### War Now

#### US-China War is inevitable – Attacking now is better than later

Aaron L. **Friedberg, 2009** a professor of politics and international affairs at the Woodrow Wilson School at Princeton University. His book, A Game for Half the World: America, China and the Struggle for Mastery in Asia, will be published next year by W. W. Norton & Company. September 2009 - October 2009, (The National Interest, HEADLINE: Here Be Dragons, Robert S. Ross and Aaron L. Friedberg Debate: Is China a Military Threat?, p. Lexis)

THIS COMBINATION of rapidly advancing offensive and defensive capabilities is beginning to raise doubts in the region about America’s ability to defend its allies and project its power. What is worse, over the next several years there will be an increasing danger that, in an extreme crisis, China’s leaders might believe that they have a chance of starting a war by effectively knocking the United States out of the western Pacific and blunting its initial, retaliatory response, all without striking the American homeland and without the need to fire a single nuclear weapon. If it were successful, such an attack would leave a president with some agonizing choices. Much as during the cold war, if faced with the possibility of a quick conventional defeat in Western Europe, American decision makers would have to contemplate the use of nuclear weapons. But, as was true then, the plausibility of escalatory threats will diminish as the probability of retaliation rises. Beijing **is fast approaching the point** where it will have a secure second-strike force capable of dealing a devastating blow no **matter how hard the United States might try to prevent it**. As risky as an American attack on Chinese nuclear forces, ports, airfields and communications centers would be today, it will be considerably more so a few years from now. Beijing is in the process of deploying intercontinental-range ballistic missiles (ICBMs) that will be far less vulnerable than their predecessors. In addition to its small force of fixed, single-warhead ICBMs, over the next few years China will place in service several dozen hard-to-locate road-mobile and submarine-launched missiles, each capable of striking the United States with multiple warheads.

### We Win

#### No Offense – Risk of war means we would preemptively attack with few causalities

**Lieber and Press, 2007**, Keir A. Lieber is an assistant professor of political science at the University of Notre Dame and the author of War and the Engineers: The Primacy of Politics Over Technology (2005). Daryl G. Press has worked as a consultant on military analysis projects for the U.S. Department of Defense for 13 years, and he is an associate professor of government at Dartmouth College, July 1, 2007, (The Atlantic Monthly, HEADLINE: Superiority complex: why America's growing nuclear supremacy may make war with China more likely, p. Lexis)

From a military perspective, this modernization has paid off: A U.S. nuclear first strike could **quickly destroy** China's strategic nuclear arsenal. Whether launched in peacetime or during a crisis, a preemptive strike would likely leave China with **no means of nuclear retaliation** against American territory. And given the trends in both arsenals, China may live under the shadow of U.S. nuclear primacy for years to come. This assessment is based on unclassified information, standard targeting principles, and formulas that defense analysts have used for decades. (And we systematically chose conservative estimates for key unknowns, meaning that our analysis understates U.S. counterforce capabilities.) The simplest version of an American preemptive strike would have nuclear-armed submarines in the Pacific launch Trident II missiles at the Chinese ICBM field in Henan province. The Navy keeps at least two of these submarines on "nard alert" in the Pacific at all times, meaning they're ready to fire within 15 minutes of a launch order. Since each submarine carries 24 nuclear-tipped missiles with an average of six warheads per missile, commanders have almost 300 warheads ready for immediate use. This is **more than enough** to assign multiple warheads to each of the 18 Chinese silos. Chinese leaders would have **little or no warning** of the attack. During the Cold War, U.S. submarines posed little danger to China's silos, or to any other hardened targets. Each warhead on the Trident I missiles had little chance--roughly 12 percent--of success. Not only were those missiles inaccurate, their warheads had a relatively small yield. (Similarly, until the late 1980s, U.S. ICBMs lacked the accuracy to carry out a reliable disarming attack against China.) But the Navy's new warheads and missiles are far more lethal. A Trident II missile is so accurate, and the newer W88 warhead so powerful, thatif the warhead and missile function normally, the destruction of thesilo is virtually assured (the likelihood is calculated as greater than 99 percent). In reality, American planners could not assume such near-perfect results. Some missiles or warheads could malfunction: One missile's rockets might fail to ignite; another's guidance system might be defective. So a realistic counterforce plan might assign four warheads to each silo. The U.S. would "cross-target" the missiles, meaning that the warheads on each missile would each go to different silos, so that a silo would be spared only if many missiles malfunctioned. **Even assuming that 20 percent of missiles malfunctioned**--the standard, conservative assumption typically used by nuclear analysts--there is **a 97 percent chance** that **every Chinese** DF-5 **silo would be destroyed** in a 4-on-1 attack. (By comparison, a similar attack using Cold War-era Trident I missiles would have produced less than a 1 percent chance of success. The leap in American counterforce capabilities since the end ofthe Cold War is staggering.) Beyond bolstering the ability to conduct a first strike, the improvements to U.S. counterforce weapons also allow war planners to design nuclear options that will make the weapons more "usable" during high-stakes crises. Nuclear planners face many choices when they consider striking a given target. First, they must choose a warhead yield. The American arsenal includes low-yield weapons such as the B-61 bomb,which can detonate with as little explosive force as 0.3 kilotons (one-fiftieth the power of the bomb that destroyed Hiroshima), and high-yield weapons such as the B-83 bomb, which can yield 1,200 kilotons (80 times the strength of the Hiroshima bomb). For a military planner, high-yield weapons are attractive because they're very likely to destroy the target--even if the weapon misses by some distance. Low-yield warheads, on the other hand, can be more discriminating, if planners want to **minimize civilian casualties**. A second key decision for war planners is whether to set the weapon to detonate at ground level or in the air above the target. A groundburst creates enormous overpressure and ground shock, ideal for destroying a hardened target. But groundbursts also create a lot of radioactive fallout. Dirt and other matter is sucked up into the mushroom cloud, mixes with radioactive material, and, after being carried by the wind, falls to earth in the hours after the blast, spreading lethal radiation. Airbursts create smaller zones of extremely high overpressure, butthey also generate very little fallout. If the detonation occurs above a threshold altitude (which depends on the weapon yield), virtually no heavy particles from the ground mix with the radioactive material in the fireball. The radioactive material rises into the high atmosphere and then falls to earth over the course of several weeks in a far less dangerous state and over a very wide area, greatly reducing the harm to civilians. In the past, a nuclear attack on China's arsenal would have had horrific humanitarian consequences. The weapons were less accurate, so an effective strike would have required multiple high-yield warheads,detonating on the ground, against each target. The Federation of American Scientists and the Natural Resources Defense Council modeled the consequences of such an attack--similar to the submarine attack described above--and published their findings in 2006. The results were sobering. Although Chinas long-range missiles are deployed in a lightly populated region, lethal fallout from an attack would travel hundreds of miles and kill more than 3 million Chinese civilians. Americanleaders might have contemplated such a strike, but only in the most dire circumstances. But things are changing radically. Improved accuracy now allows war planners to target hardened sites with low-yield warheads and even airbursts. And the United States is pushing its breakthroughs in accuracy even further. For example, for many years America has used global-positioning systems in conjunction with onboard inertial-guidance systems to improve the accuracy of its conventionally armed (that is, nonnuclear) cruise missiles. Although an adversary may jam the GPS signal near likely targets, the cruise missiles use GPS along their flight route and then--if they lose the signal--use their backup inertial-guidance system for the final few kilometers. This approach has dramatically improved a cruise missile's accuracy and could be applied to nuclear-armed cruise missiles as well. The United States is deploying jam-resistant GPS receivers on other weapons, experimenting with GPS on its nuclear-armed ballistic missiles, and planning to deploy a new generation of GPS satellites--with higher-powered signals to complicate jamming. The payoff for equipping cruise missiles (or nuclear bombs) with GPS is clear when one estimates the civilian casualties from a lower-yield, airburst attack. We asked Matthew McKinzie, a scientific consultant to the Natural Resources Defense Council and coauthor of the 2006 study, to rerun the analysis using low-yield detonations compatible with nuclear weapons currently in the U.S. arsenal. Using three warheads per target to increase the odds of destroying every silo, the model predicts **fewer than 1,000 Chinese casualties from fallout**. In some low-yield scenarios, **fewer than 100 Chinese would be killed or injured from fallout**. The model is better suited to predicting fallout casualties than to forecasting deaths from the blast and fire, but given the low population in the rural region where the silos are, Chinese fatalities **would be fewer than 6,000 in even the most destructive scenario we modeled**. And in the future, there may be reliable nonnuclear options for destroying Chinese silos. Freed from the burden of killing millions, a U.S. president staring at **the threat** of a Chinese nuclear attack on U.S. forces, allies, or territory might be more inclined to **choose preemptive action**.

#### War with China would completely reverse modernization and nationalism – solves the impact

**Harries, 2002** (Owen, think tank, author, and editor of National Interest, China in the National Interest, Transaction Publishers, ISBN 0-7658-0561-8, p. 247-8)

Military defeat by the United States would not only weaken China vis-à-vis the United States but would also dramatically reverse China’s position in the regional balance of power. China would lose its current advantages with regard to Russia, with implications for border security in Central Asia and Northeast Asia. Similarly, Japanese and Indian power would pose greater challenges to Chinese security in the aftermath of a U.S.-China conflict. A weakened China might also face security challenges from foreign-supported disaffected minorities on its borders and Tibetan independence activists. Indeed, Chinese territorial integrity depends on its avoiding war with the United States. The strategic costs to China of a war with the United States are only part of the deterrence equation. China also possesses vital economic interests in stable relations with the United States. War would **end China’s quest for modernization** by severely constraining its access to U.S. markets, capital and technology, and by requiring China to place its economy on permanent wartime footing. The resultant economic reversal would derail China’s quest for “comprehensive national power” and great power status. Serious economic instability would also destabilize China’s political system on account of the resulting unemployment in key sectors of the economy and the breakdown of social order. Both would probably impose insurmountable challenges to party leadership. Moreover, defeat in a war with the United States over Taiwan would impose devastating nationalist humiliation on the Chinese Communist Party. In all, the survival of the party depends on preventing a Sino-American war.

#### -- The nature of Chinese landscape and US force allocation guaranteed it's a limited war.

Jeffrey **Record**, Professor at the US Air War College, Senior Fellow at CISP, Institute for Foreign Policy Analysis at Brookings, Winter, **2001** (Thinking About China and War. Aerospace Power Journal. Infotrac | SWON)

Assuming the absence of mindless escalation to a general nuclear exchange, a war between China and the United States would be constrained by limited military capacity and political objectives. For openers, neither China nor the United States is capable of invading and subjugating the other, and even if the United States had the ability to do so, avoidance of a land war on the Asian mainland has long been an injunction of American strategy. The objectives of a Sino-American war over Taiwan or freedom of navigation in the South China Sea would be limited-just as they were in the Sino-American war in Korea. And since the outcome in either case would be decided by naval and air forces, with regular ground forces relegated to a distinctly secondary role, a war over Taiwan or the South China Sea would also be limited in terms of the type of force employed. This was not the case in the Korean War, in which ground combat dominated. (To be sure, the US position on the ground would have been untenable without air dominance.)

