# 1AC

## Cyber Aff Coast

### Contention 1 – Preemption

#### Cyber Space is militarized – the US executive branch is engaged in a clandestine war against every other state

Gellman & Nakashima 8/30/13 (Barton, Pulitzer Prize-winning American journalist, blogger and bestselling author, Ellen, is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties. She previously served as a Southeast Asia correspondent for the paper. She wrote about the presidential candidacy of Al Gore and co-authored a biography of Gore, and has also covered federal agencies, Virginia state politics and local affairs. She joined the Post in 1995. “U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show”, <http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html>)

U.S. intelligence services carried out 231 offensive cyber-operations in 2011, the leading edge of a clandestine campaign that embraces the Internet as a theater of spying, sabotage and war, according to top-secret documents obtained by The Washington Post.

That disclosure, in a classified intelligence budget provided by NSA leaker Edward Snowden, provides new evidence that the Obama administration’s growing ranks of cyberwarriors infiltrate and disrupt foreign computer networks.

Additionally, under an extensive effort code-named GENIE, U.S. computer specialists break into foreign networks so that they can be put under surreptitious U.S. control. Budget documents say the $652 million project has placed “covert implants,” sophisticated malware transmitted from far away, in computers, routers and firewalls on tens of thousands of machines every year, with plans to expand those numbers into the millions.

The documents provided by Snowden and interviews with former U.S. officials describe a campaign of computer intrusions that is far broader and more aggressive than previously understood. The Obama administration treats all such cyber-operations as clandestine and declines to acknowledge them.

The scope and scale of offensive operations represent an evolution in policy, which in the past sought to preserve an international norm against acts of aggression in cyberspace, in part because U.S. economic and military power depend so heavily on computers.

“The policy debate has moved so that offensive options are more prominent now,” said former deputy defense secretary William J. Lynn III, who has not seen the budget document and was speaking generally. “I think there’s more of a case made now that offensive cyberoptions can be an important element in deterring certain adversaries.”

Of the 231 offensive operations conducted in 2011, the budget said, nearly three-quarters were against top-priority targets, which former officials say includes adversaries such as Iran, Russia, China and North Korea and activities such as nuclear proliferation. The document provided few other details about the operations.

#### This pre-emption is a direct result of congressional abdication of war powers – Stuxnet opened the floodgate, and PPD 20 prooves that the Presidents capabilities are being expanded without restraint – collapses bureaucratic restraint

Walker 8/2/13 (Richard, Pen Name for New York News Producer, American free Press, “OBAMA EXPANDS WAR POWERS; CAN UNLEASH CYBERWAR ANY TIME <http://americanfreepress.net/?p=11966#sthash.GqeI03l8.dpuf>)

The very moment United States President Barack Obama authorized the “dropping” of an electronic bomb on Iran’s nuclear industry he crossed a line into a new kind of warfare that could have global consequences today and far into the future. The weapon used against Iran was built with the cooperation of Israel and was named Stuxnet. It was a “worm” that infected the computers running Iran’s nuclear industry. German systems control expert, Ralph Langer, who told the world about Stuxnet, remarked Stuxnet represented a dangerous capability and that its code could be used by hackers and others. In other words, Obama had unleashed a weapon that could be re-engineered by anyone to attack computer networks controlling American infrastructure.

Perhaps the most significant aspect of the Stuxnet attack was it demonstrated how Obama had given to himself new powers to launch a cyberwar against any country without Congressional approval. Unlike conventional war in which soldiers are sent to the front and bombs are dropped from the skies, cyberweapons silently and stealthily attack information systems, as well as financial and power centers. We do not know how many times Obama has used his new Cyber Command unit to attack nations other than Iran.

Obama’s Presidential Policy Directive 20, known as PPD 20, which he signed in October 2012, was a stark example of a power grab to accord to him special powers to launch a cyber war at a moment of his choosing. The Guardian newspaper, which first revealed the existence of the directive, claimed it sought a larger target list for cyber attacks and contemplated the use of cyber weapons within the U.S. if the president gave the green light and only in an emergency. But what kind of emergency remains unclear, as does the list of nations he might target in the future.

#### Lack of bureaucracy makes nuclear war inevitable

Austin 8/6/13 (Director of Policy Innovation at the EastWest Institute, “Costs of American Cyber Superiority”<http://www.chinausfocus.com/peace-security/costs-of-american-cyber-superiority/>)

The United States is racing for the technological frontier in military and intelligence uses of cyber space. It is ahead of all others, and has mobilized massive non-military assets and private contractors in that effort. This constellation of private sector opportunity and deliberate government policy has been aptly labeled in recent months and years by so many credible observers (in The Economist, The Financial Times and the MIT Technology Review) as the cyber industrial complex.

The United States is now in the unusual situation where the head of a spy agency (NSA) also runs a major military unified command (Cyber Command). This is probably an unprecedented alignment of Praetorian political power in any major democracy in modern political history. This allocation of such political weight to one military commander is of course for the United States to decide and is a legitimate course of action. But it has consequences. The Snowden case hints at some of the blow-back effects now visible in public. But there are others, less visible.

The NSA Prism program exists because it is technologically possible and there have been no effective restraints on its international targeting. This lack of restraint is especially important because the command and control of strategic nuclear weapons is a potential target both of cyber espionage and offensive cyber operations. The argument here is not to suggest a similarity between the weapons themselves, but to identify correctly the very close relationship between cyber operations and nuclear weapons planning. Thus the lack of restraint in cyber weapons might arguably affect (destabilize) pre-existing agreements that constrain nuclear weapons deployment and possible use.

The cyber superiority of the United States, while legal and understandable, is now a cause of strategic instability between nuclear armed powers. This is similar to the situation that persisted with nuclear weapons themselves until 1969 when the USSR first proposed an end of the race for the technological frontier of potential planetary devastation. After achieving initial capability, the U.S. nuclear missile build up was not a rational military response to each step increase in Soviet military capability. It was a race for the technological frontier – by both sides – with insufficient recognition of the consequences. This conclusion was borne out by a remarkable Top Secret study commissioned in 1974 by the U.S. Secretary of Defense, Dr James Schlesinger. By the time it was completed and submitted in 1981, it assessed that the nuclear arms build-up by both sides was driven – not by a supposed tit for tat escalation in capability of deployed military systems – but rather by an unconstrained race for the technological limits of each side’s military potential and by its own military doctrinal preferences. The decisions of each side were not for the most part, according to this now declassified study, a **direct** response to particular systems that the other side was building.

In 1969, the USSR acted first to propose an end to the race for the technological frontier of nuclear weapons because it knew it was losing the contest and because it knew there was political sentiment in the United States and in its Allied countries that supported limitations on the unbridled nuclear fetish.

As we ponder the American cyber industrial complex of today, we see a similar constellation of opposition to its power emerging. This constellation includes not just the political rivals who see they are losing in cyber space (China and Russia), but nervous allies who see themselves as the likely biggest victims of the American race for cyber superiority, and loyal American military commanders who can see the risks and dangers of that quest.

It is time for the United States to take stock of the collateral damage that its quest for cyber military power, including its understandable quest for intelligence superiority over the terrorist enemy, has caused amongst its allies. The loss has not yet been seen at the high political level among allies, in spite of several pro forma requests for information from countries such as Germany. The loss of U.S. credibility has happened more at the popular level. Around the world, once loyal supporters of the United States in its war on terrorism had a reasonable expectation to be treated as faithful allies. They had the expectation, perhaps naïve, that privacy was a value the Americans shared with them. They did not expect to be subject to such a crude distinction (“you are all non-Americans now”). They did not want to know that their entire personal lives in cyber space are now recoverable – should someone so decide – by the running of a bit of software in the NSA. After the Prism revelations, so many of these foreign citizens with an internationalist persuasion and solidarity for the United States now feel a little betrayed.

Yet, in the long run, the most influential voice to end the American quest for cyber military superiority may come from its own armed forces. There are military figures in the United States who have had responsibility for nuclear weapons command and control systems and who, in private, counsel caution. They advocate the need to abandon the quest for cyber dominance and pursue a strategy of “mutual security” in cyber space – though that has yet to be defined. They cite military exercises where the Blue team gets little or no warning of Red team disruptive cyber attack on systems that might affect critical nuclear command and control or wider war mobilization functions. Strategic nuclear stability may be at risk because of uncertainty about innovations in cyber attack capability. This question is worth much more attention.

U.S. national security strategy in cyber space needs to be brought under stronger civilian oversight and subject to more rigorous public scrutiny. The focus on Chinese cyber espionage has totally preempted proper debate about American cyber military power. Most in the United States Congress have lined up to condemn Snowden. That is understandable. But where are the critical voices looking at the bigger picture of strategic instability in cyberspace that existed before Snowden and has now been aggravated because of him? The Russian and Chinese rejections of reasonable U.S. demands for Snowden’s extradition may be every bit as reasonable given their anxiety about unconstrained American cyber superiority.

#### Independently – Cyber attacks breaks down command and control – causes nuclear response. The bureaucratic decision to react without information is a result of situating offensive cyber ops with the president

Cimbala 11(Stephen J. Cimbala 2011. Professor of Political Science at Penn State. “Nuclear Crisis Management and “Cyberwar” Phishing for Trouble?” Strategic Studies Quarterly Spring 2011)

This section discusses how cyberwar might adversely affect nuclear crisis management. Readers are advised, however, that history is indeterminate.It might turn out that, in some fortuitous cases, the United States coulduse nuclear deterrence and cyberwar as joint multipliers toward a success-ful outcome in crisis or war. For example, in facing down an opponentwith a comparatively small or no nuclear arsenal and inferior conventionalstrike capabilities, the United States or another power could employ infor-mation warfare aggressively “up front” while forgoing explicit mention ofits available nuclear capability. Russia’s five-day war against Georgia inAugust 2008 involved obvious cyber attacks as well as land and air opera-tions, but no explicit nuclear threats. On the other hand, had Georgia al-ready been taken into membership by NATO prior to August 2008 or hadRusso-Georgian fighting spread into NATO member-state territory, thevisibility of Russia’s nuclear arsenal as a latent and potentially explicitthreat would have been much greater.Notwithstanding the preceding disclaimers, information warfare has the potential to attack or disrupt successful crisis management on each offour dimensions. First, it can muddy the signals being sent from one side to the other in a crisis. This can be done deliberately or inadvertently. Sup-pose one side plants a virus or worm in the other’s communications net-works.19 The virus or worm becomes activated during the crisis and destroys or alters information. The missing or altered information may make itmore difficult for the cyber victim to arrange a military attack. But de-stroyed or altered information may mislead either side into thinking that its signal has been correctly interpreted when it has not. Thus, side A mayintend to signal “resolve” instead of “yield” to its opponent on a particularissue. Side B, misperceiving a “yield” message, may decide to continue its aggression, meeting unexpected resistance and causing a much more dan-gerous situation to develop.Infowar can also destroy or disrupt communication channels necessary for successful crisis management. One way it can do this is to disrupt communication links between policymakers and military commanders during a period of high threat and severe time pressure. Two kinds of un-anticipated problems, from the standpoint of civil-military relations, arepossible under these conditions. First, political leaders may have pre-delegated limited authority for nuclear release or launch under restric-tive conditions; only when these few conditions obtain, according to the protocols of predelegation, would military commanders be authorized toemploy nuclear weapons distributed within their command. Clogged,destroyed, or disrupted communications could prevent top leaders from knowing that military commanders perceived a situation to be far more desperate, and thus permissive of nuclear initiative, than it really was.During the Cold War, for example, disrupted communications betweenthe US National Command Authority and ballistic missile submarines,once the latter came under attack, could have resulted in a joint decisionby submarine officers to launch in the absence of contrary instructions.Second, information warfare during a crisis will almost certainly in-crease the time pressure under which political leaders operate. It may dothis literally, or it may affect the perceived timelines within which thepolicymaking process can make its decisions. Once either side sees parts ofits command, control, and communications (C3) system being subvertedby phony information or extraneous cyber noise, its sense of panic at thepossible loss of military options will be enormous. In the case of US ColdWar nuclear war plans, for example, disruption of even portions of thestrategic C3 system could have prevented competent execution of parts ofthe SIOP (the strategic nuclear war plan). The SIOP depended upon finelyorchestrated time-on-target estimates and precise damage expectanciesagainst various classes of targets. Partially misinformed or disinformednetworks and communications centers would have led to redundant at-tacks against the same target sets and, quite possibly, unplanned attacks onfriendly military or civilian installations.A third potentially disruptive effect of infowar on nuclear crisis man-agement is that it may reduce the search for available alternatives to thefew and desperate. Policymakers searching for escapes from crisis denoue-ments need flexible options and creative problem solving. Victims of in-formation warfare may have a diminished ability to solve problems routinely,let alone creatively, once information networks are filled with flotsam andjetsam. Questions to operators will be poorly posed, and responses (ifavailable at all) will be driven toward the least common denominator ofpreviously programmed standard operating procedures. Retaliatory sys-tems that depend on launch-on-warning instead of survival after riding out an attack are especially vulnerable to reduced time cycles and restricted alternatives: A well-designed warning system cannot save commanders from misjudging the situation under the constraints of time and information imposed by a posture of launch on warning. Such a posture truncates the decision process too early for iterative estimates to converge on reality. Rapid reaction is inherently unstable because it cuts short the learning time needed to match perception with reality.20 The propensity to search for the first available alternative that meetsminimum satisfactory conditions of goal attainment is strong enough undernormal conditions in nonmilitary bureaucratic organizations.21 In civil-military command and control systems under the stress of nuclear crisis decision making, the first available alternative may quite literally be the last; or so policymakers and their military advisors may persuade them-selves. Accordingly, the bias toward prompt and adequate solutions is strong. During the Cuban missile crisis, a number of members of thepresidential advisory group continued to propound an air strike and inva-sion of Cuba during the entire 13 days of crisis deliberation. Had less timebeen available for debate and had President Kennedy not deliberatelystructured the discussion in a way that forced alternatives to the surface,the air strike and invasion might well have been the chosen alternative.22Fourth and finally on the issue of crisis management, infowar can cause flawed images of each side’s intentions and capabilities to be conveyed tothe other, with potentially disastrous results. Another example from theCuban crisis demonstrates the possible side effects of simple misunder-standing and noncommunication on US crisis management. At the mosttense period of the crisis, a U-2 reconnaissance aircraft got off course andstrayed into Soviet airspace. US and Soviet fighters scrambled, and a pos-sible Arctic confrontation of air forces loomed. Khrushchev later toldKennedy that Soviet air defenses might have interpreted the U-2 flight asa prestrike reconnaissance mission or as a bomber, calling for a compensa-tory response by Moscow.23 Fortunately Moscow chose to give the UnitedStates the benefit of the doubt in this instance and to permit US fightersto escort the wayward U-2 back to Alaska. Why this scheduled U-2 mis-sion was not scrubbed once the crisis began has never been fully revealed;the answer may be as simple as bureaucratic inertia compounded by noncommunication down the chain of command by policymakers who failed to appreciate the risk of “normal” reconnaissance under these extra-ordinary conditions.

#### CERTAIN CONGRESSIONAL Consultation is necessary – preemption is inevitable without congressional checks. Decreasing BUREAUCRATIC INERTIA in response to a cyber attack is the only way to avoid conflict.

Dycus 10 (Professor Vermont Law School, “Congress’s Role in Cyber Warfare”, 8/11/2010, <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>)

III. ALEGISLATIVE HAND ON THE CYBER WAR MOUSE Cyber warfare, as that term is used here, refers to conflicts that utilize cyber or electronic weapons either offensively or defensively, or both. Cyber weapons are currently employed offensively in kinetic warfare, for example, to suppress an enemy’s air defenses or disrupt its communications, or defensively to track enemy troop movements. These weapons might also be used offensively to disable an enemy’s cyber weaponry or defensively in response to an enemy attack, to prevent further aggression. The term “cybersecurity” might be understood to refer to defense against cyber attacks. “Cyber attack” suggests offensive use, but the label is inexact and might be misleading. A preemptive strike to ward off an imminent enemy attack is considered defensive. Digital espionage might be part of the preparation for an attack, or it might be perceived that way by the target, which might then be provoked to defend itself by responding with a preemptive attack, either cyber or kinetic. The important point here is that any use of cyber weapons, offensive or defensive, could have enormous consequences for the security and other interests of the United States. The effect of such use, actual or potential, matters more than the labels. And if the effect – on human life or property, for example, or diplomatic relations or compliance with the law of armed conflict – is substantial, Congress has a role to play in adopting policy for that use. Congress has not thus far adopted measures suited to the regulation of cyber warfare. The War Powers Resolution, for example, is concerned with sending U.S. troops into harm’s way, rather than with clicking a computer mouse to launch a cyber attack, although the strategic consequences might be similar. And the WPR’s relatively relaxed timetable for executive notice and legislative response is unrealistic for war on a digital battlefield. Similarly, if cyber warfare is regarded as an intelligence activity, the intelligence oversight measures just described cannot, for reasons already indicated, ensure that Congress will be able to play a meaningful role. In the words of the National Research Council study cited above, “Today’s policy and legal framework for guiding and regulating the use of cyberattack is ill-formed, undeveloped, and highly uncertain.”45 Our experience with nuclear weapons may point to needed reforms. Since the beginning of the Cold War, the United States has had a fairly clear nuclear policy (albeit one that deliberately includes an element of ambiguity) – one known generally to Congress, the American public, and potential enemies.46 Congress has approved or disapproved the purchase of the weapons and delivery systems. It has been briefed on the policy, and it has debated that policy vigorously.47 While Congress has not articulated U.S. nuclear policy in any coherent form, it has collaborated closely with the executive branch in the development and execution of that policy. Cyber weapons bear a striking resemblance to nuclear weapons in some important ways. An enemy’s cyber attack would, like a nuclear strike, probably come without a clear warning. There are as yet no reliable defenses against either a cyber attack or a nuclear attack. Collateral damage from a nuclear attack would almost certainly be very extensive and would linger for an extended period.48 The direct and indirect effects of a cyber attack, while different in kind and degree, still could be widespread and indiscriminate.49 In other ways, cyber weapons are critically different from their nuclear counterparts. For one thing, the time frame for response to a cyber attack might be much narrower. A nuclear weapon delivered by a land-based ICBM could take 30 minutes to reach its target. An electronic attack would arrive instantaneously, and leave no time to consult with or even inform anyone outside the executive branch before launching a counterstrike, if that were U.S. policy. What most distinguishes digital warfare, however, is the potential difficulty in identifying the source of a cyber attack. It is always possible, of course, that an enemy might covertly deliver a nuclear device to the U.S. homeland in a shipping container or a Cessna. But the apparent ease with which a cyber attack may be carried out without attribution could make it impossible to fight back at all. If an attacker made it appear that the source was an innocent neutral state or perhaps another enemy of the attacker, a misdirected U.S. response might provoke a wider conflict. The potential difficulty in tracking the source also makes a policy of deterrence based on a threat of retaliation far less credible. Given these characteristics of cyber warfare, and the continuing refinement of cyber weaponry, we approach a state of extreme strategic instability, with each nation on hair-trigger alert. The execution of an illconceived cyber war policy calling for a prompt response – or any response – to an attack or threatened attack could have disastrous, unanticipated consequences. It also might, depending on the circumstances, violate the law of armed conflict. Congress accordingly needs to work closely with the executive branch in the development of a policy for this new kind of conflict. Such a policy ought to reflect the distinctive technology and strategy of digital warfare, and it should be reviewed constantly as the technology evolves. Like other regulations dealing with dynamic subjects, this policy should include general approaches that reflect this nation’s broad strategic concerns and fundamental values. But the policy must also be crafted with enough flexibility to allow those charged with its execution to deal with future developments that cannot now be predicted. And it should set out a procedure for such adaptive use by identifying, for example, who must be consulted under what circumstances, and who will make the final critical decisions. It is at least theoretically possible that Congress could play an active, real-time role in the implementation of whatever cyber warfare policy is adopted. The policy might, for example, like the War Powers Resolution, require consultation “in every possible circumstance.”50 But it seems more likely that a digital war would begin and end before any notice could ever reach Capitol Hill. Congress therefore needs to lay down clear guidelines, with as much flexibility as prudence requires, for executive branch officials to follow if consultation is not reasonably possible. And Congress should require a prompt and full account of every significant use of cyber weapons.

