### DA

#### The US has established Cyber Deterrence

Eric Talbot Jensen, ‘12 (Associate Professor, Brigham Young University Law School. , “CYBER DETERRENCE”, Emory law Journal)

Among the most worrisome of hacking incidents are those focused on critical national infrastructure.14 This infrastructure is the backbone of United States’ transportation and economic systems.15 The cost of downtime alone from major attacks on critical national infrastructure “exceeds . . . $6 million per day.”16 The attacks have caused President Barack Obama to recently state, From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.17 President Obama’ s recognition of the role and importance of deterring malicious cyber operations, including cyber attacks, incorporates the traditional notions of deterrence to this modern risk to national security. Deterrence has been a part of Western political security doctrine since ancient Greece18 and played a particularly key role in the post-World War II nuclear world.19 It is equally important in today’s world of cyber operations 20 and will continue to play a key role in the U.S. national security strategy.21 In fact, just as cyber operations offer unique capabilities as tools to accomplish national goals,22 they also present distinctive aspects of deterrence, both in line with traditional notions of deterrence and also some innovative and progressive ways of viewing deterrence.23

#### Offensive Cyber capabilities are key to an effective deterrent

Jari Rantapelkonen & Mirva Salminen, ’13 (“THE FOG OF CYBER DEFENCE”, National Defence University Department of Leadership and Military Pedagogy Publication Series 2 Article Collection n:o 10)

Offensive Weaponry is Required for Credibility and Deterrence¶ Discussion on offensive cyber weaponry should begin. As emphasized, currently there is no credible status for the armed forces and the nation states without cyber capabilities – this includes the offensive capability. The arms race is on and accelerating, even if we would like to turn a blind eye to it. The most frantic contemporary race is about talented individuals. When it comes to the creation of cyber capabilities, the question is not about the number of people one employs but about the talent the employed have. The US, China, Russia and many other countries are actively recruiting promising hackers. So are, most likely, Al Qaeda and other organizations. The real cyber question is about the talent and about creating cyber capabilities with the help of the most talented individuals.¶ It is not very popular or even desirable to talk publicly about offensive cyber weaponry in most countries. However, it has become necessary to explain the logic of offensive cyber capabilities to the general public. Naturally, this has to be done in various ways in different countries due to cultural and national reasons. The reasons why countries are developing offensive weapons and why they need them can be summarized into the following four points.¶ First, if one wishes to be a credible actor both in the military battlefield and in world politics, one must have offensive capabilities – as one must have defensive capabilities and the ability to be resilient. One simply cannot have a credible cyber defence without offensive abilities.¶ Second, in order to achieve and raise her deterrence, one must possess offensive capabilities. The ability to act offensively includes a strong preventive message to the others – provided that they understand it and believe it. Offensive capabilities represent the key component of deterrence.¶ Third, offensive thinking and building offensive weaponry are vital in order to create a strong and credible defence. With just “defence thinking” one will not succeed. One has to have an understanding of how the attacker acts, and one should try to find all possible vulnerabilities in her own defence. It is also a matter of developing one’s defensive potentials, testing the current defence and training one’s forces. All this becomes much more efficient if one can test it with her own capabilities. Without the ability to act as an attacker, no country can build an effective and credible cyber defence.

#### The threat is real – Russia is an example

Landon J. Wedermyer, Spring ’12 (“The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict”, Michigan State University College of Law, http://www.law.msu.edu/king/2011-2012/Wedermyer.pdf )

Since the early 2000’s, Russian military leaders have enthusiastically embraced the adoption of cyber weapons. 60 Used in a conventional military capacity, Russia envisions its cyber weapons as a “force multiplier. 61” In military strategy, a force multiplier is a component of a military force that increases the effectiveness or fighting efficiency of a unit or group.62 Like all offensive cyber strategies, Russia's includes the capability to disrupt the information infrastructure of their enemies and includes strategies that would attack financial markets and military and civilian communications capabilities as well as other parts of an enemy's critical infrastructure prior to the initiation of traditional military operations.63 Additionally, rumors have swirled for years that the Russian government maintains close ties with various “underworld” organizations within Russia, providing them with tools and tacit support to launch cyber vandalism, espionage, and other activities.64

#### Cyber Deterrence is ultimate deterrent- prevents Great Power War

Jari Rantapelkonen & Mirva Salminen, ’13 (“THE FOG OF CYBER DEFENCE”, National Defence University Department of Leadership and Military Pedagogy Publication Series 2 Article Collection n:o 10)

Based on that logic, cyber deterrence should play a similar role in the digitalized world. However, anonymity, advantage of attacks, global reach and interconnectedness greatly reduce the efficiency of cyber deterrence. Simultaneously, there is a lot of suspicion and rumours travelling around: what kind of capabilities the others might have and how they are using them already?¶ In the kinetic world, it is much easier to evaluate the opponent’s capabilities. It is quite easy to make a valid estimate on how many tanks, interceptors or submarines a country possesses. Countries also openly expose their arsenal, for example, in military parades, as well as their operational skills, for example, by organizing large military exercises. In the logic of deterrence, it is even more important to manifest force than to have real capabilities – yet the others have to know it.¶ Awareness Prevents Conflicts¶ Deterrence depends upon effective communication between the state and the entity it wishes to deter. One has to convince the others that if they attack, one has the capability and the capacity to do something about it. This is also the case in the cyber domain. If a country wants to be a credible actor in this domain, it should openly declare its offensive policy and expose its offensive capabilities. The policy acts as the rules for engagement. This is the trend some countries are already moving toward. For example, for the first time since the Second World War, Germany has publicly disclosed that it is developing offensive cyber weapons.5 In addition, in the latest Cyber Strategy of the United States, offensive cyber policy is strongly emphasized, and it has been said in public that the US Defense Advanced Research Projects Agency (DARPA) is focusing its research on offensive cyber capabilities.6 It has also been announced by many countries that a response to a cyber attack is not limited to the cyber domain, which is very understandable. The world needs to start talking openly about offensive cyber capabilities and the readiness levels – just as we discuss missile arsenals, air force, submarine fleets, or doctrines. We talk about great military exercises taking place in the kinetic world, but there is very little public discussion on things happening in cyberspace. Today, countries are aware of and appreciate the kinetic capacities which the others have. This is one reason why there are so few on- going wars in the world. Awareness prevents conflicts – at least, between the nation states – and it raises the threshold for conducting an attack. The defence policy of many countries is based on this assumption – if you have and if you are able to expose strong enough military capability, the likelihood of being attacked decreases.

#### Nuclear war

Harrell 2/20/09 (Eben, pg. http://www.time.com/time/world/article/0,8599,1880702,00.html)

But to marvel at the bizarre coincidence of the collision, or to breathe a sigh of relief that nuclear safety was not breached, is to miss the point. The seemingly impossible collision of two subs in a large ocean should remind us of the fallacy by which we assume nuclear weapons will never be used. Because the threat of global nuclear war is not zero, even a small chance of war each year, multiplied over a number of years, adds up to the likelihood that the weapons will be used. Like those two subs stalking through the Atlantic, the odds will begin to align. Mathematically, they are destined to. This is not a mere logic game. If there is a single "big idea" to have emerged in the first decade of the new millennium — from [the September 11 attacks](http://www.time.com/time/magazine/article/0%2C9171%2C1000761%2C00.html) to the [financial crash](http://www.time.com/time/business/article/0%2C8599%2C1846450%2C00.html) — it is the notion of the ["black swan,"](http://www.time.com/time/business/article/0%2C8599%2C1853531%2C00.html) the danger posed by difficult to predict, high-impact events. The short history of nuclear weapons is already scattered with unplanned and seemingly improbable incidents that suggest we feel more secure than we should. In 1995, a communication failure with the Russian Embassy led the Russian military to believe that a weather rocket launched off the coast of Norway was an incoming submarine-launched ballistic missile. In the 1980s, malfunctioning U.S. missile defense systems relayed information to U.S. officials of a massive incoming first strike — twice. As recently as 2007, a U.S. Air Force plane flew across the American heartland while unknowingly carrying several live warheads on board. At the time, all of these events were described as freak occurrences. The truth is they were freak occurrences. But they happened.([Read the Top 10 underreported stories of 2008.](http://www.time.com/time/specials/2008/top10/article/0%2C30583%2C1855948_1861760%2C00.html%22%20%5Ct%20%22_new)) A day after the latest nuclear accident became public, an analyst from the Federation of American Scientists, a nonproliferation think tank, released U.S. Naval intelligence documents obtained through the Freedom of Information Act that showed that the Russian Navy undertook more underwater ballistic missile submarine patrols in 2008 than it has in a decade. The Russian subs are joined in the word's oceans by nuclear-armed vessels from France, Britain, and China. Under the plains of the American West, and in similar silos in Russia, Air Force missile operators keep constant vigil, launch keys at the ready. Nuclear missiles have no self-destruct button; once launched, they cannot be called back. Twenty years after the end of the cold war, humanity still lives within 30 minutes of its own destruction. The price we pay for maintaining nuclear weapons is the gamble that the highly improbable will not lead to the unthinkable. The question to ask after this latest nervy episode: is it worth it?

### CP

#### Alex and I affirm the United States federal government should order a preemptive offensive cyber operation against the Peoples Republic of China.

#### The US must strike before china, attack is imminent

Avery Goldstein, 2013 (David M. Knott Professor of Global Politics and International Relations, Director of the Center for the Study of Contemporary China, and Associate Director of the Christopher H. Browne Cen- ter for International Politics at the University of Pennsylvania. , “First Things First, The Pressing Danger of Crisis Instability in U.S.-China Relations”, International Security, Vol. 37, No. 4 (Spring 2013), pp. 49–89)

Fourth, developments in technology since the third quarter of the twentieth century have dramatically improved the offensive conventional military capabilities available to states.46 In the European theater during the Cold War, the strategic advantage that would derive from a conventional first strike, especially during a Soviet-American crisis in which both sides were mobilized, was far from clear. Put another away, the weapons available did not clearly confer a decisive edge to either offense or defense.47 By contrast, in the early twentyarst century, although the United States enjoys a huge advantage over China in conventional military power, both sides possess capabilities that are much more effective, indeed perhaps only effective, if used to attack before the other side has either attacked or adopted countermeasures.¶ In particular, to the extent the effectiveness of the most advanced conventional weapons is tied to sophisticated command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) networks that can be degraded through kinetic strikes or electronic and cyberwarfare, their distinctive usefulness for striking the adversary, or for signaling resolve and warning of escalation, may evaporate once the ability to conadently track and target is damaged. If, as is generally believed, emerging cyber- and space-warfare capabilities favor the attacker over the defender, once peacetime restraint based on mutual vulnerability gives way to the search for advantage in a crisis, neither side can be confident about the durability of its C4ISR.48 The weaker Chinese side will have especially powerful incentives to use its most sophisticated capabilities before the integrity of elements essential to command and control over them is compromised. This may induce pressures to initiate the use of force that are as great as those induced by more traditional concerns about losing the weapons themselves.49 The stronger U.S. side, too, will face incentives to act first, though its considerations would be different

#### China first strike is inevitable: Non-Cyber based pentagon strategic choices make miscalc likely

David C. Gompert, 8-2-13 (is an adjunct senior fellow and Terrence K. Kelly is the director of the Strategy, Doctrine, and Resources Program at the Arroyo Center at the nonprofit, nonpartisan RAND Corporation.; he served as President Obama's principal deputy director of national intelligence., “Escalation Cause: How the Pentagon's New Strategy Could Trigger War with China”, RanD)

Air-Sea Battle increases the odds that a crisis will turn violent. Already, the Chinese People's Liberation Army (PLA) leans toward early strikes on U.S. forces if hostilities have begun or appear imminent (this inclination is a first premise of the Air-Sea Battle concept). Given that, to be most effective, Air-Sea Battle would need to take down Chinese targeting and strike capabilities before they could cause significant damage to U.S. forces and bases. It follows, and the Chinese fear, that such U.S. capabilities are best used early and first — if not preemptively, then in preparation for further U.S. offensive action. After all, such U.S. strikes have been used to initiate conflict twice in Iraq. This perception will, in turn, increase the incentive for the PLA to attack preemptively, before Air-Sea Battle has degraded its ability to neutralize the U.S. strike threat. It could give the Chinese cause to launch large-scale preemptive cyber- and anti-satellite attacks on our Air-Sea Battle assets. Indeed, they might feel a need, out of self-defense, to launch such attacks even if they had not planned to start a war. It is a dangerous situation when both sides put a premium on early action.

