# 1AC

### Plan

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

### Preemption

#### 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.

#### 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.

#### 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.

#### The president will comply

KRINER 10 Assistant professor of political science at Boston University [Douglas L. Kriner, “After the Rubicon: Congress, Presidents, and the Politics of Waging War”, page 228-231]

Conclusion

The sequence of events leading up to the sudden reversal of administration policy and the dramatic withdrawal of U.S. Marines from Lebanon clearly demonstrates that open congressional opposition to Reagan's conduct of the mission in Beirut was critically important in precipitating the change in course. By tracing the pathways of congressional in- fluence, the case study achieves two important objectives. First, it vividly illustrates Congress's capacity to influence the scope and duration of a use of force independent of major shifts in public opinion and changing conditions on the ground. The analysis makes clear that there was no dramatic shift in public opinion after the Beirut barracks bombing that compelled the Reagan administration to withdraw the Marines; in fact, in the wake of the attack the public rallied behind the president. As such, opponents of Reagan's policies in Congress initially fought against the tide of public opinion, and the modest decline in popular support for the president's handling of the Lebanon mission occurred only after a sustained campaign against the deployment on Capitol Hilt.89 Similarly, the administration's own internal analysis of the situation in early January 1984 makes clear that changing conditions on the ground did not necessitate a dramatic change in the nature of the Marine mission. Indeed, by the National Security Council's own estimate, some conditions in the region were actually improving. Instead, administration officials repeatedly emphasized domestic pressures to curtail the scope and duration of the Marine mission.90 Moreover, as the political and military situation in Lebanon worsened in late January and early February 1984, it is interesting that a number of key administration officials publicly and privately believed that there was a direct link between congressional opposition at home and the deterioration of the situation on the ground in the Middle East.

Second, the case study illustrates how the formal and informal congressional actions examined in the statistical analyses of chapter 4 affected presidential decision-making through the proposed theoretical mechanisms for congressional influence over presidential conduct of military affairs developed in chapter 2. Vocal opposition to the president in Congress-expressed through hearings and legislative initiatives to curtail presidential authority, and the visible defection from the White House of a number of prominent Republicans and erstwhile Democratic allies-raised the political stakes of staying the course in Lebanon. Nothing shook Reagan's basic belief in the benefits to be gained from a strong, defiant stand in Beirut. But the political pressure generated by congressional opposition to his policies on both sides of the aisle raised the likely political costs of obtaining these policy benefits. Congressional opposition also influenced the Reagan administration's decision-making indirectly by affecting its estimate of the military costs that would have to be paid to achieve American objectives. In the final analysis, through both the domestic political costs and signaling mechanisms discussed in chapter 2 , congressional opposition contributed to the administration's ultimate judgment that the benefits the United States might reap by continuing the Marine mission no longer outweighed the heightened political and military costs necessary to obtain them.

Finally, while the Marine mission in Lebanon is admittedly but one case, it is a case that many in the Reagan administration believed had important implications for subsequent military policymaking. In a postmortem review, Don Fortier of the National Security Council and Steve Sestanovich at the State Department warned that the debacle in Lebanon raised the possibility that, in the future, the decision to use force might be akin to an all-or-nothing decision. "If the public and Congress reject any prolonged U.S. role (even when the number of troops is small)," the administration analysts lamented, "we will always be under pressure to resolve problems through briefer, but more massive involvements-or to do nothing at all." Thus, from the administration's "conspicuously losing to the Congress" over Lebanon policy, Fortier and Sestanovich argued that the White House would have to anticipate costly congressional opposition if similar actions were launched in the future and adjust its conduct of military operations accordingly, with the end result being a "narrowing of options" on the table and more "limited flexibility" when deploying major contingents of American military might abroad.91 This last point echoes the first anticipatory mechanism posited in chapter 2, and reminds us that Congress need not overtly act to rein in a military action of which it disapproves for it to have an important influence on the scope and duration of a major military endeavor. Rather, presidents, having observed Congress's capacity to raise the political and tangible costs of a given course of military action, may anticipate the likelihood of congressional opposition and adjust their conduct of military operations accordingly.

### Cyber Strategy

#### Cyber has become the NEW NUCLEAR strategy – our cyber attack policy is born from rational thought that has become irrational with anxiety and obsession with victory via rapid response that has pushed us dangerously close to full on attacks. Getting rid of OCOs authority transforms cyber strategy.

Burke 09 Associate Professor of Politics and International Relations

(Anthony, Nuclear Reason: At the Limits of Strategy, International Relations 23: 506-529 2009, December)

**Working between nuclear history and recent development**s, and between philosophical critique and strategic debate, **this article seeks to ask some hard questions about the viability of nuclear strategy as a system of reason.** While this is certainly not the first piece of writing to do so,16 it is worth revisiting the issue now because of the widely stated fears that the non-proliferation regime is in imminent danger of collapse in ways that will radically undermine stable deterrence, at the same time as **there remains a strong belief in the utility and legitimacy of nuclear weapons amongst many academic and government strategists.17** The article’s normative inspiration derives from Kant’s moral philosophy and the critique of pragmatism and instrumental reason in critical theory,18 and its **analytical methodology,** is an adaptation of Foucault’s dynamic history **of ‘problematizations’: the critical examination of processes through which problems are constructed and defined; knowledge developed, fought over and applied; institutions, practices and subjectivities established; and fields of reality thus enabled and transformed.** **It is also informed by his advice ‘not to take as a whole the rationalisation of society or of culture, but to analyse this process in several fields’.19 It is a method that throws light on how human constructions constitute and affect the real; however, in contrast to Foucault, the article will emphasise how this often occurs in ways that their architects never intended, and in ways that resist and complicate the processes of rationalisation that gave birth to them**. **The ‘problematization’ here placed under particular scrutiny is that which,** following the creation of nuclear weapons at Los Alamos and their use in Japan, **began to ponder whether and how the new weapons could be assimilated into national policy frameworks and modern** (that is, Clausewitzian) **ideas of strategy.** This is the story of Brodie’s *The Absolute Weapon*. However the article shifts register away from the rich and often considered academic debate about nuclear strategy to consider, both during the Cold War and more recently, how the rationalisations of theorists and policymakers coalesced to generate nuclear policies that, whatever their differences of scale and context, exhibit a powerful continuity: a conviction in the rationality of nuclear weapons as instruments of state. **Ever more sophisticated strategic analysis** sought to develop doctrines **for the manufacture, deployment,** threat and use of nuclear weapons for US and European security, only to find fatal problems continually emerging that could not be solved by the next RAND study or analytical permutation. While there is a difference of moral scale between Cold War strategies which threatened to destroy hundreds of millions and newer strategies which envision much more limited nuclear use (that may at worst kill tens of thousands**), it is probably better to** avoid moral hair splitting and **acknowledge that what have long underpinned the rationalistic anxiety about the viability of nuclear strategy are powerful moral intuitions about the illegitimacy of using such weapons in anger**. My concern, however, is that **moral revulsion has little impact when policymakers feel confronted by perceived strategic necessities and failures of trust,** which today are manifested in arguments about uncertainty and hedging.20 Whatever the weight of such concerns, **it is time** to accept that most strategies we can imagine contain unbearable risks of failure. The only **exceptions** are those **strategies that** will be needed for a world that has both few (or no) nuclear weapons and the nevepr-eradicable capability to build them. **These** will **look most unlike the strategies of the past, and** **will replace** Clausewitzian **concerns with prosecuting national policy through force with** collective security of a profound kind**.** My use of the framing idea ‘**nuclear reason’ is not a claim about an overarching ‘nuclear enlightenment’**, of the kind made by William Walker in an important 2007 *International Affairs* article, **where** he warns of the non-proliferation system breaking down because of powerful actors stepping outside its norms. Here he argued that national nuclear deterrence strategies and the international legal non-proliferation regime came after 1960 to form a coherent ‘grand enlightenment project’: **a ‘nuclear ordering strategy … rooted in a belief that security and stability lay** – and transcendence might eventually lie – **in regulative action … through the institutions of deterrence, arms control and the non-proliferation regime’**.21 Notwithstanding the great significance of his essay, Walker’s broader claim is problematic. **It conflates state and cosmopolitan forms of reason into an imagined harmony, and thus neglects the power play and unhappy compromise inherent in the NPT regime** – tensions that have only worsened as it has aged. To the extent that policymakers may have felt such an accommodation between national security and international law to have been ideal, I argue that it is not sustainable and support Walker’s conclusion that ‘given the many dangers of nuclear catastrophe arising from the behaviour of states and non-state actors in a globalizing environment, the pursuit of nuclear disarmament has a security logic that is stronger than ever’.22 Another point of difference is that, where Walker saw US policy during the Cold War as an attempt to balance deterrence with non-proliferation based on ‘reason, containment and mutual obligation’,23 this article highlights **US and Soviet** nuclear strategic options that sought to make nuclear weapons usable or otherwise undermined strategic stability. It explores how the inner **logics of nuclear reason** during this period – especially the repetitive **concern** **that threats and deployment options were not credible or survivable enough to ensure deterrence,** thus pushing deterrence perilously close to pre-emption – **drove the arms race and created unacceptable risks of nuclear war.** Like post-Renaissance military strategy, nuclear strategy is certainly a modern phenomenon – an extreme (if **not** the only) culmination of a modern desire to use science, technology and political science to control and make use of human and natural material for instrumental ends.24 As such **it bears the marks of the darker, more mechanistic qualities of the Enlightenment** (what Horkheimer and Adorno25 called ‘rationality in domination’) **and challenges its more hopeful, critical qualities, which sought to place reason under critique and enhance human dignity.** However, **this** article’s **ambition is** more limited than Walker’s – **not to see nuclear politics and policy as a grand teleological project, but to locate its perseverance in a powerful, self-enclosed form of strategic reason that encompasses both conventional and mass destruction weapons, and runs along lines of logic that are self-defeating and dangerous**. Laid out in this form, the **analysis is meant as a contribution to** Marianne Hanson’s call for ‘**an informed critical security studies project that explicitly tackles the question of nuclear weapons at a global level’**.26 The practical and ethical test, in **this perspective, is whether the system will enable a profound and enduring security for all human beings**. While we can appreciate that governments have important responsibilities to their own citizens, merely *national* policy or security imperatives, especially those that place others at grave risk, are inadequate.

