# 1AC

### Plan

#### The United States federal government should statutorily prohibit the authority of the President of the United States to authorize the preemptive use of offensive cyber-attacks.

### Adv- CyberWar

#### The Squo offensive cyber posture attacks risk retaliatory cycles and arms races

Moss 13

Columnist at The Diplomat Trefor Moss is an independent journalist based in Hong Kong. He covers Asian politics, defence and security, and was Asia-Pacific Editor at Jane’s Defence Weekly until 2009, Is Cyber War the New Cold War?, 4/19/13, <http://thediplomat.com/2013/04/19/is-cyber-war-the-new-cold-war/2/>

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](http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?_r=4&) 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 21stcentury 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.

#### New rules change the restrained conduct of cyberwar up to this point – grant Obama unfettered power do define the threat – makes a cyber aggression inevitable

RT 13 < Hacker in chief: Obama given right to launch 'preemptive' cyberattacks, Published time: February 04, 2013 18:39, http://rt.com/usa/obama-us-administration-cyber-435/>#SPS

¶ A secret review has concluded that US President Obama has the authority to launch a preemptive cyber attack on any country on the basis that they are considered a ‘cyber threat’ – even if there is no concrete evidence of this threat.¶ It may not be long before the US conducts crippling attacks on foreign soil with little more than a mouse click, thereby sparing itself the effort of sending its military oversees or declaring war.¶ The Obama administration is currently drawing up a set of rules about how the US military can defend against or conduct cyberattacks, the New York Times reports. The Obama administration is also allowing intelligence agencies to declare potential threats. But even if these threats are nothing more than a suspicion without evidence, the military now has the authority to attack foreign nations, regardless of whether or not the US is involved in a conflict with them.¶ This would not only spare the US from sending its own troops overseas, but it would also allow the administration to make decisions without the deliberation that usually occurs before sending Americans into a conflict zone. And if the administration conducts an attack based on false premises, it would be saved the embarrassment that occurred when President George W. Bush sent thousands of US troops into a war with Iraq that lasted nearly 9 years, based on the false premise that Iraq possessed weapons of mass destruction and was a security threat.¶ With no overseas deployments necessary to conduct a cyberattack, the administration would have nothing to lose by anonymously targeting and destroying infrastructure based on its own suspicions of a threat. The administration’s new rules would also allow the military to operate domestically, the thought of which has always made many people uncomfortable. The White House in October [signed](http://rt.com/usa/news/directive-military-deployment-us-892/) a presidential policy directive that aims to “finalize new rules of engagement that would guide commanders when and how the military can go outside government networks to prevent a cyberattack that could cause significant destruction or casualties.”¶ A senior administration official told the Times that the US has so far kept its cyber capabilities restrained and that the new rules could allow the administration to exercise its full potential.¶ “There are levels of cyberwarfare that are far more aggressive than anything that has been used or recommended to be done,” the official said.¶ The administration has already used computer worms to cripple other countries’ infrastructure, including a series of attacks against Iran’s nuclear power plants, one of which took out nearly 1,000 of the 5,000 centrifuges of the Natanz plant. The attack was controlled from inside the Pentagon, which now has a new Cyber Command and a growing budget that would allow it to conduct more extensive cyberattacks. ¶ The Pentagon’s foundation of such an office demonstrates the administration’s preparation for cyberwarfare, in which both the US and terrorists can strike each other by taking down power grids, financial systems and communications networks. The Cyber Command office is experiencing a growing budget, while the Department of Defense is preparing for spending cuts and is slashing budgets for other Pentagon departments, indicating the importance of its work to the administration.¶ The rules have been in development for nearly two years, but they were leaked to the Times at a convenient moment for the administration: The New York Times, Bloomberg L.P., the Wall Street Journal and the Washington Post all claim that their computers have been penetrated by Chinese hackers and had been targeted for years. The computer security company Mandiant also alleged that Chinese hackers had stolen contacts, information and files from more than 30 US newspaper journalists and executives, many of which had written about Chinese leaders and political and legal issues in China.¶ But the Chinese Ministry of National Defense has denied that its people had anything to do with the suspected attacks, stating that “Chinese laws prohibit any action including hacking that damages Internet security.” The ministry also expressed anger about the accusations, stating that “to accuse the Chinese military of launching cyberattacks without solid proof is unprofessional and baseless.”¶ “We have seen over the last years an increase in not only the hacking attempts on government institutions but also nongovernmental ones,” US Secretary of State Hillary Clinton told reporters on Thursday, emphasizing that the Chinese “are not the only people who are hacking us.”¶ The administration has also recently announced that an unnamed American power station was crippled for weeks by cyberattacks, without releasing details about the location of the plant. With little proof about the alleged cyberattacks and the suspected threats, the White House now reserves the right to make major cyberwarfare decisions, despite Congress’ long-standing disapproval.¶ “The [National Security Administration’s] cyber security operations have been kept very, very secret, and because of that it has been impossible for the public to react to them,” said Electronic Privacy Information Center attorney Arnie Stepanovich in November. “[That makes it] very difficult, we believe, for Congress to legislate in this area.”¶ The Obama administration has long pushed for Congress to pass the Cyber Intelligence Sharing and Protection Act, which would grant the government greater access to the Internet and cybersecurity information from the private sector. US Homeland Security Secretary Janet Napolitano, [claims](http://rt.com/usa/news/napolitano-us-cyber-attack-761/) it is necessary to prevent a “cyber 9/11” attack that would knock out water, electricity and gas, causing destruction similar to that left behind by Hurricane Sandy.¶ But privacy advocates have long expressed concern that this measure would give the government access to Americans’ personal e-mails, online chat conversations, and other personal information that only private companies and servers might have access too, prompting Congress to reject the measure.¶ Alongside privacy concerns, the Obama administration’s increasing access to cybersecurity information and cyberwarfare capabilities provides the president with an unknown amount of power to conduct anonymous attacks on foreign infrastructure.¶ While using this technology to attack military objects, such as anti-aircraft or missile defense radars in war zones, would not surprise anyone, the US now also reserves the right to attack other countries with which it has not declared war.¶ With the US ranking first in a 2012 study that drew up a “Cyber Power Index”, other nations whose conduct conflicts with US wishes could become more vulnerable than ever – especially since International Law allows countries to defend themselves against foreign threats, and these “threats” can now be concluded based on vague intelligence analysis of a 'potential' cyber attack.

#### It goes nuclear

[we don’t even have to win escalation -- command and control hacking, crisis instability, and fracturing nuclear agreements all ensure independent nuclear response- congressional restrictions are key to solve]

Austin, 8/6

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.

#### Cyber preemption escalates to a shooting war

Clarke 2009

(Richard Clarke, special adviser to the president for cybersecurity in the George W. Bush administration and chairman of Good Harbor Consulting, November/December 2009, “War from Cyberspace,” The National Interest, <http://web.clas.ufl.edu/users/zselden/coursereading2011/Clarkecyber.pdf>)

As in the 1960s, **the speed of war is rapidly accelerating.** Then, long-range ¶ ¶ missiles could launch from the prairie of ¶ ¶ Wyoming and hit Moscow in only thirtyfive minutes. Strikes in cyber war move at ¶ ¶ a rate approaching the speed of light. And ¶ ¶ **this speed favors a strategy of preemption, which means the chances that people can become trigger-happy are high.** **This**, in ¶ ¶ turn, **makes cyber war all the more likely.** ¶ ¶ If a cyber-war commander does not attack quickly, his network may be destroyed first. **If a commander does not preempt an enemy, he may find that the target nation has suddenly raised new defenses or even disconnected from the worldwide Internet.** ¶ ¶ There seems to be a premium in cyber war ¶ ¶ to making the first move.¶ ¶ And much as in the nuclear era, **there is a real risk of escalation with cyber war.** ¶ ¶ Nuclear war was generally believed to be ¶ ¶ something that might quickly grow out of ¶ ¶ conventional combat, perhaps initiated with ¶ ¶ tanks firing at each other in a divided Berlin. The speed of new technologies created ¶ ¶ enormous risks for crisis instability and miscalculation. Today, **the risks of miscalculation are even higher, enhancing the chances that what begins as a battle of computer programs ends in a shooting war.** Cyber ¶ ¶ war, with its low risks to the cyber warriors, ¶ ¶ may be seen by a decision maker as a way ¶ ¶ of sending a signal, making a point without ¶ ¶ actually shooting. An attacker would likely ¶ ¶ think of a cyber offensive that knocked out ¶ ¶ an electric-power grid and even destroyed ¶ ¶ some of the grid’s key components (keeping ¶ ¶ the system down for weeks), as a somewhat ¶ ¶ antiseptic move; a way to keep tensions ¶ ¶ as low as possible. But **for the millions of people thrown into the dark** and perhaps ¶ ¶ the cold, unable to get food, without access ¶ ¶ to cash and dealing with social disorder, ¶ ¶ **it would be in many ways the same as if bombs had been dropped on their cities. Thus, the nation attacked might well respond with “kinetic activity.”**