### Contention 2 – Unipolarity

#### China is counterbalancing the US in cyber space – offensive weapon systems only make the problem worse

Hjortdal 11 ( Magnus Hjortdal is a 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, “China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence”, Journal of Strategic Security Volume IV Issue 2 2011, pp. 1-24)

In spite of the constraints above, an understanding of the importance of cyber warfare is found in the PLA's strategic thinking.92 This form of asymmetric strategy has been debated internally for a long time,93 and a book that attracted much attention, Unrestricted Warfare, written by two Chinese colonels, states that "[i]n the information age, the influence exerted by a nuclear bomb is perhaps less than the influence exerted by a hacker."94

Conclusion

The evidence in this article has contextualized the elements of cyber warfare capabilities. On the basis of three reasons put forward for states to maintain and utilize the cyber domain aggressively, an analysis was made of China's cyber warfare capabilities. The analysis has shown that China is likely to have conducted several cyber attacks in the past and present, and probably will continue with that strategy in the future, as this is of great importance for its economy, military, and deterrence of the United States.

Implications: China as Cyberpower and Superpower

In the foreword to the Australian Defense White Paper entitled Defending Australia in the Asia Pacific Century: Force 2030, on the country's future defense policy, the Australian defense minister, Joel Fitzgibbon, writes: "[C]yber warfare has emerged as a serious threat to critical infrastructure [and] the biggest changes to our outlook over the period have been the rise of China […] [T]he beginning of the end of the so-called unipolar moment; the almost two-decade-long period in which the pre-eminence of our principal ally, the United States, was without question."95

The unipolar moment during which the United States could ensure all its allies' security is undergoing change, and China's capabilities for cyber warfare are an important element in this change.

In order to meet this challenge, the United States has now launched a new "Cyber Command" and appointed a "Cyber Czar" to coordinate national preparedness.96 It should also not be forgotten that the United States is doing a lot on both defensive and offensive cyber network operations.97 In the dynamics of CNO, where it is far more difficult to defend than to attack,98 it will be extremely difficult for the United States to counter China's capabilities in this area. America will continue to give its cyber capabilities a high priority, but the cumulative deterrence effect may not be known until the future, if at all.99 But along with such efforts, the Chinese will also try to avoid a situation in which their deterrent capabilities become neutralized.

In sum, ascending states have much to gain from an offensive and aggressive cyber capability, primarily because of the fact that it is difficult to prove directly who is behind such attacks. Thus, there is a high probability that the Chinese build-up in the cyber area will continue. China's cyber deterrence capability in the longer term will make it possible for further Chinese expansion in the political-military area so that one day, China may become a de jure superpower across economic, technological, and military domains.

#### Offensive posture causes Chinese counterbalancing

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

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

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

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

#### Lack of legal norms make miscalculation and conflict inevitable

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

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

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

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

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

U.S. Experience with the LOAC

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

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

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

The Tallinn Manual and Emerging Cyber Norms

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

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

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

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

Cyber in China’s Recent Defense White Paper

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

Troubling Prospects for U.S.-Chinese Cyber Operations

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

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

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

#### Lack of LOAC makes Russia a dangerous challenger

Walker 8/2/13 (Richard, Pen Name for New York News Producer, American free Press, “OBAMA EXPANDS WAR POWERS; CAN UNLEASH CYBERWAR ANY TIME http://americanfreepress.net/?p=11966#sthash.GqeI03l8.dpuf)

An East European cyber war specialist, speaking on condition of anonymity to AMERICAN FREE PRESS, said he was unhappy with Obama’s refusal to work more closely with Russia on cyber threats. He pointed to the fact Obama abandoned a joint approach by U.S.–Russian experts, who issued a cyber-conflict report in 2011 under the auspices of the East-West Institute. It was the first joint effort of its kind designed to define the “rules of the road” for cyber conflict.

“Obama is more of as hawk in this field than people imagine. His cyber war policy has the potential for global consequences in which cyber wars will be launched by many nations and it will be impossible to identify the culprits. Russia wanted a cyber-partnership with America, but Obama wanted to go it alone with the exception of working with the Israelis on projects of mutual interest like Iran and now Syria. That should concern his allies as much as the American people,” he warned.

#### Russia counterbalancing causes nuclear conflict

Blank 9 (Dr. Stephen, Research Professor of National Security Affairs at the Strategic Studies Institute of the U.S. Army War College, March, “Russia And Arms Control: Are There Opportunities For The Obama Administration?,” <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub908.pdf>)

Proliferators or nuclear states like China and Russia can then deter regional or intercontinental attacks either by denial or by threat of retaliation.168 Given a multipolar world structure with little ideological rivalry among major powers, it is unlikely that they will go to war with each other. Rather, like Russia, they will strive for exclusive hegemony in their own “sphere of influence” and use nuclear instruments towards that end. However, wars may well break out between major powers and weaker “peripheral” states or between peripheral and semiperipheral states given their lack of domestic legitimacy, the absence of the means of crisis prevention, the visible absence of crisis management mechanisms, and their strategic calculation that asymmetric wars might give them the victory or respite they need.169 Simultaneously,¶ The states of periphery and semiperiphery have far more opportunities for political maneuvering. Since war remains a political option, these states may find it convenient to exercise their military power as a means for achieving political objectives. Thus international crises may increase in number. This has two important implications for the use of WMD. First, they may be used deliberately to offer a decisive victory (or in Russia’s case, to achieve “intra-war escalation control”—author170) to the striker, or for defensive purposes when imbalances in military capabilities are significant; and second, crises increase the possibilities of inadvertent or accidental wars involving WMD.171¶ Obviously nuclear proliferators or states that are expanding their nuclear arsenals like Russia can exercise a great influence upon world politics if they chose to defy the prevailing consensus and use their weapons not as defensive weapons, as has been commonly thought, but as offensive weapons to threaten other states and deter nuclear powers. Their decision to go either for cooperative security and strengthened international military-political norms of action, or for individual national “egotism” will critically affect world politics. For, as Roberts observes,¶ But if they drift away from those efforts [to bring about more cooperative security], the consequences could be profound. At the very least, the effective functioning of inherited mechanisms of world order, such as the special responsibility of the “great powers” in the management of the interstate system, especially problems of armed aggression, under the aegis of collective security, could be significantly impaired. Armed with the ability to defeat an intervention, or impose substantial costs in blood or money on an intervening force or the populaces of the nations marshaling that force, the newly empowered tier could bring an end to collective security operations, undermine the credibility of alliance commitments by the great powers, [undermine guarantees of extended deterrence by them to threatened nations and states] extend alliances of their own, and perhaps make wars of aggression on their neighbors or their own people.172

#### Global counterbalancing in cyber space is inevitable absent a shift in US policy – the result is a collapse of military primacy

Kallberg & Thuraisingham 13 (Jan Kallberg is a research scientist and lead at the Cyber Operations Research Lab at the Cyber Security Research and Education Institute (CSI) in the Erik Jonsson School of Engineering and Computer Science at The University of Texas at Dallas. His research interests include offensive cyberoperations and societal stability. Kallberg received his PhD in public affairs from the University of Texas at Dallas. Bhavani Thuraisingham is a Louis A. Beecherl, Jr. Distinguished Professor and an executive director of the Cyber Security Research and Education Institute (CSI) in the Erik Jonsson School of Engineering and Computer Science at The University of Texas at Dallas. Her research interests include information assurance, system theory, and secure dependable data management. Thuraisingham received her PhD in theoretical computer science from University of Wales and the higher doctorate of engineering from University of Bristol. “State Actors’ Offensive Cyberoperations: The Disruptive Power of Systematic Cyberattacks” IT Pro May/June 2013 Published by the IEEE Computer Society 1520-9202/13/$31.00 © 2013 IEEE, <http://ieeexplore.ieee.org.proxy.library.emory.edu/stamp/stamp.jsp?tp=&arnumber=6471711>)

The Internet has experienced developments similar to those of the armored tank and helicopter— and the intellectual ceiling for Internet militarization has been incrementally breaking since 2010.

Militarizing the Internet didn’t require new technology or networking capabilities; rather, it required rethinking how the Internet application layer could be used for political or military gains.

Stuxnet—the set of code that affected the Iranian nuclear centrifuges—is the product of such a change in thinking. Designing Stuxnet to target and deliberately damage the Iranian nuclear centrifuges turned an existing technology into a new cyberweapon. Applying this type of weapon, nation states could potentially attack industrial control systems, such as municipal waterworks or other local infrastructure, damaging a society’s ability to function.

The increased number of SCADA (supervisory control and data acquisition) systems attacks are a product of the shift in the cyberattack modus operandi, from marginally funded cybercriminals are replaced with well-funded state actors with a completely different objective and agenda.1 A state actor seeking an advantage over another state might attack the core industrial backbone of a targeted country in the hopes of creating havoc in the transportation and communication infrastructure. For the traditional threat, cybercriminals, this would be a pointless operation, which is why we now must quickly change how we view, design, create, and maintain information security and protect our assets connected to cyberspace.

A militarized Internet and the potential for intelligence and economic espionage, which could destabilize adversarial states, radically changes the fundamentals for cyberspace security. State actors could exploit weaknesses in national infrastructures and information systems as well as exploit the public’s heavy reliance on the Internet.

Although the goal for individuals and criminal networks is usually financial gain, a state might seek to optimize its influence and power or avoid being overpowered by others. It thus has a vested interest in being able to destabilize the systems of other nations and could employ a full-system attack strategy instead of the traditional cyberattack, which seeks limited goals with a quick turnaround. Nation states have more time, resources, and opportunities, making them a far more capable perpetrator for covert cyberoperations.

Certain areas, previously sheltered from cyberattacks—such as the space-borne US global information grid—could be a target for state actors.4 A criminal network or hackers didn’t stand to gain financially from attacking the US global information grid, and even if they could sell the accessed information, it wouldn’t be worth the risk, given the repercussions if caught.

Thus, the satellite infrastructure wasn’t considered vulnerable. Attacking the global information grid represents no quick financial gain for a criminal network or hackers, and any marginal gain from selling the information would be drastically outweighed by the repercussions of the act, which have left the satellite infrastructure untouched by serious and capable cyberattacks.

However, in 2011, William J. Lynn III, former US deputy secretary of defense, reflected on the US national security space strategy:5 ”The willingness of states to interfere with satellites in orbit has serious implications for our national security. Space systems enable our modern way of war. They allow our warfighters to strike with precision, to navigate with accuracy, to communicate with certainty, and to see the battlefield with clarity. Without them, many of our most important military advantages evaporate.”

A kinetic antisatellite missile attack against the US would catapult the missile-launching nation on a confrontational course likely to lead to war or other uncertain drastic repercussions. However, a cyberattack carries much less risk, and it would be significantly harder to identify the perpetrator with sufficient satisfaction to warrant sanctions from the international community.

Attacking the superpowers’ space-borne grids presents an opportunity to undermine information supremacy and war-fighting abilities, with direct geopolitical consequences.

John Fraser, a British editor, wrote in The Spectator after a major British security breach:6 “ Suddenly, the western Internet “firewalls” are looking like a digital Maginot Line, so vulnerable that amateur hackers [could] steal hundreds of thousands of secrets for fun. So what might a cyberarmy be able to achieve?”

This analogy relates back to the history of the tank, when the French built the Maginot Line on their border with Germany to ensure the Germans couldn’t successfully attack France after World War I. Work started in 1930, and this construction project was one of the largest of its time. However, the Maginot Line was based on a major flaw—the French assumed the attacker would use a designated path and thus planned on fighting in fortified positions along that path. Using the new mindset of armored and mobile warfare, the Germans took another route, and the French endured one of history’s most humiliating defeats.

The entrance of state actors into cyberoperations represents the same drastic change of mindset and concept as the Germans using mobile armored warfare to overrun French defenses in 1940. A digital Maginot Line would be pouring in money and resources into a defensive position that assumes that cyberattacks occur as expected. The vast effort in cybersecurity today is placed on addressing the threats of the past, where a few unfunded individuals pound a single point of system entry using often crude tools to find configuration errors.

Information assurance strategies thus resemble trench and position warfare, fought from fixed positions in a known terrain using hardened positions and pre-assessed planning. The hardened system defends against a few limited attacks trying to penetrate a specific sector, server, or area. We can’t continue to focus on information assurance. By continuously hardening systems, a false sense of control and security is maintained, mainly based on the earlier attacker profile with single individuals or small criminal efforts penetrating the system. State actors have far more options to attack a system than solely trying to penetrate a firewall, so we need to redesign and restructure cybersecurity from a systems perspective.

The well-funded and geopolitically driven militarization of the Internet is a recent development—and represents a major shift in the related risks and threats. Security analyst Dan Geer has said that researching cybersecurity requires embracing the unknown —in other words, cybersecurity researchers must step out of their comfort zone of traditional IT security, taking a higher-level systematic view of system security.

Political scientist Kenneth N. Waltz said that the power with nuclear arms isn’t what you do with them but instead what you can do with them.8 Similarly, a state could use the mere threat of cyberoperations to deter other states from taking certain actions. However, once states engage their resources in cyberoperations, universities and intelligence agencies can become armories,9 and defense industries can receive contracts to identify weaknesses in foreign systems, redefining how we address cybersecurity.

#### Unipolarity creates structural incentives for peace

Wohlforth 09 – Professor of government @ Dartmouth College [[William C. Wohlforth](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#back), “Unipolarity, Status Competition, and Great Power War,” World Politics, Volume 61, Number 1, January 2009, http://www.polisci.wisc.edu/Uploads/Documents/IRC/Wohlforth%20(2009).pdf]

Second, I question the dominant view that status quo evaluations are relatively independent of the distribution of capabilities. If the status of states depends in some measure on their relative capabilities, and if states derive utility from status, then different distributions of capabilities may affect levels of satisfaction, just as different income distributions may affect levels of status competition in domestic settings. [6](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f6) Building on research in psychology and sociology, I argue that even capabilities distributions among major powers foster ambiguous status hierarchies, which generate more dissatisfaction and clashes over the status quo. And the more stratified the distribution of capabilities, the less likely such status competition is. Unipolarity thus generates far fewer incentives than either bipolarity or multipolarity for direct great power positional competition over status. Elites in the other major powers continue to prefer higher status, but in a unipolar system they face comparatively weak incentives to translate that preference into costly action. And the absence of such incentives matters because social status is a positional good—something whose value depends on how much one has in relation to others.[7](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f7) “If everyone has high status,” Randall Schweller notes, “no one does.”[8](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f8) While one actor might increase its status, all cannot simultaneously do so. High status is thus inherently scarce, and competitions for status tend to be zero sum.[9](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f9) I begin by describing the puzzles facing predominant theories that status competition might solve. Building on recent research on social identity and status seeking, I then show that under certain conditions the ways decision makers identify with the states they represent may prompt them to frame issues as positional disputes over status in a social hierarchy. I develop hypotheses that tailor this scholarship to the domain of great power politics, showing how the probability of status competition is likely to be linked to polarity. The rest of the article investigates whether there is sufficient evidence for these hypotheses to warrant further refinement and testing. I pursue this in three ways: by showing that the theory advanced here is consistent with what we know about large-scale patterns of great power conflict through history; by [End Page 30] demonstrating that the causal mechanisms it identifies did drive relatively secure major powers to military conflict in the past (and therefore that they might do so again if the world were bipolar or multipolar); and by showing that observable evidence concerning the major powers’ identity politics and grand strategies under unipolarity are consistent with the theory’s expectations. Puzzles of Power and War Recent research on the connection between the distribution of capabilities and war has concentrated on a hypothesis long central to systemic theories of power transition or hegemonic stability: that major war arises out of a power shift in favor of a rising state dissatisfied with a status quo defended by a declining satisfied state.[10](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f10) Though they have garnered substantial empirical support, these theories have yet to solve two intertwined empirical and theoretical puzzles—each of which might be explained by positional concerns for status. First, if the material costs and benefits of a given status quo are what matters, why would a state be dissatisfied with the very status quo that had abetted its rise? The rise of China today naturally prompts this question, but it is hardly a novel situation. Most of the best known and most consequential power transitions in history featured rising challengers that were prospering mightily under the status quo. In case after case, historians argue that these revisionist powers sought recognition and standing rather than specific alterations to the existing rules and practices that constituted the order of the day. In each paradigmatic case of hegemonic war, the claims of the rising power are hard to reduce to instrumental adjustment of the status quo. In R. Ned Lebow’s reading, for example, Thucydides’ account tells us that the rise of Athens posed unacceptable threats not to the security or welfare of Sparta but rather to its identity as leader of the Greek world, which was an important cause of the Spartan assembly’s vote for war.[11](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f11) The issues that inspired Louis XIV’s and Napoleon’s dissatisfaction with the status quo were many and varied, but most accounts accord [End Page 31] independent importance to the drive for a position of unparalleled primacy. In these and other hegemonic struggles among leading states in post-Westphalian Europe, the rising challenger’s dissatisfaction is often difficult to connect to the material costs and benefits of the status quo, and much contemporary evidence revolves around issues of recognition and status.[12](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f12) Wilhemine Germany is a fateful case in point. As Paul Kennedy has argued, underlying material trends as of 1914 were set to propel Germany’s continued rise indefinitely, so long as Europe remained at peace.[13](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f13) Yet Germany chafed under the very status quo that abetted this rise and its elite focused resentment on its chief trading partner—the great power that presented the least plausible threat to its security: Great Britain. At fantastic cost, it built a battleship fleet with no plausible strategic purpose other than to stake a claim on global power status.[14](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f14) Recent historical studies present strong evidence that, far from fearing attacks from Russia and France, German leaders sought to provoke them, knowing that this would lead to a long, expensive, and sanguinary war that Britain was certain to join.[15](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f15) And of all the motivations swirling round these momentous decisions, no serious historical account fails to register German leaders’ oft-expressed yearning for “a place in the sun.” The second puzzle is bargaining failure. Hegemonic theories tend to model war as a conflict over the status quo without specifying precisely what the status quo is and what flows of benefits it provides to states.[16](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f16) Scholars generally follow Robert Gilpin in positing that the underlying issue concerns a “desire to redraft the rules by which relations among nations work,” “the nature and governance of the system,” and “the distribution of territory among the states in the system.”[17](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f17) If these are the [End Page 32] issues at stake, then systemic theories of hegemonic war and power transition confront the puzzle brought to the fore in a seminal article by James Fearon: what prevents states from striking a bargain that avoids the costs of war? [18](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f18) Why can’t states renegotiate the international order as underlying capabilities distributions shift their relative bargaining power? Fearon proposed that one answer consistent with strict rational choice assumptions is that such bargains are infeasible when the issue at stake is indivisible and cannot readily be portioned out to each side. Most aspects of a given international order are readily divisible, however, and, as Fearon stressed, “both the intrinsic complexity and richness of most matters over which states negotiate and the availability of linkages and side-payments suggest that intermediate bargains typically will exist.”[19](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f19) Thus, most scholars have assumed that the indivisibility problem is trivial, focusing on two other rational choice explanations for bargaining failure: uncertainty and the commitment problem.[20](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f20) In the view of many scholars, it is these problems, rather than indivisibility, that likely explain leaders’ inability to avail themselves of such intermediate bargains. Yet recent research inspired by constructivism shows how issues that are physically divisible can become socially indivisible, depending on how they relate to the identities of decision makers.[21](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f21) Once issues surrounding the status quo are framed in positional terms as bearing on the disputants’ relative standing, then, to the extent that they value their standing itself, they may be unwilling to pursue intermediate bargaining solutions. Once linked to status, easily divisible issues that theoretically provide opportunities for linkages and side payments of various sorts may themselves be seen as indivisible and thus unavailable as avenues for possible intermediate bargains. The historical record surrounding major wars is rich with evidence suggesting that positional concerns over status frustrate bargaining: expensive, protracted conflict over what appear to be minor issues; a propensity on the part of decision makers to frame issues in terms of relative rank even when doing so makes bargaining harder; decision-makers’ [End Page 33] inability to accept feasible divisions of the matter in dispute even when failing to do so imposes high costs; demands on the part of states for observable evidence to confirm their estimate of an improved position in the hierarchy; the inability of private bargains to resolve issues; a frequently observed compulsion for the public attainment of concessions from a higher ranked state; and stubborn resistance on the part of states to which such demands are addressed even when acquiescence entails limited material cost. The literature on bargaining failure in the context of power shifts remains inconclusive, and it is premature to take any empirical pattern as necessarily probative. Indeed, Robert Powell has recently proposed that indivisibility is not a rationalistic explanation for war after all: fully rational leaders with perfect information should prefer to settle a dispute over an indivisible issue by resorting to a lottery rather than a war certain to destroy some of the goods in dispute. What might prevent such bargaining solutions is not indivisibility itself, he argues, but rather the parties’ inability to commit to abide by any agreement in the future if they expect their relative capabilities to continue to shift.[22](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f22) This is the credible commitment problem to which many theorists are now turning their attention. But how it relates to the information problem that until recently dominated the formal literature remains to be seen.[23](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f23) The larger point is that positional concerns for status may help account for the puzzle of bargaining failure. In the rational choice bargaining literature, war is puzzling because it destroys some of the benefits or flows of benefits in dispute between the bargainers, who would be better off dividing the spoils without war. Yet what happens to these models if what matters for states is less the flows of material benefits themselves than their implications for relative status? The salience of this question depends on the relative importance of positional concern for status among states. Do Great Powers Care about Status? Mainstream theories generally posit that states come to blows over an international status quo only when it has implications for their security or material well-being. The guiding assumption is that a state’s satisfaction [End Page 34] with its place in the existing order is a function of the material costs and benefits implied by that status.[24](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f24) By that assumption, once a state’s status in an international order ceases to affect its material wellbeing, its relative standing will have no bearing on decisions for war or peace. But the assumption is undermined by cumulative research in disciplines ranging from neuroscience and evolutionary biology to economics, anthropology, sociology, and psychology that human beings are powerfully motivated by the desire for favorable social status comparisons. This research suggests that the preference for status is a basic disposition rather than merely a strategy for attaining other goals.[25](http://muse.jhu.edu/journals/world_politics/v061/61.1.wohlforth.html#f25) People often seek tangibles not so much because of the welfare or security they bring but because of the social status they confer. Under certain conditions, the search for status will cause people to behave in ways that directly contradict their material interest in security and/or prosperity.