#### We endorse a mode of politics that engages the government directly – only that can understand the complexity and intersubjectivities that the Cold War created – this is a prerequisite to solving global problems

Kennedy-Pipe 07 Professor of IR at the University of Warwick

(caroline, At a Crossroads – and Other Reasons to be Cheerful: The Future of International Relations, *International Relations* 2007; 21; 351

My suggestion for the future of the discipline is that, fi rst, we forget about it as a discipline. It is not. When asked about his ‘fi eld’ the late Ernest Gellner (who had held chairs in philosophy, sociology and anthropology) used to reply ‘I’m not a donkey! I don’t have a fi eld.’ Exactly so; and in International Relations (or International Studies) we do not have a discipline. Rather we have a meeting point, or even perhaps a crossroads. Philip Windsor, one of the best and most acute British scholars of the ‘international’ of the last 50 years, observed that International Relations is better seen as a ‘crossroads, rather than as an academic discipline’, a crossroads where many disciplines meet. That is why it is such an exciting place to be. How could anyone suppose that to understand something as protean as war, or the global economy, or the interweaving of domestic and international politics you could look at them from only one standpoint, say the political one? No: there are **historical dimensions, economic dimensions, scientifi c and technological dimensions and philosophical and ethical ones. All of these voices must have a part in our understanding and thus in that crossroads that is International Relations. To eliminate any of them would be to cheapen all of them and short cut our own possibilities of understanding any of them.** For me, I think the best way of highlighting **the centrality and importance** (and intrinsic interest) **of our crossroads is to focus our attention on the real-world dilemmas people face.** And, yes, politicians are people too. Raymond Aron, another great International Relations scholar (though he too was active in many other areas as well), always used to say that whenever he was asking about politics or international affairs he would always ask ‘What would I have done had I been in the position of X?’ Answering ‘I wouldn’t ever let myself be in that position’ was, for Aron, the mistake – and the delusion – of people like Sartre. And it was a path that led towards the elimination of real choice and the valorisation of the abstract**.** In one of my own fi elds of study, for example – the Cold War and its history and impact – that claim of Aron’s needs constantly to be remembered. **For statesman** – **and** the occasional **stateswoman**, such as Margaret Thatcher or Indira Ghandi – **the Cold War was a shifting collage of assumptions, choices and decisions. Each decision could influence the next, often in ways unintended or unforeseen by its originator.** The Cold War **and the decisions taken during the years of confrontation with Communism** casts long shadows down to our own time. We need only think of, say, the experiences of Osama bin Laden during the war in Afghanistan to see that events have multiple consequences. To simply assume that one can ‘reject’ all of that complexity**,** that one should adopt an automatic stance of ‘bad faith’ for elites **and the decisions they made** – as Noam Chomsky has done with the United States, for example – is not merely unfair on those decision-makers as individuals**,** itblocks off the possibility of real understanding of the ebbs and flows of world politics which are precisely not ‘determined’ **in the way that he appears to think.** But **this rejection** does not simply emerge from the Chomskyite left; it **is precisely the mirror image of this one finds in ‘social scientific’ accounts of International Relations that stress ‘material forces’ or ‘rational choice’ as a ‘structural determinant of action’** (and as an explanandum as well). What I would say is that **the** ‘British’ **way in international studies is to accept its ‘messiness’ and to work with it: to cut with the grain of trying to understand the ‘shapes and shadows’ that make up our complex,** endlessly contestable – and endlessly exciting **– field.** **Our students and the public are right that what matters is the world out there and the choices we all have to make in it.** Of course, **‘**theorising’suchchoices – either normatively or in terms of how we might come to know and understand – is a perfectly good angle of vision. But it is certainly not the only one and it should go hand in hand with the others. In Britain, then – and indeed in Europe more generally – I think there is good reason to be pleased – which is, of course, not the same as self-satisfied. **We do not need to cringe about the alleged US ‘dominance’ of the field for the simple reason that** – in the sense I have been using the term here **– it does not exist. If scholars in the United States want to keep excluding themselves from the ways in which people really engage with IR, so much the worse for them**. For the rest of us, we can just get on with the job**. Some might argue that it is a bit rich to be ‘cheerful’ about the fact that there are so many wars and conflicts, so much poverty and disease, and so many vested interests that block serious or meaningful reform about the way international relations operates**. But my argument would be simply that, of course, **no one is cheerful about that – but rather that understanding why and how there are wars and conflicts, or poverty and disease, or powerful vested interests, is the first step to being able to do something about them.** That is what those enthusiastic students sense when you give them a book or an article that discusses International Relations as it should be discussed – rather than turning it into the social scientific version of sudoku. One of the twentieth century’s most interesting commentators on International Relations, Walter Lippman, once remarked to a room full of political journalists that what they did was to try and read what not everyone could (or had the time) to read, to interpret events for those who were not there when they occurred, who cannot research their causes or interview and debate with those involved. ‘We are right to be proud of this’, Lippman told his audience, ‘and be glad that it is our work.’ While the academy has, of course, a different role from even the best political journalism or commentary (and Lippman’s was among the very best) – a role that asks hard questions of all kinds, of the shapes and shadows that go to make up the world of International Relations – so we too can be proud of what we do in the study of International Relations, and be glad that it is our work.

#### This presentation in debate form prevents corruption of rationality by encouraging dissent and discussion and places constrains on secret actions with opaque reasoning

Payne 07 Professor of IR at the university of Louisville

(Rodger, Neorealists as Critical Theorists: The Purpose of Foreign Policy Debate, Perspectives on Politics (2007), **5**:**3**:503-514 Cambridge University Press

