# Kentucky Round 2

## 1AC

### 1AC Plan

#### The United States federal government should require consultation with congress prior to the use of offensive cyber operations by President of the United States and require a prompt and full account to congress of every significant use of cyber weapons by the President of the United States.

### 1AC Adv One (9)

Contention \_\_\_ is 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.

Stuxnet, a computer worm reportedly developed by the United States and Israel that destroyed Iranian nuclear centrifuges in attacks in 2009 and 2010, is often cited as the most dramatic use of a cyberweapon. Experts said no other known cyberattacks carried out by the United States match the physical damage inflicted in that case.

U.S. agencies define offensive cyber-operations as activities intended “to manipulate, disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves,” according to a presidential directive issued in October 2012.

Most offensive operations have immediate effects only on data or the proper functioning of an adversary’s machine: slowing its network connection, filling its screen with static or scrambling the results of basic calculations. Any of those could have powerful effects if they caused an adversary to botch the timing of an attack, lose control of a computer or miscalculate locations.

U.S. intelligence services are making routine use around the world of government-built malware that differs little in function from the “advanced persistent threats” that U.S. officials attribute to China. The principal difference, U.S. officials told The Post, is that China steals U.S. corporate secrets for financial gain.

“The Department of Defense does engage” in computer network exploitation, according to an e-mailed statement from an NSA spokesman, whose agency is part of the Defense Department. “The department does \*\*\*not\*\*\* engage in economic espionage in any domain, including cyber.”

‘Millions of implants’

The administration’s cyber-operations sometimes involve what one budget document calls “field operations” abroad, commonly with the help of CIA operatives or clandestine military forces, “to physically place hardware implants or software modifications.”

Much more often, an implant is coded entirely in software by an NSA group called Tailored Access Operations (TAO). As its name suggests, TAO builds attack tools that are custom-fitted to their targets.

The NSA unit’s software engineers would rather tap into networks than individual computers because there are usually many devices on each network. Tailored Access Operations has software templates to break into common brands and models of “routers, switches and firewalls from multiple product vendor lines,” according to one document describing its work.

The implants that TAO creates are intended to persist through software and equipment upgrades, to copy stored data, “harvest” communications and tunnel into other connected networks. This year TAO is working on implants that “can identify select voice conversations of interest within a target network and exfiltrate select cuts,” or excerpts, according to one budget document. In some cases, a single compromised device opens the door to hundreds or thousands of others.

Sometimes an implant’s purpose is to create a back door for future access. “You pry open the window somewhere and leave it so when you come back the owner doesn’t know it’s unlocked, but you can get back in when you want to,” said one intelligence official, who was speaking generally about the topic and was not privy to the budget. The official spoke on the condition of anonymity to discuss sensitive technology.

Under U.S. cyberdoctrine, these operations are known as “exploitation,” not “attack,” but they are essential precursors both to attack and defense.

By the end of this year, GENIE is projected to control at least 85,000 implants in strategically chosen machines around the world. That is quadruple the number — 21,252 — available in 2008, according to the U.S. intelligence budget.

The NSA appears to be planning a rapid expansion of those numbers, which were limited until recently by the need for human operators to take remote control of compromised machines. Even with a staff of 1,870 people, GENIE made full use of only 8,448 of the 68,975 machines with active implants in 2011.

For GENIE’s next phase, according to an authoritative reference document, the NSA has brought online an automated system, code-named TURBINE, that is capable of managing “potentially millions of implants” for intelligence gathering “and active attack.”

‘The ROC’

When it comes time to fight the cyberwar against the best of the NSA’s global competitors, the TAO calls in its elite operators, who work at the agency’s Fort Meade headquarters and in regional operations centers in Georgia, Texas, Colorado and Hawaii. The NSA’s organizational chart has the main office as S321. Nearly everyone calls it “the ROC,” pronounced “rock”: the Remote Operations Center.

“To the NSA as a whole, the ROC is where the hackers live,” said a former operator from another section who has worked closely with the exploitation teams. “It’s basically the one-stop shop for any kind of active operation that’s not defensive.”

Once the hackers find a hole in an adversary’s defense, “[t]argeted systems are compromised electronically, typically providing access to system functions as well as data. System logs and processes are modified to cloak the intrusion, facilitate future access, and accomplish other operational goals,” according to a 570-page budget blueprint for what the government calls its Consolidated Cryptologic Program, which includes the NSA.

Teams from the FBI, the CIA and U.S. Cyber Command work alongside the ROC, with overlapping missions and legal authorities. So do the operators from the NSA’s National Threat Operations Center, whose mission is focused primarily on cyber­defense. That was Snowden’s job as a Booz Allen Hamilton contractor, and it required him to learn the NSA’s best hacking techniques.

According to one key document, the ROC teams give Cyber Command “specific target related technical and operational material (identification/recognition), tools and techniques that allow the employment of U.S. national and tactical specific computer network attack mechanisms.”

The intelligence community’s cybermissions include defense of military and other classified computer networks against foreign attack, a task that absorbs roughly one-third of a total cyber operations budget of $1.02 billion in fiscal 2013, according to the Cryptologic Program budget. The ROC’s breaking-and-entering mission, supported by the GENIE infrastructure, spends nearly twice as much: $651.7 million.

#### 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.

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.

#### Our pre-emption policy has created a cyber cold-war

Benavides 7/30/13 (Stephen Benavides is a policy analyst and union organizer from Dallas. He holds a bachelor's degree in political science from the University of North Texas and has done graduate research in econometrics and economic theory. , “The Coming Cyber-Cold War: US Pioneering Online Attacks”, <http://truth-out.org/news/item/17714-the-coming-cyber-cold-war>)

The US government is openly and actively engaged in a reincarnation of the Cold War. Physical assets such as spies and informants have been replaced with zero-day software exploits and network security analysts. Old-school intelligence gathering, while effective to some degree, pales in comparison with the scope of big-data firms such as Endgame and Palantir. Instead of war-ravaged proximity states in Eastern Europe or the Middle East, we have shadowy "actors in cyberspace" and network backdoors on the Internet. The development and expansion of cyber-security, and hence cyber-warfare - equivalent to an arms race - has been in the works for decades and is now a prime objective for the executive branch and the Department of Defense. As the US prepares to deploy weaponized malware and viruses against its enemies, it is forcing those enemies to respond in kind. We are witnessing the first stage of an America-led arms race that undoubtedly will result in a cyber cold war.

Before Edward Snowden released details about foreign and domestic spying program PRISM, low-level and continuous cyber espionage was well underway. As far back as 2002, a three-year attack accessed and downloaded 10 to 20 terabytes of sensitive information from the Department of Defense in an operation titled "Titan Rain." The culprit - whether an individual or a state - was never identified. In 2009, there were cyber attacks on the US water and sewage systems, as well as the national electrical grid. China and Russia are alleged to have accessed secure systems and mapped out the entire infrastructure of the country. More recently, the Obama administration was forced to admit that it had deployed Stuxnet against Iranian nuclear centrifuges and that the NSA attacked Tsinghua University, a research facility in China.

"Cyber warfare attacks" are the new terrorism, with risk to economic and national security elevated to Orwellian heights found post-9/11. At least that's what US military commanders want the public to believe.

#### Un-regulated offensive postures uniquely are bad – Complexity and inter-connected infrastructures means any pre-emption is BOUND to escalate

Benavides 7/30/13 (Stephen Benavides is a policy analyst and union organizer from Dallas. He holds a bachelor's degree in political science from the University of North Texas and has done graduate research in econometrics and economic theory. , “The Coming Cyber-Cold War: US Pioneering Online Attacks”, <http://truth-out.org/news/item/17714-the-coming-cyber-cold-war>)

The unregulated nature of the cyber arms trade not only leaves open the possibility of technology falling into an opposition organization's possession, but guarantees it. Once again, the US is leading weapons proliferation. Political inconvenience of a militarized conventional war also may play a part in the burgeoning cyber war. It is much more difficult for military commanders to justify the death of a sister or brother in combat operations widely understood to be about maintaining access to energy resources than a "victimless" attack on a foreign government to protect internal bank documents or dam vulnerabilities.

The government does acknowledge that the directive may raise unique national security and foreign policy concerns, and it states, "DCEO (Defensive Cyber Effects Operations) and OCEO (Offensive Cyber Effects Operations), even for subtle or clandestine operations, may generate cyber effects in locations other than the intended target, with potential unintended or collateral consequences that may affect U.S. national interests in many locations." One issue with waging war in an unknown environment, often against unknown enemies, is that an actor is unable to predict with any accuracy how weaponized software may interact with different systems. Even the most professional attacks have been known to spiral out of control, which leaves open the risk that an attack on an enemy ultimately will affect those it was designed to "protect."

Governments have not moved to apply international laws of war to cyberspace, although they call it warfare nonetheless. The Pentagon says the same rules of engagement apply, which is patently false because the US is under constant attack and also is attacking every day. Where is the open declaration of war? There is none. Instead the Internet is a militarized proxy, a theater for a new cold war. And anyone who wants to participate can. It took only 20 years for the parent of the Internet, the US military, to exercise overwhelming influence on its once-free and forlorn child. The Internet is now, or maybe has always been, an agent of the state.

#### Lack of civilian bereucratic control proliferation and nuclear war are 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.

#### US cyber attacks inevitably escalate to kinetic war

Moss 4/19/13 (Trefor, covers Asian politics, defence and security, and was Asia-Pacific Editor at Jane’s Defence Weekly until 2009 The Diplomat- - “Is Cyber War the New Cold War?”, <http://thediplomat.com/2013/04/19/is-cyber-war-the-new-cold-war/3/>)

Cyberspace matters. We know this because governments and militaries around the world are scrambling to control the digital space even as they slash defense spending in other areas, rapidly building up cyber forces with which to defend their own virtual territories and attack those of their rivals.

But we do not yet know how much cyberspace matters, at least in security terms. Is it merely warfare’s new periphery, the theatre for a 21st century Cold War that will be waged unseen, and with practically no real-world consequences? Or is it emerging as the most important battle-space of the information age, the critical domain in which future wars will be won and lost?

For the time being, some states appear quite content to err on the side of boldness when it comes to cyber. This brazen approach to cyber operations – repeated attacks followed by often flimsy denials – almost suggests a view of cyberspace as a parallel universe in which actions do not carry real-world consequences. This would be a risky assumption. The victims of cyber attacks are becoming increasingly sensitive about what they perceive as acts of aggression, and are growing more inclined to retaliate, either legally, virtually, or perhaps even kinetically.

The United States, in particular, appears to have run out of patience with the stream of cyber attacks targeting it from China – Google and The New York Times being just two of the most high-profile victims – and which President Obama has now insisted are at least partly state-sponsored.

Although setting up a cybersecurity working group with China, Washington has also signaled it intends to escalate. U.S. Cyber Command and NSA chief General Keith Alexander signaled this shift of policy gears earlier this month when he told Congress that of 40 new CYBERCOM teams currently being assembled, 13 would be focused on offensive operations. Gen Alexander also gave new insight into CYBERCOM’s operational structure. The command will consist of three groups, he said: one to protect critical infrastructure; a second to support the military’s regional commands; and a third to conduct national offensive operations.

As cyber competition intensifies between the U.S. and China in particular, the international community approaches a crossroads. States might begin to rein in their cyber operations before things get further out of hand, adopt a rules-based system governing cyberspace, and start respecting one another’s virtual sovereignty much as they do one another’s physical sovereignty. Or, if attacks and counter-attacks are left unchecked, cyberspace may become the venue for a new Cold War for the Internet generation. Much as the old Cold War was characterized by indirect conflict involving proxy forces in third-party states, its 21st century reboot might become a story of virtual conflict prosecuted by shadowy actors in the digital realm. And as this undeclared conflict poisons bilateral relations over time, the risk of it spilling over into kinetic hostilities will only grow.

#### Kinetic attacks causes nuclear war

Roth 07 professor in IR at Goucher College 7 [Ariel Ilan Roth, “Nuclear Weapons in Neo-Realist Theory”, REFLECTION, EVALUATION, INTEGRATION, International Studies Review, pg 369-384]

Critical, though not explicit, in Waltz is the belief that **a war between nuclear powers will be hard to maintain at the conventional level.** Waltz (Waltz and Sagan 2003:9) allows that such **a sub-nuclear war may be fought but** considers **the risk of it escalating to the nuclear level with its accompanying certain destruction as too high for the risk tolerance of most leaders**. The strategic studies literature has played host to this debate for decades. Some, like Snyder (1965), have argued that **nuclear weapons are**, in a sense, **mutually negating, creating what has been called the stability-instability paradox, wherein stability at the nuclear level breeds instability at the conventional level**. It is, in this conception, as if two duelists stand with guns loaded and cocked at each other’s heads yet proceed to have their fight with daggers instead (Jervis 1989:19-20). Others, like Barry Posen (1982), have argued that **even though nuclear states may wish to limit their conflict to conventional weapons**, actions that occur during wartime can lead to what he calls “inadvertent escalation.” In his “Cold War Turned Hot” example, NATO attacks near Soviet ballistic submarine bases could draw a nuclear response even though the aim of NATO is not to harm the strategically stabilizing Soviet submarine-based missile arsenal (Posen 1982:29-30). Such an interaction would then escalate further as American targets were hit with nuclear weapons and a war that was supposed to be both limited and sub-nuclear is now an apocalyptic doomsday. **The prospects for inadvertent escalation are recognized by Jervis** (1989:21) as well who comments that “**because escalation can occur although no one wants it to, mutual second-strike capability does not make the world safe for major provocations and limited wars**.” This conclusion leads to the first of Jervis’ (1989:23-24) expected outcomes from what he calls the “nuclear revolution,” namely, that there will be peace among the great powers.

#### Uniquely true because of mis-perceptions

Rosenzweig 9, Professor at Georgetown Law

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

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

#### 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.

#### This is particularly true of bureaucratic decision makers and cyber war – who have a “do something” mentality – escalates the impact

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)

If an adversary conducts a cyberattack against the United States, a first question for U.S. decision makers will be knowledge of the attack’s impact and magnitude. Such knowledge is necessary to inform an appropriate U.S. response. (If, for example, the United States wishes to make a commensurate response, it needs to know what parameters of the incoming attack would characterize a commensurate response.)

But in many kinds of cyberattack, the magnitude of the impact of the first cyberattack will be uncertain at first, and may remain so for a considerable period of time. Decision makers may then be caught between two challenges—a policy need to respond quickly and the technical fact that it may be necessary to wait until more information about impact and damage can be obtained. (As noted in Section 2.5, these tensions are especially challenging in the context of active defense.)

Decision makers often feel intense pressure to “do something” immediately after the onset of a crisis, and sometimes such pressure is warranted by the facts and circumstances of the situation. On the other hand, the lack of immediate information may prompt decision makers to take a worst-case view of the attack and thus to assume that the worst that might have happened was indeed what actually happened. Such a situation has obvious potential for inappropriate and unintended escalation.