#### We have passed the point of no return- China has no incentive to halt Cyber attacks

* China has too much to gain
* Diplomatic outreach has failed
* PLA is in control of offensive capabilities

Gordon G. Chang, 6-6-13 (JD Cornell law and Author of many books about China, “Cyber Détente with China”, World Affairs)

The ultimate goal is to arrive at understandings with the Chinese. As a “senior American official involved in the negotiations” told the paper, “We need to get some norms and rules.”¶ Actually, we have long passed that stage. What we need to do at this point is stop Chinese cyber intrusions, cyber attacks, and cyber espionage, all part of what many suspect to be the most extensive cyber campaign conducted by one country against another¶ Administration officials, according to the Times, say they do not expect the talks will result in an immediate and significant reduction in Chinese attacks. And as Stanford University’s Tim Junio told the AP, “China benefits too much by stealing intellectual property from the US, so it’s really hard to imagine anyone convincing them to slow down.”¶ So what is the purpose of further talks? It’s not as if the Obama administration has not already broached the subject with Beijing. The president and various officials had numerous conversations with the Chinese during the first term, but the attacks increased dramatically in the middle of last year. This year, Treasury Secretary Jack Lew, Secretary of State John Kerry, and Joint Chiefs Chairman Martin Dempsey have all trooped to Beijing to discuss the issue with no apparent result. Despite the persistent effort to establish a cooperative relationship, the People’s Liberation Army reportedly ramped up its cyber attacks sometime around the beginning of April.

#### The CP solves and prevents nuclear escalation

DOD DSC, Department of defense Defense science board, 1-’13 (“Resilient Military Systems and the Advanced Cyber Threat”, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf)

To provide a non-nuclear but cyber survivable escalation ladder between conventional conflict and the nuclear threshold – that is to increase stability and build a new sub- nuclear red line in this emerging era of a cyber peer competitor delivering a catastrophic attack. Despite the past decade of policy deliberations on new conventional global strike capabilities as part of a deterrence strategy, the situation today is such that the ultimate U.S. deterrent, including response against a catastrophic full spectrum cyber attack, is the nuclear triad– intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), and nuclear-capable heavy bombers. The nuclear command and control (NC2) of the nuclear forces is comprised of systems, communication paths, and procedures associated with National Security Presidential Directive (NSPD)-28, which provides guidance to the Military Departments on the nature of redundant survivable communication paths to each nuclear delivery platform. Importantly, the definition of “survivability” in the traditional context of Nuclear C2 and forces usually referred to their credible ability to withstand a massive nuclear strike, with all of its attendant effects (including Electromagnetic Pulse (EMP)), and then provide a counter value retaliatory response. The Task Force expands the definition of survivability to include credible capability to withstand a Type V-VI cyber attack.

#### China is preparing for a cyber Spacewar- It ensures they beat the United States

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

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

**Extinction**

**Mitchell, et al 01** -Associate Professor of Communication and Director of Debate at the University of Pittsburgh

(Dr. Gordon, ISIS Briefing on Ballistic Missile Defence, “Missile Defence: Trans-Atlantic Diplomacy at a Crossroads”, No. 6 July, <http://www.isisuk.demon.co.uk/0811/isis/uk/bmd/no6.html>)

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

#### Chinese cyber offensive capabilities destroy Hegemony and cause china to attack Taiwan

Magnus Hjortdal, ’11 (researcher associated with CHINA-SEC, Centre for Military Studies at the University of Copenhagen. He holds an M.Sc. in Political Science from the University of Copenhagen and is owner of MH International Relations, which advises private and public institutions. Former Research Fellow at the Royal Danish Defense College “China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence”, Journal of strategic security)

Virtually all digital and electronic military systems can be attacked via cyberspace. Therefore, it is essential for a state to develop capabilities in this area if it wishes to challenge the present American hegemony. The interesting question then is whether China is developing capabilities in cyberspace in order to deter the United States.16 China's military strategists describe cyber capabilities as a powerful asymmetric opportunity in a deterrence strategy.19 Analysts consider that an "important theme in Chinese writings on computer-network operations (CNO) is the use of computer-network attack (CNA) as the spear- point of deterrence."20 CNA increases the enemy's costs to become too great to engage in warfare in the first place, which Chinese analysts judge to be essential for deterrence.21 This could, for example, leave China with the potential ability to deter the United States from intervening in a scenario concerning Taiwan. CNO is viewed as a focal point for the People's Liberation Army, but it is not clear how the actual capacity functions or precisely what conditions it works under.22¶ If a state with superpower potential (here China) is to create an opportunity to ascend militarily and politically in the international system, it would require an asymmetric deterrence capability such as that described here.23¶ It is said that the "most significant computer network attack is characterized as a pre-emption weapon to be used under the rubric of the rising Chinese strategy of [...] gaining mastery before the enemy has struck."24 Therefore, China, like other states seeking a similar capacity, has recruited massively within the hacker milieu inside China.25 Increasing resources in the PLA are being allocated to develop assets in relation to cyberspace.26 The improvements are visible: The PLA has established "information warfare" capabilities,27 with a special focus on cyber war- fare that, according to their doctrine, can be used in peacetime.28 Strategists from the PLA advocate the use of virus and hacker attacks that can paralyze and surprise its enemies.29

#### Heg solves great power war and dampens all global violence

Brooks et al 13

Stephen G. Brooks is Associate Professor of Government at Dartmouth College, John Ikenberry is the Albert G. Milbank Professor of Politics and International Affairs at Princeton University in the Department of Politics and the Woodrow Wilson School of Public and International Affairs. He is also a Global Eminence Scholar at Kyung Hee University, William C. Wohlforth is the Daniel Webster Professor in the Department of Government at Dartmouth College, International Security, Winter 2012/2013, "Don’t Come Home, America", MIT Press Journals