#### We could strike before they arm

**Lieber and Press, 2006** (Keir, assistant prof. of polisci at Notre Dame, and Daryl, associate prof. of polisci at UPenn, “The Rise of U.S. Nuclear Primacy”, http://www.foreignaffairs.org/20060301faessay85204-p20/keir-a-lieber-daryl-g-press/the-rise-of-u-s-nuclear-primacy.html)

China's nuclear arsenal is even more vulnerable to a U.S. attack. A U.S. first strike could succeed **whether it was launched as a surprise or in the midst of a crisis** during a Chinese alert. China has a limited strategic nuclear arsenal. The People's Liberation Army currently possesses no modern SSBNs or long-range bombers. Its naval arm used to have two ballistic missile submarines, but one sank, and the other, which had such poor capabilities that it never left Chinese waters, is no longer operational. China's medium-range bomber force is similarly unimpressive: the bombers are obsolete and vulnerable to attack. According to unclassified U.S. government assessments, China's entire intercontinental nuclear arsenal consists of **18 stationary** single-warhead ICBMs. **These** **are not ready to launch on warning**: their warheads are kept in storage and the missiles themselves are unfueled. (China's ICBMs use liquid fuel, which corrodes the missiles after 24 hours. Fueling them is estimated to take two hours.) The lack of an advanced early warning system adds to the vulnerability of the ICBMs. It appears that China would **have no warning at all** of a U.S. submarine-launched missile attack or a strike using hundreds of stealthy nuclear-armed cruise missiles.

#### -- A US success in war leads to a regime change.

Robert D. **Kaplan**, Author of Imperial Grunts, June, **2005** (How We Would Fight China. Atlantic Monthly. EBSCO Host | SWON)

Like the nations involved in World War I, and unlike the rogue states everyone has been concentrating on, the United States and China in the twenty-first century would have the capacity to keep fighting even if one or the other lost a big battle or a missile exchange. This has far-reaching implications. "Ending a war with China," Vickers says, "may mean effecting some form of regime change, because we don't want to leave some wounded, angry regime in place." Another analyst, this one inside the Pentagon, told me, "Ending a war with China will force us to substantially reduce their military capacity, thus threatening their energy sources and the Communist Party's grip on power. The world will not be the same afterward. It's a very dangerous road to travel on."

### Cyber We Win

#### CURRENT US cyber capabilities will win us the war and de-escalate global conflict, but China will out-pace us soon ---

**Thompson ‘10** (Mark, Feb 02, “U.S. Cyberwar Strategy: The Pentagon Plans to Attack”, http://www.time.com/time/nation/article/0,8599,1957679,00.html)

The China-U.S. diplomatic spat over cyberattacks on Google has highlighted the growing significance of the Internet as a theater of combat. Deputy Defense Secretary William Lynn recently warned of its appeal to foes who are unable to match the U.S.'s conventional military might. An enemy country could deploy hackers to take down U.S. financial systems, communications and infrastructure, he suggested, at a cost far below that of building a trillion-dollar fleet of fifth-generation jet fighters. "Knowing this, **many militaries are developing offensive cyber capabilities**," Lynn said. "Some governments already have the capacity to disrupt elements of the U.S. information infrastructure." (On Tuesday, the nation's top intelligence official warned that cyber-enemies have "severely threatened" U.S. computer systems. "Malicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication," Dennis Blair, the director of national intelligence, told a Senate committee.) What U.S. officials don't like to acknowledge is that the Pentagon is hard at work developing an offensive cyber capability of its own. In fact, it has even begun using that capability to wage war. Beyond merely shutting down enemy systems, the U.S. military is crafting a witch's brew of stealth, manipulation and falsehoods designed to lure the enemy into believing he is in charge of his forces when in fact they have been secretly enlisted as allies of the U.S. military. And some in Washington fear that there hasn't been sufficient debate over the proper role of U.S. cyberweapons that are now being secretly developed. Pentagon officials acknowledge privately that such work is under way, though nearly all of it is classified. The recent creation of U.S. Cyber Command shows that the U.S. military is taking this mission seriously. "You have to be very careful about what you say in this area," says a top cyberwarrior of the Pentagon. "But you can tell there's something going on because the services are putting their money there and contractors are going after it in a big way." The Joint Chiefs of Staff want the ability to destroy an enemy's computer network "so badly that it cannot perform any function," according to the handbook on what the Pentagon calls "Information Operations." The U.S. military wants to keep foes "from accessing and using critical information, systems and services" and to spoof adversaries "by manipulating their perception of reality." Just how such wizardry is to be accomplished is contained in a classified supplement. But hints can be gleaned in a trickle of contracts and budget documents, larded with geek-speak, that have begun seeping onto the public record. The Air Force wants the ability to burrow into any computer system anywhere in the world "completely undetected." It wants to slip computer code into a potential foe's computer and let it sit there for years, "maintaining a 'low and slow' gathering paradigm" to thwart detection. Clandestinely exploring such networks, the Dominant Cyber Offensive Engagement program's goal is to "stealthily exfiltrate information" in hopes it might "discover information with previously unknown existence." The U.S. cyberwarriors' goal: "**complete functional** **capabilities**" of an enemy's computer network — from U.S. military keyboards. The Army is developing "techniques that capture and identify data traversing enemy networks for the purpose of Information Operations or otherwise countering adversary communications." And the Navy is developing "a non-lethal, non-attributable system designed to offer non-kinetic offensive information operation solutions," according to Pentagon budget documents. Yet concepts that have regulated war forever, such as **deterrence** and attribution, **are** slippery or **missing in cyberspace**. National boundaries don't exist, making moot the question of sovereignty. Asymmetries abound: defenders must defend everything, all the time, while an attacker can prevail by exploiting a single vulnerability. Tracking down the source of cybersabotage, routed like a skipping stone through a series of innocent servers, can be all but impossible. Are the attackers curious teenagers, criminal gangs, a foreign power — or, more likely, a criminal gang sponsored by a foreign power? Deterrence becomes meaningless when the identity of an attacker is unknown. "**We're in the stage before warfare**," cyberwarfare expert James Lewis told a Washington audience on Jan. 27. "We're in the stages of people poking around." Lewis, with the Center for Strategic and International Studies (CSIS), said cyberdefenses are inadequate. "Unless we find a way to use offensive capabilities as part of a deterrence or strategic defense," he said, "we will be unable to defeat these opponents." CSIS also released last week a survey of cybersecurity experts from around the world who "rank the U.S. as the country 'of greatest concern' in the context of foreign cyberattacks, just ahead of China." It's the instantaneous nature of cyberattacks that has rendered defenses against them obsolete. Once an enemy finds a chink in U.S. cyberarmor and opts to exploit it, it will be too late for the U.S. to play defense (it takes 300 milliseconds for a keystroke to travel halfway around the world). Far better to be on the prowl for cybertrouble and — with a few keystrokes or by activating secret codes long ago secreted in a prospective foe's computer system — **thwart any attack.** Cyberdefense "never works" by itself, says the senior Pentagon officer. "There has to be an element of offense to have a credible defense."

### Turns ASATs

#### Offensive Chinese ASATs take out US shit

Leonard **David**, Senior Space Writer, 7-27, **2005** (U.S. Defense Report: China Working on Anti-Satellite Systems. Space.com. http://www.space.com/news/050727\_china\_military.html | SWON)

In the arena of anti-satellite (ASAT) weapons, China is making headway, the report claims. "China is working on, and plans to field, ASAT systems. Beijing has and will continue to enhance its satellite tracking and identification network - the first step in establishing a credible ASAT capability. China can currently destroy or disable satellites only by launching a ballistic missile or space-launch vehicle armed with a nuclear weapon. However, there are many risks associated with this method, and consequences from use of nuclear weapons," the report says. China is also conducting research to develop ground-based laser ASAT weapons. The report cites the U.S. Defense Intelligence Agency as believing that Beijing "eventually could develop a laser weapon capable of damaging

or destroying satellites." Given this technology -- at lower power thresholds – "Chinese researchers may believe that low-energy lasers can ‘blind’ sensors on low-Earth-orbiting satellites," the report suggests, but whether Beijing has tested such a capability is unclear.

### Russia Collapse

#### Chinese disintegration is key to prevent Russian collapse.

**Hsi-mo, 2005**, professor at the Institute for Interdisciplinary Studies at Sun Yat-Sen U, 05 (Taipei Times, May 28, http://www.taipeitimes.com/News/editorials/archives/2005/05/28/2003256964)

Russia is facing disintegration. Although President Vladimir Putin is promoting an anti-US line to hold off this crisis, at a deeper level, Russia is not competing with the US, but with China. Disintegration has taken forms such as Georgia's Rose Revolution in 2003, Ukraine's Orange Revolution last year and Kyrgyzstan's Tulip Revolution this year. This wave of revolutions has even hit areas within Russia, including Bashkortostan, Tatarstan, Sakha (Yakutia), Tuva (Tyva), Karelia and Kalmykija. Some of these areas are strategically important to Russia, and if they become independent, **the country will break up**. For example, if Sakha becomes independent, northeastern regions like Chukotka and Kamchatka will be exposed to US influence, separated as they are from Alaska only by the Bering Strait. The US, and to some extent Europe, is exploiting and even encouraging this situation. In fact, by permitting and encouraging certain ethnic minority regions in Russia to initiate revolutions, the administration of US President George W. Bush is doing much the same thing as the UK, Nazi Germany, the administration of former US president Ronald Reagan and other superpowers have done in the past -- namely, to weaken and divide Russia. Russians are also aware of the imminent danger to their country. Last month, Presidential Administration Director Dmitri Medvedev, for the first time publicly admitted the danger. But this is not the whole story. The Putin administration has launched a national life-saving strategy: accelerating the concentration of power and sniping at the US by selling weapons to Syria and China, cooperating with Iran on nuclear technology and conducting joint military exercises with China this summer. As long as Moscow pursues these tactics with sufficient determination, it can cause serious trouble for the US. But Putin is unlikely to stop the drift toward disintegration, because the current crisis is only a consequence of the disintegration of the USSR. And this disintegration was simply a case of a 20th-century party-state aberration failing to keep up with the times. The breakup of the USSR was an expression of a party-state in crisis. It was not a solution to the crisis. Almost 10 years of a chaotic Boris Yeltsin administration could not completely uproot the party-state system. The Putin administration not only does not seek to eradicate the system, but has utilized its vestiges -- such as the Communist Information Bureau -- to establish its power while economically returning to the well-trodden path of strong state control. As a result, Russia has regained a superficial prosperity, such as its inclusion in the BRIC countries (Brazil, Russia, India and China), which are seen as leading emergent regional economies. But the agglomeration of problems that Russia continues to experience are sufficient to bring about its disintegration. The Putin administration has made clear that unless there is a major realignment of powers -- such as that caused by World War I -- **Russia's disintegration will be inevitable**. Looking at Eurasia as a whole, clearly only the disintegration of China would be sufficient to cause such a realignment and redistribution. Russia hopes to save itself by supporting those who resist the US, and is therefore cooperating more closely with China, among other nations. But, practically speaking, Russia is not the US' equal. So while Russia may oppose the US, this will not be sufficient to hold off its disintegration. The dialectics of history mean that **China is Russia's only hope; Russia can only hope that China will collapse before it does**.