In various recent interviews and papers, Mearsheimer and other neorealists have gone even further toward aligning with the critical or constructivist positions about the importance of political communication and public debate. Most notably, Mearsheimer frequently now argues, as do critical theorists, that the veracity of public debate is central to assuring the well-being of democratic life. [46](http://journals.cambridge.org/action/displayFulltext?type=6&fid=1300784&jid=&volumeId=&issueId=03&aid=1300776&bodyId=&membershipNumber=&societyETOCSession=&fulltextType=RA&fileId=S1537592707071514#fn46#fn46) In his paper on “Lying in International Politics,” Mearsheimer wrote that “Democracies work best when they include a reasonably efficient marketplace of ideas, which can only work when citizens are given reliable information and there are high levels of transparency and honesty.” [47](http://journals.cambridge.org/action/displayFulltext?type=6&fid=1300784&jid=&volumeId=&issueId=03&aid=1300776&bodyId=&membershipNumber=&societyETOCSession=&fulltextType=RA&fileId=S1537592707071514#fn47#fn47) Stephen Van Evera made a similar argument concerning the need for public debate about biological and technological research on potential weapons of mass destruction. “**If the progress of science risks bringing the democratization of the power to destroy,** the public has a right to know this and form a reasoned response**.** **We should acknowledge a duty to put the matter before the world so that all of society can together consider what response would be most appropriate.**” [48](http://journals.cambridge.org/action/displayFulltext?type=6&fid=1300784&jid=&volumeId=&issueId=03&aid=1300776&bodyId=&membershipNumber=&societyETOCSession=&fulltextType=RA&fileId=S1537592707071514#fn48#fn48) Perhaps even more importantly, some neorealists argue thatopendebate fosters selection of the best policy choices. In their widely-discussed March 2006 article on the influence of the Israeli lobby, Mearsheimer and Walt condemned “the Lobby's” apparent ability to limit public deliberation in the American democracy. Truly opendebate would expose the limits of current policy and “could move the U.S. to a position more consistent with its ownnationalinterest**.”** [49](http://journals.cambridge.org/action/displayFulltext?type=6&fid=1300784&jid=&volumeId=&issueId=03&aid=1300776&bodyId=&membershipNumber=&societyETOCSession=&fulltextType=RA&fileId=S1537592707071514#fn49#fn49) In his 2004 Graduation Address at the University of Chicago, Mearsheimer claimed that “**the best way to maximize the prospects of producing a sound foreign policy is to expose it early on to the marketplace of ideas**.” [50](http://journals.cambridge.org/action/displayFulltext?type=6&fid=1300784&jid=&volumeId=&issueId=03&aid=1300776&bodyId=&membershipNumber=&societyETOCSession=&fulltextType=RA&fileId=S1537592707071514#fn50#fn50)Like critical theorists, these neorealists worry that **public discussion of** foreign policy is too often marred by secrecy **and dishonesty of public officials**—and in the cited examples **normatively urge improved deliberative practices** **to promote democracy** and superior outcomes. In fact, their own contributions to these debates promote the kind of transparency and public accountability they purport to seek. Contra their theoretical critique, which emphasizes fixed and enduring raison d'étre, these neorealists **embrace reflective processes as a means by which to construct ideal outcomes**. “I think that scholars can go a long way towards making that debate richer and healthier,” Mearsheimer claims [51](http://journals.cambridge.org/action/displayFulltext?type=6&fid=1300784&jid=&volumeId=&issueId=03&aid=1300776&bodyId=&membershipNumber=&societyETOCSession=&fulltextType=RA&fileId=S1537592707071514#fn51#fn51) Indeed, presaging the advice of the Coalition for a Realistic Foreign Policy, he asserts thatscholars should actively try to intervene in foreign policy discussions. In an April 2002 interview conducted at the University of California, Berkeley, Mearsheimer noted **that academics “should study problems that are of great public importance, and when we come to our conclusions regarding those problems, we should go to considerable lengths to communicate our findings to the broader population, so that we can help influence the debate in positive ways**.” He noted that professors in private institutions in the U.S., as well as those with tenure at public institutions, have the freedom to speak openly on matters of great interest and to make significant contributions to public deliberation. “I thinkwe have a very important responsibility to talk about important issues, and to challenge conventional wisdoms **that other people might be unwilling to challenge. We have a real social responsibility here**.” [52](http://journals.cambridge.org/action/displayFulltext?type=6&fid=1300784&jid=&volumeId=&issueId=03&aid=1300776&bodyId=&membershipNumber=&societyETOCSession=&fulltextType=RA&fileId=S1537592707071514#fn52#fn52) In a newspaper interview about the provocative article on the Israeli lobby, Mearsheimer acknowledged that he and Walt aimed to promote debate and take their concerns out of the closet.[53](http://journals.cambridge.org/action/displayFulltext?type=6&fid=1300784&jid=&volumeId=&issueId=03&aid=1300776&bodyId=&membershipNumber=&societyETOCSession=&fulltextType=RA&fileId=S1537592707071514#fn53#fn53) This is a remarkably deliberative perspective, going a long way towards embracing what constructivist scholar Thomas Risse calls “argumentative rationality.” [54](http://journals.cambridge.org/action/displayFulltext?type=6&fid=1300784&jid=&volumeId=&issueId=03&aid=1300776&bodyId=&membershipNumber=&societyETOCSession=&fulltextType=RA&fileId=S1537592707071514#fn54#fn54) This conception of social responsibility certainly takes ideas and persuasion seriously**,** if not the pursuit of collective truth. After all, the realists acting alone or together in the Coalition for a Realistic Foreign Policy ultimately intervene in public debates to help steer the American ship of state in the most appropriate direction. Scholars like Mearsheimer want others to recognize “that they're part of the body politic and that **the** ideas that they are developing should be articulated to the body politic for the purposes of influencing thepublicdebate and particular policies in important ways.” [55](http://journals.cambridge.org/action/displayFulltext?type=6&fid=1300784&jid=&volumeId=&issueId=03&aid=1300776&bodyId=&membershipNumber=&societyETOCSession=&fulltextType=RA&fileId=S1537592707071514#fn55#fn55) Quite apparently, realist skepticism about the value of political communication in international relations theory does not deter many of these same scholars from engaging in political debate about foreign policy with national leaders, who may well employ cheap talk, lies, or other distortions to carry a point. In these instances, **realists value** at least their own **discursive attempts to shape foreign policy choices and correct the different falsehoods**. A number of important **realists** seem to believe, and often **declare outright, that public argument not only influences the search for the best policy choice, but it can also promote deliberative ideals and public accountability**. At minimum, public debate about policy establishes the groundwork for negative feedback and promotes the search for truth and legitimate decisions in the marketplace of ideas.

#### Requiring prior Congressional authorization for war deters adventurism

Dickerson 9 – Annette Warren Dickerson, Director of Education & Outreach for the Center for Constitutional Rights, “Restore. Protect. Expand. Amend the War Powers Resolution”, Center for Constitutional Rights White Paper, http://ccrjustice.org/files/CCR\_White\_WarPowers.pdf

Reform the War Powers Resolution

The War Powers Resolution has failed. Every president since the enactment of the Act has considered it to be unconstitutional. Presidents have generally not filed a report that would start the 60-day clock running, despite repeated executive introduction of armed forces into places like Indochina, Iran, Lebanon, Central America, Grenada, Libya, Bosnia, Haiti, Kosovo and Somalia, among others. Congress has usually not challenged this non-compliance. And, the judiciary has persistently refused to adjudicate claims challenging executive action as violating the War Powers Resolution, holding that members of Congress have no standing to seek relief, or that the claim presents non-justifiable political questions.

The War Powers Resolution, as written, was flawed in several key respects. The first flaw was that the Resolution imposed no operative, substantive limitations on the executive’s power to initiate warfare, but rather created a time limit of 60 days on the president’s use of troops in hostile situations without explicit congressional authorization. This approach was a mistake, because as a practical matter it recognized that the President could engage in unilateral war-making for up to 60 days, or 90 days with an extension. But the Constitution requires that Congress provide authorization prior to initiating non-defensive war, not within a period of months after warfare is initiated. As history has demonstrated time and again, it is difficult to terminate warfare once hostilities have begun. The key time for Congress to weigh in is before hostilities are commenced, not 60 or 90 days afterward.

Secondly, the War Powers Resolution correctly recognized that even congressional silence, inaction or even implicit approval does not allow the president to engage in warfare – but it failed to provide an adequate enforcement mechanism if the president did so. Under the resolution, wars launched by the executive were supposed to be automatically terminated after 60 or 90 days if not affirmatively authorized by Congress – but this provision proved unenforceable. Presidents simply ignored it, Congress had an insufficient interest in enforcing it and the courts responded by effectually saying: if Congress did nothing, why should we?

Reforming the War Powers Resolution is a project that will require leadership from the President and the political will of Congress, working together in the service and preservation of the Constitution. In light of the abuses that have taken place under the Bush administration, it is the responsibility of a new administration to insist on transparency in the drafting of new legislation.

There is a long history of attempts to revise the War Powers Resolution. As new legislation is drafted, though, it will be important to focus on the central constitutional issues. Much time has been spent in debating how to address contingencies. It will be impossible to write into law any comprehensive formula for every conceivable situation, though; much more important will be establishing the fundamental principles of reform:

The War Powers Resolution should explicitly prohibit executive acts of war without previous Congressional authorization. The only exception should be the executive’s power in an emergency to use short-term force to repel sudden attacks on US territories, troops or citizens.

It is true that many potential conflict situations will be murky, complicated or divisive, and that quick congressional action may not always be forthcoming. Yet, history shows the folly of launching wars that are not supported by the American people. The United States should not use military force until a substantial consensus develops in Congress and the public that military force is necessary, appropriate and wise.

Today, as in 1787, the reality is that the interests of the people of the United States are best served if the Congress retains the power to declare war, and the President’s unilateral power to use American forces in combat should be reserved to repelling attacks on American troops or territories and evacuating citizens under actual attack. Repelling does not equate retaliation for an attack on an American city that occurred in the past, be it several days, weeks or months prior; it also does not mean launching a surprise invasion of a nation that has not attacked us. Repelling similarly does not permit the inflation of supposed threats against US citizens as justification to invade another country, as was the case in the Dominican Republic in 1965 and Grenada in 1983. The president can respond defensively to attacks that have been launched or are in the process of being launched, but not to rumors, reports, intuitions, or warnings of attacks. Preventive war, disguised as preemptive war, has no place in constitutional or international law.