Assessing the Security Benefits of Deep Engagement Even if deep engagement’s costs are far less than retrenchment advocates claim, they are not worth bearing unless they yield greater benefits. We focus here on the strategy’s major security benefits; in the next section, we take up the wider payoffs of the United States’ security role for its interests in other realms, notably the global economy—an interaction relatively unexplored by international relations scholars. A core premise of deep engagement is that it prevents the emergence of a far more dangerous global security environment. For one thing, as noted above, the United States’ overseas presence gives it the leverage to restrain partners from taking provocative action. Perhaps more important, its core alliance commitments also deter states with aspirations to regional hegemony from contemplating expansion and make its partners more secure, reducing their incentive to adopt solutions to their security problems that threaten others and thus stoke security dilemmas. The contention that engaged U.S. power dampens the baleful effects of anarchy is consistent with influential variants of realist theory. Indeed, arguably the scariest portrayal of the war-prone world that would emerge absent the “American Pacifier” is provided in the works of John Mearsheimer, who forecasts dangerous multipolar regions replete with security competition, arms races, nuclear proliferation and associated preventive war temptations, regional rivalries, and even runs at regional hegemony and full-scale great power war.72 How do retrenchment advocates, the bulk of whom are realists, discount this benefit? Their arguments are complicated, but two capture most of the variation: (1) U.S. security guarantees are not necessary to prevent dangerous rivalries and conflict in Eurasia; or (2) prevention of rivalry and conflict in Eurasia is not a U.S. interest. Each response is connected to a different theory or set of theories, which makes sense given that the whole debate hinges on a complex future counterfactual (what would happen to Eurasia’s security setting if the United States truly disengaged?). Although a certain answer is impossible, each of these responses is nonetheless a weaker argument for retrenchment than advocates acknowledge. The first response flows from defensive realism as well as other international relations theories that discount the conflict-generating potential of anarchy under contemporary conditions.73 Defensive realists maintain that the high expected costs of territorial conquest, defense dominance, and an array of policies and practices that can be used credibly to signal benign intent, mean that Eurasia’s major states could manage regional multipolarity peacefully without the American pacifier. Retrenchment would be a bet on this scholarship, particularly in regions where the kinds of stabilizers that nonrealist theories point to—such as democratic governance or dense institutional linkages—are either absent or weakly present. There are three other major bodies of scholarship, however, that might give decisionmakers pause before making this bet. First is regional expertise. Needless to say, there is no consensus on the net security effects of U.S. withdrawal. Regarding each region, there are optimists and pessimists. Few experts expect a return of intense great power competition in a post-American Europe, but many doubt European governments will pay the political costs of increased EU defense cooperation and the budgetary costs of increasing military outlays.74 The result might be a Europe that is incapable of securing itself from various threats that could be destabilizing within the region and beyond (e.g., a regional conflict akin to the 1990s Balkan wars), lacks capacity for global security missions in which U.S. leaders might want European participation, and is vulnerable to the influence of outside rising powers. What about the other parts of Eurasia where the United States has a substantial military presence? Regarding the Middle East, the balance begins to swing toward pessimists concerned that states currently backed by Washington— notably Israel, Egypt, and Saudi Arabia—might take actions upon U.S. retrenchment that would intensify security dilemmas. And concerning East Asia, pessimism regarding the region’s prospects without the American pacifier is pronounced. Arguably the principal concern expressed by area experts is that Japan and South Korea are likely to obtain a nuclear capacity and increase their military commitments, which could stoke a destabilizing reaction from China. It is notable that during the Cold War, both South Korea and Taiwan moved to obtain a nuclear weapons capacity and were only constrained from doing so by a still-engaged United States.75 The second body of scholarship casting doubt on the bet on defensive realism’s sanguine portrayal is all of the research that undermines its conception of state preferences. Defensive realism’s optimism about what would happen if the United States retrenched is very much dependent on its particular—and highly restrictive—assumption about state preferences; once we relax this assumption, then much of its basis for optimism vanishes. Specifically, the prediction of post-American tranquility throughout Eurasia rests on the assumption that security is the only relevant state preference, with security defined narrowly in terms of protection from violent external attacks on the homeland. Under that assumption, the security problem is largely solved as soon as offense and defense are clearly distinguishable, and offense is extremely expensive relative to defense. Burgeoning research across the social and other sciences, however, undermines that core assumption: states have preferences not only for security but also for prestige, status, and other aims, and they engage in trade-offs among the various objectives.76 In addition, they define security not just in terms of territorial protection but in view of many and varied milieu goals. It follows that even states that are relatively secure may nevertheless engage in highly competitive behavior. Empirical studies show that this is indeed sometimes the case.77 In sum, a bet on a benign postretrenchment Eurasia is a bet that leaders of major countries will never allow these nonsecurity preferences to influence their strategic choices. To the degree that these bodies of scholarly knowledge have predictive leverage, U.S. retrenchment would result in a significant deterioration in the security environment in at least some of the world’s key regions. We have already mentioned the third, even more alarming body of scholarship. Offensive realism predicts that the withdrawal of the American pacifier will yield either a competitive regional multipolarity complete with associated insecurity, arms racing, crisis instability, nuclear proliferation, and the like, or bids for regional hegemony, which may be beyond the capacity of local great powers to contain (and which in any case would generate intensely competitive behavior, possibly including regional great power war). Hence it is unsurprising that retrenchment advocates are prone to focus on the second argument noted above: that avoiding wars and security dilemmas in the world’s core regions is not a U.S. national interest. Few doubt that the United States could survive the return of insecurity and conflict among Eurasian powers, but at what cost? Much of the work in this area has focused on the economic externalities of a renewed threat of insecurity and war, which we discuss below. Focusing on the pure security ramifications, there are two main reasons why decisionmakers may be rationally reluctant to run the retrenchment experiment. First, overall higher levels of conflict make the world a more dangerous place. Were Eurasia to return to higher levels of interstate military competition, one would see overall higher levels of military spending and innovation and a higher likelihood of competitive regional proxy wars and arming of client states—all of which would be concerning, in part because it would promote a faster diffusion of military power away from the United States. Greater regional insecurity could well feed proliferation cascades, as states such as Egypt, Japan, South Korea, Taiwan, and Saudi Arabia all might choose to create nuclear forces.78 It is unlikely that proliferation decisions by any of these actors would be the end of the game: they would likely generate pressure locally for more proliferation. Following Kenneth Waltz, many retrenchment advocates are proliferation optimists, assuming that nuclear deterrence solves the security problem.79 Usually carried out in dyadic terms, the debate over the stability of proliferation changes as the numbers go up. Proliferation optimism rests on assumptions of rationality and narrow security preferences. In social science, however, such assumptions are inevitably probabilistic. Optimists assume that most states are led by rational leaders, most will overcome organizational problems and resist the temptation to preempt before feared neighbors nuclearize, and most pursue only security and are risk averse. Confidence in such probabilistic assumptions declines if the world were to move from nine to twenty, thirty, or forty nuclear states. In addition, many of the other dangers noted by analysts who are concerned about the destabilizing effects of nuclear proliferation—including the risk of accidents and the prospects that some new nuclear powers will not have truly survivable forces—seem prone to go up as the number of nuclear powers grows.80 Moreover, the risk of “unforeseen crisis dynamics” that could spin out of control is also higher as the number of nuclear powers increases. Finally, add to these concerns the enhanced danger of nuclear leakage, and a world with overall higher levels of security competition becomes yet more worrisome. The argument that maintaining Eurasian peace is not a U.S. interest faces a second problem. On widely accepted realist assumptions, acknowledging that U.S. engagement preserves peace dramatically narrows the difference between retrenchment and deep engagement. For many supporters of retrenchment, the optimal strategy for a power such as the United States, which has attained regional hegemony and is separated from other great powers by oceans, is offshore balancing: stay over the horizon and “pass the buck” to local powers to do the dangerous work of counterbalancing any local rising power. The United States should commit to onshore balancing only when local balancing is likely to fail and a great power appears to be a credible contender for regional hegemony, as in the cases of Germany, Japan, and the Soviet Union in the midtwentieth century. The problem is that China’s rise puts the possibility of its attaining regional hegemony on the table, at least in the medium to long term. As Mearsheimer notes, “The United States will have to play a key role in countering China, because its Asian neighbors are not strong enough to do it by themselves.”81 Therefore, unless China’s rise stalls, “the United States is likely to act toward China similar to the way it behaved toward the Soviet Union during the Cold War.”82 It follows that the United States should take no action that would compromise its capacity to move to onshore balancing in the future. It will need to maintain key alliance relationships in Asia as well as the formidably expensive military capacity to intervene there. The implication is to get out of Iraq and Afghanistan, reduce the presence in Europe, and pivot to Asia— just what the United States is doing.83 In sum, the argument that U.S. security commitments are unnecessary for peace is countered by a lot of scholarship, including highly influential realist scholarship. In addition, the argument that Eurasian peace is unnecessary for U.S. security is weakened by the potential for a large number of nasty security consequences as well as the need to retain a latent onshore balancing capacity that dramatically reduces the savings retrenchment might bring. Moreover, switching between offshore and onshore balancing could well be difficult. Bringing together the thrust of many of the arguments discussed so far underlines the degree to which the case for retrenchment misses the underlying logic of the deep engagement strategy. By supplying reassurance, deterrence, and active management, the United States lowers security competition in the world’s key regions, thereby preventing the emergence of a hothouse atmosphere for growing new military capabilities. Alliance ties dissuade partners from ramping up and also provide leverage to prevent military transfers to potential rivals. On top of all this, the United States’ formidable military machine may deter entry by potential rivals. Current great power military expenditures as a percentage of GDP are at historical lows, and thus far other major powers have shied away from seeking to match top-end U.S. military capabilities. In addition, they have so far been careful to avoid attracting the “focused enmity” of the United States.84 All of the world’s most modern militaries are U.S. allies (America’s alliance system of more than sixty countries now accounts for some 80 percent of global military spending), and the gap between the U.S. military capability and that of potential rivals is by many measures growing rather than shrinking.85 In the end, therefore, deep engagement reduces security competition and does so in a way that slows the diffusion of power away from the United States. This in turn makes it easier to sustain the policy over the long term.

#### Dialogue fails- US and China views on cyber capabilities are too far apart to overcome

Diane Bartz and Paul Eckert, 7-14-11 (“U.S. and China face vast divide on cyber issues”, Reuters)

For two years, academic experts from the United States and China have quietly held talks on cyber-security, straining to establish rules of the road in a realm that has proven a persistent irritant between the world's two largest economies.¶ The informal discussions have yielded modest progress in areas such as cooperation to combat Internet fraud, where both Beijing and Washington have an incentive to work together, according to participants.¶ But mostly, the talks appear to have exposed a wide gap between the United States and China over almost everything virtual: policing computer networks, moderating cyber warfare, even controlling information.¶ China's contrasting view of cyber security was made clear as soon as the United States began discussing the need to protect computer networks, James Mulvenon, a China expert at the Defense Group Inc, told a recent Washington conference.¶ China wanted to talk about censorship. "The Chinese came back immediately and said no, no, no, we want to talk about information security, which is both protecting the network and policing the content on the network," Mulvenon said.¶ "Right from the outset, we were talking past one another," he added.

### Advantage

#### Government behaviors can be read with linear models of decision making – you should prefer our analysis

Wight 06 – Professor of IR @ University of Sydney –

(Colin, Agents, Structures and International Relations: Politics as Ontology, pgs. 48-50

One important aspect of this relational ontology is that these relations constitute our identity as social actors. According to this relational model of societies, one is what one is, by virtue of the relations within which one is embedded. A worker is only a worker by virtue of his/her relationship to his/her employer and vice versa. ‘Our social being is constituted by relations and our social acts presuppose them.’ At any particular moment in time an individual may be implicated in all manner of relations, each exerting its own peculiar causal effects. This ‘lattice-work’ of relations constitutes the structure of particular societies and endures despite changes in the individuals occupying them. Thus, the relations, the structures, are ontologically distinct from the individuals who enter into them. At a minimum, the social sciences are concerned with two distinct, although mutually interdependent, strata. There is an ontological difference between people and structures: ‘people are not relations, societies are not conscious agents’. Any attempt to explain one in terms of the other should be rejected. If there is an ontological difference between society and people, however, we need to elaborate on the relationship between them. Bhaskar argues that we need a system of mediating concepts, encompassing both aspects of the duality of praxis into which active subjects must fit in order to reproduce it: that is, a system of concepts designating the ‘point of contact’ between human agency and social structures. This is known as a ‘positioned practice’ system. In many respects, the idea of ‘positioned practice’ is very similar to Pierre Bourdieu’s notion of *habitus*. Bourdieu is primarily concerned with what individuals do in their daily lives. He is keen to refute the idea that social activity can be understood solely in terms of individual decision-making, or as determined by surpa-individual objective structures. Bourdieu’s notion of the *habitus* can be viewed as a bridge-building exercise across the explanatory gap between two extremes. Importantly, the notion of a habitus can only be understood in relation to the concept of a ‘social field’. According to Bourdieu, a social field is ‘a network, or a configuration, of objective relations between positions objectively defined’. A social field, then, refers to a structured system of social positions occupied by individuals and/or institutions – the nature of which defines the situation for their occupants. This is a social field whose form is constituted in terms of the relations which define it as a field of a certain type. A *habitus* (positioned practices) is a mediating link between individuals’ subjective worlds and the socio-cultural world into which they are born and which they share with others. The power of the habitus derives from the thoughtlessness of habit and habituation, rather than consciously learned rules. The habitus is imprinted and encoded in a socializing process that commences during early childhood. It is inculcated more by experience than by explicit teaching. Socially competent performances are produced as a matter of routine, without explicit reference to a body of codified knowledge, and without the actors necessarily knowing what they are doing (in the sense of being able adequately to explain what they are doing). As such, the *habitus* can be seen as the site of ‘internalization of reality and the externalization of internality.’ Thus social practices are produced in, and by, the encounter between: (1) the *habitus* and its dispositions; (2) the constraints and demands of the socio-cultural field to which the habitus is appropriate or within; and (3) the dispositions of the individual agents located within both the socio-cultural field and the *habitus*. When placed within Bhaskar’s stratified complex social ontology the model we have is as depicted in Figure 1. The explanation of practices will require all three levels. Society, as field of relations, exists prior to, and is independent of, individual and collective understandings at any particular moment in time; that is, social action requires the conditions for action. Likewise, given that behavior is seemingly recurrent, patterned, ordered, institutionalised, and displays a degree of stability over time, there must be sets of relations and rules that govern it. Contrary to individualist theory, these relations, rules and roles are not dependent upon either knowledge of them by particular individuals, or the existence of actions by particular individuals; that is, their explanation cannot be reduced to consciousness or to the attributes of individuals. These emergent social forms must possess emergent powers. This leads on to arguments for the reality of society based on a causal criterion. Society, as opposed to the individuals that constitute it, is, as Foucault has put it, ‘a complex and independent reality that has its own laws and mechanisms of reaction, its regulations as well as its possibility of disturbance. This new reality is society…It becomes necessary to reflect upon it, upon its specific characteristics, its constants and its variables’.