Much of this research concerns individuals, but international politics takes place between groups. Is there reason to expect individuals who act in the name of states to be motivated by status concerns? Compelling findings in social psychology suggest a positive answer. Social identity theory (SIT) has entered international relations research as a psychological explanation for competitive interstate behavior. 26 According to the theory’s originator, Henri Tajfel, social identity is “that part of an individual’s self-concept which derives from his knowledge of his membership of a social group (or groups) together with the value and emotional significance attached to that membership.” 27 Tajfel and his followers argue that deep-seated human motivations of self-definition and self-esteem induce people to define their identity in relation to their in-group, to compare and contrast that in-group with out-groups, and to want that comparison to reflect favorably on themselves. In a remarkable set of experiments that has since been replicated dozens of times, Tajfel and his collaborators found that simply assigning subjects to trivially defined “minimal” in-groups led them to discriminate in favor of their in-group at the expense of an out-group, even when nothing else about the setting implied a competitive relationship. Although SIT appears to provide a plausible candidate explanation for interstate conﬂict, moving beyond its robust but general implication about the ubiquitous potential for status seeking to speciﬁc hypotheses about state behavior has proved challenging. In particular, experimental ﬁndings concerning which groups individuals will select as relevant comparisons and which of many possible identity-maintenance strategies they will choose have proved highly sensitive to the assumptions made about the social context. The results of experimental research seeking to predict responses to status anxiety—whether people will choose social mobility (identifying with a higher status group), social creativity (seeking to redeﬁne the relevant status-conferring dimensions to favor those in which one’s group excels), social conﬂict (contesting the status-superior group’s claim to higher rank), or some other strategy—are similarly highly context dependent. 28 For international relations the key unanswered question remains: under what circumstances might the constant underlying motivation for a positive self-image and high status translate into violent conﬂict? While SIT research is suggestive, standard concerns about the validity of experimental ﬁndings are exacerbated by the fact that the extensive empirical SIT literature is generally not framed in a way that captures salient features of international relations. The social system in which states operate is dramatically simpler than the domestic social settings much of the research seeks to capture. Decision makers’ identiﬁcation with the state is generally a given, group boundaries are practically impermeable, and there are very few great powers and very limited mobility. For states, comparison choice and the selection of status-maintenance strategies are constrained by exogenous endowments and geographical location. Natural and historical endowments—size and power potential—vary much more among states than among indi- iduals and so play a much larger role in determining hierarchies and inﬂuencing the selection of identity maintenance strategies. Assumptions built into most SIT research to date generally do not capture these realities of interstate life. In particular, standard SIT research designs beg the question of the expected costs of competing for status. Experiments do not generally posit situations in which some groups are endowed with demonstrably superior means with which to discriminate in favor of their own group at the expense of out-groups. Indeed, built in to most experimental setups is an implied assumption of material equality among groups. Yet international politics is notable as a social realm with especially large disparities in material capabilities, and decision makers are unlikely to follow identity-maintenance strategies that are demonstrably beyond their means. Nevertheless, there is no reason to doubt the relevance for states of SIT’s core finding that individual preferences for higher status will affect intergroup interactions. Individuals who identify with a group transfer the individual’s status preference to the group’s relations with other groups. If those who act on behalf of a state (or those who select them) identify with that state, then they can be expected to derive utility from its status in international society. In addition, there are no evident reasons to reject the theory’s applicability to interstate settings that mimic the standard SIT experimental setup—namely, in an ambiguous hierarchy of states that are comparable in material terms. As Jacques Hymans notes: “in the design of most SIT experiments there is an implicit assumption of rough status and power parity. Moreover, the logic of SIT theory suggests that its findings of ingroup bias may in fact be dependent on this assumption.” 29 Status conflict is thus more likely in flat, ambiguous hierarchies than in clearly stratified ones. And there are no obvious grounds for rejecting the basic finding that comparison choice will tend to be “similar but upward” (that is, people will compare and contrast their group with similar but higher status groups). 30 In most settings outside the laboratory this leaves a lot of room for consequential choices, but in the context of great power relations, the set of feasible comparison choices is constrained in highly consequential ways.

#### American power solves global problems

Barnett 2011, Thomas P.M. Barnett, Former Senior Strategic Researcher and Professor in the Warfare Analysis & Research Department, Center for Naval Warfare Studies, U.S. Naval War College American military geostrategist and Chief Analyst at Wikistrat., worked as the Assistant for Strategic Futures in the Office of Force Transformation in the Department of Defense, 3-7-2011, “The New Rules: Leadership Fatigue Puts U.S., and Globalization, at Crossroads,” , http://www.worldpoliticsreview.com/articles/8099/the-new-rules-leadership-fatigue-puts-u-s-and-globalization-at-crossroads

It is worth first examining the larger picture: We live in a time of arguably the greatest structural change in the global order yet endured, with this historical moment's most amazing feature being its relative and absolute lack of mass violence. That is something to consider when Americans contemplate military intervention in Libya, because if we do take the step to prevent larger-scale killing by engaging in some killing of our own, we will not be adding to some fantastically imagined global death count stemming from the ongoing "megalomania" and "evil" of American "empire." We'll be engaging in the same sort of system-administering activity that has marked our stunningly successful stewardship of global order since World War II. Let me be more blunt: As the guardian of globalization, the U.S. military has been the greatest force for peace the world has ever known. Had America been removed from the global dynamics that governed the 20th century, the mass murder never would have ended. Indeed, it's entirely conceivable there would now be no identifiable human civilization left, once nuclear weapons entered the killing equation. But the world did not keep sliding down that path of perpetual war. Instead, America stepped up and changed everything by ushering in our now-perpetual great-power peace. We introduced the international liberal trade order known as globalization and played loyal Leviathan over its spread. What resulted was the collapse of empires, an explosion of democracy, the persistent spread of human rights, the liberation of women, the doubling of life expectancy, a roughly 10-fold increase in adjusted global GDP and a profound and persistent reduction in battle deaths from state-based conflicts. That is what American "hubris" actually delivered. Please remember that the next time some TV pundit sells you the image of "unbridled" American military power as the cause of global disorder instead of its cure. With self-deprecation bordering on self-loathing, we now imagine a post-American world that is anything but. Just watch who scatters and who steps up as the Facebook revolutions erupt across the Arab world. While we might imagine ourselves the status quo power, we remain the world's most vigorously revisionist force. As for the sheer "evil" that is our military-industrial complex, again, let's examine what the world looked like before that establishment reared its ugly head. The last great period of global structural change was the first half of the 20th century, a period that saw a death toll of about 100 million across two world wars. That comes to an average of 2 million deaths a year in a world of approximately 2 billion souls. Today, with far more comprehensive worldwide reporting, researchers report an average of less than 100,000 battle deaths annually in a world fast approaching 7 billion people. Though admittedly crude, these calculations suggest a 90 percent absolute drop and a 99 percent relative drop in deaths due to war. We are clearly headed for a world order characterized by multipolarity, something the American-birthed system was designed to both encourage and accommodate. But given how things turned out the last time we collectively faced such a fluid structure, we would do well to keep U.S. power, in all of its forms, deeply embedded in the geometry to come. To continue the historical survey, after salvaging Western Europe from its half-century of civil war, the U.S. emerged as the progenitor of a new, far more just form of globalization -- one based on actual free trade rather than colonialism. America then successfully replicated globalization further in East Asia over the second half of the 20th century, setting the stage for the Pacific Century now unfolding.

#### Plan solves international counter balancing – it creates a LOAC for cyber space

Bradbury 11 (Steven Assistant Attorney General for the Office of Legal Counsel, The Developing Legal Framework for Defensive and Offensive Cyber Operations, <http://harvardnsj.org/wp-content/uploads/2011/02/Vol.-2_Bradbury_Final1.pdf>)

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

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

And if you just review the literature on cyber war, you quickly see that that’s where we are: precisely how the laws and customs of war should apply to offensive cyber operations is not yet crystallized in key respects.

For example, there aren’t always bright lines to tell us when a cyber attack on computer systems constitutes an “armed attack” or a “use of force” that justifies a nation in launching a responsive military strike under Article 51 of the U.N. Charter.

Some questions are easy: Hacking into a sensitive government computer system to steal information is an act of espionage, not an armed attack. It’s clearly not prohibited by the laws and customs of war.

On the other hand, if the cyber intrusion inflicts significant physical destruction or loss of life by causing the failure of critical infrastructure, like a dam or water supply system, then it obviously would constitute an armed attack under the law of war and would justify a full military response if it could be attributed to a foreign power. Where committed as an offensive act of aggression, such an attack may violate international law.

If significant enough, the effect of the attack will determine its treatment, not necessarily whether the attack is delivered through computer lines as opposed to conventional weapons systems. In these cases, the laws and customs of war provide a clear rule to apply.

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

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

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

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

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

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

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

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

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

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

Conclusion. So here’s my thesis: To my view, the lack of clarity on certain of these issues under international law means that with respect to those issues, the President is free to decide, as a policy matter, where and¶ how the lines should be drawn on the limits of traditional military power in the sphere of cyberspace. For example, that means that within certain parameters, the President could decide when and to what extent military cyber operations may target computers located outside areas of hot fighting that the enemy is using for military advantage. And when a cyber attack is directed at us, the President can decide, as a matter of national policy, whether and when to treat it as an act of war.

The corollary to all this is that in situations where the customs of war, in fact, are not crystallized, the lawyers at the State Department and the Justice Department shouldn’t make up new red lines — out of some aspirational sense of what they think international law ought to be — that end up putting dangerous limitations on the options available to the United States. Certainly, the advice of lawyers is always important, especially so where the legal lines are established or firmly suggested. No one would contend that the laws of war have no application to cyber operations or that cyberspace is a law-free zone. But it’s not the role of the lawyers to make up new lines that don’t yet exist in a way that preempts the development of policy.14

In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention on cyberwarfare —¶ perhaps a kind of arms control agreement for cyber weapons. I believe there is no foreseeable prospect that that will happen. Instead, the outlines of accepted norms and limitations in this area will develop through the practice of leading nations. And the policy decisions made by the United States in response to particular events will have great influence in shaping those international norms. I think that’s the way we should want it to work.

One final admonition I’ll offer on the topic of offensive cyber operations: In cases where the President shapes new policy by choosing military action over covert action for a cyber operation, or vice versa, I would strongly urge that the President fully brief both sets of committees in Congress — the Intelligence Committees and the Armed Services Committees — and explain the basis for the choice. It’s inevitable the committees will find out anyway when a jurisdictional marker is crossed, and it will help smooth the development of consistent policies and standards for the committee members and staff to understand and appreciate the choices made on both sides of the question.

#### Congressional restrictions on OCOs reestablish US leadership

Bastby 12 (Judy, Chairwoman of the American Bar Association’s Privacy and Computer Crime Committee, CEO of Global Cyber Risk, “U.S. Administration's Reckless Cyber Policy Puts Nation at Risk” June 4, 2012, <http://www.forbes.com/sites/jodywestby/2012/06/04/u-s-administrations-reckless-cyber-policy-puts-nation-at-risk/2/>)

Perhaps more important than being out of the cyber coordination loop, is the how the U.S.’s attitude is being perceived by others in the international community. If the U.S. were a member of IMPACT and taking an active role in the investigation, it would be upholding its role as a global cybersecurity power. Instead, the U.S. appears as the shirking nation state quietly standing on the sidelines while being accused of engaging in cyberwarfare tactics. “People look to the U.S., Russia, and China for leadership and when the U.S. is absent, they will turn to the other two,” observes Dr. Amin.

The U.S. Administration’s failure to develop a strong foreign policy with respect to cybersecurity reveals a gross lack of attention at the highest levels of the U.S. Government to one of the country’s most vulnerable areas — the IT systems that underpin the functioning of our society and economy. This failure begins at basic strategy levels and extends to reckless disregard for the consequences of the risky covert Stuxnet operation and failure to secure classified information about the program. For example, in May 2011, government delegations from around the world gathered in Geneva for the World Summit on the Information Society (WSIS), one of the most important communications and technology conferences globally. Noticeably, the U.S. did not have a delegation present. Yet, it was during the WSIS event that the U.S. Administration chose to release its International Strategy for Cyberspace – from Washington, D.C. rather than Geneva. WSIS participants were dumbstruck. For the few private sector Americans who were present, including myself, it was embarrassing.

If in fact the Administration did authorize targeting Iranian nuclear systems with Stuxnet and/or Flame, it was a dangerous and reckless decision, especially since the U.S. Government has no idea how many computers in America may be infected with malware capable of being activated by Iran or one of its allies in retaliation. Such “backdoor” malware is capable of having enormous consequences to life and property. A similar CIA covert operation successfully destroyed a Soviet pipeline. In 1982, President Reagan approved a plan to transfer software used to run pipeline pumps, turbines, and valves to the Soviet Union that had embedded features designed to cause pump speeds and valve settings to malfunction. The plot was revealed in a 2004 Washington Post article by David Hoffman in advance of its discussion in former Air Force Secretary Thomas C. Reed’s book, At the Abyss: An Insider’s History of the Cold War. Reed recalled to Hoffman that, “The result was the most monumental non-nuclear explosion and fire ever seen from space.” Unlike Stuxnet, however, the program remained classified for 22 years until the CIA authorized Reed to discuss it in his book. Sanger’s information came from loose-lipped persons involved with the Stuxnet operation.

Before pulling a trigger (or launching malware) a nation should assess its strengths and resources and its correlation of vulnerabilities, which, in 2012, includes understanding what an adversary can do when firing back using cyber capabilities. In addition, before launching covert operations, such as Stuxnet, a nation also should ensure that the secrecy of the intelligence operations can be maintained.

Conversations with Hill staffers indicate that Congress believes the State Department’s 2011 appointment of Coordinator for Cyber Issues has sufficiently addressed concerns about the lack of U.S. involvement in international cybersecurity matters. Clearly, this is narrow, wishful thinking. Congress needs to stop focusing on what it believes it should force businesses to do about cybersecurity and instead focus on what it should demand that the U.S. Government do to protect our critical infrastructure businesses and avoid retaliatory cyber attacks. The kind of reckless cyber diplomacy and foreign policy now at work has put our nation at risk and demonstrates cyber irresponsiblity, not cyber leadership.

#### Creation of US led international norms reestablishes international credibility and soft power – XO can’t solve – preserves expediency.

Belk & Noyes 12 (Robert Belk Naval aviator and Politico-Military Fellow, studying international and global affairs at the Harvard Kennedy School, and Matthew Noyes studies international security policy and is a senior associate with the cybersecurity practice at Good Harbor Consulting. Prior to attending the Harvard Kennedy School, he served for five years as an infantry officer in the US army serving multiple tours in Iraq. Following graduation he plans to continue working on cybersecurity issues. He has a degree in Computer Science and Applied Computational Mathematics from the University of Washington., Advised by Professor Joseph Nye & Professor Monica Toft 20 March 2012, “On the Use of Offensive Cyber Capabilities A Policy Analysis on Offensive US Cyber Policy”, <http://belfercenter.ksg.harvard.edu/files/cybersecurity-pae-belk-noyes.pdf>)

The U.S. must be able to project the second and third order effects of conducting external operations in cyberspace. One critical example would be the soft power implications for such operations. Specifically, most civilian global perceptions of the Internet (especially in light of the Arab Awakening) focus on peaceful uses. External cyber operations or other actions that may affect normal cyber activities, therefore, can adversely affect America’s soft power.