#### 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.

### 1AC Advantage 2 (10)

#### Contention \_\_\_ is the Law of Armed Conflict

#### Squo OCO policy violates the Law of Armed conflict – Lack of congressional checks make Jus in Bellum impossible to establish

Dycus 10(Professor Stephen Dycus is an internationally recognized authority on national security law and environmental law. The courses he has taught at Vermont Law School include Public International Law, National Security Law, Estates, Property, and Water Law. He was founding chair of the National Security Law Section of the Association of American Law Schools. He is the lead author of "National Security Law" (the field's leading casebook) and "Counterterrorism Law", and he was founding co-editor in chief of the Journal of National Security Law & Policy. (Stephen, "Congress' Role in Cyber Warfare," National Security Journal, Volume 4, Issue 155, 2010 <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>)

The term “cybersecurity” might be understood to refer to defense against cyber attacks. “Cyber attack” suggests offensive use, but the label is inexact and might be misleading. A preemptive strike to ward off an imminent enemy attack is considered defensive. Digital espionage might be part of the preparation for an attack, or it might be perceived that way by the target, which might then be provoked to defend itself by responding with a preemptive attack, either cyber or kinetic. The important point here is that any use of cyber weapons, offensive or defensive, could have enormous consequences for the security and other interests of the United States. The effect of such use, actual or potential, matters more than the labels. And if the effect – on human life or property, for example, or diplomatic relations or compliance with the law of armed conflict – is substantial, Congress has a role to play in adopting policy for that use. Congress has not thus far adopted measures suited to the regulation of cyber warfare. The War Powers Resolution, for example, is concerned with sending U.S. troops into harm’s way, rather than with clicking a computer mouse to launch a cyber attack, although the strategic consequences might be similar. And the WPR’s relatively relaxed timetable for executive notice and legislative response is unrealistic for war on a digital battlefield. Similarly, if cyber warfare is regarded as an intelligence activity, the intelligence oversight measures just described cannot, for reasons already indicated, ensure that Congress will be able to play a meaningful role. In the words of the National Research Council study cited above, “Today’s policy and legal framework for guiding and regulating the use of cyberattack is ill-formed, undeveloped, and highly uncertain.”45 Our experience with nuclear weapons may point to needed reforms. Since the beginning of the Cold War, the United States has had a fairly clear nuclear policy (albeit one that deliberately includes an element of difficulty in tracking the source also makes a policy of deterrence based on a threat of retaliation far less credible. Given these characteristics of cyber warfare, and the continuing refinement of cyber weaponry, we approach a state of extreme strategic instability, with each nation on hair-trigger alert. The execution of an illconceived cyber war policy calling for a prompt response – or any response – to an attack or threatened attack could have disastrous, unanticipated consequences. It also might, depending on the circumstances, violate the law of armed conflict. Congress accordingly needs to work closely with the executive branch in the development of a policy for this new kind of conflict. Such a policy ought to reflect the distinctive technology and strategy of digital warfare, and it should be reviewed constantly as the technology evolves. Like other regulations dealing with dynamic subjects, this policy should include general approaches that reflect this nation’s broad strategic concerns and fundamental values. But the policy must also be crafted with enough flexibility to allow those charged with its execution to deal with future developments that cannot now be predicted. And it should set out a procedure for such adaptive use by identifying, for example, who must be consulted under what circumstances, and who will make the final critical decisions. It is at least theoretically possible that Congress could play an active, real-time role in the implementation of whatever cyber warfare policy is adopted. The policy might, for example, like the War Powers Resolution, require consultation “in every possible circumstance.”50 But it seems more likely that a digital war would begin and end before any notice could ever reach Capitol Hill. Congress therefore needs to lay down clear guidelines, with as much flexibility as prudence requires, for executive branch officials to follow if consultation is not reasonably possible. And Congress should require a prompt and full account of every significant use of cyber weapons.

#### They uniquely makes modeling by china impossible

Sanger 9/1/13 (David, A 1982 graduate of Harvard College, Sanger has been writing for the Times for 30 years covering foreign policy, globalization, nuclear proliferation, and the presidency., He has been a member of two teams that won the Pulitzer Prize, and has been awarded numerous honors for national security and foreign policy coverage. “Documents detail U.S. cyber-espionage plans”, <http://www.thehindu.com/news/international/documents-detail-us-cyberespionage-plans/article5083012.ece>)

231 operations planned for 2011 – both small scale and large scale

Newly disclosed budget documents for America’s intelligence agencies show how aggressively the United States is conducting offensive cyber-operations against other states, even while the Obama administration protests attacks on U.S. computer networks by China, Iran and Russia.

The documents, obtained by The Washington Post from Edward J. Snowden, the former National Security Agency contractor, indicate 231 such operations in 2011, a year after the first evidence emerged of a U.S.-and Israeli-led cyberattack against Iran’s nuclear-enrichment centre.

It suggests that President Barack Obama was not deterred by the disclosure of the Iranian operation, which became evident because of a technological error, and is pressing ahead on using cyber-weapons against a variety of targets.

The Post had said it has withheld most of the 178 pages of documents at the request of government officials because of the sensitivities of the spying operations they describe.

Unlike drone attacks, which the administration has begun to acknowledge publicly and provide legal justifications for, cyberattacks are still regarded as part of a secret arsenal.

The attacks described in the budget documents appear to be on a far smaller scale than the series of attacks on Iran, which were part of a classified operation called “Olympic Games”.

The Post talked of a parallel effort, code-named GENIE, which it described as an effort by U.S. intelligence officials working for the NSA and the military’s Cyber Command to insert surreptitious controls into foreign computer networks. That computer code, a form of malware, allows U.S. officials to hijack the computers or route some of their data to servers that enable U.S. espionage.

It is unclear how many, if any, of those 231 operations are merely for espionage or data manipulation, and how many may be intended to destroy or disable infrastructure. Mr. Obama, in an executive order signed last year, has reserved the right to decide when the United States should conduct such operations. It is not clear how many of the 231 he approved.

Diplomatically, the disclosure of the latest Snowden documents poses a new challenge to Mr. Obama. He has pressed China to cease its own cyber-operations in the United States, many of which are aimed at the theft of intellectual property — including corporate secrets and plans for the F-35 Joint Strike Fighter, the country’s most expensive new weapons system.

The Chinese have responded that America also conducts extensive cyber-operations — including against China — and will doubtless use the most recent disclosures to press that case. So far, Mr. Obama’s effort to get the Chinese engaged in a deeper dialogue on cyberissues has yielded discussions, but little fruit.

#### Ambiguity in definitions for attack policies means we cant adhere to UN charter

Adkisson et al. 12 Carnagie Mellon University (CDR James Adkisson, Mr. Tokunbo Davies, LT Brian Evans,¶ Mr. Rick Lanchantin, Ms. Patty Walters, “Law of Armed Conflict:¶ Implications for Navy Cyber Strategy¶ Masters of Information Technology Strategy¶ Practicum – 2012”, <http://www.cmu.edu/mits/files/random/mits-cohort1-practicumfinal-lawarmedconflict-implications-aug-2012.pdf>)

The uncertain definition of the ‘use of force’ is increasingly problematic when analyzing cyber attacks. Although cyber attacks do not utilize lethal effects, cyber attacks present a clear danger due to their ability to inflict both intended and unintended damage to critical infrastructure, financial markets, banks and the overall welfare of a nation. Such attacks could lead to the paralysis of a nation due to an inability to support its population, resulting in significant suffering and/or death of non-combatants. As a result, there is a strong argument that the threat of cyber attack is itself a violation of the U.N. Charter and LOAC. In contrast, there is also an argument that cyber should be used in preference to conventional weapons in order to comply with LOAC. This argument is based on the assertion that cyber attacks are more humanitarian because they have less potential to create collateral damage than conventional weapons. These are the issues that commanders and military planners must balance when

conducting operations in cyberspace.

In a February 2012 testimony to Congress, the Director of National Intelligence (DNI), Director of the Central Intelligence Agency (CIA), and Director of the Federal Bureau of Investigations (FBI) stated that cyber security ranks among the top national security concerns. They also indicated that current policy requires revision to address how the use of force in cyberspace conforms to national and international law, including LOAC.

The previous section reviewed the applicability of LOAC to cyber operations. This section builds on that understanding and reviews national policy that impact DoD operations in cyberspace.

B. Defining Policy

The DoD does not expressly define the term ‘policy’. A standard dictionary definition implies that policy provides guidance for solving problems without explicitly defining the solution.2 Accordingly, policy for cyber operations should offer a means to arrive at solutions for achieving the established operational objectives within cyberspace.

While DoD policy is designed to guide the decision-making process, the policies must conform to LOAC. Accordingly, the DoD has stated that current policy and legal regimes that govern actions in traditional warfare domains also apply to cyberspace operations.3¶ The U.S. Navy has in turn stated that Navy cyberspace operations will conform to DoD and national efforts.4 Despite these efforts, cyber policy across the U.S. Government remains severely underdeveloped. Many of the policy documents from the Executive Branch, DoD, individual military services, and Department of Homeland Security (DHS) were written more than ten years ago. Despite their age, these documents continue to influence decisions about cyber operations that result in “legally acceptable plans and orders that support national security objectives.”¶ 5

While there is significant debate regarding cyber operations amongst the international community, the U.S. Government (USG) is moving forward to try and establish domestic strategies and policies. These policies can generally be examined from the perspectives of offense and defense. Due to lack of international consensus regarding the characteristics of an ‘armed attack’ in cyberspace, there is minimal policy regarding Offensive Cyber Operations (OCO) or Exploitation Cyber Operations (ECO). Policy concerning OCO continues to suffer from a lack of authorities concerning its use. ECO is conducted under U.S. Title 50 authorities that govern the operations of the Intelligence Community (IC).

#### Impacts –

#### A) China doesn’t have a model for LOAC in cyberspace – that escalates ANY SKIRMISH.

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.

#### Structural Tensions make conflict inevitable

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

Underlying Structural Tensions

■■ Established and rising power. Beyond specific disputes and exacerbating factors, tensions¶ between the United States and China are likely to persist for the simple reason that a rising¶ great power such as China is bound to cause friction as its expanding objectives and growing¶ strength rub against the interests of other nations in its region, including the long-established¶ dominant power—the United States. The study of international relations has long suggested¶ that such “power transitions” are especially fraught with the danger of conflict for reasons¶ having to do both with concrete calculations of power and wealth and with more ineffable¶ factors of honor and pride.17 Historically, a rising nation usually expects to be granted greater¶ influence and respect in accordance with its growing stature, but nations that already possess¶ that influence are generally reluctant to part with it, especially if they do not trust or share¶ basic values with the rising state. Thus tensions can grow. The basic structural problems of¶ how China’s rise can be squared with the U.S. established position and the existing regional¶ order Washington has underwritten are intensified by the ideological tensions between a global¶ power structure established and overseen by liberal democratic powers and a rising power with¶ an avowedly authoritarian government. Again, such tensions do not need to lead to conflict and¶ war, but they might.

■■ Security dilemma. Within this broader dynamic, there is a real danger that the emerging structural¶ dynamics between the United States and China are generating a classic security dilemma,¶ in which the actions taken by one side to increase its defensive strength are interpreted as¶ hostile or threatening by the other side, thereby eliciting a defensive response that the first side¶ views as hostile or threatening, and so forth.18 Although it appears that this dynamic already¶ exists in some respects in the arena of conventional military competition—for example, China’s conventional ballistic and cruise missile program, undertaken at least in part in response to improved

U.S. conventional capabilities, is now leading to a countervailing U.S. response—such¶ a dynamic has thus far had a limited effect on U.S.-China nuclear dynamics. This is fortunate¶ because a security dilemma in the nuclear realm would be destabilizing, intensify suspicions,¶ and potentially raise the danger of conflict escalation. The conditions do, however, exist for¶ such a dynamic to develop: China’s significant missile buildup (conventional and nuclear), the¶ gradual expansion of its nuclear force in the last decade, and its development of asymmetric¶ capabilities—combined with Chinese concerns about the U.S. development of new ballistic¶ missile defense (BMD) and conventional prompt global strike (CPGS) capabilities—provide¶ the ingredients for a security dilemma in the strategic arena.19 Several Chinese scholars already¶ claim that the expansion of China’s nuclear missile force is designed to compensate for advances¶ in U.S. BMD, CPGS, and strategic strike capabilities.20 Meanwhile, some U.S. voices point to¶ China’s expansion of its nuclear and missile forces as proof of hostile intent and the need for¶ improved U.S. capabilities.

#### China perceives US policy – lack of CLARITY makes Chinese invasion of Taiwan inevitable.

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.

#### Miscalc alone causes Extinction

Gompert & Saunders 11 (David C. Gompert, bachelor's degree in engineering from the U.S. Naval Academy, where he once served on the faculty, and a master of public affairs degree from Princeton University's Woodrow Wilson School of Public and International Affairs. Office of the Director of National Intelligence, Gompert most recently worked as a senior fellow at the RAND Corp, and Phillip C. Saunders, phD in IR from Princeton, Distinguished Research Fellow Director of Studies, Center for Strategic Research Director, Center for Study of Chinese Military Affairs, “The Paradox of Power Sino-American Strategic Restraint in an Age of Vulnerability”, <http://www.ndu.edu/inss/docuploaded/Paradox%20of%20Power.pdf>)

Cyber war capabilities can contribute to crisis instability. Cyber attacks have little or no counterforce potential for either side, in the sense that the attacking side is no less vulnerable to cyber attacks for having conducted them. The advantage in striking first in cyberspace lies not in protecting oneself from retaliatory strikes but in degrading the opponent’s C 4 ISR and operations before one’s own are degraded. Conversely, exercising restraint with no expectation that the opponent will do likewise could be disadvantageous. In any case, if either side is inclined to use cyber war to degrade the capabilities and performance of the other’s military forces, there is logic in doing so early. Because striking early could be advantageous, there is the potential that a cyber attack could be the trigger that turns a confrontation into a conflict. The United States (or China) would likely interpret Chinese (or American) cyber attack as a prelude to physical attack.

An improbable but extremely consequential danger is that an attack by either side on the other’s C4 ISR could be interpreted as intended to obstruct the ability to mobilize strategic nuclear forces. The separation of tactical and strategic C4 ISR is not a public matter. However, in the confusion of disrupted surveillance and command networks, the possibility cannot be excluded that strategic forces would at least be placed on higher alert, creating a risk of faulty calculation with incalculable results.

The Chinese would be imprudent to think that the United States would respect firebreaks in cyberspace. Whether it acts preemptively or in retaliation, the United States would have an incentive to attack Chinese cyberspace broadly rather than narrowly on dedicated and protected Chinese military networks. Not only would this harm China’s economic activity, it could also degrade the ability of the leadership to direct Chinese operations and even to communicate with the population. U.S. attacks could isolate Chinese leadership and sow confusion in the population. Chinese cyber attacks could prompt the United States to retaliate without diminishing U.S. capability to do so. The Chinese have a lot to consider before beginning cyber war.

