## 1AC Cyberwar Opinio Juris

**Status quo unregulated policy means there are no common rules of engagement in cyberspace –causes militarization**

**Gjelten 13**, Tom, correspondent for NPR, “Pentagon Goes On The Offensive Against Cyberattacks” February 11, 2013, http://www.npr.org/2013/02/11/171677247/pentagon-goes-on-the-offensive-against-cyber-attacks

Those assurances are deceptive. Behind the scenes, U.S. commanders are committing vast resources and large numbers of military personnel to planning offensive cyberattacks and, in at least some cases, actually carrying them out. But the secrecy surrounding offensive cyberwar planning means there has been almost no public discussion or debate over the legal, ethical and practical issues raised by waging war in cyberspace. Offensive cyberattacks carried out by the United States could set precedents other countries would follow. The rules of engagement for cyberwar are not yet clearly defined. And the lack of regulation concerning the development of cyberweapons could lead to a proliferation of lethal attack tools — and even to the possibility that such weapons could fall into the hands of unfriendly states, criminal organizations and even terrorist groups. In some cases, offensive cyberattacks are being conducted within the parameters of conventional military operations. In Afghanistan, soldiers and Marines depend heavily on video and data links when they go into combat. As part of the process of "prepping the battlefield," commanders may want to launch pre-emptive attacks on the adversary's cybercapabilities in order to make sure their data networks do not get interrupted. Marine Lt. Gen. Richard Mills, in a rare acknowledgment that the military engages in offensive cyber operations, discussed just such a situation during a military conference in August 2012. "I can tell you that as a commander in Afghanistan in the year 2010, I was able to use my cyber operations against my adversary with great impact," Mills declared. "I was able to get inside his nets, infect his command and control, and in fact defend myself against his almost constant incursions to get inside my wire." Another reference to the military's use of cyberattacks as part of a traditional combat operation came in 2009, during a presentation at the Brookings Institution by Air Force Gen. Norton Schwartz. Now retired, Schwartz at the time was serving as Air Force chief of staff. He told his audience that his airmen were prepared to carry out cyberattacks on another country's radar and missile installations before launching airstrikes against that country. "Traditionally, we take down integrated air defenses via kinetic [physical] means," Schwartz said. "But if it were possible to interrupt radar systems or surface-to-air missile systems via cyber, that would be another very powerful tool in our tool kit." Schwartz hinted that the Air Force already had that capability, and in the nearly four years since he gave that speech, such a capability has certainly matured. Cyberattacks, however, are also being used independently of traditional or kinetic operations, according to Jason Healey, a former Air Force officer who now directs the Cyber Statecraft Initiative at the Atlantic Council. "It might happen that we will use them as an adjunct to kinetic," Healey says, "but it's quite clear that we're using [cyber] quite a bit more freely." The best example of an offensive cyberattack independent of a kinetic operation would be Stuxnet, the cyberweapon secretly used to damage nuclear installations in Iran. A U.S. official has privately confirmed to NPR what the New York Times reported last summer — that the United States had a role in developing Stuxnet. Because the operation has been shrouded in secrecy, however, there has been no public discussion about the pros and cons of using a cyberweapon in the way Stuxnet was used. Among the top concerns is that other countries, seeing Stuxnet apparently used by the United States and Israel, might conclude that they would also be justified in carrying out a cyberattack. The British author Misha Glenny, writing in the Financial Times, argued that the deployment of Stuxnet may be seen "as a starting gun; countries around the world can now argue that it is legitimate to use malware pre-emptively against their enemies." Another concern is that the malicious software code in Stuxnet, instructing computers to order Iranian centrifuges to spin out of control, could be modified and used against U.S. infrastructure assets. "Now that technology is out there," cautions Michigan Rep. Mike Rogers, the Republican chairman of the House Permanent Select Committee on Intelligence. "People are taking a look at it. We are just a few lines of code away from someone else getting closer to a very sophisticated piece of malware that they either wittingly or unwittingly unleash across the world [and cause] huge, huge damage." The absence of debate over the pros and cons of using cyberweapons is in sharp contrast to the discussion of nuclear weapons. The United States has adopted a "declaratory policy" regarding why it has nuclear weapons and when it would be justified to use them. There is nothing comparable for the cyberweapon arsenal. Rep. Rogers says such gaps in military doctrine and strategy indicate that developments on the cyberwar front are getting ahead of U.S. thinking about cyberwar. "The capabilities, I think, are keeping pace with technology," Rogers said in an interview with NPR. "It's the policy that I worry about. We have not fully rounded out what our [cyber] policies are." The advantages of using cyberweapons are clear. They are more precise than bombs or missiles, and because they damage data rather than physical installations, they are far less likely to hurt innocent civilians. But they are new weapons, and critics say their use should be given careful consideration. "If we are allowing ourselves to go on the offense without thinking about it, we're likely to militarize cyberspace," says the Atlantic Council's Jason Healey. "We will end up with a cyberspace where everyone is attacking everyone else. I don't believe we need to go on the offense just yet. The downside is higher than the government acknowledges."

**Digital cat and mouse between the US and China on the law of armed conflict guarantees miscalc and escalation**

**VornDick 13**, Wilson,lieutenant commander in the U.S. Navy, where he is assigned to the Pentagon. Previously, he worked at the Chinese Maritime Studies Institute at the U.S. Naval War College, "The Real U.S.-Chinese Cyber Problem", 6/30, 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. Chinese Concepts of War Containment, War Control & ROE 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.

#### Cyber attack by China means the US escalates the conflict

Dobbins et al. ‘11

[Ambassador James F. Dobbins, a veteran diplomat and the current director of the RAND International Security and Defense Policy Center as well the US special representative for Afghanistan and Pakistan. David C. Gompert was Principal Deputy Director of National Intelligence from 2009 to 2010. During 2010, he served as Acting Director of National Intelligence, in which capacity he provided strategic oversight of the U.S. Intelligence Community, and acted as the President's chief intelligence advisor. Gompert is currently Distinguished Visiting Professor for National Security Studies at the United States Naval Academy, and Adjunct Senior Fellow of the RAND Corporation. He is a Trustee of Hopkins House Academy, a Director of the Rufus Porter Museum, a Director of Global Integrated Security (USA), Inc., a member of the Advisory Board of the Naval Academy Center for Cyber Security Studies, and Chairman of the Advisory Board of the Institute for the Study of Early Childhood Education. David A. Shlapak, Senior International Policy Analyst @ RAND. Andrew Scobell is a senior political scientist at the RAND Corporation. Prior to this he was an associate professor of international affairs at the George H. W. Bush School of Government and Public Service (with tenure) and director of the China certificate program at Texas A&M University in College Station, Texas. From 1999 until 2007, he was associate research professor in the Strategic Studies Institute at the U.S. Army War College and adjunct professor of political science at Dickinson College. http://www.rand.org/content/dam/rand/pubs/occasional\_papers/2011/RAND\_OP344.pdf ETB]

**The difficulties of direct defense could be greatly accelerated by Chinese** development and ¶ **use of cyber-attack** and ASAT weapons, given the dependence of U.S. forces and operating ¶ concepts on computer-networked and space-based C4ISR. For this reason, the PLA appears to ¶ think that hostilities in space and cyber-space would favor China, and so might initiate them. ¶ At the same time, as China extends the reach of its own forces and C4ISR into the Pacific, they will become vulnerable to U.S. cyber-attack and ASAT. In any case, **any Sino-U.S. armed** ¶ **conflict will be increasingly affected if not decided by warfare in these new domains.** ¶ **The** erosion of capabilities **for direct defense will push the U**nited **S**tates toward enhanced ¶ weapons, ranges, geography, and targets both to regain survivability and to strike Chinese ¶ forces, launchers, sensors, and other capabilities on the mainland (or elsewhere in the region ¶ outside of the immediate theater). In addition, as the PLA develops cyber and ASAT capabilities but also comes to rely more on advanced C4ISR, the United States will have to consider ¶ striking Chinese satellites and computer networks. These trends will thus lead both sides to ¶ widen their choice of targets in order to achieve dominance over any particular geographic ¶ objective, however limited. ¶ **The increasing difficulty in ensuring direct defense can be consequential** even if **Sino-U.S.** ¶hostilities are unlikely**, for they could stimulate Chinese risk-taking, increase U.S. inhibitions,** ¶ **and** weaken the resolve **of U.S. allies and China’s neighbors in facing a China more insistent** ¶ **on settling disputes on its terms.** These trends are the result of underlying general technological progress, sustainable growth in military spending, PLA reform and doctrinal adaptation, ¶ and geographic distances for China and the United States. On the other hand, most of China’s ¶ neighbors are growing economically and in technological sophistication, and some may choose ¶ to keep pace in quality if not quantity with Chinese advances in the military field.

**Presidential discretion causes Russia and China to use nuclear first strike**

**Rothschild 13**, Matthew, the editor of The Progressive magazine, “The Dangers of Obama’s Cyber War Power Grab,” February 4th, http://progressive.org/dangers-of-obama-cyber-war-power-grab

According to The New York Times, the Obama Administration has concluded that the President has the authority to launch preemptive cyberattacks. This is a very dangerous**,** and very undemocratic power grab**.** There are no checks or balances when the President, alone, decides when to engage in an act of war. And this new aggressive stance will lead to a cyber arms race. The United States has evidently already used cyber weapons against Iran, and so many other countries will assume that cyber warfare is an acceptable tool and will try to use it themselves. Most troubling, U.S. cybersupremacy—and that is Pentagon doctrine—will also raise fears among nuclear powers like Russia, China, and North Korea that the United States may use a cyberattack as the opening move in a nuclear attack. For if the United States can knock out the command and control structure of an enemy’s nuclear arsenal, it can then launch an all-out nuclear attack on that enemy with impunity. This would make such nuclear powers more ready to launch their nuclear weapons preemptively for fear that they would be rendered useless. So we’ve just moved a little closer to midnight. Now, I don’t think Obama would use cyberwafare as a first strike in a nuclear war. But our adversaries may not be so sure, either about Obama or his successors. They, too, worry about the temptations of a President.