A recent example of this is the Egyptian protesters’ reaction to the Bay Area Transit Authority’s (BART) shut down of cell service in one of their stations in August 2011. In anticipation of a protest at one of its stations, BART officials halted cell service in order to minimize the gathering. Many Bay Area citizens viewed this as a limit on their right to peaceful assembly. Egyptian activists from the Tahrir Square demonstrations seemed to agree. They began voicing their disapproval by referencing BART in tweets as “MuBARTak.”62 Likening BART’s actions to those of the deposed president reflects a certain loss of prestige abroad, signifying an erosion of soft power.

In that vein, the U.S. must consider the implications for external cyber operations in affecting perceptions of the U.S. abroad. A cyber action that is Executionally or Strategically expedient may have second or third order effects that diminish American soft power.

#### Our use of cyber ops as coercion represents a barrier to international credibility

Belk & Noyes 12 (Robert Belk Naval aviator and Politico-Military Fellow, studying international and global affairs at the Harvard Kennedy School, and Matthew Noyes studies international security policy and is a senior associate with the cybersecurity practice at Good Harbor Consulting. Prior to attending the Harvard Kennedy School, he served for five years as an infantry officer in the US army serving multiple tours in Iraq. Following graduation he plans to continue working on cybersecurity issues. He has a degree in Computer Science and Applied Computational Mathematics from the University of Washington., Advised by Professor Joseph Nye & Professor Monica Toft 20 March 2012, “On the Use of Offensive Cyber Capabilities A Policy Analysis on Offensive US Cyber Policy”, <http://belfercenter.ksg.harvard.edu/files/cybersecurity-pae-belk-noyes.pdf>)

The use of coercive means against any actor is certain to reduce U.S. influence among supporters of that actor. As such, the U.S. should be especially careful in conducting cyber attacks against organizations that enjoy popular support among key audiences. Like using any form of coercion, the U.S. should seek to legitimize the action by using less coercive means first. It should also have declared and generally internationally accepted policies that clearly define when cyber attacks are appropriate. In conducting a cyber attack the U.S. should provide reasonable explanations to the global community of the justice and necessity of U.S. action and how it servers the general good.

#### The lack of transparency reduces US credibility

Belk & Noyes 12 (Robert Belk Naval aviator and Politico-Military Fellow, studying international and global affairs at the Harvard Kennedy School, and Matthew Noyes studies international security policy and is a senior associate with the cybersecurity practice at Good Harbor Consulting. Prior to attending the Harvard Kennedy School, he served for five years as an infantry officer in the US army serving multiple tours in Iraq. Following graduation he plans to continue working on cybersecurity issues. He has a degree in Computer Science and Applied Computational Mathematics from the University of Washington., Advised by Professor Joseph Nye & Professor Monica Toft 20 March 2012, “On the Use of Offensive Cyber Capabilities A Policy Analysis on Offensive US Cyber Policy”, <http://belfercenter.ksg.harvard.edu/files/cybersecurity-pae-belk-noyes.pdf>)

If properly executed in self-defense, we see no adverse soft power consequences of employing a cyber counterattack. The rationale lies within the natural bias toward defense. In this, there is a distinct second mover legitimacy advantage. In the wake of the 9/11 terrorist attacks, international support for theU.S. was very high. But when nations began to believe that the response to the terrorist attacks was not proportionate, discrete, or necessary, they changed their opinions.110 This loss of prestige inevitably had an impact on the U.S.’s soft power.111

The key, therefore, for executing a successful cyber counterattack that maintains the U.S.’s soft power will be in ensuring the conditions from the principles of distinction, proportionality, and necessity are met. To demonstrate to the international community that the government response was in line with these principles, the U.S. must be prepared to essentially defend its case. This entails the government’s having a series of facts at its disposal: 1) attribution; 2) effect on internal networks; 3) action taken by U.S.; 4) effect on external networks; and 5) measures taken to ensure discrimination, proportionality, and necessity. In some instances, it may be prudent to also have record of post-action diplomatic communiqués to show the importance of dialogue in resolving conflict. All of these actions may require revisiting the classification scheme for U.S. cyber operations in order to better balance the need for operational security with transparency.

#### Congress is crucial to change the perception

Butler 4/26 (Appellate Advocacy Counsel for the Electronic Privacy Information Center, When Cyberweapons End Up On Private Networks: Third Amendment Implications for Cybersecurity Policy, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2257078>)

A. Authority: Congress Must Be Involved in Establishing Any Framework for the Authorization of Cyberoperations **Given that the Third Amendment requires war-time quartering be conducted “in a manner to be prescribed by law**,”223 Congress must have a role in establishing the framework used to authorize any offensive cyberoperation. This **legislative involvement would not only ensure that all cyberoperations have adequate legal authorization but** it would also **promote** the **broader goals of transparency and cooperation that the President has emphasized throughout this process**. So far Congress has focused its energy on perceived problems rather than real solutions.224 A debate raged in the 112th Congress over whether to let DHS or NSA take the lead on a proposed information-sharing environment.225 This turf war was quite tangential from the problems of substandard security for critical systems and a lack of legal clarity as to the role of each government agency in responding to an external threat or strategic opportunity.226 **The only congressional involvement in developing a cybersecurity framework so far has been its brief affirmance in the 2012 National Defense Authorization Act227 that the President may conduct “operations in cyberspace” subject to the traditional legal regimes applicable to kinetic warfare.228 Congress’s active role in setting our nation’s military actions in cyberspace is the only way to have a national dialogue and to avoid relying on secret legal interpretations about important national security matters. The President took steps to begin a national dialogue when he issued an Executive Order** on the same day as the 2013 State of the Union Address.229 The Executive Order focused on improving critical infrastructure cybersecurity while promoting privacy, civil liberties, and the economy.230 The Order also provided for sharing of “cyber threat information” from executive branch agencies to private sector entities,231 and the development of a framework by the National Institute of Standards and Technology (NIST) to establish baseline security standards for government agencies and critical infrastructure companies.232 The Order also required that privacy and civil liberties protections be incorporated into the cybersecurity program and that the Chief Privacy Officer of DHS assess the privacy risks and publish a report.233 The Executive Order did not address the “information sharing environment” proposed in Congress during 2012 and again in 2013.234 The Order also did not address the legal determination of when and how cyberoperations can be authorized, which has apparently already been made in an internal executive-branch memorandum.235 **The** President’s Executive **Order** is a step in the right direction but it does not provide sufficient authority for cyberoperations that could intrude upon civilian systems; only Congress can authorize such quartering.

#### Solves extinction – largest international threat

Kempe 2012, Frederick Kempe, president and chief executive officer of the Atlantic Council, a foreign policy think tank and public policy group, President and Chief Executive Officer of the Atlantic Council since December 1, 2006, and is a Visiting Fellow at Oxford University's Saïd Business School, April 18, 2012, “Does America still want to lead the world?”, http://blogs.reuters.com/thinking-global/2012/04/18/does-america-still-want-to-lead-the-world/

For all their bitter differences, President Obama and Governor Romney share one overwhelming challenge. Whoever is elected will face the growing reality that the greatest risk to global stability over the next 20 years may be the nature of America itself. Nothing – not Iranian or North Korean nuclear weapons, not violent extremists or Mideast instability, not climate change or economic imbalances – will shape the world as profoundly as the ability of the United States to remzain an effective and confident world player advocating its traditional global purpose of individual rights and open societies. That was the conclusion of the Global Agenda Council on the United States, a group of experts that was brought together by the World Economic Forum and that I have chaired. Even more intriguing, our group tested our views on, among others, a set of Chinese officials and experts, who worried that we would face a world overwhelmed by chaos if the U.S. – facing resource restraints, leadership fatigue and domestic political dysfunction – disengaged from its global responsibilities. U.S. leadership, with all its shortcomings and missteps, has been the glue and underwriter of global stability since World War Two – more than any other nation. Even with the world experiencing its greatest shift of economic and political power since the 19th century, no other country is emerging – or looks likely to emerge – that would be as prepared or equipped to exercise leadership on behalf of the global good. Yet many in the world are questioning the role of U.S. leadership, the governance architecture it helped create and even the values for which the U.S. stands. Weary from a decade of war and strained financially, Americans themselves are rethinking whether they can afford global purpose. The election campaign is unlikely to shed much light on these issues, yet both candidates face an inescapable truth: How the U.S. evolves over the next 15 to 20 years will be most important single variable (and the greatest uncertainty) hovering over the global future. And the two most important elements that will shape the U.S. course, in the view of the Global Agenda Council on the United States, will be American intentions and the capability to act on them. In short, will Americans continue to see as part of their identity the championing of values such as individual opportunity and open societies that have contributed so richly to the global commons? Second, can the U.S. sufficiently address its domestic challenges to assure its economic, political and societal strength while the world changes at unprecedented velocity? Consider this: It took Great Britain 155 years to double its gross domestic product per capita in the 18th and 19th centuries, when it was the world’s leading power. It took the U.S. 50 years to do the same by 1950, when its population was 152 million. Both India and China have achieved the same growth on a scale and at a pace never experienced before. Both countries have more than a hundred times the population of Britain during its heyday, yet they are achieving similar outcomes in a tenth of the time. Although China will likely surpass the U.S. as the world’s largest economy by 2030, Americans retain distinct advantages that could allow them to remain the pivotal power. Think of Uncle Sam as a poker player sitting at a global table of cohorts, holding better cards than anyone else: a free and vibrant society, a history of technological innovation, an ability to attract capital and generate jobs, and a relatively young and regenerating population. However, it doesn’t matter how good your cards are if you’re playing them poorly. Put another way, the candidate who wins in November is going to be faced with the reality summed up by the cartoon character Pogo in 1971 as he was trying to make his way through a prickly primeval forest without proper footwear: “We have met the enemy and he is us.” Imagine two very different scenarios for the world, based on how America rises to its challenges. The positive scenario would require whoever is elected in November to be a unifier, someone who can rise above our current squabbles and galvanize not only the U.S. but also the world around a greater understanding of this historic moment. He would address the larger U.S. issues of failing infrastructure, falling educational standards, widening deficits and spiraling healthcare costs. He would partner more effectively with rising powers, and China in particular. And he would recognize and act upon the strategic stake the U.S. has in a politically confident, economically healthy Europe. The doubling of the global middle class by a billion people by 2030 plays into U.S. political and economic strengths, increasing demand for the products and services of information technology where the U.S. excels. Developments that improve the extraction of shale natural gas and oil provide the U.S. and some of its allies disproportionate benefits. Under this positive scenario, the U.S. could log growth rates of 2.7 percent or more each year, compared with 2.5 percent over the past 20 years. Average living standards could rise by 40 percent through 2030, keeping alive the American dream and restoring the global attractiveness of the U.S. model. The negative scenario results from a U.S. that fails to rise to its current challenges. Great powers decline when they fail to address the problems they recognize. U.S. growth could slow to an average of 1.5 percent per year, if that. The knock-on impact on the world economy could be a half-percent per year. The shift in the perception of the U.S. as a descending power would be more pronounced. This sort of United States would be increasingly incapable of leading and disinclined to try. It is an America that would be more likely to be protectionist and less likely to retool global institutions to make them more effective. One can already see hints of what such a world would look like. Middle Eastern diplomats in Washington say the failure of the U.S. to orchestrate a more coherent and generous transatlantic and international response to their region’s upheavals has resulted in a free-for-all for influence that is favoring some of the least enlightened players. Although the U.S. has responded to the euro zone crisis, as a result of its own economic fears, it hasn’t offered a larger vision for the transatlantic future that recognizes its enormous strategic stake in Europe’s future, given global shifts of influence. The U.S. played a dominant role in reconstructing the post-World War Two international order. The question is whether it will do so again or instead contribute to a dangerous global power vacuum that no one over the next two decades is willing or capable of filling.

#### US leadership creates a global concert of power that solves

**Nye 08 (**Joseph is professor of international relations at Harvard University, “American Power After the Financial Crises,” <http://www.foresightproject.net/publications/articles/article.asp?p=3533>)

Power always depends on context, and in today's world, it is distributed in a pattern that resembles a complex three-dimensional chess game. On the top chessboard, military power is largely unipolar and likely to remain so for some time. But on the middle chessboard, economic power is already multi-polar, with the US, Europe, Japan and China as the major players, and others gaining in importance. **The bottom chessboard is the realm of transnational relations that cross borders outside of government control,** and **it includes actors as** **diverse as bankers** electronically **transferring sums larger than most national budgets** at one extreme, **and terrorists transferring weapons** **or hackers disrupting Internet operations** at the other. **It** also **includes new challenges like pandemics and climate change**. On this bottom board, power is widely dispersed, and it makes no sense to speak of unipolarity, multi-polarity or hegemony. **Even in the aftermath of the financial crisis, the giddy pace of technological change is likely to continue to drive globalisation, but the political effects will be quite different for the world of nation states and the world of non-state actors**. In inter-state politics, the most important factor will be the continuing "return of Asia". In 1750, Asia had three-fifths of the world population and three-fifths of the world's product. By 1900, after the industrial revolution in Europe and America, Asia's share shrank to one-fifth of the world product. By 2040, Asia will be well on its way back to its historical share. **The "rise" in the power of China and India may create instability**, but it is a problem with precedents, and we can learn from history about how our policies can affect the outcome. **A century ago, Britain managed the rise of American power without conflict, but the world's failure to manage the rise of German power led to two devastating world wars.** In transnational politics, **the information revolution is dramatically reducing the costs of computing and communication. Forty years ago, instantaneous global communication was possible but costly, and restricted to governments and corporations**. Today it is virtually free to anyone with the means to enter an internet café. **The barriers to entry into world politics have been lowered, and non-state actors now crowd the stag**e. In 2001, **a non-state group killed more Americans than the government of Japan killed at Pearl Harbor**. **A pandemic** spread by birds or travelers on jet aircraft **could kill more people than perished in the first or second world wars**. This is a new world politics with which we have less experience. The problems of power diffusion (away from states) may turn out to be more difficult than power transition among states. **The problem for American power in the 21st century is that there are more and more things outside the control of even the most powerful state**. Although the United States does well on the traditional measures, there is increasingly more going on in the world that those measures fail to capture. **Under the influence of the information revolution and globalisation, world politics is changing in a way that means Americans** cannot achieve all their international goals acting alone. For example, **international financial stability** **is vital to the prosperity of Americans,** but the United States needs the cooperation of others to ensure it. **Global climate change too will affect the quality of life, but the United States cannot manage the problem alone**. **And in a world where borders are becoming more porous than ever to everything from drugs to infectious diseases to terrorism, America must mobilise international coalitions to address shared threats and challenges.** As the largest country, American leadership will remain crucial. The problem of American power after this crisis is not one of decline, but realisation that **even the largest country cannot achieve its aims without the help of others.**

### Plan

#### The United States federal government should require the President of the United States consult Congress prior to the use of offensive cyber operations or provide a prompt and full account of the use of offensive cyber operations by the United States.

# 2AC

### Case

#### Deterrence is impossible in cyber space – Attriibution, Identity, Proxies, Escalation incentive

Owens et al. 09 (WILLIAM A. OWENS, AEA Holdings, Inc., Co-chair KENNETH W. DAM, University of Chicago, Co-chair THOMAS A. BERSON, Anagram Laboratories GERHARD CASPER, Stanford University DAVID D. CLARK, Massachusetts Institute of Technology RICHARD L. GARWIN, IBM Fellow Emeritus JACK L. GOLDSMITH III, Harvard Law School CARL G. O’BERRY, The Boeing Company JEROME H. SALTZER, Massachusetts Institute of Technology (retired) MARK SEIDEN, MSB Associates SARAH SEWALL, Harvard University WALTER B. SLOCOMBE, Caplin & Drysdale WILLIAM O. STUDEMAN, U.S. Navy (retired) MICHAEL A. VATIS, Steptoe & Johnson LLP, “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities”, pdf)

It remains an open question as to whether the concepts of deterrence are relevant when applied to the domain of cyberconflict per se (that is, cyberconflict without reference to conflict in physical domains). For example, a credible threat to impose costs requires knowledge of the party on which the costs should be imposed—and as discussed in Chapter 2, attribution of a cyberattack is a very difficult and time-consuming—and perhaps insoluble—problem.

Moreover, even if the adversary is known, and known to be a specific nation-state, the costs to be imposed must be judged by the adversary as greater than the gain that might result from his aggressive actions. Thus, the United States must be able to identify cyber targets in or of the adversary nation whose loss would be costly to the adversary, and it must be able to attack them with high confidence of success.

In a nation that is not highly dependent on information technology, such assets would be hard to find. Even if the nation did have valuable information technology assets, specific individual targets (perhaps numbering in the dozens or hundreds—a wild guess!) most valuable to the adversary are likely to be very well protected against cyberattack. The civilian IT infrastructure at large may be less well protected, but largescale attacks on such infrastructure raise ethical and moral questions about targeting civilians. The military IT infrastructure could be targeted as well, but the degree to which it is well protected may be unknown to the attacker (see discussion in Chapter 2 regarding intelligence requirements for successful focused cyberattacks).

In addition, an attacker that launches a cyberattack should also be expected to take action to change its own defensive posture just prior to doing so. As discussed in Chapter 2, much can be done to invalidate an adversary’s intelligence preparations, which are necessary for discriminating counterattacks. And since the attacker knows when he will launch the attack, he can create a window during which his defensive posture will be stronger. The window would last only as long as it would take for new intelligence efforts to collect the necessary information, but it would likely be long enough to forestall immediate retaliation.

A threat to deny benefits to a cyberattacker also lacks credibility in certain important ways. In principle, defensive technologies to harden targets against cyberattacks can be deployed, raising the difficulty of attacking them. But decades of experience suggest that deploying these technologies and making effective use of them on a society-wide basis to improve the overall cybersecurity posture of a nation is difficult indeed. And there is virtually no prospect of being able to reduce a cyberattacker’s capabilities through offensive action, because of the ease with which cyberattack weapons can be acquired. Thus, counterforce capabilities—which in the nuclear domain have been justified in large part as necessary to reduce the threat posed by an adversary’s nuclear weapons—do not exist in any meaningful way in contemplating cyberconflict.

How do the considerations above change if, as in the real world, the states involved also have kinetic capabilities, which may include nuclear weapons, and physical vulnerabilities? That is, each side could, in principle, use kinetic weapons to attack physical targets, and these targets might be military or dual purpose in nature as long as they are legitimate targetsunder LOAC. Because a transition from cyber-only conflict to kinetic conflict would likely constitute an escalation (and would in any case make the conflict more overt), this point is discussed in more detail below.

