks that are too painful to accept, thus convincing theadversary that punishment would outweigh any expected successes. Deterrence by encouraging restraint means convincing the adversary that not attacking will result in an acceptable, attractive outcome.

#### Cyber war causes extinction.

Rothkopf 11 (David, Visiting Scholar at Carnegie, “Where Fukushima meets Stuxnet: The growing threat of cyber war”, 3/17/11, <http://rothkopf.foreignpolicy.com/posts/2011/03/17/where_fukushima_meets_stuxnet_the_growing_threat_of_cyber_war>)

The Japanese nuclear crisis, though still unfolding, may, in a way, already be yesterday's news. For a peek at tomorrow's, review the testimony of General Keith Alexander, head of U.S. Cyber Command. Testifying before Congress this week and seeking support to pump up his agency budget, the general argued that all future conflicts would involve cyber warfare tactics and that the U.S. was ill-equipped to defend itself against them.

Alexander said, "We are finding that we do not have the capacity to do everything we need to accomplish. To put it bluntly, we are very thin, and a crisis would quickly stress our cyber forces. ... This is not a hypothetical danger."

The way to look at this story is to link in your mind the Stuxnet revelations about the reportedly U.S. and Israeli-led cyber attacks on the Iranian nuclear enrichment facility at Natanz and the calamities at the Fukushima power facilities over the past week. While seemingly unconnected, the stories together speak to the before and after of what cyber conflict may look like. Enemies will be able to target one another's critical infrastructure as was done by the U.S. and Israeli team (likely working with British and German assistance) targeting the Iranian program and burrowing into their operating systems, they will seek to produce malfunctions that bring economies to their knees, put societies in the dark, or undercut national defenses.

Those infrastructures might well be nuclear power systems and the results could be akin to what we are seeing in Japan. (Although one power company executive yesterday joked to me that many plants in the U.S. would be safe because the technology they use is so old that software hardly plays any role in it at all. This hints at a bit of a blessing and a curse in the fractured U.S. power system: it's decentralized which makes it hard to target overall but security is left to many power companies that lack the sophistication or resources to anticipate, prepare for or manage the growing threats.)

Importantly, not only does the apparent success of the Stuxnet worm demonstrate that such approaches are now in play but it may just be the tip of the iceberg. I remember over a decade ago speaking to one of the top U.S. cyber defenders who noted that even during the late 90s banks were losing millions and millions every year to cyber theft -- only they didn't want to report it because they felt it would spook customers. (Yes.) Recently, we have seen significant market glitches worldwide that could easily have been caused by interventions rather than just malfunctions. A couple years back I participated in a scenario at Davos in which just such a manipulation of market data was simulated and the conclusion was it wouldn't take much to undermine confidence in the markets and perhaps even force traders to move to paper trading or other venues until it was restored. It wouldn't even have to be a real cyber intrusion -- just the perception that one might have happened.

What makes the nuclear threat so unsettling to many is that it is invisible. It shares this with the cyber threat. But the cyber attacks have other dimensions that suggest that General Alexander is not just trying to beef up his agency's bank accounts with his description of how future warfare will always involve a cyber component. Not only are they invisible but it is hard to detect who has launched them, so hard, in fact, that one can imagine future tense international relationships in which opposing sides were constantly, quietly, engaging in an undeclared but damaging "non-war," something cooler than a Cold War because it is stripped of rhetoric and cloaked in deniability, but which might be much more damaging. While there is still ongoing debate about the exact definition of cyber warfare there is a growing consensus that the threats posed by both state-sponsored and non-state actors to power grids, telecom systems, water supplies, transport systems and computer networks are reaching critical levels. This is the deeply unsettling situation effectively framed by General Alexander in his testimony and rather than having been obscured by this week's news it should only have been amplified by it.