#### War with China goes nuclear

**Kulacki 12**, Gregory, Senior Analyst & China Project Manager for the Global Security Program at the Union of Concerned Scientists, “The Risk of Nuclear War with China,” 9/21, <http://www.huffingtonpost.com/gregory-kulacki/the-risk-of-nuclear-war-w_b_1903336.html>

Last week two separate studies warned that China and the United States are pursuing military strategies and implementing defense policies that could lead to a nuclear war. John Lewis and Xue Litai of Stanford University concluded a detailed exposition of China's nuclear war plans with a very sober warning. "Both sides, clinging to incongruous assessments, run the risk of provoking unanticipated escalation to nuclear war by seeking a quick victory or tactical advantages in a conventional conflict. This dilemma is not only real, but perilous." Thomas Christensen of Princeton expressed concern about the same problem; the possibility that a conventional military conflict between the United States and China could end in a nuclear exchange. "For example, if strikes by the United States on China's conventional coercive capabilities or their critical command and control nodes and supporting infrastructure were to appear in Beijing as a conventional attack on its nuclear retaliatory capability or as a precursor to a nuclear first strike, even a China that generally adheres to a No-First-Use posture might escalate to the nuclear level." Neither study suggests that the military or political leadership of China or the United States intends to resort to nuclear weapons in the event of a military conflict. China's commitment not to be the first to use nuclear weapons "at any time under any circumstances" is drilled into the officers and soldiers of China's strategic missile forces. A classified text used to train those forces, The Science of Second Artillery Operations, unambiguously instructs, "In accord with our national principle not to be the first to use nuclear weapons under any circumstances, the Second Artillery's strategic nuclear forces can carry out a retaliatory nuclear attack against the enemy, following the command of the 'high leadership,' only after the enemy has first attacked us with nuclear weapons." Although the United States is unwilling to make a similar commitment, U.S. superiority in conventional weapons and overall military capabilities makes it unlikely the United States would consider using nuclear weapons for any purpose other than preventing a Chinese nuclear attack on the United States. The most recent U.S. Nuclear Posture Review, in an effort to deemphasize the role of nuclear weapons in U.S. defense policy, declared that the "fundamental role of U.S. nuclear weapons...is to deter a nuclear attack on the United States, our allies and partners." The risk of a nuclear war with China lies in the potential for misunderstanding or miscommunication during a conventional conflict. China's current strategy for employing its conventional and nuclear missile forces during a future conflict with the United States is self-consciously designed to create uncertainty, with the expectation that uncertainty will restrain U.S. military action. Unfortunately, China's strategy could also precipitate a large-scale U.S. attack on China's missile forces. There are several Chinese military policies that might confuse U.S. decision-makers in a time of war. Some Chinese conventional missiles are located on the same missile bases as Chinese nuclear missiles. Some Chinese missiles, particularly the DF-21, can be armed with either a conventional or a nuclear warhead. Chinese conventional war plans call for long-range "strategic" conventional missile strikes at key enemy targets, including U.S. military bases on allied soil and the continental United States. If this were not confusing enough already, The Science of Second Artillery Operations contains a section on "lowering the nuclear threshold" that details procedures for alerting China's nuclear forces in a crisis for the express purpose of forcing a halt to an enemy's conventional attacks on a select group of targets, such as Chinese nuclear power plants, large dams and civilian population centers. Although the Science of Second Artillery Operations unambiguously states that if alerting China's nuclear missile forces fails to halt conventional enemy attacks China will hold firm to its "no first use" commitment, U.S. decision-makers might not believe it. Indeed, U.S. interlocutors have repeatedly told their Chinese counterparts that they do not find China's "no first use" pledge credible. The combination of these factors makes a nuclear exchange between the United States and China not only plausible, but also probable if the two countries were to become embroiled in a military conflict. As Lewis and Xue explain, "If, in a time of high tension, the Chinese command authorized a conventional missile attack as an act of preemptive self-defense, the enemy and its allies could not know if the incoming missiles were conventional or nuclear. In a worst-case scenario, a Chinese first-strike conventional attack could spark retaliation that destroys Chinese nuclear assets, creating a situation in which escalation to full-scale nuclear war would not just be possible, but even likely." The Obama administration is "rebalancing" U.S. military forces in response to perceived relative increases in Chinese military capabilities. China sees this so-called "pivot" to Asia, especially when pared with new U.S. military strategies such as "Air-Sea Battle," as a policy of containment. Both sides downplay the risks of conflict, but they also see each other as potential adversaries, and are hedging their diplomatic bets with expensive investments in new military hardware, including new technologies that will expand the conflict into cyberspace and outer space. Territorial disputes between China and U.S. allies, rising nationalist sentiment in the region, and the potential for domestic political instability within China could produce any number of casussen belli that could trigger the conventional conflict that carries the risk of ending in a nuclear war.

**China will cyberstrike in space**

**Gertz 13**, Bill Gertz, 7-30-’13 (lectured on defense, national security, and media issues at the Defense Department’s National Security Leadership Program, Johns Hopkins University School of Advanced International Studies, the FBI National Academy, the National Defense University, and the CIA , media fellow at the Hoover Institution on War, Revolution and Peace at Stanford University, editor of the Washington Free Beacon. Prior to joining the Beacon he was a national security reporter, editor, and columnist for 27 years at the Washington Times. Bill is the author of six books, four of which were national bestsellers. ,“China’s Military Preparing for ‘People’s War’ in Cyberspace, Space” , The Washington Free Bacon, <http://freebeacon.com/china-military-preparing-for-peoples-war-in-cyberspace-space/>)

Translated report reveals high-tech plans for cyber attacks, anti-satellite strikes”, ¶ China’s military is preparing for war in cyberspace involving space attacks on satellites and the use of both military and civilian personnel for a digital “people’s war,” according to an internal Chinese defense report.¶ “As cyber technology continues to develop, cyber warfare has quietly begun,” the report concludes, noting that the ability to wage cyber war in space is vital for China’s military modernization.¶ According to the report, strategic warfare in the past was built on nuclear weapons. “But strategic warfare in the information age is cyber warfare,” the report said.¶ “With the reliance of information warfare on space, cyberspace will surely become a hot spot in the struggle for cyberspace control,” the report said.¶ The new details of Chinese plans for cyber and space warfare were revealed in a report “Study on Space Cyber Warfare” by four engineers working at a Chinese defense research center in Shanghai.¶ The report presents a rare inside look of one of Beijing’s most secret military programs: Cyber warfare plans against the United States in a future conflict.¶ “Cyber warfare is not limited to military personnel. All personnel with special knowledge and skills on information system may participate in the execution of cyber warfare. Cyber warfare may truly be called a people’s warfare,” the report says.¶ People’s War was first developed by China’s Communist founder Mao Zedong as a Marxist-Leninist insurgency and guerrilla warfare concept. The article provides evidence that Chinese military theorists are adapting Mao’s peasant uprising stratagem for a future conflict with the United States.¶ A defense official said the report was recently circulated in military and intelligence circles. Its publication came as a surprise to many in the Pentagon because in the past, U.S. translations of Chinese military documents on similar warfighting capabilities were not translated under a directive from policy officials seeking to prevent disclosure of Chinese military writings the officials feared could upset U.S.-China relations.¶ A Chinese government spokesman could not be reached for comment. However, Chinese spokesmen in the past have denied reports that China engages in cyber attacks.¶ The study links China’s space warfare development programs with its extensive cyber warfare capabilities. Both programs are considered “trump card” weapons that would allow a weaker China to defeat a militarily stronger United States in a conflict.¶ “Cyber warfare is an act of war that utilizes space technology; it combines space technology and cyber technology and maintains and seizes the control of cyberspace,” the study says.¶ Because cyberspace relies on satellites, “space will surely be the main battlefield of cyber warfare,” the report said.¶ Satellites and space vehicles are considered the “outer nodes” of cyber space and “are clear targets for attack and may be approached directly,” the report said, adding that ground-based cyberspace nodes are more concealed and thus more difficult to attack.¶ Additionally, satellites have limited defenses and anti-jamming capabilities, leaving them very vulnerable to attack.¶ The report reveals that China’s military, which controls the country’s rapidly growing space program, is preparing to conduct space-based cyber warfare—“cyber reconnaissance, jamming, and attack”—from space vehicles.¶ Space-based cyber warfare will include three categories: space cyber attack, space cyber defense, and space cyber support. The space cyber support involves reconnaissance, targeting, and intelligence gathering.¶ “A space cyber-attack is carried out using space technology and methods of hard kill and soft kill,” the report said. “It ensures its own control at will while at the same time uses cyberspace to disable, weaken, disrupt, and destroy the enemy’s cyber actions or cyber installations.”

**That causes extinction**

**Mitchell, et al 01** -Associate Professor of Communication and Director of Debate at the University of Pittsburgh (Dr. Gordon, ISIS Briefing on Ballistic Missile Defence, “Missile Defence:  Trans-Atlantic Diplomacy at a Crossroads”, No. 6 July, <http://www.isisuk.demon.co.uk/0811/isis/uk/bmd/no6.html>)

A buildup of space weapons might begin with noble intentions of 'peace through strength' deterrence, but this rationale glosses over the tendency that '… the presence of space weapons…will result in the increased likelihood of their use'.33 This drift toward usage is strengthened by a strategic fact elucidated by Frank Barnaby: when it comes to arming the heavens, 'anti-ballistic missiles and anti-satellite warfare technologies go hand-in-hand'.34  The interlocking nature of offense and defense in military space technology stems from the inherent 'dual capability' of spaceborne weapon components. As Marc Vidricaire, Delegation of Canada to the UN Conference on Disarmament, explains: 'If you want to intercept something in space, you could use the same capability to target something on land'. 35 To the extent that ballistic missile interceptors based in space can knock out enemy missiles in mid-flight, such interceptors can also be used as orbiting 'Death Stars', capable of sending munitions hurtling through the Earth's atmosphere.  The dizzying speed of space warfare would introduce intense 'use or lose' pressure into strategic calculations, with the spectre of split-second attacks creating incentives to rig orbiting Death Stars with automated 'hair trigger' devices. In theory, this automation would enhance survivability of vulnerable space weapon platforms. However, by taking the decision to commit violence out of human hands and endowing computers with authority to make war, military planners could sow insidious seeds of accidental conflict.  Yale sociologist Charles Perrow has analyzed 'complexly interactive, tightly coupled' industrial systems such as space weapons, which have many sophisticated components that all depend on each other's flawless performance. According to Perrow, this interlocking complexity makes it impossible to foresee all the different ways such systems could fail. As Perrow explains, '[t]he odd term "normal accident" is meant to signal that, given the system characteristics, multiple and unexpected interactions of failures are inevitable'.36Deployment of space weapons with pre-delegated authority to fire death rays or unleash killer projectiles would likely make war itself inevitable, given the susceptibility of such systems to 'normal accidents'.  It is chilling to contemplate the possible effects of a space war. According to retired Lt. Col. Robert M. Bowman, 'even a tiny projectile reentering from space strikes the earth with such high velocity that it can do enormous damage — even more than would be done by a nuclear weapon of the same size!'. 37 In the same Star Wars technology touted as a quintessential tool of peace, defence analyst David Langford sees one of the most destabilizing offensive weapons ever conceived: 'One imagines dead cities of microwave-grilled people'.38 Given this unique potential for destruction, it is not hard to imagine that any nation subjected to space weapon attack would retaliate with maximum force, including use of nuclear, biological, and/or chemical weapons. An accidental war sparked by a computer glitch in space could plunge the world into the most destructive military conflict ever seen.