Another feature of cyber warfare may aggravate this crisis instability: the option of subtle attacks or demonstrations. Before hostilities have begun, it might occur to one side that a mild cyber attack—a nonlethal display of one’s resolve—could warn and deter the other side and demonstrate its vulnerability. Knowing this, the side attacked might well opt to escalate in cyberspace. Even more dangerous is the potential that a cyber attack intended to show resolve could be interpreted as a prelude to general hostilities, thus triggering, instead of deterring, a conflict.

It would be a gamble for either side to bet that cyber war could be controlled. Every network, whether military or dual-use, that could support military operations would likely be targeted. Networks that support intelligence collection and dissemination would be attacked, making both sides less certain about what was happening but by no means more passive in the conflict. Moreover, one side or the other might consider escalating cyber war to critical networks such as those supporting economic and financial functions, transportation, power, and state control. In sum, the existence of dual-use networks, the possibility of willful escalation, and the difficulty of controlling viruses, worms, and other infections, regardless of human plans, lead to a conclusion that limiting cyber war to the tactical military level would be hard.

#### B) Human survival hangs in the balance. Absent LOAC wars are more likely to break out and make extinctions.

**Weston 91** – Chair of the International and Comparative Law Program @ The University of Iowa [Weston, Burns H., “Logic and Utility of a Lawful United States Foreign Policy,” Transnational Law & Contemporary Problems, Vol. 1, Issue 1 (Spring 1991), pp. 1-14

George Will and others like him are right, of course, that the rhetoric of **international law can be used**, like a double-edged sword, **against the** **U**nited **S**tates **as well as by it**. They are wrong, however, to bemoan this fact-unless, of course, they bemoan the nature of law itself, a process of legitimized politics that, in Benjamin Cardozo's unforgettable words, seeks the "reconciliation of the irreconcilable," the "merger of antitheses," the "synthesis of opposites," in "one unending paradox."12 Though the "real world" often is not a very nice place and though for this reason it sometimes may seem that the responsible pursuit of national interests requires realpolitik policies and practices, **a foreign policy that corresponds with** what most people have in mind when they think of "**The Rule of Law**" (i.e., notions of equality, mutuality, reciprocity, cooperation, and third-party procedure) **is more likely to find itself on the winning side of most political and strategic** **battles than one that does not. Legality**, like honesty**, is generally the best** **policy. It enhances power used under its aegis.**

In the pages following, I suggest six concrete reasons why **the U**nited **S**tates-indeed, all nations- **should take international law seriously**, even¶ when others do not. Viewed in isolation, they may not persuade the hardened realpolitiker. Viewed together, however, they should.

1. Respect for International Law Assists Human Survival

To begin with, **it is not healthy** for people (and for other living things) **to resist** principles of **international law in a world that is bristling with** **more than 50,000 nuclear weapons and other greatly expanded technologies** **of war and mass destruction**. **If** the **history** of the last half century **has** **taught us anything, it is that our present militarily competitive international** **order** cannot be expected to prevent large-scale war **for very long** (e.g.,Kuwait). **There is**, therefore, **little hope for genuine security**, national or global, **without** a strengthening of the **legal foundations**, bilateral and multilateral, **for** the **nonmilitary**-preferably democratic-**resolution of** **international disputes.** These would include, but not be limited to, the improvement of U.N. peacekeeping and peacemaking opportunities and capabilities, and the improvement of both national and international opportunities and capabilities for legal challenges to coercive foreign policies. 13 Even if other countries do not always follow suit, surely **our** **country and our children's future will be better served if we strive** hard **to build as peaceful and just** a world **society** as we can, and **while we still** **have the chance**. 14 The Soviet Union, home to more than 25,000 nuclear weapons and many newly-awakened nationalisms, faces a world history that demonstrates little support for the proposition that collapsing empires fade quietly. And **in our increasingly "high-tech" world, with military** **research and development fast at work on** atomic guns**,** particle-beam cannons**, and** other space age deviltries **that divert attention from the perils** **of nuclear proliferation, many** regimes in Western Asia and elsewhere **have** **been acquiring** nuclear and other weapons of mass destruction**-and the** **means to deliver them, with frightening ease and speed, to almost anywhere** **on earth.**

In sum, **it is respect** (or lack of respect) **for international law that**, in the end, **will** determine the fate of the Earth. As the late Bill Bishop counseled pithily over two decades ago, "under present conditions **all [States]**¶ **need international law in order to continue to exist together on this planet.**"15 **Rededication to the world rule of law and cooperation in this Age of Nuclear** **Anxiety is not a matter of choice. It is**, quite simply, **a** matter of survival.

2. Respect for International Law Enhances International Stability

Living as we do in the twilight years of the global Middle Ages, characterized by more than 160 separate fiefdoms, each with a monopoly control over the military instrument and each only barely accountable in any formal sense either to each other or to the larger arena in which each operates, it is easy to be seduced by the popular claim that ours is an anarchical world. Such an outlook does not, however, comport with reality. Every hour of every day, ships ply the sea, planes pierce the clouds, and artificial satellites probe outer space. Every hour of every day, communications are transmitted, goods and services traded, and people andthings transported from one country to another. Every hour of every day, transactions are negotiated, resources exploited, and institutions established across national and equivalent frontiers. And in all these respects, the many processes of authoritative and controlling decision that help to regulate such endeavors-what we call international law-are observed rather well on the whole.

On the other hand, **when States bend, twist, or** otherwise show **disrespect** for this ordering force to suit their special interests, **international law**, because **it** is an essentially voluntarist process of decision that is seriously lacking in centralized command and enforcement structures, quickly loses its otherwise stabilizing influence. The kidnapping of sixty-two Americans at the U.S. Embassy in Teheran in 1979, for example, demonstrates well the fundamental instability that can flow from a failure or refusal to abide by international law. Without, in this instance, a commitment to the basic rules of diplomatic protection, diplomacy ceased to exist and respectable discourse became impossible. Without a commitment to the world rule of law there could be no assurance of inter-governmental stability.

Of course, States-especially the major powers-are perfectly capable of unilaterally resisting the doctrines, principles, and rules of international law without necessarily feeling directly the destabilizing impact that their noncompliance ultimately has on the wider structure of international law and order itself. The probability of being formally punished for violating international law is usually so slim that foreign policy strategists commonly give little or no weight to the cost of decision-making marked by dubious legality.

However, **the increasingly interdependent** and interpenetrating **character** **of today's world is of such magnitude** and complexity **that** **no nation, least** **of all the U**nited **S**tates, **can sensibly afford to insist upon its own** **independence of action without simultaneously threatening its own ultimate** **good and the ultimate good of others**, and potentially **in very fundamental** **ways**. Though not understood by most Americans, it is in fact the United States "which stands to lose the most in a state of world anarchy." 16 **Because** **the U**nited **S**tates and its **citizens have such wide-ranging and far-flung** **international interests, we urgently need a stable, predictable environment of international legal rules and procedures that can help to secure those** **interests on a cooperative basis worldwide**. It is not in the first instance our freedom of action that should be our concern when we refuse to commit to the world rule of law, but rather, the stability of our world public order itself.

3. Respect for International Law Advances Our Geopolitical Interests

Allowing principles of international law and multilateral cooperation to inform our foreign policy also serves our geopolitical interests, especially our long-term geopolitical interests. For example, in contrast to our recent hegemonic warmongering in Grenada, Nicaragua, and Panama, a record of faithful adherence to the principle of nonintervention and to the right to self-determination would have helped, politically at least, to neutralize the Israelis in southern Lebanon and the Occupied Territories, the Soviets in the Baltics, and the Iraqis in Kuwait. As the late L.F.E. Goldie observed a number of years ago: "Obedience to law... is not only a categorical value but also a prudential one." 1'7 My colleague and former Prime Minister of New Zealand Sir Geoffrey W. R. Palmer, referring to the need for strict compliance with arms control and disarmament treaties, once put it this way: "[I]s it possible on the one hand to look to international law to provide essential security guarantees, while on the other hand, in other areas, the right is quietly being reserved to undermine, ignore and indeed walk away from the rule of law in international affairs?"18

In recent years, however, during the Reagan presidency especially, the United States has come before the world community more to bury international law than to praise it. Selectively displaying its military strength to the general disregard of international law, it has chosen, at least when the risks have been low, to advance several broadly defined but narrowly determined national interests:

(1) demonstrating American will to act with decisiveness and reinforcing deterrence against the Soviet Union in the Third World; (2) displaying the ability of U.S. armed forces to defend American and allied interests; (3) inducing countries that challenge the U.S. to cease and desist; and (4) enhancing in the broadest terms an international perception of the U.S. as the great world power. 19

But to favor such special interests over the common interest of a world rule of law is to shoot ourselves in the geopolitical foot-perhaps not always, but more often than is commonly realized. It gets us into quagmires from which it is hard to extricate ourselves and it subverts our ability to ensure in other settings that other governments, especially our adversaries, will fulfill their obligations under international law that are in our interest for them to fulfill.

The point is depressingly simple to illustrate. If we can unilaterally reinterpret and abrogate an arms control treaty with the Soviet Union,20 why cannot the Soviets do the same with us? If we can excuse the kidnapping and killing of innocent civilians by the Nicaraguan Contras because they were "freedom fighters,"21 what right do we have to condemn the Palestinians or Shiites for doing the same thing in Lebanon? If we can ignore a World Court decision relative to the human rights violations we encouraged in Nicaragua,2 how can we complain when Iran ignores a World Court decision relative to the taking of U.S. hostages in Teheran?2 If we can claim the right to seize fugitives from abroad,2 what logic compels our right to object when the Iranian Majlis (parliament) approves legislation authorizing Iranian officials to arrest Americans anywhere in the world for violations of Iranian law?25 If we can intercept a civilian aircraft over the Mediterranean on the grounds that it appears to threaten our national security interests, 26 what is to stop the Soviet Union from doing the same thing over the Pacific for the same reason?27 If we can condone a U.S. military raid upon an ambassadorial residence in Panama despite our obligations under the 1961 Vienna Convention on Diplomatic Relations, how can we complain when Iranian students seize a U.S. embassy protected by the 1961 Vienna Convention on Diplomatic Relations? 28 And so forth.

Such partisan uses of international law are illustrative of what, during the 1980s, has been referred to as the "Reagan Corollary" of international law-which is to claim a right "to pressure the international legal system into changing in a manner beneficial to United States interests."9 However, such uses do not, in the end, correspond to our long-term national interest of ensuring that other governments in other settings fulfill their obligations under international law. Were every nation to adopt this Reagan Corollary, a perverted interpretation of international doctrines, principles, and rules would become the standard practice and the international legal system would quickly disintegrate into a system of retributive justice extremely unsafe for the geopolitical interests of even the most powerful States.

Thus, if the United States wants to insist upon compliance with international law to protect American interests, it will be to its advantage to obey international law, even when its application proves inconvenient. If we want meaningful international law to be available when we find it useful, we must respect it even when we do not.

4. Respect for International Law Promotes Policy Efficacy

**A failure to adhere to international law-in particular the prohibitions** **against the threat and use of nondefensive force** and the admonitions to¶ promote and safeguard human rights**-tends** also **to be counterproductive**, hence not very efficacious. **While militarism** and support of repressive regimes to the disregard of international law **may sometimes yield tactical victories that are viscerally pleasing in the short-run, they rarely achieve** **strategically satisfying gains, to say nothing of justice, over the long-run**. Consider, for example, the Reagan administration's decision, pursuant to what came to be known as the "Schultz Doctrine," to fight terrorism with American-sponsored counterterrorism, 30 the ultimate denouement of which was the sordid Iran-Contra affair. In keeping with this decision, the United States provided Israel with diplomatic, financial, and material support of Israel's illegal invasion of southern Lebanon in 1982,31 in violation of common Article 1 of the four Geneva Conventions on the laws of war of 194932 and involving the killing of more than 20,000 people (at a time when, ironically, Palestinian terrorist attacks against American persons and property had been in decline). Not surprisingly, the victims of the invasion and their sympathizers held Washington responsible, in conjunction with Israel, for the atrocities committed by the Israeli army and the Lebanese Phalange militia against Palestinian civilians in the Sabra and Shatilla refugee camps in southern Lebanon.33 American interests immediately began to experience a pronounced increase in terrorist attacks-via airplane hijackings, kidnappings, assassinations, bombings, and other paramilitary activitiesfrom Palestinian, Shiite, and other groups throughout the Middle East.

Consider also the refusal of the United States to accept the jurisdiction of the International Court of Justice in the case brought by Nicaragua in April 1985 in protest of Washington's illegal assistance to, and support of, the Contra guerrillas against Nicaragua's democratically elected Sandinista government.34 Instead of making its substantive case before the Court, the United States contended that what it considered to be an issue of Western Hemispheric security was not properly for the World Court to decide and that, in any event, there was no reason for the United States to submit to the Court's jurisdiction when, over the years, the Soviet Union had consistently refused to do so. 35 As one sensitive observer put it, "[this] argument was politically attractive domestically, but it eroded the stature of the World Court that American values had once tried to build up."36 More such examples could easily be recounted. It might be asked, for example, whether our aiding and abetting the assassination of Chile's Allende or our legally dubious support of the Shah of Iran really did serve our long-term national interest. And the same might be asked, as well, of the Iran-Contra affair and of our legally questionable assistance to Saddam Hussein during and after the Iran-Iraq war.

But the efficacy argument is perhaps best demonstrated by noting the large-scale political support that was extended to Washington, internationally as well as nationally, during at least the early months of the 1990-91 Persian Gulf crisis when the United States pressed hard for economic sanctions against Iraq that were, it can be said, not only timely and measured but in keeping with the collective security system authorized in San Francisco in 1945.37 Adherence to the principles and procedures of international law, President Bush discovered, was essential to gaining the world's support to force Iraq's hand. Lawful foreign policies are consensusbuilding policies-politically pragmatic or efficient policies-and they are useful even to a superpower.