#### Cyber-attacks will destroy US space assets

**Donahue, 10** – USAF Major (Jack, “CATASTROPHE ON THE HORIZON: A SCENARIO-BASED FUTURE EFFECT OF ORBITAL SPACE DEBRIS,” https://www.afresearch.org/skins/rims/q\_mod\_be0e99f3-fc56-4ccb-8dfe-670c0822a153/q\_act\_downloadpaper/q\_obj\_af691818-359f-4999-be24-f88ca154bd94/display.aspx?rs=enginespage)

Another unpredictable driving force that needs to be considered is adversary exploitation of space vulnerabilities via the cyber domain. Through cyberspace, enemies (both state and non-state actors) will target industry, academia, government, as well as the military in the air, land, maritime, and space domains.86 One of the easiest ways to disrupt, deny, degrade, or destroy the utility of space assets is to attack or sabotage the associated ground segments through cyberspace.87 The ground segment includes telemetry, tracking, and commanding of space assets and space-launch functions. Ground stations are an **extremely critical piece** of a satellites continued operation. However, many satellite tracking and control stations are lightly guarded and many satellite communications, launch, data reception, and control facilities are described in numerous open-source materials making the ground segment extremely vulnerable to cyber attack.88 An attack on a fixed ground facility can stop data transmission, render launch facilities unusable, and prevent control of satellites.89 Thus, rendering affected orbiting satellites inoperative from the communication disruption and creating a risk to other active satellites and a potential for additional orbital debris. A single incident or a small number of incidents could significantly impact space systems for years.90

#### Loss of space assets risks miscalculation --- unique escalation to nuclear war

**Tyson 07** (Rhianna Tyson, Program Officer of the Global Security Institute, “Advancing a Cooperative Security Regime in Outer Space,” Global Security Institute, May 2007, http://www.worldacademy.org/files/Advancing%20a%20Cooperative%20Security%20Regime%20in%20Outer%20Space.pdf)

Beyond the severe economic repercussions resulting from disrupted commercial satellite communications, hostile actions in space can result in grave security threats, especially in times of war. Militaries rely on satellites for monitoring of and communication with troops on the ground. If a military satellite was deceived, **disrupted,** denied, **degraded** or destroyed, commanders lose their communication capabilities, resulting in **mounting tensions** and an escalation of conflict. A worst-case scenario could involve inadvertent **use of nuclear weapons;** without satellite-enabled monitoring capability in a time of tension, or, if early warning systems give a false reading of an attack, governments may **resort to using nuclear weapons.**

#### Independently undermines the balance of deterrence and leads to global preemptive aggression

**Burke, 6** – Lt Col, USAF, command space professional with operational experience in missile operations, space surveillance, space control, missile warning, and command and control (Alan, “SPACE THREAT WARNING: FOUNDATION FOR SPACE SUPERIORITY, AVOIDING A SPACE PEARL HARBOR,” https://www.afresearch.org/skins/RIMS/display.aspx?moduleid=be0e99f3-fc56-4ccb-8dfe-670c0822a153&mode=user&action=researchproject&objectid=07acf878-3a5f-4a2c-8259-4a34c0717e9b)

The erosion of the US ability to execute the space threat warning mission has serious implications for US national security to include: the loss of a key early warning indicator of an attack on the US homeland; the loss of space capabilities which would degrade US warfighting effectiveness; the preventable loss of critical high-value satellites, facilities or services; the increased possibility that adversaries could develop new weapons or covertly conduct probing attacks on US space systems; and the lack of a credible means to execute stated US policy in response to an attack against space assets. One of the most serious impacts of the failure to develop or execute a reliable space threat warning and attack verification system is the loss of a key early warning indicator of an attack on the US homeland or an attack that is part of a major regional action by a near-peer adversary such as an attack on Taiwan by the Chinese mainland. The Japanese attack on Pearl Harbor, whose goal was the destruction of the Pacific Fleet, was not done as an isolated act, but as part of the start of a larger campaign to establish a Japanese Pacific sphere of influence which included the forceful acquisition of US territories. At this time, the Pacific Fleet was viewed as a US center of gravity whose destruction would enable Japan to achieve regional domination and discourage future US intervention. Today, our space-based assets may represent the equivalent of the WWII Pacific Fleet. Further, other nations have stated they view the US reliance on space as a potential Achilles ’ heel and a center of gravity whose destruction or disruption is critical to future military success against the US.44 Although a major attack on the US is not likely, the loss of US space-based early warning capability and ground-based missile warning radars could **undermine** nuclear **deterrence** strategy resulting in a **devastating miscalculation** that the US was vulnerable to a **nuclear first strike.** The **perception** that US space capabilities are vulnerable to a surprise attack also **weakens** conventional **deterrence.** In the case of a US-China conflict over Taiwan, the Chinese might seek to disrupt or destroy regional space capabilities as part of a delaying strategy to deny US forces access to the region until their military operations were well underway, making the Chinese **takeover of Taiwan a fait accompli.**45 A successful Pearl Harbor-type attack on US space assets would degrade US fighting effectiveness. Today, space represents the ultimate high ground and it is unlikely that a nation, whose military ambitions might provoke US involvement, will willingly cede that high ground. The level of battlespace awareness space-based platforms provide makes any attack using large massed forces difficult to accomplish. The ability to neutralize these platforms would improve the circumstances required to gain a strategic advantage over US and allied forces. As General Lord stated in his Congressional testimony: “A resourceful enemy will look at our centers of gravity and try to attack them. Our adversaries understand our global dependence on space capabilities, and we must be ready to handle any threat to our space infrastructure.”46 With the increased US reliance on space assets for communication, intelligence, surveillance, and reconnaissance (ISR); and command and control of our deployed forces; a successful space attack could significantly delay US response to regional aggression. During Operation IRAQI FREEDOM (OIF), over 60% of theater communications traveled via satellites.47 The Defense Satellite Communication System (DSCS) provided 90% of all protected communications and 70% of all military satellite communications into theater.48 These capabilities significantly enhanced command and control of US and allied forces. Further, the employment of the satellite-based Blue Force Tracker system resulted in an unprecedented level of situational awareness which decreased fratricide and facilitating search and rescue operations and reinforcement operations.49