#### Global nuclear war

Steven **David, ‘99**, Professor of Political Science at The Johns Hopkins University, Foreign Affairs, Jan/Feb, 1999, http://www.foreignaffairs.org/19990101faessay955/steven-r-david/saving-america-from-the-coming-civil-wars.html

As the central government finds itself unable to force its will beyond Moscow (if even that far), power devolves to the periphery. With the economy collapsing, republics feel less and less incentive to pay taxes to Moscow when they receive so little in return. Three-quarters of them already have their own constitutions, nearly all of which make some claim to sovereignty. Strong ethnic bonds promoted by shortsighted Soviet policies may motivate non-Russians to secede from the Federation. Chechnya's successful revolt against Russian control inspired similar movements for autonomy and independence throughout the country. If these rebellions spread and Moscow responds with force, civil war is likely. Should Russia succumb to internal war, the consequences for the United States and Europe will be severe. A major power like Russia -- even though in decline -- does not suffer civil war quietly or alone. An embattled Russian Federation might provoke opportunistic attacks from enemies such as China. Massive flows of refugees would pour into central and western Europe. Armed struggles in Russia **could easily spill into its neighbors**. Damage from the fighting, particularly attacks on nuclear plants, would poison the environment of much of Europe and Asia. Within Russia, the consequences would be even worse. Just as the sheer brutality of the last Russian civil war laid the basis for the privations of Soviet communism, a second civil war might produce another horrific regime. Most alarming is the real possibility that the violent disintegration of Russia could lead to loss of control over its nuclear arsenal. No nuclear state has ever fallen victim to civil war, but even without a clear precedent the grim consequences can be foreseen. Russia retains some 20,000 nuclear weapons and the raw material for tens of thousands more, in scores of sites scattered throughout the country. So far, the government has managed to prevent the loss of any weapons or much material. If war erupts, however, Moscow's already weak grip on nuclear sites will slacken, making weapons and supplies available to a wide range of anti-American groups and states. Such dispersal of nuclear weapons **represents the greatest physical threat America now faces**. And it is hard to think of anything that would increase this threat more than the chaos that would follow a Russian civil war.

### NATO

#### US-China War key to revive NATO

Robert D. **Kaplan, 2005**, is an Atlantic correspondent and the author of Imperial Grnts: The American Military on the Ground, forthcoming in September from Random House—the first of several books he is writing about the armed forces, June 2005 (The Atlantic, How We Would Fight China)

The first thing to understand is that the alliance system of the latter half of the twentieth century **is dead**. Warfare by committee, as practiced by NATO, has simply become too cumbersome in an age that requires light and lethal strikes. During the fighting in Kosovo in 1999 (a limited air campaign against a toothless enemy during a time of Euro-American harmony; a campaign, in other words, that should have been easy to prosecute) dramatic fissures appeared in the then-nineteen-member NATO alliance. The organization's end effectively came with the U.S. invasion of Afghanistan, in the aftermath of which, despite talk of a broad-based coalition, European militaries have usually done little more than patrol and move into areas already pacified by U.S. soldiers and Marines—a job more suggestive of the United Nations. NATO today is a medium for the expansion of bilateral training missions between the United States and formerly communist countries and republics: the Marines in Bulgaria and Romania, the Navy in Albania, the Army in Poland and the Czech Republic, Special Operations Forces in Georgia—the list goes on and on. Much of NATO has become a farm system for the major-league U.S. military. The second thing to understand is that the functional substitute for a NATO of the Pacific already exists, and is indeed up and running. It is the U.S. Pacific Command, known as PACOM. Unencumbered by a diplomatic bureaucracy, PACOM is a large but nimble construct, and its leaders understand what many in the media and the policy community do not: that the center of gravity of American strategic concern is already the Pacific, not the Middle East. PACOM will soon be a household name, as CENTCOM (the U.S. Central Command) has been in the current epoch of Middle Eastern conflict—an epoch that will start to wind down, as far as the U.S. military is concerned, during the second Bush administration.nThe third thing to understand is that, ironically, the vitality of NATO itself, the Atlantic alliance, could be revived by **the Cold War in the Pacific**—and indeed the **re-emergence of NATO** as an indispensable war-fighting instrument should be America's unswerving aim. In its posture toward China the United States will look to Europe and NATO, whose help it will need as a strategic counterweight and, by the way, as a force to patrol seas more distant than the Mediterranean and the North Atlantic. That is why NATO's current commander, Marine General James L. Jones, emphasizes that NATO's future lies in amphibious, expeditionary warfare.

#### Nuclear War

John S. **Duffield, ‘94**, assistant professor of government and foreign affairs at the University of Virginia, Winter 1994, Political Science Quarterly, Vol. 109, No. 5, “NATO's functions after the Cold War,” p. infotrac

Initial analyses of NATO's future prospects overlooked at least three important factors that have helped to ensure the alliance's enduring relevance. First, they underestimated the extent to which external threats sufficient to help justify the preservation of the alliance would continue to exist. In fact, NATO still serves to secure its members against a number of actual or potential dangers emanating from outside their territory. These include not only the residual threat posed by Russian military power, but also the relatively new concerns raised by conflicts in neighboring regions. Second, the pessimists failed to consider NATO's capacity for institutional adaptation. Since the end of the cold war, the alliance has begun to develop two important new functions. NATO is increasingly seen as having a significant role to play in containing and controlling militarized conflicts in Central and Eastern Europe. And, at a deeper level, it works to **prevent such conflicts from arising** at all by actively promoting stability within the former Soviet bloc. Above all, NATO pessimists overlooked the valuable intra-alliance functions that the alliance has always performed and that remain relevant after the cold war. Most importantly, NATO has helped stabilize Western Europe, whose states had often been bitter rivals in the past. By damping the security dilemma and providing an institutional mechanism for the development of common security policies, NATO has contributed to making the use of force in relations among the countries of the region **virtually inconceivable**. In all these ways, NATO clearly serves the interests of its European members. But even the United States has a significant stake in preserving a peaceful and prosperous Europe. In addition to strong transatlantic historical and cultural ties, American economic interests in Europe - as a leading market for U.S. products, as a source of valuable imports, and as the host for considerable direct foreign investment by American companies - remain substantial. If history is any guide, moreover, the United States could easily be drawn into a future major war in Europe, the consequences of which would likely be even more devastating than those of the past, **given the existence of nuclear weapons**.

### Prolif

#### Also, Chinese modernization would spur uncontrolled international proliferation

**Sanders and Jing-Dong 00** Phillip and Yuan, (China's Strategic ForceModernization: Issues and Implications in Proliferation Challenges andNonproliferation Opportunities for New Administrations. OccasionalPaper No. 4. Center for Nonproliferation Studies, July, <http://cns.miis.edu/cns/projects/eanp/conf/op4_sjd.pdf>) //khirn

Because this scenario involves a significant expansion of China’s strategic nuclear force, it would have a broad negative impact on international arms control and nonproliferation regimes. In the worst case, the United States might interpret China’s buildup in response to a US NMD deployment as evidence of hostile Chinese intentions, stimulating an arms race and an end to cooperation on regional security, nonproliferation, and arms control issues. The United States might also respond by attempting to build a “thick” NMD system capable of neutralizing China’s nuclear deterrent. The costs of such an offense-defense arms race would be very heavy for both sides, and it is not clear whether the technology for a “thick” missile defense system would be effective or affordable. China’s nuclear buildup in an arms race with the United States would have major negative consequences for other regional actors, such as Japan, Russia, and India. A doctrinal shift from minimal deterrence to limited deterrence would call China’s NFU pledge into question. The associated build-up of Chinese nuclear missile forces, coupled with a US-Russian START III build-down, would move China closer to numerical parity. This could have two contradictory consequences. China’s two-decade free ride on superpower nuclear weapons reductions might end, as international pressure mounted for China to participate in the global nuclear disarmament process. However, the United States and Russia might reconsider the further reductions in their strategic nuclear arsenals, especially if China refused to make reductions in its arsenal. A shift in Chinese nuclear doctrine would probably be interpreted by the United States as evidence of Chinese hostility, which would worsen relations and undermine regional stability. Any significant expansion of China’s nuclear force would have important implications for regional security dynamics. Some Japanese analysts would interpret China’s strategic modernization as a threat, especially if it includes a shift to limited deterrence and an expansion in the number of MRBMs. The closing of the gap between Chinese nuclear missile forces and US military capabilities and the potential for nuclear exchanges in the western Pacific could cause Tokyo to question the credibility of extended deterrence and the US nuclear umbrella. This might lead Japan to make a greater commitment to theater missile defense and to reconsider its nuclear and ballistic missile options. This reassessment might also be triggered by an easing of tensions on the Korean peninsula, which might undercut the rationale for a forward-based US presence in Northeast Asia.

#### That causes extinction

**Utgoff, ‘2** [Victor, Deputy Director of the Strategy, Forces, and Resources Division of the

Institute for Defense Analyses, “Proliferation, Missile Defence, and American Ambitions,” Survival, V. 44, Summer]

Hitler tried to impose a ‘victory or destruction’ policy on his people as Nazi Germany was going down to defeat.4 And Japan’s war minister, during debates on how to respond to the American atomic bombing, suggested ‘Would it not be wondrous for the whole nation to be destroyed like a beautiful flower?’5 If leaders are willing to engage in conflict with nuclear-armed nations, use of nuclear weapons in any particular instance may not be likely, but its probability would still be dangerously significant. In particular, human nature suggests that the threat of retaliation with nuclear weapons is not a reliable guarantee against a disastrous first use of these weapons. While national leaders and their advisors everywhere are usually talented and experienced people, even their most important decisions cannot be counted on to be the product of well-informed and thorough assessments of all optionsfrom all relevant points of view. This is especially so when the stakes are so large as to defy assessment and there are substantial pressures to act quickly, as could be expected in intense and fast-moving crises between nuclear-armed states.6 Instead, like other human beings, national leaders can be seduced by wishful thinking. They can misinterpret the words or actions of opposing leaders. Their advisors may produce answers that they think the leader wants to hear, or coalesce around what they know is an inferior decision because the group urgently needs the confidence or the sharing of responsibility that results from settling on something. Moreover, leaders may not recognise clearly where their personal or party interests diverge from those of their citizens. Under great stress, human beings can lose their ability to think carefully**.** They can refuse to believe that the worst could really happen, oversimplify the problem at hand, think in terms of simplistic analogies and play hunches. The intuitive rules for how individuals should respond to insults or signs of weakness in an opponent may too readily suggest a rash course of action. Anger, fear, greed, ambition and pride can all lead to bad decisions. The desire for a decisive solution to the problem at hand may lead to an unnecessarily extreme course of action. We can almost hear the kinds of words that could flow from discussions in nuclear crises or war. ‘These people are not willing to die for this interest’. ‘No sane person would actually use such weapons’. ‘Perhaps the opponent will back down if we show him we mean business by demonstrating a willingness to use nuclear weapons’. ‘If I don’t hit them back really hard, I am going to be driven from office, if not killed’. Whether right or wrong, in the stressful atmosphere of a nuclear crisis or war, such words from others, or silently from within, might resonate too readily with a harried leader. Thus, both history and human nature suggest that nuclear deterrence can be expected to fail from time to time, and we are fortunate it has not happened yet. But the threat of nuclear war is not just a matter of a few weapons being used. It could get much worse. Once a conflict reaches the point where nuclear weapons are employed, the stresses felt by the leaderships would rise enormously. These stresses can be expected to further degrade their decision-making. The pressures to force the enemy to stop fighting or to surrender could argue for more forceful and decisive military action, which might be the right thing to do in the circumstances, but maybe not. And the horrors of the carnage already suffered may be seen as justification for visiting the most devastating punishment possible on the enemy.7 Again, history demonstrates how intense conflict can lead the combatants to escalate violence to the maximum possible levels. In the Second World War, early promises not to bomb cities soon gave way to essentially indiscriminate bombing of civilians. The war between Iran and Iraq during the 1980s led to the use of chemical weapons on both sides and exchanges of missiles against each other’s cities. And more recently, violence in the Middle East escalated in a few months from rocks and small arms to heavy weapons on one side, and from police actions to air strikes and armoured attacks on the other. Escalation of violence is also basic human nature. Once the violence starts, retaliatory exchanges of violent acts can escalate to levels unimagined by the participants beforehand.8 Intense and blinding anger is a common response to fear or humiliation or abuse. And such anger can lead us to impose on our opponents whatever levels of violence are readily accessible. In sum, widespread proliferation is likely to lead to an occasional shoot-out with nuclear weapons, and that such shoot-outs will have a substantial probability of escalating to the maximum destruction possible with the weapons at hand. Unless nuclear proliferation is stopped, we are headed toward a world that will mirror the American Wild West of the late 1800s. With most, if not all, nations wearing nuclear ‘six-shooters’ on their hips, the world may even be a more polite place than it is today, but every once in a while we will all gather on a hill to bury the bodies of dead cities or even whole nations.