**US-Russia cyber conflict escalates**

Cimbala 12, Stephen J, Professor of Political Science at Penn State, “Chasing its Tail” 2012 www.au.af.mil/au/ssq/2012/summer/cimbala.pdf

Related to this possibility, Russia’s war against Georgia in August 2008 demonstrated how cyber war and information operations might be used in support of conventional military operations. The Russian cyber campaign reportedly attacked some 38 Georgian and Western websites upon the outbreak of war, including ranking Georgian government oices and the US and British embassies in Georgia, and appeared to be centrally directed and coordinated with the tempo of force operations. 26 Instead of a single integrated operational plan (SIOP), however lexible, for ighting a nuclear war if deterrence failed, planners would have to devise a matrix of plans linking information strike with kinetic options. How complicated this might be is probably beyond the power of mere mortals to demonstrate with any proiciency—much is speculative as to the two-way complexity of combined cyber and nuclear or conventional kinetic attacks. On the other hand, analysts and planners must do what they can in the face of questions and demands for performance that will not go away. A simpliied approach to one aspect of a cyber-soaked SIOP might be illustrated as follows. Let us assume that both the United States and Russia were required to carry out second-strike retaliation after having absorbed both cyber and kinetic first strikes. To measure the impact of such strikes, we estimate that the cyber component directly or indirectly neutralizes as many surviving and retaliating weapons as does the kinetic portion. The second-strike surviving forces would therefore be in a position equivalent to that of a third striker in a series of exchanges without information weapons. In effect, they would be fighting World War III-b. he additive efects of both cyber and kinetic strikes are summarized in igures 5 and 6 repre­ senting the 1,000- and 500-weapon prewar deployment limit (without defenses), respectively. Figures 5 and 6 show that, in a hypothetical but not necessarily unrealistic exercise of cyber-kinetic nuclear strike plans, the United States and Russia could still retain sufficient numbers of weapons to create historically un­ precedented and socially unacceptable damage in retaliation. Cyber attacks on command-control, communications, and warning systems might lead to ragged retaliations and strikes more dependent upon the most survivable launch platforms such as submarines and mobile missiles. Alternatively, two expectations about such a scenario would be mistaken. First, information operations cannot make any nuclear war between states with large arsenals into a surgical operation or an exercise in “soft” power. Second, a state’s cyber and kinetic strategies need to be carefully coordinated as to their political and military objectives, not only up to the brink of war but even beyond that threshold. Otherwise, the objectives of escalation control and conflict termination will be impossible to realize for either state when its op­ posite number is brain dead as well as partly but not completely disarmed. Faced with exigent threats, states with cyber capabilities will be tempted to employ them to good effect. For example, imagine a replay of the Cuban missile crisis between a future Russia and the United States, with Rus­ sia having deployed nuclear-capable missiles and/or warheads into South Ossetia. Or, to lip the example, hypothesize a NATO missile defense installation deployed to protect Tbilisi or Kiev, supported by short- and medium-range ballistic missiles as a trip wire. One can expect that cyber operations of the information-technical type (attacking enemy systems and networks) as well as the information-psychological variety (inluenc­ ing public opinion among foreign and domestic audiences, including elites and general publics) will commend themselves to peacetime and crisis political leaders and their military advisors.

**Extinction**

Corcoran 9 (PhD, Senior Fellow @ Global Security, Frmr. Strategic Analyst at the US Army War College where he chaired studies for the Office of the Deputy Chief of Operations and member of the National Advisory Board for the Alsos Digital Library for Nuclear Issues, we win the qualification game, 4/21, http://sitrep.globalsecurity.org/articles/090421301-strategic-nuclear-targets.htm)

That brings us to Russia, our former main adversary, now a competitive partner and still a potential future adversary, particularly as relations have gradually soured in recent years. Russia is the only other nation with a formidable arsenal of some three thousand strategic weapons. Our opposing arsenals were built up in the period when Mutually Assured Destruction (MAD) was the underlying strategic concept -- each side deterred from striking the other by the prospect of assured retaliatory destruction. The situation became even madder as both sides worked to develop a capability to destroy the other's strike force with a crippling first strike. This resulted in further large increases in the sizes of the arsenals, as well as early warning systems and hair-trigger launch-on-warning alert procedures. The final result was an overall system in which each side could destroy the other in a matter of minutes. And it also raised another chilling specter, Nuclear Winter, in which the atmospheric dust raised from a major nuclear exchange would block sunlight for an extended period and essentially destroy human civilization globally. The collapse of the Soviet Union collapsed this threat, but did not eliminate it. US and Russian nuclear forces remained frozen in adversarial positions. The May 2002 Moscow Treaty began to address this legacy and is leading to a reduction in strategic nuclear forces down to levels of about two thousand on each side by 2012. These levels are still sufficient to destroy not only both nations but also human civilization. It is hard to even construct scenarios where the use of even a few strategic nuclear weapons does not risk a total escalation. Strikes on Russian warning facilities or strike forces would almost certainly bring a wave of retaliatory strikes. Strikes on hardened command centers would be of questionable effectiveness and also risk total escalation. In addition, successful elimination of Russian leaders could greatly complicate any efforts to stop escalation short of a total nuclear exchange.

**US opinio juris key**

**Watts 10/10**, Sean, Professor of Law at Creighton University Law School where he teaches Constitutional Law, Federal Courts, Federal Habeas Corpus, Law of Armed Conflict, International Criminal Law, and Military Law, “Guest Post: Reviving Opinio Juris and Law of Armed Conflict Pluralism,” 10/10, http://justsecurity.org/2013/10/10/reviving-opinio-juris-law-armed-conflict-pluralism-2/

Admittedly, government representatives’ presentations and public writings still offer highly relevant and informed perspectives on LOAC. Yet the absence of official government opinions unequivocally stated inevitably robs the conversation of a degree of magnitude, significance, and clarity. Is it any wonder that lawyers exhaustively deconstruct the comments of a State Department Legal Advisor when he is willing to speak disclaimer-free? Conditioned to a wet blanket of disclaimers, the LOAC community craves official views. **The stifling effect** of official disclaimers is not limited to academic panels and conferences. State disclaimers, legal equivocation, and worse, silence extend to the general dialogue of LOAC. The result is an **increasingly unbalanced LOAC colloquy**, deprived of the pluralistic balance of State and non-State, military and humanitarian, European and American perspectives that would enrich and balance the development and direction of LOAC. It has not always been so. Recent LOAC history reveals episodes of rough proportionality between State opinio juris and non-State expressions of law. In the immediate aftermath of the Second World War, non-State actors produced important and influential interpretations of LOAC such as Jean Pictet’s 1949 Geneva Convention Commentaries. Scholars, non-governmental groups, and international organizations produced persuasive, even fairly authoritative constructions of LOAC and treaty proposals. Jurists also made important contributions to LOAC through reasoned judgments and briefs in war crimes trials. The United States kept pace for a time. U.S.-convened and supported criminal prosecutions of war crimes were instrumental to the development and efficacy of LOAC. The U.S. also produced comprehensive LOAC analyses and guidance for its armed forces such as the influential 1956 U.S. Army Field Manual on the Law of Land Warfare. In 1996, despite enjoying relative peace, U.S. attention to and concern for the development of LOAC even extended to submitting an amicus curiae brief in the seminal Tadić case at the International Criminal Tribunal for Former Yugoslavia. The result of these efforts was a more pluralistic, balanced, and active LOAC dialogue – a rough proportionality between State and non-State input on this critical and central facet of international law. Today’s international LOAC dialogue appears in stark contrast to the vibrant and pluralistic exchanges of the past. To be sure, non-State LOAC commentary continues to thrive. Legal journals routinely feature challenging LOAC articles, library shelves groan under ever-expanding collections of impressive LOAC doctoral dissertations, and war crimes tribunal judgments run to 1300 pages or more. All the while, humanitarian organizations publish extraordinary and imposing multi-volume LOAC studies, with more in development. And “groups of experts” publish private manuals on a growing number of LOAC topics, available here, here, and here. Meanwhile, the U.S. guns of LOAC opinio juris have fallen nearly silent. The 1956 Army Field Manual remains in service, still the only comprehensive and inter-service law-of-war manual. Interagency bickering and turf battles stymie decades-long efforts to publish crucial legal and operational guidance. Long-promised updates appear to be in the works, as they have been for decades. However, the fact remains that despite the addition of nearly a dozen major LOAC treaties since publication and despite well over fifty years of regularly occurring armed conflict, U.S. military lawyers deploy with the law-of-war manual of their grandfathers. U.S. inactivity and silence is not limited to national military legal doctrine. International criminal convictions grounded in interpretations directly at odds with U.S. understandings of targeting rules provoke virtual silence, leaving only former officers to respond in their private capacities. The ICRC’s now authoritative, 3000-page customary IHL study inspires not a competing product, but rather a 29-page “cross-section[al]” review, focused primarily on general international law methodology. Drastic reinterpretations of fundamental legal guidance for detainee status determinations and armed conflict classification by the Department of Justice and White House are not published as open contributions to LOAC doctrine and dialogue. They are buried in classified legal opinions, unavailable until leaked, even to military lawyers responsible for developing and teaching U.S. LOAC doctrine. Emerging forms of warfare and a broadening operational spectrum provoke “law by analogy” or merely policy statements rather than definitive legal analysis. And meanwhile the ongoing proliferation of private LOAC manuals inspires no substantial, official response. It is no wonder the U.S. Supreme Court mistakes Pictet’s Commentary as “the official commentary to the [Geneva] Conventions” (see n.48), despite the authors’ disclaimer to the contrary. It is no wonder international war crimes tribunals cite humanitarian organizations’ reports and studies rather than States’ opinio juris. The U.S. government and many other specifically-affected States offer them little choice. It is necessary to remember that States and their agents enjoy unique relevance in the formation and interpretation of international law and LOAC. As the primary authors and subjects of LOAC, States should actively shape its content and direction, through both direct means, such as treaty formation and state practice, and indirect means, such as positions proffered in litigation, legal publications, public statements, and diplomatic communications. Even as scholars challenge sovereign-centric understandings of international law, near universal respect endures for the special role of sovereigns in the formation of international law. To coopt and modify a common observation with respect to Originalism in constitutional interpretation, “Everyone is a Sovereigntist sometimes.” That is, what distinguishes dyed-in-the-wool international law Sovereigntists from non-Sovereigntists is probably not acceptance of the legitimacy of State input but rather attitudes toward non-State actors’ international legal contributions. Few international lawyers contest that resort to State expressions of opinio juris constitutes a principled method of interpretation. Disagreements seem instead to concern the effect that absence of State opinio juris has on an international norm. And while there is surely value in the balanced pluralism that results from having both State and non-State contributions to LOAC, State input has always been singularly significant. State opinio juris remains the critical bellwether for the degree of consensus, acceptance, and therefore effectiveness and legitimacy of any international legal rule. In addition to formal authority, States possess unique competency, facility with, and access to the inputs of LOAC. While many grasp the harsh consequences of armed conflict, few outside the ambit of States’ defense agencies and armed forces fully appreciate armed conflict’s operational challenges, demands, and limitations, so essential to striking the delicate LOAC balance between military necessity and humanity. Not unlike the government speaker’s conference disclaimer, the effect of States’ retreat from LOAC dialogue is an impoverishment of dialogue. LOAC discussions, debates, and deliberations, both descriptive and normative, founder in the absence of authoritative State opinio juris. Whatever one’s opinion of the substantive quality or correctness of State opinio juris, State legal opinions provide indispensable control samples for meaningful analyses and critiques. The efforts of legal practitioners and scholars, commanders and humanitarian workers, advocates and judges all suffer when States do not make clear and frequently update their views on the content, interpretation, and future direction of LOAC. Parity of input, especially in quantitative terms, is surely too much to demand and surely not necessary given the special status of State opinio juris. However, States’ legal agencies and agents should be equipped, organized, and empowered to participate actively in the interpretation and development of LOAC. States, and specially-affected States in particular, should make active responses to emerging LOAC scholarship, investigations and jurisprudence a regular facet of their opinio juris. Reinvigorating opinio juris would do far more than satisfy international law sovereigntists. It would go a long way toward reestablishing the pluralistic LOAC dialogue that formerly tested, updated, and enriched the balance between military necessity and humanity. This post surely leaves a number of associated issues unaddressed and assumptions unexplained. For instance, the causes of and motives behind U.S. LOAC opinio juris atrophy are undoubtedly complex and not fully understood. Is desire to maintain operational and diplomatic flexibility to blame? Does retreat from opinio juris reflect a deliberate and considered evaluation of the costs and benefits of silence? Are institutional competence, bureaucratic friction, or organizational culture to blame? Or is ascendancy of a general international law skepticism the cause? Whatever the true causes or motives of the U.S. retreat to the sidelines of LOAC, more active U.S. participation would be a meaningful step toward restoring a truly pluralistic LOAC.