### 2AC – Disease Add-On

#### Soft power solves disease – causes extinction

Toolis 2009, the director of a major television series on the history of plagues, 09 (Kevin, The Express, April 28, 2009 U.K. 1st Edition “Pandemic Pandemonium” lexis)

It destroyed the Roman Empire, wiped out most of the New World and killed millions in Europe. How disease - not just Mexico's swine fever - has shaped the planet SCIENTISTS call it the Big Die Off, when a terrifying new virus rips through a species and kills up to a third of the entire population. And we all now could be facing a new apocalypse, though no one yet knows how potent the new strain of Mexican swine fever will be, or how many millions could die. Yet if history teaches us anything it tells us that the greatest danger the human race faces is not some crackpot North Korean dictator but a six-gene virus that could wipe out one third of the global population. Our real enemy, a new plague virus, is so small you can barely see it even with an advanced electron microscope. It has no morality, no thought or no plan. All it wants to do is reproduce itself inside another human body. We are just another biological opportunity, a nice warm place to feed and replicate. Viruses are as old as life itself. What is startling though is how vulnerable our globalised societies are to the threat of a new deadly plague. Before World

### 2AC Fully Restrict (New)

#### We meet --- we prohibit unrestrained executive authority to use offensive cyber operations --- prohibition of authority is different than elimination of the activity

#### Counterinterp --- restrict is to limit not to prohibit

**Oklahoma Attorney General 04** Opinions - 3/19/2004, Question Submitted by: The Honorable Mark Campbell, District Attorney, 19th District; The Honorable Jay Paul Gumm, State Senator, District 6, 2004 OK AG 7, [http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=43849](http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=438494)

Accordingly, we must look to the plain and ordinary meaning of the term.*Webster's New International Dictionary*defines restrictions as follows: "something that restricts" and "a regulation that restricts or restrains." *Id.* at 1937 (3d ed. 1993). Restrict is defined as follows: "to set bounds or limits to: hold within bounds: as a : to check free activity, motion, progress, or departure." Id. Restrain is defined as to "prevent from doing something." *Id.* at 1936. Therefore, as used in Section 1125, "restrictions" is meant to describe those conditions of parole or probation which are intended to restrain or prevent certain conduct of the person subject thereto.

#### And authority is the permission to act not the ability to act

**Taylor, 1996**  (Ellen, 21 Del. J. Corp. L. 870 (1996), Hein Online)

The term authority is commonly thought of in the context of the law of agency, and the Restatement (Second) of Agency defines both power and authority.'89 Power refers to an agent's ability or capacity to produce a change in a legal relation (whether or not the principal approves of the change), and authority refers to the power given(permission granted) to the agent by the principal to affect the legal relations of the principal; the distinction is between what the agent can do and what the agent may do.

#### Prefer our interp ---

#### a) Overlimits --- their interp means we get four affs to choose from --- that crushes aff ground and aff creativity

#### b) Aff flexibility --- prohibit affs don’t have a defense of the process of restriction --- we need answers to the executive CP or we’ll always lose

#### c) Process education --- the topic isn’t about the object of the restriction but the different types of restrictions --- legal topic means this education is uniquely key to engaged citizenry

#### No limits explosion --- affs that limit only have a few mechanisms in which they can statutorily restrict --- that also guarantees neg ground because their links and cp’s are all based off of the mechanism for restriction

#### Reasonability is best competing interpretations lead to a race to the bottom which arbitrarily exclude the aff

### 2AC XO CP

#### **Lack of statutory clarification means we have NO DETERRENCE POSTURE the exec is in a zone of twilight – only stator clarification solves.**

Huston 11 (Warner Todd Huston Political analyst, and freelance writer, <http://www.conservativecrusader.com/articles/we-need-rules-for-cyberwarfare-before-a-president-steals-that-power-too>)

**Presidents** have had certain restrictions for war-making ever since because the founders wanted to make sure that war was something duly considered not easily engaged.

**This should** hold as much for use of computer-based warfare as it does for any other type of military attack. **Currently** computer-based war, or cyberwarfare, presents a new field of military application and we have no legal precedent to govern its use.

**Despite the last 200 years of presidents slowly stealing away power from Congress to initiate military actions, we should really think long and hard about allowing any president to unleash cyberwarfare at his discretion**. In fact, we should set a precedent immediately to prevent any president from using cyberwarfare without the consent of Congress**.**

Why? Because cyberwarfare is a far, far different animal than use of conventional military forces and indiscriminate use of it **would endanger** our way of **life** in harsh and immediate terms if used against us. For that reason, **we should be very careful when we use it against others**. We should have solid legal definitions behind its use so as not to give enemies the excuse to resort to it quickly themselves.

You see, cyberwarfare is a relatively cheap war power, easier to implement, and requires far fewer in personnel and facilities than launching an invasion using conventional military forces. This is not to say that cyberwarfare is easy -- far from it. But it is cheaper and easier than deploying regular military forces.

So, we should casually resort to cyberwarfare no more easily than we would to using conventional forces. But **if we do not set down** specific and binding rules for its use we risk giving this power over to a president which could cause less considered use of this sort of warfare. **That** in turn, would give enemies an excuse to do the same. Further, remember that setting legally binding reasons for warfare is a long and proud American tradition, one that legitimizes our nation and one we should not casually toss aside simply under the assumption that enemies will not be as thoughtful as we.

**We should lead the world in** **considered** **use of cyberwarfare** **and we should do so now**. Any of those that felt we illicitly launched into the war on terror should no less worry about indiscriminate use of cyberwarfare. But illicit use or no, **we should be** deadly certain of what powers our president can have**,** **when and how he can use them, and where the line should be drawn, even in cyberspace.**

**Only a change in CHECKS AND BALANCES solve – international distrust of US policies means the cred advantage is still a DA to the CP**

Rothschild 13 (Matthew, Feb 4, "The Danger's of Obama's Cyber War Power Grab," [www.progressive.org/dangers-of-obama-cyber-war-power-grab](http://www.progressive.org/dangers-of-obama-cyber-war-power-grab))

When our founders were drafting the Constitution, they went out of their way to give warmaking powers to Congress, not the President.

They understood that if the President could make war on his own, he’d be no different than a king.

And they also understood, as James Madison said, that such power “would be too much temptation” for one man.

And so they vested that power in Congress.

But since World War II, one President after another has usurped that power.

The latest usurper is President Obama, who did so in Libya, and with drones, and now is prepared to do so in cyberspace.

According to The New York Times, the Obama Administration has concluded that the President has the authority to launch preemptive cyberattacks.

This is a very dangerous, and very undemocratic power grab.

There are no checks or balances when the President, alone, decides when to engage in an act of war.

And this new aggressive stance will lead to a cyber arms race. The United States has evidently already used cyber weapons against Iran, and so many other countries will assume that cyber warfare is an acceptable tool and will try to use it themselves.

Most troubling, U.S. cybersupremacy—and that is Pentagon doctrine—will also raise fears among nuclear powers like Russia, China, and North Korea that the United States may use a cyberattack as the opening move in a nuclear attack.

For if the United States can knock out the command and control structure of an enemy’s nuclear arsenal, it can then launch an all-out nuclear attack on that enemy with impunity. This would make such nuclear powers more ready to launch their nuclear weapons preemptively for fear that they would be rendered useless. So we’ve just moved a little closer to midnight.

Now, I don’t think Obama would use cyberwafare as a first strike in a nuclear war. But our adversaries may not be so sure, either about Obama or his successors.

They, too, worry about the temptations of a President.

#### B) Cant solve china or Russia – lack of change in US TRANSPERENCY means they’ll still build up weapons.

Namkung 07 – Research assistant at Pacific Forum CSIS [Sun Namkung, “Overcoming Divergences,” INTERNATIONAL RELATIONS AND SECURITY NETWORK, July 2007, pg. http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ord588=grp1&ots591=0C54E3B3-1E9C-BE1E-2C24-A6A8C7060233&lng=en&id=57863] Pg. 21-22

This transparency does not exist in China. The Peoples’ Liberation Army (PLA) is secretive about its forces and its force strength. Its opacity creates concern. China may feel that since it is a “rising” state that it needs to keep its numbers ambiguous. This need for secrecy has caused many in the U.S. and in the region to call for a reexamination of its modernization and the increased military budget. Having a no first use policy does not mean much when the rest of China’s military establishment is cloaked in secrecy. The Chinese insistence on opacity is one of the reasons that East Asian nations hedge against China and why the Europeans continue their arms embargo. Declaratory policies have less value than a transparent system. In the end, China will need to become more transparent to prevent incorrect guestimates of their forces and armament capabilities by U.S. and their East Asian neighbors.

The U.S. needs to lead by example and continue to be transparent. U.S. Pacific Command Commander Adm. William Fallon was correct in pushing for military-to-military relations. The interaction between high-level and working-level officers is critical in dispelling misperceptions that Chinese forces have about the U.S. and vice versa. The divergences of U.S. and Chinese views on no first use and transparency will matter less as more visits and exercises take place comfort levels and trust is built between the two sides. As China modernizes its military, it will need to be transparent to assuage the concerns of its immediate neighbors like South Korea, Japan, and Vietnam. The increased numbers of China and U.S. bilateral and multilateral exercises show that China sees some utility in these contacts.

Policy recommendations

It is important that the U.S. and China be able to work together. The U.S. Congress should recognize that there are confidence building measures that can draw upon the trust that will be built on the increasing contact between the U.S. and Chinese militaries. Funding should be set aside to make more exercises between the U.S. forces and the PLA possible. It could also address space cooperation. More importantly the U.S. should assist China in building systems that will allow for increased transparency. One thing that prevents greater transparency is not political will, but the lack of a systematic and verifiable process to track munitions and personnel. As the Chinese are well-known to value face, the possibility of restating munitions and personnel counts could be very embarrassing to the leadership at the national and international levels.

### 2AC – Legalism

#### FW

#### Legal reforms restrain the cycle of violence and prevent error replication

Colm O’Cinneide 8, Senior Lecturer in Law at University College London, “Strapped to the Mast: The Siren Song of Dreadful Necessity, the United Kingdom Human Rights Act and the Terrorist Threat,” Ch 15 in Fresh Perspectives on the ‘War on Terror,’ ed. Miriam Gani and Penelope Mathew, <http://epress.anu.edu.au/war_terror/mobile_devices/ch15s07.html>

This ‘symbiotic’ relationship between counter-terrorism measures and political violence, and the apparently inevitable negative impact of the use of emergency powers upon ‘target’ communities, would indicate that it makes sense to be very cautious in the use of such powers. However, the impact on individuals and ‘target’ communities can be too easily disregarded when set against the apparent demands of the greater good. Justice Jackson’s famous quote in Terminiello v Chicago [111] that the United States Bill of Rights should not be turned into a ‘suicide pact’ has considerable resonance in times of crisis, and often is used as a catch-all response to the ‘bleatings’ of civil libertarians.[112] The structural factors discussed above that appear to drive the response of successive UK governments to terrorist acts seem to invariably result in a depressing repetition of mistakes.¶ However, certain legal processes appear to have some capacity to slow down the excesses of the counter-terrorism cycle. What is becoming apparent in the UK context since 9/11 is that there are factors at play this time round that were not in play in the early years of the Northern Irish crisis. A series of parliamentary, judicial and transnational mechanisms are now in place that appear to have some moderate ‘dampening’ effect on the application of emergency powers.¶ This phrase ‘dampening’ is borrowed from Campbell and Connolly, who have recently suggested that law can play a ‘dampening’ role on the progression of the counter-terrorism cycle before it reaches its end. Legal processes can provide an avenue of political opportunity and mobilisation in their own right, whereby the ‘relatively autonomous’ framework of a legal system can be used to moderate the impact of the cycle of repression and backlash. They also suggest that this ‘dampening’ effect can ‘re-frame’ conflicts in a manner that shifts perceptions about the need for the use of violence or extreme state repression.[113] State responses that have been subject to this dampening effect may have more legitimacy and generate less repression: the need for mobilisation in response may therefore also be diluted.

#### Perm – Endorse political rather than legal restrains on executive power and do the plan

#### Affective resistance isn’t sufficient. Security framing is a pre-requisite for changing authority. Liberalism can be redeemed

David COLE Law @ Georgetown ’12 “Confronting the Wizard of Oz: National Security, Expertise, and Secrecy” CONNECTICUT LAW REVIEW 44 (5) p. 1629-1633

Rana is right to focus our attention on the assumptions that frame modern Americans' conceptions about national security, but his assessment raises three initial questions. First, it seems far from clear that there ever was a "golden" era in which national security decisions were made by the common man, or "the people themselves," as Larry Kramer might put it.8 Rana argues that neither Hobbes nor Locke would support a worldview in which certain individuals are vested with superior access to the truth, and that faith in the superior abilities of so-called "experts" is a phenomenon of the New Deal era. 9 While an increased faith in scientific solutions to social problems may be a contributing factor in our current overreliance on experts,' 0 I doubt that national security matters were ever truly a matter of widespread democratic deliberation. Rana notes that in the early days of the republic, every able-bodied man had to serve in the militia, whereas today only a small (and largely disadvantaged) portion of society serves in the military." But serving in the militia and making decisions about national security are two different matters. The early days of the Republic were at least as dominated by "elites" as today. Rana points to no evidence that decisions about foreign affairs were any more democratic then than now. And, of course, the nation as a whole was far less democratic, as the majority of its inhabitants could not vote at all. 12 Rather than moving away from a golden age of democratic decision-making, it seems more likely that we have simply replaced one group of elites (the aristocracy) with another (the experts). Second, to the extent that there has been an epistemological shift with respect to national security, it seems likely that it is at least in some measure a response to objective conditions, not just an ideological development. If so, it's not clear that we can solve the problem merely by "thinking differently" about national security. The world has, in fact, become more interconnected and dangerous than it was when the Constitution was drafted. At our founding, the oceans were a significant buffer against attacks, weapons were primitive, and travel over long distances was extremely arduous and costly. The attacks of September 11, 2001, or anything like them, would have been inconceivable in the eighteenth or nineteenth centuries. Small groups of non-state actors can now inflict the kinds of attacks that once were the exclusive province of states. But because such actors do not have the governance responsibilities that states have, they are less susceptible to deterrence. The Internet makes information about dangerous weapons and civil vulnerabilities far more readily available, airplane travel dramatically increases the potential range of a hostile actor, and it is not impossible that terrorists could obtain and use nuclear, biological, or chemical weapons. 13 The knowledge necessary to monitor nuclear weapons, respond to cyber warfare, develop technological defenses to technological threats, and gather intelligence is increasingly specialized. The problem is not just how we think about security threats; it is also at least in part objectively based. Third, deference to expertise is not always an error; sometimes it is a rational response to complexity. Expertise is generally developed by devoting substantial time and attention to a particular set of problems. We cannot possibly be experts in everything that concerns us. So I defer to my son on the remote control, to my wife on directions (and so much else), to the plumber on my leaky faucet, to the electrician when the wiring starts to fail, to my doctor on my back problems, and to my mutual fund manager on investments. I could develop more expertise in some of these areas, but that would mean less time teaching, raising a family, writing, swimming, and listening to music. The same is true, in greater or lesser degrees, for all of us. And it is true at the level of the national community, not only for national security, but for all sorts of matters. We defer to the Environmental Protection Agency on environmental matters, to the Federal Reserve Board on monetary policy, to the Department of Agriculture on how best to support farming, and to the Federal Aviation Administration and the Transportation Security Administration on how best to make air travel safe. Specialization is not something unique to national security. It is a rational response to an increasingly complex world in which we cannot possibly spend the time necessary to gain mastery over all that affects our daily lives. If our increasing deference to experts on national security issues is in part the result of objective circumstances, in part a rational response to complexity, and not necessarily less "elitist" than earlier times, then it is not enough to "think differently" about the issue. We may indeed need to question the extent to which we rely on experts, but surely there is a role for expertise when it comes to assessing threats to critical infrastructure, devising ways to counter those threats, and deploying technology to secure us from technology's threats. As challenging as it may be to adjust our epistemological framework, it seems likely that even if we were able to sheer away all the unjustified deference to "expertise," we would still need to rely in substantial measure on experts. The issue, in other words, is not whether to rely on experts, but how to do so in a way that nonetheless retains some measure of self-government. The need for specialists need not preclude democratic decision-making. Consider, for example, the model of adjudication. Trials involving products liability, antitrust, patents, and a wide range of other issues typically rely heavily on experts.' 4 But critically, the decision is not left to the experts. The decision rests with the jury or judge, neither of whom purports to be an expert. Experts testify, but do so in a way that allows for adversarial testing and requires them to explain their conclusions to laypersons, who render judgment informed, but not determined, by the expert testimony. Similarly, Congress routinely acts on matters over which its members are not experts. Congress enacts laws governing a wide range of very complex issues, yet expertise is not a qualification for office. Members of Congress, like many political appointees in the executive branch, listen to and consider the views of experts to inform their decisions. Congress delegates initial consideration of most problems to committees, and by serving on those committees and devoting time and attention to the problems within their ambit, members develop a certain amount of expertise themselves. They may hire staff who have still greater expertise, and they hold hearings in which they invite testimony from still other experts. But at the end of the day, the decisions about what laws should be passed are made by the Congress as a whole, not by the experts. A similar process operates in the executive branch. The President and Vice-President generally need not be experts in any particular field, and many of the cabinet members they appoint are not necessarily experts either. They are managers and policy makers. They spend much of their day being briefed by people with more specialized expertise than they have. But at the end of the day, the important decisions are made by politically accountable actors. Thus, deference to experts need not preclude independent or democratically accountable decision-making. The larger problem may be one that Rana notes but does not sufficiently emphasize-an inordinate reliance on classified information and covert operations. 5 Secrecy is in many ways the ultimate enemy of democracy in the national security realm. 16 As Judge Damon Keith has written, "democracy dies behind closed doors.' ' 7 The experts in the intelligence community have the power to hide their decisions from external review and checks by classifying the information they consider or the actions they take.18 Even if they do so in good faith, the inevitable result is that their actions are increasingly insulated from scrutiny by others and immune from democratic checks. Virtually everyone who has had access to classified information concedes that the system leads to massive over-classification. 19 Our overreliance on secrecy may well be more central to the problem of inordinate deference than assumptions about the nature of knowledge regarding security. And in any event, the problems are mutually reinforcing. The inaccessibility of the information the experts rely upon compels us to defer to them because we lack sufficient grounds to question them. And that, in turn, may well make the experts more protective of their information and more likely to classify their actions, decisions, and considerations.

### 2AC – Prez Flex

#### Reject their impacts – it’s a laundry list – ill assert all their impacts are wrong – as much of a warrant as their li evidence

#### Disad inevitable -- the supreme court will rule on cyber

Gaskell 1/2-- Stephanie Gaskell is associate editor and senior reporter for Defense One. She previously covered the Pentagon for Politico. Gaskell has covered war, politics and breaking news for nearly 20 years, including at the Associated Press, the New York Post and the New York Daily News. She has reported from Iraq, Afghanistan, Guantanamo and the World Trade Center site after 9/11. She has also launched and edited two blogs, War Zone and The War Report (Stephanie, "Eight challenges awaiting the pentagon in 2014," nationaljournal.com, January 2, 2014, <http://www.nationaljournal.com/defense/eight-challenges-awaiting-the-pentagon-in-2014-20140102>)

Gen. Keith Alexander, the outgoing head of the National Security Agency and U.S. Cyber Command, warned this year that cyber threats are an increasing threat to the United States. "When you look at the strategic landscape from our perspective, it's getting worse," Alexander said during congressional testimony in March. New technologies – and new threats – emerge almost daily. While the Pentagon faces more budget threats in the New Year, they have pledged to protect cyber programs. There's also growing concern that a cyber threat could lead to real conflict. And 2014 will see the controversial Alexander, who was on the hot seat much of the year over the Edward Snowden leaks, exit his dual post early next year. One leading candidate to replace Alexander is Vice Admiral Michael Rogers, currently commander of the U.S. Navy's 10th Fleet and U.S. Fleet Cyber Command, according to Reuters. But it's clear that the battle between cyber secrecy and public pressure for transparency will heat up. Expect cybersecurity to head from the shadows to the Supreme Court, as 2013 closed with a federal judge warning that the NSA's core mission could be a Constitutional violation.