#### Prolif technology is evolving- spread is much easier and faster

**Heisbourg 4-4**-12 [François, chairman of the International Institute for Strategic Studies, special adviser at the Fondation pour la Recherche Stratégique, “How Bad Would the Further Spread of Nuclear Weapons Be?” http://www.npolicy.org/article.php?aid=1171&rtid=2]

**Ongoing proliferation differs from that of the first half-century of the nuclear era** in three essential ways: on the demand side, the set of putative nuclear actors is largely focused in the most strategically stressed regions of the world; on the supply side, **the actual or potential purveyors of proliferation are no longer principally the first, industrialized, generation of nuclear powers; the technology involved in proliferation is somewhat less demanding than it was during the first nuclear age**. Taken together, **these changes entail growing risks of nuclear use**. Demand is currently focusing on two regions, the Middle East and East Asia (broadly defined) and involves states and, potentially, non-state actors. In the Middle East, Iran’s nuclear program is the focus of the most intense concerns. A potential consequence in proliferation terms would be to lead regional rivals of Iran to acquire nuclear weapons in term: this concern was vividly in 2007 by the then President of France, Jacques Chirac (19) who specifically mentioned Egypt and Saudi Arabia. The likelihood of such a “proliferation chain-reaction” may have been increased by President Obama’s recent repudiation of containment as an option (20): short of Iran being persuaded or forced to abandon its nuclear ambitions, the neighboring states would presumably have to contemplate security options other than a Cold War style US defense guarantee. Given prior attempts by Iraq, Syria and Libya to become nuclear powers, the probability of a multipolar nuclear Middle East has to be rated as high in case Iran is perceived as having acquired a military nuclear capability. Beyond the Middle East, the possibility of civil war in nuclear-armed Pakistan leading to state failure and the possibility of nukes falling out of the hands of an effective central government. There are historical precedents for such a risk, most notably, but not only(21)in the wake of the collapse of the Soviet Union: timely and lasting action by outside powers, such as the US with the Nunn-Lugar initiative, and the successor states themselves has prevented fissile material from falling into unauthorized hands in significant quantities. Pakistan could pose similar problems in a singularly more hostile domestic environment. As things stand, non-state actors, such as post-Soviet mafiya bosses (interested in resale potential) or Al Qaeda (22) have sought, without apparent success, to benefit from opportunities arising from nuclear disorder in the former USSR and Central Asia. Mercifully, the price Al Qaeda was ready to pay was way below the going rate (upwards of hundreds of $million) for the sorts of services provided by the A.Q.Khan network (see below) to some of his clients. Although North Korea’s nuclear ambitions appear to be both more self-centered and more containable than is the case for Iran, the possibility of state collapse in combination with regional rivalry leave no room for complacency. More broadly we are facing the prospect of a multipolar nuclear Middle East, linked to an uncertain nuclear Pakistan already part of a nuclear South Asia tied via China to the Korean nexus in which nuclear America and Russia also have a stake. More broadly still, such a nuclear arc-of-crisis from the Mediterranean to the Sea of Japan, would presumably imply the breakdown of the NPT regime, or at least its reversion to the sort of status it had during the Seventies, when many of its currently significant members had not yet joined (23), unloosening both the demand and supply sides of proliferation. On the supply side, “old style” proliferation relied on official cooperation between first-generation nuclear or nuclearizing powers, of which the Manhattan project was a forerunner (with American, British and Canadian national contributions and multinational scientific teams), followed inter alia by post-1956 French-Israeli, post-1958 US-UK, pre-1958 USSR-China cooperation. If India relied heavily on the “unwitting cooperation” , notably on the part of Canada and the US involved in the Atoms for Peace CIRUS research reactor, Pakistan set up the first dedicated, broad spectrum, cross-border trading network to make up for the weakness of its limited industrial base. This import-focused organization thus went beyond traditional espionage-aided efforts (as practiced by the USSR during and after the Manhattan project) or case-by-case purloining or diversion of useful material on the global market (as practiced by Israeli operatives). Even before the Pakistani network had fulfilled its primary task of supplying the national program, it began its transformation into an export-oriented venture. Libya, Iran, North Korea and a fourth country which remains officially unnamed became the main outlets of what became the world’s first private-sector (albeit government originated and ,presumably, supported)proliferation company which was only wound down after strong Western pressure on Pakistan after 9/11. Although **the** by-now richly documented **A.Q.Khan network** (24) appears to have ceased to function in its previous incarnation, it **has powerfully demonstrated that there is an international market for proliferation which other operators can expect to exploit**. Furthermore, budding, resource-weak nuclear powers have a strong incentive to cover the cost of their investment by selling or bartering their nuclear-related assets, including delivery systems. The fruits of state-to-state cooperation between Iran, North Korea and Pakistan are clearly apparent in the close-to-identical genealogy of their nuclear-capable ballistic missiles of the No-Dong/Ghauri/Shahab families displayed in military parades and test launches. Not all such cooperation consists of televised objects. Even in the absence of game-changing breakthroughs, technical trends facilitate both demand and supply-side proliferation. For the time being, the plutonium route towards the bomb remains essentially as easy and as difficult as from the earliest years of the nuclear era. Provided a country runs a (difficult-to-hide) research or a power reactor from which low-irradiated fuel can be downloaded at will (such as CANDU-type natural uranium reactors), **reprocessing is** a comparatively straightforward and **undemanding** task. Forging and machining a multiple-isotope metal which is notorious for its numerous physical states and chemical toxicity is a substantial challenge, with the companion complications of devising a reliable implosion mechanism. Nuclear testing is highly desirable to establish confidence in the end-result. **Opportunities for taking the plutonium-proliferation road may increase somewhat as new techniques** (such as pyro-processing) **come on stream**. Developments in the enriched uranium field have been more substantial in facilitating proliferation. **The development of lighter and more efficient centrifuges make it easier for a state to extract enriched uranium speedily in smaller and less visible facilities**. Dealing with the resulting military-level HEU is a comparatively undemanding task. **The long-heralded advent of industrially effective and reliable laser enrichment technology may eventually further increase ease of access**. Downstream difficulties would still remain. Although implosion-mechanisms are not mandatory, they are desirable in order both to reduce the critical mass of U235 for a nuclear explosion and to make for a lighter and smaller more-readily deliverable weapons package. In sum, incremental improvements increase the risk of proliferation. However, non-state actors are not yet, and will not be on the basis of known technical trends, in a position to master the various steps of the two existing military nuclear fuel cycles, which remain the monopoly of states. Non-state actors would need the active complicity from (or from accomplices within) states, or benefit from the windfall of state collapse, to acquire a military nuclear capability. The threat of nuclear terrorism continues to be subordinated to developments involving state actors, a remark which is not meant to be reassuring since such developments (see above) are increasingly likely as proliferation spreads to new states and as state failure threatens in the ‘arc of proliferation’ extending from the Mediterranean to North-East Asia. Furthermore, non-state actors can be satisfied with levels of nuclear reliability and performance which states could not accept. A difficult-to-deliver or fizzle-prone nuclear device would not provide a state with the level of deterrence needed to shield it from pre-emptive or retaliatory action, whereas a terrorist group would not be seeking such immunity. A road or ship-delivered imperfect device, which would be closer to a radiological bomb than to a fully-fledged atomic weapon would provide its non-state owners with immense potential. The road to a non-state device does not need to be as well-paved.

#### Prolif causes nuclear wars in the short-term- answers all of their deterrence arguments

**Kroenig 5-26**-12 [Matthew, assistant professor in the Department of Government at Georgetown University and a research affiliate with The Project on Managing the Atom at Harvard University, he served as a strategist on the policy planning staff in the Office of the Secretary of Defense where he received the Office of the Secretary of Defense’s Award for Outstanding Achievement. He is a term member of the Council on Foreign Relations and has held academic fellowships from the National Science Foundation, the Belfer Center for Science and International Affairs at Harvard University, the Center for International Security and Cooperation at Stanford University, and the Institute on Global Conflict and Cooperation at the University of California, “The History of Proliferation Optimism: Does It Have A Future?” <http://www.npolicy.org/article.php?aid=1182&rtid=2>]

**The spread of nuclear weapons poses a number of severe threats to international peace** and U.S. national security **including: nuclear war, nuclear terrorism, emboldened nuclear powers, constrained freedom of action, weakened alliances, and further nuclear proliferation**. This section explores each of these threats in turn. Nuclear War. The greatest threat posed by the spread of nuclear weapons is nuclear war. **The more states in possession of nuclear weapons, the greater the probability that** somewhere, someday, **there is a catastrophic nuclear war. A nuclear exchange between the two superpowers during the Cold War could have arguably resulted in human extinction** and a nuclear exchange between states with smaller nuclear arsenals, such as India and Pakistan, could still result in millions of deaths and casualties, billions of dollars of economic devastation, environmental degradation, and a parade of other horrors. To date, nuclear weapons have only been used in warfare once. In 1945, the United States used one nuclear weapon each on Hiroshima and Nagasaki, bringing World War II to a close. Many analysts point to sixty-five-plus-year tradition of nuclear non-use as evidence that nuclear weapons are unusable, but **it would be naïve to think that nuclear weapons will never be used again**. After all, analysts in the 1990s argued that worldwide economic downturns like the great depression were a thing of the past, only to be surprised by the dot-com bubble bursting in the later 1990s and the Great Recession of the late Naughts.[53] This author, for one, would be surprised if nuclear weapons are not used in my lifetime. **Before reaching a state of MAD, new nuclear states go through a transition period in which they lack a secure-second strike capability. In this context, one or both states might believe that it has an incentive to use nuclear weapons first**. For example, if Iran acquires nuclear weapons neither Iran, nor its nuclear-armed rival, Israel, will have a secure, second-strike capability. Even though it is believed to have a large arsenal, given its small size and lack of strategic depth, Israel might not be confident that it could absorb a nuclear strike and respond with a devastating counterstrike. Similarly, Iran might eventually be able to build a large and survivable nuclear arsenal, but, when it first crosses the nuclear threshold, Tehran will have a small and vulnerable nuclear force. **In these pre-MAD situations, there are at least three ways that nuclear war could occur. First, the state with the nuclear advantage might believe it has a splendid first strike capability**. In a crisis, Israel might, therefore, decide to launch a preemptive nuclear strike to disarm Iran’s nuclear capabilities and eliminate the threat of nuclear war against Israel. Indeed, this incentive might be further increased by Israel’s aggressive strategic culture that emphasizes preemptive action. **Second, the state with a small and vulnerable nuclear arsenal**, in this case Iran, **might feel use ‘em or loose ‘em pressures**. That is, if Tehran believes that Israel might launch a preemptive strike, Iran might decide to strike first rather than risk having its entire nuclear arsenal destroyed. Third, as Thomas Schelling has argued, **nuclear war could result due to the reciprocal fear of surprise attack**.[54] **If there are advantages to striking first, one state might start a nuclear war in the belief that war is inevitable and that it would be better to go first than to go second**. In a future Israeli-Iranian crisis, for example, Israel and Iran might both prefer to avoid a nuclear war, but decide to strike first rather than suffer a devastating first attack from an opponent. **Even in a world of MAD, there is a risk of nuclear war.**