#### Their approach lacks support and lacks a model for future action – only predictive analysis based on causal chains solves

Dr. Sebastian L. V. Gorka et al 12, Director of the Homeland Defense Fellows Program at the College of International Security Affairs, National Defense University, teaches Irregular Warfare and US National Security at NDU and Georgetown, et al., Spring 2012, “The Complexity Trap,” Parameters, http://www.carlisle.army.mil/USAWC/parameters/Articles/2012spring/Gallagher\_Geltzer\_Gorka.pdf

We live in a world of unprecedented complexity, or so we are told. President Obama’s words above echo an increasingly common narrative in the American foreign policy and national security establishments: the forces of globalization, rising nonstate actors, irregular conflict, and proliferating destructive technologies have made crafting sound national security strategy more elusive than ever before. 2 If “strategy is the art of creating power” by specifying the relationship among ends, ways, and means, 3 then the existence of unprecedented complexity would seem to make this art not only uniquely difficult today but also downright dangerous, inasmuch as choosing any particular course of action would preclude infinitely adaptive responses in the future. As Secretary of Defense Robert Gates memorably described, the pre-9/11 challenges to American national security were “amateur night compared to the world today.” 4 And as former State Department Director of Policy Planning Anne-Marie Slaughter recently stated, there is a “universal awareness that we are living through a time of rapid and universal change,” one in which the assumptions of the twentieth century make little sense. 5 The “Mr. Y” article that occasioned her comments argued that, in contrast to the “closed system” of the twentieth century that could be controlled by mankind, we now live in an “open system” defined by its supremely complex and protean nature. 6 Unparalleled complexity, it seems, is the hallmark of our strategic age.¶ These invocations of complexity permeate today’s American national security documents and inform Washington’s post-Cold War and -9/11 strategic culture. The latest Quadrennial Defense Review begins its analysis with a description of the “complex and uncertain security landscape in which the pace of change continues to accelerate. Not since the fall of the Soviet Union or the end of World War II has the international terrain been affected by such farreaching and consequential shifts.” 7 In a similar vein, the National Intelligence Council’s Global Trends 2025 argues that the international system is trending towards greater degrees of complexity as power is diffused and actors multiply. 8 The Director of National Intelligence’s Vision 2015 terms our time the “Era of Uncertainty,” one “in which the pace, scope, and complexity of change are increasing.” 9 Disturbingly, the younger generation of foreign policy and national security professionals seems to accept and embrace these statements declaiming a fundamental change in our world and our capacity to cope with it. The orientation for the multi-thousand-member group of Young Professionals in Foreign Policy calls “conquering complexity” the fundamental challenge for the millennial generation. Complexity, it appears, is all the rage. ¶ We challenge these declarations and assumptions—not simply because they are empirically unfounded but, far more importantly, because they negate the very art of strategy and make the realization of the American national interest impossible. We begin by showing the rather unsavory consequences of the current trend toward worshipping at complexity’s altar and thus becoming a member of the “Cult of Complexity.” Next, we question whether the world was ever quite as simple as today’s avowers of complexity suggest, thus revealing the notion of today’s unprecedented complexity to be descriptively false. We then underscore that this idea is dangerous, given the consequences of an addiction to complexity. Finally, we offer an escape from the complexity trap, with an emphasis on the need for prioritization in today’s admittedly distinctive international security environment. Throughout, we hope to underscore that today’s obsession with complexity results in a dangerous denial of the need to strategize.

Policymakers will inevitably make predictions—the only question is whether they’re based off of explicit or implicit threats. Failure to make predictions based off of explicit risk calculation guarantees poor decisionmaking.

Fitzsimmons, 07 (Michael, defense analyst in Washington DC. “The Problem of Uncertainty in Strategic Planning”, Survival, Winter 06/07)

In defence of prediction Uncertainty is not a new phenomenon for strategists. Clausewitz knew that ‘many intelligence reports in war are contradictory; even more are false, and most are uncertain’. In coping with uncertainty, he believed that ‘what one can reasonably ask of an officer is that he should possess a standard of judgment, which he can gain only from knowledge of men and affairs and from common sense. He should be guided by the laws of probability.’34 Granted, one can certainly allow for epistemological debates about the best ways of gaining ‘a standard of judgment’ from ‘knowledge of men and affairs and from common sense’. Scientific inquiry into the ‘laws of probability’ for any given strate- gic question may not always be possible or appropriate. Certainly, analysis cannot and should not be presumed to trump the intuition of decision-makers. Nevertheless, Clausewitz’s implication seems to be that the burden of proof in any debates about planning should belong to the decision-maker who rejects formal analysis, standards of evidence and probabilistic reasoning. Ultimately, though, the value of prediction in strategic planning does not rest primarily in getting the correct answer, or even in the more feasible objective of bounding the range of correct answers. Rather, prediction requires decision- makers to expose, not only to others but to themselves, the beliefs they hold regarding why a given event is likely or unlikely and why it would be impor- tant or unimportant. Richard Neustadt and Ernest May highlight this useful property of probabilistic reasoning in their renowned study of the use of history in decision-making, Thinking in Time. In discussing the importance of probing presumptions, they contend: The need is for tests prompting questions, for sharp, straightforward mechanisms the decision makers and their aides might readily recall and use to dig into their own and each others’ presumptions. And they need tests that get at basics somewhat by indirection, not by frontal inquiry: not ‘what is your inferred causation, General?’ Above all, not, ‘what are your values, Mr. Secretary?’ ... If someone says ‘a fair chance’ ... ask, ‘if you were a betting man or woman, what odds would you put on that?’ If others are present, ask the same of each, and of yourself, too. Then probe the differences: why? This is tantamount to seeking and then arguing assumptions underlying different numbers placed on a subjective probability assessment. We know of no better way to force clarification of meanings while exposing hidden differences ... Once differing odds have been quoted, the question ‘why?’ can follow any number of tracks. Argument may pit common sense against common sense or analogy against analogy. What is important is that the expert’s basis for linking ‘if’ with ‘then’ gets exposed to the hearing of other experts before the lay official has to say yes or no.’35 There are at least three critical and related benefits of prediction in strate- gic planning. The first reflects Neustadt and May’s point – prediction enforces a certain level of discipline in making explicit the assumptions, key variables and implied causal relationships that constitute decision-makers’ beliefs and that might otherwise remain implicit. Imagine, for example, if Shinseki and Wolfowitz had been made to assign probabilities to their opposing expectations regarding post-war Iraq. Not only would they have had to work harder to justify their views, they might have seen more clearly the substantial chance that they were wrong and had to make greater efforts in their planning to prepare for that contingency. Secondly, the very process of making the relevant factors of a decision explicit provides a firm, or at least transparent, basis for making choices. Alternative courses of action can be compared and assessed in like terms. Third, the transparency and discipline of the process of arriving at the initial strategy should heighten the decision-maker’s sensitivity toward changes in the environment that would suggest the need for adjustments to that strategy. In this way, prediction enhances rather than under-mines strategic flexibility. This defence of prediction does not imply that great stakes should be gambled on narrow, singular predictions of the future. On the contrary, the central problem of uncertainty in plan- ning remains that any given prediction may simply be wrong. Preparations for those eventualities must be made. Indeed, in many cases, relatively unlikely outcomes could be enormously consequential, and therefore merit extensive preparation and investment. In order to navigate this complexity, strategists must return to the dis- tinction between uncertainty and risk. While the complexity of the international security environment may make it somewhat resistant to the type of probabilistic thinking associated with risk, a risk-oriented approach seems to be the only viable model for national-security strategic planning. The alternative approach, which categorically denies prediction, precludes strategy. As Betts argues, Any assumption that some knowledge, whether intuitive or explicitly formalized, provides guidance about what should be done is a presumption that there is reason to believe the choice will produce a satisfactory outcome – that is, it is a prediction, however rough it may be. If there is no hope of discerning and manipulating causes to produce intended effects, analysts as well as politicians and generals should all quit and go fishing.36 Unless they are willing to quit and go fishing, then, strategists must sharpen their tools of risk assessment. Risk assessment comes in many varieties, but identification of two key parameters is common to all of them: the consequences of a harmful event or condition; and the likelihood of that harmful event or condition occurring. With no perspective on likelihood, a strategist can have no firm perspective on risk. With no firm perspective on risk, strategists cannot purposefully discriminate among alternative choices. Without purposeful choice, there is no strategy. \* \* \* One of the most widely read books in recent years on the complicated relation- ship between strategy and uncertainty is Peter Schwartz’s work on scenario-based planning, The Art of the Long View. Schwartz warns against the hazards faced by leaders who have deterministic habits of mind, or who deny the difficult implications of uncertainty for strategic planning. To overcome such tenden- cies, he advocates the use of alternative future scenarios for the purposes of examining alternative strategies. His view of scenarios is that their goal is not to predict the future, but to sensitise leaders to the highly contingent nature of their decision-making.37 This philosophy has taken root in the strategic-planning processes in the Pentagon and other parts of the US government, and properly so. Examination of alternative futures and the potential effects of surprise on current plans is essential. Appreciation of uncertainty also has a number of organisational impli- cations, many of which the national-security establishment is trying to take to heart, such as encouraging multidisciplinary study and training, enhancing information sharing, rewarding innovation, and placing a premium on speed and versatility. The arguments advanced here seek to take nothing away from these imperatives of planning and operating in an uncertain environment. But appreciation of uncertainty carries hazards of its own. Questioning assumptions is critical, but assumptions must be made in the end. Clausewitz’s ‘standard of judgment’ for discriminating among alternatives must be applied. Creative, unbounded speculation must resolve to choice or else there will be no strategy. Recent history suggests that unchecked scepticism regarding the validity of prediction can marginalise analysis, trade significant cost for ambig- uous benefit, empower parochial interests in decision-making, and undermine flexibility. Accordingly, having fully recognised the need to broaden their strategic-planning aperture, national-security policymakers would do well now to reinvigorate their efforts in the messy but indispensable business of predicting the future.

Scenario planning is vital to create appropriate risk assessments—policymakers have an obligation to engage in these predictions

Kurasawa, 04 (Professor of Sociology, York University of Toronto, Fuyuki, Constellations Volume 11, No 4, 2004)

A radically postmodern line of thinking, for instance, would lead us to believe that it is pointless, perhaps even harmful, to strive for farsightedness in light of the aforementioned crisis of conventional paradigms of historical analysis. If, contra teleological models, history has no intrinsic meaning, direction, or endpoint to be discovered through human reason, and if, contra scientistic futurism, prospective trends cannot be predicted without error, then the abyss of chronological inscrutability supposedly opens up at our feet. The future appears to be unknowable, an outcome of chance. Therefore, rather than embarking upon grandiose speculation about what may occur, we should adopt a pragmatism that abandons itself to the twists and turns of history; let us be content to formulate ad hoc responses to emergencies as they arise. While this argument has the merit of underscoring the fallibilistic nature of all predictive schemes, it conflates the necessary recognition of the contingency of history with unwarranted assertions about the latter’s total opacity and indeterminacy. Acknowledging the fact that the future cannot be known with absolute certainty does not imply abandoning the task of trying to understand what is brewing on the horizon and to prepare for crises already coming into their own. In fact, the incorporation of the principle of fallibility into the work of prevention means that we must be ever more vigilant for warning signs of disaster and for responses that provoke unintended or unexpected consequences (a point to which I will return in the final section of this paper). In addition, from a normative point of view, the acceptance of historical contingency and of the self-limiting character of farsightedness places the duty of preventing catastrophe squarely on the shoulders of present generations. The future no longer appears to be a metaphysical creature of destiny or of the cunning of reason, nor can it be sloughed off to pure randomness. It becomes, instead, a result of human action shaped by decisions in the present – including, of course, trying to anticipate and prepare for possible and avoidable sources of harm to our successors. Combining a sense of analytical contingency toward the future and ethical responsibility for it, the idea of early warning is making its way into preventive action on the global stage.