**That also causes miscalculation of nuclear forces**

**Clark and Andreasen 13**

(Richard A. Clarke, the chairman of Good Harbor Security Risk Management, was special adviser to the president for cybersecurity in the George W. Bush administration. Steve Andreasen, a consultant to the Nuclear Threat Initiative, was the National Security Council’s staff director for defense policy and arms control from 1993 to 2001, “Cyberwar’s threat does not justify a new policy of nuclear deterrence” June 14, 2013, <http://articles.washingtonpost.com/2013-06-14/opinions/39977598_1_nuclear-weapons-cyber-attack-cyberattacks>, KB)

President Obama is expected to unveil a new nuclear policy initiative this week in Berlin. Whether he can make good on his first-term commitments to end outdated Cold War nuclear policies may depend on a firm presidential directive to the Pentagon rejecting any new missions for nuclear weapons — in particular, their use in response to cyberattacks.¶ The Pentagon’s Defense Science Board concluded this year that **China and Russia could develop capabilities to launch an “existential cyber attack” against the United States** — that is, **an attack causing sufficient damage that our government would lose control of the country.** “**While the manifestation of a nuclear and cyber attack are** very **different**,” the board concluded, “in the end, **the existential impact to the United States is the same.”**¶ Because it will be impossible to fully defend our systems against existential cyberthreats, the board argued, the United States must be prepared to threaten the use of nuclear weapons to deter cyberattacks. In other words: I’ll see your cyberwar and raise you a nuclear response.¶ Some would argue that Obama made clear in his 2010 Nuclear Posture Reviewthat the United States has adopted the objective of making deterrence of nuclear attacks the “sole purpose” of our nuclear weapons. Well, the board effectively reviewed the fine print and concluded that the Nuclear Posture Review was “essentially silent” on the relationship between U.S. nuclear weapons and cyberthreats, so connecting the two “is not precluded in the stated policy.”¶ As the board noted, cyberattacks can occur very quickly and without warning, requiring rapid decision-making by those responsible for protecting our country. **Integrating the nuclear threat into the equation means making clear to any potential adversary that the United States is prepared to use nuc**lear weapon**s very early in response to a major cyberattack — and is maintaining nuclear forces on “prompt launch” status to do so.**¶ **Russia and China would** certainly take note — and presumably **follow suit**. Moreover, **if the United States, Russia and China adopted policies threatening an early nuclear response to cyber­attacks, more countries would surely take the same approach.**¶ It’s hard to see how this cyber-nuclear action-reaction dynamic would improve U.S. or global security. It’s more likely to lead to a new focus by Pentagon planners on generating an expanding list of cyber-related targets and the operational deployment of nuclear forces to strike those targets in minutes.¶ Against that backdrop, maintaining momentum toward reducing the role of nuclear weapons in the United States’ national security strategy (and that of other nations) — a general policy course pursued by the past five presidents — would become far more difficult. **Further reductions in nuclear forces and changes in “hair-trigger” postures, designed to lessen the risk of an accidental or unauthorized nuclear launch, would** also probably **stall**.¶ Fortunately, Obama has both the authority and the opportunity to make clear that he meant what he said when he laid out his nuclear policy in Prague in 2009. For decades, presidential decision directives have made clear the purpose of nuclear weapons in U.S. national security strategy and provided broad guidance for military planners who prepare the operations and targeting plans for our nuclear forces. An update to existing presidential guidance is one of the homework items tasked by the 2010 Nuclear Posture Review.¶ Cyberthreats are very real, and **there is** much we ne**ed to do to defend our military and critical civilian infrastructure against** what former defense secretary Leon E. Panetta referred to as **a “cyber Pearl Harbor”** — including enhancing the ability to take action, when directed by the president, against those who would attack us. We also need more diplomacy such as that practiced by Obama with his Chinese counterpart, Xi Jinping, at their recent summit. Multinational cooperation centers could ultimately lead to shared approaches to cybersecurity, including agreements related to limiting cyberwar.

**Criticizing the probability of our impacts is meaningless – all wars are low probability, what matters is that cyberwar is more likely to escalate than other conflicts, which uniquely warrants academic attention**

**Junio ‘13**

[Timothy J. Junio (Tim)is a doctoral candidate of political science at the¶ University of Pennsylvania and a predoctoral fellow at the Center for¶ International Security and Cooperation (CISAC) at Stanford University.¶ He also develops new cyber capabilities at the Defense Advanced¶ Research Projects Agency (DARPA). How Probable is Cyber War? Bringing¶ IR Theory Back In to the Cyber Conflict Debate, Journal of Strategic Studies, 36:1,¶ 125-133. ETB]