**Rational deterrence theory assumes nuclear-armed states are governed by rational leaders that would not intentionally launch a suicidal nuclear war**. This assumption appears to have applied to past and current nuclear powers, but there is no guarantee that it will continue to hold in the future. For example, Iran’s theocratic government, despite its inflammatory rhetoric, has followed a fairly pragmatic foreign policy since 1979, but it contains leaders who genuinely hold millenarian religious worldviews who could one day ascend to power and have their finger on the nuclear trigger. **We cannot rule out the possibility that, as nuclear weapons continue to spread, one leader will choose to launch a nuclear war, knowing full well that it could result in self-destruction. One does not need to resort to irrationality, however, to imagine a nuclear war under MAD**. Nuclear weapons may deter leaders from intentionally launching full-scale wars, but they do not mean the end of international politics. As was discussed above, nuclear-armed states still have conflicts of interest and leaders still seek to coerce nuclear-armed adversaries. This leads to the credibility problem that is at the heart of modern deterrence theory: how can you threaten to launch a suicidal nuclear war? Deterrence theorists have devised at least two answers to this question. First, as stated above, leaders can choose to launch a limited nuclear war.[55] This strategy might be especially attractive to states in a position of conventional military inferiority that might have an incentive to escalate a crisis quickly. During the Cold War, the United States was willing to use nuclear weapons first to stop a Soviet invasion of Western Europe given NATO’s conventional inferiority in continental Europe. As Russia’s conventional military power has deteriorated since the end of the Cold War, Moscow has come to rely more heavily on nuclear use in its strategic doctrine. Indeed, Russian strategy calls for the use of nuclear weapons early in a conflict (something that most Western strategists would consider to be escalatory) as a way to de-escalate a crisis. Similarly, Pakistan’s military plans for nuclear use in the event of an invasion from conventionally stronger India. And finally, Chinese generals openly talk about the possibility of nuclear use against a U.S. superpower in a possible East Asia contingency. Second, as was also discussed above leaders can make a “threat that leaves something to chance.”[56] They can initiate a nuclear crisis. **By playing these risky games of nuclear brinkmanship, states can increases the risk of nuclear war in an attempt to force a less resolved adversary to back down**. Historical crises have not resulted in nuclear war, but many of them, including the 1962 Cuban Missile Crisis, have come close. And scholars have documented historical incidents when accidents could have led to war.[57] When we think about future nuclear crisis dyads, such as India and Pakistan and Iran and Israel, there are fewer sources of stability that existed during the Cold War, meaning that there is a very real risk that a future Middle East crisis could result in a devastating nuclear exchange.

### Heg

#### Coming modernization will collapse US hegemony.

**Waldron**, Lauder Professor of International Relations at University of Pennsylvania, **2004**

(Arthur, Hearing of the Subcommittee on East Asian and Pacific Affairs, Federal News Service, lexis-nexis)

Now let me briefly say something about the military build up. I thought Mr. Lawless' testimony was excellent, although as he said to me in the break, it's just the tip of the iceberg. The military is now the king maker in China. Politicians who want to advance, lavish money on the military, create generals and so forth. The Chinese build up is substantial and it does not affect just, for instance, Taiwan. It directly affects Japan, Korea, India, Indonesia, you name it. Even Russia. I always wonder why the Russians are selling all of this stuff to China. But they are, but it makes no sense. And if this military rearmament were to continue without some kind of countervailing rebalancing, we would have a very, very serious situation in East Asia. Two specific points on this. First, Americans should understand that the new Chinese military is the only one in the world that is being developed specifically to fight the United States. If you look at, for instance, the purchases of missiles from the former Soviet Union, many of these have only one use and that is to destroy aircraft carriers,

which they can do. We have no defense against these supersonic missiles. Now, you might say that their target was the aircraft carrier Charles de Gaulle, but I don't think so. I think that they have the great American carrier battle groups in mind. And, as I say, we have no defense against this. This is certainly not a cause for complacency. The second point -- and I thought your questioning of Mr. Lawless brought this out -- is that although many people will say that China seeks only minimal deterrence and has no great power ambitions, my own view is that there's no objective reason that if the present regime stays in power -- this is why regime change is so important and regime type -- there is no reason that China should not become every bit as strong and threatening as the Soviet Union was at its height because, as Mr. Lawless pointed out, the conditions that constrained the Soviet Union, economic conditions and so forth, don't apply in the case of China.

#### US leadership is key to prevent a global nuclear exchange.

Zalmay **Khalilzad**, Research Analyst at the RAND Institute, Spring, **1995** (Losing the Moment? The United States and the World After the Cold War. Washington Quarterly. Lexis | SWON)

Under the third option, the United States would seek to retain global leadership and to preclude the rise of a global rival or a return to multipolarity for the indefinite future. On balance, this is the best long-term guiding principle and vision. Such a vision is desirable not as an end in itself, but because a world in which the United States exercises leadership would have tremendous advantages. First, the global environment would be more open and more receptive to American values -- democracy, free markets, and the rule of law. Second, such a world would have a better chance of dealing cooperatively with the world's major problems, such as nuclear proliferation, threats of regional hegemony by renegade states, and low-level conflicts. Finally, U.S. leadership would help preclude the rise of another hostile global rival, enabling the United States and the world to avoid another global cold or hot war and all the attendant dangers, including a global nuclear exchange. U.S. leadership would therefore be more conducive to global stability than a bipolar or a multipolar balance of power system.

#### First- heg prevents proliferation

Mandelbaum ‘5 (Michael, Professor and Director of the American Foreign Policy Program at Johns Hopkins, “The Case for Goliath,” 2005, p. 39)

American forces remained in Europe and East Asia because the countries located in these two regions wanted them there, even if they did not always say so clearly or even explicitly. They wanted them there because the American presence offered the assurance that these regions would remain free of war and, in the case of Europe, free of the costly preparations for war that had marked the twentieth century. The American military presence was in both cases [is] a confidence-building measure, and if that presence were with-drawn, the countries in both regions would feel less confident that no threat to their security would appear. They would, in all likelihood, take steps to compensate for the absence of these forces. Those steps would surely not include war, at least not in the first instance. Instead, since the American forces serve as a hedge against uncertainty, some of the countries of East Asia and Europe might well seek to replace them with another source of hedging. A leading candidate for that role would be nuclear weapons of their own.9 The possession of nuclear weapons equips their owner with a certain leverage, a geopolitical weight that, unless somehow counterbalanced, can confer a political advantage in dealing with countries lacking them. Like the relationship between employer and employee, the one between a nuclear-weapon state and a non-nuclear-weapon state has inequality built into it, no matter how friendly that relationship may be. During the Cold War, the American military presence, and the guarantee of protection by the mighty nuclear arsenal of the United States that came with it, neutralized the nuclear weapons that the Soviet Union and the People's Republic of China accumulated. Russia and China retain nuclear stock-piles in the wake of the Cold War, and with the end of the American military presence in their regions, several of their non-nuclear neighbors—Germany, Poland, Japan, South Korea, and Taiwan, for example—might feel the need to off-set those stockpiles with nuclear forces of their own. Perhaps the process of replacing American nuclear armaments with those of other countries, if this should take place, would occur smoothly, with Europe and East Asia remaining peaceful throughout the transition. But this is not what most of the world believes. To the contrary, the spread of nuclear weapons to countries that do not already have them is widely considered to be the single greatest threat to international tranquillity in the twenty-first century. The United States has made the prevention of nuclear proliferation one of its most important foreign policies, and its efforts to this end constitute, like reassurance, a service to the other members of the international system. The greatest threat to their security that the members of the international system did face in the new century, one that the United States had devoted considerable resources and political capital to containing and that a serious reduction in the American global rule would certainly aggravate, was the spread of nuclear weapons. Nuclear proliferation poses three related dangers. The first is that, in the absence of an American nuclear guarantee, major countries in Europe and Asia will feel the need to acquire their own nuclear armaments. If the United States withdrew from Europe and East Asia, Germany might come to consider it imprudent to deal with a nuclear-armed Russia, and Japan with a nuclear-armed China, without nuclear arms of their own. They would seek these weapons in order to avoid an imbalance in power that might work to their disadvantage. The acquisition of nuclear weapons by such affluent, democratic, peaceful countries would not, by itself, trigger a war. It could, however, trigger arms races similar to the one between the United States and the Soviet Union during the Cold War. It would surely make Europe and East Asia less comfortable places, and relations among the countries of these regions more suspicious, than was the case at the outset of the twenty-first century. The spread of nuclear weapons poses a second danger, which the United States exerted itself to thwart to the extent of threatening a war in North Korea and actually waging one in Iraq and that the recession of American power would increase: the possession of nuclear armaments by "rogue" states, countries governed by regimes at odds with their neighbors and hostile to prevailing international norms. A nuclear-armed Iraq, an unlikely development after the over-throw of Saddam Hussein's regime, or a nuclear-armed Iran, a far more plausible prospect, would make the international relations of the Persian Gulf far more dangerous. That in turn would threaten virtually every country in the world because so much of the oil on which they all depend comes from that region.' A nuclear-armed North Korea would similarly change the international relations of East Asia for the worse. Especially if the United States withdrew from the region, South Korea and Japan, and perhaps ultimately Tai-wan, might well decide to equip themselves with nuclear weapons of their own. A North Korean nuclear arsenal would pose yet a third threat: nuclear weapons in the hands of a terrorist group such as al Qaeda. Lacking the infrastructure of a sovereign state, a terrorist organization probably could not construct a nuclear weapon itself. But it could purchase either a full-fledged nuclear explosive or nuclear material that could form the basis for a device that, while not actually exploding, could spew poisonous radiation over populated areas, killing or infecting many thousands of people.' Nuclear materials are potentially available for purchase not only in North Korea but elsewhere as well.

