# \*\*\*FULLERTON 1AC\*\*\*

# 1ac – china adv.

**Status quo lack of congressional checks on offensive cyber operations violates legal norms of conflict --- restrictions are key**

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.

**This lack of legal codification has blurred the lines between non-destructive and incredibly destructive cyberattacks which lowers the threshold for escalatory cyberwarfare**

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

**Specifically, this hampers efforts at mutual drawdown and cyber de-escalation with China**

Sanger 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. September 1, 2o13, “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.

**Lack of legal codification uniquely makes miscalculation likely --- it is a unique escalation scenario for war**

VornDick 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. 6/30/13, “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.

**Lack of legal clarity is the key internal link --- low transparency results in aggression over Taiwan and makes the US likely to be overaggressive**

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.

**Cyberspace is key --- eviscerates other known barriers to conflict and leads to full scale conflict**

Moss 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**

**Colby et al. 13** (Elbridge A. Colby, graduate of Harvard College and Yale Law School and is a member of the Council on Foreign Relations (term) and of the International Institute of Strategic Studies., Abraham M. Denmark, M.A. in international security from the Josef Korbel School of International Studies at the University of Denver and has studied at China’s Foreign Affairs University and Peking University., John K. Warden, After receiving a B.A. in history and political science from Northwestern University, he joined CSIS as a recipient of the William J. Taylor debate internship., James M. Acton, He holds a Ph.D. in theoretical physics from Cambridge University., Jay K. Brotz, M.S. in electrical and computer engineering from Carnegie Mellon University., Michael S. Chase, M.A. in China studies from SAIS and a B.A. in politics from Brandeis University., AND more, “Nuclear Weapons and U.S.-China Relations: A way forward,” http://csis.org/files/publication/130307\_Colby\_USChinaNuclear\_Web.pdf)

Miscommunication and misunderstanding. The danger posed by these potential flashpoints is magnified by the potential for miscommunication and misunderstanding between China and the United States. Although Beijing and Washington have agreed to a range of crisis management mechanisms, such as the Military Maritime Consultative Agreement (MMCA) and the establishment of a direct hotline between the Pentagon and the Ministry of National Defense, the bases for miscommunication and misunderstanding remain and draw on deep historical reservoirs of suspicion.15 For example, it is unclear whether either side understands what kinds of **actions would elicit a military,** or even **nuclear, response** by the other party. Furthermore, neither side seems to believe the other’s declared policies and intentions, suggesting that escalation management, already a very uncertain endeavor, could be especially difficult in any conflict. Moreover, the continued **expansion of the military relationship in** space and **cyberspace** introduces additional exacerbating factors.

**Extinction**

**Cheong 2k** (Ching Cheong, Senior Writer at the Strait Times, “No one gains in a war over Taiwan,” June 25th, Lexis)

THE high-intensity scenario postulates a cross-strait war escalating into a full-scale war between the US and China. If Washington were to conclude that splitting China would better serve its national interests, then a full-scale war becomes unavoidable. Conflict on such a scale would embroil other countries far and near and -horror of horrors -raise the possibility of a nuclear war. Beijing has already told the US and Japan privately that it considers any country providing bases and logistics support to any US forces attacking China as belligerent parties open to its retaliation. In the region, this means South Korea, Japan, the Philippines and, to a lesser extent, Singapore. If China were to retaliate, east Asia will be set on fire. And the conflagration may not end there as opportunistic powers elsewhere may try to overturn the existing world order. With the US distracted, Russia may seek to redefine Europe's political landscape. The balance of power in the Middle East may be similarly upset by the likes of Iraq. In south Asia, hostilities between India and Pakistan, each armed with its own nuclear arsenal, could enter a new and dangerous phase. Will a full-scale Sino-US war lead to a nuclear war? According to General Matthew Ridgeway, commander of the US Eighth Army which fought against the Chinese in the Korean War, the US had at the time thought of using nuclear weapons against China to save the US from military defeat. In his book The Korean War, a personal account of the military and political aspects of the conflict and its implications on future US foreign policy, Gen Ridgeway said that US was confronted with two choices in Korea -truce or a broadened war, which could have led to the use of nuclear weapons. If the US had to resort to nuclear weaponry to defeat China long before the latter acquired a similar capability, there is little hope of winning a war against China, 50 years later, short of using nuclear weapons. The US estimates that China possesses about 20 nuclear warheads that can destroy major American cities. Beijing also seems prepared to go for the nuclear option. A Chinese military officer disclosed recently that Beijing was considering a review of its "non first use" principle regarding nuclear weapons. Major-General Pan Zhangqiang, president of the military-funded Institute for Strategic Studies, told a gathering at the Woodrow Wilson International Centre for Scholars in Washington that although the government still abided by that principle, there were strong pressures from the military to drop it. He said military leaders considered the use of nuclear weapons mandatory if the country risked dismemberment as a result of foreign intervention. Gen Ridgeway said that should that come to pass, **we would see the destruction of civilization.**

**The plan is key --- eyes are on the US and our adherence to legal restrictions shapes the cybernorm**

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.