**International law in cyberspace is shaped by norms about what constitutes a use of force**

**Brown and Poellet 12** <Colonel Gary Brown, JD Senior Legal Counsel for U.S. Cyber Command, Fort Meade, Maryland and Keira Pollet, JD and LLM Judge Advocate General and former Operations Law Attorney at US CYBERCOM, Strategic Studies Quarterly, Fall 2012, The Customary International Law of Cyberspace. [www.au.af.mil/au/ssq/2012/fall/brown-poellet.pdf](http://www.au.af.mil/au/ssq/2012/fall/brown-poellet.pdf)?>

The international legal system operates under its own rules, which are established by consensus and are fundamentally different than domestic law. The law of war is driven almost entirely by the effect of actions rather than by some sort of “national mens rea.”46 The intent of an actor taking an action against another state that could be interpreted as hostile is, for practical purposes, irrelevant to the international law analysis. All this leads back to the current international legal regime governing cyber activities. The question is whether state practice coincides with these norms and whether states are complying out of a sense of legal obligation. Otherwise, it is still the “Wild West” when it comes to behavior in cyberspace.¶ In general, cyberspace is a permissive regime, analogous to the espionage rule set—little is prohibited, but states can still do their best to prevent others from playing in the arena. There is also nothing to prevent states from prohibiting cyber behavior with national laws. Specifically, as long as cyber activity remains below the level of a use of force and does not otherwise interfere with the target nation’s sovereignty, it would not be prohibited by international law, regardless of the actor’s intent. ¶ One important caveat is that aggressive cyber activities resulting in kinetic effects (i.e., physical destruction, damage, or injury) are covered by the law regarding the use of force and armed attack. They are kinetic events, governed by the traditional law of war just like kinetic effects caused by more traditional means of warfare. So, for example, a cyber event resulting in the physical destruction of a power plant turbine would be a military attack subject to the same international law governing any other kinetic attack.47 Although determining exactly what constitutes a kinetic effect is not always simple, this line is as clear as others governing the murky corners of customary law and is clear enough effectively to distinguish cyber attacks from something less. One example of the gray area is a cyber action against an electric power grid that causes it to temporarily cease functioning. Although no actual kinetic event may occur, the reliance of modern societies on electricity for health care, communications, and the delivery of essential services makes it clear this would qualify as a kinetic-like effect and would therefore constitute a military attack if the disruption were for a significant period of time.48

**Clarity in the legal language about what constitutes an act of war is key to reign in escalation of cyber conflict**

Rosenzweig 9,

(Paul, founder of Reid Branch Consulting, specializing in homeland security, senior advisor to the Chertoff Group, Carnegie Fellow at Northwestern, professor at National Defense University, Editorial board at the Journal of National Security Law & Policy, deputy assistant secretary for policy at the US Department of Homeland Security, "National Security Threatsin Cyberspace" merican Bar Association Standing Committee on Law andNational Security And National Strategy Forum, September 2009, [www.utexas.edu/law/journals/tlr/sources/Issue%2088.7/Jensen/fn137.Rosenwieg.pdf](http://www.utexas.edu/law/journals/tlr/sources/Issue%2088.7/Jensen/fn137.Rosenwieg.pdf))

Offensive dominance creates a great risk of cyber arms races. State and non-state actors are likely to view the prevalence of offensive cyber threats as a legitimate rationale for bolstering their own capabilities, both defensive and offensive, thus fueling an action-reaction dynamic of iterative arming. Experts believe that at least 20 nations are engaged in a cyber arms competition and possess the type of advanced capabilities needed to wage cyber war against the United States.121 As Michael Nacht, Former Assistant Secretary of Defense for Global Strategic Affairs, told us, “An arms race is already going on in cyberspace and it is very intense.”122 Conflict in cyberspace is uniquely predisposed to escalation given uncertainties about what constitutes an act of war and the growing number of state and non-state actors seeking offensive capabilities. Actors are more likely to misperceive or miscalculate actions in cyberspace, where there is no widely understood strategic language for signaling intent, capability and resolve.123 Uncertainty will encourage states to prepare for worst-case contingencies, a condition that could fuel escalation. Furthermore, “false flag” attacks, in which an actor purposefully makes an attack look like it came from a third party, could also ignite a conflict.124

Cyber attacks on infrastructure destroy the economy

AAP 13 AAP (Australian Associated Press) 06/12/13, Cyber wars would cripple economies: experts, http://www.businessspectator.com.au/news/2013/6/12/global-news/cyber-wars-would-cripple-economies-experts, (08/13/13

Cyber attackers have the power to shut down economies and a global cyber war could cause destruction on the scale of an atomic war, a cyber security expert says.¶ United States cyber security expert Scott Borg told a conference in Canberra that cyber attackers could completely destroy power generators using malicious software code.¶ "We are talking about nuclear exchange level destruction by pure cyber attack," Mr Borg added.¶ A loss of electric power for a few days would cause limited damage but a widespread shutdown beyond eight to ten days could effectively halt a nation's economy for months.¶ Speaking at the Australian Defence Magazine Cyber Security summit in Canberra, he said similar attacks could be mounted against other critical infrastructure like oil pipelines or refineries, railways and the financial sector.¶ Food and medicine distribution would be affected, along with transport and access to other necessities like heating.¶ "If you shut down the economy to that degree, we're not talking about people being inconvenienced," Mr Borg said. ¶ "In America, it's hundreds of thousands - maybe millions - die.¶ "For any other part of the world it's similar destruction."

#### Economic decline causes nuclear war.

ROYAL ‘10 – Director of Cooperative Threat Reduction at the U.S. Department of Defense (Jedediah, “Economic Integration, Economic Signaling and the Problem of Economic Crises,” in Economics of War and Peace: Economic, Legal and Political Perspectives, ed. Goldsmith and Brauer, p. 213-215)

Less intuitive is how periods of economic decline may increase the likelihood of external conflict. Political science literature has contributed a moderate degree of attention to the impact of economic decline and the security and defence behaviour of interdependent states. Research in this vein has been considered at systemic, dyadic and national levels. Several notable contributions follow. First, on the systemic level, Pollins (2008) advances Modelski and Thompson's (1996) work on leadership cycle theory, finding that rhythms in the global economy are associated with the rise and fall of a pre-eminent power and the often bloody transition from one pre-eminent leader to the next. As such, exogenous shocks such as economic crises could usher in a redistribution of relative power (see also Gilpin. 1981) that leads to uncertainty about power balances, increasing the risk of miscalculation (Feaver, 1995). Alternatively, even a relatively certain redistribution of power could lead to a permissive environment for conflict as a rising power may seek to challenge a declining power (Werner. 1999). Separately, Pollins (1996) also shows that global economic cycles combined with parallel leadership cycles impact the likelihood of conflict among major, medium and small powers, although he suggests that the causes and connections between global economic conditions and security conditions remain unknown. Second, on a dyadic level, Copeland's (1996, 2000) theory of trade expectations suggests that 'future expectation of trade' is a significant variable in understanding economic conditions and security behaviour of states. He argues that interdependent states are likely to gain pacific benefits from trade so long as they have an optimistic view of future trade relations. However, if the expectations of future trade decline, particularly for difficult to replace items such as energy resources, the likelihood for conflict increases, as states will be inclined to use force to gain access to those resources. Crises could potentially be the trigger for decreased trade expectations either on its own or because it triggers protectionist moves by interdependent states.4 Third, others have considered the link between economic decline and external armed conflict at a national level. Blomberg and Hess (2002) find a strong correlation between internal conflict and external conflict, particularly during periods of economic downturn. They write: The linkages between internal and external conflict and prosperity are strong and mutually reinforcing. Economic conflict tends to spawn internal conflict, which in turn returns the favour. Moreover, the presence of a recession tends to amplify the extent to which international and external conflicts self-reinforce each other. (Blomberg & Hess, 2002. p. 89) Economic decline has also been linked with an increase in the likelihood of terrorism (Blomberg, Hess, & Weerapana, 2004), which has the capacity to spill across borders and lead to external tensions. Furthermore, crises generally reduce the popularity of a sitting government. “Diversionary theory" suggests that, when facing unpopularity arising from economic decline, sitting governments have increased incentives to fabricate external military conflicts to create a 'rally around the flag' effect. Wang (1996), DeRouen (1995). and Blomberg, Hess, and Thacker (2006) find supporting evidence showing that economic decline and use of force are at least indirectly correlated. Gelpi (1997), Miller (1999), and Kisangani and Pickering (2009) suggest that the tendency towards diversionary tactics are greater for democratic states than autocratic states, due to the fact that democratic leaders are generally more susceptible to being removed from office due to lack of domestic support. DeRouen (2000) has provided evidence showing that periods of weak economic performance in the United States, and thus weak Presidential popularity, are statistically linked to an increase in the use of force. In summary, recent economic scholarship positively correlates economic integration with an increase in the frequency of economic crises, whereas political science scholarship links economic decline with external conflict at systemic, dyadic and national levels.5 This implied connection between integration, crises and armed conflict has not featured prominently in the economic-security debate and deserves more attention. This observation is not contradictory to other perspectives that link economic interdependence with a decrease in the likelihood of external conflict, such as those mentioned in the first paragraph of this chapter. Those studies tend to focus on dyadic interdependence instead of global interdependence and do not specifically consider the occurrence of and conditions created by economic crises. As such, the view presented here should be considered ancillary to those views.