#### The lack of settled framework makes the threat of retaliation and counterstrike IMPOSSIBLE. The aff makes counterstrike effective.

KESAN & HAYES 12 \* Professor, H. Ross & Helen Workman Research Scholar, and Director of the Program in Intellectual Property & Technology Law, University of Illinois College of Law. \*\* Research Fellow, University of Illinois College of Law [Jay P. Kesan\* and Carol M. Hayes\*\*, MITIGATIVE COUNTERSTRIKING: SELF-DEFENSE AND DETERRENCE IN CYBERSPACE, Spring, 2012, Harvard Journal of Law & Technology, 25 Harv. J. Law & Tec 415]

Ideas, computers, and intellectual property have become extremely important in the modern Information Age. The Internet has become so essential to modern life that several countries have declared Internet access to be a fundamental right. n4 But the importance of technology in the Information Age comes with a downside: the vulnerability of modern society and the global economy to minimally funded cyberat-tacks from remote corners of the world.

In the 1950s, American school children were taught to "duck and cover" in the event of an atomic bomb explosion. n5 A popular cautionary film from 1951 warns that a flash of light brighter than the sun accompanies such an explosion and that the flash could cause an injury [\*418] more painful than a terrible sunburn. n6 The film, however, asserts that a child who "ducks and covers" will be more protected from the aftermath of nuclear detonation than otherwise. n7 Fortunately, no American city has ever experienced a nuclear attack, so no child has ever learned the hard way that a newspaper or a coat affords little protection against the heat from the detonation of an atomic bomb. The nuclear capabilities on both sides of the Cold War served as a deterrent against nuclear strikes and helped avoid an all-out nuclear conflict. n8 "Duck and cover," however, had no deterrent effect.

The Cold War ended about two decades ago, but new threats have emerged. The conflicts have shifted, the battlefields have morphed, and technologies that were not even dreamed of in 1951 now form the foundations for our everyday lives. The Internet, a technology partially developed to facilitate communication in the event of a nuclear attack, n9 changed the world forever. It is quite possible that future wars will be fought primarily in cyberspace, with the lines between civilian and military becoming increasingly blurred. n10 Instead of "duck and cover," computer users must now "scan, firewall, and patch." n11 However, like "duck and cover," purely passive defenses have questionable utility in the face of zero-day vulnerabilities n12 and sophisticated cyberweapons like the Stuxnet worm. n13 Likewise, law enforcement [\*419] and judicial action against malicious cyber intrusions currently do not present enough of a practical threat to deter potential attackers. n14

The weaknesses of the current reliance on employing passive defense methods and seeking help from the authorities -- who are both technologically and legally ill-equipped to seek justice for victims -- present a difficult situation. Considering how modern society relies on the Internet and networked services, there is an urgent need for proactive policy to help insulate critical services from damage as well as mitigate harm from potential attacks. For a number of reasons explored below, we argue that, in some circumstances, permitting mitigative counterstrikes in response to cyberattacks would be more optimal. There is an urgent need for dialog on this topic as the development of technology has outpaced the law in this area. n15 While progress has been made in the form of executive orders addressing cybersecurity, n16 the proposed Cyber Intelligence Sharing and Protection Act ("CISPA"), n17 and cybersecurity provisions of the National Defense Authorization Act ("NDAA"), n18 these measures do not go far enough. New discussions and analyses are needed to ensure that responsive actions can be grounded in sound policy.