To put it all another way, **we abandoned lynching parties on the western** **frontier not only because they turned into orgies of wasteful bloodlust but** **also because they simply did not stop horse thieves. International law** **violations, like violations of law in general, have a dubious pragmatic record** **at best.**

5. Respect for International Law Safeguards Domestic Society

**Disregard of international law** and institutions **tends to be self destructive** **as well as destructive of international order.** **The consequences** **of our** unilateral and disproportionate **uses of force in Vietnam should be** **proof enough.** Over a decade and a half later, as such movies as Platoon, Born on the Fourth of July, and Casualties of War alone bear witness, **we are still** **licking the socioeconomic, political, and ethical wounds**. Though not always immediately apparent or discernible, **international law violations and "go-it-** **alone" policies** that fail to show a decent respect for the rights and opinions of others i**nvariably corrode our core essence, diminishing our national** **integrity and** threatening even our individual liberties. As Professor Bilder has asked, **can we legitimately expect to separate the standards that govern** **the way our government operates internationally from those that govern** **it internally?** 8 **If we tell our elected officials that it's okay to act** illegally, corruptly, or **brutally abroad, can we be completely sure that they will really** **listen when we tell them that they should not act that way at home**? **If** **we say** to the Secretary of State, the CIA, or the National Security Council **that it's okay to bend the law a little because we do not like another** **country's ideology, can we rightfully expect that the** Attorney General or **the FBI will not bend the law a little when it comes to** those of **our citizens** who do not share the government's ideology in domestic affairs?

In other words, **when we show contempt for international law and** **cooperation, we badly** damage our sense of national self-respect and purpose **and, in so doing,** invite civil unrest. In addition to the widespread civil disobedience that characterized the era of the legally problematic Vietnam War, we may note the popular protests that, more recently, accompanied Washington's extraordinary build-up of offensive nuclear weapons, its policy of "constructive engagement" with apartheid South Africa, and its military adventurism in Central America.3 9 One of the wondrous things about our country-deep-rooted in our ideology even if not always borne out in practice-is our commitment to decent behavior and the rule of law. From our very beginnings, we have officially embraced the notion of a Higher Law based upon "principles of right and justice that prevail because of their own obvious merit:"40 liberty, equality, participation, and due process. And since at least the turn of the century, cognate international principles have been added: the self-determination of peoples, the sovereign equality of States, respect for international law and organization, and the peaceful settlement of international disputes. So, **when our government resorts to**¶ **foreign policy plots and maneuvers of a Machiavellian sort** that sacrifice or otherwise diminish these principles, **the** spillover into the domestic arena **is predictable**. The government soon loses the support of the people.

Our Founding Fathers established that ours is a society of laws, not of men. To most of us, therefore, "**standing tall" in the global community** **does not mean being the toughest kid on the block**, pushing other countries around and breaking our promises as we once accused the Soviet Union of doing, **but acting humanely and honorably**. **Intuitively we know that it is necessary for us to uphold the rule of law abroad in order to uphold it** **at home. Intuitively we know that "[t]he** two are inextricably connected." 41 **Intuitively we know that a double standard erodes our claim to moral** **leadership** in the international community.42

6. Respect for International Law Ennobles Our National Rectitude

As evidenced by the U.N. General Assembly's declaration of the 1990s as the "Decade of International Law,"43 **there is a growing realization that** **an effective system of international law is fundamental to the achievement**¶ **of a world public order of** human dignity. **It is essential to** peace and security**,** **and it is** indispensable for just solutions **to** the many **complex and urgent** **problems** that otherwise currently make up the human agenda.

**International law provides**, potentially, **the most durable framework for** **undertaking cooperative action toward the** abolition of war, **the promotion** **of** human rights**, the ending of** mass poverty**, and the creation of a** sustainable global environment. **Its progressive evolution**, in keeping with Article 28 of the Universal Declaration of Human Rights ("Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized"),4 **is the** key to all that is right and good.

**To insist upon respect for international law and cooperation is**, thus, **the** morally correct **thing to do, and for this reason alone it is in our longterm** **best interest**. **Rather than throw our weight around as if at some** shootout at the OK Corral**, the U**nited **S**tates **should reaffirm its commitment** **to a law-oriented foreign policy and**, from this posture, through carefully planned and diligently executed diplomatic strategy, **regain** **a once assumed** (even if not always demonstrated) **moral stature** among the family of nations-the "American difference," as President Reagan used to call it. Along the way, discovering that it would thus gain the upper hand in the global competition for hearts and minds, including the enthusiastic support of otherwise doubting allies, the United States would also discover that commitment to international law and cooperation is fundamentally a matter of self-interest. **Our reputation as a law-abiding nation**, one that genuinely honors the world rule of law in practice, **is a vital asset, strongly affecting** **our ability to win friends and influence people. It is a reputation that** **cannot-must not-be squandered.**

Most importantly, however, **the U**nited **S**tates **has an especial obligation** **in this regard. Quite simply, the size of our economy**, the sophistication of our technology, the ubiquity of our investments, **and the power of our arsenals make us so globally consequential that the acts and omissions of** **our government transmit a powerful and usually** lasting message. **Like** **it or not, our words and our deeds count heavily in the normative,** **institutional, and procedural development of world affairs**. 45 **And this** **establishes for us,** a professedly democratic and peace-loving country, **an** **historically** unique moral responsibility. Pg. 4-13 // AT: K

#### We solve- our adherence to LOAC is modeled globally. OCO ambiguity is the biggest internal link

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 send a global signal of cyber leadership that solves reckless use of OCOs

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.

#### Action now is key – failure will result in a rapidly created worse legal system that non uniques all their offense

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

IX. CONCLUSION

Nothing in international law explicitly prohibits cyber warfare operations. However, legal limitations surely exist with regard to their application. Also, cyber warfare operations have the potential of constituting a use of force or a violation under the law of war.

Cyber warfare operations offer a variety of methods to impact an adversary's ability to conduct war. They may enable a state to infiltrate an adversary's network, acquire files, spread misinformation, or introduce weaknesses into an adversary's systems. Cyber warfare operations may also make it possible for a state to take control of an adversary's network for the purpose of temporarily or permanently disabling it or affecting the infrastructure it supports. n344 Additionally, cyber warfare operations have the potential of depriving an adversary of essential infrastructure that supports military actions, such as communication satellites. One advantage of cyber warfare operations is that they will often achieve their desired results with less collateral damage than traditional warfare, such as, disabling an electrical grid by accessing its network in lieu of bombing the power plant. n345

Despite the fact that cyber warfare operations have the potential of limiting collateral damage during times of hostilities, they pose several risks to states that may employ such warfare. One example would be the potential escalation of minor hostilities into a full blown armed conflict. For example, State A, having received specific evidence establishing that State B was behind DoS attacks against State A's government, declares the acts an unlawful use of force and orders an aerial bombing campaign against State B's communication facilities, the source of the attack. State B may in turn declare the acts of State A as acts of war and launch missiles into State A. In this scenario who is to blame? Did anyone actually violate international law?

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

#### We have to focus on particular security problems – cyber operations preemption is uniquely important that policy must deal with

NICHOLAS D. ANDERSON Georgetown University M.A., Security Studies, 2012, ““Re re defining” International Security”, The Josef Korbel Journal of Advanced International Studies Summer 2012, Volume 4, PDF, http://www.du.edu/korbel/jais/journal/volume4/volume4\_anderson.pdf, KENTUCKY

agency overlap won’t lead to detrimental results. Third,unlike academics, policymakers are tasked with the difficult requirement of allocating resources. Considering these requirements, if everything is a security threat, it is difficult to set priorities or single out areas of particular concern (Koblentz 2010, 108; Paris 2001, 92). If we conceive of such disparate issues as defic it spending, illegal immigration, the H1N1 virus, and the receding Arctic ice cap as “vital” security threats, right alongside the rise of China in Asia, Iranian nuclear proliferation, and al Qaeda training camps, knowing what matters when will be next to impossible. Fourth, if what constitutes a security problem or security threat is too broad, problems will be subject to incompatible policy solutions that could undercut each other, or will be paralyzed by competing demands, relegating them to lowest comm on denominator compromises (Koblentz 2010, 108). At the best of times, as thebureaucratic politics literature points out, this “pulling and hauling” in inter and intra agency battle leads to less than optimal outcomes, generally far from what would be decided upon according to more rational calculation (Allison 1969). If the meaning of what is being battled over lacks consensus, and the means to solve such problems come from every different direction, matters will be made far worse. F inally and perhaps mo st importantly, it is worth pointing out that security threats are used to justify the suspension of civil liberties, waging war, and legitimizing the reallocation of vast resources. In many cases , thisis a necessary cost for maintaining securityand part of the burden we must bear as citizens and members of democratic societies. And yet, even in the healthiest of democracies, we would be ill advised to provide the government an exponentially expanding list of “vital” security threats to protect against (B aldwin 1997, 8; Caldwell and Williams, Jr., 2006, 12). One can easily see how this is a potential first step on the road toward an Orwellian world much like that described in 1984: Oce ania being at war with Eurasia, and having always been at war with Euras ia (Orwell 2004). “Re redefinition”: Bringing Intent Back In How then, are we to define international security and what should be categorized as international security threats ? Arguably, the most intelligent way of narrowing the definition of internatio nal security is to accept the wide variety of possible threatened agents, but to restrict allowable threats to those with international implications that include the fundamental aspect of human agency or intent. This circumscription of the concept will hel p avoid many of the critical theoretical and policy problems outlined above. Furthermore, it is important to distinguish between tangible international security problems and what might be termed “ latent security problems.” Adherents to the human security p aradigm may argue that this distinction is not worth making, but it is important to recognize that nearly anything can have international security implications if the causal chain is drawn long enough. A useful rule of thumb is the more deliberate an inter national threat, the more justifiably it can be classified as a security issue (Caldwell and Williams, Jr., 2006, 11). Under this definition then, many of the modern era’s purported rising “nontraditional threats” (Mathews 1997, 51) do not necessarily me rit classification as international security problems. Rather than being vital security issues in and of themselves, those that exclude the important aspect of human agency are better classified as “latent . ” Climate change in the developing world, for inst ance, promises to bring food and water shortages, catastrophic natural disasters, deadly disease, mass human migration, and resource competition (Podesta and Ogden 2007 2008, 116). And yet, while it certainly poses an international threat, it does not meri t classification as a vital security threat in itself, because of the absence of intent. Deadly infectious diseases such as HIV/AIDS or the Avian flu are another such example. While they are clearly important problems posing potentially grave threats to individuals around the globe, classifying them as threats to international security will only cloud the necessary clarity needed to think and act intelligently in dealing with these problems (McInnes and Rushton 2010, 225). A great number of other examples that are often raised, such as poverty, economic recession, drug abuse, declining natural resources, and rapid urbanization and population growth, simply are what they are , and are not definitively vital issues of international security. While each has the potential to lead to serious international problems, even security problems, they are simply too many steps removed from posing a direct security threat to states, governments, militaries, communities, and individuals in the international system. A number of today’s oft cited threats to international security, on the other hand, are rightly categorized as such. The traditional issues of interstate conflict, military threats, arms races, nuclear deterrence, and contestation of the commons obviously continue to fit the definition. Some of the more recent threats , too, such as nuclear proliferation among “rogue” and weak states (Litwak 2007), increased international piracy, expanding organized crime rings, and international terrorism (Byman 2008; Cronin 2006; Rob erts 2005) all include human agency and have international implications, therefore befit ting the classification as international security problems. Even many emerging threats can be considered as such . Cyber threats, for instance, fit this classificat ion if they are carried out with the intent to threaten the state, its military, or its people (Diebert and Rohozinski 2010). For example, Chinese hackers stealing trade secrets is not an international security issue, whereas cyber penetration of classifie d intelligence files or online te rrorist recruitment and funding are. Biosecurity threats , too, can be justifiably classified as international security problems, but only if they include the fundamental issue of intent. Bio warfare, bio terrorism, maliciou s dual use biological research, and bio crime with violent intent or consequences are all obvious threats to international security. Laboratory accidents, pandemic and epidemic diseases, and agricultural blights, on the other hand, are not (Koblentz 2008, 111). 7 Admittedly, the lines are not nearly as clear as they have been made out to be here. Issues like military accidents, inadvertent missile launches, and abandoned mine fields fit within a grey area between tangible and potential international security problems. But these problems , among many others, can still be traced back to the key concept of intent. Militaries, missiles, and landmines are created and maintained with the intent of deterring, threatening, or even harming governments, militaries, co mmunities, and individuals, and although the harms they may happen to commit may not be intentional on given occasions, they still carry with them this important aspect of intentionality. And so an accidental nuclear weapon detonation should certainly be considered a true international security problem, but nuclear reactor accidents, even meltdowns, no matter how threatening, should not.

## 2AC

### Risk

#### Positivism is inevitable – without it we cant construct any theory – the possibility of some flawed theory construction is better than epistemological anarchy

Brown 11 [Vernon, Cadiff University, 2/27/11, “The Reflectivist Critique of Positivist IR Theory,” <http://www.e-ir.info/?p=7328> ]

There is a great deal of support for the positivist approach in IR despite the critiques presented above. As the survey by Maliniak et al. showed, seventy percent of American IR scholars still consider themselves as positivists with a number of the rest not yet reflectivist. This is significant as the United States is still considered to be the major force in IR scholarship. There are many reasons for this continued success of positivism in IR, the majority of which have to do with either the continued reliance on empirical methods or the failure of many reflectivists, especially the post-modernists, to offer any suggestions to fill the epistemological void left by their passing. David Houghton (2008, p.118) addresses both of these by writing that despite their critique, reflectivists continue to use empirical, observational methods and that it is not possible to be anything but positivist because, as he writes, ‘truth claims about the world have to come from somewhere’. He also suggests that reflectivists are essentially engaging in what can only be perceived as a negative exercise since by continually deconstructing theories one will eventually be left with nothing that is considered a legitimate theory. Another issue raised in response to the reflectivist critique focuses on the pluralism which scholars have called for in the face of epistemological relativism. Lapid (1989, p.249) warns that such pluralism, ‘If adopted uncritically or taken to its logical conclusion, [can] deteriorate into a condition of epistemological anarchy under which almost any position can legitimately claim equal hearing’, and that in such a state it would become nearly impossible to distinguish theoretical proliferation from theoretical growth. Positivism defends itself by claiming that scholarship is inherently observational, therefore empirical, and that if reflectivism is followed to its logical endpoint there would be no legitimate theories left because they would have been either deconstructed or created without a means of testing their legitimacy. Conclusion: The critique of positivism by the reflectivists is fundamentally an epistemological one. Each side can and does make compelling arguments showing the strength of their position. While it is important to acknowledge the positivists’ attempts to ground the discipline in a naturalist, scientific area there is still the obvious fact that the assumptions on which their epistemology is based are too easily deconstructed when they attempt to explain phenomena and make predictions in the socially constructed world which IR purports to study. As Milja Kurki (2009, p.442) suggests, positivism fails to acknowledge the possibility that all theories are at some level ‘politically and socially contextualized’. This creates the possibility for positivist theories to create predictions that are fundamentally flawed as they have failed to take into account the context within which their facts are constructed. This in turn allows the reflectivist theorists to deconstruct the predictions due to misunderstandings that arise from the lack of context in the positivists’ predictions. The question of what positivism has to say in a socially constructed and interpreted world is still an important one, however, since the study of IR is still in many ways observational and therefore empirical. There is also the valid claim that in the face of the possible anarchical pluralism or lack of legitimate theories left by reflectivist critiques there needs to be some sense of scientific and theoretical grounding, and that positivism provides that very thing. In the end, reflectivism performs a valuable service in widening the range of legitimate research that is possible by IR scholars and allowing such research to take into account the understanding that the issues studied are birthed by social conventions. There still must be, however, some framework within this study to prevent the anarchy that could follow in the wake of reflectivism and while positivism is in no ways perfect, or even close to it, it still provides such a framework that if made to be self-reflective and continually evolving, could provide the stability needed.