Two recent articles in the pages of this journal contribute to an¶ important debate about how information technology (IT) inﬂuences¶ international politics.1¶ Thomas **Rid and** Adam **Liff argue that** **cyber**¶ **‘war’** has never happened and probably **will not happen. A fundamental**¶ **problem** with these articles **is that Rid and Liff do not commit to a**¶ **theoretical framework regarding the causes of war.** **Doing so yields an**¶ **opposite conclusion:** i**nternational** r**elations theory identiﬁes many**¶ **mechanisms that may cause violent escalation with cyber weapons**.¶ This brief response article explains why **cyber war is sufﬁciently**¶ **probable to merit serious attention from scholars and practitioners**,¶ and proposes a theoretical research agenda. **First, domestic political**¶ **factors** – such as states’ command and control over cyber operations –¶ **must be problematized**. **The principal-agent approach demonstrates**¶ **how variation in incentives and preferences may make militaries more**¶ **likely to favor cyber attack than other kinds of bureaucracies.** This¶ matters in societies with poor civilian control over the military. Second,¶ **the unique material qualities of IT must be evaluated alongside**¶ **traditional mechanisms that cause war**. For instance, **the attribution**¶ **problem and computational complexity in modeling cyber operations**¶ **may increase the odds of inadvertent cyber war by causing states to**¶ **retaliate against the wrong targets or miscalculate the potential costs**¶ **and gains of attacking.**¶What is Cyber War? (Again. . .)¶ Rid and Liff do not deﬁne cyber war the same way, and there is no¶ disciplinary consensus. Rid, Liff, and this author at least agree on the¶ following: **cyber war is a coercive act involving computer network**¶ **attack. Network attack means information is disrupted, degraded, or**¶ **destroyed**. **‘Coercive’ means using force to change or preserve a political**¶ **status quo**. A point of contention is lethality, which Rid believes is¶ necessary for cyber ‘war’.2¶ This is an extreme and undesirable¶ requirement, particularly because (as Rid himself points out) non-lethal¶ cyber attacks may be more costly than conventional warfare.3¶ It is¶ important to note that Rid focuses on network attack, whereas Liff¶ considers a broader conﬂict process. This response addresses both.¶ The central point of Rid’s article is that it is difﬁcult to cause lethal¶ effects with cyber weapons, and that politically motivated, instrumental cyber attack has never killed anyone.4¶ While the empirics of his¶ article are sound – he describes recent cyber attacks accurately – **Rid**¶ **never explains what causes war or makes war more or less likely. The**¶ **arguments in his article are exclusively deﬁnitional, and do not directly**¶ **support his title’s assertion that ‘Cyber War Will Not Take Place**.’¶ Liff does better from a theoretical point of view; he links his article to¶ the bargaining approach to war.5¶ He does an excellent job of offering¶ counterpoints to four arguments about why cyber attack may increase¶ the probability of war. However, **Liff** never establishes why his¶ reasonable views are more plausible than their alternatives. This is¶ because he **is not explicit about assumptions that are necessary for his**¶ **arguments to hold, nor about the circumstances under which those**¶ **assumptions break down**. For example, Liff argues that private¶ information may make war less likely because states poorly estimate he gains from cyber attack.6¶ Although Liff is right to point out that¶ ambiguity in cyber operations is important, he is wrong to assume the¶ causal arrow points in one direction. Ambiguity can make war more or¶ less likely, because it may lead states to overestimate their potential¶ gains, overestimate their stealth, and/or underestimate their adversary’s¶ skill.¶ Finally, **it must be recognized that any future war is a low probability event. Crafting claims that particular conﬂict scenarios are improbable** is rather unimpressive**; what is important to understand is the potential cost and probability of cyber war relative to other kinds of conﬂict.**¶Causes of Cyber War¶ **The noted problems in the Rid and Liff articles could have been**¶ **avoided by drawing on structured theoretical approaches that are**¶ **common to the study of the causes of all kinds of warfare**. What would¶ such an approach look like? This response lacks the space to fully¶ develop one, but recommends a way forward. Literally **dozens of**¶ **arguments have been advanced in the political science discipline**¶ **regarding the causes of war, and very many of these offer reasons to**¶ **believe cyber war is** plausible or even **probable**.7¶ An approach,¶ advanced in James Fearon’s modern classic ‘Rationalist Explanations¶ for War,’ is to list assumptions that create an ideal condition in which¶ war should never happen.8¶ One way to structure scientiﬁc inquiry¶ regarding the probability of cyber war is to examine how **the unique**¶ **material qualities of IT affect each of the assumptions**. Table 1 offers a¶ cursory version of such an analysis to identify priority areas for further¶ study. Among a large number of revealed paths to cyber war, one –¶ principal-agent problems involving the bureaucracies that conduct¶ cyber operations – is detailed here to demonstrate the plausibility of¶ speciﬁc mechanisms and what follow-on empirical work should look¶ like.¶ Principal-Agent Problems¶ Rid and Liff appear to assume that states are unitary rational actors¶ (URAs), and do not explain the domestic political processes whereby¶ states make foreign policy choices. **Empirically and theoretically, it is important to relax the URA assumption and problematize who has**¶ **formal and actual release authority over cyber weapons.** **The principal agent approach**, for instance, **works from the premise that** individuals and **organizations often vary in their incentives and preferences, which could make war beneﬁcial for some at the cost of others**.9¶ **This** and¶ related **thinking inform how scholars study other military technologies,**¶ **such as nuclear weapons**. Scott Sagan points out **that although unauthorized nuclear war is improbable, it is sufﬁciently probable that people should worry a great deal about command and control (C2)** **issues**.10 Many anecdotes echo Sagan’s work. For example, a Russian¶ general was asked during the Cold War about his backup plan in the¶ event he could not open the safe containing his nuclear launch codes.¶ His answer was that he would bash the safe open with a sledgehammer¶ he kept nearby!11¶ Consideration of how bureaucracies do what they do – like keeping¶ emergency nuclear war sledgehammers – is of critical importance to the¶ cyber C2 question. Although controlling large organizations is a core¶ function of militaries, **the conduct of cyber operations is different from**¶ **other kinds of activity in a way that greatly magniﬁes the ‘strategic corporal’ problem. This is because constant cyber operations** other than¶ war **decrease the bureaucratic friction that normally alerts superiors to**¶ **aberrant behavior.** In the case of nuclear weapons, a long chain of¶ events is required before unauthorized activities occur. Someone¶ probably would notice a crazed general using his sledgehammer on¶ the launch codes safe, turning keys, fueling missiles, and so on. In¶ contrast, **it is a core function of cyber bureaucrats to access adversary**¶ **networks constantly, and to develop push-button solutions to minimize**¶ **lags during war**. Furthermore**, if the perception that cyber weapons are**¶ **non-lethal comes to be widely perceived** (as Rid would prefer), **it is**¶ **reasonable to conclude that** the threshold for their use will be lower¶ **than other kinds of weapons – even if the cost of cyber attacks is**¶ **greater.**¶While weak C2 is a necessary condition for a war caused by¶ principal-agent problems, it is not sufﬁcient, because bureaucracies¶ (agents) must also have different incentives or preferences from their¶ populations or leaders (the ‘principals’). A deep political science literature argues that militaries are more prone to favor offensive operations than other kinds of bureaucracies.12 Early evidence suggests that¶ **this ‘cult of the offensive’ operates regarding cyber warfare**. James¶ **Cartwright**, the former Vice Chairman of the US Joint Chiefs of Staff,¶ **calls for the United States to engage in more offensive cyber operations,**¶ **and reportedly created a bureaucracy to that end.**13 **This perspective exists in other countries; ofﬁcials with** South Korea’s Cyber Command¶ believe that ‘the best defense is a good offense’**, and that they should**¶ **preemptively disable menacing foreign servers.14** Chinese military¶ textbooks recommend ‘information offensive through computer network attack’in advance of conventional warfare.15 In contrast, nearly¶ all other bureaucracies – such as those responsible for diplomacy, law¶ enforcement, and homeland security – appear oriented toward cyber¶ defense.¶ **If this offensive mindset is observed in countries where civilians have**¶ **ﬁrm control over military organizations, then what is the risk from**¶ **countries with different civil-military relations?16 The thought of weak**¶ **or military-dominated states possessing advanced cyber capabilities is**¶ **troubling,** to say the least, **and offers highly plausible paths to cyber**¶ **wa**r. An example, **North Korea, already has demonstrated offensive**¶ **tendencies, as that government appears to have conducted disruptive**¶ **and destructive cyber attacks**.17¶ **Many potential paths to war result from a combination of ‘cult of the**¶ **offensive’ reasoning and weak C2. One is for militaries to justify cyber**¶ **attack as acts of self-defense or preemption. Another is for militaries to**¶ **conduct offensive cyber operations without informing their superiors.**¶ **Yet another is the potential for offensive biases to make them more**¶ **easily fall bait to ‘false ﬂag’ operations**. These are merely derivatives of¶ principal-agent problems that arise among politically motivated actors;¶ the outlook worsens when considering other incentives, such as proﬁt,¶ that may lead corrupt bureaucrats to sell lethal skills or software to the¶ highest bidder.¶ **So, how much should scholars and practitioners care about cyber wa**r?¶ A belief that cyber war is hyped appears to have motivated Rid and Liff¶ to pen their pieces. **A satisfying answer must explain at least two things:**¶ **the destructive potential of cyber war, and the probability that it will**¶ **happen. It appears uncontroversial that,** if **cyber war** happens, it **will be** ¶ **highly costly** even if not lethal. Few contest the idea that a successful¶ and sustained degradation of military capabilities, deprivation of¶ civilian services, destruction of ﬁnancial records, or other such ‘digital¶ Pearl Harbor’ scenarios, would be pretty bad.¶ On the other hand, there is little agreement in academic or policy¶ circles regarding whether or not cyber war will happen. **This response**¶ **offers an important corrective to narratives that cyber war is**¶ **improbable. A small number of premises lead to a conclusion that**¶cyber war is, at a minimum, plausible enough to merit serious¶ attention. Further research would do well to commit to theoretical¶ paradigms, such as the approach recommended in Table 1. This kind of¶ rigorous scholarship is a prerequisite to reducing the incidence of cyber¶ conﬂict and avoiding cyber war.

**Understanding the risks of current US posture reduces the chances of cyber war escalation- worst case assessments are the best preparation**

**Clarke and Knake ‘10**

[Richard Alan Clarke is the former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States. Robert K. Knake, Former international affairs fellow in residence @ CFR. Cyber War. ETB]

In the seminal 1983 movie about computers and war, War Games, ¶ starring a young Matthew Broderick, the tinny computer voice ¶ asked haltingly, “Do you want to play a game of thermonuclear war?” ¶ Why don’t we play a game of cyber war in order to elucidate some of ¶ the policy choices that shape a strategy. DoD runs such exercises, ¶ called Cyber Storm, annually. The CIA’s annual cyber war exercise, ¶ Silent Horizon, has been happening since 2007. For the purposes of ¶ this analysis, I’ll make the same request of you that I made of students ¶ at Harvard’s Kennedy School and national security bureaucrats sitting ¶ around the White House Situation Room conference table: “Don’t ¶ fight the scenario.” By that I mean, do not spend a lot of timerejecting ¶ thepremise that circumstances couldhappen someday that would ¶result inthe U.S. being on the edgeofconflict with Russia or China**. When U.S. cyber warriors talk about the “big one,” they usually** ¶ **have in mind a conflict in cyberspace with Russia or China**, the two ¶ nations with the most sophisticated offensive capability other than ¶ the U.S. **No one wants hostilities with those countries to happen.** ¶ **Thinking about it, for the purposes of understanding what cyber** ¶ **war would look like, does not make it more likely**. In fact, by understanding the risks of our current cyber war posture, we might reduce ¶ the chances of a real cyber war**.** **And if, despite our intentions, a** ¶ **cyber war does happen, it would be best to have thought in advance** ¶ **about how it could unravel.**¶ **Certainly, I did not want to see the attack of 9/11 happen, but I** ¶ **had chaired countless** “tabletop exercises,” or **war game scenarios,** **to** ¶ **get myself and the bureaucracy ready in case something like it did** ¶ **happen**. **When it came, we had already thought through how to re­**¶ **spond on the day of an attack and the few days thereafter**. We spent ¶ enormous effort to try to prevent attacks, but we also devoted some ¶ time to thinking about what we would do if one succeeded. **Had we** ¶ **not done so, that awful day would have been even worse**. **So**, **in that** ¶ **spirit of learning by visualizing, let’s think about a period of rising** ¶ **tensions** between the U.S. and China.