# 1ac – plan text

**The United States Federal Government should require the President of the United States to consult with the legislative branch prior to the use of offensive cyber operations.**

# 1ac – deterrence adv.

**Advantage 2 is deterrence**

**Cyberwar is coming now --- other countries are ramping up their cyberweapons --- they will target our space assets, disrupt the grid, and disrupt information and data transfer within the Armed Forces**

**Daheem 14** – writer for the Frontier Post, a leading Pakistani journal (Muhammad, "Cyber Warfare," The Fronteir Post, January 5, 2014, http://www.thefrontierpost.com/article/66472/Cyber-warfare/)

Cyber war is a new domain in warfare. It is now acknowledged as “the fifth domain of warfare.” Its target and objective is cyberspace. Professor Alexander Merezhko defines cyber war “as the use of Internet and related technological means by one state against political, economic, technological and information sovereignty and independence of any other state.” Richard A. Clarke, in his book Cyber War, defines “Cyber-warfare” as “actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.” Pakistan, just like several other countries, will have to face the challenge of Cyber war in the near future. The question is: does Pakistan have the ability to counter sophisticated cyber-attacks? In case of cyber-attacks Pakistan will have to fight back in self-defense. It should have a concrete counterattack strategy and capability to trace attacks to their origin and fight back against enemies. The Defense Ministry and other government agencies should take concrete measures for this purpose. Cyber-attack demands sophisticated and complex technology. Computers and satellite play an important role in cyber warfare. It is just possible that a foreign enemy may try to intrude into the computer system of a government agency or military installation to steal secret information. The intruder may try to disrupt the system or temper with the data to harm the national integrity. The enemy may try to create national security breaches. Sometimes cutting undersea communication cables is also part of the cyber-attack. The typical target sites or services can be banks and credit card services. These attacks can be devastating and may disrupt the economy of the country. The enemy can also target industry, academia, military, navy and air force and **space domains.** Potential targets in internet sabotage may include: web, the Internet Service Providers, various types of data communication mediums and network equipment etc. Then there are certain criminal activities such as commercial espionage or theft of intellectual property. These pieces of information can be used for sabotage purposes. Several specific attacks like Titan Rain and Moonlight Maze have already occurred in the United States of America. In Cyber war secret information can be obtained for military, political and financial purposes from individuals, competitors, rivals, and governments. It has a vast battlefield and command-and-control system. All the services depending on computers such as banking and finance, transportation, manufacturing and medical education are under cyber threat. The cyber war may also involve electrical grids. America had blamed China and Russia for infiltration in the U.S. electrical grid system in 2009. The North American Electric Reliability Corporation (NERC) has warned that that the electrical grid is not adequately protected from cyber-attack. China has denied any intruding into the US electrical grid system. Indian government is also under cyber-attack. There are at least 23 reports of Indian cyber security breaches. Nonetheless, it is thwarting attacks against heavy odds in the field of energy, transport, banking, telecom, defense, space and other sensitive areas. It is reported that Chinese ‘nationalist hackers’ attacked CNN in 2008. Russia started a cyber-attack on the Georgian government in 2008. These examples simply show cyber-attacks can be politically motivated worldwide. Sometimes cyber-attacks are as dangerous as biological attacks. The cruel attacks are made time and again without any particular information about the attackers. It is reported that **more than 120 countries** are making efforts to develop ways to use internet as a weapon. Some are already using it as a weapon. George W. Bush, the former American President, once informed the Reuters news agency that “the U.S. has already launched attacks on computer networks in other countries.” In June 2012 the New York Times reported that “President Obama had ordered the cyber-attack on Iranian nuclear enrichment facilities.” The major targets, in general, are financial markets, government computer networks and utilities. Several countries including Russia, Iran, Israel and North Korea have already organized themselves in this field. Iran claims that it has second-largest cyber-army in the world. It is just possible that wars may have a different style by the mid-21st century. America has a severe shortage of computer security specialists. It has about 1000 qualified persons in this field while it needs 20,000 to 30,000 skilled experts. On the other hand North Korea has more than 3,000 highly trained hackers. It is reported that several organizations are using “information warfare units” to develop viruses to attack enemy computer systems and networks, and those units include civilian computer professionals. These organizations are constantly developing their programs and capabilities to counter any potential cyber threat. The use of computers and the Internet to conduct warfare in cyberspace can be a threat to national security. It can be used to “attack, degrade, and **disrupt communications** and the flow of information.” Internet has posed certain threats to the Armed Forces of powerful countries. Potential targets in internet sabotage may include: web, the Internet Service Providers, various types of data communication mediums and network equipment etc.