#### Reject their impact calculus collapsing policy making into affect fails – Decisionmakers will rely on preconceived conceptions of threat rather than the more qualified predictions of analysts

Fitzsimmons, 07 (Michael, “The Problem of Uncertainty in Strategic Planning”, Survival, Winter 06/07)

But handling even this weaker form of uncertainty is still quite challeng- ing. If not sufficiently bounded, a high degree of variability in planning factors can exact a significant price on planning. The complexity presented by great variability strains the cognitive abilities of even the most sophisticated decision- makers.15 And even a robust decision-making process sensitive to cognitive limitations necessarily sacrifices depth of analysis for breadth as variability and complexity grows. It should follow, then, that in planning under conditions of risk, variability in strategic calculation should be carefully tailored to available analytic and decision processes. Why is this important? What harm can an imbalance between complexity and cognitive or analytic capacity in strategic planning bring? Stated simply, where analysis is silent or inadequate, **the personal beliefs of decision-makers** **fill the void**. As political scientist Richard Betts found in a study of strategic sur- prise, in ‘an environment that lacks clarity, abounds with conflicting data, and allows no time for rigorous assessment of sources and validity, ambiguity allows intuition or wishfulness to drive interpretation ... The greater the ambiguity, the greater the impact of preconceptions.’16 The decision-making environment that Betts describes here is one of political-military crisis, not long-term strategic planning. But a strategist who sees uncertainty as the central fact of his environ- ment brings upon himself some of the pathologies of crisis decision-making. He invites ambiguity, takes conflicting data for granted and **substitutes a priori scepticism about the validity of prediction** for time pressure as a rationale for discounting the importance of analytic rigour. It is important not to exaggerate the extent to which data and ‘rigorous assessment’ can illuminate strategic choices. Ambiguity is a fact of life, and scepticism of analysis is necessary. Accordingly, the intuition and judgement of decision-makers will always be vital to strategy, and attempting to subordinate those factors to some formulaic, deterministic decision-making model would be both undesirable and unrealistic. All the same, there is danger in the opposite extreme as well. Without careful analysis of what is relatively likely and what is relatively unlikely, what will be the possible bases for strategic choices? A decision-maker with no faith in prediction is left with little more than a set of worst-case scenarios and his existing beliefs about the world to confront the choices before him. Those beliefs may be more or less well founded, but if they are not made explicit and subject to analysis and debate regarding their application to particular strategic contexts, they remain only beliefs and premises, rather than rational judgements. Even at their best, such decisions are likely to be poorly understood by the organisations charged with their implementation. At their worst, such decisions may be poorly understood by the decision-makers themselves.

#### Dis-regard affect – Multiplying *probability* and *magnitude* is key to ethical risk assessment—the most serious threats to humanity are the unknown and unthinkable.

Rees 08— Sir Martin J. Rees, Professor of Cosmology and Astrophysics and Master of Trinity College at the University of Cambridge, Astronomer Royal and Visiting Professor at Imperial College London and Leicester University, Director of the Institute of Astronomy, Research Professor at Cambridge, 2008 (“Foreward,” Global Catastrophic Risks, Edited by Nick Bostrom and Milan M. Cirkovic, Published by Oxford University Press, ISBN 9780198570509, p. x-xi)

These concerns are not remotely futuristic - we will surely confront them within next 10-20 years. But what of the later decades of this century? It is hard to predict because some technologies could develop with runaway speed. Moreover, human character and physique themselves will soon be malleable, to an extent that is qualitatively new in our history. New drugs (and perhaps even implants into our brains) could change human character; the cyberworld has potential that is both exhilarating and frightening. We cannot confidently guess lifestyles, attitudes, social structures or population sizes a century hence. Indeed, it is not even clear how much longer our descendants would remain distinctively 'human'. Darwin himself noted that 'not one living species will transmit its unaltered likeness to a distant futurity'. Our own species will surely change and diversify faster than any predecessor - via human-induced modifications (whether intelligently controlled or unintended) not by natural selection alone. The post-human era may be only centuries away. And what about Artificial Intelligence? Super-intelligent machine could be the last invention that humans need ever make. We should keep our minds open, or at least ajar, to concepts that seem on the fringe of science fiction. These thoughts might seem irrelevant to practical policy - something for speculative academics to discuss in our spare moments. I used to think this. But humans are now, individually and collectively, so greatly empowered by rapidly changing technology that we can—by design or as unintended consequences—engender irreversible global changes. It is surely irresponsible not to ponder what this could mean; and it is real political progress that the challenges stemming from new technologies are higher on the international agenda and that planners seriously address what might happen more than a century hence. We cannot reap the benefits of science without accepting some risks - that has always been the case. Every new technology is risky in its pioneering stages. But there is now an important difference from the past. Most of the risks encountered in developing 'old' technology were localized: when, in the early days of steam, a boiler exploded, it was horrible, but there was an 'upper bound' to just how horrible. In our evermoreinterconnected world, however, there are new risks whose consequences could be global. **Even a tiny probability of global catastrophe is deeply disquieting.** We cannot eliminate all threats to our civilization (even to the survival of our entire species). But it is surely incumbent on us to think the unthinkable and study how to apply twenty-first centurytechnology optimally, while minimizing the 'downsides'. If we apply to catastrophic risks the same prudent analysis that leads us to take everyday safety precautions, and sometimes to buy insurance—**multiplying probability by consequences**—we had surely conclude that some of the scenarios discussed in this book deserve more attention that they have received. My background as a cosmologist, incidentally, offers an extra perspective -an extra motive for concern - with which I will briefly conclude. The stupendous time spans of the evolutionary past are now part of common culture - except among some creationists and fundamentalists. But most educated people, even if they are fully aware that our emergence took billions of years, somehow think we humans are the culmination of the evolutionary tree. That is not so. Our Sun is less than halfway through its life. It is slowly brightening, but Earth will remain habitable for another billion years. However, even in that cosmic time perspective—extending far into the future as well as into the past - the twenty-first century may be a defining moment. It is the first in our planet's history where one species—ours—has Earth's future in its hands and could jeopardise not only itself but also lifes immense potential. The decisions that we make, individually and collectively, will determine whether the outcomes of twenty-first century sciences are benign or devastating. We need to contend not only with threats to our environment but also with an entirely novel category of risks—with seemingly low probability, but with such colossal consequences that they merit far more attention than they have hitherto had. That is why we should welcome this fascinating and provocative book. The editors have brought together a distinguished set of authors with formidably wide-ranging expertise. The issues and arguments presented here should attract a wide readership - and deserve special attention from scientists, policy-makers and ethicists

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

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.

#### Call for end of security frame sparks American natioanalist backlash and international chaos – we should channel American identity productively.

Michael **HUNT** History @ UNC (Chapel Hill) **‘9** *Ideology and U.S. Foreign Policy* p. 214-218

The third and last facet of the momentous U.S . encounter with the world was the establishment of pervasive economic and cultural influence-what might be described as hegemony. Woodrow Wilson gave voice to hege- monic aspirations that had in view (prematurely, to be sure) nothing less than the remaking of the world. Already in the 1920s American values and institutions were having a widening impact, and they grew even greater after World War II. Washington's success at establishing an international leadership historically unprecedented in its breadth had important ideological consequences. Above all, it confirmed long-standing assumptions about an exceptional U.S. role in the world: people everywhere must deep down admire Americans, would gladly (if possible) become American, and surely looked to Washington as a repository of wisdom to which all countries should defer. Less noticed was how this special postwar standing created problems at home and set limits on U.S. action abroad. Dominance spawned resentments that on occasion inspired direct resistance and made hegemony more difficult to exercise. Faced with surly foreigners, perplexed officials tried to speak more clearly or more loudly. But the angry voices persisted, while a consumer-minded electorate wondered why bother with a benighted and ungrateful world. More serious still, these claims to international leadership imposed constraints on U.S. policymakers and their public. Americans had to actually know something about the world they claimed to lead. This was an inherently difficult task given the breadth of the U.S. reach. Making it even more trying was the notoriously insular nature of U.S. society, with its strongly nationalist bent shaped by animosity to one external threat after another. Compounding the problem, the public put an ever-higher value on individualism and consumerism. Citizens devoted to their distinctly materialist and individualist sense of the good life wanted ever-rising abundance and proved allergic, even phobic, when faced with military service or higher taxes. Further complicating the exercise of hegemony, policymakers limited their own freedom of action by paying obeisance to the invisible hand of the marketplace and embracing the utopian notion of a world turned over to international market forces in which corporations rather than states represented the highest form of human organization and activity. Policymakers operating on the global stage found themselves bound in yet another way-by the need to pay attention to the opinion of other international leaders as the price for securing deference and maintaining legitimacy. These crosscurrents engulfing U.S. policymakers over the twentieth century are an important part of any effort to understand the career of my core policy ideas. These several neglected dimensions to my argument have major implications for the controversial call in the concluding chapter of Ideology for a more modest (some might say "isolationist") foreign policy. I now have to concede that I was on the wrong trail. The United States is now implicated in world affairs in such a deep and complex fashion that a retreat is hard to imagine and if attempted might produce dire consequences overseas, notably a breakdown of global integration, with international anarchy a likely prospect. Moreover, an assertive U.S. nationalism is so important in providing social glue for a diverse, mobile people that a repudiation of the country's leading role on the international stage might well prove deeply divisive at home and spawn bitter cries of betrayal. Finally, pressing domestic problems are now inextricably entangled with international trends and pressures, ranging from climate change to global finance and trade to resource scarcity to immigrant pressures generated by failed states and stagnant economies. Rather than calling for a more modest foreign policy, I would now praise mid-twentieth-century U.S.leaders for following a visionary policy that included the Bretton Woods reforms for the international economy, the creation of the United Nations and other international organizations, the assertion of basic human rights, the decision to hold state leaders responsible for their crimes, and the priority given to economic recovery and relief. These measures were all conducive to world order and prosperity. U.S. leaders in recent decades deserve censure precisely because they neglected or even repudiated the public goods that the United States as hegemon is obligated to provide. A policy at once more territorially interventionist (imperial) and hands-off (neoliberal) in matters of global governance endangers the system of values and institutions promoted in the wake of World War II. The problem I am left with today is not much different from the one that haunted me in the conclusion of Ideology twenty years ago. How does one create an ideological foundation for a different kind of policy-one that serves the American people well while also advancing the cause of human welfare? Reflecting on this question has provided a chastening but useful reminder that ideologies are a lot easier to identify and explore than to construct or transform.

#### There is, humans just have psychological pre-dispositions to assume otherwise

**Cost benefit analysis can be applied to existential risk**

**Posner, ‘04** (Richard, Judge of the U.S. Court Appeals for the Seventh Circuit, and a senior lecturer at the University of Chicago Law School, Oxford University Press, “Catastrophe: Risk and Response”//sb)

The critical analytical technique for evaluating and ameliorating the catastrophic risks is cost-benefit analysis. It remains a usable tool despite the pervasive uncertainties, ethical and conceptual as well as fac-tual, concerning those risks—that is one of the most important points that I have tried to make in this book. But cost-benefit analysis of catastrophic risks must be enriched with recognition of the cognitive difficulty that people encounter in dealing with very small probabilities and very large magnitudes. And the uncertainties arising from the peculiar character of the catastrophic risks create an inescapable need for value judgments concerning such matters as the proper weight to be given the interests of remote future generations, the nonmonetizable social benefits to be ascribed to basic scientific research, and the degree of risk aversion appropriate in responding to the catastrophic risks. Bridging the gap between a purely economic analysis of these responses and the ultimate decision that answers the question “what is to be done?” is another project in which properly informed lawyers can play a critical role. But emphasis must fall on “properly informed,” as yet merely an aspiration.

### AT: Bilat

#### They’ll say yes – incentives.

Gompert & Saunders 11 (David C. Gompert, bachelor's degree in engineering from the U.S. Naval Academy, where he once served on the faculty, and a master of public affairs degree from Princeton University's Woodrow Wilson School of Public and International Affairs. Office of the Director of National Intelligence, Gompert most recently worked as a senior fellow at the RAND Corp, and Phillip C. Saunders, phD in IR from Princeton, Distinguished Research Fellow Director of Studies, Center for Strategic Research Director, Center for Study of Chinese Military Affairs, “The Paradox of Power Sino-American Strategic Restraint in an Age of Vulnerability”, <http://www.ndu.edu/inss/docuploaded/Paradox%20of%20Power.pdf>)

In sum, Chinese economic and political exposure to large-scale network attacks should provide a basis for deterrence and an incentive to explore mutual restraint with the United States in strategic cyberspace, especially when taking into account that China could suffer secondary network and economic effects of large-scale network attacks it may conduct. Given its acknowledged vulnerability, the United States should have a similar incentive. Demarcating critical national networks—“strategic cyberspace”—is hard but not impossible. Restraint in strategic cyberspace without restraint in tactical-military cyberspace may be even harder.

### AT: Dycuz

#### AT Congressional Approval Affs

#### Dycus assumes Congressional approval is impossible

Dycus ‘10

Stephen is a Professor of national security law at Vermont Law School, former member of the National Academies committee on cyber warfare, LLM, Harvard University, LLB, BA, Southern Methodist University, "Congress’ Role in Cyber Warfare," Journal of National Security Law 26 Policy, 4(1), 2010, p.161-164, http://www.jnslp.com/read/vol4no1/11\_Dycus.pdf

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.

### 2AC Afro Pessimism

#### Afro-pessimism is inaccurate and is used to justify white supremacy

Patterson 98—Orlando Patterson is a Jamaican-born American historical and cultural sociologist known for his work regarding issues of race in the United States, as well as the sociology of development [The Ordeal Of Integration: Progress And Resentment In America's "Racial" Crisis]

In the attempt to understand and come to terms with the problems of Afro-Americans and of their interethnic relations, the country has been ill served by its intellectuals, policy advocates, and leaders in recent years. At present, dogmatic ethnic advocates and extremists appear to dominate discourse on the subject, drowning out both moderate and other dissenting voices. A strange convergence has emerged between these extremists. On the left, the nation is misled by an endless stream of tracts and studies that deny any meaningful change in America's "Two Nations," decry "The Myth of Black Progress," mourn "The Dream Deferred," dismiss AfroAmerican middle-class status as "Volunteer Slavery," pronounce AfroAmerican men an "Endangered Species," and apocalyptically announce "The Coming Race War." On the right is complete agreement with this dismal portrait in which we are fast "Losing Ground," except that the road to "racial" hell, according to conservatives, has been paved by the very pQlicies intended to help solve the problem, abetted by "The Dream and the Nightmare" of cultural changes in the sixties and by the overbreeding and educational integration of inferior Afro-Americans and very policies intended to help solve the problem, abetted by "The Dream and the Nightmare" of cultural changes in the sixties and by the overbreeding and educational integration of inferior Afro-Americans and lower-class Euro-Americans genetically situated on the wrong tail of the IQ "Bell Curve." If it is true that a "racial crisis" persists in America, this crisis is as much one of perception and interpretation as of actual socioeconomic and interethnic realities. By any measure, the record of the past half century has been one of great achievement, thanks in good part to the suecess of the government policies now being maligned by the left for not having gone far enough and by the right for having both failed and gone too far. At the same time, there is still no room for complacency: because our starting point half a century ago was so deplorably backward, we still have some way to go before approaching anything like a resolution.