**Arguing against the practices of the USFG in the context of war powers allows for an engaged public that can expose the hypocrisy of the federal government – only focus on specific policy questions can actualize change by making it relevant to policy-makers –**

**Mellor 13**

The Australian National University, ANU College of Asia and the Pacific, Department Of International Relations,
“Why policy relevance is a moral necessity: Just war theory, impact, and UAVs,” European University Institute, Paper Prepared for BISA Conference 2013, DOA: 8-14-13

**This** section of the paper **considers** more generally **the need for** just war **theorists to engage with policy debate** **about the use of force**, **as** **well as to engage with the** more **fundamental moral and philosophical principles** of the just war tradition. **It draws on** John **Kelsay’s** **conception of just war thinking as being a social practice**,35 **as well as on** Michael **Walzer’s understanding of the role of the social critic in society**.36 It argues that the just war tradition is a form of “practical discourse” which is concerned with questions of “how we should act.”37 Kelsay argues that: **[T]he criteria of jus ad bellum and jus in bello provide a framework for structured participation in a public conversation about the use of military force** . . . **citizens who choose to speak in just war terms express commitments** . . . [i**]n the process of giving and asking for** **reasons for going to war**, **those who argue** in just war terms **seek to influence policy** **by persuading others that their analysis provides a way to express and fulfil the desire that military actions be** both **wise and just.38** He also argues that “**good just war thinking involves continuous and complete deliberation**, in the sense that one attends to all the standard criteria at war’s inception, at its end, and **throughout the course of the conflict**.”39 **This** is important as it **highlights the need for** just war **scholars to engage** **with the ongoing operations in war and the specific policies that are involved**. **The question of** **whether a particular** war is just or unjust, and the question of whether a particular **weapon (like drones**) **can be used in accordance with the jus in bello criteria**, only **cover a part of the overall justice of the war**. **Without an engagement with the reality of war**, **in** **terms of the policies used** in waging it, **it is impossible to engage with the “moral reality of war,”40 in terms of being able to discuss it and judge it in moral terms** Kelsay’s description of just war thinking as a social practice is similar to Walzer’s more general description of social criticism. The just war theorist, **as a social critic, must be involved with his or her own society and its practices**. In the same way that the social critic’s distance from his or her society is measured in inches and not miles,41 the just war **theorist must be close to and must understand the language through which war is constituted, interpreted and reinterpreted**.**42 It is only by understanding the values and language that their own society purports to live by that the social critic can hold up a mirror to that society to** **demonstrate** its **hypocrisy** **and to show the gap that exists** between its practice and its values.43 **The tradition** itself **provides a set of** **values and principles and**, as argued by Cian O’Driscoll, **constitutes a “language of engagement**” **to spur participation in public and political debate**.44 This language is part of “our common heritage, the product of many centuries of arguing about war.”45 **These principles and this language provide the terms through which people understand and come to interpret war, not in a deterministic way but by providing the categories necessary for moral understanding and moral argument about the legitimate and illegitimate uses of force**.46 **By spurring and providing the basis for political engagement the just war tradition ensures that the acts that occur within war are considered according to just war criteria and allows policy-makers to be held to account on this basis. Engaging with the reality of war requires** recognising that war is, as Clausewitz stated, **a continuation of policy**. **War**, according to Clausewitz, **is subordinate to politics and to political choices and these political choices can, and must, be judged and critiqued**.47 **Engagement and political debate are morally necessary** **as the alternative is disengagement and moral quietude**, **which is a sacrifice of the obligations of citizenship**.48 **This engagement must bring** just war **theorists into contact with the policy makers** **and** **will require work that is** accessible and **relevant to policy makers**, **however this does not mean a sacrifice of critical distance or an abdication of truth in the face of power.** **By engaging in detail** **with the policies being pursued** and their concordance or otherwise with **the principles of the just war tradition the policy-makers will be forced to account for their decisions and justify them in just war language.** **In contrast to the view**, **suggested** by Kenneth **Anderson, that “the public cannot be made part of the debate**” **and that “[w]e are** necessarily **committed into the hands of our political leadership**”,49 it is incumbent upon just war theorists to ensure that the public are informed and are capable of holding their political leaders to account. **To accept the idea that the political leadership are stewards and that accountability will not benefit the public, on whose behalf action is undertaken, but will only benefit al Qaeda,50 is a grotesque act of intellectual irresponsibility**. As Walzer has argued, it is precisely because it is “our country” that we are “especially obligated to criticise its policies.”51 This paper has discussed the empirics of the policies of drone strikes in the ongoing conflict with those associate with al Qaeda. It has demonstrated that there are significant moral questions raised by the just war tradition regarding some aspects of these policies and it has argued that, thus far, just **war scholars have not paid sufficient attention or engaged in sufficient detail with the policy implications of drone use.** **As such it has been argued that it is necessary for just war theorists to engage more directly with these issues and to ensure that their work is policy relevant**, **not in a utilitarian sense of abdicating from speaking the truth in the face of power**, **but by forcing policy makers to justify** their **actions according to the principles of the just war tradition, principles which they invoke themselves in formulating policy.** **By highlighting hypocrisy and providing the tools and language** **for the interpretation of action**, **the just war tradition provides the basis for the public engagement and political activism that are necessary for democratic politics.52**

**Debate about the repercussions of cyber preemption is good- it generates a broader literature base that encourages restraint**

**Magnuson ‘9**

[Stew, National Defense Magazine. <http://www.nationaldefensemagazine.org/archive/2009/June/Pages/USPlanstoDestroyEnemyComputerNetworksQuestioned.aspx> ETB]

¶ Retired Adm. William **Owen**, **former vice chairman of the Joint Chiefs of Staff,** said he **sees little evidence that there is a government-wide understanding of the repercussions of launching an attack on enemy computers. And that goes for the military as well.**¶¶ “My guess is that most of **the generals and admirals don’t really understand** **what** the hell **we’re** **playing with here** and we need to find a way to get some focused attention” on this topic, he told National Defense.¶ ¶ Owen is the co-author of a National Research Council report, “Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber-Attack Capabilities.”¶ ¶ The study — two-and-a-half years in the making — concludes that **policies and regulations for carrying out computer attacks are “ill-formed, undeveloped and highly uncertain,”** said Kenneth Dam, a former deputy secretary of state who also contributed to the report.¶ ¶ The authors could not identify any single authority in the government responsible for coordinating cyber-attacks or promulgating policy — if there is any policy at all. Further, there are no congressional committees designated to oversee the government’s efforts. ¶ ¶ In short, if the United States government goes on the offense in cyberspace, there may be a lack of accountability, the report concluded.¶ ¶ Secrecy has impeded widespread debate about the nature and implications of cyber-attack, the authors asserted. Much of the defense community’s efforts in this realm are top secret.¶ ¶ “It’s not so much secrecy, it’s actual silence. It just isn’t discussed,” Dam said at a press briefing. **There needs to be a public debate about the repercussions of launching cyber-attacks**, the report said. **In the early days of nuclear weapons, there was a great deal of literature coming out of think tanks, universities and other institutions about when and how to use atomic bombs. That just isn’t happening in this new kind of warfare**, Dam added.