Nuclear weapons are a massive alt cause the aff – they don’t solve that – so it makes their impacts inevitable – but not ours cuz our DAs are about pre-emptive OCOs

**No impact to the aff – war powers-specific**

Eric A. Posner and Adrian Vermeule 3, Law Professors at Chicago and Harvard, Accommodating Emergencies, September, <http://www.law.uchicago.edu/files/files/48.eap-av.emergency.pdf>

Against the view that panicked government officials overreact to an emergency, and unnecessarily curtail civil liberties, we suggest a more constructive theory of the role of fear. Before the emergency, government officials are complacent. They do not think clearly or vigorously about the potential threats faced by the nation. After the terrorist attack or military intervention, their complacency is replaced by fear. Fear stimulates them to action. Action may be based on good decisions or bad: fear might cause officials to exaggerate future threats, but it also might arouse them to threats that they would otherwise not perceive. **It is impossible to say in the abstract whether decisions and actions provoked by fear are likely to be better than decisions and actions made in a state of calm**. But our limited point is that there is no reason to think that the fear-inspired decisions are likely to be worse. For that reason, the existence of fear during emergencies does not support the antiaccommodation theory that the Constitution should be enforced as strictly during emergencies as during non-emergencies.¶ C. The Influence of Fear during Emergencies ¶ Suppose now that the simple view of fear is correct, and that it is an unambiguously negative influence on government decisionmaking. Critics of accommodation argue that this negative influence of fear justifies skepticism about emergency policies and strict enforcement of the Constitution. However, this argument is implausible. It is doubtful that fear, so understood, has more influence on decisionmaking during emergencies than decisionmaking during non-emergencies.¶ The panic thesis, implicit in much scholarship though rarely discussed in detail, holds that citizens and officials respond to terrorism and war in the same way that an individual in the jungle responds to a tiger or snake. The national response to emergency, because it is a standard fear response, is characterized by the same circumvention of ordinary deliberative processes: thus, (i) the response is instinctive rather than reasoned, and thus subject to error; and (ii) the error will be biased in the direction of overreaction. While the flight reaction was a good evolutionary strategy on the savannah, in a complex modern society the flight response is not suitable and can only interfere with judgment. Its advantage—speed—has minimal value for social decisionmaking. No national emergency requires an immediate reaction—except by trained professionals who execute policies established earlier—but instead over days, months, or years people make complex judgments about the appropriate institutional response. And the asymmetrical nature of fear guarantees that people will, during a national emergency, overweight the threat and underweight other things that people value, such as civil liberties. ¶ But if decisionmakers rarely act immediately, then the tiger story cannot bear the metaphoric weight that is placed on it. Indeed, the flight response has nothing to do with the political response to the bombing of Pearl Harbor or the attack on September 11. The people who were there—the citizens and soldiers beneath the bombs, the office workers in the World Trade Center—no doubt felt fear, and most of them probably responded in the classic way. They experienced the standard physiological effects, and (with the exception of trained soldiers and security officials) fled without stopping to think. It is also true that in the days and weeks after the attacks, many people felt fear, although not the sort that produces a irresistible urge to flee. **But this kind of fear is not the kind in which cognition shuts down**. (Some people did have more severe mental reactions and, for example, shut themselves in their houses, but these reactions were rare.) The fear is probably better described as a general anxiety or jumpiness, an anxiety that was probably shared by government officials as well as ordinary citizens.53¶ While, as we have noted, there is psychological research suggesting that normal cognition partly shuts down in response to an immediate threat, we are aware of no research suggesting that people who feel anxious about a non-immediate threat are incapable of thinking, or thinking properly, or systematically overweight the threat relative to other values. Indeed, it would be surprising to find research that clearly distinguished “anxious thinking” and “calm thinking,” given that anxiety is a pervasive aspect of life. People are anxious about their children; about their health; about their job prospects; about their vacation arrangements; about walking home at night. No one argues that people’s anxiety about their health causes them to take too many precautions—to get too much exercise, to diet too aggressively, to go to the doctor too frequently—and to undervalue other things like leisure. So it is hard to see why anxiety about more remote threats, from terrorists or unfriendly countries with nuclear weapons, should cause the public, or elected officials, to place more emphasis on security than is justified, and to sacrifice civil liberties.¶ Fear generated by immediate threats, then, causes instinctive responses that are not rational in the cognitive sense, not always desirable, and not a good basis for public policy, but it is not this kind of fear that leads to restrictions of civil liberties during wartime. The internment of Japanese Americans during World War II may have been due to racial animus, or to a mistaken assessment of the risks; it was not the direct result of panic; indeed there was a delay of weeks before the policy was seriously considered.54 Post-9/11 curtailments of civil liberties, aside from immediate detentions, came after a significant delay and much deliberation. The civil libertarians’ argument that fear produces bad policy trades on the ambiguity of the word “panic,” which refers both to real fear that undermines rationality, and to collectively harmful outcomes that are driven by rational decisions, such as a bank run, where it is rational for all depositors to withdraw funds if they believe that enough other depositors are withdrawing funds. Once we eliminate the false concern about fear, it becomes clear that the panic thesis is indistinguishable from the argument that during an emergency people are likely to make mistakes. But if the only concern is that during emergencies people make mistakes, there would be no reason for demanding that the constitution be enforced normally during emergencies. Political errors occur during emergencies and nonemergencies, but the stakes are higher during emergencies, and that is the conventional reason why constitutional constraints should be relaxed.

#### Security is self-reflexive – solves the impact

**Roe, 12** (Paul Roe, Associate Professor in the Department of International Relations and European Studies at Central European University, Budapest, “Is securitization a ‘negative’ concept? Revisiting the normative debate over normal versus extraordinary politics,” Security Dialogue vol. 43 no. 3, June 2012)

For the Copenhagen School, securitization represents a panic politics: we must do something now, as our very survival is at stake. In such a scenario, it is hardly surprising that Aradau and Huysmans both see the possibilities for debate and deliberation as being minimal: normal procedures must be circumvented, otherwise it might all be too late. The speed of decisionmaking and the accompanying silence on the part of those outside the relevant elite are made all the more salient by the so-called internalist (Stritzel, 2007) or philosophical (Balzacq, 2011) view of securitization, whereby the security speech act possesses its own performative power. The internalist reading is characteristic of Wæver’s (1995) earlier work on securitization and accords with the notion of performativity. Performativity corresponds to John L. Austin’s illocutionary act. Here, uttering security is more than just describing something: it is performing an action that creates new realities (Balzacq, 2005: 177, 2011: 20; Stritzel, 2007: 361). The security speech act thus has the power to enable emergency measures and to (re)order sociopolitical relations (friend/enemy, us/them). In other words, security is a self-referential practice. The internalist reading of securitization closely resembles the Schmittian conception of the political inasmuch as both are decisionist: the securitizing actor, like Schmitt’s sovereign, defines what is exceptional. The silence that arguably marks the internalist reading therefore reflects the lack of oversight to which the securitizing actor is subject, while, with regard to speed, there is a distinct sense of automaticity in the moment when a political issue is rapidly transformed into a matter of security by virtue of its very utterance as such. This is problematized, however, by the so-called externalist (Stritzel, 2007) or sociological (Balzacq, 2011**) view, which emphasizes instead the intersubjectivity of the securitization process.** With the externalist reading, the authority to speak and the power of the speech act itself are subject to the context in which security is uttered. Most importantly, **the framing of something as a security issue is not the sole preserve of the securitizing actor but must also be accepted by a relevant audience**. As Buzan et al. (1998: 25) make clear, presenting something as an existential threat is merely a ‘securitizing move’, as ‘the issue is [successfully] **securitized only if and when the audience accepts it as such’**. Accordingly, with its emphasis on the intersubjective establishment of threat, **the externalist rendering of securitization makes problematic Wæver’s earlier assertion of security as a self-referential practice**. And this conceptual tension is reflected in the specific debate over the nature of the speech act itself. For both Thierry Balzacq and Holger Stritzel, Wæver/the Copenhagen School thus present securitization as both an illocutionary act and a perlocutionary act – that is, they discuss what is done in saying security, as well as what is done by saying security. Perlocutionary acts are external to the performative aspect of the speech act and thereby correspond not to the utterance itself but to its effects: did the securitizing actor manage to convince the relevant audience. Balzacq (2005: 177–8) sums up the situation thus: either we argue that securitization is a self-referential practice, in which case we forsake perlocution with the related acquiescence of the audience … or we hold fast to the creed that using the conception of security also produces a perlocutionary effect, in which case we abandon self-referentiality. He goes on: I suspect instead that the CS [Copenhagen School] leans towards the first option…. [A]lthough the CS appeals to an audience, its framework ignores the audience, which suggests that the CS opts for an illocutionary view of security yielding a ‘magical efficiency’ rather than a fully-fledged model encompassing perlocution as well (Balzacq, 2005: 177–8).9 It is indeed the case that the Copenhagen School has underconceptualized the role of the audience.10 This is something of which Wæver (2003) himself is well aware. But, it is debatable whether the Copenhagen School favours an internalist reading of the securitization concept. Although Wæver is keen to stress the importance of the ‘moment’ of the speech act, and thus retain its illocutionary force, he nevertheless also leans towards the importance of the relationship between securitizing actor and audience. Wæver warns of viewing securitization as a ‘unilateral performance’ – that undertaken only by the sovereign – and thus its equivalence to a ‘Schmittian anti-democratic decisionism’. Rather: We [members of the Copenhagen School] preserve the event-ness of the speech act and the performative moment, but locate it in-between the actors…. This might look like perlocution because it includes something after the speaker’s first action, but if the speech act is viewed as a larger whole including audience, it is more appropriate to see securitization as what is done in the (collective) act, rather than dissolving the move into one component of a larger complex social explanation of processes (Wæver, 2007: 4). The important point here is how the security speech act moves away from a Schmittian to an Arendtian conception of politics, ‘because the theory places power in-between humans … and insists on securityness being a quality not of threats but of their handling, that is, the theory places power not with “things” external to a community but internal to it’ (Wæver, 2011: 468). For Wæver, securitization thus **takes place in a context where there is space for open politics**: actors and audiences together agree as to what constitutes security and what does not. This is not to say that agreement is necessarily reached on an equal basis, as actors often possess, and indeed employ, the resources to cajole and bully audiences into acquiescing to their depiction of events. But, it is to say that some kind of agreement is nevertheless required. Indeed, the potential for securitization to avoid its Schmittian connotations in this way is also recognized by Williams. For Williams, the importance of the audience relates to a ‘discursive ethics’ that goes against the decisionist account of securitization. **The security speech act entails the possibility of dialogue and thereby also the potential for the transformation of security** (Williams, 2003: 522–3). And although Williams (2003: 524) seems somewhat sceptical as to the extent to which securitizations are subject to such ‘discursive legitimation’ – also noting how security issues often ‘operate in the realm of secrecy, of “national security”, of decision’ – he nonetheless makes clear the potential for securitizations to be ‘pulled back’ into the public realm, ‘particularly when the social consensus underlying the capacity for decision is challenged, either by questioning the policies, or by disputing the threat, or both’.