#### Preventitve forsight is key.

Hayward, 2006 (Peter C., Ph.D. from Swinburne University of Technology, From Individual to Social Foresight, The Case for Foresight, November 8, http://adt.lib.swin.edu.au/uploads/approved/adt-VSWT20061108.153623/public/02whole.pdf)

The second response is commonly referred to as `TINA', (There Is No Alternative). However, there are alternatives and this is the primary justification for this research. Rather than accepting the `default' future of queue sera, there is the possibility of considering what future(s) we wish to live in; and of taking steps in the present to increase the likelihood of `desired' futures and to reduce the likelihood of the `undesired' ones. To do this is to employ foresight. Foresight is an innate capability of every person, and it operates in us as an adjunct to other human capabilities like experiential learning (Bell 1997). Rather than having to experience a challenge in order to learn how best to manage it, foresight allows us to prepare for a challenge and even to take actions to prevent the challenge occurring. Most importantly through social modelling, the advantages gained from the foresight of one person can be gifted to others, thereby making foresight a social as well as an individual capability. It is an explicit wish of many that we do not want to have to experience dystopia in order to learn how to prevent it. While there is a relationship between foresight and experience it is to be hoped that we do not require the latter in order to engage the former (Slaughter 2002b). If we have to wait until the challenges to our survival are so obvious before we take them seriously, then there will be no way back from the brink. If we want to maintain and realise notions of social justice, humanity and dignity for all, rather than human worth determined through social Darwinism, then it must be through purposeful human action. Foresight that can separate out the retrograde elements from our Western inheritance will play a significant role in such a process (Gaspar & Novaky 2002). Figure 1.1 is a simple representation of the intent of this thesis. The vertical axis represents an increasing scale of challenges over time. To respond to this the horizontal axis represents the expansion of our foresight capacity, both individual and social, over time. As the challenges to existence grow in scale then so to must our foresight capacities. The dotted line represents the belief that expanding foresight capacities will give us the ability to anticipate, perceive and act on our present and future challenges and thereby produce a trajectory of preferable futures for ourselves and future generations. The nature of human existence is that we will continue to face challenges into the future. Existence is precarious, and precious. No matter how good our thinking and technologies are, we will continue to face an increasing scale of challenges to our existence. Our ancestors were aware of localised challenges. We, on the other hand, are aware of planetary challenges. Furthermore as we learn more about our planet and the galactic neighbourhood more challenges will be detected. This research seeks to make a contribution to understanding the expansion of foresight capacities and thereby, in some small way, to the trajectory towards preferable futures.

# 2AC

## Case

### 2AC Overivew

#### Bureaucratic decision making has corrupted politics – the inertia that the president has to give orders of cyber operations and subsequently nuclear use makes.

#### Cyber Space has become NEW NUCLEAR strategy – our cyber attack policy is born from rational thought – the idea that we can control the vaste interconnected cyber space through the use of offensive posture, but anxiety and obsession with victory via rapid response has turned the cyber game into a global war of attrition.

#### Prefer our impact for explanatory power – OCO authority allows the president to get away with a nasty echo chamber of authority –

#### Too much entrenched resistance to the alternative exists in complexity that the Cold War has left us – the alternative fails to account for all the different reasons why the status quo is the way it is – this will leave in place bureaucratized politics that relies on quick – hair-trigger responses. Current bureaucratic politics is self-enclosed and insulates itself from alien discourses – the alternative will be shut out – That’s Kennedy

### 2AC Condo

#### Conditionality is a voting issue for fairness and education

#### A. Makes debate sophistry – Time and strat skew—makes it impossible to generate offense and forces shallow debating—kills advocacy skills

#### B. Justifies contradictions—illogical and force us to double turn

#### C. One conditional advocacy solves

#### Turns their args – role of the ballots that are conditional uniquely take out their first-priroty type args and prevents coherent critique.

## Complexity

### Framework

#### We get to weigh the implications of our affirmative with the framing that we presented it – they get their alt – ignoring the entire 1ac is unfair. hypothetical policymaking is important – facilitates real understanding of global complexities – kennedy.

#### Political Engagement with law is key. Communicative mechanism that question the validity of cyber pre-emption become institutionalized – this serves to check administrative power and fundamentally shifts societal interests.

#### Critiquing cyber ops in the context of nuclear issues is important –

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)

A historical analogy might be drawn to the study of nuclear issues. In many ways, today’s state of affairs regarding public discourse on cyberattack is analogous to the nuclear debate of 50 years ago. At that time, nuclear policy issues were veiled in secrecy, and there was little public debate about them. Herman Kahn’s books (On Thermonuclear War, Thinking the Unthinkable) were the first that addressed in the open literature what it might mean to fight a nuclear war. These seminal pieces did much to raise the public profile of these issues and stimulated an enormous amount of subsequent work outside government that has had a real impact on nuclear policy. From our perspective as the co-chairs of this study, the topic of cyberattack is so important across a multitude of national interests—not just defense or even just national security—that it deserves robust and open discussion and debate, both among thoughtful professionals in the policy, military, intelligence, law enforcement, and legal fields and among security practitioners in the private sector. But for such discussion and debate to be productive, they must be based on some common foundation of information about the topic at hand. Thus,the report’s role in providing education and background is in our view its most important function.

#### The alt fails – tangible policy steps are critical to changing public thinking about nukes

USITW 09 (US in the World Initiative, “Talking about Nuclear Weapons with the Persuadable Middle”, November, http://www.stanleyfoundation.org/Talking\_About\_Nuclear\_Weapons\_-\_Final\_Report.pdf)

Advocates need to remember the stereotypes that the public has about progressives—caring more about domestic/social programs than national security. And, research has repeatedly shown that the American public is willing to pay any price to keep the U.S. safe. Implications for Communicators: If advocates are going to make the case that the U.S. nuclear arsenal is a drain on our pocketbook, advocates first must overcome the perception that nuclear weapons are a necessary and valuable part of our security apparatus. Additionally, advocates must steer clear of anything that could sound like a “guns vs. butter” argument and instead focus on more effective and efficient ways to safeguard the U.S. Advocates must take advantage of the public’s initial support by “blocking” concerns about policy before those concerns can be inflamed by opponents. This means that advocates must be proactive in re-framing nuclear weapons as themselves a source of risk, and **advancing the idea that there are tangible steps** (or a process) by which reductions (and eventual elimination) can occur. In addition, advocates must avoid some tempting pitfalls – like discussing good vs. bad countries and allowing for the need to retain our arsenals for deterrence purposes. The story we are telling hangs together and research suggests that it can promote a different kind of public thinking about nuclear weapons that leads to support for some of the policy choices we advocate. Now the challenge is to tell that story consistently, coherently, and over time.

### AT: Episteme

#### Permutation do the plan and explore the gaps of 1AC knolwexle

#### Epistemology is irrelevant – truth comes from many different epistemological grounds – invalid arguments are readily apparent

Wight 07 Department of Politics, School of Humanities and Social Science, University of Exeter

(Colin, Inside the epistemological cave all bets are off, Journal of International Relations and Development, 2007, 10, (40–56)

In some respects, this might seem to place me close to the position that Kratochwil suggests is absurd. For is not my position a form of ‘anything goes’? Well, again agreeing with Kratochwil that we should reject traditional logic and its associated yes or no answers, I will reply both yes and no.10 Yes, it is an ‘anything goes’position insofar as I reject outright that we need to commit ourselves to any particular epistemological position in advance of making or judging particular knowledge claims. I can see no good reason for giving any specific epistemological standpoint a position of a priori privilege. But I can also answer no because this position does not mean that we are unable to make informed judgements on the basis of the evidence for the claim. The fact that philosophers have been unable to provide secure foundations for one or other epistemological stance does not alter the fact that we continue to use these positions to get along in the world. In this respect, I agree completely with Kratochwil’s claim (2007: 11) that both absolute certainty and absolute doubt are impossible positions to hold, and that we ‘go on’in a situation located somewhere in between. It may be philosophically naı¨ve of me to claim that if I wish to know how many cars are parked in my drive, then the easiest way is to probably go and look. But I can do this without needing philosophy to prove empiricism infallible. Equally, in certain circumstances I might be able to ascertain how many cars are in my drive without looking; if, for example, I know that at time T1 that there were three cars and that one went away at time T2, then, if asked at time T3 (assuming these events are sequential), I have a legitimate case to say ‘two’. Of course, in either case, I could still be wrong but the point is that the claim about the existence of a certain number of cars can justifiably be supported on various epistemological grounds and we do not know in advance which will be the most appropriate. Hence the context in which the claim emerges is also an important aspect of its validity. In both cases, there is no doubt that observation or the process of rational deduction is theoretically laden, but to say that our concepts help carve up the world in certain ways is not to accept that they either determine the physicality of what exists or can, in all cases, stop an object from existing.

### 2AC Politics of Risk

#### Unique offense – This is OUR ARGUMENT. The conjunctive fallacy has pervaded the squo bureaucratic thinking of officials. They believe that one offensive attack will be able to take out all of china’s space assets or nuclear assets, but ignore the EXTREME complexity and inter-connectedness of infrastructures – this causes escalating wars, meltdowns, etc.

#### We also don’t link – our arg is that we CANNOT KNOW the complexity of a cyber attack therefore we shouldn’t try or attempt to use them pre-emptively on targets beyond the scope of our squo reach.

#### WE think the 1AC Role of the ballot is superior in THIS CONTEXT – who did the better debating – their role of the ballots will be inherently self-serving and arbitrary – the only question is impact calc.