#### War fuels structural violence

Goldstein 2001

IR professor at American University (Joshua, War and Gender, p. 412, Google Books)

First, peace activists face a dilemma in thinking about causes of war and working for peace. **Many peace scholars and activists support the approach, “if you want peace, work for justice.”** Then, if one believes that sexism contributes to war, one can work for gender justice specifically (perhaps. among others) in order to pursue peace. This approach brings strategic allies to the peace movement (women, labor, minorities), but rests on the assumption that injustices cause war. The evidence in this book suggests that **causality runs at least as strongly the other way. War is not a product of capitalism, imperialism, gender, innate aggression,** or any other single cause, **although all of these influence wars’ outbreaks and outcomes. Rather, war has in part** fueled and sustained **these and other injustices**.9 So, “if you want peace, work for peace.” Indeed, if you want justice (gender and others), work for peace. **Causality does not run just upward through the levels of analysis, from types of individuals, societies, and governments up to war. It runs downward too**. Enloe suggests that changes in attitudes towards war and the military may be the most important way to “reverse women’s oppression.” The dilemma is that peace work focused on justice brings to the peace movement energy, allies, and moral grounding, yet, in light of this book’s evidence, **the emphasis on injustice as the main cause of war seems to be** empirically inadequate.

**Squo makes Obama judge, jury, and executioner when it comes to cyberwarfare**

**Gosztola ‘13**

[Kevin Gosztola is a trusted author who publishes his writing regularly to OpEdNews and Open Salon and he is a 2009 Young People For Fellow. <http://dissenter.firedoglake.com/2013/02/04/legal-review-of-presidential-power-to-engage-in-preemptive-cyber-strikes-to-remain-secret/> ETB]

Finally, like with the drone program, President Barack **Obama is presiding over the creation and development of a power that previous presidents never imagined having.** **The** national security **state is effectively appointing him and all future presidents the** proverbial **judge, jury and executioner when it comes to cyber warfare.**¶ There is no indication that any group of members in Congress or judicial body will have to approve of a preemptive strike before it is carried out. As has become typical, the president wants to be able to conduct war without needing authorization.¶ **The policy will expand the imperial presidency and the public and civil society organizations, which** have a distinct interest in knowing what the government is doing, **will be kept in the dark on what is legal and illegal in cyber operations. The Congress will barely make any effort to defend its right to provide oversight of this new power.** And any future details on this power will mostly come from selective leaks provided by officials, who do not think they will face repercussions for talking to the press. **The policy itself, the rules for cyber war, will remain concealed.**

#### Our discussion raises awareness of cyber militarism and spills over to policy

**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.**

#### War facilitates lashout against the other

Rangelov and Kaldor 12

Iavor Rangelov and Mary Kaldor. 2012. Global Security Research Fellow at the Civil Society and Huamn Security Research Unit, Dept of Int’l Development at the Loncon School of Economics and Political Science; Professor of Global Governance and Director of the Civil Society and Human Security Research Unit. Persistent Conflict. Conflict, Security & Development 12:3.

One problem with the literature is the preoccupation with the term ‘conﬂict’. The Uppsala Conﬂict Data Program, which is the source of most statistics on conﬂict including the World Development Report, the Human Security Report and the SIPRI Yearbook on Armaments, Disarmament and International Security, deﬁnes conﬂict as a ‘contested incompatibility’. 7 The implicit assumption is that two or more sides have (legitimate) grievances that can be resolved either through violence or negotiation. Yet as Michel Wieviorka points out, violence may be the opposite of conﬂict; it may close down conﬂict. 8 Conﬂict is the normal human condition and is indeed a source of creativity in society. Democracy can be understood as a peaceful mechanism for managing conﬂict. In conditions of violence, people live in fear and dare not express their grievances. They may and probably do, of course, hate those who kill them or their neighbours and family and they may kill in revenge, but this does not mean they also have some underlying grievance that can be resolved. Their conﬂict is the consequence of violence rather than the other way round. Fine grained analyses of places where violence occurs, such as the ones included in this special issue, suggest that a range of motivations are relevant in explaining violence. For many, though not of course all, it is violence rather than the resolution of conﬂict that is the main goal. Firstly, violence constructs a context in which it is possible to mobilise around extremist ideologies. Xenophobic, fundamentalist, racist or ethnicist political philosophies tend to be marginal in peacetime. In violent situations, people learn to hate ‘the other’ and to seek the ‘protection’ of those who defend them against ‘the other’. Amartya Sen describes the Hindu–Muslim riots in 1947, and how people were ‘trapped into that vicious mode of thinking, and the more savage among them [. . .] were induced to kill “the enemies who kill us” (as they were respectively deﬁned)’. 9 Secondly, of course, violence creates a context for criminal gain—loot, pillage, hostage-taking, various kinds of smuggling. And ﬁnally, all kinds of personal motives, such as land disputes, family feuds, honour killings, excitement, adventure and perversion, are given free rein in violent contexts

#### The state must be engaged---action can be reoriented away from past abuses

Williams and Krause 97

Michael, assistant professor of political science at the University of Southern Maine and Keith, professor of political science at the Graduate Institute of International Studies, associate professor of political science at York University, Critical Security Studies: Concepts and Cases, edited by Krause and Williams, p. xvi

Many of the chapters in this volume thus retain a concern with the centrality of the state as a locus not only of obligation but of effective political action. In the realm of organized violence, states also remain the preeminent actors. The task of a critical approach is not to deny the centrality of the state in this realm but, rather, to understand more fully its structures, dynamics, and possibilities for reorientation. From a critical perspective, state action is flexible and capable of reorientation, and analyzing state policy need not therefore be tantamount to embracing the statist assumptions of orthodox conceptions. To exclude a focus on state action from a critical perspective on the grounds that it plays inevitably within the rules of existing conceptions simply reverses the error of essentializing the state. Moreover, it loses the possibility of influencing what remains the most structurally capable actor in contemporary world politics.

#### Simulated national security law debates preserve agency and enhance decision-making---avoids cooption

Donohue 13

Laura K. Donohue 13, Associate Professor of Law, Georgetown Law, 4/11, “National Security Law Pedagogy and the Role of Simulations”, <http://jnslp.com/wp-content/uploads/2013/04/National-Security-Law-Pedagogy-and-the-Role-of-Simulations.pdf>