Resentment is wrong – there is no opposition between arguing for pragmatic change in the world and affirming life in a Nietzschean sense – their refusal of change and reform is self-delusion that withdraws from the world and denies an important aspect of life

May 05 (Todd, Professor of Philosophy at Clemson University, September 2005, “To change the world, to celebrate life,” Philosophy & Social Criticism, Vol. 31, No. 5-6)

For those among us who seek in philosophy a way to grapple with our lives rather than to solve logical puzzles; for those whose reading and whose writing are not merely appropriate steps toward academic advancement but a struggle to see ourselves and our world in a fresher, clearer light; for those who find nourishment among impassioned ideas and go hungry among empty truths: there is a struggle that is often waged within us. It is a struggle that will be familiar to anyone who has heard in Foucault’s sentences the stammering of a fellow human being struggling to speak in words worth hearing. Why else would we read Foucault? We seek to conceive what is wrong in the world, to grasp it in a way that offers us the possibility for change. We know that there is much that is, to use Foucault’s word, ‘intolerable’. There is much that binds us to social and political arrangements that are oppressive, domineering, patronizing, and exploitative. We would like to understand why this is and how it happens, in order that we may prevent its continuance. In short, we want our theories to be tools for changing the world, for offering it a new face, or at least a new expression. There is struggle in this, struggle against ideas and ways of thinking that present themselves to us as inescapable. We know this struggle from Foucault’s writings. It is not clear that he ever wrote about anything else. But this is not the struggle I want to address here. For there is, on the other hand, another search and another goal. They lie not so much in the revisioning of this world as in the embrace of it. There is much to be celebrated in the lives we lead, or in those led by others, or in the unfolding of the world as it is, a world resonant with the rhythms of our voices and our movements. We would like to understand this, too, to grasp in thought the elusive beauty of our world. There is, after all, no other world, except, as Nietzsche taught, for those who would have created another one with which to denigrate our own. In short, we would like our thought to celebrate our lives. To change the world and to celebrate life. This, as the theologian Harvey Cox saw, is the struggle within us.1 It is a struggle in which one cannot choose sides; or better, a struggle in which one must choose both sides. The abandonment of one for the sake of the other can lead only to disaster or callousness. Forsaking the celebration of life for the sake of changing the world is the path of the sad revolutionary. In his preface to Anti-Oedipus, Foucault writes that one does not have to be sad in order to be revolutionary. The matter is more urgent than that, however. One cannot be both sad and revolutionary. Lacking a sense of the wondrous that is already here, among us, one who is bent upon changing the world can only become solemn or bitter. He or she is focused only on the future; the present is what is to be overcome. The vision of what is not but must come to be overwhelms all else, and the point of change itself becomes lost. The history of the left in the 20th century offers numerous examples of this, and the disaster that attends to it should be evident to all of us by now. The alternative is surely not to shift one’s allegiance to the pure celebration of life, although there are many who have chosen this path. It is at best blindness not to see the misery that envelops so many of our fellow humans, to say nothing of what happens to sentient nonhuman creatures. The attempt to jettison world-changing for an uncritical assent to the world as it is requires a self-deception that I assume would be anathema for those of us who have studied Foucault. Indeed, it is anathema for all of us who awaken each day to an America whose expansive boldness is matched only by an equally expansive disregard for those we place in harm’s way. This is the struggle, then. The one between the desire for life-celebration and the desire for world-changing. The struggle between reveling in the contingent and fragile joys that constitute our world and wresting it from its intolerability. I am sure it is a struggle that is not foreign to anyone who is reading this. I am sure as well that the stakes for choosing one side over another that I have recalled here are obvious to everyone. The question then becomes one of how to choose both sides at once.

Global extinction risks require rereading resentiment – extinction outweighs

**Winchester 94** (James J. Winchester teaches Philosophy at Spelman College, “Nietzsche's Aesthetic Turn”)

As uninformed as it is to assume that there is an easy connection between his thought and National Socialism, it is neither difficult nor misguided to consider his lack of social concern. Nietzsche saw one danger in our century, but failed to see a second. His critique of herd mentality reads like a prophetic warning against the dictatorships that have plagued and continue to haunt the twentieth century. **But the context of our world has changed in ways that Nietzsche never imagined. We now have, as never before, the ability to destroy the planet.** The threat of the destruction of a society is not new. From the beginnings of Western literature in the Iliad and the Odyssey, the Western mind has contemplated the destruction that, for example, warfare has wrought. Although the Trojan war destroyed almost everyone involved, both the victors and the vanquished, it did not destroy the entire world. **In the twentieth century, what has changed is the scale of destruction**. If a few countries destroy the ozone layer, the whole world perishes, or if two countries fight a nuclear or biological war, the whole planet is threatened. This is something new in the history of the world. The interconnectedness of the entire world has grown dramatically. We live, as never before, in a global community where our actions affect ever-larger numbers of the world's population. The earth's limits have become more apparent. Our survival depends on working together to solve problems like global pollution. Granted mass movements have instituted reigns of tenor, but **our survival as a planet is becoming ever-more predicated on community efforts of the sort that Nietzsche's thought seems to** denigrate if not **preclude**. I do not criticize Nietzsche for failing to predict the rise of problems requiring communal efforts such as the disintegration of the ozone layer, acid rain, and the destruction of South American rain forests. Noting his lack of foresight and his occasional extremism, I propose, in a Nietzschean spirit, to reconsider his particular tastes, without abandoning his aesthetic turn. Statements like "common good is a self-contradiction" are extreme, even for Nietzsche. He was not always so radical. Yet there is little room in Nietzsche's egoism for the kind of cooperation and sense of community that is today so important for our survival. I am suggesting that the time for Nietzsche's radical individualism is past. There are compelling pragmatic and aesthetic reasons why we should now be more open to the positive possibilities of living in a community. There is nothing new about society's need to work together. What has changed is the level of interconnectedness that the technological age has pressed upon us.

Prefer util – consequences matter

Isaac 02 (Jeffrey C., James H. Rudy professor of Political Science and director of the Center for the Study of Democracy and Public Life at Indiana University, Bloomington, “Ends, Means and politics,” *Dissent*, Spring)

As writers such as Niccolo Machiavelli,Max Weber, Reinhold Niebuhr, and HannahArendt have taught, an unyielding concern with moral goodness undercuts political responsibility.The concern may be morally laudable, reflectinga kind of personal integrity, but it suffersfrom three fatal flaws: (1) It fails to see that the purity of one’s intention does not ensure the achievement of what one intends. Abjuring violence or refusing to make commoncause with morally compromised parties may seem like the right thing; but if such tactics entail impotence, then it is hard to view them as serving any moral good beyond the clean conscience of their supporters; (2) it fails to see that in a world of real violence and injustice, moral purity is not simply a form of powerlessness; it is often a form of complicity in injustice. This is why, from the standpoint of politics—as opposed to religion—pacifism is alwaysa potentially immoral stand. In categorically repudiatingviolence, it refuses in principle tooppose certain violent injustices with any effect;and (3) it fails to see that politics is as much about unintended consequences as it is about intentions; it is the effects of action, rather than the motives of action, that is most significant. Just as the alignment with “good”may engender impotence, it is often the pursuit of “good” that generates evil. This is thelesson of communism in the twentieth century:it is not enough that one’s goals be sincere oridealistic; it is equally important, always, to askabout the effects of pursuing these goals andto judge these effects in pragmatic and historicallycontextualized ways. Moral absolutism inhibits this judgment. It alienates those who are not true believers. It promotes arrogance. And it undermines political effectiveness.

#### K’s of util are wrong

Shaw 99 (William H, Professor of Philosophy @ San Jose State, Contemporary Ethics, p.185-186)

One of the most widespread criticisms of utilitarianism is that it cannot take rights seriously enough. Generally speaking, rights take precedence over considerations of immediate utility. They limit or restrict direct appeals to welfare maximization. For example, to have a right to free speech means that one is free to speak one's mind even if doing so will fail to maximize happiness because others will dislike hearing what one has to say. The right not to be compelled to incriminate oneself entails that it would be wrong to force a criminal defendant to testify against himself even if the results of doing so would be good. If rights are moral claims that trump straightforward appeals to utility," then utilitarianism, the critics argue, cannot meaningfully respect rights because their theory subordinates them to the promotion of welfare. However, the criticism that utilitarianism cannot do right by rights ignores the extent to which utilitarianism can, as discussed in Chapter 5, accommodate the moral rules, principles, and norms other than welfare maximization that appear to constitute the warp and woof of our moral lives. To be sure, utilitarians look at rights in a different light than do . moral theorists who see them as self-evident or as having an independent deontic status grounded on non-utilitarian considerations. For utilitarians, it is not rights, but the promotion of welfare, that lies at the heart of morality. Bentham was consistently hostile to the idea of natural rights, in large measure because he believed that invoking natural rights was only a way of dressing up appeals to intuition in fancy rhetoric. In a similar vein, many utilitarians today believe that in both popular and philosophical discourse people are too quick to declare themselves possessors of all sorts of putative rights and that all too frequently these competing claims of rights only obscure the important, underlying moral issues.

**Their impacts are overdetermined non-sense – democracy and economic liberalization checks their impacts**

**O’Kane 97  (“Modernity, the Holocaust, and politics”, Economy and Society, February, ebsco)**

Chosen policies cannot be relegated to the position of immediate condition (Nazis in power) in the explanation of the Holocaust.  Modern bureaucracy is not ‘intrinsically capable of genocidal action’ (Bauman 1989: 106).  Centralized state coercion has no natural move to terror.  In the explanation of modern genocides it is chosen policies which play the greatest part, whether in effecting bureaucratic secrecy, organizing forced labour, implementing a system of terror, harnessing science and technology or introducing extermination policies, as means and as ends. As Nazi Germany and Stalin’s USSR have shown, furthermore, those chosen policies of genocidal government turned away from and not towards modernity.  The choosing of policies,however, is not independent of circumstances.  An analysis of the history of each case plays an important part in explaining where and how genocidal governments come to power and analysis of political institutions and structures also helps towards an understanding of the factors which act as obstacles to modern genocide.  But it is not just political factors which stand in the way of another Holocaust in modern society.  Modern societies have not only pluralist democratic political systems but also economic pluralism where workers are free to change jobs and bargain wages and where independent firms, each with their own independent bureaucracies, exist in competition with state-controlled enterprises.  In modern societies this economic pluralism both promotes and is served by the open scientific method.  By ignoring competition and the capacity for people to move between organizations whether economic, political, scientific or social, Bauman overlooks crucial but also very ‘ordinary and common’ attributes of truly modern societies.  It is these very ordinary and common attributes of modernity which stand in the way of modern genocides.

#### Their impacts are wrong

**Dickinson 04**, associate professor of history – UC Davis,

(Edward, Central European History, 37.1)

In short, the continuities between early twentieth-century biopolitical discourse and the practices of the welfare state in our own time are unmistakable. Both are instances of the “disciplinary society” and of biopolitical, regulatory, social-engineering modernity, and they share that genealogy with more authoritarian states, including the National Socialist state, but also fascist Italy, for example. And it is certainly fruitful to view them from this very broad perspective. **But that analysis can easily become superficial and misleading**, because it obfuscates the **profoundly different** strategic and local dynamics of power in the two kinds of regimes. Clearly the democratic welfare state is not only formally but also substantively **quite different from totalitarianism.** Above all, again, it has nowhere developed the fateful, radicalizing dynamic that characterized National Socialism (or for that matter Stalinism), the psychotic logic that leads from economistic population management to mass murder. Again, there is always the potential for such a discursive regime to generate coercive policies. In those cases in which the regime of rights does not successfully produce “health,” such a system can —and historically does— create compulsory programs to enforce it. But again, there are political and policy potentials and constraints in such a structuring of biopolitics that are very different from those of National Socialist Germany. Democratic biopolitical regimes require, enable, and incite a degree of self-direction and participation that is **functionally incompatible** with authoritarian or totalitarian structures. And this pursuit of biopolitical ends through a regime of democratic citizenship does appear, historically, to have imposed increasingly **narrow limits on coercive policies**, and to have generated a “logic” or imperative of increasing liberalization. Despite limitations imposed by political context and the slow pace of discursive change, I think this is the unmistakable message of the really very impressive waves of legislative and welfare reforms in the 1920s or the 1970s in Germany.90 Of course it is not yet clear whether this is an irreversible dynamic of such systems. Nevertheless, such regimes are characterized by sufficient degrees of autonomy (and of the potential for its expansion) for sufé cient numbers of people that I think it becomes useful to conceive of them as productive of a strategic coné guration of power relations that might fruitfully be analyzed as a condition of “liberty,” just as much as they are productive of constraint, oppression, or manipulation. At the very least, **totalitarianism cannot be the sole orientation point** for our understanding of biopolitics, the only end point of the logic of social engineering. **This notion is not at all at odds with the core of Foucauldian** (and Peukertian) **theory.** Democratic welfare states are regimes of power/knowledge no less than early twentieth-century totalitarian states; these systems are not “opposites,” in the sense that they are two alternative ways of organizing the same thing. But they are two very different ways of organizing it. The concept “power” should not be read as a universal stiè ing night of oppression, manipulation, and entrapment, in which all political and social orders are grey, are essentially or effectively “the same.” Power is a set of social relations, in which individuals and groups have varying degrees of autonomy and effective subjectivity. And discourse is, as Foucault argued, “tactically polyvalent.” Discursive elements (like the various elements of biopolitics) can be combined in different ways to form parts of quite different strategies (like totalitarianism or the democratic welfare state); they cannot be assigned to one place in a structure, but rather circulate. The varying possible constellations of power in modern societies create “multiple modernities,” modern societies with quite **radically differing potentials.**91