## 1AC LOAC Cred

#### The US position as a UNSC member and military superpower means its enforcement of LOAC uniquely sets precedent – compliance is key to enforcing the laws of war

**Bialke in 4** – Lt. Colonel, MA and JD at the University of North Dakota. LLM at University of Iowa. <”Al-Qaeda & Taliban Unlawful Combatant Detainees, Unlawful Belligerency, and the International Laws of Armed Conflict” 55 A.F.L. Rev. 1. Lexis>

The U.S. is in compliance with its international obligations and responsibilities. Al-Qaeda and Taliban combatants willfully engaged in unlawful belligerency en masse in violation of LOAC. Taliban combatants en masse willfully failed to meet the four criteria of lawful belligerency. Al-Qaeda combatants are stateless hostes humani generis, and also en masse willfully failed to meet the four criteria. As a matter of international law, both the Taliban and al-Qaeda are unlawful combatants. The U.S. has no requirement under international law to bestow POW status to such enemy al-Qaeda and Taliban unlawful combatants upon capture. No requirement exists to hold individual Geneva Convention art. 5 POW status tribunals to reaffirm gratuitously the unlawful combatant status of either the Taliban or al-Qaeda, nor, upon capture, their lack of POW status. The U.S. is treating humanely, beyond what is required by international standards, all al-Qaeda and Taliban unlawful combatant detainees interned at Guantanamo Bay. In accordance with customary international law, the U.S. is authorized to continue to hold these detainees until the end of armed conflict. At present, however, Taliban remnants and al-Qaeda remain a viable military threat against the national security interests of the U.S. and its allies. Unfortunately, the international armed conflict against al-Qaeda is highly likely to be long and sustained. The U.S. and its allies, through their militaries and other instruments of national power, in the exercise of their inherent right of collective self-defense, may continue to use armed force until the threat posed by al-Qaeda and its affiliates no longer exists. Al-Qaeda should not be underestimated in the wake of continuing international progress in the Global War against Terrorism. Considering al-Qaeda's declared hegemonic theocratic-political ideology, and the proven terrorist capabilities it continues to possess, al-Qaeda remains a clear and present danger to the national security interests of the U.S. and its allies. Nevertheless, the U.S. has no desire to, and will not, hold any unlawful [\*82] combatant indefinitely., When individual detainees no longer pose a significant security threat to the international community, no longer possess any intelligence value, and are not facing criminal charges, the U.S. will release them. However, an unlawful combatant detainee accused of war crimes may be tried before a U.S. military commission. n83 Beginning in November 2001, the U.S. has spent over two and one half years updating its military commission procedures; and developing a military commission system that is just, in complete compliance with contemporary U.S. and international law, and one that is consistent with U.S. national security interests and its ongoing war efforts against al-Qaeda. If convicted in such a U.S. military commission, the detainee may be further confined to serve the term of imprisonment adjudged by the military commission. However, adherence to the international Rule of Law is at the crux of this entire matter. As an influential member in the international community and full supporter of the international Rule of Law, U.S. actions in regards to al-Qaeda and Taliban detainees could not be anything less than what is noted above. The U.S. and every nation in the world have the cardinal international duty, indeed the moral imperative, to encourage compliance with, and to discourage violations of international humanitarian law and LOAC regardless of domestic or international political objections and criticisms, ensuing controversies, or the difficulties of doing so. Casually affording Geneva Convention III POW status with its greater privileges and attendant implicit legitimacy to either al-Qaeda or the Taliban would turn a blind eye to this foundational duty. n84 To grant POW status to al-Qaeda or Taliban detainees [\*83] would be to acknowledge that they are privileged combatants, and convey that they and these groups have a right to associate together and wage war in the manner that they do. It would be incorrect, irresponsible, and unwise for the U.S. to afford POW status to captured members of al-Qaeda and the Taliban as they are not entitled to, and are undeserving of this status. n85 International terrorists, and civilian-dressed combatants of a collapsed state ruled by a de facto government that willfully provides the terrorists safe haven, have never before been granted POW status upon capture in an international armed conflict. For a permanent member of the United Nations Security Council, who also is the world's premier military superpower and its leading global economic power, to do so would set a highly injudicious international legal precedent inconsistent with the Rule of Law and the long-term interests of the international community. It would recklessly foster future abuses in armed conflict by undermining directly long-standing rules of war crafted carefully to protect noncombatants [\*84] by deterring combatants in armed conflicts from pretending to be protected civilians and hiding among them. All nations and their armed forces are subject to LOAC. Combatants in armed conflict who blatantly disregard these laws are outside of them and do not, upon capture at the discretion of the capturing party, receive several of their benefits. LOAC is only effective, and civilians protected in armed conflict, when the parties to a conflict comport their belligerency to such laws, and enforce consistently strict compliance with all the provisions of such laws. Parties to a conflict are significantly more likely to observe such laws if they have both affirmative incentives for complying with them and if appreciable negative consequences follow when such laws are disregarded or violated. Designating captured members of al-Qaeda or the Taliban as POWs would consequently place protected civilians and other noncombatants into much greater peril during future armed conflicts, because unlawful combatants would no longer experience sufficient negative consequences from endangering protected noncombatants by egregiously violating international law and customs. This eventuality is not attractive. A carte blanche designation of Geneva Convention III POW status by the U.S. to Taliban and al-Qaeda unlawful combatants certainly would be politically expedient internationally. By letting captured Taliban and al-Qaeda reap and enjoy every benefit of POW status, the U.S. would mollify temporarily some U.S. detractors. But, such U.S. action would be wrong. Just as protected noncombatant civilians have borne the consequences of the Taliban and al-Qaeda's previous perfidies and patent violations of international law, protected noncombatant civilians would also then be relegated to shoulder and suffer all the concomitant burdens and costs of the Taliban and al-Qaeda being accorded POW status. Shortsighted action to placate U.S. critics and dissentients momentarily would lastingly reward, rather than penalize, all unlawful combatants who contravene international humanitarian law and LOAC intentionally, continually, and abhorrently. LOAC should never be utilized, construed, or developed in such a way that would benefit terrorists and rogue states that provide aegis to terrorists, or in such a way that would otherwise serve the ends of terrorism. The negative prices that combatants who engage in armed conflict without meeting the requirements of lawful belligerency pay, that hostes humani generis pay, and that rogue states pay for unlawfully hosting or otherwise willfully supporting hostes humani generis, must remain high. Endorsing captured al-Qaeda, the Taliban, or other agents of global terror as POWs would be inapposite, as it may be viewed as symbolically elevating their international status. It would be tantamount to bestowing tacit international recognition and credibility to their reprehensible objectives, appalling atrocities, and insidious terrorist tactics. n86 [\*85] The U.S. does not take lightly its international role, influence, obligations, and responsibilities. Classifying al-Qaeda or the Taliban captured enemy combatants as POWs under Geneva Convention III would have broad, and most undesirable ramifications. It would erode significantly a combatant's considerable, at times primary, incentive to comply with LOAC and thereby would increase substantially and unnecessarily the risks to civilians and other protected noncombatants in future armed conflicts. n87 Ultimately, woefully undercutting customary LOAC and international humanitarian law by granting POW status arbitrarily to unworthy, unlawful combatants would simply lead to an added loss of international respect for, and future observance of, long-established international armed conflict norms, customs, and laws. This would be unacceptable.

This is particularly true in the context of cyber – US restrictions of cyber is modeled

Belk and Noyes in 12 - <Robert and Matthew. “On the Use of Offensive Cyber Capabilities” March 20, 2013. http://ecir.mit.edu/images/stories/cybersecurity-pae-belk-noyes%202012.pdf>

The NRC report rightly observes that U.S. cyber operations have the potential to interfere with similar operations of our allied nations.136 When considering the damaging effects of cyber force, the U.S. should liaise with allied nations to discuss possible conflict with their cyber operations. There are myriad ways in which U.S. cyber operations could affect those of our allies, but what is critical here is the recognition that, particularly with cyber force, the U.S. should deconflict with friendly nations operating on the systems the U.S. plans to exploit.

Also, because cyberspace is a rapidly developing domain, there is great potential for norm-setting. Psychologically, there are various reasons for conforming to a particular conduct, and unanimity of action is one of the more potent methods of strengthening conformity.137 Thus, it would benefit the U.S. to support the conduct it would wish to become the norm. That is, if the U.S. has an interest, as it likely does, in restricting the use of cyber force internationally, then it should seek to adhere to this standard.

**Strong LOAC stops WMD firebreak - nuclear war only possible without LOAC Delahunty and Yoo 10** – Associate professor at the University of St. Thomas Law and Law Professor at UC Berkeley <Robert and John. 59 DePail L. Rev. 803)

Finally, the extension of IHRL to armed conflict may have significant consequences for the success of international law in advancing global welfare. Rules of the LOAC represent the delicate balancing between the imperatives of combat and the humanitarian goals in wartime. The LOAC has been remarkably successful in achieving compliance from warring nations in obeying these rules. This is most likely due to the reciprocal nature of the obligations involved. Nations treat prisoners of war well in order to guarantee that their own captive soldiers will be treated well by the enemy; nations will refrain from usingweapons of mass destruction because they are deterred by their enemy's possession of the same weapons. It has been one of the triumphs of international law to increase the restrictions on the use of unnecessarily destructive and cruel weapons, and to advance the norms of distinction and the humane treatment of combatants and civilians in wartime. IHRL norms, on the other hand, may suffer from much lower rates of compliance. This may be due, in part, to the non-reciprocal nature of the obligations. One nation's refusal to observe freedom of speech, for example, will not cause another country to respond by depriving its own citizens of their rights. If IHRL norms--which were developed without much, if any, consideration of the imperatives of combat--merge into the LOAC, it will be likely that compliance with international law will decline. If nations must balance their security [\*849] needs against ever more restrictive and out-of-place international rules supplied by IHRL, we hazard to guess that the latter will give way. Rather than attempt to superimpose rules for peacetime civilian affairs on the unique circumstances of the "war on terror," a better strategy for encouraging compliance with international law would be to adapt the legal system already specifically designed for armed conflict.

#### LOAC key to norm against CBW use

Malviya, 1

(Law Prof-Banaras Hindu University, “Laws Of Armed Conflict And Environmental Protection: An Analysis Of Their Inter-Relationship,” http://www.worldlii.org/int/journals/ISILYBIHRL/2001/5.html)

The following analysis of the international law of armed conflict extends to the limitations on the types of weapons **or methods of warfare that can be used** as well as the limitations on the objects of these weapons and methods. The early international customary and treaty law of war can be said to have an environmental protection character but it was never intended to be so by its creators. For example, treaties and customs limiting the use of poisons in war were established to avoid unnecessary sufferings to combatants and not out of concern for the residual effects of these poisons on the surrounding eco-systems. Nevertheless, due to humanity’s increased sensitivity to environmental matters, there is now an additional reason for adhering to such rules. (i) Chemical Warfare Chemical warfare means international employment of toxic gases, liquids or solids to produce casualities. The Hague Conventions of 1899 and 1907 on Laws and Customs of War on Land forbid the use of poison or poisoned weapons. The 1925 Geneva Gas Protocol also forbids chemical warfare. The environmental impact of chemical warfare is particularly serious in cases of use of herbicides-chemical defoliants such as those used in the Vietnam war by U.S.A. to destroy enormous stretches of tropical jungle.