The concept of simulations as an aspect of higher education, or in the law school environment, is not new.164 Moot court, after all, is a form of simulation and one of the oldest teaching devices in the law. What is new, however, is the idea of designing a civilian national security course that takes advantage of the doctrinal and experiential components of law school education and integrates the experience through a multi-day simulation. In 2009, I taught the first module based on this design at Stanford Law, which I developed the following year into a full course at Georgetown Law. It has since gone through multiple iterations. The initial concept followed on the federal full-scale Top Official (“TopOff”) exercises, used to train government officials to respond to domestic crises.165 It adapted a Tabletop Exercise, designed with the help of exercise officials at DHS and FEMA, to the law school environment. The Tabletop used one storyline to push on specific legal questions, as students, assigned roles in the discussion, sat around a table and for six hours engaged with the material. The problem with the Tabletop Exercise was that it was too static, and the rigidity of the format left little room, or time, for student agency. Unlike the government’s TopOff exercises, which gave officials the opportunity to fully engage with the many different concerns that arise in the course of a national security crisis as well as the chance to deal with externalities, the Tabletop focused on specific legal issues, even as it controlled for external chaos. The opportunity to provide a more full experience for the students came with the creation of first a one-day, and then a multi-day simulation. The course design and simulation continues to evolve. It offers a model for achieving the pedagogical goals outlined above, in the process developing a rigorous training ground for the next generation of national security lawyers.166 A. Course Design The central idea in structuring the NSL Sim 2.0 course was to bridge the gap between theory and practice by conveying doctrinal material and creating an alternative reality in which students would be forced to act upon legal concerns.167 The exercise itself is a form of problem-based learning, wherein students are given both agency and responsibility for the results. Towards this end, the structure must be at once bounded (directed and focused on certain areas of the law and legal education) and flexible (responsive to student input and decisionmaking). Perhaps the most significant weakness in the use of any constructed universe is the problem of authenticity. Efforts to replicate reality will inevitably fall short. There is simply too much uncertainty, randomness, and complexity in the real world. One way to address this shortcoming, however, is through design and agency. The scenarios with which students grapple and the structural design of the simulation must reflect the national security realm, even as students themselves must make choices that carry consequences. Indeed, to some extent, student decisions themselves must drive the evolution of events within the simulation.168 Additionally, while authenticity matters, it is worth noting that at some level the fact that the incident does not take place in a real-world setting can be a great advantage. That is, the simulation creates an environment where students can make mistakes and learn from these mistakes – without what might otherwise be devastating consequences. It also allows instructors to develop multiple points of feedback to enrich student learning in a way that would be much more difficult to do in a regular practice setting. NSL Sim 2.0 takes as its starting point the national security pedagogical goals discussed above. It works backwards to then engineer a classroom, cyber, and physical/simulation experience to delve into each of these areas. As a substantive matter, the course focuses on the constitutional, statutory, and regulatory authorities in national security law, placing particular focus on the interstices between black letter law and areas where the field is either unsettled or in flux. A key aspect of the course design is that it retains both the doctrinal and experiential components of legal education. Divorcing simulations from the doctrinal environment risks falling short on the first and third national security pedagogical goals: (1) analytical skills and substantive knowledge, and (3) critical thought. A certain amount of both can be learned in the course of a simulation; however, the national security crisis environment is not well-suited to the more thoughtful and careful analytical discussion. What I am thus proposing is a course design in which doctrine is paired with the type of experiential learning more common in a clinical realm. The former precedes the latter, giving students the opportunity to develop depth and breadth prior to the exercise. In order to capture problems related to adaptation and evolution, addressing goal [1(d)], the simulation itself takes place over a multi-day period. Because of the intensity involved in national security matters (and conflicting demands on student time), the model makes use of a multi-user virtual environment. The use of such technology is critical to creating more powerful, immersive simulations.169 It also allows for continual interaction between the players. Multi-user virtual environments have the further advantage of helping to transform the traditional teaching culture, predominantly concerned with manipulating textual and symbolic knowledge, into a culture where students learn and can then be assessed on the basis of their participation in changing practices.170 I thus worked with the Information Technology group at Georgetown Law to build the cyber portal used for NSL Sim 2.0. The twin goals of adaptation and evolution require that students be given a significant amount of agency and responsibility for decisions taken in the course of the simulation. To further this aim, I constituted a Control Team, with six professors, four attorneys from practice, a media expert, six to eight former simulation students, and a number of technology experts. Four of the professors specialize in different areas of national security law and assume roles in the course of the exercise, with the aim of pushing students towards a deeper doctrinal understanding of shifting national security law authorities. One professor plays the role of President of the United States. The sixth professor focuses on questions of professional responsibility. The attorneys from practice help to build the simulation and then, along with all the professors, assume active roles during the simulation itself. Returning students assist in the execution of the play, further developing their understanding of national security law. Throughout the simulation, the Control Team is constantly reacting to student choices. When unexpected decisions are made, professors may choose to pursue the evolution of the story to accomplish the pedagogical aims, or they may choose to cut off play in that area (there are various devices for doing so, such as denying requests, sending materials to labs to be analyzed, drawing the players back into the main storylines, and leaking information to the media). A total immersion simulation involves a number of scenarios, as well as systemic noise, to give students experience in dealing with the second pedagogical goal: factual chaos and information overload. The driving aim here is to teach students how to manage information more effectively. Five to six storylines are thus developed, each with its own arc and evolution. To this are added multiple alterations of the situation, relating to background noise. Thus, unlike hypotheticals, doctrinal problems, single-experience exercises, or even Tabletop exercises, the goal is not to eliminate external conditions, but to embrace them as part of the challenge facing national security lawyers. The simulation itself is problem-based, giving players agency in driving the evolution of the experience – thus addressing goal [2(c)]. This requires a realtime response from the professor(s) overseeing the simulation, pairing bounded storylines with flexibility to emphasize different areas of the law and the students’ practical skills. Indeed, each storyline is based on a problem facing the government, to which players must then respond, generating in turn a set of new issues that must be addressed. The written and oral components of the simulation conform to the fourth pedagogical goal – the types of situations in which national security lawyers will find themselves. Particular emphasis is placed on nontraditional modes of communication, such as legal documents in advance of the crisis itself, meetings in the midst of breaking national security concerns, multiple informal interactions, media exchanges, telephone calls, Congressional testimony, and formal briefings to senior level officials in the course of the simulation as well as during the last class session. These oral components are paired with the preparation of formal legal instruments, such as applications to the Foreign Intelligence Surveillance Court, legal memos, applications for search warrants under Title III, and administrative subpoenas for NSLs. In addition, students are required to prepare a paper outlining their legal authorities prior to the simulation – and to deliver a 90 second oral briefing after the session. To replicate the high-stakes political environment at issue in goals (1) and (5), students are divided into political and legal roles and assigned to different (and competing) institutions: the White House, DoD, DHS, HHS, DOJ, DOS, Congress, state offices, nongovernmental organizations, and the media. This requires students to acknowledge and work within the broader Washington context, even as they are cognizant of the policy implications of their decisions. They must get used to working with policymakers and to representing one of many different considerations that decisionmakers take into account in the national security domain. Scenarios are selected with high consequence events in mind, to ensure that students recognize both the domestic and international dimensions of national security law. Further alterations to the simulation provide for the broader political context – for instance, whether it is an election year, which parties control different branches, and state and local issues in related but distinct areas. The media is given a particularly prominent role. One member of the Control Team runs an AP wire service, while two student players represent print and broadcast media, respectively. The Virtual News Network (“VNN”), which performs in the second capacity, runs continuously during the exercise, in the course of which players may at times be required to appear before the camera. This media component helps to emphasize the broader political context within which national security law is practiced. Both anticipated and unanticipated decisions give rise to ethical questions and matters related to the fifth goal: professional responsibility. The way in which such issues arise stems from simulation design as well as spontaneous interjections from both the Control Team and the participants in the simulation itself. As aforementioned, professors on the Control Team, and practicing attorneys who have previously gone through a simulation, focus on raising decision points that encourage students to consider ethical and professional considerations. Throughout the simulation good judgment and leadership play a key role, determining the players’ effectiveness, with the exercise itself hitting the aim of the integration of the various pedagogical goals. Finally, there are multiple layers of feedback that players receive prior to, during, and following the simulation to help them to gauge their effectiveness. The Socratic method in the course of doctrinal studies provides immediate assessment of the students’ grasp of the law. Written assignments focused on the contours of individual players’ authorities give professors an opportunity to assess students’ level of understanding prior to the simulation. And the simulation itself provides real-time feedback from both peers and professors. The Control Team provides data points for player reflection – for instance, the Control Team member playing President may make decisions based on player input, giving students an immediate impression of their level of persuasiveness, while another Control Team member may reject a FISC application as insufficient. The simulation goes beyond this, however, focusing on teaching students how to develop (6) opportunities for learning in the future. Student meetings with mentors in the field, which take place before the simulation, allow students to work out the institutional and political relationships and the manner in which law operates in practice, even as they learn how to develop mentoring relationships. (Prior to these meetings we have a class discussion about mentoring, professionalism, and feedback). Students, assigned to simulation teams about one quarter of the way through the course, receive peer feedback in the lead-up to the simulation and during the exercise itself. Following the simulation the Control Team and observers provide comments. Judges, who are senior members of the bar in the field of national security law, observe player interactions and provide additional debriefing. The simulation, moreover, is recorded through both the cyber portal and through VNN, allowing students to go back to assess their performance. Individual meetings with the professors teaching the course similarly follow the event. Finally, students end the course with a paper reflecting on their performance and the issues that arose in the course of the simulation, develop frameworks for analyzing uncertainty, tension with colleagues, mistakes, and successes in the future. B. Substantive Areas: Interstices and Threats As a substantive matter, NSL Sim 2.0 is designed to take account of areas of the law central to national security. It focuses on specific authorities that may be brought to bear in the course of a crisis. The decision of