#### Cyberspace must be treated as much of a threat as other forms of war

ERIK M. MUDRINICH, ’12 (Major Erik M. Mudrinich (B.A., cum laude, St. Olaf College; J.D. Hamline University School of Law; L.L.M., University of Nebraska College of Law) is the Chief, Space and Operations Law, 14th Air Force, Vandenberg AFB, “CYBER 3.0: THE DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE AND THE ATTRIBUTION PROBLEM”, Air Force Law Review, 68 A.F. L. Rev. 167)

To begin an analysis of cyberspace, it is important to understand why labeling cyberspace a war-fighting domain is even necessary. Military strategists, policymakers, and innovators have long dealt with the challenges found in the tradi-tional domains of land, air, and sea. The many historical failures and successes in the traditional domains have shaped understanding and strategic vision; doctrine and technologies were then adjusted and developed accordingly. A new and complex domain has arisen--cyberspace. It "presents security challenges that are too novel and too serious for it to be treated as an add-on to our traditional operations on land, at sea, or in the air." n34¶ The importance of treating cyberspace as an operational domain cannot be overstated. The DOD recognizes cyber-space as a domain carried forward from the traditional domains for the purposes of organizing, training, and equipping its forces. Air Force Doctrine 3-12, Cyber Operations characterizes cyberspace as:¶ [\*174] [A] man-made domain, and is therefore unlike the natural domains of air, land, and maritime. It requires continued attention from humans to persist and encompass the features of specificity, global scope, and emphasis on the electromagnetic spectrum. Cyberspace nodes physically reside in all do-mains. Activities in cyberspace can enable freedom of action for activities in the other domains, and ac-tivities in the other domains can create effects in and through cyberspace. n35¶ By treating cyberspace as a war-fighting domain, it establishes the necessary organizational foundation to operate in a degraded cyber environment by setting the stage for DOD to ready its cyber forces accordingly. Cyber 3.0 recog-nizes that "degraded cyberspace operations for extended periods may be a reality and disruption may occur in the midst of a mission." n36 In the case of a contingency involving network failure or significant compromise, Cyber 3.0 requires the U.S. organize, train, and equip within the domain so that it is "able to remain operationally effective by isolating and neutralizing the impact, using redundant capacity, or shifting its operations from one system to another." n37

#### Cyber war is possible – cyber Attack means we lose control of nuclear weapons

Ejaz Haider, 5-7-’13 (News Editor of The Friday Times and Foreign Editor of Daily Times in Pakistan, “A cut-off point for nuclear weapons?”, International tribune)

Cyber-war is a reality. It means the keyboard and the internet. It means the issue of safety and security of nuclear weapons is not just about someone stealing a weapon or nuclear materials or even attacking a facility. Those possibilities are largely passé. The new threat is someone getting into the command and control systems. That’s the new game. I am not sure we — or any of the nuclear-weapon states — are prepared for that. Nothing can be foolproof. As someone said, for every proof there’s always a fool. There’s also the issue of technologies that can neutralise the adversary from the air, even from space.

#### Miscalc is likely – we’re key to solve it

Jari Rantapelkonen & Mirva Salminen, ’13 (“THE FOG OF CYBER DEFENCE”, National Defence University Department of Leadership and Military Pedagogy Publication Series 2 Article Collection n:o 10)

Today, cyber capabilities are essential for the nation states and the armed forces that wish to be treated as credible actors. Cyberspace, the fifth dimension of warfare, has already become an important arena of world politics – especially, since the times of war and peace have been blurred and become the grey area we are currently living in. The nature of cyberreality (the blurring of peace and war) adds a dangerous new dimension of instability: future conflicts may become vague, without a clear beginning and end. Sometimes the actor may not even be conscious of being in conflict with someone, when unpleasant tangible things "just happen" all the time or just every once in a while. The digital world has become a domain where strategic advantage can either be lost or won.

#### Eliminating Offensive Cyber operations risks destruction of the economy, national security and war

ERIK M. MUDRINICH, ’12 (Major Erik M. Mudrinich (B.A., cum laude, St. Olaf College; J.D. Hamline University School of Law; L.L.M., University of Nebraska College of Law) is the Chief, Space and Operations Law, 14th Air Force, Vandenberg AFB, “CYBER 3.0: THE DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE AND THE ATTRIBUTION PROBLEM”, Air Force Law Review, 68 A.F. L. Rev. 167)

¶ [T]he emergence of the Stuxnet worm is the type of risk that threatens to cause harm to many activities deemed critical to the basic functioning of modern society. The Stuxnet worm covertly attempts to iden-tify and exploit equipment that controls a nation's critical infrastructure. A successful attack by a soft-ware application such as the Stuxnet worm could result in manipulation of control system code to the point of inoperability or long-term damage . . . . The resulting damage to the nation's critical infrastruc-ture could threaten many aspects of life, including the government's ability to safeguard national security interests. n9¶ The advent of worms like Stuxnet has demonstrated that actors within the global digital environment possess the capability to "weaponize" software code. By doing this they can seize control of systems and disrupt their operations throughout the world, unconstrained by political and territorial borders. Nations, their militaries, and their economies are vulnerable to ever sophisticated cyber threats. Cyber threats manipulate, alter, degrade or destroy information systems. A cyber threat can manifest itself in many forms from an attack from a foreign nation to espionage to cyber crime and computer viruses. Malicious cyber activities pose a very real and immediate security threat to national security and commerce. Therefore, an appropriate strategic foundation to counter this emerging threat is needed.¶ In developing a strategy responsive to the threat, policymakers and military strategists alike have focused on the central characteristics of the growing cyber environment. U.S. Deputy Secretary of Defense William J. Lynn discussed the Pentagon's new strategy for securing cyberspace. n10 He noted that cyber warfare by design is akin to asymmetric warfare, even when prosecuted by superpowers. U.S. [\*170] policymakers have not adequately addressed this emerging threat environment and adapting a strategic vision to it should be made a top priority.¶ Crafting the ways and means to achieve the desired security end state, however, is complicated. In the asymmetric environment of cyberspace, there are no simple solutions and there are typically more questions than answers. The late Arthur Cebrowski, retired Admiral, U.S. Navy, and a pioneer in cyber analysis agreed with this assessment when he observed, "There is no technology, government policy, law, treaty or program that can stop the acceleration of competi-tion in cyberspace." n11 Low entry costs, evolving technological capabilities, and ease of attack make operation in the cyber domain a basic capability that can be easily achieved by adversaries. As noted by Deputy Secretary William J. Lynn, "Advances in technology have created a situation in which extremely robust capabilities can be developed at considerably low cost." n12¶ The danger and potency of the threat is exacerbated by the very nature of the system one wants to protect. For ex-ample, Internet architecture was designed to be open, collaborative, and rapidly expandable to support ease of use, in-novation, and continued growth. n13 These built-in dynamics of design allowed for a reliable and efficient means to connect disparate networks into a single global system, a "network of networks." In shaping the system, security and identity management considerations were, and continue to be, low priorities. n14 Confronted with an open architecture, net-work defenders must guard against all that is thrown against them while aggressors need only discover one breach in the digital armor for their attack to be successful. n15 It is an overwhelming task. It only takes a scant amount of coding for malware to be successful. n16 To defend against malware, anti-virus companies write millions of lines of code, and spend millions of dollars in research, to detect and counteract malicious script. Malware can be written in as little as twenty-five lines and the result can easily remain viable in the digital environment. n17 Another unique feature of cyber-space is that it defies traditional sovereign borders with relative ease. n18 Geographic and political boundaries are of little consequence. Skilled attackers can hold military or national security systems at risk, but their activities can [\*171] also threaten large portions of private sector networks, regardless of location. n19 The integration of U.S. military and civilian networks complicates defense efforts for U.S. military planners. U.S. Department of Defense (DOD) networks are largely reliant on networks outside of the .mil domain, to include national critical infrastructure. n20 As Professor Eric Talbot Jensen notes:¶ ¶ This near-complete intermixing of civilian and military computer infrastructures makes many of those civilian objects and providers legitimate targets under the law of armed conflict. The current integration of U.S. government assets with civilian systems makes segregation impossible and therefore creates a responsibility for the United States to protect those civilian networks, services, and communications. n21¶ Cyberspace is a domain where information is created, stored, modified, and exploited via interconnected networks. n22 Since it is relatively easy to seize the initiative and launch an attack against an information system, one can consider cyberspace an opportunistic and offense-dominant environment. In an offense-dominant cyber threat environment, a purely defensive or "bunker mentality" cannot keep pace. Static defenses can always be circumvented by ingenuity, tenacity, and technology--common virtues possessed by most skilled cyber operators. Deputy Secretary Lynn recog-nized this fact, stating, "A fortress mentality will not work . . . from a defense point of view it is difficult to protect eve-ry portal. What is needed is a strategy to deny the benefit to the attackers who need only a single point of entry to dis-rupt our systems." n23 Securing the nation's critical infrastructure, its networks and servers, should be an essential consideration of an ef-fective cyber strategy. In order to respond to cyber threats, the DOD developed and announced its first strategy that pro-vides for operational flexibility and adaptability in cyberspace. Released on July 14, 2011, this cyber strategy is entitled "Department of Defense Strategy for Operating in Cyberspace" (hereinafter "Cyber 3.0"). n24 Its central focus is one of deterrence by denial. Cyber 3.0 proposes to make U.S. networks and critical infrastructure more robust, resilient, and redundant, thereby denying the benefit of [\*172] attack. The strategy aims to mitigate vulnerabilities and acknowledg-es the growing cyber threat environment: "The Department and nation have vulnerabilities in cyberspace. Our reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity--the security of the technologies that we use each day." n25¶ Cyber 3.0 proposes to employ five initiatives to secure cyberspace. n26 The first is noteworthy for its recognition of cyberspace as an emergent war-fighting domain. n27 As mankind has evolved using first land, then sea, air and space to conduct commerce and compete for resources, conflict has also developed in these domains. As the only man-made and largely privately owned domain, cyberspace is as critical to national security as the other more traditional domains. n28 The first initiative proposes that the military must now be able to defend, deter, and operate within this domain. The second initiative predictably relies on the military developing the ability to respond to cyber attacks as they occur and to employ active defenses before serious damage occurs. n29 The third initiative seeks to ensure that the nation's civilian critical infrastructure is secured and is also able to withstand attacks. n30 Collective defense and deterrence is the fourth initiative. Due to the global and interconnected nature of the Internet, U.S. global allies can offer real-time assistance in detecting, deterring, and responding to attacks. n31 Finally, the fifth initiative proposes to leverage the U.S. technological base, banking on the nation's "geek capital," to assist in the development of cyber defense technologies and training to defeat threats. n32¶ While the introductions of the Cyber 3.0 strategic initiatives are a welcome development, they are incomplete. The strategy's overarching thrust is denying the benefit of an attack rather than penalizing attackers. While Cyber 3.0 dis-cusses the role of the traditional instruments of power, it fails to address the DOD's own core competency--direct mili-tary action. Simply put, the cyber strategy fails to address the application and appropriate use of force in cyberspace.