**We’ll impact each scenario ---**

**First, space assets --- they are uniquely vulnerable to cyber attacks**

**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

**This risks miscalculation and 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

**Second, the grid --- it’s a prime target for cyberattacks**

**Bloomberg, 1/31/12** (Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months

<http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html>

\*\*\*edited for ableist rhetoric

A blackout that swept parts of [North America](http://topics.bloomberg.com/north-america/) in August 2003, leaving 50 million people in the dark for as long as four days, provides a glimpse of the havoc a cyber attack could inflict on the nation’s power grid. Internet-based terrorists would be capable of causing blackouts “on the order of nine to 18 months” by [destroying] critical systems such as transformers, said Joe Weiss, managing director of Applied Control Solutions LLC, a Cupertino, California-based security consulting company. “The dollars are incalculable,” Weiss said in a phone interview. The 2003 event, triggered when a power line touched tree branches in [Ohio](http://topics.bloomberg.com/ohio/), caused losses of as much as $10 billion, according to a study by the U.S. and Canadian governments. Energy companies including utilities would have to increase their investment in computer security more than seven-fold to reach an ideal level of protection, according to a survey done for Bloomberg Government by the Ponemon Institute LLC, a data- security research firm based in Traverse City, [Michigan](http://topics.bloomberg.com/michigan/). Electric utilities fail to recognize the risk because, unlike banks and telecommunications companies, they aren’t prime targets for Internet theft or espionage, said [James Lewis](http://topics.bloomberg.com/james-lewis/), technology program director at the Center for Strategic & International Studies in Washington. Yet “if there was a cyber attack, the electrical grid would be **target number one” for terrorists,** he said. “There’s some percentage of utilities out there that just don’t take this seriously,” Lewis said.

**Extinction**

**Stein 12** (Matthew Stein, 3/24/12, Bachelor’s degree in engineering MIT, design engineer, green builder, “Four Hundred Chernobyls: Solar Flares, Electromagnetic Pulses, and Nuclear Armageddon,” http://truth-out.org/news/item/7301-400-chernobyls-solar-flares-electromagnetic-pulses-and-nuclear-armageddon)

Unfortunately, the world's nuclear power plants, as they are currently designed, are critically dependent upon maintaining connection to a **functioning electrical grid,** for all but relatively short periods of electrical blackouts, in order to keep their reactor cores continuously cooled so as to avoid catastrophic reactor core meltdowns and fires in storage ponds for spent fuel rods. If an extreme GMD were to cause widespread grid collapse (which it most certainly will), in as little as one or two hours after each nuclear reactor facility's backup generators either fail to start, or run out of fuel, the reactor cores will start to melt down. After a few days without electricity to run the cooling system pumps, the water bath covering the spent fuel rods stored in "spent-fuel ponds" will boil away, allowing the stored fuel rods to melt down and burn [2]. Since the Nuclear Regulatory Commission (NRC) currently mandates that only one week's supply of backup generator fuel needs to be stored at each reactor site, it is likely that, after we witness the spectacular nighttime celestial light show from the next extreme GMD, we will have about one week in which to prepare ourselves for Armageddon. To do nothing is to behave like ostriches with our heads in the sand, blindly believing that "everything will be okay" as our world drifts towards the next natural, inevitable super solar storm and resultant extreme GMD. Such a storm would **end the** industrialized **world as we know it,** creating almost incalculable suffering, death and environmental destruction on a scale not seen since the extinction of the dinosaurs some 65 million years ago.

**Third --- communications hacking --- it causes miscalc and great power global nuclear war**

**Rosenbaum 08** (Ron Rosenbaum, American journalist and author, “A Real Nuclear Option for the Nominees,” Slate, May 9, 2008, http://www.slate.com/articles/life/the\_spectator/2008/05/a\_real\_nuclear\_option\_for\_the\_nominees.single.html)

According to a recent paper by Blair (whose account of these procedures has been made public in the Congressional Record), an "assessment drill ... is supposed to yield a preliminary assessment three minutes after the arrival of the initial sensor data. Analogous drills take place under comparable deadlines in Russia. A rush of adrenaline and rote processing of checklists, often accompanied by confusion, characterize the process." Rising levels of "strategic tension" between the superpowers may lend more credibility to what are actually false-positive warning signals. The time pressure to make momentous decisions is the key problem. After the three minutes are up, if the warnings are assessed as "serious," there follows a quick conference between the president and his nuclear advisers "whereupon, on the U.S. side, the commanding duty officer at Strategic Command headquarters in Omaha, Neb., would brief the U.S. president on the nature of the apparent attack, the wide array of response options and their anticipated consequences [human casualties and physical damage]." Blair noted that "the time allocated for this briefing is as little as 30 seconds," and that afterward the president's "decision window is typically twelve minutes, although under certain conditions it can be much shorter." The reason for the 12-minute deadline is that missiles launched from offshore submarines can reach coastal targets in less than 15 minutes. So it's insanely short-fused as it is. But when I spoke to Blair in Washington last week, he noted an additional cause for concern: cyber-attacks. He pointed to the preface of his Oslo paper, which focused on how **"information warfare" in cyberspace heightened the threat of "inadvertent" nuclear war.** "The nuclear command systems today operate in an intense information battleground," Blair wrote, "on which more than 20 nations including Russia, China, and North Korea have developed dedicated computer attack programs. These programs deploy viruses to disable, confuse, and delay nuclear command and warning processes in other nations. At the brink of conflict, nuclear command and warning networks around the world may be besieged by electronic intruders whose onslaught degrades the coherence and rationality of nuclear decision-making. **The potential for** perverse consequences with computer-launched **weapons on hair-trigger is clear."**