#### Second- alt is worse

Rosen ‘3 (Stephen, Professor of National Security and Military Affairs at Harvard, “An Empire, If you can keep it,” The National Interest, Spring 2003)

Rather than wrestle with such difficult and unpleasant problems, the United States could give up the imperial mission, or pretensions to it, now. This would essentially mean the withdrawal of all U.S. forces from the Middle East, Europe and mainland Asia. It may be that all other peoples, without significant exception, will then turn to their own affairs and leave the United States alone. But those who are hostile to us might remain hostile, and be much less afraid of the United States after such a withdrawal. Current friends would feel less secure and, in the most probable post-imperial world, would revert to the logic of self-help in which all states do what they must to protect themselves. This would imply the relatively rapid acquisition of weapons of mass destruction by Japan, South Korea, Taiwan, Iran, Iraq and perhaps Algeria, Saudi Arabia, Malaysia, Indonesia and others. Constraints on the acquisition of biological weapons would be even weaker than they are today. Major regional arms races would also be very likely throughout Asia and the Middle East. This would not be a pleasant world for Americans, or anyone else. It is difficult to guess what the costs of such a world would be to the United States. They would probably not put the end of the United States in prospect, but they would not be small. If the logic of American empire is unappealing, it is not at all clear that the alternatives are that much more attractive.

### A2 Early Warning/Accidents

#### Zero risk of accidents

**Quinlan 9** (Sir Michael Quinlan, Former Permanent Under-Secretary of State UK Ministry of Defense, Thinking About Nuclear Weapons: Principles, Problems, Prospects, p. 63-69, The book reflects the author's experience across more than forty years in assessing and forming policy about nuclear weapons, mostly at senior levels close to the centre both of British governmental decision-making and of NATO's development of plans and deployments, with much interaction also with comparable levels of United States activity in the Pentagon and the State department)

There have certainly been, across the decades **since** 19**45, many known accidents** involving nuclear weapons, from transporters skidding off roads to bomber aircraft crashing with or accidentally dropping the weapons they carried (in past days when such carriage was a frequent feature of readiness arrangements it no longer is). A few of these accidents may have released into the nearby environment highly toxic material. **None** however has entailed a nuclear detonation. Some commentators suggest that this reflects bizarrely good fortune amid such massive activity and deployment over so many years. A more rational deduction from the facts of this long experience would however be that the probability of any accident triggering a nuclear explosion is extremely low. It might be further nested that the mechanisms needed to set of such an explosion are technically demanding, and that in a large number of ways the past sixty years have seen extensive improvements in safety arrangements for both the design and the handling of weapons. It is undoubtedly possible to see respects in which, after the cold war, some of the factors bearing upon risk may be new or more adverse; but some are now plainly less so. The years which the world has come through entirely without accidental or unauthorized detonation have included early decades in **which knowledge was sketchier, precautions** were **less developed, and** weapon **designs were less ultra-safe** than they later became, as well as substantial periods in which weapon numbers were larger, deployments immure widespread arid diverse, movements more frequent, and several aspects of doctrine and readiness arrangements more tense. Similar considerations apply to the hypothesis of nuclear war being mistakenly triggered by false alarm. Critics again point to the fact, as it is understood, of numerous occasions when initial steps in alert sequences for US nuclear forces were embarked upon, or at least called for, by indicators mistaken or misconstrued. In none of these instances, it is accepted, did matters get at all near to nuclear launch—extraordinary good fortune again, critics have suggested. But the rival and more **logical inference** from **hundreds of events** stretching over **sixty years** of experience presents itself once more: that the probability of initial misinterpretation leading far towards mistaken launch **is remote**

. Precisely because any nuclear weapon processor recognizes the vast gravity of any launch, release sequences have **many steps**, and human decision is **repeatedly interposed** as well as capping the sequences. To convey that because a first step was prompted the world somehow came close to accidental nuclear war is wild hyperbole, rather like asserting, when a tennis champion has lost his opening service game, that he was nearly beaten in straight sets. **History** anyway **scarcely offers any** ready **example** of major war started by accident **even before the nuclear revolution imposed an order-of-magnitude increase of caution**. In was occasion conjectured that nuclear war might be triggered by the real but accidental or unauthorized launch of a strategic nuclear-weapon delivery system in the direction of a potential adversary. No such launch is known to have occurred in over sixty years. The probability of it is therefore very low. But even if it did happen, the further hypothesis of it initiating a general nuclear exchange is far-fetched. It fails to consider the real situation of decision-makers, as pages 63-4 have brought out. The notion that cosmic holocaust might be mistakenly precipitated in this way **belongs to science fiction**.

### A2 Environment

#### The environment is resilient and indestructible

**Easterbrook ‘95** (Distinguished Fellow, Fullbright Foundation (Gregg, A Moment on Earth pg 25)

IN THE AFTERMATH OF EVENTS SUCH AS LOVE CANAL OR THE Exxon Valdez oil spill, every reference to the environment is prefaced with the adjective "fragile." "Fragile environment" has become a welded phrase of the modern lexicon, like "aging hippie" or "fugitive financier." But the notion of a fragile environment is profoundly wrong. Individual animals, plants, and people are distressingly fragile. **The environment** that contains them **is** close to **indestructible.** The living environment of **Earth has survived ice ages;** bombardments of **cosmic radiation more deadly than atomic fallout**; **solar radiation more powerful than the worst-case projection for ozone depletion; thousand-year periods of intense volcanism releasing global air pollution** **far worse than** that made by **any factory**; **reversals of the planet's magnetic poles; the rearrangement of continents**; transformation of plains into mountain ranges and of seas into plains; fluctuations of ocean currents and the jet stream; **300-foot vacillations in sea levels**; shortening and lengthening of the seasons caused by shifts in the planetary axis; **collisions of asteroids and comets** **bearing far more force than man's nuclear arsenals**; and the years without summer that followed these impacts. Yet hearts beat on, and petals unfold still. **Were the environment fragile it would have expired many eons** **before** the advent of the industrial affronts of the dreaming ape. Human assaults on the environment, though mischievous, **are pinpricks compared to forces of the magnitude nature is accustomed to resisting.**

### A2 CCP Lashout

#### No lashout- CCP would fear retaliation AND even if the order was issuds the PLA would not obey

**Gilley 5** (Bruce, Professor of International Affairs @ New School University and Former Contributing Editor @ the Far Eastern Economic Review, “China’s Democratic Future,” mss)

More ominous as a piece of "last ditchism" would be an attack on Taiwan. U.S. officials and many overseas democrats believe that there is a significant chance of an attack on Taiwan if the CCP is embattled at home. Indeed, China's strategic journals make frequent reference to this contingency: "The need for military preparations against Taiwan is all the more pressing in light of China's growing social tensions and unstable factors which some people, including the U.S. might take advantage of under the flag of 'humanism' to paralyze the Chinese government," one wrote. Such a move would allow the government to impose martial law on the country as part of war preparations, making the crushing of protest easier. It would also offer the possibility, if successful, of CCP survival through enhanced nationalist legitimacy. Yet **the risks, even to a dying regime, may be too high**. **An unprovoked attack on Taiwan would almost certainly bring the U.S. and its allies to the island's rescue**. **Those forces would not stop at Taiwan but might march on Beijing and oust the CCP**, **or attempt to do so through stiff sanctions,** calling it a threat to regional and world peace. **Such an attack might also face the opposition of the peoples of Fujian, who would be expected to** provide logistical support and possibly **bear the worst burdens of war. They, like much of coastal China, look to Taiwan for investment and culture and have a close affinity with the island**. As a result, **there are doubts about whether such a plan could be put into action**. **A failed war would prompt a Taiwan declaration** **of independence and a further backlash against the CCP** at home, just as the May Fourth students of 1919 berated the Republican government for weakness in the face of foreign powers. **Failed wars brought down authoritarian regimes in Greece and Portugal** in 1974 **and** in **Argentina** in 1983. **Even if CCP leaders wanted war, it is unlikely that the PLA would oblige. Top officers would see the disastrous implications of attacking Taiwan. Military caution would** also **guard against the even wilder scenario of the use of** **nuclear weapons against Japan or the U. S.** At the height of the Tiananmen protests it appears there was consideration given to the use of nuclear weapons in case the battle to suppress the protestors drew in outside Countries .41 But even then, the threats did not appear to gain even minimal support. **In an atmosphere in which the military is thinking about its future, the resort to nuclear confrontation would not make sense.**

# CP

#### 2NC Text: The United States Federal Government should not prohibit all of cyber operations

# On Case

### Cyber D

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

Libicki 8/16/13

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

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

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

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

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

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

#### Uncontrollability of cyber-war is a neg warrant --- means countries won’t use them

Thomas P.M. Barnett 13, special assistant for strategic futures in the U.S. Defense Department's Office of Force Transformation from 2001 to 2003, is chief analyst for Wikistrat, March/April 2013, “Think Again: The Pentagon,” Foreign Policy, http://www.foreignpolicy.com/articles/2013/03/04/the\_pentagon?page=full

As for cyber serving as a stand-alone war-fifighting domain, there you'll find the debates no less theological in their intensity. After serving as senior managing director for half a dozen years at a software firm that specializes in securing supply chains, I'm deeply skeptical. Given the uncontrollable nature of cyberweapons (see: Stuxnet's many permutations), I view them as the 21st century's version of chemical weapons -- nice to have, but hard to use. Another way to look at it is to simply call a spade a spade: Cyberwarfare is nothing more than espionage and sabotage updated for the digital era. Whatever cyberwar turns out to be in the national security realm, it will always be dwarfed by the industrial variants -- think cyberthieves, not cyberwarriors. But you wouldn't know it from the panicky warnings from former Defense Secretary Leon Panetta and the generals about the imminent threat of a "cyber Pearl Harbor."¶ Please remember amid all this frenetic scaremongering that the Pentagon is never more frightened about our collective future than when it's desperately uncertain about its own. Given the rising health-care costs associated with America's aging population and the never-ending dysfunction in Washington, we should expect to be bombarded with frightening scenarios of planetary doom for the next decade or two. None of this bureaucratic chattering will bear any resemblance to global trends, which demonstrate that wars have grown increasingly infrequent, shorter in duration, and diminished in lethality. But you won't hear that from the next-warriors on the Potomac.

#### No risk of cyber war

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

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

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

#### Uncontrollability of cyber-war is a neg warrant --- means countries won’t use them

Thomas P.M. Barnett 13, special assistant for strategic futures in the U.S. Defense Department's Office of Force Transformation from 2001 to 2003, is chief analyst for Wikistrat, March/April 2013, “Think Again: The Pentagon,” Foreign Policy, http://www.foreignpolicy.com/articles/2013/03/04/the\_pentagon?page=full

As for cyber serving as a stand-alone war-fifighting domain, there you'll find the debates no less theological in their intensity. After serving as senior managing director for half a dozen years at a software firm that specializes in securing supply chains, I'm deeply skeptical. Given the uncontrollable nature of cyberweapons (see: Stuxnet's many permutations), I view them as the 21st century's version of chemical weapons -- nice to have, but hard to use. Another way to look at it is to simply call a spade a spade: Cyberwarfare is nothing more than espionage and sabotage updated for the digital era. Whatever cyberwar turns out to be in the national security realm, it will always be dwarfed by the industrial variants -- think cyberthieves, not cyberwarriors. But you wouldn't know it from the panicky warnings from former Defense Secretary Leon Panetta and the generals about the imminent threat of a "cyber Pearl Harbor."¶ Please remember amid all this frenetic scaremongering that the Pentagon is never more frightened about our collective future than when it's desperately uncertain about its own. Given the rising health-care costs associated with America's aging population and the never-ending dysfunction in Washington, we should expect to be bombarded with frightening scenarios of planetary doom for the next decade or two. None of this bureaucratic chattering will bear any resemblance to global trends, which demonstrate that wars have grown increasingly infrequent, shorter in duration, and diminished in lethality. But you won't hear that from the next-warriors on the Potomac.