#### 3) No link or Internal link – the plan doesn’t sacrifice all prez flex – AUMF gives self D war authority

**Greenwald 13** – Columnist on civil liberties and US national security issues for the Guardian. [[Glenn Greenwald](http://www.theguardian.com/profile/glenn-greenwald), “Washington gets explicit: its 'war on terror' is permanent,”  [theguardian.com](http://www.theguardian.com/), Friday 17 May 2013 07.54 EDT, pg. http://www.theguardian.com/commentisfree/2013/may/17/endless-war-on-terror-obama

On Thursday, the Senate Armed Services Committee held a hearing on whether the statutory basis for this "war" - the **2001 Authorization to Use Military Force (AUMF)** - should be revised (meaning: expanded). [This is how](http://www.wired.com/dangerroom/2013/05/decades-of-war/) Wired's Spencer Ackerman (soon to be the Guardian US's national security editor) described the most significant exchange:

"Asked at a Senate hearing today how long the war on terrorism will last, Michael Sheehan, the assistant secretary of defense for special operations and low-intensity conflict, answered, 'At least 10 to 20 years.' . . . A spokeswoman, Army Col. Anne Edgecomb, clarified that Sheehan meant the conflict is likely to last 10 to 20 more years from today - atop the 12 years that the conflict has already lasted. Welcome to America's Thirty Years War."

That the **Obama** administration **is now repeatedly declaring that the "war on terror" will last at least another decade (or two) is** vastly more **significant** than all three of this week's big media controversies (Benghazi, IRS, and AP/DOJ) combined. The **military historian** Andrew **Bacevich has** [spent years warning](http://www.nytimes.com/2010/09/05/books/review/Bass-t.html) **that US policy planners have adopted an explicit doctrine of "**endless war**"**. **Obama officials**, despite [repeatedly boasting](http://abcnews.go.com/blogs/headlines/2012/04/al-qaeda-shadow-of-former-self/) that they have delivered [permanently crippling blows to al-Qaida](http://www.wired.com/dangerroom/2013/03/spy-terrorism/), **are now**, as clearly as the English language permits, **openly declaring this to be so**.

It is hard to resist the conclusion that **this war has no purpose other than its own eternal perpetuation**. **This war is not a means to any end but rather is the end in itself**. Not only is it the end itself, but it is also its own fuel: it is precisely this endless war - justified in the name of stopping the threat of terrorism - that is the single greatest cause of that threat.

In January, former Pentagon general counsel Jeh Johnson delivered a highly-touted speech suggesting that the war on terror will eventually end; he advocated that outcome, arguing:

**'War' must be regarded as a finite, extraordinary and unnatural state of affairs. We must not accept the current conflict**, and all that it entails, **as the** 'new normal**.**'"   
In response, [I wrote that](http://www.guardian.co.uk/commentisfree/2013/jan/04/war-on-terror-endless-johnson) **the "war on terror"** cannot and **will not end on its own** for two reasons: (1) it is designed by its very terms to be permanent, incapable of ending, **since the war itself ironically ensures that there will never come a time when people stop wanting to bring violence back to the US (the operational definition of "terrorism"),** **and** (2) **the nation's most powerful political and economic factions reap a bonanza of benefits from its continuation**. Whatever else is true, it is now beyond doubt that ending this war is the last thing on the mind of the 2009 Nobel Peace Prize winner and those who work at the highest levels of his administration. Is there any way they can make that clearer beyond declaring that it will continue for "at least" another 10-20 years?

The genius of America's endless war machine is that, learning from the unplesantness of the Vietnam war protests, it has rendered the costs of war largely invisible. That is accomplished by heaping all of the fighting burden on [a tiny](http://ggsidedocs.blogspot.com.br/2013/05/who-bears-fighting-burden.html) and [mostly economically marginalized faction](http://www.washingtonpost.com/wp-dyn/content/article/2005/11/03/AR2005110302528.html) of the population, by using sterile, mechanized instruments to deliver the violence, and by suppressing any real discussion in establishment media circles of America's innocent victims and the [worldwide anti-American rage](http://www.pewglobal.org/2012/06/13/global-opinion-of-obama-slips-international-policies-faulted/) that [generates](http://www.salon.com/2011/07/13/arabs/).

Though rarely visible, the costs are nonetheless gargantuan. Just in financial terms, as Americans are told they must sacrifice Social Security and Medicare benefits and place their children in a crumbling educational system, the Pentagon [remains the world's largest employer](http://www.bbc.co.uk/news/magazine-17429786) and continues to [militarily outspend the rest of the world by a significant margin](http://www.globalissues.org/article/75/world-military-spending). The mythology of the Reagan presidency is that he induced the collapse of the Soviet Union by luring it into unsustainable military spending and wars: should there come a point when we think about applying that lesson to ourselves?

Then there are the threats to Americans' security. **Having their government spend decades** proudly **touting itself as "A Nation at War" and bringing horrific violence to the world is certain to prompt more and more people to want to attack Americans**, as the [US government itself claims took place just recently in Boston](http://www.guardian.co.uk/world/2013/may/16/dzhokhar-tsarnaev-message-boat-cbs-news) (and as [clearly took place multiple other times over the last several years](http://www.guardian.co.uk/commentisfree/2013/apr/24/boston-terrorism-motives-us-violence)).

And then there's the most intangible yet most significant cost: **each year of endless war that passes further** normalizes the endless rights erosions **justified in its name**. The second term of the **Bush** administration **and** first five years of the **Obama** presidency **have been devoted to codifying and institutionalizing the vast and unchecked powers that are** typically **vested in leaders in the name of war**. **Those powers of** secrecy, indefinite detention, mass surveillance, and due-process-free assassination **are not going anywhere**. **They are** now permanent fixturesnot only in the US political system but, worse, **in** American political culture**.**

### 2AC – PTX

#### Your authors overstate the risks and pace of Middle East proliferation

Carpenter 7 [Ted Galen, Vice President for Defense and Foreign Policy Studies—Cato, Mediterranean Quarterly, “Toward a Grand Bargain with Iran,” Vol. 18, Iss. 1, Project Muse]

Finally, those who favor a more confrontational policy toward Iran warn that if Tehran succeeds in its quest for nuclear weapons, other nations in the region will quickly do the same, creating an especially dangerous security environment. As in the case of concerns about possible blackmail, this fear has some validity. Because of the uncertain reliability of the protection afforded by the US umbrella for some US allies and client states in the Middle East, there is a very real prospect that if Iran develops a nuclear arsenal, sooner or later such countries as Saudi Arabia, Egypt, and Turkey might follow suit. Indeed, Egypt may already be thinking along those lines. In late September, Gamal Mubarak, President Hosni Mubarak's son and political heir apparent, stated that his country needed to develop a nuclear program for power generation.19 Although he stressed that the program would be entirely peaceful, his proposal had all the earmarks of a hedging strategy. As we have seen with India, Pakistan, North Korea, and Iran, "peaceful" nuclear programs can easily become the foundation for a nuclear weapons program. Whether additional proliferation would reach epidemic proportions and create the nightmare scenarios forecast by some analysts is uncertain. It is important to recall that pundits and even international relations experts have tended to overestimate both the probability and the extent of proliferation in the past. The conventional wisdom in the 1960s was that there would be as many as two dozen nuclear weapons powers within a generation.20 Similar predictions took place in the late 1970s and early 1980s.21 [End Page 22] Moreover, it is not an established fact that nuclear weapons in the hands of a larger number of nations would necessarily be a bad development. Indeed, some respected International Relations scholars have argued that nuclear proliferation might be stabilizing rather than destabilizing.22 Given its volatile political makeup, though, the Middle East is probably not the best region to test that thesis.

#### Nuclear Iran doesn't change anything

Walt 12 [Stephen M, professor of international relations at Harvard, "The mother of all worst-case assumptions about Iran," 11-30, http://walt.foreignpolicy.com/category/topic/nukes]

The debate on Iran and its nuclear program does little credit to the U.S. foreign policy community, because much of it rests on dubious assumptions that do not stand up to even casual scrutiny. Lots of ink, pixels, and air-time has been devoted to discussing whether Iran truly wants a bomb, how close it might be to getting one, how well sanctions are working, whether the mullahs in charge are "rational," and whether a new diplomatic initiative is advisable. Similarly, journalists, politicians and policy wonks spend endless hours asking if and when Israel might attack and whether the United States should help. But we hardly ever ask ourselves if this issue is being blown wildly out of proportion. At bottom, the whole debate on Iran rests on the assumption that Iranian acquisition of a nuclear weapon would be an event of shattering geopolitical significance: On a par with Hitler's rise to power in Germany in 1933, the fall of France in 1940, the Sino-Soviet split, or the breakup of the former Soviet Union. In this spirit, Henry Kissinger recently argued that a latent Iranian capability (that is, the capacity to obtain a bomb fairly quickly) would have fearsome consequences all by itself. Even if Iran stopped short of some red line, Kissinger claims this would: 1) cause "uncontrollable military nuclear proliferation throughout [the] region," 2) "lead many of Iran's neighbors to reorient their political alignment toward Tehran" 3) "submerge the reformist tendencies in the Arab Spring," and 4) deliver a "potentially fatal blow" to hopes for reducing global nuclear arsenals. Wow. And that's just if Iran has nuclear potential and not even an actual weapon! It follows that the United States must either persuade them to give up most of their enrichment capacity or go to war to destroy it. Yet this "mother of all assumptions" is simply asserted and rarely examined. The obvious question to ask is this: did prior acts of nuclear proliferation have the same fearsome consequences that Iran hawks now forecast? The answer is no. In fact, the spread of nuclear weapons has had remarkably little impact on the basic nature of world politics and the ranking of major powers. The main effect of the nuclear revolution has been to induce greater caution in the behavior of both those who possessed the bomb and anyone who had to deal with a nuclear-armed adversary. Proliferation has not transformed weak states into influential global actors, has not given nuclear-armed states the ability to blackmail their neighbors or force them to kowtow, and it has not triggered far-reaching regional arms races. In short, fears that an Iranian bomb would transform regional or global politics have been greatly exaggerated; one might even say that they are just a lot of hooey. Consider the historical record. Did the world turn on its axis when the mighty Soviet Union tested its first bomb in 1949? Although alarmist documents like NSC-68 warned of a vast increase in Soviet influence and aggressiveness, Soviet nuclear development simply reinforced the caution that both superpowers were already displaying towards each other. The United States already saw the USSR as an enemy, and the basic principles of containment were already in place. NATO was being formed before the Soviet test and Soviet dominance of Eastern Europe was already a fait accompli. Having sole possession of the bomb hadn't enabled Truman to simply dictate to Stalin, and getting the bomb didn't enable Stalin or his successors to blackmail any of their neighbors or key U.S. allies. It certainly didn't lead any countries to "reorient their political alignment toward Moscow." Nikita Khrushchev's subsequent missile rattling merely strengthened the cohesion of NATO and other U.S.-led alliances, and we now know that much of his bluster was intended to conceal Soviet strategic inferiority. Having a large nuclear arsenal didn't stop the anti-commnist uprisings in East Germany, Hungary, Czechoslovakia, or Poland, and didn't allow the Soviet Union to win in Afghanistan. Nor did it prevent the USSR from eventually collapsing entirely. Did British and French acquisition of nuclear weapons slow their decline as great powers? Not in the slightest. Having the force de frappe may have made De Gaulle feel better about French prestige and having their own deterrent made both states less dependent on America's security umbrella, but it didn't give either state a louder voice in world affairs or win them new influence anywhere. And you might recall that Britain couldn't get Argentina to give back the Falklands by issuing nuclear threats -- even though Argentina had no bomb of its own and no nuclear guarantee -- they had to go retake the islands with conventional forces. Did China's detonation of a bomb in 1964 suddenly make them a superpower? Hardly. China remained a minor actor on the world stage until it adopted market principles, and its rising global influence is due to three decades of economic growth, not a pile of nukes. And by the way, did getting a bomb enable Mao Zedong--a cruel megalomaniac who launched the disastrous Great Leap Forward in 1957 and the destructive Cultural Revolution in the 1960s -- to start threatening and blackmailing his neighbors? Nope. In fact, China's foreign policy behavior after 1964 was generally quite restrained. What about Israel? Does Israel's nuclear arsenal allow it to coerce its neighbors or impose its will on Hezbollah or the Palestinians? No. Israel uses its conventional military superiority to try to do these things, not its nuclear arsenal. Indeed, Israel's bomb didn't even prevent Egypt and Syria from attacking it in October 1973, although it did help convince them to limit their aims to regaining the territory they had lost in 1967. It is also worth noting that Israel's nuclear program did not trigger a rapid arms race either. Although states like Iraq and Libya did establish their own WMD programs after Israel got the bomb, none of their nuclear efforts moved very rapidly or made it across the finish line. But wait, there's more. The white government in South Africa eventually produced a handful of bombs, but nobody noticed and apartheid ended anyway. Then the new government gave up its nuclear arsenal to much acclaim. If anything, South Africa was more secure without an arsenal than it was before. What about India and Pakistan? India's "peaceful nuclear explosion" in 1974 didn't turn it into a global superpower, and its only real effect was to spur Pakistan -- which was already an avowed rival -- to get one too. And it's worth noting that there hasn't been a large-scale war between the two countries since, despite considerable grievances on both sides and occasional skirmishes and other provocations. Finally, North Korea is as annoying and weird as it has always been, but getting nuclear weapons didn't transform it from an economic basket case into a mighty regional power and didn't make it more inclined to misbehave. In fact, what is most remarkable about North Korea's nuclear program is how little impact it has had on its neighbors. States like Japan and South Korea could go nuclear very quickly if they wanted to, but neither has done so in the six years since North Korea's first nuclear test. In short, both theory and history teach us that getting a nuclear weapon has less impact on a country's power and influence than many believe, and the slow spread of nuclear weapons has only modest effects on global and regional politics. Nuclear weapons are good for deterring direct attacks on one's homeland, and they induce greater caution in the minds of national leaders of all kinds. What they don't do is turn weak states into great powers, they are useless as tools of blackmail, and they cost a lot of money. They also lead other states to worry more about one's intentions and to band together for self-protection. For these reasons, most potential nuclear states have concluded that getting the bomb isn't worth it. But a few states-and usually those who are worried about being attacked-decide to go ahead. The good news is that when they do, it has remarkably little impact on world affairs. For some strange reason, however, the U.S. national security community seems to think that both logic and all this prior history does not apply to Iran. They forget that similarly dire warnings were uttered before many of these others states got the bomb, yet none of these fearsome forecasts took place. Ironically, by repeatedly offering doom-and-gloom scenarios about the vast geopolitical consequences of an Iranian bomb, they may be strengthening the hands of Iranian hardliners who might be interested in actually obtaining a working weapon. After all, if getting a bomb would give Iran all the influence that Kissinger and others fear, why wouldn't Tehran want one?

#### Dire proliferation predictions never come true—a nuclear Iran would establish stability in the region—empirically proved

Van Creveld 6 [Martin, Prof. Military History—Hebrew U., The Forward, “Knowing Why Not to Bomb Iran Is Half the Battle”, 4-26, http://www.d-n-i.net/creveld/to\_bomb\_iran.htm]

The first and most obvious question is whether it is worth doing in the first place. Starting right after Hiroshima, each time a country was about to go nuclear Washington went out of its way to sound the alarm, warning of the dire consequences that would surely follow. From 1945 to 1949 it was the Soviet Union which, once it had succeeded in building nuclear weapons, was supposed to make an attempt at world conquest. In the 1950s it was America's own clients, Britain and France, who were regarded as the offenders and put under pressure. Between 1960 and 1993, first China, then Israel (albeit to a limited extent) and finally India and Pakistan were presented as the black sheep, lectured, put under pressure and occasionally subjected to sanctions. Since then, the main victim of America's peculiar belief that it alone is sufficiently good and sufficiently responsible to possess nuclear weapons has been North Korea. As the record shows, in none of these cases did the pessimists' visions come true. Neither Stalin, Mao nor any of the rest set out to conquer the world. It is true that, as one country after another joined the nuclear club, Washington's ability to threaten them or coerce them declined. However, nuclear proliferation did not make the world into a noticeably worse place than it had always been — and if anything, to the contrary. As Europe, the Middle East and South Asia demonstrate quite well, in one region after another the introduction of nuclear weapons led, if not to brotherhood and peace, then at any rate to the demise of large-scale warfare between states. Given the balance of forces, it cannot be argued that a nuclear Iran will threaten the United States. Iranian President Mahmoud Ahmadinejad's fulminations to the contrary, the Islamic Republic will not even be a threat to Israel. The latter has long had what it needs to deter an Iranian attack. Should deterrence fail, Jerusalem can quickly turn Tehran into a radioactive desert — a fact of which Iranians are fully aware. Iran's other neighbors, such as Russia, Pakistan and India, can look after themselves. As it is, they seem much less alarmed by developments in Iran than they do by those thousands of miles away in Washington.