Because of the inadequacy in current means to address cyber threats, this Article examines other possible methods to deter cyberattacks, specifically the use of cyber counterstrikes as part of a model of active defense. Active defense involves (1) detecting an intrusion, (2) tracing the intruder, and (3) some form of cyber counterstrike. n19

[\*420] Though intrusion detection and tracing are essential, counterstriking is key to enhancing the deterrent effects of active defense. At its core, cyber counterstriking is about two things: (1) deterring attackers and (2) ensuring that attacked parties are not deprived of the inherent right to defend themselves and their property. There are many views of deterrence, but deterrence is generally accomplished by the threat of some combination of the following elements: (1) punishing attackers by inflicting unacceptable costs, or (2) preventing attackers from succeeding in their attacks. n20 These two elements of deterrence have led us to apply the terms "retributive counterstriking" and "mitigative counterstriking," respectively, to the counterstriking component of active defense.

In the cyber context, a "counterstrike" can involve any number of actions. As discussed in Part III.B, a counterstrike can involve the target executing its own Denial of Service ("DoS") attack against the attacker (for example, by redirecting the attacker's packets back at the attacker to knock the attacker's systems offline), n21 infecting the attacker's system with a virus or worm to permit the victim to take control, or a number of other options. The technologies available to execute counterstrikes are generally the same ones used in initial attacks; as we examine in more detail below, some of these currently available technologies permit an attack to be traced back to its origin -- with varying degrees of accuracy. Furthermore, there is now evidence that "cyber contractors" exist as part of what some have termed the new "military digital complex," whose work involves creating offensive cyber technologies that can have applications in the context of counterstriking. n22

The goal of a counterstrike can vary, from punishing the attacker to simply mitigating the harm to the target. We call the former "retributive counterstriking"; this type should remain under the sole control [\*421] of the military, as a national security matter relating to sensitive domestic and international legal issues. We define "mitigative counterstriking" as taking active efforts to mitigate harm to a targeted system, in a manner strictly limited to the amount of force necessary to protect the victim from further damage. We recognize there may be overlap between retributive and mitigative counterstriking, as the latter could potentially result in damage to the attacker's system. How-ever, the goal of mitigative counterstriking must be to mitigate damage from a current and immediate threat. We argue that whatever measures are deployed must be justifiable under a mitigation frame-work.

Cyber counterstrikes, however, are currently controversial, and it can be difficult under the current framework to differentiate between "hack back" vigilantism and legitimate exercises of a right to self-help. n23 Our proposal in this area is both modest and bold. Modest, because while we also discuss active defense as a broad topic, our primary focus is on mitigative counterstriking as a discrete subcategory of active defense activities. Bold, because we advocate for a significant shift from the prevailing approach to cyber intrusions. In recommending a new regime, we have chosen to focus on mitigative counterstriking as a starting point for two reasons. First, it is likely to be more effective than passive defense at accomplishing the goal of deterrence by denial. Second, a mitigative counterstriking regime would endow network administrators with the right to actively defend their property, thereby legitimizing the right to self-defense in the cyber realm. The current regime creates an unconscionable situation where parties are expected to give up the right to actively defend themselves against threats and instead rely on passive defense measures that may prove ineffective. Parties are left with no practical recourse through criminal enforcement or civil litigation for a number of reasons we discuss below.

Currently, the biggest barrier to defending against cyberattacks is the lack of a legal method to respond to cyberattacks that also has a credible deterrent effect on potential attackers. We posit that accurate and consistent use of mitigative counterstrikes could serve to deter cyberattacks against sensitive systems such as hospitals, government defense systems, and critical national infrastructure ("CNI"), and argue that implementing a regime to permit these sorts of counterattacks should be a priority. There is some evidence that the private sector has [\*422] been tacitly utilizing this sort of technology to protect their systems, n24 effectively acting as cyber vigilantes under the current regime. Such behavior is at best legally ambiguous, and at worst illegal. Currently, the idea of mitigative counterstriking is treated like the proverbial elephant in the room, with legal commentators largely ignoring it. n25 After careful analysis, we conclude that this neglect is due to the lack of an analytical framework distinguishing between the perceived vigilantism of retributive counterstriking and the employment of self-help through mitigative counterstriking.