#### 1) infinite regression – they could always make it about the team that best addresses hetero-normativity, or gender discrimination, or native rights wins the debates. It moots any aff predictability because we come here to win that our resolutional advocacy is a net good

#### 2) Moots the 1AC – allowing a K to come prior to the aff means that refutation becomes impossible – necessary to decision making and topic education – they cant CP away our offense, it sets the bar too high they can effectively PIC out a single word

#### Our affect is DOESN’T LINK – ours is a fundamentally defensive – we think there is a bad affect in the squo of US preemption – security justifications have been used to attack everyone – our aff is a restraint on the president authority to use those justufications to attack

**Reducing existential risk by even a tiny amount outweighs every other impact — the math is conclusively on our side.**

**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]

#### 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.

#### Our affect is DOESN’T LINK – ours is a fundamentally defensive – we think there is a bad affect in the squo of US preemption – security justifications have been used to attack everyone – our aff is a restraint on the president authority to use those justufications to attack

#### 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.

#### 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

#### Securitizing cyber space is the ONLY way to prevent large scale cyber war – the alt can’t solve fast enough or change US doctrine – vulnerability creates a Unique need for it

Pickin 12 (Matthew, MA War Stuides – Kings College, “What is the securitization of cyberspace? Is it a problem?”, http://www.academia.edu/3100313/What\_is\_the\_securitization\_of\_cyberspace\_Is\_it\_a\_problem)

In evaluating whether securitization of cyberspace is a problem, it is very clear that securitization is a growing concern with many complications. There are many issues including privacy, regulation, surveillance, internet regulation and the growing tension in the international system. However, because the United States is a superpower contesting with other cyber-heavyweights such as Iran, Russia and China the issue will not be de-securitized in the short term. With the discovery and use of cyber-weapons, many states are in the process of making their own for defensive and offensive purposes. The government of the United States will not de-securitize the issue of cyberspace while there are rival states and groups which prove a threat to the national security agenda. These problems will continue to exist until there is no defensive agenda and the issue is de-securitized, for now securitization is a necessary evil.

#### Existential threat doesn’t promote securitization – we use it to challenge concentration of power in the executive. This is a more effective challenge to security.

Michael **WILLIAMS** Graduate School of Public and International Affairs, University of Ottawa **’11** “Securitization and the liberalism of fear” *Security Dialogue* 42 p. 457-459 [acronyms clarified – Turner]

These dynamics point to a second area where the liberalism of fear can play a restraining role in securitization. Since it sees the **abuse of power** as a **continual possibility**, the liberalism of fear seeks its **controlled dispersal** and stresses the importance of pluralism in combating its potential excesses. Socially, multiple centres of power provide sites from which securitizations can be contested and resisted. Importantly, however, this is a pluralism that is conscious of the limits of the facile political rationalism that so exercised critics of liberalism throughout the first half of the 20th century, and that has had such an important influence on the development of the discipline of international relations as a whole and parts of securitization theory in particular.14 Both in its philosophic foundations and in its historical awareness of past liberal failings, the pluralism of the liberalism of fear is markedly distant from that of its ‘depoliticized’ predecessors. This alternative vision of liberalism provides an intriguingly different connection between the Copenhagen School and classical realism, for while the lion’s share of attention in this area has been devoted to their shared concerns with the nature of ‘the political’ and the role of enmity in countering the potentially debilitating effects of liberal pluralism, this has tended to obscure the ways in which classical realists such as Morgenthau sought to counter and restrain the role of fear and enmity in political life rather than embracing it. And, intriguingly, one of the chief instruments that they advocated in this battle was pluralism. In contrast to the idea (all too automatically accepted in some discussions of securitization theory) that liberal pluralism was inescapably atomizing and socially debilitating, and that liberal societies were inevitably forced to call upon a politics of enmity in order to recover and secure their properly ‘political’ foundations, classical realists presented a much more subtle and sophisticated vision of the merits of pluralism and its role in supporting solidarity within a liberal society (Tjalve, 2007). As William Scheuerman has shown in his revealing recovery of this ‘progressive’ dimension of realism, pluralism could help offset the politics of fear and could be valued by citizens for precisely this reason. As he puts it: For Progressive Realists, as for some astute present-day analysts, social integration was at least as much a matter of ‘doing’ as ‘being’: concrete social practices which generated meaningful cooperation and relations of trust could prove even more vitalthan shared notions of collective destiny.... Progressive Realists underscored the pivotal role of a pluralistic social order in which one could identify a rich variety of cross-cutting social cleavages and loyalties, which they thought most likely to mitigate intense conflict. Under the proper conditions, social pluralism potentially civilized conflict: social actors could learn that a rival in one social arena might be an ally or even a friend in another (Scheuerman, 2011: 174–5). This concern with the merits of pluralism as a mechanism for limiting fearful power, as well as for restraining the politics of fear, also finds clear expression in liberalism’s stress on institutional pluralism. Here, the rule of law, the division of power between different institutions of government, the desire that they check and balance each other, and the dispersal of power among a wide range of civil society actors also provide important bulwarks against securitization in a liberal society. Consider again in this context Salter’s (2011: 128) treatment of the fate of TIA [Total Information Awareness] when, despite the endeavours of George W. Bush’s administration, as a result of initiatives ‘spearheaded by library, privacy, and libertarian groups, funding for the TIA (whether terrorist or total) was halted by the US Senate in July 2003’. Here, social and institutional pluralism combine to render difficult, and potentially even to reverse, emergency decisions characteristic of securitization.15 As Jef Huysmans (2004) has articulately demonstrated, the admonition to ‘mind the gap’, to prevent any of the institutions of a liberal-democratic polity from usurping the roles of the others – something particularly worrisome when the politics of security is involved – is a vital component of a liberal-democratic polity. The importance of the fear that this might happen, the institutional positions, principled resources and public perceptions that actors may be able to draw on, or be constrained by, as a consequence of this fear, and the combined role of these elements in countering the logics of extremity and emergency in liberal societies should not be underestimated. The rule of law provides similar lessons. While the aftermath of 9/11 and the actions of George W. Bush’s administration have led many to see securitized liberal societies as embracing a ‘permanent emergency’ and adopting a generalized politics of exception, it is not at all clear that these appraisals do not reflect a series of a priori claims about the supposed (philosophic) necessity of enmity in (and for) liberal polities more than they do careful and concrete analysis of the actual practices in those polities.16 Despite the rhetoric and, in many ways, the efforts of the Bush administration to ‘break free from rules’, it is at best questionable that it was in fact able completely to do so – and the significant opposition to its policies from social actors as well as in challenges in a variety of legal forums demonstrate the limits of its securitizing acts as clearly as they do their pervasiveness. **Securitization theory** has shown relatively **little interest** in the **legal dynamics** and debates surrounding **emergency powers**, an engagement with them seemingly closed off either by an acceptance that issues like Guantanamo Bay already reside in the domain of ‘security’ or by a preference for claims about the decisionistic nature of law and the exceptionality of Schmittian-inspired legal theory and visions of sovereignty.17 But, if we take fear seriously, law – and especially the ‘laws of fear’ (Sunstein, 2005; see also Ackerman, 2006) – becomes a **crucial battleground** in the politics of securitization. The actors involved in these struggles are not the security professionals of state security institutions and their associates analysed by Didier Bigo and others, but they are professionals of security in the wider sense of the politics of fear – and the fear of fear. Despite the seemingly general acceptance by the political institutions and much of the population of the USA that Al-Qaeda was indeed an existential threat, the use of all extraordinary means was not accepted, nor did the situation resemble a ‘**generalized exception’** brought about through the claims of security. Take the use of torture as a policy, for instance. As Salter (2011: 126) points out, and numerous political and legal analyses have gone to great lengths to assess, in the USA ‘the courts and the populace rejected the use of torture for interrogation – even if it was accepted by some part of the military and bureaucratic establishment’. Salter sees this as calling for a new category in securitization theory: the **acceptance of existential threat**, but the **failure to authorize extraordinary powers.** I speculate that it might also be assessed in terms of a struggle within and over the politics of fear, and the existence and operation of countervailing practices and powers. The liberalism of fear may thus help explain how these practices function, with both the attitudes of individuals and the institutional pluralism with which they are entwined providing restraints upon the logic of security and significant points of resistance against the powerful (but not all-powerful) actors who attempted to mobilize it.