#### Their link argument is non-sense – recognition of US violence doesn’t preclude us from recognizing other violence

Rorty, Professor of Comparative Literature @ Stanford, `02 (Richard, Peace Review, vol. 14, no. 2, p. 152-153)

I have no quarrel with Cornell's and pivak's claim that "what is missing in a literary text or historical narrative leaves its mark through the traces of its expulsion." For that seems simply to say that any text will presupospe the existence of people, things, and institutions that it hardly mentions. So the readers of a literary text will always be able to ask themselves questions such as: "Who prepared the sumptuous dinner the lovers enjoyed?" "How did they get the money to afford that meal?" The reader of a historical narrative will always be able to wonder about where the money to finance the war came from and about who got to decide whether the war would take place. "Expulsion," however, seems too pejorative a term for the fact that no text can answer **all possible questions** about its own background and its own presuppositions. Consider Captain Birch, the agent of the East Indian Company charged with persuading the Rani of Sirmur not to commit suicide. Spivak is not exactly "expelling" Captain Birch from her narrative by zeroing in on the Rani, even though she does not try to find out much about Birch's early days as a subaltern, nor about the feelings of pride or shame or exasperation he may have experienced in the course of his conversations with the Rani. In the case of Birch, Spivak does not try to "gently blow precarious ashes into their ghostly shape," nor does she speculate about the possible sublimity of his career. Nor should she. S.ivak has her own fish to and her own witness to bear just as Kipling had his when he spun tales of the humiliations to which newly arrived subalterns were subjected in the regimental messes of the Raj. So do all authors of literary texts and historical narratives, and such texts and narratives should not alwa s be read as disingenuous exercises in repression. They should be read as one version of a story that could have been told, and should be told, in many other ways.

#### We should treat war out there differently than structural violence. The tradeoff only goes in the other direction – we lose what is distinctive about organized violence.

Tarak BARKAWI Associate Professor of Politics at the New School for Social Research ’12 “Of Camps and Critiques: A Reply to ‘Security, War, Violence’” *Millennium* 41 (1) p. 129-130

A final totalising move in ‘Security, War, Violence’ is the idea that the study of war should be subsumed under the category of ‘violence’. The reasons offered for this are: violence does not entail a hierarchy in which war is privileged; a focus on violence encourages us to see war in relational terms and makes visible other kinds of violence besides that of war; and that the analysis of violence somehow enables the disentangling of politics from war and a proper critique of liberal violence.22 I have no particular objection to the study of violence, and I certainly think there should be more of it in the social sciences. However, why and how this obviates or subsumes the study of war is obscure to me. Is war not historically significant enough to justify inquiry into it? War is a more specific category relative to violence in general, referring to reciprocal organised violence between political entities. I make no claims that the study of war should be privileged over that of other forms of violence. Both the violence of war, and that of, say, patriarchy, demand scholarly attention, but they are also distinct if related topics requiring different forms of theorisation and inquiry. As for relationality, the category of war is already inherently relational; one does not need the concept of violence in general to see this. What precisely distinguishes war from many other kinds of violence, such as genocide or massacre, is that war is a relational form of violence in which the other side shoots back. This is ultimately the source of war’s generative social powers, for it is amidst the clash of arms that the truths which define social and political orders are brought into question. A broader focus on violence in general risks losing this central, distinctive character of the violence of war. Is it really more theoretically or politically adequate to start referring to the Second World War as an instance of ‘violence’? Equally, while I am all for the analysis of liberal violence, another broad category which would include issues of ‘structural violence’, I also think we have far from exhausted the subject of liberalism and war, an important area of inquiry now dominated by the mostly self-serving nostrums of the liberal peace debates.

#### We should separate intentional violent actions from background structures. Their alternative decreases the effectiveness of response to different types of social problems.

Claire THOMAS Int’l Pol @ Sheffield ’11 “Why don’t we talk about ‘violence’ in International Relations?” *Review of Int’l Studies* 37 p. 1829-1831

Much of the attractiveness of this idea of structural violence is that it broadens the remit of security studies, or of research into violence. Thus, economic issues and the damage done by poverty and so on become just as important as the damage done by direct, physical violence. Authors who work with the concept of structural violence aim to highlight the hidden structures in order to work towards their transformation.63 The problem with this is that it is defining a concept dependent on what we want to be able to study within its remit. A concept should not depend for its meaning on how we want to study it, but rather on what the concept means. The concept of structural violence is performing a similar role to the debate about broadening the definition of security. Within the security debate we are used to people posing the challenge of securitisation – that people call something a security problem in order to make it sound more urgent, more policy relevant and so on. One can pose the same challenge to structural violence. Rather than having a clear academic reason for stretching the concept of violence to incorporate other, equally bad, social ills, the main reason proposed is that these other social ills cause as much or more damage than the damage caused by violence. This may well be the case, and these issues should have urgent academic and policy attention. However, re-defining a concept like violence to incorporate these issues in order to gain that attention is a poor way of achieving this. A clear argument that states the reasons why wider social ills are more worthy of our attention does not need the further argument that we should also call them violence. So, by calling something violent, or designating it as an issue of security, an author is claiming a certain importance for the issue, escalating it up the policy agenda, and allowing for extraordinary reactions. For example, by saying that extremists use violence, one designates it as a significant and bad problem, which allows an exceptional response of violence (called military force) to counter it. The aim of calling something violence in order to push it up the policy agenda, meaning it requires special, urgent action, can also lead to dealing with these issues in a different, exceptional way, outside the realm of ‘ordinary’ politics. This may or may not be beneficial in dealing with the issue in question, or for our politics in general.64 A similar move is made by Žižek when he claims that alongside subjective violence (direct, intentional violence), there is also objective violence, one form of which is systemic violence – the damaging consequences of the ‘normal’ functioning of the system. This systemic violence must be taken into account, according to Žžiek, in order to make sense of subjective violence.65 He argues that this systemic violence needs to be given prominence, despite the urgency attributed to direct violence which fights for our attention.66 Again, this argument is valid in that systemic problems cause more suffering in the world than direct violence. But there has to be a further reason to also call this violence. After all, the argument can be made without the need to label something as violence. One could argue that seeing as our concepts are important because they change the way we think about the world, and change the way we act in it, a definition of violence that incorporates these other social ills would be valuable. However, broadening the concept in this way also has the potential for being damaging. If we conceive of all these things as equally violent, in order to see them as equally important, there is an implication that we are also going to tackle the issues as problems of violence. Issues of poverty are not helpfully tackled in the same way as issues of direct violence. The concept of structural violence is problematical as it means that the definition of violence becomes linked to the result of an act (or influence), and not to the intention or actual action of the actor. This illustrates a key difference in the way violence is conceived: one way sees violence from the perspective of the perpetrator, and sees it as intentional, destructive force; the other way sees violence from the point of view of the victim, and sees it as a form of violation.67 Bufacchi points out that these two concepts of violence stem from the Latin roots of the term. The root of the word violence is violentia, meaning a passionate and uncontrolled force, but the meaning is often conflated with ‘violation’, from the Latin violare, meaning ‘infringement’.68 Although the definition of violence is partly contingent on the result of an act, in that it requires that the intention is to physically harm the victim, it is also necessary for that result to be a means to an end, not an end in itself. Because the result of many different acts or situations is physical harm or death (or unequal power or life chances), many things become incorporated into the definition of violence if the concept of intention is not used, and if the instrumental nature of violence is ignored. Roberts goes some way to improving on the debate about structural violence by pointing out that structures are created by people, and thus structural violence can be prevented and does have responsible actors. He also operationalises it by referring to specific acts of structural violence, looking at avoidable civilian deaths. He argues that his way of looking at human insecurity enables the analysis of structures, institutions and human agency, but without the problems caused by broadening the debate to include Galtung’s concept of realising full human psychosomatic potential.69 But this does not prevent the problem that structural violence still refers to anything an author wants it to. Interestingly, many of Roberts’ choice of examples can be incorporated under the title of direct violence in any case (they are preventable female deaths: infanticide, maternal mortality, intimate killings (normal domestic murder, dowry murders and ‘honour’ killings), lethal female genital mutilation; and avoidable deaths in children under five).70 Some caution is needed in this approach, however. It is easy to think of examples where violence is not intentional, for example a natural disaster, or bombing an empty building that accidentally harms someone nearby. We have already recognised that the concept has fuzzy boundaries, and thus we can recognise that some violence occurs naturally. The point here is to discuss that violence which is most relevant for the study of international politics. This is not the same as accepting that everything that causes harm in some way can be captured within the term violence. It is also not going so far as to say that accidental acts of violence are not violence at all. Collateral damage is still violent. The point of including the idea of intentionality in the definition of violence is that it ensures the violence we are discussing in international politics has an actor and does not end up including indeterminate ideas like a state of violence. It does not just happen on its own. It is also an action that is done with the intention of harming, unlike acts such as a doctor causing some pain in order to heal.

#### Perm solves – study of intentional violence should parallel response to social injustice.

Claire THOMAS Int’l Pol @ Sheffield ’11 “Why don’t we talk about ‘violence’ in International Relations?” *Review of Int’l Studies* 37 p. 1832

Structural or systemic violence focuses almost completely on the result of violence, and does not include a requirement of intention or the instrumental nature of violence. Therefore it ends up including a broad range of acts or occurrences that lead to physical or mental harm. This is not useful for the study of international politics. As Keane puts it, this ‘makes violence indistinguishable from experiences like “harm”, “misery”, “unhappiness”, “alienation”, “cultural discrimination” and “repression”’.73 This does not completely negate the insight the concept of structural violence can bring into the structural cause of injustice and so on. These insights have been important in bringing social injustice into the foreground. The study of IR needs to be careful not to prioritise the study of direct violence over other forms of suffering like poverty. However in conceptual terms structural violence needs to be seen as different to violence. In fact, as Derriennic points out, Galtung’s concept of structural violence makes much of what is usually seen as nonviolence (for example, passive resistance, strike, civil disobedience) a violent act. Derriennic does not see this as a problem, as non-violence in this context refers to a particular tactic, and could easily be referred to as a less-violent action.74 However, this point does bring into question a definition of violence which cannot distinguish between violence and non-violence. We do not need to refer to all social ills as violence in order to recognise that they bring human suffering and need to be eradicated. Nor do we need to refer to structural forces as violence in order to recognise the role they play in instigating acts of violence. What we do need is an understanding of the complex nature of structure and agency regarding violence. Calling everything violence does not contribute to this understanding. The choice to use violence is conscious, but the choice is made from a series of socially acceptable choices, and structure plays an important role in defining what those choices are.75 Although the structural aspect of violence is an important issue, it moves too far away from the central meaning of the word. Galtung says ‘[i]n order not to overwork the word violence we shall sometimes refer to the condition of structural violence as social injustice’.76 Social injustice is not the same as violence. It may be a bad thing, but the aim is not to give the label violence to everything that one disagrees with.

#### White supremacy isn’t a monolithic root cause—proximate causes determined through empirics are more likely—and their arg shuts off productive debate over solutions

Shelby 7—Tommie Shelby, Professor of African and African American Studies and of Philosophy at Harvard [2007, We Who Are Dark: The Philosophical Foundations of Black Solidarity]

Others might challenge the distinction between ideological and structural causes of black disadvantage, on the grounds that we are rarely, if ever, able to so neatly separate these factors, an epistemic situation that is only made worse by the fact that these causes interact in complex ways with behavioral factors. These distinctions, while perhaps straightforward in the abstract, are difficult to employ in practice. For example, it would be difficult, if not impossible, for the members of a poor black community to determine with any accuracy whether their impoverished condition is due primarily to institutional racism, the impact of past racial injustice, the increasing technological basis of the economy, shrinking state budgets, the vicissitudes of world trade, the ascendancy of conservative ideology, poorly funded schools, lack of personal initiative, a violent drug trade that deters business investment, some combination of these factors, or some other explanation altogether. Moreover, it is notoriously difficult to determine when the formulation of putatively race-neutral policies has been motivated by racism or when such policies are unfairly applied by racially biased public officials.

There are very real empirical difficulties in determining the specific causal significance of the factors that create and perpetuate black disadvantage; nonetheless, it is clear that these factors exist and that justice will demand different practical remedies according to each factor's relative impact on blacks' life chances. We must acknowledge that our social world is complicated and not immediately transparent to common sense, and thus that systematic empirical inquiry, historical studies, and rigorous social analysis are required to reveal its systemic structure and sociocultural dynamics. There is, moreover, no mechanical or infallible procedure for determining which analyses are the soundest ones. In addition, given the inevitable bias that attends social inquiry, legislators and those they represent cannot simply defer to social-scientific experts. We must instead rely on open public debate—among politicians, scholars, policy makers, intellectuals, and ordinary citizens—with the aim of garnering rationally motivated and informed consensus. And even if our practical decision procedures rest on critical deliberative discourse and thus live up to our highest democratic ideals, some trial and error through actual practice is unavoidable.

These difficulties and complications notwithstanding, a general recognition of the distinctions among the ideological and structural causes of black disadvantage could help blacks refocus their political energies and self-help strategies. Attention to these distinctions might help expose the superficiality of theories that seek to reduce all the social obstacles that blacks face to contemporary forms of racism or white supremacy. A more penetrating, subtle, and empirically grounded analysis is needed to comprehend the causes of racial inequality and black disadvantage. Indeed, these distinctions highlight the necessity to probe deeper to find the causes of contemporary forms of racism, as some racial conflict may be a symptom of broader problems or recent social developments (such as immigration policy or reduced federal funding for higher education).

#### Turn – Starting with Middle Passage decontextualizes slavery and supports the Eurocentric slave-trader perspective. This undermines an effective criticism of imperial relations that support white supremacy.