which areas to explore is made well in advance of the course. It is particularly helpful here to think about national security authorities on a continuum, as a way to impress upon students that there are shifting standards depending upon the type of threat faced. One course, for instance, might center on the interstices between crime, drugs, terrorism and war. Another might address the intersection of pandemic disease and biological weapons. A third could examine cybercrime and cyberterrorism. This is the most important determination, because the substance of the doctrinal portion of the course and the simulation follows from this decision. For a course focused on the interstices between pandemic disease and biological weapons, for instance, preliminary inquiry would lay out which authorities apply, where the courts have weighed in on the question, and what matters are unsettled. Relevant areas might include public health law, biological weapons provisions, federal quarantine and isolation authorities, habeas corpus and due process, military enforcement and posse comitatus, eminent domain and appropriation of land/property, takings, contact tracing, thermal imaging and surveillance, electronic tagging, vaccination, and intelligence-gathering. The critical areas can then be divided according to the dominant constitutional authority, statutory authorities, regulations, key cases, general rules, and constitutional questions. This, then, becomes a guide for the doctrinal part of the course, as well as the grounds on which the specific scenarios developed for the simulation are based. The authorities, simultaneously, are included in an electronic resource library and embedded in the cyber portal (the Digital Archives) to act as a closed universe of the legal authorities needed by the students in the course of the simulation. Professional responsibility in the national security realm and the institutional relationships of those tasked with responding to biological weapons and pandemic disease also come within the doctrinal part of the course. The simulation itself is based on five to six storylines reflecting the interstices between different areas of the law. The storylines are used to present a coherent, non-linear scenario that can adapt to student responses. Each scenario is mapped out in a three to seven page document, which is then checked with scientists, government officials, and area experts for consistency with how the scenario would likely unfold in real life. For the biological weapons and pandemic disease emphasis, for example, one narrative might relate to the presentation of a patient suspected of carrying yersinia pestis at a hospital in the United States. The document would map out a daily progression of the disease consistent with epidemiological patterns and the central actors in the story: perhaps a U.S. citizen, potential connections to an international terrorist organization, intelligence on the individual’s actions overseas, etc. The scenario would be designed specifically to stress the intersection of public health and counterterrorism/biological weapons threats, and the associated (shifting) authorities, thus requiring the disease initially to look like an innocent presentation (for example, by someone who has traveled from overseas), but then for the storyline to move into the second realm (awareness that this was in fact a concerted attack). A second storyline might relate to a different disease outbreak in another part of the country, with the aim of introducing the Stafford Act/Insurrection Act line and raising federalism concerns. The role of the military here and Title 10/Title 32 questions would similarly arise – with the storyline designed to raise these questions. A third storyline might simply be well developed noise in the system: reports of suspicious activity potentially linked to radioactive material, with the actors linked to nuclear material. A fourth storyline would focus perhaps on container security concerns overseas, progressing through newspaper reports, about containers showing up in local police precincts. State politics would constitute the fifth storyline, raising question of the political pressures on the state officials in the exercise. Here, ethnic concerns, student issues, economic conditions, and community policing concerns might become the focus. The sixth storyline could be further noise in the system – loosely based on current events at the time. In addition to the storylines, a certain amount of noise is injected into the system through press releases, weather updates, private communications, and the like. The five to six storylines, prepared by the Control Team in consultation with experts, become the basis for the preparation of scenario “injects:” i.e., newspaper articles, VNN broadcasts, reports from NGOs, private communications between officials, classified information, government leaks, etc., which, when put together, constitute a linear progression. These are all written and/or filmed prior to the exercise. The progression is then mapped in an hourly chart for the unfolding events over a multi-day period. All six scenarios are placed on the same chart, in six columns, giving the Control Team a birds-eye view of the progression. C. How It Works As for the nuts and bolts of the simulation itself, it traditionally begins outside of class, in the evening, on the grounds that national security crises often occur at inconvenient times and may well involve limited sleep and competing demands.171 Typically, a phone call from a Control Team member posing in a role integral to one of the main storylines, initiates play. Students at this point have been assigned dedicated simulation email addresses and provided access to the cyber portal. The portal itself gives each team the opportunity to converse in a “classified” domain with other team members, as well as access to a public AP wire and broadcast channel, carrying the latest news and on which press releases or (for the media roles) news stories can be posted. The complete universe of legal authorities required for the simulation is located on the cyber portal in the Digital Archives, as are forms required for some of the legal instruments (saving students the time of developing these from scratch in the course of play). Additional “classified” material – both general and SCI – has been provided to the relevant student teams. The Control Team has access to the complete site. For the next two (or three) days, outside of student initiatives (which, at their prompting, may include face-to-face meetings between the players), the entire simulation takes place through the cyber portal. The Control Team, immediately active, begins responding to player decisions as they become public (and occasionally, through monitoring the “classified” communications, before they are released). This time period provides a ramp-up to the third (or fourth) day of play, allowing for the adjustment of any substantive, student, or technology concerns, while setting the stage for the breaking crisis. The third (or fourth) day of play takes place entirely at Georgetown Law. A special room is constructed for meetings between the President and principals, in the form of either the National Security Council or the Homeland Security Council, with breakout rooms assigned to each of the agencies involved in the NSC process. Congress is provided with its own physical space, in which meetings, committee hearings and legislative drafting can take place. State government officials are allotted their own area, separate from the federal domain, with the Media placed between the three major interests. The Control Team is sequestered in a different area, to which students are not admitted. At each of the major areas, the cyber portal is publicly displayed on large flat panel screens, allowing for the streaming of video updates from the media, AP wire injects, articles from the students assigned to represent leading newspapers, and press releases. Students use their own laptop computers for team decisions and communication. As the storylines unfold, the Control Team takes on a variety of roles, such as that of the President, Vice President, President’s chief of staff, governor of a state, public health officials, and foreign dignitaries. Some of the roles are adopted on the fly, depending upon player responses and queries as the storylines progress. Judges, given full access to each player domain, determine how effectively the students accomplish the national security goals. The judges are themselves well-experienced in the practice of national security law, as well as in legal education. They thus can offer a unique perspective on the scenarios confronted by the students, the manner in which the simulation unfolded, and how the students performed in their various capacities. At the end of the day, the exercise terminates and an immediate hotwash is held, in which players are first debriefed on what occurred during the simulation. Because of the players’ divergent experiences and the different roles assigned to them, the students at this point are often unaware of the complete picture. The judges and formal observers then offer reflections on the simulation and determine which teams performed most effectively. Over the next few classes, more details about the simulation emerge, as students discuss it in more depth and consider limitations created by their knowledge or institutional position, questions that arose in regard to their grasp of the law, the types of decision-making processes that occurred, and the effectiveness of their – and other students’ – performances. Reflection papers, paired with oral briefings, focus on the substantive issues raised by the simulation and introduce the opportunity for students to reflect on how to create opportunities for learning in the future. The course then formally ends.172 Learning, however, continues beyond the temporal confines of the semester. Students who perform well and who would like to continue to participate in the simulations are invited back as members of the control team, giving them a chance to deepen their understanding of national security law. Following graduation, a few students who go in to the field are then invited to continue their affiliation as National Security Law fellows, becoming increasingly involved in the evolution of the exercise itself. This system of vertical integration helps to build a mentoring environment for the students while they are enrolled in law school and to create opportunities for learning and mentorship post-graduation. It helps to keep the exercise current and reflective of emerging national security concerns. And it builds a strong community of individuals with common interests. CONCLUSION The legal academy has, of late, been swept up in concern about the economic conditions that affect the placement of law school graduates. The image being conveyed, however, does not resonate in every legal field. It is particularly inapposite to the burgeoning opportunities presented to students in national security. That the conversation about legal education is taking place now should come as little surprise. Quite apart from economic concern is the traditional introspection that follows American military engagement. It makes sense: law overlaps substantially with political power, being at once both the expression of government authority and the effort to limit the same. The one-size fits all approach currently dominating the conversation in legal education, however, appears ill-suited to address the concerns raised in the current conversation. Instead of looking at law across the board, greater insight can be gleaned by looking at the specific demands of the different fields themselves. This does not mean that the goals identified will be exclusive to, for instance, national security law, but it does suggest there will be greater nuance in the discussion of the adequacy of the current pedagogical approach. With this approach in mind, I have here suggested six pedagogical goals for national security. For following graduation, students must be able to perform in each of the areas identified – (1) understanding the law as applied, (2) dealing with factual chaos and uncertainty, (3) obtaining critical distance, (4) developing nontraditional written and oral communication skills, (5) exhibiting leadership, integrity, and good judgment in a high-stakes, highly-charged environment, and (6) creating continued opportunities for self-learning. They also must learn how to integrate these different skills into one experience, to ensure that they will be most effective when they enter the field. The problem with the current structures in legal education is that they fall short, in important ways, from helping students to meet these goals. Doctrinal courses may incorporate a range of experiential learning components, such as hypotheticals, doctrinal problems, single exercises, extended or continuing exercises, and tabletop exercises. These are important classroom devices. The amount of time required for each varies, as does the object of the exercise itself. But where they fall short is in providing a more holistic approach to national security law which will allow for the maximum conveyance of required skills. Total immersion simulations, which have not yet been addressed in the secondary literature for civilian education in national security law, may provide an important way forward. Such simulations also cure shortcomings in other areas of experiential education, such as clinics and moot court. It is in an effort to address these concerns that I developed the simulation model above. NSL Sim 2.0 certainly is not the only solution, but it does provide a starting point for moving forward. The approach draws on the strengths of doctrinal courses and embeds a total immersion simulation within a course. It makes use of technology and physical space to engage students in a multi-day exercise, in which they are given agency and responsibility for their decision making, resulting in a steep learning curve. While further adaptation of this model is undoubtedly necessary, it suggests one potential direction for the years to come.