#### Alt cant solve

#### Decreasing existential risks are key!

**Anissimov, ‘04** — Michael Anissimov, science and technology writer focusing specializing in futurism, founding director of the Immortality Institute—a non-profit organization focused on the abolition of nonconsensual death, member of the World Transhumanist Association, associate of the Institute for Accelerating Change, member of the Center for Responsible Nanotechnology's Global Task Force, 2004 (“Immortalist Utilitarianism,” Accelerating Future, May, Available Online at <http://www.acceleratingfuture.com/michael/works/immethics.htm>, Accessed 09-09-2011)

The value of contributing to Aubrey de Grey's anti-aging project assumes that there continues to be a world around for people's lives to be extended. But if we nuke ourselves out of existence in 2010, then what? The probability of human extinction is the gateway function through which all efforts toward life extension must inevitably pass, including cryonics, biogerontology, and nanomedicine. They are all useless if we blow ourselves up. At this point one observes that there are many working toward life extension, but few focused on explicitly preventing apocalyptic global disaster. Such huge risks sound like fairy tales rather than real threats - because we have never seen them happen before, we underestimate the probability of their occurrence. An existential disaster has not yet occurred on this planet. The risks worth worrying about are not pollution, asteroid impact, or alien invasion - the ones you see dramaticized in movies - these events are all either very gradual or improbable. Oxford philosopher Nick Bostrom warns us of existential risks, "...where an adverse outcome would either annihilate Earth-originating intelligent life or permanently and drastically curtail its potential." Bostrom continues, "Existential risks are distinct from global endurable risks. Examples of the latter kind include: threats to the biodiversity of Earth’s ecosphere, moderate global warming, global economic recessions (even major ones), and possibly stifling cultural or religious eras such as the “dark ages”, even if they encompass the whole global community, provided they are transitory." The four main risks we know about so far are summarized by the following, in ascending order of probability and severity over the course of the next 30 years: Biological. More specifically, a genetically engineered supervirus. Bostrom writes, "With the fabulous advances in genetic technology currently taking place, it may become possible for a tyrant, terrorist, or lunatic to create a doomsday virus, an organism that combines long latency with high virulence and mortality." There are several factors necessary for a virus to be a risk. The first is the presence of biologists with the knowledge necessary to genetically engineer a new virus of any sort. The second is access to the expensive machinery required for synthesis. Third is specific knowledge of viral genetic engineering. Fourth is a weaponization strategy and a delivery mechanism. These are nontrivial barriers, but are sure to fall in due time. Nuclear. A traditional nuclear war could still break out, although it would be unlikely to result in our ultimate demise, it could drastically curtail our potential and set us back thousands or even millions of years technologically and ethically. Bostrom mentions that the US and Russia still have huge stockpiles of nuclear weapons. Miniaturization technology, along with improve manufacturing technologies, could make it possible to mass produce nuclear weapons for easy delivery should an escalating arms race lead to that. As rogue nations begin to acquire the technology for nuclear strikes, powerful nations will feel increasingly edgy. Nanotechnological. The Transhumanist FAQ reads, "Molecular nanotechnology is an anticipated manufacturing technology that will make it possible to build complex three-dimensional structures to atomic specification using chemical reactions directed by nonbiological machinery." Because nanomachines could be self-replicating or at least auto-productive, the technology and its products could proliferate very rapidly. Because nanotechnology could theoretically be used to create any chemically stable object, the potential for abuse is massive. Nanotechnology could be used to manufacture large weapons or other oppressive apparatus in mere hours; the only limitations are raw materials, management, software, and heat dissipation. Human-indifferent superintelligence. In the near future, humanity will gain the technological capability to create forms of intelligence radically better than our own. Artificial Intelligences will be implemented on superfast transistors instead of slow biological neurons, and eventually gain the intellectual ability to fabricate new hardware and reprogram their source code. Such an intelligence could engage in recursive self-improvement - improving its own intelligence, then directing that intelligence towards further intelligence improvements. Such a process could lead far beyond our current level of intelligence in a relatively short time. We would be helpless to fight against such an intelligence if it did not value our continuation. So let's say I have another million dollars to spend. My last million dollars went to Aubrey de Grey's Methuselah Mouse Prize, for a grand total of billions of expected utiles. But wait - I forgot to factor in the probability that humanity will be destroyed before the positive effects of life extension are borne out. **Even if my estimated probability of existential risk is very low, it is still rational to focus on addressing the risk because my whole enterprise would be ruined if disaster is not averted**. If we value the prospect of all the future lives that could be enjoyed if we pass beyond the threshold of risk - possibly quadrillions or more, if we expand into the cosmos, then we will deeply value minimizing the probability of existential risk above all other considerations. If my million dollars can avert the chance of existential disaster by, say, 0.0001%, then the expected utility of this action relative to the expected utility of life extension advocacy is shocking. **That's 0.0001% of the utility of quadrillions or more humans, transhumans, and posthumans leading fulfilling lives**. I'll spare the reader from working out the math and utility curves - I'm sure you can imagine them. So, why is it that people tend to devote more resources to life extension than risk prevention? The follow includes my guesses, feel free to tell me if you disagree: They estimate the probability of any risk occurring to be extremely low. They estimate their potential influence over the likelihood of risk to be extremely low. They feel that positive PR towards any futurist goals will eventually result in higher awareness of risk. They fear social ostracization if they focus on "Doomsday scenarios" rather than traditional extension. Those are my guesses. Immortalists with objections are free to send in their arguments, and I will post them here if they are especially strong. As far as I can tell however, the predicted utility of lowering the likelihood of existential risk outclasses any life extension effort I can imagine. I cannot emphasize this enough. If a existential disaster occurs, not only will the possibilities of extreme life extension, sophisticated nanotechnology, intelligence enhancement, and space expansion never bear fruit, but everyone will be dead, **never to come back**. **Because the we have so much to lose, existential risk is worth worrying about even if our estimated probability of occurrence is extremely low**. It is not the funding of life extension research projects that immortalists should be focusing on. It should be projects that decrease the risk of existential risk. By default, **once the probability of existential risk is minimized, life extension technologies can be developed and applied.** There are powerful economic and social imperatives in that direction, but few towards risk management. Existential risk creates a "loafer problem" — we always expect someone else to take care of it. I assert that this is a dangerous strategy and should be discarded in favor of making prevention of such risks a central focus.

#### their takeouts are a product of the availability heuristic and “good-story bias”.

**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)

Many kinds of cognitive bias and other psychological phenomena impede efforts at thinking clearly and dealing effectively with existential risk.[32] For example, use of the availability heuristic may create a “good-story bias” whereby people evaluate the plausibility of existential-risk scenarios on the basis of experience, or on how easily the various possibilities spring to mind. Since nobody has any real experience with existential catastrophe, expectations may be formed instead on the basis of fictional evidence derived from movies and novels. Such fictional exposures are systematically biased in favor of scenarios that make for entertaining stories. Plotlines may feature a small band of human protagonists successfully repelling an alien invasion or a robot army. A story in which humankind goes extinct suddenly—without warning and without being replaced by some other interesting beings—is less likely to succeed at the box office (although more likely to happen in reality).

### AT: Cyber Link

#### A catch all security possibly makes action impossible and matters worse – we must combine cyber policy with the alternative strategically – conceptualizing security in terms of intention is a viable vision for change

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

First, too expansive a definition for security would make comparing similar policies essentially impossible, and distinguishing between different policy options inherently difficult (Baldwin 1997, 6). Take, for instance, the types of discussions surrounding counterinsurgency versus counterterrorism policies for the war in Afghanistan, with counterinsurgency being more people centered and counterterrorism being more threat centered. It is important to note that both are centrally concerned with security . But security for whom? And security fro m what? This is where a catch all security concept becomes problematic, for those advocating different positions will, in effect, be arguing for the same thing. And those making these ominous,life and death decisions will be left without the requisite clarity to make prudent, rational, and at times moral, judgments. Secondly, the human security concept has a bearing on bureaucratic questions concerning areas and responsibilities . Should we expect, for instance, the Department of Defense to be putting together clim ate change legislation proposals or running HIV/AIDS relief centers? Conversely, would it be wise to have the State Department, USAID, or the U.S. Geological Survey conducting operational planning? This isn’t to say that there shouldn’t be cross departmental collaboration and exchange, for today’s most complex security problems are often too much to handle for any one department alone. But these different agencies are designed, funded, and staffed according to different criteria and for different purposes. While more holistic approaches are undoubtedly necessary, a more clearly circumscribed security concept will help ensure that 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 the bureaucratic 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.

## Critique

### Anthro

#### Only the permutation solves – we must combine qualified-anthropocentrism with concern for the human-world

Grey, 1993 (William, Lecturer at the University of Queensland, Australia, “Anthropocentrism and Deep Ecology,” Australian Journal of Philosophy, Vol. 71, no 4, 1993, www.uq.edu.au/~pdwgrey/pubs/anthropocentrism.html, acc 9-30-04//uwyo-ajl)

That we habitually assume characteristically anthropocentric perspectives and values is claimed by deep ecologists to be a defect. And as a corrective to this parochialism, we are invited to assume an "ecocentric" (Rolston 1986, Callicott 1989) or "biocentric" (Taylor 1986) perspective. I am not persuaded, however, that it is intelligible to abandon our anthropocentric perspective in favour of one which is more inclusive or expansive. We should certainly abandon a crude conception of human needs which equates them (roughly) with the sort of needs which are satisfied by extravagant resource use. But the problem with so-called "shallow" views lies not in their anthropocentrism, but rather with the fact that they are characteristically short-term, sectional, and self-regarding. A suitably enriched and enlightened anthropocentrism provides the wherewithal for a satisfactory ethic of obligation and concern for the nonhuman world. And a genuinely non-anthropocentric view delivers only confusion.