**We need a deterrence strategy for cyberspace --- it 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.

**But the US currently has no such strategy and we are 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.

**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.

**Clarifying the legal framework on cyber operations is key to a credible cyber deterrence strategy**

**Goldsmith, prof of law @ Harvard, 12** [Jack, Henry L. Shattuck Professor @ Harvard Law School, where he teaches and writes about national security law, presidential power, cybersecurity, international law, internet law, foreign relations law, and conflict of laws, served as Assistant Attorney General, Office of Legal Counsel from 2003–2004, and Special Counsel to the Department of Defense from 2002–2003, member of the Hoover Institution Task Force on National Security and Law, 10/15, “The Significance of Panetta’s Cyber Speech and the Persistent Difficulty of Deterring Cyberattacks,” Lawfare, <http://www.lawfareblog.com/2012/10/the-significance-of-panettas-cyber-speech-and-the-persistent-difficulty-of-deterring-cyberattacks/>]

Secretary of Defense Leon Panetta’s speech last week on cyber is more significant than has been reported. Most of the coverage focused on Panetta’s grave warnings about cyber threats facing the nation, but the speech’s real significance, I think, concerns DOD’s evolving deterrence posture. (The speech has other significant elements, but I focus here on deterrence.) Panetta had two main messages related to deterrence. First, because the USG’s attribution skills have improved, “[p]otential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America.” Second, “If we detect an imminent threat of attack that will cause significant, physical destruction in the United States or kill American citizens,” then on the orders of the President, DOD can “conduct effective operations to counter threats to our national interests in cyberspace.” (This second point echoes earlier USG statements, including one made earlier this month by DRNSA Keith Alexander, who said, somewhat less cautiously than Panetta, that DOD must be able to “stop [an attack] before it happens. . . . Part of our defense has to consider offensive measures like that to stop it from happening.”) Here is what I think is significant about Panetta’s speech.¶ First, DOD has previously said that it is trying to improve is attribution capabilities, and in conversation officials have noted some success. Panetta goes further, saying concretely and definitively that DOD has “made significant advances in solving” the attribution problem, presumably through a combination of tracing back the source of a cyber attack and identifying the attacker through “behavior-based algorithms” and human and electronic intelligence. Panetta does not tell us how good or fast DOD is at attribution, and he may to some unknown degree be puffing. Nonetheless, this is a potentially big deal for cyber deterrence. Second, Panetta was more aggressive than DOD has been in the past about the trigger for a self-defensive cyberattack by the United States. Previously, DOD has stated that adversaries would face a “grave risk” if they launched a “crippling” or “significant” cyberattack on the homeland. Panetta’s speech changes this posture in two ways. He is less definitive about the high threshold of a “significant” or “crippling” attack as a trigger for a USG response, and indeed implies that the threshold is (or can be) lower. And more importantly, he makes plain that the DOD has the capabilities and desire to engage in a preemptive attacks against imminent cyber threats. This possibility has been hinted at before (most recently, in Alexander’s comment above and in Harold Koh’s NSA Cyber Command legal conference speech last month). But Panetta was more definitive about DOD’s capacity and desire to engage in such attacks. (Herb Lin, chief scientist at the National Research Council’s Computer Science and Telecommunications Board, noted to me that Panetta referred to the need to “take action” with “effective operations” against imminent cyberthreats, and pointedly did not state that such actions or operations would necessarily involve cyber means or cyber targets. This is consistent with DOD’s prior claims that it would use “cyber and/or kinetic capabilities” to redress large-scale cyberattacks.) Panetta was ambiguous, however, about whether DOD currently has the authorities to engage in such preemptive attacks (by cyber means or other means) in the face of cyber threats. He said that “we need to have the option to take action against those who would attack us to defend this nation when directed by the president” (emphasis added), and he emphasized DOD capabilities while several times calling for more DOD authorities. I have previously criticized DOD’s announced deterrence policy, so I should say that Panetta’s speech takes steps in the right direction. Panetta noted improvement in attribution (which is potentially huge), he warned that the USG would hold attackers responsible, he appeared to eliminate unjustifiably super-high thresholds for a self-defensive responses to cyberattacks, and he noted DOD’s capacity and need for preemptive attacks in the face of imminent cyberattacks. That said, Panetta made these points in an after-dinner speech, not an official declaratory policy. And many questions remain, such as: How much better (in terms of speed and accuracy) is our attribution capacity? How do adversaries know whether the USG’s supposed attribution advances are not a bluff? What exactly is the threshold for a self-defensive offensive operation in response to a cyber attack? What counts as an imminent threat of cyberattack that would warrant a preemptive attack by the USG? The effectiveness of any deterrence posture depends on the answers to these (and related) questions, and (very importantly) on our adversaries’ beliefs about the answers to these questions. Ambiguity about the answers might over-deter (as vague criminal law often does), but it might also under-deter (because the adversary misperceives where the red lines are). The effectiveness of deterrence also depends, crucially, on the credibility of our threat to attack in the face of actual or imminent attacks. Several obstacles prevent our threats from being entirely credible. Panetta’s speech and other DOD pronouncements, as well as news reports, indicate that DOD does not think it has adequate legal authorities to engage in offensive operations related to defense, and that USG lawyers are currently putting up affirmative obstacles to such operations. To the extent that the USG is and appears to be legally constrained from acting as it says it needs to, its threats to act are not credible.