Walter JOHNSON History @ NYU **‘**4 “Time and Revolution in African America: temporality and the history of Atlantic Slavery” in *A New Imperial History* ed. Kathleen Wilson p. 198-204

Let me begin with a famous misunderstanding. As he later recounted it, when Olaudah Equiano first saw the white slave traders who eventually carried him to the West Indies, he thought they were "bad spirits" who were going to eat him. Awaiting shipment across an ocean he had never heard of, Equiano, like many of the slaves carried away by the traders, made sense of an absurd situation with a narrative of supernatural power.' When he sat down to write his narrative, of course, Equiano knew better than to believe that the white men on the coast were "spirits." By that time he called himself Gustavas Vassa, and, having spent ten years as a slave in the Americas and another twenty-three as a free man traveling throughout the world, Vassa could see what Equiano could not: that he was a descendant of the Lost Tribes of Israel, that his deliverance from heathenism marked him as a "particular favorite of heaven," and that the events in his life were effects not of the evil intentions of African spirits but of the Christian God's "Providence."' Vassa resolved the collision of contending versions of cause and consequence in his own mind through a narrative of progressive enlightenment: he had learned that it was God's Providence to steal him away from Africa and carry him to London where he could spread the gospel of anti-slavery. Vassa's time travel reminds *us* that global historical processes are understood through locally and historically specific narratives of time and history. And yet by invoking God's Providence, Vassa did not so much resolve the contention of these temporal narratives as superimpose one upon the other. Equiano's initial understanding of the situation of the coast was incorporated into the story of Vassa's eventual enlightenment. His African history was reframed according to the conventions of his European one. Recent work in the humanities and social sciences has emphasized the darker side of the temporal conventions that have framed many western histories of the rest of the world: their role in underwriting global and racial hierarchy. Concepts like primitiveness, backwardness, and underdevelopment rank areas and people of the world on a seemingly naturalized timeline — their "present" is our "past" — and reframe the grubby real-time politics of colonial domination and exploitation as part of an orderly natural process of evolution toward modernity. More than a fixed standard of measure by which the progress of other processes can be measured, time figures in these works as, in the words of Johannes Fabian, a culturally constructed "dimension of power."3 Seen in this light, Equiano's anachronistic account of the situation on the coast raises a host of questions about the history of Atlantic slavery. What were the historical and temporal narratives through which Africans and Europeans understood what was happening on the coast, in the slave ships, and in the slave markets of the Americas? How did these various understandings shape the historical process in which they were joined? In what cultural institutions were these ideas of time rooted and through what practices were they sustained? What was the fate of African time in the Americas? What were the practical processes of temporal domination and resistance? Taking time seriously suggests, at the very least, that the slave trade was not the same thing for Olaudah Equiano that it was for his captors. Most simply, this difference might be thought of spatially: "**the slave trade"** did not begin or end in the same place for European traders, American buyers, and African slaves. The African slave trade, after all, had an eastern branch stretching to Asia as well as a western one which stretched to the Americas. Thus a historical account of the African experience of "the slave trade" necessarily has a different shape from an account of the European experience; indeed, properly speaking, "the slave trade" has not yet ended in some parts of Africa.4 But **even if** we confine ourselves to the history of the Atlantic slave trade, the problem of boundaries persists. The journeys of the slaves who were shipped across the Atlantic Ocean often began in the interior of Africa, hundreds of miles from the coast where they eventually met the European slave traders, hundreds of miles away from where any European had ever been. Indeed, **the First Passage was integral to the experience of those who eventually made the Middle Passag**e — to their understanding of what it was that was happening, their emotional condition going into the journey, and their ability to survive it.' And yet the First Passage is often elided from historians' accounts of "the slave trade**,**" many of which focus solely on the Middle Passage, treating the trade as if it were something which began on the west coast of Africa with a sale to a European trader and ended in a port in the Americas with a sale to a colonial slaveholder. In so doing **they have unwittingly embedded the historical perspective of a European slave trader** — for it was only for the traders, not for the slaves or the buyers, that "the slave trade" happened only in the space between the coasts — in the way they have bounded their topics.6 The historical disjuncture marked by Equiano's version of the situation on the coast, however, was much deeper than a difference about beginnings and endings. It signals a fundamental difference between the versions of slavery which met in the Atlantic trade. To oversimplify: in Euro-America, slavery was, above all, a system of economic exploitation; in much of West Africa slavery was, above all, a system of political domination. In the Americas slaves were purchased in markets, held as legally alienable property, and put to work as laborers producing staple crops and some other goods which were generally shipped to Europe in exchange for money and more goods.7 In much of precolonial West Africa, slavery began with capture: a warrior who would otherwise have been killed was allowed to live on as a socially dead slave. Though most slaves in West Africa were agricultural laborers, many were employed as soldiers, state ministers, and diplomats, and even as governing placeholders for princes and kings. Some slaves owned slaves.8 As such, West African slavery has often been described as a system of "institutionalized marginality," one among a set of intertwined social relations — kinship, fealty, clientage, etc. — by which one group of people held "wealth in people" in another. Some slaves, over time and generation, through mar¬riage and connection, were able to move out of slavery and into another status.9 Equiano's confusion on the coast reminds us that two versions of slavery — "aristocratic slavery" and "merchant slavery" in Claude Meillassoux's formulation — met in the African trade. Those who entered the slave trade had been extracted from histories of enslavement and slavery which sometimes had very little to do with the Atlantic slave trade in the first instance. Rather their story as they understood it was embedded in personal histories of iso¬lation from protective kinship and patronage networks, in local histories of slave-producing ethnic conflicts, in political struggles, and wars which occurred hundreds of miles from the coast.'" This is not, however, to say that all African slavery was aristocratic slavery. The jagged boundary between aristocratic and merchant slavery, after all, often lay hundreds of miles into the interior of the African continent — hundreds of miles beyond where any European had ever been. Many of the slaves who were eventually shipped across the Atlantic had been captured, transported to the coast, and sold by people who were themselves Africans. The frontier between the two types of slavery was patrolled by an African supervisory elite who presumably knew the difference between them and made their living by transmuting the one into the other. And just as the protocols of merchant slavery stretched well into the interior ofAfrica, those of aristocratic slavery could stretch well into the journey across the Atlantic. To describe the people they transported to the Americas, the ship captains and clerks of the French West India Company used the word " captif' rather than the more familiar "esclave," a designation which apparently referred to the aristocratic slavery origins of those in the trade rather than their merchant slavery destinations." Corresponding to the different versions of slavery which met in the Atlantic trade were different ways of measuring the extent of slavery and marking its progress through time. The (aristocratic) slaveholding kings of precolonial Dahomey, for instance, represented their history as a story of continuous growth through military expansion and enslavement. Their history was measured in a yearly census — taken, historian Robin Law argues, as a means of "political propaganda . . . advertising the kingdom's successful growth" — and in mythical bags of pebbles kept in the castle which tracked the kingdom's expansion — one pebble per person — over time.' Other sys¬tems of aristocratic slavery had other measures. In precolonial equatorial Africa, Jane Guyer and Samuel M. Eno Belinga have argued, political power and historical progress were measured as wealth-in-knowledge rather than wealth-in-people. Rather than accumulating numbers of people, the leaders of kingdoms like that of the Kongo enhanced their power by acquiring, through capture or purchase, people with different types of knowledge.'3 The African and European merchant slave traders with whom these kingdoms sometimes did business had still other ways of measuring the trade and imagining the history they were making: sacred time measured against an injunction to enslave non-Islamic outsiders or propelled by the "providence" of a Christian God; political history imagined as the conquest of monopoly rights along the African coast and market position in the Americas; market time imagined in macroeconomic cycles of depression and speculation; the microeconomic time of the slave trader, progress tracked across the pages of the ship's log, days defined by the weather and ship's speed, nights marked by the number of slaves who died in the hold — time reckoned in dead bodies and lost profits.14 For many of the slaves who were packed into the holds of the Atlantic slave ships we can imagine still another set of temporal frames: those derived from local political histories of war and slave raiding; a cultural cycle of social death and rebirth, the ethnic and political disorientation of capture and separation eventually giving way to new identifications with "shipmates" and "fictive kin"; a biographical culmination of lifetime fears of capture, kidnapping, or simply of falling through the cracks in the protections of patronage and kinship; the metaphysical horror of a "middle" passage that some must have thought would never end and others might only have recognized as a trip across the "kalunga," the body of water which separated the world of the living from that of the dead — a flight from time measured in the gradual physical deterioration of the worldly body.“ And so on: as many journeys on a single ship as there were ways to imagine the journey.

#### Reducing slavery to the enactment of white supremacy denies the agency of slaves, turns the case.

Walter JOHNSON History @ NYU ’97 “Inconsistency, Contradiction, and Complete Confusion: The Everyday Life of the Law of Slavery” *Law and Social Inquiry* 22 (2) p. 427-429

But race could not simply be enacted, it had also to be acted out (Fields 1990, 95-181; Johnson 1996).37 When Southern whites came into court to talk about race, they talked about biology but also about behavior; about runaways with bad character but also about those who had run away from bad treatment; about lineage and local history but also about who acted like a lady and who was treated as a free man; they talked about hair follicles and foot shapes but also about who was invited around to visit and who was allowed to dance at the ball; they justified their opinions with references to race science and biblical truth but also with the impervious confidence that they knew Negroes when they saw them and they could sense “black blood” the way an alligator could sense a storm (Hodes, forthcoming; Johnson 1996; Gross 1995).38 Most importantly, they argued openly about what it was they were talking about. **Racial identity, their testimony reveals, was as much a contested practice as a codified presumption.** And if race was as much practice as it was presumption, the racial edifice remained vulnerable to occasional subversion by those upon whom it depended to act it out. Recently, historians like Victoria Bynum (1992) and Martha Hodes (forthcoming) have searched out areas of the antebellum South where the social relations script stopped making sense, where interracial social life and sexual practice provided a continual counterpoint to official ideology. Many of the cases cited by Morris suggest a similar set of **subversions of the race-slavery nexus**: cases in which black slaves came into conflict with poor white people. What is interesting about these cases is not (only) that black slaves regularly gave the lie to race-slavery ideology by refusing to play the part they had been assigned but that slaveholding and nonslaveholding white people continually found themselves unable to agree on what that part was. Murder, rape, arson, and assault: it has always puzzled historians that slaves accused of these crimes came to trial at all. Looking back through the decades of vigilante lynching and state-sponsored terror, historians have asked how it was that “justice” for black slaves sometimes included the trials and procedures so apparently absent from postbellum racial regulation. Southern lawmakers gave one answer: they defined slaveholders’ unwillingness to see their slaves punished by the state as a matter of financial interest, and they tried to buy the slaveholders off by giving them a fair price for their convicted property. Historians (again including Morris) have followed the courts, defining these cases as conflicts between the slaveholders’ property interest in their slaves and the general interests of their class and communities (see also Genovese 1974a; Tushnet 1981). But the question as I have posed it-the difference between “justice” in the antebellum South, a society based on slavery, and “justice” in the postbellum South, a society based on race-suggests that “private property versus public safety” may be an inadequate accounting of what was at stake in these cases-unless we rethink what we mean by “property.” Cheryl Harris (1993) has recently noted the way in which “whiteness” is a form of property, a jealously guarded entitlement that allows its possessors to expect that events will break in their favor (see also Roediger 1991). It was surely this kind of property right-the legal privilege of acting out their whiteness- that nonslaveholding white people were asserting when they stopped slaves along the sides of Southern roads and asked them questions, and it was this type of property that made them believe they deserved honest and respectful answers, and made them angry if they received otherwise, and it was this type of property that made them believe that assaults on their persons or possessions were attacks on the social order, and that (white) slaveholders would join with them in punishing those responsible. When they sought compensation for the damage to their whiteness, however, these nonslaveholders often found themselves facing the same enemy they had faced on the road: s l a v e r ~Asked to choose between their own slaves and their nonslaveholding neighbors, slaveholders could be counted on to side with the slaves: they valued their own property rights, those defined by slavery, more than they did the property claims their nonslaveholding neighbors rooted in whiteness. Slaveholders’ stake in these conflicts was, arguably, more complicated than simple economic interest. After all, Kenneth Greenberg (1996, 16) has recently added his name to the long list of historians who think that slaveholders were less likely to calculate their interests in dollars and cents than in honor and reputation. And I have argued that slaveholders’ own social identities as masters, men, and so on were embodied in the very slaves upon whom nonslaveholding whites attempted to exert their own peculiar brand of property right (Johnson 1995, 81-136; 1996). But even if we figure the slaveholders’ interest in contesting these cases in narrow economic terms, the larger point remains the same: the Southern courts were full of cases in which nonslaveholders contended with slaveholders over who had what rights to slaves. These, then, were class conflicts between whites which were themselves expressed and experienced in terms of race, over which rights followed from whiteness and which from slavery, over exactly how far nonslaveholding white people could hold property in their own race if that meant interfering with other people’s slaves. As Barbara Fields has put it: “Race became the ideological medium through which people posed and apprehended basic questions of power and dominance, sovereignty and citizenship, justice and right. Not only questions involving the status and condition of black people, but also those involving relations between whites who owned slaves and whites who did not were drawn into these terms of reference, as a ray of light is deflected when it passes through a gravitational field” (1982, 162; see also E. Higginbotham 1992).