CBWs cause extinction

Mhyrvold ’13 <Nathan, Began college at age 14, BS and Masters from UCLA, Masters and PhD, Princeton “Strategic Terrorism: A Call to Action,” Working Draft, The Lawfare Research Paper Series

Research paper NO . 2 – 2013>

As horrible as this would be, such a pandemic is by no means the worst attack one can imagine, for several reasons. First, most of the classic bioweapons are based on 1960s and 1970s technology because the 1972 treaty halted bioweapons development efforts in the United States and most other Western countries. Second, the Russians, although solidly committed to biological weapons long after the treaty deadline, were never on the cutting edge of biological research. Third and most important, the science and technology of molecular biology have made enormous advances, utterly transforming the field in the last few decades. High school biology students routinely perform molecular-biology manipulations that would have been impossible even for the best superpower-funded program back in the heyday of biological-weapons research. The biowarfare methods of the 1960s and 1970s are now as antiquated as the lumbering mainframe computers of that era. Tomorrow’s terrorists will have vastly more deadly bugs to choose from. Consider this sobering development: in 2001, Australian researchers working on mousepox, a nonlethal virus that infects mice (as chickenpox does in humans), accidentally discovered that a simple genetic modification transformed the virus.10, 11 Instead of producing mild symptoms, the new virus killed 60% of even those mice already immune to the naturally occurring strains of mousepox. The new virus, moreover, was unaffected by any existing vaccine or antiviral drug. A team of researchers at Saint Louis University led by Mark Buller picked up on that work and, by late 2003, found a way to improve on it: Buller’s variation on mousepox was 100% lethal, although his team of investigators also devised combination vaccine and antiviral therapies that were partially effective in protecting animals from the engineered strain.12, 13 Another saving grace is that the genetically altered virus is no longer contagious. Of course, it is quite possible that future tinkering with the virus will change that property, too. Strong reasons exist to believe that the genetic modifications Buller made to mousepox would work for other poxviruses and possibly for other classes of viruses as well. Might the same techniques allow chickenpox or another poxvirus that infects humans to be turned into a 100% lethal bioweapon, perhaps one that is resistant to any known antiviral therapy? I’ve asked this question of experts many times, and no one has yet replied that such a manipulation couldn’t be done. This case is just one example. Many more are pouring out of scientific journals and conferences every year. Just last year, the journal Nature published a controversial study done at the University of Wisconsin–Madison in which virologists enumerated the changes one would need to make to a highly lethal strain of bird flu to make it easily transmitted from one mammal to another.14 Biotechnology is advancing so rapidly that it is hard to keep track of all the new potential threats. Nor is it clear that anyone is even trying. In addition to lethality and drug resistance, many other parameters can be played with, given that the infectious power of an epidemic depends on many properties, including the length of the latency period during which a person is contagious but asymptomatic. Delaying the onset of serious symptoms allows each new case to spread to more people and thus makes the virus harder to stop. This dynamic is perhaps best illustrated by HIV , which is very difficult to transmit compared with smallpox and many other viruses. Intimate contact is needed, and even then, the infection rate is low. The balancing factor is that HIV can take years to progress to AIDS , which can then take many more years to kill the victim. What makes HIV so dangerous is that infected people have lots of opportunities to infect others. This property has allowed HIV to claim more than 30 million lives so far, and approximately 34 million people are now living with this virus and facing a highly uncertain future.15 A virus genetically engineered to infect its host quickly, to generate symptoms slowly—say, only after weeks or months—and to spread easily through the air or by casual contact would be vastly more devastating than HIV . It could silently penetrate the population to unleash its deadly effects suddenly. This type of epidemic would be almost impossible to combat because most of the infections would occur before the epidemic became obvious. A technologically sophisticated terrorist group could develop such a virus and kill a large part of humanity with it. Indeed, terrorists may not have to develop it themselves: some scientist may do so first and publish the details. Given the rate at which biologists are making discoveries about viruses and the immune system, at some point in the near future, someone may create artificial pathogens that could drive the human race to extinction. Indeed, a detailed species-elimination plan of this nature was openly proposed in a scientific journal. The ostensible purpose of that particular research was to suggest a way to extirpate the malaria mosquito, but similar techniques could be directed toward humans.16 When I’ve talked to molecular biologists about this method, they are quick to point out that it is slow and easily detectable and could be fought with biotech remedies. If you challenge them to come up with improvements to the suggested attack plan, however, they have plenty of ideas. Modern biotechnology will soon be capable, if it is not already, of bringing about the demise of the human race— or at least of killing a sufficient number of people to end high-tech civilization and set humanity back 1,000 years or more. That terrorist groups could achieve this level of technological sophistication may seem far-fetched, but keep in mind that it takes only a handful of individuals to accomplish these tasks. Never has lethal power of this potency been accessible to so few, so easily. Even more dramatically than nuclear proliferation, modern biological science has frighteningly undermined the correlation between the lethality of a weapon and its cost, a fundamentally stabilizing mechanism throughout history. Access to extremely lethal agents—lethal enough to exterminate Homo sapiens—will be available to anybody with a solid background in biology, terrorists included.

Effective LOAC regime key to prevent destabilizing nanoweapon use

Nasu and Faunce 10

Hitoshi Nasu, Lecturer, The Australian National University College of Law, Australia, Thomas Faunce, Associate Professor, The Australian National University College of Law and Medical School, Australia. Australian Research Council Future Fellow, Journal of Law, Information and Science, 2010, Vol. 20, "Nanotechnology and the International Law of Weaponry: Towards International Regulation of NanoWeapons", http://www.isodarco.it/courses/andalo13/doc/Nano-and-IL-2010-Article.pdf

2 Military Applications of Nanotechnology

The military use of nanotechnology is already a reality, as is illustrated by the funding poured into military research and development in nanotechnology in the US, UK, India, Sweden, and Russia.15 In 2001, for example, the US established the National Nanotechnology Institute (NNI) as an inter-agency cross-cut program that coordinates federal research and development activities in nanotechnology. The NNI allocated US$460–464 million in 2008–2009 and proposed US$379 million for 2010 as investment in nanotechnology research and development in the Department of Defense.16 The UK initiated its military nanotechnology program in a much smaller scale, investing £1.5 million in 2001.17 Sweden has reportedly invested 111 million over five years in nanotechnology research for military purposes.18 More recently, India has sanctioned expenditure of Rs12.48 crore under the Armament Research Board in the fields of high energy materials, armament sensors and electronics, ballistics, aerodynamics, detonics, technology for the detection of explosives, and small and nano-materials.19 India’s Defence Research and Development Organisation has proposed to establish five centres of excellence, including a centre for nanotechnology-based sensors for WMD detection, and a centre for nano optoelectronic devices, each having been budgeted Rs50 crore over five years.20 Although figures are not made public, Russia has also reportedly been investing in nanotechnology that will enable new offensive and defensive weapons system.21 Government departments are not the only actors in this area. The US government, for example, has used public funds to establish the Institute for Soldier Nanotechnologies (ISN) as a centre for research collaboration between the United States Army and the Massachusetts Institute of Technology (MIT), combining basic and applied research into military applications of nanoscience and nanotechnology in three broad areas: ‘protection; injury intervention and cure; and human performance improvement.’22 Private companies such as QinetiQ,23 BAE Systems,24 Industrial Nanotech Inc,25 and Raytheon,26 have also been heavily involved in the research and development of military nanotechnology, often in partnership with the government, especially in the areas of nano-sensors and body armour. An advanced armour-piercing projectile involving the potential use of NanoSteelTM was recently patented in the US.27 Currently, no effective method exists for monitoring ENP exposure, and the health risks involved are potentially unique and only partially documented. Crucial chronic in vivo animal exposure studies (in particular of reproductive toxicity) have not been published to date. Research suggests that the health risks of nanostructures cannot be predicted a priori from their bulk equivalents. Yet, some ENPs have also been shown in isolated cell experiments to preferentially accumulate in mitochondria and inhibit function. Others may become unstable in biological settings and release elemental metals. Furthermore, short-term animal exposure to some (but not all) ENPs has produced dose-dependent inflammatory responses and pulmonary fibrosis.28 Ensuring the safety of nanotechnology presents global policy challenges for public health, not only because gathering, analysing, categorising, and characterising safety data for individual nanotherapeutic products may be unusually difficult, but also because it is unclear whether there are general safety risks or whether risks are confined to uniquely engineered nanomaterials with novel surface binding properties.29 The relevance of nanotechnology to the military resides particularly in its enabling applications in electronics, optoelectronics, and information and communication systems for detecting, preventing and deterring bioterrorism, the latter being a national research priority in developed nations.30 Nanotechnology thus has a recognised defensive military capability. Standard bioterrorist threats, for example, could involve aerosol attacks on individuals or crowds, ‘dirty’ bombs and targeted contamination of food sources, each utilising chemical or biological agents of a size, amount or distribution that nanotechnology sensors and computing will greatly assist in uncovering.31 Bioterrorist threats such as botulinum in milk,32 or release of pathogenic organisms and biotoxins in the water supply may not themselves involve nanoscale agents, but their detection may require correlation of vast amounts of information beyond the capacity of non-nanotechnology sensing, information and communication systems.33 Likewise, threat responses to unexpectedly virulent modifications such as mousepox IL-4,34 or a highly virulent strain of influenza virus (akin to the strain which caused the Spanish influenza pandemic in the winter of 1918–1919 and killed up to 50 million people worldwide),35 are likely to benefit greatly from defensive nanotechnology surveillance systems. Atlantic Storm, for example, was a simulated bioterrorism exercise based on the deliberate release of smallpox viruses in various European and North American cities. It revealed that many nations had inadequate vaccine stockpiles, response plans, and public health laws to effectively respond. Such exercises have illuminated the need to develop innovative defensive technologies (including nanotechnology) capable of allowing health officials to promptly detect minute amounts of viral loads in widely dispersed locations and effectively communicate the relevant details to public health authorities.36 States negotiating under the Biological Weapons Convention (BWC) recently emphasised the need for broad-based codes of conduct for both scientists and public health physicians to counter future bioterrorist threats, partly by warning of the professional perils involved in deliberate or inadvertent release of information and substances.37 Military applications of nanotechnology will not be confined to defensive capabilities, however. Nanotechnology allows the building of conventional missiles with reduced mass and enhanced speed, small metal-less weapons made of nanofibre composites, small missiles as well as artillery shells with enhanced accuracy guided by inertial navigation systems, and armour-piercing projectiles with increased penetration capability. Although it is still highly speculative, further research could lead to the development of micro-combat robots, micro-fusion nuclear weapons, new chemical agents carried by nanoparticles, and new biological agents with self-replication capability.38 Some of the potential offensive military applications of nanotechnology could span several traditional technological compartments and blur the distinction between conventional weapons and weapons of mass destruction. The ability of nanotechnology to design and manipulate molecules with specific properties could lead to biochemicals capable of altering metabolic pathways and causing defined hostile results ranging from temporary incapacitation to death.39 Nanotechnology could also make it possible to contain and carry a minute amount of pure-fusion fuel safely until released, detonating a micro-nuclear bomb at a microspot.40 As will be shown below, it is likely that those new weapons would be subjected to prohibition and inspection under existing treaties, as long as currently available chemicals and biological agents are used in nano-size.41 However, the dual-use potential of nanotechnology and the low visibility of nanoparticles in weapons make it hard to detect their development and use as weapons. Concern has been raised about the potentially unique harmful effects of nanoweapons. At an individual level, explosives such as those using nano-energetic particles, nano-aluminum or non-metal nano-fibre composites, and nanomedicines that improve soldiers’ ability to overcome sleep deprivation,42 could cause unnecessary suffering to both combatants and non-combatants. At a larger, strategic level, the development and deployment of smaller, longer range missiles with greater precision, or new bio-chemical agents could dramatically change the balance of military power and the way in which a war is fought. Because of these concerns, there have been calls for moratoriums or bans on nanotechnology.43 Others have proposed the creation of a preventative arms control regime based on prospective scientific, technical, and military operational analysis of nanotechnology.44 However, no international agreement alone would be effective or even feasible in halting or controlling the development of nanotechnology without proper regulatory mechanisms that will address the right balance between military necessity, humanitarian considerations and peaceful applications of nanotechnology. The next section will examine the current state of international law to ascertain the extent to which nano-weapons might already be, or can be, prohibited or regulated, before turning to the issue of potential new regulatory mechanisms. 3 International Law Governing Nano-Weaponry 3.1 Arms Control Law and Nano-Weaponry Currently there is no international treaty that has specific provisions regulating nano-weapons. Therefore, in order to determine the extent to which nanoweapons are covered by existing international law it will be necessary to examine whether general principles governing weaponry apply, or whether extant arms control treaties impose restrictions by reasonable extension. States have agreed in a variety of international treaties to specific and express rules on arms control, which apply even in peacetime. Yet, the adoption of treaties to prohibit certain weapons tends to be reactive (rather than preemptive) and limited in scope, and has been largely dictated by considerations of military effectiveness.45 Thus, states have agreed to ban the use of projectiles of a weight below 400 grams that are explosive or charged with fulminating or inflammable substances,46 expanding bullets,47 asphyxiating, poisonous or other gases,48 biological weapons,49 chemical weapons,50 blinding laser weapons,51 anti-personnel mines,52 and most recently, cluster munitions.53 Nanotechnology, if used as an enabling technology for weapons development in these areas, would be regulated at least in part by the relevant convention. For example, prototype nanotechnology lasers producing megawatts of continuous power are far more powerful than those previously known,54 and are likely to be subject to the 1995 Protocol on Blinding Laser Weapons in the visible region.55 Nanotechnology can also produce toxic chemicals with novel properties,56 and may facilitate the development of synthetic organisms with a high degree of lethality.57 Yet the arms control treaties in these areas were drafted without any consideration of nanotechnological developments. The recent development and deployment of DIME, for example, illustrates the difficulty in defining whether new weapons fall within the nanotechnology category, or within existing rules of international arms control law. DIME was developed at the US Air Force Research Laboratory in order to achieve low collateral damage by producing a highly powerful blast within a relatively small area. Its development originates from depleted uranium research and is the latest innovation in the US military’s long-running development of Focused Lethality Munitions (FLM),58 designed to provide the ‘weapons of choice’ in targeting terrorists hiding among civilians.59 Upon detonation, the carbon fibre warhead case disintegrates into minute, non-lethal fibres with little or no metallic fragments, then sprays a superheated micro-shrapnel of powdered (potentially nano-scale) tungsten particles with sufficient penetration mass for disabling the target within a small lethal footprint. Due to the undetectable nature of tungsten micro-particles in human tissue, the question arises whether this weapon falls within the scope of the 1980 Protocol (I) on Non-Detectable Fragments to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons (‘1980 Protocol (I)’).60 It appears that the design intent of this weapon meets the threshold for the prohibition, as the primary effect of metal dust sprayed with DIME is to kill, injure, or damage by blast without leaving much trace of fragments.61 When the 1980 Protocol (I) was adopted unanimously, states did not have such weapons in their inventory, nor did they foresee any conceivable use of them in the future.62 It could well be argued, according to a textual interpretation, that DIME is not prohibited under the 1980 Protocol (I), as micro-shrapnel could still be detectable by X-ray, no matter how difficult it might be in practice. Yet, both a contextual and purposive interpretation of the Protocol support the case that DIME is prohibited given the potential seriousness of injuries caused by DIME attacks and the difficulty of treatment due to the size of the fragments.63 DIME bombs were reportedly employed by Israel during the 2006 conflicts in Gaza and Southern Lebanon, and more recently during the Gaza conflict in January 2009.64 As Israel is a party to the 1980 Protocol (I),65 it is arguable that it breached those treaty obligations by employing DIME bombs. Few authoritative allegations, however, have been made against the use of DIME by Israeli forces on such grounds.66 If DIME is to be considered at least in some respects a nano-weapon chiefly due to the potential nano-scale of powders produced upon impact, this would complicate the assessment of its legality under the existing treaty obligations. Arms control regimes also face an inherent problem with application to noncontracting parties. Whilst resorting to an examination of customary law status of a particular prohibition remains an option for long-existing weapons, this is generally not the case for new weapons because of the inevitable absence of state practice. In fact, the customary law status of the prohibition on nondetectable fragments has been subject to considerable disagreement among commentators for this reason.67 3.2 International Humanitarian Law Principles and Nano-Weaponry The international arms control treaties noted above usually concentrate on regulating or prohibiting the specified weapon’s construction aims and characteristics. General principles of international humanitarian law, on the other hand, tend to regulate the conduct of warfare by reference to the harmful effects produced by the use of means or methods of warfare.68 The general principle, for example, that ‘the right of belligerents to adopt means of warfare is not unlimited’ may have had its roots in compassion and rejection of unnecessary suffering textually manifesting in Ancient Greece and India.69 No matter how nascent this was as a legal principle before the emergence of modern international law of armed conflict, it has received widespread support amongst the leaders of nations over many years. There is now little doubt about whether this broad statement about the regulation of weaponry is a reflection of ‘elementary considerations of humanity’.70 More specifically, there are two basic principles of international humanitarian law highly relevant to nano-weaponry: one prohibiting the employment of arms, projectiles, or material ‘of a nature to cause superfluous injury’ (or ‘calculated to cause unnecessary suffering’);71 and the other prohibiting the use of weapons that indiscriminately affect both combatants and non-combatants.72 The principle of prohibiting superfluous injury or unnecessary suffering is central to the consideration of legality under the international law of conventional weapons, as opposed to weapons of mass destruction.73 It was first enunciated in the preamble to the 1868 St Petersburg Declaration,74 but was a rhetorical expression of the drafters’ inspiration, rather than their intention to impose legal obligations.75 It was formally adopted as a binding rule in the subsequent treaties,76 and since then has attained the status of customary international law.77 This is so irrespective of the distinction between civilian and military targets.78 The prohibition is now incorporated into the 1998 Rome Statute of the International Criminal Court as one of the criminal offences.79 This principle appears to be principally relevant to the international regulation of nano-weapons insofar as those weapons could pose novel, unnecessarily severe and long-term health and environmental impacts. The specific rules of arms control law, as they potentially apply to nanoweapons, are thus a subset of the general principles of international humanitarian law on weaponry.80 Assuming that it may not be clear whether a nano-weapon is prohibited, general humanitarian law principles then may serve as a general legal or moral basis for questioning its legality and starting negotiations which may result in its prohibition.81 Such a debate will have to take account of the ‘Martens Clause’,82 although ‘principles of humanity’ and ‘dictates of public conscience’ alone provide no firm legal basis to prohibit the use of particular weapons.83