#### No motivation or will

Cavelty ’12 (Myriam Dunn Cavelty, Dr. Myriam Dunn Cavelty is Head of the New Risk Research Unit at the Center for Security Studies, ETH Zurich, Switzerland and was Fellow at the “stiftung neue verantwortung” in Berlin, Germany, Center for Security Studies (CSS), “The militarisation of cyber security as a source of global tension”, <http://www.academia.edu/1471717/The_militarisation_of_cyber_security_as_a_source_of_global_tension>, March 29, 2012)

Cyber war remains unlikely Since the potentially devastating effects of cyber attacks are so scary, the temptation is very high not only to think about worst-case scenarios, but also to give them a lot of (often too much) weight despite their very low probability. However, most experts agree that strategic cyber war remains highly unlikely in the foreseeable future, mainly due to the uncertain results such a war would bring, the lack of motivation on the part of the possible combatants, and their shared inability to defend against counterattacks. Indeed, it is hard to see how cyber attacks could ever become truly effective for military purposes: It is exceptionally diffcult to take down multiple, specific targets and keep them down over time. the key difficulty is proper reconnaissance and targeting, as well as the need to deal with a variety of diverse systems and be ready for countermoves from your adversary. Furthermore, nobody can be truly interested in allowing the unfettered proliferation and use of cyber war tools, least of all the countries with the offensive lead in this domain. Quite to the contrary, strong arguments can be made that the world’s big powers have an overall strategic interest in developing and accept- ing internationally agreed norms on cyber war, and in creating agreements that might pertain to the development, distribution, and de- ployment of cyber weapons or to their use (though the effectiveness of such norms must remain doubtful). the most obvious reason is that the countries that are currently openly discussing the use of cyber war tools are precisely the ones that are the most vulnerable to cyber warfare at- tacks due to their high dependency on information infrastructure. the features of the emerging information environment make it extremely unlikely that any but the most limited and tactically oriented instances of computer attacks could be con- tained. More likely, computer at- tacks could ‘blow back’ through the interdependencies that are such an essential feature of the environment. Even relatively harmless viruses and worms would cause considerable random disruption to businesses, governments, and consumers. this risk would most likely weigh much heavier than the uncertain benefits to be gained from cyber war activities.

#### Studies go negative

Leyden ’11 (The ill-informed leading the ill-informed... By [John Leyden](http://forms.theregister.co.uk/mail_author/?story_url=/2011/01/17/cyberwar_hype_oecd_study/) • Get more from this author Posted in [Government](http://www.theregister.co.uk/public_sector/government/), 17th January 2011)

Cyberwar hype is inhibiting government attempts to develop an appropriate response to cybersecurity threats, say computer scientists. A heavyweight study by UK computer scientists for the Organisation for Economic Cooperation and Development (OECD) concludes that it is "highly unlikely" there will ever be a "pure cyber war”, comparable with recent conflicts in Afghanistan or the Balkans. Suggestions to the contrary are down to "heavy lobbying" by suppliers, the report's authors – Professor Peter Sommer of the London School of Economics and Dr Ian Brown of the Oxford Internet Institute, University of Oxford – conclude. It is unlikely that there will ever be a true cyberwar. The reasons are: many critical computer systems are protected against known exploits and malware so that designers of new cyberweapons have to identify new weaknesses and exploits; the effects of cyberattacks are difficult to predict – on the one hand they may be less powerful than hoped but may also have more extensive outcomes arising from the interconnectedness of systems, resulting in unwanted damage to perpetrators and their allies. More importantly, there is no strategic reason why any aggressor would limit themselves to only one class of weaponry.

#### Cyberattacks impossible – no capabilities

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

"Cyberwar Is Already Upon Us." No way. "Cyberwar is coming!" John Arquilla and David Ronfeldt predicted in a celebrated Rand paper back in 1993. Since then, it seems to have arrived -- at least by the account of the U.S. military establishment, which is busy competing over who should get what share of the fight. Cyberspace is "a domain in which the Air Force flies and fights," Air Force Secretary Michael Wynne claimed in 2006. By 2012, William J. Lynn III, the deputy defense secretary at the time, was writing that cyberwar is "just as critical to military operations as land, sea, air, and space." In January, the Defense Department vowed to equip the U.S. armed forces for "conducting a combined arms campaign across all domains -- land, air, maritime, space, and cyberspace." Meanwhile, growing piles of books and articles explore the threats of cyberwarfare, cyberterrorism, and how to survive them. Time for a reality check: Cyberwar is still more hype than hazard. Consider the definition of an act of war: It has to be potentially violent, it has to be purposeful, and it has to be political. The cyberattacks we've seen so far, from Estonia to the Stuxnet virus, simply don't meet these criteria. Take the dubious story of a Soviet pipeline explosion back in 1982, much cited by cyberwar's true believers as the most destructive cyberattack ever. The account goes like this: In June 1982, a Siberian pipeline that the CIA had virtually booby-trapped with a so-called "logic bomb" exploded in a monumental fireball that could be seen from space. The U.S. Air Force estimated the explosion at 3 kilotons, equivalent to a small nuclear device. Targeting a Soviet pipeline linking gas fields in Siberia to European markets, the operation sabotaged the pipeline's control systems with software from a Canadian firm that the CIA had doctored with malicious code. No one died, according to Thomas Reed, a U.S. National Security Council aide at the time who revealed the incident in his 2004 book, At the Abyss; the only harm came to the Soviet economy. But did it really happen? After Reed's account came out, Vasily Pchelintsev, a former KGB head of the Tyumen region, where the alleged explosion supposedly took place, denied the story. There are also no media reports from 1982 that confirm such an explosion, though accidents and pipeline explosions in the Soviet Union were regularly reported in the early 1980s. Something likely did happen, but Reed's book is the only public mention of the incident and his account relied on a single document. Even after the CIA declassified a redacted version of Reed's source, a note on the so-called Farewell Dossier that describes the effort to provide the Soviet Union with defective technology, the agency did not confirm that such an explosion occurred. The available evidence on the Siberian pipeline blast is so thin that it shouldn't be counted as a proven case of a successful cyberattack. Most other commonly cited cases of cyberwar are even less remarkable. Take the attacks on Estonia in April 2007, which came in response to the controversial relocation of a Soviet war memorial, the Bronze Soldier. The well-wired country found itself at the receiving end of a massive distributed denial-of-service attack that emanated from up to 85,000 hijacked computers and lasted three weeks. The attacks reached a peak on May 9, when 58 Estonian websites were attacked at once and the online services of Estonia's largest bank were taken down. "What's the difference between a blockade of harbors or airports of sovereign states and the blockade of government institutions and newspaper websites?" asked Estonian Prime Minister Andrus Ansip. Despite his analogies, the attack was no act of war. It was certainly a nuisance and an emotional strike on the country, but the bank's actual network was not even penetrated; it went down for 90 minutes one day and two hours the next. The attack was not violent, it wasn't purposefully aimed at changing Estonia's behavior, and no political entity took credit for it. The same is true for the vast majority of cyberattacks on record. Indeed, there is no known cyberattack that has caused the loss of human life. No cyberoffense has ever injured a person or damaged a building. And if an act is not at least potentially violent, it's not an act of war. Separating war from physical violence makes it a metaphorical notion; it would mean that there is no way to distinguish between World War II, say, and the "wars" on obesity and cancer. Yet those ailments, unlike past examples of cyber "war," actually do kill people. "A Digital Pearl Harbor Is Only a Matter of Time." Keep waiting. U.S. Defense Secretary Leon Panetta delivered a stark warning last summer: "We could face a cyberattack that could be the equivalent of Pearl Harbor." Such alarmist predictions have been ricocheting inside the Beltway for the past two decades, and some scaremongers have even upped the ante by raising the alarm about a cyber 9/11. In his 2010 book, Cyber War, former White House counterterrorism czar Richard Clarke invokes the specter of nationwide power blackouts, planes falling out of the sky, trains derailing, refineries burning, pipelines exploding, poisonous gas clouds wafting, and satellites spinning out of orbit -- events that would make the 2001 attacks pale in comparison. But the empirical record is less hair-raising, even by the standards of the most drastic example available. Gen. Keith Alexander, head of U.S. Cyber Command (established in 2010 and now boasting a budget of more than $3 billion), shared his worst fears in an April 2011 speech at the University of Rhode Island: "What I'm concerned about are destructive attacks," Alexander said, "those that are coming." He then invoked a remarkable accident at Russia's Sayano-Shushenskaya hydroelectric plant to highlight the kind of damage a cyberattack might be able to cause. Shortly after midnight on Aug. 17, 2009, a 900-ton turbine was ripped out of its seat by a so-called "water hammer," a sudden surge in water pressure that then caused a transformer explosion. The turbine's unusually high vibrations had worn down the bolts that kept its cover in place, and an offline sensor failed to detect the malfunction. Seventy-five people died in the accident, energy prices in Russia rose, and rebuilding the plant is slated to cost $1.3 billion. Tough luck for the Russians, but here's what the head of Cyber Command didn't say: The ill-fated turbine had been malfunctioning for some time, and the plant's management was notoriously poor. On top of that, the key event that ultimately triggered the catastrophe seems to have been a fire at Bratsk power station, about 500 miles away. Because the energy supply from Bratsk dropped, authorities remotely increased the burden on the Sayano-Shushenskaya plant. The sudden spike overwhelmed the turbine, which was two months shy of reaching the end of its 30-year life cycle, sparking the catastrophe. If anything, the Sayano-Shushenskaya incident highlights how difficult a devastating attack would be to mount. The plant's washout was an accident at the end of a complicated and unique chain of events. Anticipating such vulnerabilities in advance is extraordinarily difficult even for insiders; creating comparable coincidences from cyberspace would be a daunting challenge at best for outsiders. If this is the most drastic incident Cyber Command can conjure up, perhaps it's time for everyone to take a deep breath. "Cyberattacks Are Becoming Easier." Just the opposite. U.S. Director of National Intelligence James R. Clapper warned last year that the volume of malicious software on American networks had more than tripled since 2009 and that more than 60,000 pieces of malware are now discovered every day. The United States, he said, is undergoing "a phenomenon known as 'convergence,' which amplifies the opportunity for disruptive cyberattacks, including against physical infrastructures." ("Digital convergence" is a snazzy term for a simple thing: more and more devices able to talk to each other, and formerly separate industries and activities able to work together.) Just because there's more malware, however, doesn't mean that attacks are becoming easier. In fact, potentially damaging or life-threatening cyberattacks should be more difficult to pull off. Why? Sensitive systems generally have built-in redundancy and safety systems, meaning an attacker's likely objective will not be to shut down a system, since merely forcing the shutdown of one control system, say a power plant, could trigger a backup and cause operators to start looking for the bug. To work as an effective weapon, malware would have to influence an active process -- but not bring it to a screeching halt. If the malicious activity extends over a lengthy period, it has to remain stealthy. That's a more difficult trick than hitting the virtual off-button. Take Stuxnet, the worm that sabotaged Iran's nuclear program in 2010. It didn't just crudely shut down the centrifuges at the Natanz nuclear facility; rather, the worm subtly manipulated the system. Stuxnet stealthily infiltrated the plant's networks, then hopped onto the protected control systems, intercepted input values from sensors, recorded these data, and then provided the legitimate controller code with pre-recorded fake input signals, according to researchers who have studied the worm. Its objective was not just to fool operators in a control room, but also to circumvent digital safety and monitoring systems so it could secretly manipulate the actual processes. Building and deploying Stuxnet required extremely detailed intelligence about the systems it was supposed to compromise, and the same will be true for other dangerous cyberweapons. Yes, "convergence," standardization, and sloppy defense of control-systems software could increase the risk of generic attacks, but the same trend has also caused defenses against the most coveted targets to improve steadily and has made reprogramming highly specific installations on legacy systems more complex, not less.