#### Best studies prove economic collapse causes war

Royal 10 (Jedediah Royal, Director of Cooperative Threat Reduction at the U.S. Department of Defense, 2010, “Economic Integration, Economic Signaling and the Problem of Economic Crises,” in Economics of War and Peace: Economic, Legal and Political Perspectives, ed. Goldsmith and Brauer, p. 213-215)

Less intuitive is how periods of economic decline may increase the likelihood of external conflict. Political science literature has contributed a moderate degree of attention to the impact of economic decline and the security and defence behaviour of interdependent states. Research in this vein has been considered at systemic, dyadic and national levels. Several notable contributions follow. First, on the systemic level, Pollins (2008) advances Modclski and Thompson's (1996) work on leadership cycle theory, finding that rhythms in the global economy are associated with the rise and fall of a pre-eminent power and the often bloody transition from one pre-eminent leader to the next. As such, exogenous shocks such as economic crises could usher in a redistribution of relative power (see also Gilpin, 1981) that leads to uncertainty about power balances, increasing the risk of miscalculation (Fearon. 1995). Alternatively, even a relatively certain redistribution of power could lead to a permissive environment for conflict as a rising power may seek to challenge a declining power (Werner, 1999). Separately, Pollins (1996) also shows that global economic cycles combined with parallel leadership cycles impact the likelihood of conflict among major, medium and small powers, although he suggests that the causes and connections between global economic conditions and security conditions remain unknown. Second, on a dyadic level, Copeland's (1996. 2000) theory of trade expectations suggests that 'future expectation of trade' is a significant variable in understanding economic conditions and security behaviour of states. He argues that interdependent states are likely to gain pacific benefits from trade so long as they have an optimistic view of future trade relations. However, if the expectations of future trade decline, particularly for difficult to replace items such as energy resources, the likelihood for conflict increases, as states will be inclined to use force to gain access to those resources. Crises could potentially be the trigger for decreased trade expectations either on its own or because it triggers protectionist moves by interdependent states.4 Third, others have considered the link between economic decline and external armed conflict at a national level. Blomberg and Hess (2002) find a strong correlation between internal conflict and external conflict, particularly during periods of economic downturn. They write: The linkages between internal and external conflict and prosperity are strong and mutually reinforcing. Economic conflict tends to spawn internal conflict, which in turn returns the favour. Moreover, the presence of a recession tends to amplify the extent to which international and external conflicts self-reinforce each other. (Blomberg & Hess, 2002. p. 89) Economic decline has also been linked with an increase in the likelihood of terrorism (Blomberg. Hess. & Weerapana. 2004). which has the capacity to spill across borders and lead to external tensions. Furthermore, crises generally reduce the popularity of a sitting government. 'Diversionary theory' suggests that, when facing unpopularity arising from **economic decline**, sitting governments have increased incentives to fabricate external military conflicts to create a 'rally around the flag' effect. Wang (1990, DeRouen (1995). and Blomberg, Hess, and Thacker (2006) find supporting evidence showing that economic decline and use of force are at least indirectly correlated. Gelpi (1997), Miller (1999), and Kisangani and Pickering (2009) suggest that the tendency towards diversionary tactics are greater for democratic states than autocratic states, due to the fact that democratic leaders are generally more susceptible to being removed from office due to lack of domestic support. DeRouen (2000) has provided evidence showing that periods of weak economic performance in the United States, and thus weak Presidential popularity, are statistically linked to an increase in the use of force. In summary, recent economic scholarship positively correlates economic integration with an increase in the frequency of economic crises, whereas political science scholarship links economic decline with external conflict at systemic, dyadic and national levels.' This implied connection between integration, crises and armed conflict has not featured prominently in the economic-security debate and deserves more attention.

#### Cyberspace must be treated as much of a threat as other forms of war

ERIK M. MUDRINICH, ’12 (Major Erik M. Mudrinich (B.A., cum laude, St. Olaf College; J.D. Hamline University School of Law; L.L.M., University of Nebraska College of Law) is the Chief, Space and Operations Law, 14th Air Force, Vandenberg AFB, “CYBER 3.0: THE DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE AND THE ATTRIBUTION PROBLEM”, Air Force Law Review, 68 A.F. L. Rev. 167)

To begin an analysis of cyberspace, it is important to understand why labeling cyberspace a war-fighting domain is even necessary. Military strategists, policymakers, and innovators have long dealt with the challenges found in the tradi-tional domains of land, air, and sea. The many historical failures and successes in the traditional domains have shaped understanding and strategic vision; doctrine and technologies were then adjusted and developed accordingly. A new and complex domain has arisen--cyberspace. It "presents security challenges that are too novel and too serious for it to be treated as an add-on to our traditional operations on land, at sea, or in the air." n34¶ The importance of treating cyberspace as an operational domain cannot be overstated. The DOD recognizes cyber-space as a domain carried forward from the traditional domains for the purposes of organizing, training, and equipping its forces. Air Force Doctrine 3-12, Cyber Operations characterizes cyberspace as:¶ [\*174] [A] man-made domain, and is therefore unlike the natural domains of air, land, and maritime. It requires continued attention from humans to persist and encompass the features of specificity, global scope, and emphasis on the electromagnetic spectrum. Cyberspace nodes physically reside in all do-mains. Activities in cyberspace can enable freedom of action for activities in the other domains, and ac-tivities in the other domains can create effects in and through cyberspace. n35¶ By treating cyberspace as a war-fighting domain, it establishes the necessary organizational foundation to operate in a degraded cyber environment by setting the stage for DOD to ready its cyber forces accordingly. Cyber 3.0 recog-nizes that "degraded cyberspace operations for extended periods may be a reality and disruption may occur in the midst of a mission." n36 In the case of a contingency involving network failure or significant compromise, Cyber 3.0 requires the U.S. organize, train, and equip within the domain so that it is "able to remain operationally effective by isolating and neutralizing the impact, using redundant capacity, or shifting its operations from one system to another." n37

#### Cyber war is possible – cyber Attack means we lose control of nuclear weapons

Ejaz Haider, 5-7-’13 (News Editor of The Friday Times and Foreign Editor of Daily Times in Pakistan, “A cut-off point for nuclear weapons?”, International tribune)

Cyber-war is a reality. It means the keyboard and the internet. It means the issue of safety and security of nuclear weapons is not just about someone stealing a weapon or nuclear materials or even attacking a facility. Those possibilities are largely passé. The new threat is someone getting into the command and control systems. That’s the new game. I am not sure we — or any of the nuclear-weapon states — are prepared for that. Nothing can be foolproof. As someone said, for every proof there’s always a fool. There’s also the issue of technologies that can neutralise the adversary from the air, even from space.

#### Miscalc is likely – we’re key to solve it

Jari Rantapelkonen & Mirva Salminen, ’13 (“THE FOG OF CYBER DEFENCE”, National Defence University Department of Leadership and Military Pedagogy Publication Series 2 Article Collection n:o 10)

Today, cyber capabilities are essential for the nation states and the armed forces that wish to be treated as credible actors. Cyberspace, the fifth dimension of warfare, has already become an important arena of world politics – especially, since the times of war and peace have been blurred and become the grey area we are currently living in. The nature of cyberreality (the blurring of peace and war) adds a dangerous new dimension of instability: future conflicts may become vague, without a clear beginning and end. Sometimes the actor may not even be conscious of being in conflict with someone, when unpleasant tangible things "just happen" all the time or just every once in a while. The digital world has become a domain where strategic advantage can either be lost or won.

#### Offensive is key to defend Cyber-Space – not cyber defense strategy fails

Matthew D. Crosston, ’11 (director of the International Security and Intelligence Studies Program and chair of political science at Bellevue University, “World Gone Cyber MAD: How “Mutually Assured Debilitation” Is the Best Hope for Cyber Deterrence”, Strategic Studies Quar terly)

Clearly, the United States has the technical capability and the strategic aggressiveness to conduct such operations. It must now conceptualize an offensive mind-set to begin defending cyberspace. The problem to this point has been its relatively limited sphere of utilization—the Iraqi example was a case of open and explicit war aimed at a target that was actively and aggressively attacking American military personnel. Granted, this may not be as politically clean, but it can be dramatically more effective in limiting adversaries who are motivated to attack the United States or other countries across the virtual commons. Keep in mind that in the twenty-first century, cyberspace is no lesser space to guard. It is true news media will not be able to show body counts or bloody battlefields when a country is victim to a massive cyber attack, but the devastation and destruction of such an attack in many ways can be more comprehensive and far-reaching.

#### Defensive measures will inevitably be outpaced by offense

Matthew D. Crosston, ’11 (director of the International Security and Intelligence Studies Program and chair of political science at Bellevue University, “World Gone Cyber MAD: How “Mutually Assured Debilitation” Is the Best Hope for Cyber Deterrence”, Strategic Studies Quar terly)

One counterargument to this rejects that the cyber realm will remain inherently dominated by offensive capabilities. The most often praised defensive measures that are allegedly catching up to offensive threats (IPV-6 and gateway technologies) are unfortunately a bit of an overstatement, as the cyber arena is never static—whatever defensive countermeasures are developed, one can rest assured there will be answers to those mea- sures. And offensive answers so far have always outpaced the defensive “improvements.” There is nothing in the foreseeable future that seems to truly challenge this basic reality. The United States should indeed con- tinue to develop, improve, and refine its defensive technologies. But it should not be so naïve as to think it will ever be capable of developing a defensive deterrence that will continuously and routinely outwork and outmaneuver offensive threats. It simply does not seem that the structure of the cyber realm will allow this reality to emerge.

#### Clear demonstrations are necessary for deterrence- Cyberdefense fails

Robert Belk and Matthew Noyes, Advised by Professor Joseph Nye & Professor Monica Toft,, 3-20-12 (Robert is Naval aviator and Politico-Military Fellow, studying international and global affairs at the Harvard Kennedy School, Matthew is a senior associate with the cybersecurity practice at Good Harbor Consulting. , “On the Use of Offensive Cyber Capabilities, A Policy Analysis on Offensive US Cyber Policy”, Belfer Center)

Defense protects systems, directly increasing the cost to conduct a successful attack. Deterrence increases the cost should an attack succeed either through threatened retaliatory action or entanglement (passive deterrence). Given the valuable information stored in cyberspace and the high cost of defending this information, we agree with the analysis of retired General Cartwright32 that organizations which only defend and do not deter against cyber attacks are certain to be the victims of cyber attacks as long as they use information systems.¶ All deterrence is inherently achieved through creating a system where adversaries believe that a successful attack will imposes additional costs on them that exceed the benefits of an attack. This is generally achieved through threatening external action or entanglement, respectfully described as active and passive deterrence. Active deterrence is often achieved through threatened legal or law enforcement activity, but for actors beyond the reach of law, active deterrence is achieved through threatened military or other state action. As a part of this work we will be exploring what sorts of external cyber action could and should be employed to achieve an active deterrent effect while following, where applicable, the principles of the law of armed conflict such as military necessity, proportionality, and distinction. Active deterrence strategies are most credible when officially declared in policy along with a clear demonstration of capability, but any declared policy will have a norm setting effect in the international community. As such we explore what sorts of cyber deterrence policies, and use of offensive cyber action, that the U.S. should be willing to accept as a new norm for behavior in cyberspace.

#### Cyber defense leaves us weak

Kenneth Lieberthal and Peter W. Singer, 2-’12 (“Cybersecurity and U.S.-China Relations”, Brookings)

The one seeking to penetrate a computer network, at least at present, is at a great advantage relative to the defender. The Internet was designed to share information easily, not prevent its flow. Historically, an imbalance in favor of the offense increases the incentives to act maliciously and quickly, while it also lowers each side’s confidence in its ability to deter attack and defend itself effectively.