#### Turn – the idea that animals are equal to humans results in a devaluation of all life, makes the worst atrocities possible

Schmahmann and Polacheck, 1995 (David R. and Lori J., Partners in the firm of Nutter, McLennan & Fish, Boston College Environmental Affairs Law Review, Spring)

In the end, however, it is the aggregate of these characteristics that does render humans fundamentally, importantly, and unbridgeably different from animals, even though it is also beyond question that in individual instances -- for example, in the case of vegetative individuals -- some animals may indeed have higher cognitive skills than some humans. To argue on that basis alone, however, that human institutions are morally flawed because they rest on assumptions regarding the aggregate of human abilities, needs, and actions is to deny such institutions the capacity to draw any distinctions at all. Consider the consequences of a theory which does not distinguish between animal life and human life for purposes of identifying and enforcing legal rights. Every individual member of every species would have recognized claims against human beings and the state, and perhaps other animals as well. As the concept of rights expanded to include the "claims" of all living creatures, the concept would lose much of its force, and human rights would suffer as a consequence. Long before Singer wrote Animal Liberation, one philosopher wrote: If it is once observed that there is no difference in principle between the case of dogs, cats, or horses, or stags, foxes, and hares, and that of tsetse-flies or tapeworms or the bacteria in our own blood-stream, the conclusion likely to be drawn is that there is so much wrong that we cannot help doing to the brute creation that it is best not to trouble ourselves about it any more at all. The ultimate sufferers are likely to be our fellow men [sic], because the final conclusion is likely to be, not that we ought to treat the [\*753] brutes like human beings, but that there is no good reason why we should not treat human beings like brutes. Extension of this principle leads straight to Belsen and Buchenwald, Dachau and Auschwitz, where the German and the Jew or Pole only took the place of the human being and the Colorado beetle. 26

#### The alternative causes massive expansion of governmental authority resulting in totalitarianism

**Schmahmann & Polacheck, 1995** (David R., Lori, Partners in the firm of Nutter, McLennan & Fish, Boston College Environmental Affairs Law Review, Spring)

Reason, history, and an entire intellectual tradition compel a conclusion that any notion that the interests of animals either warrant or can have expression in a constitutional democracy, wholly independent of human interests, risks casting fundamental freedoms on a devious course. Thomas Paine once commented that "[c]ivil rights are those which appertain to man in right of his being a member of society." 56 Paine also wrote the following at the time of the American and French Revolutions: "All power exercised over a nation, must have some beginning. It must be either delegated, or assumed. There are no other sources. All delegated power is trust, and all assumed power is usurpation. Time does not alter the nature and quality of either." 57 Power that arises out of, as opposed to over, the people arises out of the consent of the governed, 58 and the limits of such delegation are carefully defined in a constitution such as ours: The fact therefore must be, that the individuals themselves, each in his own personal and sovereign right, "entered into a compact with each other" to produce a government: and this is the only mode in which governments have a right to arise, and the only principle on which they have a right to exist. 59 Paine defines civil rights as rights with a foundation in "some natural right pre-existing in the individual." 60 Civil rights in a constitutional democracy are those rights the individual reserves to himself after [\*760] delegating to the government those powers necessary to the orderly functioning of society. 61 The question which must arise in the context of any proposal that the government endow rights on animals is how such a notion can be reconciled with the very definition of "rights" in a constitutional democracy. Any real acceptance of the notion must mean reposing in the government a wholly new and undefined set of powers, presumably to be exercised on behalf of an entirely new and vague constituency. The notion contemplates the creation of a vast, unprecedented, intrusive, and uncircumscribable jurisprudence in which the government erects barriers to human conduct on the strength, not of competing human interests -- be they economic, esthetic, or humanitarian -- or the delegation of power to it by individuals, but of assumptions about the interests of animals assessed by the government apart from human interests or experience. Not only may this be impossible, but in the contemplated nonspeciesist world, where there would be no hierarchy within the animal kingdom just as there would be no hierarchy between humans and animals, the "rights" of individual animals would exist in competition with the rights of individual humans. Thus, no rat could be harmed, chicken cooked, or rabbit dissected without government permission or the prospect of government scrutiny. If some government agency were given the power to act in the interest of animals, the result would be the creation of a vast, intrusive structure which would erect barriers to human conduct on the strength, not of competing human interests, but of assessments of the interests of animals conducted without reference to human interests or experience.

#### Suffering is not part of the human condition – rather, it is a result of specific circumstances. Even if some suffering is inevitable, there are degress

Eagen, 2004 (jennifer, “Philisophical interests” September 9 http://home.earthlink.net/~jeagan/id3.html)

Suffering is the theme of two of my published papers, which both examine the question of how philosophy should respond to suffering. Suffering is a mode of living one's body that usually takes into account the ontic features that impact the body. Social and political events are often the cause of suffering, even if the event is painted as natural (example, famine, cancer whose causes are usually greater than just natural). Suffering is often where the body and the social-liguistic order that Foucault talks about meet. Many of the examples that Foucault talks about are examples of suffering, even though he dispassionately displays it without showing the effects of the individual consciousness. Maybe Foucault with a touch more phenomenology is what I'm after. Also, many of the cases of oppression and human rights violations that I deal with in my teaching are examples of suffering to greater or lesser degrees. One challenge that I face as I continue to try to define suffering is how to give an account of suffering and what constitutes suffering. Will the criteria be subjective or objective? Is suffering relative (say between the West and the developing world)? Can we legitimately compare the suffering of different individuals or groups? All good questions. I could argue along with Adorno that suffering is not natural nor is it a permanent feature of the human condition, but is primarily caused by social and political events and conditions. However, I might want to argue something like there are some seemingly permanent features of this social-political landscape that cause everyone to suffer, but to different degrees (e.g., gender). I'm looking forward to exploring this further.

#### Anthropocentrism is inevitable—the alternative links to the critique and makes it impossible to protect the biosphere.

Grey 93 — William Grey, Professor of Philosophy at the University of Queensland, 1993 (“Anthropocentrism and Deep Ecology,” Australiasian Journal of Philosophy, Volume 71, Number 4, Available Online at http://www.uq.edu.au/~pdwgrey/pubs/anthropocentrism.html, Accessed 07-27-2011)

The attempt to provide a genuinely non-anthropocentric set of values, or preferences seems to be a hopeless quest. Once we eschew all human values, interests and preferences we are confronted with just too many alternatives, as we can see when we consider biological history over a billion year time scale. The problem with the various non-anthropocentric bases for value which have been proposed is that they permit too many different possibilities, not all of which are at all congenial to us. And that matters. We should be concerned to promote a rich, diverse and vibrant biosphere. Human flourishing may certainly be included as a legitimate part of such a flourishing. The preoccupations of deep ecology arise as a result of human activities which impoverish and degrade the quality of the planet's living systems. But these judgements are possible only if we assume a set of values (that is, preference rankings), based on human preferences. We need to reject not anthropocentrism, but a particularly short term and narrow conception of human interests and concerns. What's wrong with shallow views is not their concern about the well-being of humans, but that they do not really consider enough in what that well-being consists. We need to develop an enriched, fortified anthropocentric notion of human interest to replace the dominant short-term, sectional and self-regarding conception. Our sort of world, with our sort of fellow occupants is an interesting and engaging place. There is every reason for us to try to keep it, and ourselves, going for a few more cosmic seconds [10].

#### Their radical devotion to ecocentrism fails and collapses into nihilism.

Brown 95 — Charles S. Brown, Professor of Philosophy at Emporia State University, 1995 (“Anthropocentrism and Ecocentrism: the quest for a new worldview,” The Midwest Quarterly, Volume 36, Number 2, Winter, Available Online to Subscribing Institutions via Information Access)

Deep ecologists regularly urge us to replace our anthropocentrism with an ecocentrism which advocates egalitarian attitudes toward all entities and forms in nature. In this suggestion, too, there is both promise and peril. Its promise lies in the hope that we will be able to see ourselves as enjoying a solidarity with nature. This is an expression of the (w)holistic motif present in all forms of ecological thinking. The radical egalitarianism of ecocentrism will, however, collapse into nihilism if no distinctions of value are made. To claim that everything has an equal and intrinsic value to everything else is to value nothing above anything else. Due to my place in the evolutionary-ecological system I cannot value the life of a child in a ghetto tenement and the lives of a family of rats equally. To do so would be to abdicate all value and leave me unable to act. It is a part of the predicament of every species to act from its self interest and to choose to spare the life of any innocent person over the lives of a family of rats in an expression of this evolutionary imperative.