#### Iranian nuclearization will be rational, restrained and promote stability

Waltz 12 [Kenneth, Prof. Emeritus of Pol. Sci – UC Berkeley, "Why Iran Should Get the Bomb," Foreign Affairs, Jul/Aug, Vol 91, Issue 4]

One reason the danger of a nuclear Iran has been grossly exaggerated is that the debate surrounding it has been distorted by misplaced worries and fundamental misunderstandings of how states generally behave in the international system. The first prominent concern, which undergirds many others, is that the Iranian regime is innately irrational. Despite a widespread belief to the contrary, Iranian policy is made not by "mad mullahs" but by perfectly sane ayatollahs who want to survive just like any other leaders. Although Iran's leaders indulge in inflammatory and hateful rhetoric, they show no propensity for self-destruction. It would be a grave error for policymakers in the United States and Israel to assume otherwise. Yet that is precisely what many U.S. and Israeli officials and analysts have done. Portraying Iran as irrational has allowed them to argue that the logic o fnuclear deterrence does not apply to the Islamic Republic. If Iran acquired a nuclear weapon, they warn, it would not hesitate to use it in a first strikeagainst Israel, even though doing so would invite massive retaliation and risk destroying everything the Iranian regime holds dear. Although it is impossible to be certain of Iranian intentions, it is far more likely that if Iran desires nuclear weapons, it is for the purpose of providing for its own security, not to improve its offensive capabilities (or destroy itself). Iran may be intransigent at the negotiating table and defiant in the face of sanctions, but it still acts to secure its own preservation. Iran's leaders did not, for example, attempt to close the Strait of Hormuz despite issuing blustery warnings that they might do so after the EU announced its planned oil embargo in January. The Iranian regime clearly concluded that it did not want to provoke what would surely have been a swift and devastating American response to such a move. Nevertheless, even some observers and policymakers who accept that the Iranian regime is rational still worry that a nuclear weapon would embolden it, providing Tehran with a shield that would allow it to act more aggressively and increase its support for terrorism. Some analysts even fear that Iran would directly provide terrorists with nuclear arms. The problem with these concerns is that they contradict the record of every other nuclear weapons state going back to 1945. History shows that when countries acquire the bomb, they feel increasingly vulnerable and become acutely aware that their nuclear weapons make them a potential target in the eyes of major powers. This awareness discourages nuclear states from bold and aggressive action. Maoist China, for example, became much less bellicose after acquiring nuclear weapons in 1964, and India and Pakistan have both become more cautious since going nuclear. There is little reason to believe Iran would break this mold. As for the risk of a handoff to terrorists, no country could transfer nuclear weapons without running a high risk of being found out. U.S. surveillance capabilities would pose a serious obstacle, as would the United States' impressive and growing ability to identify the source of fissile material. Moreover, countries can never entirely control or even predict the behavior of the terrorist groups they sponsor. Once a country such as Iran acquires a nuclear capability, it will have every reason to maintain full control over its arsenal. After all, building a bomb is costly and dangerous. It would make little sense to transfer the product of that investment to parties that cannot be trusted or managed. Another oft-touted worry is that if Iran obtains the bomb, other states in the region will follow suit, leading to a nuclear arms race in the Middle East. But the nuclear age is now almost 70 years old, and so far, fears of proliferation have proved to be unfounded. Properly defined, the term "proliferation" means a rapid and uncontrolled spread. Nothing like that has occurred; in fact, since 1970, there has been a marked slowdown in the emergence of nuclear states. There is no reason to expect that this pattern will change now. Should Iran become the second Middle Eastern nuclear power since 1945, it would hardly signal the start of a landslide. When Israel acquired the bomb in the 1960s, it was at war with many of its neighbors. Its nuclear arms were a much bigger threat to the Arab world than Iran's program is today. If an atomic Israel did not trigger an arms race then, there is no reason a nuclear Iran should now. [REST ASSURED](http://web.ebscohost.com.proxy.library.emory.edu/ehost/detail?sid=0d12f3e9-d5a5-40c2-b5a5-0bbb91169c98%40sessionmgr115&vid=2&hid=125&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#toc) In 1991, the historical rivals India and Pakistan signed a treaty agreeing not to target each other's nuclear facilities. They realized that far more worrisome than their adversary's nuclear deterrent was the instability produced by challenges to it. Since then, even in the face of high tensions and risky provocations, the two countries have kept the peace. Israel and Iran would do well to consider this precedent. If Iran goes nuclear, Israel and Iran will deter each other, as nuclear powers always have. There has never been a full-scale war between two nuclear-armed states. Once Iran crosses the nuclear threshold, deterrence will apply, even if the Iranian arsenal is relatively small. No other country in the region will have an incentive to acquire its own nuclear capability, and the current crisis will finally dissipate, leading to a Middle East that is more stable than it is today.

# 1AR

### Impacts

#### No Iran prolif and the timeframe is huge

Kahl 12 [Colin, Associate Professor at Georgetown University's Edmund A. Walsh School of Foreign Service and former Deputy Assistant Secretary of Defense for the Middle East, March/April, “Not Time to Attack Iran,” *Foreign Affairs*, Vol. 91 No. 2]

Kroenig argues that there is an urgent need to attack Iran's nuclear infrastructure soon, since Tehran could "produce its first nuclear weapon within six months of deciding to do so." Yet that last phrase is crucial. The International Atomic Energy Agency (IAEA) has documented Iranian efforts to achieve the capacity to develop nuclear weapons at some point, but there is no hard evidence that Supreme Leader Ayatollah Ali Khamenei has yet made the final decision to develop them. In arguing for a six-month horizon, Kroenig also misleadingly conflates hypothetical timelines to produce weapons-grade uranium with the time actually required to construct a bomb. According to 2010 Senate testimony by James Cartwright, then vice chairman of the U.S. Joint Chiefs of Staff, and recent statements by the former heads of Israel's national intelligence and defense intelligence agencies, even if Iran could produce enough weapons-grade uranium for a bomb in six months, it would take it at least a year to produce a testable nuclear device and considerably longer to make a deliverable weapon. And David Albright, president of the Institute for Science and International Security (and the source of Kroenig's six-month estimate), recently told Agence France-Presse that there is a "low probability" that the Iranians would actually develop a bomb over the next year even if they had the capability to do so. Because there is no evidence that Iran has built additional covert enrichment plants since the Natanz and Qom sites were outed in 2002 and 2009, respectively, any near-term move by Tehran to produce weapons-grade uranium would have to rely on its declared facilities. The IAEA would thus detect such activity with sufficient time for the international community to mount a forceful response. As a result, the Iranians are unlikely to commit to building nuclear weapons until they can do so much more quickly or out of sight, which could be years off.

#### Empirics clearly disprove the domino effect

Hobbs and Moran 12 [Christopher, Leverhulme Research Fellow at the Centre for Science and Security Studies within the Department of War Studies at King's College London, and Matthew, Research Associate at the Centre for Science and Security Studies within the Department of War Studies at King's College London, December 19, “Would a Nuclear Iran Really Trigger a New Arms Race in the Middle East?” http://www.guardian.co.uk/world/julian-borger-global-security-blog/2012/dec/19/iran-nuclear-middle-east-arms-race]

Inevitably, Iran's nuclear defiance has provided ammunition for the war-mongerers advocating a pre-emptive attack on Iran. Prominent commentators such as Matthew Kroenig, claim that, at the very least, a nuclear-armed Iran would prompt a 'proliferation cascade' in the Middle East. If Iran acquires nuclear weapons – whatever form that scenario may take - its regional rivals will follow suit. The argument here is seductive; it is easier to assume the worst than to hope for the best. The problem is, we find that the counter-argument is more compelling. The idea that 'proliferation begets proliferation' is not new. Dire forecasts on the seemingly inevitable increase in the number of nuclear weapon states have been made since the dawn of the nuclear age. In 1963, for example, US President JF Kennedy predicted that there might be up to twenty-five nuclear weapons powers within the next decade. However, proliferation has proven to be historically rare, with the number of nuclear weapons states expanding only slightly from five in 1964 to nine in 2006 following North Korea's nuclear test. The flawed logic of 'proliferation begets proliferation' is clearly demonstrated in North East Asia where North Korea's nuclear weapons have not provoked Japan or South Korea, countries with advanced civil nuclear programmes, to follow suit despite a long history of regional conflict and volatile relations. In this case, strong security alliances with the United States incorporating extended nuclear deterrence have played an important role in dissuading these countries from going nuclear. Ironically, the Middle East itself offers further evidence that nuclear proliferation is not inevitable. Noted for its policy of nuclear opacity (neither confirming nor denying its nuclear arsenal), Israel acquired nuclear weapons in the late 1960s and over four decades later still remains the only nuclear power in the region. Now the threat posed by Iran to its neighbours is arguably greater given Tehran's aggressive posturing and regional ambitions. However our research finds that those states deemed most likely to go nuclear due to their proximity to Iran and their suspected past interest in acquiring nuclear weapons (namely Turkey, Egypt, Syria and Saudi Arabia), would have little to gain and much to lose by embarking down such a route. Take Saudi Arabia, for example. Iran has long been at political and ideological odds with the kingdom across the Gulf. And at first sight, it seems likely that Saudi Arabia would follow Iran down the nuclear path. In February, Saudi officials were reported as claiming that Riyadh would launch a "twin-track nuclear weapons programme" in the event of a successful Iranian nuclear test. An article published in the London Times in February [£] described a scenario whereby Saudi Arabia would attempt to purchase warheads from abroad while also adding a military dimension to its planned civil nuclear programme at home. Look more closely, however, and there is a much stronger case to be made against Saudi nuclearisation. Beyond the Kingdom's primitive nuclear infrastructure – the country lacks sufficient experience and expertise in practically all areas of the nuclear fuel cycle – Saudi Arabia's political and strategic context does not favour the acquisition of nuclear weapons. From a security perspective, the relationship between Saudi Arabia and the United States has held firm since the 1940s, despite a number of challenges – most notably the participation of a number of Saudi nationals in the 9/11 terrorist attacks. The relationship barters Saudi oil for US conventional arms and an implicit commitment to Saudi's defence. In recent years, the role of Washington as the silent guarantor of Riyadh's security has grown apace with the structural changes in the Middle East. The fall of the pro-Saudi Mubarak regime in Egypt; protests and instability in Bahrain and Yemen; the collapse of the pro-Saudi government in Lebanon; and civil war in Syria have upended the established regional order and made Riyadh's position less secure. In this context, and given the determination of the United States to prevent nuclear proliferation in the region, a move by Saudi Arabia to acquire nuclear weapons holds few positives for Riyadh's security calculus. From and economic perspective, Saudi Arabia's policy outlook exemplifies Etel Solingen's seminal theory on the relationship between economic liberalism and nuclear restraint. Solingen argues that political coalitions favouring the reduction of state control over markets and increased privatisation and foreign investment – are less likely to adopt a nuclear posture that would endanger their economic interests. In this regard, Saudi Arabia's emphasis on facilitating the growth of foreign investment is significant. Riyadh has cultivated extensive trade relations with most international powers, keen to attract foreign investment as a means of reducing over-reliance on oil and gas, increasing employment opportunities for the local population (population growth of almost two percent equates to a need for some 200,000 new jobs per year), and reinvigorating the Saudi private sector. The acquisition of nuclear weapons would have far-reaching consequences, stalling progress and bringing progressive economic isolation, thus drastically changing the nature of the kingdom's international trade relations. Saudi's interests are best served by nuclear restraint. In an article published in the latest issue of The International Spectator, we argue that there are strong arguments for nuclear restraint in the cases of other regional players as well. From security guarantees and the provision of advanced conventional weapons - in December 2011, following the United States agreed a $1.7 billion deal to upgrade Saudi Arabia's Patriot missile defence system, for example – to facilitating increased integration into the international economy, there are a range of measures that can persuade a state to forgo nuclear weapons. Ultimately, many see a domino-effect as the logical response to Iranian nuclearisation. But when the stakes are this high, it is important to look at all sides of the debate. From another perspective, there is substantial evidence to suggest that regional proliferation is not a very likely outcome at all.

### A2 Aggression

#### Turn: Nuclear Iran triggers moderation of social and foreign policy

Sadr 5 [Ehsaneh, Graduate Student in Government and Politics—Maryland, Middle East Policy, “THE IMPACT OF IRAN’S NUCLEARIZATION ON ISRAEL,” Vol. XII, No. 2, Summer, p. 68]

Prospects for regime change or reform from within will not, however, be negatively affected by Iran’s nuclearization. Indeed, as mentioned above, the process of elite socialization to the facts of nuclear life would moderate calls for provocative anti- Israeli or anti-American behavior, contributing to the de-radicalization of the regime as a whole.

#### Moderates solve war—Central Asia and the Middle East

Copley 6 [Gregory, President of the International Strategic Studies Association, Defense & Foreign Affairs Strategic Policy, “Iran's Delicate Year of Living Dangerously”, Vol. 34, Iss. 1, Proquest]

IRAN IS THE DYNAMIC ELEMENT in the current global geopolitical framework; it is the driver, financier, safe-haven and logistical font for international jihadist terrorism, without which the Salafist-oriented terrorist groups and the Shi'ite Hizb Allah and other groups could not be effective. But it is also a dynamic element in the global geopolitical matrix at this time, quite apart from its covert sponsorship of terrorism, because of the prospect that Iran's clerical leadership will, in the coming year, undertake direct, overt adventures which will result in open warfare with Israel, the US, European states (through Bosnia), and/or others in the Persian Gulf. The sole reason for Iran's strident support for jihadist warfare against the West, and its direct and open confrontation with the US and Israel is the need for the clerics to legitimize their rule and obtain the subservience of the Iranian people. The Iranian clerics rode to power in 1979 not on a "revolution" of their own making, but on the collapse of the Shah's Government through international intervention and the Shah's ill-health. The clerics found themselves placed at the head of a basically leaderless mob, which had been whipped up by Soviet funding and US (Carter Administration) maneuvering. The clerics never subsequently gained popular support, and even by their own reckoning and with forced voting by civil servants in the 2005 Presidential elections, could not bring out more than a small percentage of the Iranian population to vote for a carefully-engineered slate of clerical candidates. Despite repression, Iranians have consistently denied approval to the clerics. In 1982, when the first clerical ruler, "Ayatollah" Ruhollah Khomeini, was about to be swept from power by a popular uprising, his response was to embrace a war with neighboring Iraq, in order to play on the historically strong Iranian patriotism. He succeeded in ensuring that the Iranian population would not work against the government of the day in a time of crisis. But the people paid a huge price in the number of dead, injured, and impoverished kin they suffered for their nationalism. All of Iran's clerics—'though they now compete with each other in a bitter feud—agree that a new war, or the threat of a new war, is needed to repeat the example which Khomeini set. And so Pres. Mahmud Ahmadi-Nejad courts war, when clearly Iran could have a brilliant future as one of the great, rising powers of the post-globalism era. Ahmadi-Nejad and his colleagues, including "Supreme Leader" Ali Hoseini-Khamene'i and former Pres. Ali Akbar Hashemi-Rafsanjani, are all prepared to sacrifice Iranian lives, and Iran's economic and political future (even to the point of the break-up of Iran), in order to save their positions. The claims of messianic mission, either for Islam as a whole or for Shi'ism in particular, or even for Iran, are without foundation; they are theater to disguise the goal of job security for the clerics. It is significant, then, that US Pres. George W. Bush, in his State of the Union speech to Congress on January 31, 2006, resisted the trap which the Iranian clerics laid for him; the trap of accepting the challenge of war. Many US military policy officials, whose task it is to prepare their country to face military challenges, had accepted that armed conflict with Iran was inevitable. That it may occur because of the desperation of the clerics is possible, but that it should occur because the US or Israel, for example, accepted the clerical challenge is quite another. Pres. Bush, in an earlier State of the Union speech, in 1993, noted: "In Iran, we continue to see a government that represses its people, pursues weapons of mass destruction, and supports terror. We also see Iranian citizens risking intimidation and death as they speak out for liberty and human rights and democracy. Iranians, like all people, have a right to choose their own government and determine their own destiny—and the United States supports their aspirations to live in freedom." He repeated that sentiment in his January 31, 2006, State of the Union speech, but this time added: "Tonight, let me speak directly to the citizens of Iran: America respects you, and we respect your country. We respect your right to choose your own future and win your own freedom. And our nation hopes one day to be the closest of friends with a free and democratic Iran." This brief section of his speech was of profound importance, and was a direct signal to the Iranian people to take the initiative in removing the clerics. The Bush Administration did not remove the military option for dealing with the clerics, but it opened the strategic battlefield to more positive solutions. Significantly, most US analysts paid little attention to Pres. Bush's comments, but the Iranian population understood. The Bush White House clearly recognizes that the debate over Iranian nuclear weapons is largely a political-diplomatic set piece which has little to do with reality. It suits the purposes of the West to deny that Iran has nuclear weapons at this time, despite the clear intelligence that it has probably eight to 12 warheads deployed, along with a viable first- and second-strike capability to deliver them, and other strategic payloads. By refusing to acknowledge Iran's (and North Korea's, for that matter) military nuclear capabilities, the US is able to adopt methods of confronting the leadership of Iran (and the DPRK) with methods short of a conflict based on Tehran's timetable. Significantly, in order to achieve a "poison pill" defense—the open recognition of their military nuclear capability—the Iranian and North Korean leaderships have been increasingly daring in signals showing their nuclear deterrents. Yet they have thus far failed to goad the US and the West in to accepting a showdown on Tehran's, or Pyongyang's, terms. But this "bought time" is only valuable if it is used to promote a "strategic situational change" by other means: internal, popular action in Iran. [The challenge is different in the DPRK, but, then, North Korea is strategically and vitally linked to the clerical Iranian leadership.] Pres. Bush—the most clear representative of US intent—expressed his support for the Iranian people in a totally unambiguous manner. Had earlier US presidents Franklin Roosevelt and Harry Truman, in 1944 and 1945, dropped their supposed insistence on "unconditional surrender" by Germany and Japan, and instead focused on dividing the German and Japanese populations—always, as history later proved, potential allies of the US—from their dictatorial leaderships, then World War II may have ended sooner and with less cost. How quickly can the US, the West, and Israel, follow upon this new opening to the Iranian people? At stake is the pivotal geopolitical heartland. A prosperous, independent, and moderate Iran best facilitates the security and prosperity not only of the US, but even more directly the stability and future of Russia, the People's Republic of China, Europe, the Middle East, Caucasus and Central Asia. It also paves the way for the strategic-economic rise of the Indian Ocean basin in the 21st Century.

#### Central Asia war goes global

Blank 98 [Stephen, Prof. Research—Strategic Studies Institute of US Army War College, Jane’s Intelligence Review, 5-1]

Many of the conditions for conventional war or protracted ethnic conflict in which third parties intervene are present in the Transcaucasus. For example, many Third World conflicts generated by local structural factors have a great potential for unintended escalation. Big powers often feel obliged to rescue their lesser proteges and proxies. One or another big power may fail to grasp the other side's stakes, since interests here are not as clear as in Europe. Hence commitments involving the use of nuclear weapons to prevent a client's defeat are not well established or clear as in Europe. Clarity about the nature of the threat could prevent the kind of rapid and almost uncontrolled escalation we saw in 1993 when Turkish noises about intervening on behalf of Azerbaijan led Russian leaders to threaten a nuclear war in that case. Precisely because Turkey is a NATO ally but probably could not prevail in a long war against Russia—or if it could, would trigger a potential nuclear blow (not a small possibility given the erratic nature of Russia's declared nuclear strategies)—the danger of major war is higher here than almost everywhere else.

### A2 – Israel Strike

#### Won't strike

Harel 2-12 [Amos, graduate of Tel Aviv University, military correspondent and defense analyst for Haaretz "Israel unlikely to attack Iran before summer, senior officials say," 2-12, <http://www.haaretz.com/print-edition/news/israel-unlikely-to-attack-iran-before-summer-senior-officials-say.premium-1.502969>]

Given these circumstances, the United States expects Israel not to interfere. Prime Minister Benjamin Netanyahu, who has refrained from ordering military action at several previous decision points in recent years, will have to take the views of his American visitor into account. Finally, Netanyahu must take three other things into account: the vehement opposition by defense establishment professionals to any attack at this point in time that isn't coordinated with Washington; the agenda of the party expected to be his main partner in his next government (the people who voted for Yair Lapid's Yesh Atid party wanted to bring about socioeconomic change, not open up a new military front ); and perhaps also the views of his next defense minister, whoever that may be. It's doubtful that Netanyahu has yet fully recovered from the trick played on him by outgoing Defense Minister Ehud Barak, who apparently withdrew his support for a strike on Iran at the last minute last fall. And if Moshe Ya'alon is the man who succeeds Barak, his position is even clearer: In all the discussions on Iran held by Netanyahu's octet of senior ministers over the last four years, Ya'alon was firmly in the dovish camp.