In addition, even if our attribution skills are fast and accurate (which they won’t always be), any responsive cyberattack that has public effects must be accompanied by public evidence that the attack was warranted – something very hard to do when attribution is based on sophisticated and fragile intelligence tools.  To the extent the USG cannot prove attribution publicly, its threats of a cyberattack are diminished.  This point implies that self-defensive cyberattacks are (all things equal) more likely to be unattributable than attributable.  But that conclusion in turn presents two problems.  First, how to convince the adversary that we have hit it in response to a cyberattack when we cannot take public credit for the attack? (This is potentially difficult, not impossible; Iran certainly suspected the USG even before the public revelations about Stuxnet/Olympic Games.)\*  Second, an unattributable self-defensive cyberattack is more likely in response to a relative small actual or threatened cyberattack on the nation.  If we suffer a crippling blow, we will need to respond with large public fire, in cyber or kinetic space, or both.  The worry is that the difficulties of public proof of attribution will slow the needed public response, or weaken it, or make it seem less legitimate ex post – all of which weakens the credibility of a responsive attack ex ante, and thus weakens deterrence.

Finally, some thoughts about Stuxnet/Olympic Games, the cyber operation(s) against the Iranian nuclear facilities.  While many in the USG are no doubt genuinely angry that the USG hand in Stuxnet was revealed, this revelation probably has the happy effect of **enhancing U.S. cyber deterrence**.  For it demonstrates that the USG has sophisticated cyberweapons that – despite legal and other obstacles – it is willing to deploy, even in a preemptive fashion.  For many reasons that I lack time explain (having to do with the nature of the Iranian threat, which did not present an attribution problem, and the nature of the cyber attack on the Iranian facilities), I think the legal and policy hurdles to the Iranian operation **were less significant than ones that would arise with a self-defensive USG attack** in response to an actual or threatened cyberattack.  Nonetheless, the Stuxnet/Olympic Games revelations probably **enhance U.S. cyber deterrence overall**.  (And no, the Iranian cyberattacks in the news yesterday, which reportedly inflicted “modest damage,” do not by themselves belie this claim.)

**A congressional restriction is key to both domestic and international support**

**Moss 02**, Associate Dean for Academic Programs in the Industrial College of the Armed Forces, National Defense University, and a professor in its department of grand strategy. Previously Professor Moss was a member of the staff of the House Subcommittee on Europe and the Middle East. The opinions within are his own and reflect no position of the National Defense University or the Department of Defense, Information Warfare and War Powers: Keeping the Constitutional Balance, Fletcher Forum of World Affairs

More importantly, as in any debate and vote on the use of traditional military force, **Congress's** placement of information warfare within the context of the Constitution guarantees that the President's policy towards it will have a stronger legal foundation and public support. This is critical not only for sustained acceptance of the policy at home but also for international recognition of the justification of the President's decisions abroad. Ultimately, information warfare, cyber-attacks, or cyber warfare must come under the same requirements for accountability in the Constitution as traditional military force. The President cannot be given an instrument of warfare over which Congress has no power.

**Congressional deliberation key to effective deterrence and cyberoperations**

**Griffin 12** – Professor of Constitutional Law @ Tulane University [Stephen Griffin, “The Tragedy of the War Power: Presidential Decisionmaking from Truman to Obama,” APSA 2012 Annual Meeting Paper, July 15, 2012, Pg. [http://ssrn.com/abstract=2107467](http://ssrn.com/abstract%3D2107467)