#### Non-anthropocentrism promotes detachment which is conducive to the destruction of the biosphere

Manson 2009 (Neil A, Neil A. Manson is a philosopher at the University of Mississippi. He is the editor of God and Design: The Teleological Argument and Modern Science, and is the author of a number of articles on the topic, “NECESSARY ANTHROPOCENTRISM”, <http://www.environmentalphilosophy.org/ISEEIAEPpapers/2009/Manson.pdf>, Hemanth)

I. THE PLANETARY PERSPECTIVE To be anthropocentric is to regard human beings as of primary importance in the grand scheme of reality. If being ethical requires that we not be anthropocentric, then what should we be instead? To answer “non-anthropocentric” is not to give much real guidance. For our limited minds to reason at all, we must adopt some perspective or other. One standard offering – perhaps the dominant offering in environmental philosophy today – is the perspective of the Earth as a whole. Deep ecologists, biocentrists, land ethicists, environmental holists – whatever the label, all share the belief that taking the planetary perspective is the key to following an environmental ethic. The problem with taking the planetary perspective is that from it, massive environmental damage within the next few centuries can be written off as just a blip on the screen. Suppose we cook and poison the planet, dramatically reducing biodiversity as a result (and perhaps destroying ourselves too). The result many millions of years later would be a biosphere re-set to a different equilibrium, but one with life and biodiversity comparable to that of the planet prior to our degradation of it. To say the biosphere as it is here and now is more valuable than the future one is to be guilty of “temporal parochialism,” to borrow a term from Callicott. Considering our time as but an infinitesimal moment in the three and onehalf billion year tenure of life on planet Earth, the present tendency of man to extirpate and eventually extinguish other species and take over their habitats for himself and his domesticated symbionts might be viewed quite disinterestedly as but a brief transitional stage in the Earth’s evolutionary odyssey. Non-human life will go on even under the worst possible anthropogenic destructive scenario presently conceivable, novel species will radiate anew, and novel ecosystems will mature. The new Age (of Insects, perhaps) will eventually be just as diverse, orderly, harmonious, and stable, and thus no less good than our current ecosystem with its present complement of species.

organic life is teleological and posits the alleviation of suffering and continuation of life as good—it’s biology.

**Schwartz and Wiggins 2010** –Michael A, Department of Psychiatry, University of Hawaii and Obsborne P, Department of Philosophy, University of Louisville, “Psychosomatic medicine and the philosophy of life” Philosophy, Ethics, and Humanities in Medicine 2010, 5:2

As we have said, the metabolic activity of the organism is geared toward sustaining the existence of the organism. This being geared toward the sustaining of its own being shows that the metabolism of the organism is "for the sake of" its own continuation in being. The being that the activity is geared toward preserving is the organism's future being. The metabolic functioning is for the sake of bridging the temporal gap that separates the organism in the present from its own existence in the future. In slightly different terms, metabolic activity serves the temporal enduring of the organism. Hence it is temporal duration that poses the main threat to the organism's contingent existence: the question of whether the organism will endure from moment to moment always remains an unanswered question until the future becomes the present and the organism still lives. And the threat can be defeated only if the activity of metabolism is sustained. Life is thus teleological: the present activity of the living being aims at its own future being [8,9]. If we can speak of the metabolic activity of the organism as occurring "for the sake of" the organism's future being, this means that at some fundamental level the organism posits its own continuation in reality as a "good." In other words, the organism posits its own existence as having a positive value. Value is thus built into the reality of organic life: it is organic life itself that places value there. It is not human beings and certainly not human agency that introduces value into an otherwise value-free universe. Living beings themselves, by striving to preserve themselves, already signal that, at least for the being involved, its own life is a good [10-12]. We can see, then, that the values that motivate medical practice are grounded in organic life itself. While only human beings can develop and practice medical treatment, it is not human beings who introduce into the world the values that call for and justify that treatment. Living beings themselves posit the goodness of an activity that prevents death and alleviates suffering. If for the organism its own continuation is good, then its death would be bad. Hence the moral need to combat death issues from the organism's own internal striving. And therefore the need to treat and hopefully cure the ill organism so that it does not die - at least not before its naturally allotted time - is based on a value that the organism itself posits. The same would be true for suffering and pain, at least for those organism's that can feel. Felt suffering and pain are posited by the organism feeling them as bad. Hence the moral need to relieve and even eradicate pain through medical treatment arises at the most basic levels of life, even if only human beings can recognize this value as a moral requirement and develop the medical techniques to respond to it [11,13].

### AT: Law Bad

#### Laws!

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.

### AT: “war”

#### We should treat war and other violence differently. 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.

#### 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.

#### We should focus on the use of violence as an intentional instrument in international politics – this doesn’t discount structure.

Claire THOMAS Int’l Pol @ Sheffield ’11 “Why don’t we talk about ‘violence’ in International Relations?” *Review of Int’l Studies* 37 p. 1827-1829

One of the most common discussions about violence centres on means and ends. A good social end is sometimes said to justify the means of violence. An example was the argument that the US and UK governments should go to war with Iraq in 2003 in order to stop Saddam Hussein’s atrocities. Gandhi on the other hand stated that the means must be consistent with the ends, as the means will affect the ends. This is a key argument for non-violence. It is important that violence is seen as a means and not an end. The use of violence is not the end position, but an instrument in order to achieve a certain aim.55 The aim is not to artificially rule out of debate an aspect that should or could be considered, or to artificially simplify the concept. Rather, it is to recognise that violence as an instrument is the core meaning of the concept, and stretching it to incorporate a state of violence brings in a vague concept unnecessarily. As I argued earlier, the concept of violence as a state of nature often refers to many acts of direct violence. Where it does not, it usually refers to a state that the author does not like, for example disorder. It could be argued that a state of violence exists when there is a culture of using violence, or many acts of violence make violence ubiquitous. In this case the state of violence is no different to the instrumental meaning, in that the state of violence is referring to an aspect of instrumental violence – its frequent occurrence and so on. In the same way, one could argue that violence is part of human nature, and therefore we can talk about the state of violence within humankind. I would argue that it is true that violence can be a learned pattern of action, or a culture within society. But the act of violence still is perpetrated by an actor, who at some level has a choice about whether to engage in violence, and why. It remains important to restrict the concept of violence to mean an instrument. It is an instrument that can be used to gain many things, from the oppression of another person, to a general state of world disorder, but violence is always a means aimed at achieving a certain aim. Violence is by nature instrumental; like all means, it always stands in need of guidance and justification through the end it pursues. And what needs justification by something else cannot be the essence of anything. The end of war [. . .] is peace or victory; but to the question And what is the end of peace? There is no answer.56 Frazer and Hutchings argue that it is not possible to separate ‘violent doing from violent being’ and that doing so ‘underestimates the levels of ideological and material investment needed to sustain violence as a repertoire for political action’ and overestimates the ability of actors to transcend the use of violence.57 This view should not be discounted. It is certainly important to recognise the structures and beliefs that allow the use of violence to continue so easily. However, this does not need to mean that violence is other than instrumental. Recognising the structures, institutions and beliefs that perpetuate violence can be done at the same time as recognising that violence is an act that is carried out by an actor. Although it should also be recognised that in the real world these links will be complex and the borderlines of violence may be fuzzy. Violence cannot be compared to world peace, or social justice, as they are completely different – they are the end state towards which one may choose to aim. The study of violence in international politics should treat the concept as an instrument. The instrument of violence is always used in order to achieve another aim. This may be positive or negative, and include an aim about other people’s use of violence, for example to create disorder, or to prevent another actor being able to use violence. But the use of violence is a tool nevertheless. Therefore the next question this article will look at is what kind of instrument it is, and what it includes. Aspects of violence A key debate in the definition of violence is whether it includes only acts of commission, or acts of omission also. Honderich illustrates this by asking if the following two scenarios are equally violent: I send a poisoned food parcel to India, and the people who receive it die; I do not give money to Oxfam, and people who could have been helped die. In the first example, the deaths are a direct result of my act. The only way for another person to stop those deaths would be to intervene to stop my act. If I had not been born the act would not have happened. In the second example, the deaths are a result of omissions by many people. Any one of them can act to stop the deaths. If I had not been born the deaths would still occur. Honderich concludes that the difference is intention. Honderich does not classify acts of unintentional or partly unintentional omission as violent.58 By accepting that all violence is intentional, it means that to call an event in international politics violent, we must be able to see some element of choice from the actor involved. This does not mean that structural forces are irrelevant to the subject of violence in international politics. There are clearly strong structural forces at work within the international system, and within relationships at all levels that affect international politics. However, although violence may happen as a result of the structures in society, the actual act of violence itself is intentional, in that it has a conscious actor, it is the result of a decision by the person perpetrating the act. This decision may well be made because the actor thinks he or she has no other option given the circumstances they find themselves in, but it is still an intentional act. Structural violence takes the opposite point of view, and is designed to incorporate into the definition of violence structural aspects which do not have an actor.

# 1AR

#### Especially true for cyber

Pickin 12 (Matthew, MA War Stuides – Kings College, “What is the securitization of cyberspace? Is it a problem?”, http://www.academia.edu/3100313/What\_is\_the\_securitization\_of\_cyberspace\_Is\_it\_a\_problem)

In evaluating whether securitization of cyberspace is a problem, it is very clear that securitization is a growing concern with many complications. There are many issues including privacy, regulation, surveillance, internet regulation and the growing tension in the international system. However, because the United States is a superpower contesting with other cyber-heavyweights such as Iran, Russia and China the issue will not be de-securitized in the short term. With the discovery and use of cyber-weapons, many states are in the process of making their own for defensive and offensive purposes. The government of the United States will not de-securitize the issue of cyberspace while there are rival states and groups which prove a threat to the national security agenda. These problems will continue to exist until there is no defensive agenda and the issue is de-securitized, for now securitization is a necessary evil.