#### No Israel strikes --- Netanyahu and Barak have toned down the rhetoric and pressure from the US and Israeli elections prevents action.

New York Times, 1/26/2013. “Israeli Official Hints Pentagon Plans May Make Lone Strike on Iran Unnecessary,” http://www.nytimes.com/2013/01/27/world/middleeast/defense-official-hints-that-israel-is-stepping-back-from-plans-to-unilaterally-attack-iran.html?\_r=0.

[Israel](http://topics.nytimes.com/top/news/international/countriesandterritories/israel/index.html?inline=nyt-geo)’s departing defense minister, [Ehud Barak](http://topics.nytimes.com/top/reference/timestopics/people/b/ehud_barak/index.html?inline=nyt-per), said that the Pentagon had prepared sophisticated blueprints for a surgical operation to set back [Iran’s nuclear program](http://topics.nytimes.com/top/news/international/countriesandterritories/iran/nuclear_program/index.html?inline=nyt-classifier) should the United States decide to attack — a statement that was a possible indication that **Israel might have shelved any plans for a unilateral strike**, at least for now. In an interview conducted at the World Economic Forum in Davos, Switzerland, and published by [The Daily Beast](http://www.thedailybeast.com/articles/2013/01/25/ehud-barak-at-davos-u-s-could-strike-iran-to-block-nuclear-progress.html) on Friday, Mr. Barak was asked if there was any way Israel could go to war with [Iran](http://topics.nytimes.com/top/news/international/countriesandterritories/iran/index.html?inline=nyt-geo) over what many in the West believe is a [nuclear weapons](http://topics.nytimes.com/top/news/science/topics/atomic_weapons/index.html?inline=nyt-classifier) program without dragging in the United States. Mr. Barak replied that there were more than just the two options — of full-scale war or allowing Iran to obtain nuclear weapons capability — in the event that sanctions and diplomacy failed. “What we basically say is that if worse comes to worst, there should be a readiness and an ability to launch a surgical operation that will delay them by a significant time frame and probably convince them that it won’t work because the world is determined to block them,” he said. Under orders from the White House, “the Pentagon prepared quite sophisticated, fine, extremely fine, scalpels,” Mr. Barak added, referring to the ability to carry out pinpoint strikes. Herbert Krosney, an American-Israeli analyst and the author of a book about the arming of Iran and Iraq, said Mr. Barak’s statement **now “indicates that there is close cooperation” between Israel and the United States** following months of tension between the country’s leaders (though military and intelligence services continued to work together closely). “I think **there is a realization in Israel that it would be extremely difficult for Israel to operate alone**,” he said. Last year, Prime Minister Benjamin Netanyahu of Israel was pushing hard for the Obama administration to set clear “red lines” on Iran’s nuclear progress that would prompt the United States to undertake a military strike, infuriating the administration. And Mr. Barak repeatedly warned that because of Israel’s more limited military capabilities, its own window of opportunity to carry out an effective strike was closing. It has appeared that Mr. Barak has drifted away from Mr. Netanyahu in recent months, sounding more conciliatory toward the Obama administration, **but even the prime minister has become less antagonistic**. The Pentagon declined to comment on The Daily Beast report, but a senior defense official said, “The U.S. military constantly plans for a range of contingencies we might face around the world, and our planning is often quite detailed.” The official added, “That shouldn’t come as a surprise to anyone.” In recent years, Mr. Barak and Mr. Netanyahu had become increasingly alarmed as Iran moved forward with a nuclear program that it says is solely for peaceful purposes, but that Israel, the United States and others believe is geared toward producing a bomb. The two men consistently emphasized Israel’s doctrine of self-reliance for such existential issues. **But faced with tough opposition from Washington and public criticism from a string of former Israeli security chiefs, the prospect of an imminent unilateral Israeli strike receded in recent months**. In the past few weeks Mr. Netanyahu campaigned for re-election in Israel as a strong leader who, among other things, had managed to persuade the world to deal with the Iranian threat. Mr. Netanyahu and his conservative Likud Party emerged weakened from the elections, with much of the Israeli electorate more focused on domestic issues. In a speech after the voting, he said, “The first challenge was and still is to prevent Iran from acquiring nuclear weapons.” But he did not again threaten to go it alone.

#### Israel won’t attack Iran – kills relations with the U.S.

Simon 09 (Steven, senior fellow on Council of Foreign Relations, “An Israel Strike on Iran”, http://www.cfr.org/publication/20637/israeli\_strike\_on\_iran.html?gclid=CLTSv8bqyqICFU8J2godPQqLwQ)

Israel would regard any expansion of nuclear weapons capability within its region as an intolerable threat to its survival. As such, Iran’s developing nuclear program has triggered serious concern in Israel and speculation that the Israeli government may choose to attack Iran’s nuclear installations in an effort to delay its acquisition of nuclear weapons capability**. This** [**Center for Preventive Action**](http://www.cfr.org/thinktank/cpa/) **Contingency Planning Memorandum** by [Steven Simon](http://www.cfr.org/bios/1374/) assesses the likelihood of an Israeli strike on Iran, the policy options available to diminish that likelihood, the implications should it take place, and measures that can be taken to mitigate the consequences should it occur. The memo concludes that Israel is not eager to start a war with Iran, or disrupt its relations with the United States

#### Won’t escalate

Rogan 8/18/12 (Thomas, MSc in Middle East politics from the School of Oriental and African Studies.

Israel could attack Iran without causing a major war in the region

http://www.guardian.co.uk/commentisfree/2012/aug/18/israeli-attack-iran)

While it is likely Israel will attack Iran in the near future, it is not in either party's interest to allow retaliation to escalate Over the last few days, Israeli newspapers have been consumed by reports that the prime minister, Binyamin Netanyahu, has decided to launch an attack on Iranian nuclear facilities some time this autumn. Although Netanyahu has an obvious interest in increasing pressure on Iran, it would be an error to regard these reports as simple rhetorical sensationalism. In my opinion, whether this year or next, Israel is likely to use its airforce to attack Iran. While it is impossible to know for sure whether Netanyahu will act, it is possible to consider the likely repercussions that would follow an Israeli attack. While it is likely that Iran would retaliate against Israel and possibly the US in response to any attack, it is unlikely that Iran will instigate a major war. Albeit for different reasons, Iran, Israel and the US all understand that a war would not serve their interests. First, the Israeli policy angle. If Netanyahu decides to order an attack on Iran, his focus will be on maximising the success of that action and minimising any negative consequences that might follow. In terms of Iranian retaliation, Israel would expect Iran's core non-state allies Hamas, the Palestinian Islamic Jihad and Hezbollah to launch rocket attacks into Israeli territory. However, present success with advanced defence systems has helped increase Israeli confidence in their ability to absorb this method of retaliation. Beyond rocket attacks, the Israeli leadership also understands that a likely mechanism for Iranian retaliation is via attacks against Israeli interests internationally. Whether carried out by the Iranian Quds Force or Hezbollah, or a combination of both, various incidents this year have shown Israel that Iran continues to regard covert action as a powerful weapon. The key for Israel is that, while these Iranian capabilities are seen as credible, they are not seen to pose intolerable threats to Israel. Faced with rocket strikes or limited attacks abroad – to which the likely response would be air strikes or short-duration ground operations (not a repeat of 2006) in Lebanon and Gaza – Israel would be unlikely to pursue major secondary retaliation against Iran. Certainly, Israel would not want to encourage intervention by Syria's Assad alongside Iran (an outcome that might follow major retaliatory Israeli action). If Netanyahu does decide to take action, Israeli objectives would be clearly limited. The intent would be to prevent Iran from acquiring a nuclear capability while minimising escalation towards war. Israel has no interest in a major conflict that would risk serious damage to the Israeli state. Though holding opposite objectives, Iran's attitude concerning a major war is similar to Israel's. While Iran regards nuclear capability as prospectively guaranteeing the survival of its Islamic revolution, clerical leaders also understand that initiating a major war would make American intervention likely. Such intervention would pose an existential threat to the theocratic project that underpins the Islamic Republic. Thus, in the event of an Israeli attack, Iran's response would be finely calibrated towards achieving three objectives: • First, punishing Israel for its attack. • Second, deterring further Israeli strikes and so creating space for a reconstituted Iranian nuclear programme. • Finally, weakening US/international support for Israel so as to increase Israeli isolation and vulnerability. Hezbollah, Hamas and other non-state allies would play a major role in effecting Iranian retaliation. Iran may also attempt to launch a number of its new Sajjil-2 medium-range missiles against Israel. Again, however, using these missiles would risk major retaliation if many Israeli citizens were killed. As a preference, Iran would probably perceive that utilising Hamas and Hezbollah would allow retaliation without forcing Netanyahu into a massive counter-response. Crucially, I believe Iran regards that balancing its response would enable it to buy time for a reconstituted, hardened nuclear programme. In contrast to the relatively open current structure, sites would be deeper underground and far less vulnerable to a future attack. The nuclear ambition would not be lost, simply delayed. As a final objective for retaliation, Iran would wish to weaken Israel's relationship with the US and the international community. This desire might encourage Iran to take action against US navy assets in the Gulf and/or attempt to mine the Strait of Hormuz, so as to cause a price spike in global oil markets and increased international discomfort. However, beyond their rhetoric, the Iranian leadership understand that they cannot win a military contest against the US, nor hold the strait for longer than a few days. For Iran then, as with Israel, regional war is far from desirable. Finally, consider the US. It is now clear that Obama and Netanyahu disagree on Iran. In my opinion, Netanyahu does not believe Obama will ever be willing to take pre-emptive military action against Iran's nuclear programme. Conversely, Obama believes Netanyahu's diplomatic expectations are too hasty and excessively restrictive. The policy distance between these two leaders appears increasingly irreconcilable. If Netanyahu decides to go it alone and attack Iran, the US president will face the unpleasant scenario of having to protect American interests while avoiding an escalation dynamic that might spin out of control towards war. This difficulty is accentuated by Obama's re-election race and his fear of the domestic economic fallout that may come from the decisions that he might have to make. Again, the simple point is that the US government has no interest in a war with Iran. If Netanyahu decides to take military action, he will do so in a strategic environment in which Israel, Iran and the US have no preference for a major war. Each state views the prospect of a war as counter to their particular long-term ambitions. Because of this, while serious, Iranian retaliation would be unlikely to produce an escalatory dynamic leading to war. The leadership of each of these states will restrain their respective actions in the pursuit of differing long-term objectives but common short-term ones.

#### Nuclear Iran creates stable deterrence with Israel allowing peace to progress for Palestine and reducing terrorism

Madson 6 [Peter, Graduate Student—Naval Postgraduate School, Masters Thesis, “THE SKY IS NOT FALLING: REGIONAL REACTION TO A NUCLEAR-ARMED IRAN,” STINET, p. 17-18]

The likely outcome is that Israel and Iran will enjoy a more stable relationship through mutual deterrence. Iran’s greatest reason for building nuclear weapons is to counter those of Israel and the United States. With a secure stockpile of weapons, Tehran will be able to relax its concerns of being attacked. This stability could possibly encourage Palestinian statehood and end Iranian-sponsored terrorism in Israel. Some of the key issues that must be addressed are whether Israel will strike Iran’s nuclear facilities, how nuclear weapons will impact Iran’s support to anti-Israeli terrorists, and how mutual deterrence can develop between the two.

#### That’s key to solve global ethnic conflict.

AP Worldstream 99 [“UNDATED: is dangerous.” 5-13, L/N]

There are some who believe that ethnic conflicts can only be resolved with military power. Witness the North Atlantic Treaty Organization's bombing campaign against Yugoslavia. On the other hand, the Middle East peace process could become a model for solving ethnic conflicts through dialogue. The Palestinians kept the peace process alive by forgoing a declaration of statehood. No matter who becomes the next prime minister of Israel, the time has come for the Israeli people to respond in kind by clearly voicing their support for peace.

### A2 – Global War Assertion

#### This evidence is from a blog about how the US, Russia, and China would just go to war – won’t happen – it has no logical arguments – but stoping nuclear Iran means bioweapons

Bansak 11 [Kirk, a graduate student at the Fletcher School of Law and Diplomacy at Tufts University and former research associate in the Chemical and Biological Weapons Nonproliferation Program at the James Martin Center for Nonproliferation Studies (CNS), " Managing networks of risk: A tailored approach to Iran’s biological warfare threat potential," Bulletin of the Atomic Scientists, 67(5):66-76, EBSCO]

The United States and many of its allies consider a nuclear-armed Iran an intolerable threat to stability in a volatile region and to security around the world. Failure to keep Iran from acquiring nuclear weapons, they argue, could have a range of negative consequences, including sparking a nuclear arms race in the Middle East and threatening the existence of Israel. Yet in their struggle to thwart Iran's nuclear ambitions, the United States, its allies, and like-minded members of the international community should not focus only on the dire consequences of failure in this mission. They should also consider the implications of success. Smothering Iran's prized nuclear program could well provoke dangerous reactions, including, perhaps, Iran's pursuit of other types of unconventional weapons systems. In one possible scenario, an Iran deprived of nuclear weapons is driven to develop a capability already within its technical grasp: biological weaponry. Whether manifested as the initiation of a new biological warfare program or the intensification of an existing (but so far unconfirmed) biological weapons effort, the Iranian threat is grave enough to warrant serious consideration of a rigorous biological nonproliferation strategy that could be implemented in parallel with nuclear nonproliferation efforts.

#### Bioweapons are comparatively worse than nuclear war

Singer 1— Clifford Singer, Director of the Program in Arms Control, Disarmament, and International Security at the University of Illinois at Urbana—Champaign [Spring 2001, “Will Mankind Survive the Millennium?” The Bulletin of the Program in Arms Control, Disarmament, and International Security, University of Illinois at Urbana-Champaign, 13.1, http://www.acdis.uiuc.edu/research/S&Ps/2001-Sp/S&P\_XIII/Singer.htm]

In recent years the fear of the apocalypse (or religious hope for it) has been in part a child of the Cold War, but its seeds in Western culture go back to the Black Death and earlier. Recent polls suggest that the majority in the United States that believe man would survive into the future for substantially less than a millennium was about 10 percent higher in the Cold War than afterward. However fear of annihilation of the human species through nuclear warfare was confused with the admittedly terrifying, but much different matter of destruction of a dominant civilization. The destruction of a third or more of much of the globe’s population through the disruption from the direct consequences of nuclear blast and fire damage was certainly possible. There was, and still is, what is now known to be a rather small chance that dust raised by an all-out nuclear war would cause a socalled nuclear winter, substantially reducing agricultural yields especially in temperate regions for a year or more. As noted above mankind as a whole has weathered a number of mind-boggling disasters in the past fifty thousand years even if older cultures or civilizations have sometimes eventually given way to new ones in the process. Moreover the fear that radioactive fallout would make the globe uninhabitable, publicized by widely seen works such as “On the Beach,” was a metaphor for the horror of nuclear war rather than reality. The epidemiological lethal results of well over a hundred atmospheric nuclear tests are barely statistically detectable except in immediate fallout plumes. The increase in radiation exposure far from the combatants in even a full scale nuclear exchange at the height of the Cold War would have been modest compared to the variations in natural background radiation doses that have readily been adapted to by a number of human populations. Nor is there any reason to believe that global warming or other insults to our physical environment resulting from currently used technologies will challenge the survival of mankind as a whole beyond what it has already handily survived through the past fifty thousand years. There are, however, two technologies currently under development that may pose a more serious threat to human survival. The first and most immediate is biological warfare combined with genetic engineering. Smallpox is the most fearsome of natural biological warfare agents in existence. By the end of the next decade, global immunity to smallpox will likely be at a low unprecedented since the emergence of this disease in the distant past, while the opportunity for it to spread rapidly across the globe will be at an all time high. In the absence of other complications such as nuclear war near the peak of an epidemic, developed countries may respond with quarantine and vaccination to limit the damage. Otherwise mortality there may match the rate of 30 percent or more expected in unprepared developing countries. With respect to genetic engineering using currently available knowledge and technology, the simple expedient of spreading an ample mixture of coat protein variants could render a vaccination response largely ineffective, but this would otherwise not be expected to substantially increase overall mortality rates. With development of new biological technology, however, there is a possibility that a variety of infectious agents may be engineered for combinations of greater than natural virulence and mortality, rather than just to overwhelm currently available antibiotics or vaccines. There is no a priori known upper limit to the power of this type of technology base, and thus the survival of a globally connected human family may be in question when and if this is [[1]](#footnote-1)achieved.

# 2AR

### AT: Terror

#### Iran won't give it to terrorists

Hobbs and Moran 12 [Christopher, Leverhulme Research Fellow at the Centre for Science and Security Studies within the Department of War Studies at King's College London, and Matthew, Research Associate at the Centre for Science and Security Studies within the Department of War Studies at King's College London, December, “Looking Beyond a Nuclear-Armed Iran: Is Regional Proliferation Inevitable?” *The International Spectator*, Vol. 47 No. 4, pg. 127-148]

With regard to the nightmare scenario in which Iran might pass nuclear materials or even a nuclear weapon to a terrorist group, this would seem highly improbable. Tehran has long provided ﬁnancing, training, logistical support and weapons to a number of terrorist groups within the Middle East, as a means of both exporting its Islamic revolution and striking the United States and Israel.“ This history, combined with Tehran’s belligerent rhetoric on Israel — in 2005, President Ahmadinejad appeared to suggest that Israel should be “wiped off the map” — has evoked fears of a nuclear-armed Iran facilitating nuclear terrorism.“ However, a closer analysis of this scenario reveals that this would neither ﬁt with Iran’s past behaviour nor advance Tehran’s current interests. The most obvious and compelling argument as to why Iran would abstain from proliferating to terrorist groups is the massive retaliation that would almost certainly be the ultimate consequence of a nuclear terrorist attack facilitated by Iran. While Iran would certainly seek to deny any involvement in such an attack, advances in nuclear forensics in recent years have greatly increased the likelihood of nuclear material being traced back to its source. The forensic ‘ﬁngerprint’ present in all ﬁssile materials reveals information on its geographical origins as well as the processing methods used in its production, and remains identiﬁable even after a nuclear explosion.” In this context, any evidence linking Iran to nuclear terrorism would undoubtedly signal the end of the regime in Tehran. Certainly, a nuclear-armed Iran could embolden Iran’s terrorist proxies in their conventional attacks — in this context, a variant of the stability-instability paradox mentioned earlier could see an Iranian bomb serving to deter retaliation leading to regime change even as levels of state-assisted conventional terrorism increased. And in general terms, while Iran has reduced its state-sponsored terrorism since the 1990s, it still has the capability to strike out through its proxies on a global scale. Over the past 24 months, there has been an upsurge in Iranian sponsored terrorist attacks; Tehran has been linked to bombings in Bulgaria, Georgia and India, as well as to a plot to assassinate the Saudi Arabian ambassador in Washington. However, it is also worth pointing out that “despite its messianic pretensions, Iran has observed clear limits when supporting militias and terrorist organizations in the Middle East".88 For example, Iran has the capability to supply groups such as Hezbollah with chemical or biological weapons, but has chosen not to do so.

### Yes BioWeapons Impact

#### Extinction

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

Research paper NO . 2 – 2013

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

1. [↑](#footnote-ref-1)