As a comparison of the relative ability of the executive and legislative branches to make speedy decisions, Hamilton’s argument is certainly plausible as far as it goes, but in the kind of government we have had since the Cold War began, it does not take us very far. Swift decisionmaking has little to do with a presidential decision to initiate the kind of war that has occupied us here. Wars involving the potential of thousands of American casualties, millions of foreign casualties, and the expenditure of hundreds of billions of dollars are usually not based on off-the-cuff decisions. Korea (especially taking into consideration the decision to cross the 38th parallel), Vietnam and the 1991 Gulf War were enormous undertakings and required layers of complex interagency decisionmaking, not a single swift move. Indeed, these considerations were part of what made it necessary in 1947 to establish the NSC to coordinate policy within the executive branch. During the Cold War and after, the pre-Pearl Harbor constitutional order was identified with isolationism and no one thought a return to that policy after 1945 was realistic. But while it is relevant to ask if there was an alternative, there is no escaping the ineluctable reality that the post-1945 order was a tragedy waiting to happen. That order was inconsistent with the historical meaning of the Constitution and the original constitutional order remained relevant to making decisions for war. Whether the post-1945 order was necessary or not, it introduced deep tensions into the American system of governance. The case studies presented above show that the interagency process taking place inside the executive branch was not an adequate substitute for the constitutionally mandated interbranch process. The inability of the executive branch to deliberate and make effective decisions on its own manifested itself in surprising ways. The executive branch has repeatedly failed to engage in effective war planning. With respect to Korea, Truman had to cope with the novelty of limited war and the fact that he would have been criticized by Republicans if he had ordered MacArthur to stop at the 38th parallel to restore the status quo ante. Nonetheless, it was his decision alone to unite the peninsula, a decision made essentially on the fly. In turn, that caused China to intervene. Korea then became a conflict of unanticipated scope that ended in stalemate and ruined Truman’s last years in office. True to his initial decision to intervene, Truman did not share responsibility with Congress and so Congress escaped both a valuable learning experience and the blame for the war. In addition, the case studies show that there is considerable evidence that the executive branch has had problems determining on war aims. President George H. W. Bush studiously avoided consulting Congress during the crucial period of decision in fall 1990 when it became possible to contemplate turning Operation Desert Shield into Desert Storm. This meant that he did not have to resolve on a unified set of war aims that would have been a necessary part of convincing Congress to authorize the war. Like Truman, Bush waited until it was too late to convince Congress and the public that the war had a point beyond forcing Iraq out of Kuwait. Thus the war had no substantial implications for policy and could not even help Bush remain in office. Not submitting the war to a timely congressional decision that Bush would have respected turned out not only to be counterproductive in terms of policy, but contrary to Bush’s political interests. Similarly, President George W. Bush failed to clarify what the war in Afghanistan was for beyond the removal of al Qaeda from Afghan territory. Partly as a consequence, the war became an endless struggle against the Taliban in both Afghanistan and Pakistan that is still ongoing as of 2012. It is striking that the executive, often represented by presidentialists as the branch that is most decisive and expert on matters of war, could consistently both fail to deliberate and fail to reach agreement on its goals in going to war. This suggests strongly that the pressures to shirk hard choices are too great to be overcome by one branch working alone. As I have argued throughout this article, the post-1945 constitutional order tended to derange the policy process inside the executive branch, producing not a set of swift successful decisions, but rather a series of policy disasters. The formulation of policy on Vietnam in the Johnson administration, for example, showed serious deficiencies that have not been taken into account by contemporary presidentialists. In essence, the advisers in the White House and the different departments in the executive branch found it impossible to move beyond the narrow orbit established by the president. Rather, the president and the idiosyncratic process he establishes tends to dominate the undoubted policymaking expertise of the different departments. The lack of planning for the aftermath of the Iraq War, with the president and policymakers in the White House falling prey to all sorts of false assumptions, showed that nothing had changed since Vietnam. I have also highlighted the costs of decisions for war on presidents. In doing so, I am not arguing that presidents who go to war suffer some sort of trauma. But there is good evidence that decisions for war are considerably different from other sorts of policy decisions. They can clearly impair presidential decision making, as was the case with Presidents Johnson and Nixon and probably both Bushes, father and son. There can be other, more subtle effects on policy. War can take up so much of the president’s time that other pressing concerns, including those related to foreign affairs, are crowded out. So President Johnson probably lost several chances to negotiate meaningful arms control agreements with the Soviet Union.217 This helped undermine the structure of détente in the 1970s by continuing the arms race. Preparing for and fighting the 1991 Gulf War so exhausted President Bush and his advisers that they had less capacity to make decisions with respect to the postwar environment in Iraq.218 This helped undermined the credibility of Bush’s decision not to depose Saddam Hussein. The 2003 Iraq War so consumed President George W. Bush and his advisers that they lost track of the situation in Afghanistan, leaving to President Obama the knotty task of sorting out the mess. As the discussion in this article has thus demonstrated, the defects of the post-1945 constitutional order are manifest. Experience has shown that the executive branch is incapable of handling the deliberation necessary for decisions for war on its own. Perhaps this is what we should expect, given the continued tidal pull of the original constitutional order. Yet it is still striking how consistently poor executive decision making for war has been in the post-1945 period. These defects create several distinct challenges for executive enthusiasts. For example, supporters of the presidentialist position often stress its unitary character. With a single person at the helm, the executive branch can act quickly to address foreign crises. We can now see more clearly that when the executive branch is not subject to oversight it is too easy either for presidents to dominate their advisers, thus suppressing valuable policy input (Johnson) or to so rearrange the White House policy process that an effective decisionmaking process becomes nearly impossible (Bush II). This supports the inference, which may come as a surprise to presidentialists, that a chief purpose of interbranch deliberation is to ensure that the executive branch is truly unitary and effective with respect to the all-important decision for war. Oversight also has the potential to counter the scenario in which the president totally dominates his advisers. Congressional hearings might give advisers a public forum in which they can finally get through to the president, although this is obviously a more difficult case. Without oversight, policy in the executive branch can be unsound or even deranged. One pathway to policy disaster, seen in Vietnam, is that the various departments responsible for war are never forced to agree on a unified set of goals and what means are necessary to achieve those goals. Without strong external compulsion it is too easy for the different parts of the executive branch to fall to quarreling amongst themselves without any ability to resolve their differences. When the State Department, Defense Department and the CIA fail to agree, the NSC process has been insufficient to create a consensus on a proposed course of policy. While it is reasonable to assume that the nation requires a unified foreign policy, nothing in the internal architecture of the executive branch that guarantees unity. Again, this can strike us as surprising, because the executive branch is a hierarchy and we expect presidents to have the ability to lead. Experience shows, however, that leadership is usually expressed either through domination involving the suppression of dissident views or by the president being unable or unwilling to manage the many different parts of the executive branch together with their often strong-willed department heads. Striking the appropriate balance has been difficult for presidents who are, after all, politicians, not experienced managers. Another pathway to disaster already mentioned is that it has proven difficult for the executive branch to determine war aims. Understandably the president and his advisers tend to respond to the exigencies of the moment, rather than concerning themselves with how a given military operation relates to the overall strategy of the U.S. in foreign affairs. The executive branch does not have any inherent ability to relate short-term responses to long-term goals. As we saw with the 1991 Gulf War, this inability to justify a war in terms of long-term goals can run contrary to the president’s own political interests. It is not necessary to assume anything about the policy knowledge of individual members of Congress or the quality of congressional hearings to appreciate that a world in which the executive branch is required to justify itself publicly provides a significant incentive for the president to insist on a unified approach to policy. It is plausible that repeated iterations of oversight would build up congressional expertise in foreign policy and thus begin a meaningful cycle of accountability where each branch could learn over time from experience. While there is a sense in which everyone accepts that oversight is a