## 1AR

### Pesmimisn

#### No social death—history proves

Brown 9—Vincent, Prof. of History and African and African-American Studies @ Harvard Univ. [December, “Social Death and Political Life in the Study of Slavery,” *American Historical Review*, p. 1231-1249]

THE PREMISE OF ORLANDO PATTERSON’S MAJOR WORK, that enslaved Africans were natally alienated and culturally isolated, was challenged even before he published his influential thesis, primarily by scholars concerned with “survivals” or “retentions” of African culture and by historians of slave resistance. In the early to mid-twentieth century, when Robert Park’s view of “the Negro” predominated among scholars, it was generally assumed that the slave trade and slavery had denuded black people of any ancestral heritage from Africa. The historians Carter G. Woodson and W. E. B. Du Bois and the anthropologist Melville J. Herskovits argued the opposite. Their research supported the conclusion that while enslaved Africans could not have brought intact social, political, and religious institutions with them to the Americas, they did maintain significant aspects of their cultural backgrounds.32 Herskovits ex- amined “Africanisms”—any practices that seemed to be identifiably African—as useful symbols of cultural survival that would help him to analyze change and continuity in African American culture.33 He engaged in one of his most heated scholarly disputes with the sociologist E. Franklin Frazier, a student of Park’s, who empha- sized the damage wrought by slavery on black families and folkways.34 More recently, a number of scholars have built on Herskovits’s line of thought, enhancing our understanding of African history during the era of the slave trade. Their studies have evolved productively from assertions about general cultural heritage into more precise demonstrations of the continuity of worldviews, categories of belonging, and social practices from Africa to America. For these scholars, the preservation of distinctive cultural forms has served as an index both of a resilient social personhood, or identity, and of resistance to slavery itself. 35 Scholars of slave resistance have never had much use for the concept of social death. The early efforts of writers such as Herbert Aptheker aimed to derail the popular notion that American slavery had been a civilizing institution threatened by “slave crime.”36 Soon after, studies of slave revolts and conspiracies advocated the idea that resistance demonstrated the basic humanity and intractable will of the enslaved—indeed, they often equated acts of will with humanity itself. As these writ- ers turned toward more detailed analyses of the causes, strategies, and tactics of slave revolts in the context of the social relations of slavery, they had trouble squaring abstract characterizations of “the slave” with what they were learning about the en- slaved.37 Michael Craton, who authored Testing the Chains: Resistance to Slavery in the British West Indies, was an early critic of Slavery and Social Death, protesting that what was known about chattel bondage in the Americas did not confirm Patterson’s definition of slavery. “If slaves were in fact ‘generally dishonored,’ ” Craton asked, “how does he explain the degrees of rank found among all groups of slaves—that is, the scale of ‘reputation’ and authority accorded, or at least acknowledged, by slave and master alike?” How could they have formed the fragile families documented by social historians if they had been “natally alienated” by definition? Finally, and per- haps most tellingly, if slaves had been uniformly subjected to “permanent violent domination,” they could not have revolted as often as they did or shown the “varied manifestations of their resistance” that so frustrated masters and compromised their power, sometimes “fatally.”38 The dynamics of social control and slave resistance falsified Patterson’s description of slavery even as the tenacity of African culture showed that enslaved men, women, and children had arrived in the Americas bearing much more than their “tropical temperament.” The cultural continuity and resistance schools of thought come together pow- erfully in an important book by Walter C. Rucker, The River Flows On: Black Re- sistance, Culture, and Identity Formation in Early America. In Rucker’s analysis of slave revolts, conspiracies, and daily recalcitrance, African concepts, values, and cul- tural metaphors play the central role. Unlike Smallwood and Hartman, for whom “the rupture was the story” of slavery, Rucker aims to reveal the “perseverance of African culture even among second, third, and fourth generation creoles.”39 He looks again at some familiar events in North America—New York City’s 1712 Coromantee revolt and 1741 conspiracy, the 1739 Stono rebellion in South Carolina, as well as the plots, schemes, and insurgencies of Gabriel Prosser, Denmark Vesey, and Nat Turner—deftly teasing out the African origins of many of the attitudes and actions of the black rebels. Rucker outlines how the transformation of a “shared cultural heritage” that shaped collective action against slavery corresponded to the “various steps Africans made in the process of becoming ‘African American’ in culture, orientation, and identity.”40

#### Death is bad and worse

Bauman 95 Zygmunt Bauman, University of Leeds Professor Emeritus of Sociology, 1995, Life In Fragments: Essays In Postmodern Morality, p. 66-71

The being‑for is like living towards‑the‑future: a being filled with anticipation, a being aware of the abyss between future foretold and future that will eventually be; it is this gap which, like a magnet, draws the self towards the Other,as it draws life towards the future, making life into an activity of overcoming, transcending, leaving behind. The self stretches towards the Other, as life stretches towards the future; neither can grasp what it stretches toward, but it is in this hopeful and desperate, never conclusive and never abandoned stretching‑toward that the self is ever anew created and life ever anew lived. In the words of M. M. Bakhtin, it is only in this not‑yet accomplished world of anticipation and trial, leaning toward stubbornly an‑other Other, that life can be lived ‑ not in the world of the `events that occurred'; in the latter world, `it is impossible to live, to act responsibly; in it, I am not needed, in principle I am not there at all." Art, the Other, the future: what unites them, what makes them into three words vainly trying to grasp the same mystery, is the modality of possibility. A curious modality, at home neither in ontology nor epistemology; itself, like that which it tries to catch in its net, `always outside', forever `otherwise than being'. The possibility we are talking about here is not the all‑too‑familiar unsure‑of‑itself, and through that uncertainty flawed, inferior and incomplete being, disdainfully dismissed by triumphant existence as `mere possibility', `just a possibility'; possibility is instead `plus que la reahte' ‑ both the origin and the foundation of being. The hope, says Blanchot, proclaims the possibility of that which evades the possible; `in its limit, this is the hope of the bond recaptured where it is now lost."' The hope is always the hope of *being fu filled,* but what keeps the hope alive and so keeps the being open and on the move is precisely its *unfu filment.* One may say that the paradox *of hope* (and the paradox of possibility founded in hope) is that it may pursue its destination solely through betraying its nature; the most exuberant of energies expends itself in the urge towards rest. Possibility uses up its openness in search of closure. Its image of the better being is its own impoverishment . . . The togetherness of the being‑for is cut out of the same block; it shares in the paradoxical lot of all possibility. It lasts as long as it is unfulfilled, yet it uses itself up in never ending effort of fulfilment, of recapturing the bond, making it tight and immune to all future temptations. In an important, perhaps decisive sense, it is selfdestructive and self‑defeating: its triumph is its death. The Other, like restless and unpredictable art, like the future itself, is a *mystery.* And being‑for‑the‑Other, going towards the Other through the twisted and rocky gorge of affection, brings that mystery into view ‑ makes it into a challenge. That mystery is what has triggered the sentiment in the first place ‑ but cracking that mystery is what the resulting movement is about. The mystery must be unpacked so that the being‑for may focus on the Other: one needs to know what to focus on. (The `demand' is *unspoken,* the responsibility undertaken is *unconditional;* it is up to him or her who follows the demand and takes up the responsibility to decide what the following of that demand and carrying out of that responsibility means in practical terms.) Mystery ‑ noted Max Frisch ‑ (and the Other is a mystery), is an exciting puzzle, but one tends to get tired of that excitement. `And so one creates for oneself an image. This is a loveless act, the betrayal." Creating an image of the Other leads to the substitution of the image for the Other; the Other is now fixed ‑ soothingly and comfortingly. There is nothing to be excited about anymore. I know what the Other needs, I know where my responsibility starts and ends. Whatever the Other may now do will be taken down and used against him. What used to be received as an exciting surprise now looks more like perversion; what used to be adored as exhilarating creativity now feels like wicked levity. Thanatos has taken over from Eros, and the excitement of the ungraspable turned into the dullness and tedium of the grasped. But, as Gyorgy Lukacs observed, `everything one person may know about another is only expectation, only potentiality, only wish or fear, acquiring reality only as a result of what happens later, and this reality, too, dissolves straightaway into potentialities'. Only death, with its finality and irreversibility, puts an end to the musical‑chairs game of the real and the potential ‑ it once and for all closes the embrace of togetherness which was before invitingly open and tempted the lonely self." `Creating an image' is the dress rehearsal of that death. But creating an image is the inner urge, the constant temptation, the *must* of all affection . . . It is the loneliness of being abandoned to an unresolvable ambivalence and an unanchored and formless sentiment which sets in motion the togetherness of being‑for. But what loneliness seeks in togetherness is an end to its present condition ‑ an end to itself. Without knowing ‑ without being capable of knowing ‑ that the hope to replace the vexing loneliness with togetherness is founded solely on its own unfulfilment, and that once loneliness is no more, the togetherness ( the being‑for togetherness) must also collapse, as it cannot survive its own completion. What the loneliness seeks in togetherness (suicidally for its own cravings) is the foreclosing and pre‑empting of the future, cancelling the future before it comes, robbing it of mystery but also of the possibility with which it is pregnant. Unknowingly yet necessarily, it seeks it all to its own detriment, since the success (if there is a success) may only bring it back to where it started and to the condition which prompted it to start on the journey in the first place. The togetherness of being‑for is always in the future, and nowhere else. It is no more once the self proclaims: `I have arrived', `I have done it', `I fulfilled my duty.' The being‑for starts from the realization of the bottomlessness of the task, and ends with the declaration that the infinity has been exhausted. This is the tragedy of being‑for ‑ the reason why it cannot but be death‑bound while simultaneously remaining an undying attraction. In this tragedy, there are many happy moments, but no happy end. Death is always the foreclosure of possibilities, and it comes eventually in its own time, even if not brought forward by the impatience of love. The catch is to direct the affection to staving off the end, and to do this against the affection's nature. What follows is that, if moral relationship is grounded in the being-for togetherness (as it is), then it can exist as a project, and guide the self's conduct only as long as its nature of a project (a not yet-completed project) is not denied. Morality, like the future itself, is forever not‑yet. (And this is why the ethical code, any ethical code, the more so the more perfect it is by its own standards, supports morality the way the rope supports the hanged man.) It is because of our loneliness that we crave togetherness. It is because of our loneliness that we open up to the Other and allow the Other to open up to us. It is because of our loneliness (which is only belied, not overcome, by the hubbub of the being‑with) that we turn into moral selves. And it is only through allowing the togetherness its possibilities which only the future can disclose that we stand a chance of acting morally, and sometimes even of being good, in the present

#### Framing issue – evaluate racial progress using regression – qualitative gains have been solidified – future progression is determine by effectiveness of deliberation.

Clark 95 (Leroy – Professor of Law at Catholic University Law School, A Critique of Professor Derrick A. Bell's Thesis of the Permanence of Racism and His Strategy of Confrontation, 73 Denv. U.L. Rev. 23, p. Lexis)

I must now address the thesis that there has been no evolutionary progress for blacks in America. Professor Bell concludes that blacks improperly read history if we believe, as Americans in general believe, that progress--racial, in the case of blacks--is "linear and evolutionary." n49 According to Professor Bell, the "American dogma of automatic progress" has never applied to blacks. n50 Blacks will never gain full equality, and "even those herculean efforts we hail as successful will produce no more than temporary 'peaks of progress,' short-lived victories that slide into irrelevance." n51 Progress toward reducing racial discrimination and subordination has never been "automatic," if that refers to some natural and inexorable process without struggle. Nor has progress ever been strictly "linear" in terms of unvarying year by year improvement, because the combatants on either side of the equality struggle have varied over time in their energies, resources, capacities, and the quality of their plans. Moreover, neither side could predict or control all of the variables which accompany progress or non-progress; some factors, like World War II, occurred in the international arena, and were not exclusively under American control. With these qualifications, and a long view of history, blacks and their white allies achieved two profound and qualitatively different leaps forward toward the goal of equality: the end of slavery, and the Civil Rights Act of 1964. Moreover, despite open and, lately, covert resistance, black progress has never been shoved back, in a qualitative sense, to the powerlessness and abuse of periods preceding these leaps forward. n52

#### Tiny o/w

**Bostrom, ‘11** Nick Bostrom, Professor in the Faculty of Philosophy & Oxford Martin School, Director of the Future of Humanity Institute, and Director of the Programme on the Impacts of Future Technology at the University of Oxford, recipient of the 2009 Eugene R. Gannon Award for the Continued Pursuit of Human Advancement, holds a Ph.D. in Philosophy from the London School of Economics, 2011 (“The Concept of Existential Risk,” Draft of a Paper published on ExistentialRisk.com, Available Online at <http://www.existentialrisk.com/concept.html>, Accessed 07-04-2011)

Holding probability constant, risks become more serious as we move toward the upper-right region of figure 2. For any fixed probability, existential risks are thus more serious than other risk categories. But just how much more serious might not be intuitively obvious. One might think we could get a grip on how bad an existential catastrophe would be by considering some of the worst historical disasters we can think of—such as the two world wars, the Spanish flu pandemic, or the Holocaust—and then imagining something just a bit worse. Yet if we look at global population statistics over time, we find that these horrible events of the past century fail to register (figure 3). [Graphic Omitted] Figure 3: World population over the last century. Calamities such as the Spanish flu pandemic, the two world wars, and the Holocaust scarcely register. (If one stares hard at the graph, one can perhaps just barely make out a slight temporary reduction in the rate of growth of the world population during these events.) But even this reflection fails to bring out the seriousness of existential risk. What makes existential catastrophes especially bad is not that they would show up robustly on a plot like the one in figure 3, causing a precipitous drop in world population or average quality of life. Instead, their significance lies primarily in the fact that they would destroy the future. The philosopher Derek Parfit made a similar point with the following thought experiment: I believe that if we destroy mankind, as we now can, this outcome will be much worse than most people think. Compare three outcomes: (1) Peace. (2) A nuclear war that kills 99% of the world’s existing population. (3) A nuclear war that kills 100%. (2) would be worse than (1), and (3) would be worse than (2). Which is the greater of these two differences? Most people believe that the greater difference is between (1) and (2). I believe that the difference between (2) and (3) is very much greater. … The Earth will remain habitable for at least another billion years. Civilization began only a few thousand years ago. If we do not destroy mankind, these few thousand years may be only a tiny fraction of the whole of civilized human history. The difference between (2) and (3) may thus be the difference between this tiny fraction and all of the rest of this history. If we compare this possible history to a day, what has occurred so far is only a fraction of a second. (10: 453-454) To calculate the loss associated with an existential catastrophe, we must consider how much value would come to exist in its absence. It turns out that the ultimate potential for Earth-originating intelligent life is literally astronomical. One gets a large number even if one confines one’s consideration to the potential for biological human beings living on Earth. If we suppose with Parfit that our planet will remain habitable for at least another billion years, and we assume that at least one billion people could live on it sustainably, then the potential exist for at least 1018 human lives. These lives could also be considerably better than the average contemporary human life, which is so often marred by disease, poverty, injustice, and various biological limitations that could be partly overcome through continuing technological and moral progress. However, the relevant figure is not how many people could live on Earth but how many descendants we could have in total. One lower bound of the number of biological human life-years in the future accessible universe (based on current cosmological estimates) is 1034 years.[10] Another estimate, which assumes that future minds will be mainly implemented in computational hardware instead of biological neuronal wetware, produces a lower bound of 1054 human-brain-emulation subjective life-years (or 1071 basic computational operations).(4)[11] If we make the less conservative assumption that future civilizations could eventually press close to the absolute bounds of known physics (using some as yet unimagined technology), we get radically higher estimates of the amount of computation and memory storage that is achievable and thus of the number of years of subjective experience that could be realized.[12] Even if we use the most conservative of these estimates, which entirely ignores the possibility of space colonization and software minds, we find that the expected loss of an existential catastrophe is greater than the value of 1018 human lives. This implies that the expected value of reducing existential risk by a mere one millionth of one percentage point is at least ten times the value of a billion human lives. The more technologically comprehensive estimate of 1054 human-brain-emulation subjective life-years (or 1052 lives of ordinary length) makes the same point even more starkly. Even if we give this allegedly lower bound on the cumulative output potential of a technologically mature civilization a mere 1% chance of being correct, we find that the expected value of reducing existential risk by a mere one billionth of one billionth of one percentage point is worth a hundred billion times as much as a billion human lives. One might consequently argue that even the tiniest reduction of existential risk has an expected value greater than that of the definite provision of any “ordinary” good, such as the direct benefit of saving 1 billion lives. And, further, that the absolute value of the indirect effect of saving 1 billion lives on the total cumulative amount of existential risk—positive or negative—is almost certainly larger than the positive value of the direct benefit of such an action.[13]