Extinction

Altmann 10

Jurgen Altmann, professor of experimental physics at the University of Dortmund, Germany, International Handbook on Regulation Nanotechnologies, Ch. 17, Military Applications: Special Conditions for Regulation, 2010, pg. 380-382

There are also military uses of nanotechnology which are mostly specific and which would not be developed for a civilian market. Some of these, however, once developed in a military context and made cheap by mass production, may find their way into civilian society and have negative impacts there, for example, by being used by non-state actors for illegal activity. Variable camouflage would not pose a big problem if it were used in the civilian context. However, many uses of nanotechnology for specific military application may pose serious security risks if they became available to civilians. For example, small, cheap sensors to be scattered over the battlefield could also be used for private or economic espionage, or smaller conventional weapons with highly precise guidance systems, in particular very small missiles, could be used for terrorist attacks. The same applies for firearms and munitions using nanofibre composites, which, without any metal, would be difficult to detect at security checkpoints. Soldier systems for monitoring body status from the outside, forming compresses and administering therapeutic agents if needed. are not problematic. However, implants or other body manipulation, such as a brain-machine interface or modification of the human biochemistry, may create problems for civilian society. Here the military could act as a door-opener, preempting a broad societal debate about the acceptability of non-therapeutic body modification. Uninhabited vehicles (for air, water or land) will profit from nanotechnology in materials, energy storage, sensors and computers. Some could be reduced to a few centimetres in size or below, maybe moving like insects. Alternatively, the military could take real insects as a basis for hybrid systems. Transferred to civilian society, small systems could be used for eavesdropping or terrorist attacks. The use by terrorist groups of new biochemical weapons made feasible by nanotechnological advances in biomedicine should also be feared. The use of nanotechnology here may include nanocapsules to ferry agents through the blood-brain barrier, agents which bind to specific cell types, and agents that release a toxin only if a certain DNA or protein pattern is present, thus acting selectively only on very specific target subjects. New biochemical agents would endanger the existing conventions, but of course here the needed prohibitions are already in place. Dangers for existing arms-control treaties can ensue also with uninhabited vehicles some types could undermine the CFE Treaty (Altmann 2009) - while small satellites for anti-satellite attack would counteract the space-weapons ban, which the overwhelming majority of countries have demanded for decades. Arms racing and proliferation can follow from nearly all specific military applications mentioned. Exaggerated expectations, such as those evoked by the Presidents of India and Israel. will tend to aggravate the problem: the same applies for secrecy together with misrepresentations of military aims for nanotechnology, as in a US publication about alleged Chinese plans for 'ant robots’ (Altmann and Gubrud. 2004). Problems for the stability between potential military opponents are to be feared most with uninhabited weapons systems, in particular if they will be capable of autonomous firing decision, when such systems would travel at short mutual distance (along a border, in international territory), survival may require faster reaction than possible with remote control by a human. In a crisis, when both systems would eagerly observe the other for indications of attack, a mistaken sun reflex or another error could lead to a shooting and thus unleash war by uncontrolled feedback cycles. Destabilization can work up to the level of nuclear war: if mass attack against strategic weapons and command systems using swarms of small uninhabited aircraft or missiles becomes plausible. Nervousness and pressure for early launch of one's own nuclear weapons would drastically increase. Small satellites capable of fast attacks against important satellites of an opponent would endanger stability. A particularly frightening scenario has very small mobile enemy robots covertly intruding into one’s own military systems in peacetime where they would sit, possibly for years, ready to suddenly disrupt the electronics at any time.

#### LOAC is empirically adaptive and capable of managing new tech

Stewart 11

Darren M. Stewart, Colonel, British Army; Director, Military Department, International Institute of Humanitarian Law, International Law Studies, 2011, Vol. 87, "New Technology and the Law of Armed Conflict"

Just as military doctrine has demonstrated its flexibility in coping with the relentless development and introduction of new technology, LOAC has provided— and will continue to provide—a framework for the regulation of armed conflict. Calls to create new standards or to interpret the law in ways that seek to regulate the unknown, or at least the not yet known, do not stand up against an assessment of what LOAC provides in terms of a system of law that regulates not just the introduction of new technology, but also its application.

Useful processes, such as those forming part of the AP I Article 36 weapons review, seem purpose designed not only to act as initial control valves to ensure that military methods and means can advance in a coherent and effective manner but also to act as red flags to possible LOAC issues associated with the employment of new technology. It is unfortunate that too few States engage actively in the weapons review process, an area where greater effort to comply with the law should occur.

Generally the existing LOAC rules would seem sufficiently flexible to adapt to the deployment of new technology on the battlefield. In many respects new technology has greatly aided the application of LOAC and contributed to an increase in the protection of civilians. In this sense, the story is a good news one. The extant LOAC paradigm has responded in a flexible manner, benefiting from the positive synergies afforded by technological advances. The virtue of such a system, however, comes with compliance rather than the creation of new standards or responsibilities, such as CDRs, or use of the capabilities afforded by new technology to argue that a human rights paradigm is more appropriate. Armed conflict continues to be an unpredictable, often base affair, where significant ambiguity prevails, notwithstanding the employment of considerable technological capability. The benefits afforded by new technology in such circumstances are significant if they can ameliorate even some of the suffering caused by armed conflict, but they are by no means a panacea.

New technology creates its own challenges in the context of accountability, particularly with respect to autonomous systems. The perverse effect for States and the senior civilian and military command echelon who promote the development and implementation of new technology as a means of “casualty free” warfare is that they may well find themselves with nobody to stand between the actions of such autonomous systems and themselves when things go wrong. It is hoped that the associated discomfiture from this realization may well act in a positive capacity to focus minds as to the need for such new technology, and manner in which it is employed.