traditional function of Congress, it is noteworthy that there was no strong tradition of external review established in the early Cold War. The situation with respect to the CIA eventually became notorious, with a small group of senators handling oversight on a basis akin to a private club.219 But the situation with respect to foreign affairs in general was little better, with many hearings and exchanges held in executive session or off the books in private gatherings. While it is a mistake to think that the congressional leadership had no influence over the early Cold War administrations, the lack of public oversight meant that the proper incentives were never provided to executive branch agencies. As recounted by historian Robert Johnson, later in the Cold War the influence and prestige of the Senate Foreign Relations Committee waned in comparison with the growing power of the Armed Services Committee.220 This further undermined accountability and was emblematic of the dominant militarized approach to the Cold War. While the executive branch was retooled to a certain extent for Cold War duty after 1947, nothing was done to the structure of Congress. Members of Congress assumed that the existing committee structure would suffice. Eventually the costs of this approach became apparent, at least with respect to intelligence policy. Part of the intelligence reforms of the 1970s was to establish committees to oversee the intelligence community. The subsequent difficulties with implementing this oversight have been well analyzed by a number of scholars and presidential commissions, including the 9/11 Commission. Some of the ignored proposals of the 9/11 Commission had to do with changes to congressional oversight of intelligence.221 What oversight there is has been rendered less effective by the use of term limits for service on the intelligence committees and the fact that budgetary authority is located elsewhere.222 As Amy Zegart concluded in her study of Congress, the intelligence community and 9/11: It was no secret that this fragmented oversight system desperately needed fixing. Restructuring the Congress was recommended in seven of the twelve intelligence and terrorism studies between 1991 and 2001. Yet Congress never acted. In fact, Congress was the only government entity that failed to implement a single recommendation for reform during the decade—a record worse than either the CIA’s or the FBI’s.223 One purpose of the interbranch cycle of accountability is to test the executive branch’s claims with respect to war and foreign affairs. Of all the shibboleths of the Cold War, none have arguably done more harm than the idea that the executive branch’s undoubted expertise with respect to diplomacy is relevant to the expertise necessary for planning and running a war. The experience of presidential administrations in the post-1945 period is clear – there is no such thing as a civilian “expert” in making the policy choices and decisions necessary for war. Even if we accept the reasonable point that military leaders are expert in planning and running military operations, this sort of expertise is built up over many years of service and such experience was not available to any post-1945 president except Eisenhower. Consider that the substantial expertise FDR had acquired with respect to foreign policy by the time he was elected to a third term in 1940 is barred to any contemporary president by the 22nd Amendment. Further, cabinet officials and advisers are rarely drawn from a pool of those expert in war. As we drew away from the World War II generation, the Secretaries of State and Defense have usually been different sorts of careerists or politicians. While there is nothing inherently wrong with this, none of them were experts in making war decisions.224 In fact, there have been too few major wars for any civilian adviser to acquire the sort of experience necessary before true expertise is possible. At the same time, the major wars since 1945 show that effective consultation with Congress is pragmatically possible. Because American armies have been fighting far from home in the post-World War II period, considerable time has been required to transport them to the theatre of conflict and assemble the necessary enormous amount of supply material. Aside from true crises such as the 1962 Cuban missile crisis, there has always been plenty of time for interbranch deliberation over the decision to go to war. This has not always been highlighted by presidents. In Korea, many weeks were required before the Inchon landing and break-out from the Pusan perimeter became possible. In Vietnam, it took two years, until 1967, for General Westmoreland to assemble the supply chain necessary to support the kind of military operations he envisioned in 1965.225 The build-up time required to simply provide an effective defense for Saudi Arabia (Operation Desert Shield) in the Gulf War was seventeen weeks. More weeks were required to attain an offensive capability. Months were required after 9/11 before there were sufficient regular armed forces in Afghanistan and the same was true for the Iraq War. The fact of a crisis or apparent emergency that arguably requires a military response does not necessarily mean that there is little time for proper interbranch deliberation. The war powers debate should occur on the terrain of a realistic appraisal of presidential success in making decisions for war and the possible contributions a true interbranch dialogue could make to effective decisionmaking. Such an appraisal is not found in recent works by executive enthusiasts. Eric Posner and Adrian Vermeule, for example, have recently provided a provocative theoretical grounding for executive enthusiasm. 226 They present a tightly woven argument that challenges what they describe as the “Madisonian” understanding of separation of powers. Their target, which they call “liberal legalism,” is the idea that the executive can be constrained primarily through legal means, including the constitutional law promulgated by judges as well as statutes passed by Congress.227 While their argument is wide-ranging, extending to administrative law and “global liberal legalism,” my comments here are directed at the parts of their argument most nearly relevant to war and foreign affairs. There is arguably a subtle bias in the Posner and Vermeule analysis. They criticize the eighteenth-century “Madisonian” view of how an executive should be constrained. But why constrain the executive at all? Here Posner and Vermeule confine themselves to critiquing what might be called an eighteenth-century view of the dangers posed by the executive – chiefly the threat to civil liberties and the possibility, which they rightly discount, that the American term-limited president might turn into a tyrant.228 But they do not consider reasons for caution about the executive branch connected with our twentieth-century experience with war and foreign affairs. They believe one fatal problem with liberal legalism is that Congress can never catch up with emergencies. The nature of emergencies is that rules cannot be created in advance to handle them. By contrast, the executive is well suited to handling fast-changing situations – “in emergencies, only the executive can supply new policies and real-world action with sufficient speed to manage events.”229 While this is superficially plausible, it will have a strange ring to anyone who lived through Hurricane Katrina in 2005. Of course, this does not mean Congress somehow would have done better. Posner and Vermeule’s analysis is relentlessly comparative. The fact that the executive inevitably makes mistakes and fails sometimes does not show that liberal legalism is a workable alternative. What Posner and Vermeule do not consider is the enormous influence, amply demonstrated by the narrative I have presented, of the original constitutional order. Because Posner and Vermeule do not consider how constitutional orders work, they miss the significance of the original constitutional design. My argument has concerned war and foreign affairs. But it supports the general inference that the original design made it difficult for either branch to make good policy on its own. Sound policy with respect to war requires the branches to cooperate. While political parties have made such cooperation more difficult, parties are an example of how constitutional change tends to add to, rather than completely replacing, the original constitutional order.230 The discussion in this article has shown that policymaking in the executive branch becomes deranged without the oversight and input of the legislature. Posner and Vermeule have no way to account for this because they assume that executive branch is generally competent not only to execute the law but to make policy on its own. Strangely, they do not consider the generally poor record of the executive branch in war making in the post-1945 period. This period is littered not simply with mistakes, but with policy catastrophes that undermined the stability of the government as a whole. It is also noteworthy that Posner and Vermeule focus on the executive branch without managing to say much about the person of the president or how the president runs the White House. The post-World War II experience showed that the president was incapable of managing the tasks of war without the substantial support of Congress. Briefly summarized, the biggest problem with the arguments of executive enthusiasts is that they reflect pre-Vietnam understandings of how the executive branch makes decisions in foreign policy. It is as if the substantial and closely documented historical scholarship on the Vietnam War has made no impression on legal scholars who study presidential power. These scholars continue to treat the executive branch as if it were a black box full of the “best and the brightest” – knowledgeable experts willing to make hard choices and swift, yet measured and effective decisions.231 History shows differently. Conclusion War is a unique kind of policy. Even “limited” wars tend to subordinate the rest of the nation’s foreign policy to their requirements rather than the reverse. This has meant that in starting any major military conflict, the president is almost literally betting the ranch. All the more reason to ensure that there is sufficient deliberation before going forward. In the restrained phrasing of political scientist James Kurth, the U.S. would have been better off had “an authentic democratic process” been used to approve wars since 1945.232 The question for the future is whether such a process is possible. Pg. 31-37