### Space D

#### No risk of space weapons

Rosen ‘13 (Armin Rosen, an Atlantic Media fellow, The Atlantic, "Give Peace a Chance—in Space", http://www.theatlantic.com/international/archive/2013/01/give-peace-a-chance-in-space/267223/, January 16, 2013)

"The wars of the future will not be fought on the battlefield or at sea," a military academy commandant voiced by Willem Dafoe intones toward the end of a now-classic 1997 episode of The Simpsons. "They will be fought in space, or possibly on top of a very tall mountain." This was meant as a joke, but the latter half of that statement would soon prove eerily prescient when India and Pakistan battled over Kashmir's Siachen glacier -- a strategically irrelevant ice field sitting over 18,000 feet above sea level -- during the Kargil War in 1999. For now, the prospect of military conflict in outer space still resides in the realm of dystopia or absurdity, to the point that a White House petition demanding the construction of a Star Wars-style "Death Star" could be treated as a harmless prank. In rejecting the petition this week, the White House rightly wondered why a debt-strapped U.S. government would spend $850 quadrillion on a weapons system "with a fundamental flaw that can be exploited by a one-man starship." Thankfully, the prospect of an orbital space-to-earth battlestation doesn't even need to be treated seriously. But it wasn't always this way. In 1952, the eminent rocket scientist Werner Von Braun imagined that a future space station would function as an orbital nuclear platform. Space historians believe that Russia's Salyut 3 space station, which was launched in June of 1974, had a cannon on board, in case a craft or satellite from an enemy country attempted to disrupt its mission. The Soviet Union experimented with Fractional Orbital Bombardment Systems in the 1960s and 70s -- basically nuclear delivery systems that were capable of orbiting the earth. The U.S. even detonated a nuclear weapon over 200 miles above the Pacific Ocean in July of 1962, an incident known as Starfish Prime that, according to Harvard University astrophysicist Jonathan McDowell, halved the useful lifetime of all satellites then in orbit, knocked out power in Hawaii, created an artificial Van Allen Belt that persisted for five years, and released radiation into the atmosphere that wouldn't fully dissipate until the end of the decade. For a time, it was all but taken for granted that space would not only be militarized, but weaponized -- used as a venue or staging area for violent clashes between space-faring nations, or attacks on the surface of the earth. Space war wasn't a punch line, but a possibility that nuclear-armed powers didn't think they could afford to ignore. The results of the Starfish event hint at one reason why that changed. "This is a great weapon. It does a lot of damage -- but it also killed everything you had yourself," McDowell says of the results of the high-altitude nuclear test. War in space was sure to have a cataclysmic effect on the country with the most space assets, regardless of the end result. But what about war from space? For powerful space-faring countries, space-to-earth or earth-to-space combat is about as practical as it is desirable -- which is to say, not very. "Space is incredibly useful for the military for a lot of things," McDowell explains. "It's great for intelligence, communication and navigation. The natural thing is to ask, 'where are my X-Wing fighters?' The fact is that it's hard to find a rationale for them." Laura Grego, a senior scientist in the global security program at the Union of Concerned Scientists, explained why an orbital weapons platform -- the kind of big-ticket military asset that you might want a fleet of X-Wing-type vehicles to protect -- is impractical for attacking targets on earth. "Everything in space is moving at rapid speeds. At the same time, the earth is rotating underneath it....as it's going around, you can't hold [the weapon] above your target. You might be over one country for 15 minutes and then you're gone." This tiny orbital window is called the absentee ratio, and an ICBM, which can hit any target on earth within minutes, isn't constrained by one. McDowell added that in order to reach atmospheric velocity, a rocket needs to reach a breakneck seven kilometers-per-second, far faster than the four to five kilometers-per-second an ICBM must travel. From a purely strategic standpoint, orbiting a weapon for space-to-ground use is more expensive and far less useful than existing, more earth-bound capabilities. Simply orbiting a nuke, while possible, is good for little other than blackmail, or, at best, a Dr. Strangelove or Dead Hand-style insurance policy for a paranoid and heavily-armed space-faring state. The space nuke would be a means of ensuring that someone (or some thing) has the capability of effectively wiping out most or perhaps all of the 1,016 satellites that currently orbit the earth, while rendering their orbits so debris-strewn as to be totally and perhaps permanently useless. Such dangerous and cavalier behavior is the stuff of cinematic super-villainy -- not statecraft. But there's another, more idealistic reason humanity is safe from the scourge of space war. And ironically, it suggests that we might not be safe forever. The ban on Death Star-like orbital weaponry is one of the more robust norms in international law.

A prohibition on stationing weapons of mass destruction in space, as well as the total demilitarization of the Moon, is enshrined in article 4 of the Outer Space Treaty of 1967, which 126 countries have signed. As University of Nebraska law professor and space law expert Frans von der Dunk notes, the treaty bans the stationing of weapons of mass destruction in space without banning their actual use in space. The stationing and use of kinetic or conventional weaponry is also allowed. Yet the most worrying aspect of the current legal regime is that the laws of war extend to the heavens as well. "The general international law on the law of force and the prohibition on the use of military force also applies in outer space," says von der Dunk. "If, as part of your self-defense you need your satellite to shoot down the satellite of your aggressor...that is perfectly allowed." Even so, the 1967 treaty demonstrates that in space, the peaceniks seem to be winning, at least for now. Joan Johnson-Freese of the Naval War College explained that there are two ways that, at the most schematic level, there are two ways the international legal regime could conceive of outer space: "On one end you put the view that space is a common heritage of mankind," she says. "The other end of the spectrum is that air, land and sea are all environments, and all those environments have been weaponized and therefore it's inevitable that space too will also become weaponized." The latter formulation raises a number of chilling possibilities: most people probably don't expect a war to break out in space, but the soldiers at Siachen probably didn't expect to be fighting atop an 18,000 mountain pass either. Humanity has proven willing to fight over literally anything, so long as the capability exists. Why should we assume space will be different? Space hasn't been weaponized, and the general anti-weaponization tilt of the 1967 treaty is part of the reason why. That tilt has gained the status of a respected legal norm, one arguably strengthened by the fact that the treaty itself was founded on a bedrock of mutual self-interest. "In the 1960s, the superpowers were able to agree that there was more of a benefit in keeping the other party from doing it than they saw a drawback in themselves being forced to abstain from it," von der Dunk says of the U.S. and Soviet Union's view towards stationing weapons of mass destruction in space. In other words, each side believed that preventing their opponent from weaponizing space was worth the potential strategic cost of foreclosing on their own ability to weaponize space. Even after the Cold War, the norm has endured.

#### No space war – 6 reasons

Krepon and Black 9 (Michael Krepon, co-founder of Stimson, and director of the South Asia and Space Security programs, Samuel Black, Research Associate at the Stimson Center, May 2009, “Space Security or Anti-satellite Weapons?” Stimson, [www.scribd.com/doc/30887749/Space-Security-or-Anti-Satellite-Weapons?query=ban](http://www.scribd.com/doc/30887749/Space-Security-or-Anti-Satellite-Weapons?query=ban))

Every US President since Dwight D. Eisenhower has recognized the value of satellites and has championed the peaceful uses of space. Consequently, ASAT tests have been rare. Another reason for restraint is that satellites serve as the eyes and ears of nations that have nuclear weapons. An attack on satellites could therefore trigger a nuclear war. Third, major powers that start a war in space would have great difficulty protecting their own satellites. Fourth, space warfare could cause massive amounts of debris, which would indiscriminately endanger essential satellite operations and manned spaceflight. Fifth, major space powers have interlinked economies. A war in space could do great harm to their financial transactions and international commerce. Sixth, space is widely viewed as a global commons that should remain a sanctuary blessedly free from the disputes that plague us on Earth. Because all major powers could be seriously disadvantaged by a war in space, none have wished to open this Pandora’s Box.

### No Lashout

#### No nuclear lashout

Rogin ‘10 (Josh, “Obama embraces missile defense in nuclear review,” Foreign Policy, <http://thecable.foreignpolicy.com/posts/2010/04/06/obama_embraces_missile_defense_in_nuclear_review>, April 6, 2010)

The document claims that missile defense is critical to allowing the United States to shift away from nuclear weapons, especially now that the U.S. will no longer threaten to use nukes to retaliate against non-nuclear attacks, such as from chemical or biological weapons. The review even features a photo of a missile being shot from an Aegis destroyer in 2007, in what many outside experts saw at the time as a clear demonstration of the fact that U.S. missile defense capabilities can also have offensive uses as well, such as shooting down a satellite. "Major improvements in missile defenses and counter-weapons of mass destruction (WMD) capabilities have strengthened deterrence and defense against CBW attack," reads the document, known as the Nuclear Posture Review, which will stand as the Obama administration's guiding document on all things nuclear. "With the advent of U.S. conventional military preeminence and continued improvements in U.S. missile defenses

and capabilities to counter and mitigate the effects of [chemical and biological weapons], the role of U.S. nuclear weapons in deterring non-nuclear attacks -- conventional, biological, or chemical -- has declined significantly," the document claims. Later on in the document, the administration points to Russia and China's nuclear modernization and notes that both countries view U.S. missile-defense expansion as destabilizing. Secretary Clinton addressed that issue in Tuesday's press conference. The NPR itself was careful to mention missile defense as only one of several capabilities needed to counter non-nuclear attacks. But Secretary Clinton was less careful. "It's no secret that countries around the world remained concerned about our missile-defense program," Clinton said, explaining that the NPR weighs in on "the role [missile defense] can and should play in deterring proliferation and nuclear terrorism." Ok, so now missile defense can deter chemical attacks, biological attacks, proliferation of nuclear technology, and suitcase bombs? Regardless, the document makes clear that with fewer nukes to be deployed once the new START agreement goes into effect, and with the role of nuclear weapons now limited to responding to nuclear threats, the administration is now looking to missile defense, among other technologies, to fill in the gap. "As the role of nuclear weapons is reduced in U.S. national security strategy, these non-nuclear elements will take on a greater share of the deterrence burden," the review reads.