Consider the mutually assured destruction scenario, which hung over the world during the Cold War and led to the notion that nuclear weapons should be treated as a “special case.” This was largely due to the nature of such weapons, dehumanizing war and giving rise to massive destruction on a wide-scale basis. Autonomous weapons systems as an example of the changing character of weapons may not involve such destruction; indeed one of the consequences of their use is that it avoids such a scenario. However, an increasing reliance upon technology clearly has the potential to dehumanize armed conflict, creating a perception of low or no risk and, in doing so, possibly convincing States of the viability of the recourse to the use of force to resolve disputes.

In the face of this, LOAC continues to offer a balanced, civilizing effect as part of a system of law providing a broad regulatory framework intended to afford protection to the most vulnerable. In this context, flexibility (of course coupled with compliance) is its greatest strength. Whether the current developments in technology will constitute a “watershed” or defining moment in the evolution of warfare remains to be seen. What is clear is that LOAC is capable of keeping pace and continuing to meet its mission of protection and humanity.

#### Courts are key to apply IHL to domestic policy

**Blank 11** - Director, International Humanitarian Law Clinic, Emory University School of Law <Laurie. “Understanding When and How Domestic Courts Apply IHL” (2011). Case Western Reserve Journal of International Law, Vol. 44, 2011; Emory Legal Studies Research Paper No. 12-200>

When Courts Do—or Should—Apply IHL¶ One primary factor that often arises in situations that involve IHL is¶ whether IHL is the only applicable law or whether human rights law, domestic¶ criminal law, constitutional law or other legal regimes also have an¶ important contribution to the adjudication of the case. Understanding when¶ courts choose to apply IHL alone or in concert with other legal paradigms¶ has a direct effect on both litigation strategy and jurisprudential predictability¶ and continuity. These considerations also contribute to effective advocacy¶ to press for more frequent and more robust judicial application of IHL.¶ A first factor is the suitability of IHL for the analysis at issue in the¶ case. Looking back to the categories set forth briefly in the previous section,¶ the question of the existence of an armed conflict is highly suitable for the¶ application of IHL, which sets forth a framework for determining when an¶ armed conflict exists to trigger the law of war. Even in situations in which¶ the question arising in the case does not then involve the application of IHL,¶ such as appropriations of funds or the tolling of a statute of limitations during¶ wartime, IHL gives a clear picture of when events on the ground constitute an armed conflict.42 Although it is not the only relevant body of law for¶ such determinations—domestic law does indeed have an important contribution¶ to make in the constitutional sphere regarding the existence of armed¶ conflict—IHL is the lex specialis and the most directly on point.43 In other¶ areas, such as treatment, fair trial rights and, potentially, detention in noninternational¶ armed conflict or counterterrorism operations, human rights¶ law and other domestic or international legal frameworks have important¶ contributions that inform how IHL applies to a particular situation. Here, we¶ might thus see courts showing greater reluctance or uncertainty about incorporating¶ IHL into their analysis and decisions. Second, some of the categories and issues highlighted in the first¶ section above may pose greater challenges for a domestic court’s application¶ of IHL. These challenges can arise when IHL is not as well developed¶ in a particular area—such as the parameters of detention in noninternational¶ armed conflict, for which the authority derives from the principle¶ of military necessity, but treaty law offers little in the way of comprehensive¶ details. Alternatively, some courts may view the application of IHL¶ to complex questions that arise in the intersection between counterterrorism¶ and armed conflict as more challenging than the application of domestic¶ criminal law or human rights law in such situations, even if IHL is equally¶ or more appropriate.¶ A third consideration is the range of legal regimes that apply to a¶ given case before a domestic court and how they relate to each other. This¶ factor is closely related to the suitability factor above, but has a broader¶ perspective. In addition to other legal frameworks, this analysis should also¶ take into account whether there are judicial or other legal doctrines that impact¶ how a court views a case, such as state secrets or the political question¶ doctrine. While some alternative sources of law can be helpful in the adjudication¶ or resolution of a particular issue, some can also be potentially¶ problematic for the protection of individual rights and the fulfillment of¶ fundamental principles. A first level of analysis therefore would consider¶ how many other legal regimes are relevant and how they all interrelate,¶ which can offer some clues into not only how a court would and should¶ view the contribution IHL can make to the case’s resolution, but also how¶ many other legal principles are central to the issues at hand. At a second¶ level, we can look to the centrality of the IHL principles at the heart of the¶ case in viewing how a court should approach political question determinations.¶ In the U.S. at least, courts tend to defer to the executive on wartime¶ matters;44 however, it is precisely when wartime cases strike at the very core¶ principles of IHL that a court should rethink that automatic deference and¶ focus on the rights and obligations demanding protection and fulfillment. At¶ the opposite end of the spectrum, the Israeli Supreme Court is the epitome¶ of robust judicial engagement during wartime, hearing cases in real-time on¶ issues ranging from the conduct of military operations to the protection of¶ civilians to detention of suspected terrorists.45¶ Once a court does incorporate IHL into its analysis, either as the¶ dominant legal paradigm or as one of multiple sources that bear on the case¶ at hand, a range of additional factors are relevant for understanding how¶ courts will approach this task. As noted above, IHL is fundamentally international¶ law but also forms part of the domestic law of most states. How a¶ court chooses to address IHL’s key provisions, principles and obligations¶ will vary widely depending not only on the categories of issues detailed in¶ the first section above, but also on how the court relates to other courts in¶ the international system, how it views international law in general, and other¶ considerations.¶ The first, and most foundational, factor is how international law is¶ incorporated into or viewed in relation to a state’s domestic law. For example,¶ states with a monist system treat international treaties as automatically¶ incorporated into national law;47 in states with a dualist tradition, international¶ law must be translated into national law through legislation.48 In the¶ U.S., another consideration is whether a particular treaty—and concomitant¶ international obligation—is self-executing, meaning it has direct effect as¶ law in domestic courts.49 In the case of the Geneva Conventions, the primary¶ modern law of war treaties, states take different approaches to how these¶ treaty obligations are incorporated into national law. Some states have legislation¶ implementing the Geneva Conventions and the obligations therein;50¶ some have national traditions—such as monism—that automatically give¶ the Conventions the full force of domestic law.51 In others, such as in the¶ U.S., the approach to the Geneva Conventions has proven more complex,¶ with courts debating the applicability of the Conventions and Congress¶ passing legislation declaring that the Geneva Conventions cannot be used as¶ a source of rights in U.S. domestic courts.52¶ IHL is more than the Geneva Conventions and other treaties, however.¶ Customary law plays a substantial role in the law of war and the obligations¶ of states to conduct hostilities in a lawful manner and protect civilians¶ from the ravages of war.53 Understanding how particular courts view¶ customary law is therefore an important part of anticipating how the law of¶ war will be incorporated into national court decisions and jurisprudence.¶ Beyond the willingness—or unwillingness—of courts to contemplate customary¶ international law, the manner in which such courts explore and determine¶ the content of customary law is central to this analysis as well. Is¶ the court conservative in its understanding of the content and development¶ of customary international law or does it take an expansive view, one that¶ might encapsulate modern trends in conflict and still burgeoning developments¶ in the law? These questions arise in a range of international legal¶ issues, such as Alien Tort Statute litigation in the U.S., but are particularly¶ important in the IHL arena, where the pace of developments on the ground¶ is extremely quick and customary law often develops “in the reverse”, based¶ on reactions to violations rather than on statements of opinio juris. Finally, examining how courts treat comparative, regional and international¶ jurisprudence can help determine both how welcoming courts¶ are to the application of IHL in general and, more specifically, how courts¶ are likely to view and interpret the content of IHL. A greater comfort level¶ with non-national jurisprudence will likely correspond with a less rigid fo-cus on the singularity of domestic law and greater ease in incorporating¶ international law in general. In the area of IHL, this translates into a broader¶ interpretation of IHL beyond the domestic lens, raising the potential of a¶ richer treatment of the issues in the case and how the law can be applied.¶ The relationship between regional or international courts and national courts¶ is an important piece of this analysis as well. Within the European system,¶ governments and national courts are bound by decisions of the European¶ Court of Human Rights (ECHR). Any analysis of how domestic courts¶ within Europe are incorporating or will incorporate IHL must therefore take¶ into account how IHL issues arise and are or may be addressed in the¶ ECHR.55 The role of the ad hoc international criminal tribunals and special¶ courts is far less defined with regard to the force of their jurisprudence as¶ precedent in national courts, but understanding how various domestic courts¶ treat this international jurisprudence is helpful in analyzing whether and¶ how they will incorporate the content of the legal analysis and determinations¶ in those cases.

Only the courts establish legally binding precedent – solves LOAC confusion

Deeks 13, Ashley, associate professor at University of Virginia Law School, senior contributor to lawfareblog, “Domestic Humanitarian Law: Developing the Law of War in Domestic Courts,” October, http://ssrn.com/abstract=2338033

The United States is in its twelfth year of its struggle against al Qaeda. This situation, which the 1 United States has treated as an extra-territorial armed conflict with a non-state actor, has implicated a wide array of thorny questions related to international humanitarian law (‘IHL’). For structural and political reasons, however, the international community has not attempted to craft a new treaty to regulate this type of armed conflict, which does not fit the standard armed conflict paradigms. Nor has there been state practice of sufficient generality and uniformity to establish new customary IHL. A dozen years in, we have no new international rules to guide states’ conduct in this and similar contexts. But that is not to say that we have no new rules at all to regulate these types of armed conflict: the new rules simply stem from non-international sources. The domestic legislatures and, importantly for the purposes of this chapter, domestic courts of certain states have played a significant role in setting forth new rules to govern how those states must conduct themselves 2 during these armed conflicts. We might attribute this newly expanded role for courts in the armed conflict context to several factors, including a shift from collectivism to individualism in 3 armed conflict and, relatedly, a growing ability of individuals to bring before courts allegations of unlawful state conduct during wartime. Regardless of the cause, these domestic courts and on 4 a transnational level, courts like the European Court of Human Rights, have stepped in to interpret, extend, and craft laws applicable in armed conflict, producing what this chapter terms ‘domestic humanitarian law’ (‘DHL’). On occasion DHL simply reflects treaty interpretation by domestic courts, but often DHL represents court decisions that effectively create new rules, the 5 sources of which cannot be traced back to treaties alone. These court decisions help answer previously unanswered questions in IHL about who may be detained; the type of detention review to which individuals are entitled; what groups count as co-belligerents; whether there are non-refoulement-type limits on certain detainee transfers; and what the nature of these conflicts is. DHL is important for two reasons. First, by definition it establishes detailed, legally binding rules by which particular states’ militaries must conduct themselves in extra-territorial conflicts. Second, DHL has a significant effect on future IHL developments – affecting the likelihood of a future international agreement on those rules; the substance of those future rules in the event such an agreement emerges; the way in which states interpret certain existing treaty provisions; and the content of state practice that contributes to the formation of new rules of customary international law. One goal of this chapter is to examine the nature and character of DHL, in order better to understand its relationship to and effect on IHL. A second goal is to assess whether the increasing role of domestic courts in producing rules governing armed conflict is a salutary development.

## 1AC Plan

The United States Federal Judiciary should increase restrictions on the war powers authority of the president of the United States by statutorily clarify that efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them fall under the introduction of hostilities under the Law of Armed Conflict.