**Action now is key – failure will result in a rapidly created worse, more RESTRICTIVE legal system**

**SCHAAP 09** Major **–** Air Force, the Directorate of Legal Services, Headquarters Air Command, RAF High Wycombe, United Kingdom. JD Cal Western, LLM George Washington, Former Deputy Staff Judge Advocate, Lackland [Major Aire J. Schaap, CYBERLAW EDITION: CYBER WARFARE OPERATIONS: DEVELOPMENT AND USE UNDER INTERNATIONAL LAW, Air Force Law Review, 64 A.F. L. Rev. 121]

IX. CONCLUSION

One of the greatest challenges of law is keeping up with the advancement of technology. n346 The international community has often struggled to implement standards of conduct in a timely manner regarding the advancement of weaponry. n347 In the past, when new technologies emerged, in an effort to avoid war or minimize human suffering when conflicts occur, states drafted rules resulting in, for example, treaties restricting biological, chemical, and laser weapons. n348 In March 2006, Nikolai Kuryanovich, a member of the Russian Duma, noted in a letter to an ultranationalist hacker group known as the Slavic Union that, "In the very near future many conflicts will not take place [\*173] on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers . . . ." n349 I contend that the future Mr. Kuryanovich discusses is now, and that now is the time for states to determine what is and is not permitted under international law in relation to cyber warfare operations**.** Failure to do so now may result in overly restrictive, reactionary regulations in response to a cyber Pearl Harbor-likeattack, rather than a well thought out, proactive, structured approach.