We thus propose a new policy and legal regime to address the threat of cyberattacks using active defense and mitigative counterstriking. There is a grave need to standardize approaches to mitigative counterstrikes, n26 and we must determine when the use of mitigative counterstrikes is appropriate, as well as who should be permitted to conduct mitigative counterstrikes. We recognize that counterstrikes of any variety can raise a number of legal and diplomatic concerns. While additional analysis and technological development may be desirable before implementing a broad self-defense regime, we argue that implementing mitigative counterstriking capabilities to protect CNI should be the first priority. Cyberattacks significantly affect private parties, including owners of CNI, n27 so it is important to legitimize active defense and mitigative counterstriking approaches in order to afford these private parties more protection against these threats.

#### This solve future cyber conflict. Which escalates

Kramer et. al 12 (Franklin D. Kramer is a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He served as the assistant secretary of defense for international security affairs from 1996 to 2001. Stuart H. Starr is also a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He concurrently serves as the president of the Barcroft Research Institute. Larry Wentz is a senior research fellow in the Center for Technology and National Security Policy at the National Defense University., “Cyberpower and National Security”)

Cyber attacks—hacking of various kinds—are a fact of modern life. Nationstates, such as China, have been publicly accused of hacking for espionage purposes, and nonstate actors, such as criminals and terrorists, likewise have substantial capabilities. The steady state of modern life is that thousands of intrusions occur each day, some with important consequences. More ominously, there are concerns that attacks could be undertaken for geopolitical purposes by states or nonstate actors that would have far greater negative impact than has thus far occurred. The capacity to deter such attacks would be enormously valuable.

Cyber deterrence has been considered challenging because of the difficulty of attributing the source of cyber attacks. While attribution unquestionably is a consequential issue, we believe that deterrence in the context of cyber is a viable strategy and one on which the United States ought to embark much more advertently. The components of such a strategy would consist of the following elements, some of which would require development as discussed below.

First, any approach to deterrence of cyber attacks needs to be considered in an overall concept of deterrence, not as a separate cyber arena. Such an effort would use a combination of potential retaliation, defense, and dissuasion. It would be based on all elements of national power so that, for example, any retaliation would not necessarily be by cyber but could be by diplomatic, economic, or kinetic—or cyber—means, depending on the circumstances. Retaliation, when and if it occurred, would be at a time, place, and manner of our choosing.

In generating policy, some important differentiations could be consequential. State actors generally act for classic geopolitical aims and often are susceptible to classic geopolitical strategies. Retaliation of various sorts might be more available against state actors, and dissuasion likewise might be more effective. By contrast, nonstate actors could be less susceptible to classic geopolitical strategies (though indirect strategies, such as affecting the country in which they are based, may have impact). Cyber defense, law enforcement, and, for terrorists, classic counterterrorist techniques may be most effective.

One important question is whether there is a threshold at which more significant responses become appropriate. It bears restating that there are a great many intrusions already ongoing, and responses to them have not been dramatic. In analyzing this issue, it may be useful to separate what might be termed high-end attacks from low-end attacks. If one hypothesized a serious attack that rendered, for example, military or key financial systems inoperative, the probability would be that an extremely robust response would be appropriate. A state actor that undertook a high-end attack should certainly understand that the United States could carry out a countervalue response that would not be limited to a response on cyber assets. The potential of a response against the high-value elements of a state should add considerably to deterrence. Likewise, it should be clear that an attack in the context of an ongoing conflict, whether against a state or a nonstate actor, likely will receive a very significant response. Dealing with cyber actions by an actor with whom we are militarily engaged, such as al Qaeda or the insurgents in Iraq, seems different than dealing with a new problem where force has not already been used.

### 1AC Plan

|  |
| --- |
| **The United States Federal Government should substantially increase its statutory restrictions on the war powers authority of the President of the United States to require consultation with the legislative branch prior to the use of offensive cyber operations** |