**Cyber threats are real – they facilitate dangerous armed social movements**

**Deibert and Rohozinski 2010**

(Ronald J, professor of Political Science and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto, and Rafal, Canadian expert and practitioner active in the fields of information security, cyber warfare, and the globalization of armed violence at the University of Toronto, 2010, International Studies Association, “Risking Security: Policies and Paradoxes of Cyberspace Security,” International Political Sociology, vol. 4, p. 22, BS)

Even among democratic states, **the explosion of civic networks has presented serious challenges**, though of a slightly different nature. **Just as progressive and social justice groups have made use of the Internet to advance global norms, so too have a wide variety of militant groups, extremists, criminal organizations, and terrorists to serve more ulterior purposes. Cyberspace has facilitated their activities** in much the same way as it has for more benign civil society networks that often get more attention, but **the aims of these groups are often criminal, covert, and sometimes violent. We call these risks through the network dark nets**, of which there are two different sorts (Deibert and Rohozinski 2008). **The most well known of the dark nets are armed social movements, which can represent a multiplicity of local causes, but whose ability to share tactics, contacts, and at times, drink from the same ideological well, make them appear as a uniﬁed global network. In the post-9/11 era, Al Qaeda and the Jihad movements represent the most visible manifestation of this kind of armed social movement. However, they are by no means the ﬁrst and only networks of this kind.** Many of the ‘‘new wars’’ (as Mary Kaldor calls them) that occurred during the 1990s were fought essentially as transnational civil wars where participants pursued both guerilla and conventional warfare against government and rival groups (Kaldor 1999). **In conﬂicts that included Sri Lanka, Somalia, former Yugoslavia, West Africa and Chechnya, ‘‘new wars’’ demonstrated that armed social movements are capable of challenging and at times defeating state actors without the need of state-based patrons or backers. More importantly, this new generation of armed social actors has also increasingly embraced cyberspace** (Rohozinski 2004). **They recognize the capacity afforded by cyberspace to ‘‘effect’’ both their supporters and opponents**. Signiﬁcantly, it was these groups, rather than militaries of the First World War, that were the ﬁrst to leverage cyberspace as means to wage information operations redeﬁning the main battleﬁeld away from the military and towards the political sphere (Weimann 2006b). **Beginning with the ﬁrst Chechen war, the video taping of attacks on the Russian military became more important than the military signiﬁcance of the attacks themselves.** When shown to supporters, as well as the Russian public (via rebroadcast in Russian television, and later on the Internet) their shock value was enough to convey the impression that the Russian military was being defeated. Similar tactics were adopted and further reﬁned by Hezbollah in its resistance against Israeli occupation of Southern Lebanon prior to their withdrawal in 2001, and again in the 2006 summer war. Attacks were documented and produced in the form of music videos, that were both broadcast across Hezbollah’s terrestrial TV station, (al Manar) as well as made available for download from a website, the movement established as part of its strategic communications and information warfare strategy (Pahlavi 2007; Wehrey 2002). **These video shorts proved highly effective**, and have since undergone several signiﬁcant evolutions, paralleling the spread and popularity of such on-line resources as YouTube and Twitter that are used by ‘‘civil’’ networks. **They are now one of the key instruments used by these movements to attract interest in their causes and are a signiﬁcant feature of the more than 4,500+ active jihad websites, chat rooms, and forums** (Weimann 2006a; Kimmage 2008). As the resources necessary for producing multimedia technologies continue to fall, and access to inexpensive digital cameras and computers increases, the threshold and number of video and other multimedia products in circulation has grown exponentially, while the age of the producers has declined. During the early months of the second Intifada, for example, several of the more compelling PowerPoint slides circulating on the Internet depicting the brutality of the Israeli reoccupation of the West bank were produced by a 14-year-old living in a refugee camp in Lebanon.

 **Cyber threats are real – cyberspace is organized transnationally, not governed centrally, constantly changes, and is difficult to regulate**

**Deibert and Rohozinski 2010**

(Ronald J, professor of Political Science and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto, and Rafal, Canadian expert and practitioner active in the fields of information security, cyber warfare, and the globalization of armed violence at the University of Toronto, 2010, International Studies Association, “Risking Security: Policies and Paradoxes of Cyberspace Security,” International Political Sociology, vol. 4, p. 15-16, BS)

Globalization is generating new security challenges. Modern societies confront a myriad of risks that threaten economic prosperity, undermine the safety and security of citizens, and cause signiﬁcant disruption to society and politics. These risks range from empowered and militant nonstate actors to technological and human-made processes, such as environmental degradation and global warming. **Risk mitigation has become a routine matter of good public policy. Cyberspace represents a special category of risk.**1 A term once found only in science ﬁction novels, cyberspace describes the human-made domain for action that exists as a consequence of an interconnected and interdependent global communications and computing infrastructure. **Cyberspace connects more than half of all humanity and is an indispensable component of political, social, economic, and military power worldwide. In strategic terms, cyberspace is accepted now as a domain equal to land, air, sea, and space. Predictably, in the post-9/11 era, cyberspace is the focus of security concerns as states weigh the risks and beneﬁts of omnipresent global connectivity. However, cyberspace presents special security challenges, for a variety of reasons. First, and most importantly, it is a communication network that is organized transnationally and not through the institutional structures of the state system. Although states and individuals may claim sovereignty or ownership over segments of cyberspace, particularly parts of its material infrastructure, or even opt out of it entirely, once in they are never fully in control. Cyberspace has emergent properties, in other words, that elude state control. Second, and closely related, cyberspace is operated as a mix of public and private networks. Governance of cyberspace, like its architecture, is distributed, and does not take place within a singular forum or point of control** (Dutton and Peltu 2007). Even the Internet Corporation for Assigned Names and Numbers (ICANN), that is most often associated with Internet governance issues, is only narrowly concerned with domain and routing management and not with the full panoply of cyberspace governance issues (Mueller 2002). **There are instead numerous sites of cyberspace governance, from spectrum allocation to copyright and intellectual property regulation to content ﬁltering and cyber-crime (among many others). Each of these sites involves numerous stakeholders, including governments, businesses, and civil society networks. In addition, private sector actors from multiple countries operate most of the core infrastructural components of cyberspace.** What James Der Derian (2003) calls ‘‘heteropolarity’’ perhaps best characterizes the state of cyberspace governance. **Third, unlike other domains, such as the sea, land, air, or space, cyberspace is a human-made domain in constant ﬂux based on the ingenuity and participation of users /////themselves. One of the core design features of cyberspace is the end-to-end principle, which allows for generative technologies to be introduced into cyberspace by end users as long as they conform to the basic protocols of interconnectivity** (Saltzer, Reed, and Clark 1984). **The latter introduces not only great variation and constant innovation, but also new and unforeseen security risks** (Zittrain 2007). **It also creates major problems for regulation, insofar as regulators are always chasing a moving target. In other words, cyberspace is a domain of constant transformation and a high degree of complexity. Fourth, cyberspace is comprised of both a material and a virtual realm—a space of things and ideas, structure and content.** Theorists and observers of cyberspace often focus on one of these elements to the exclusion or diminution of the other, but both are important and interdependent. Cyberspace is indeed a ‘‘consensual hallucination’’ as Gibson (1984) famously deﬁned it, but one that could not exist without the physical infrastructure that supports it. **Attempts to control and monitor the virtual realm of cyberspace often begin with interventions in the physical infrastructure, at key Internet chokepoints** (Deibert, Palfrey, Rohozinski, and Zittrain 2008). **However, these efforts are never entirely comprehensive; once released into cyberspace, the distributed properties of the network help ideas and information circulate, duplicate and proliferate. Even radical measures, such as disconnecting the Internet entirely as was done recently in Burma and Nepal, can only limit, but not entirely contain the ﬂow of ideas.**

# 2AC

### 2AC Risk

#### Framework - the aff is a normative statement. Vote aff if plan is a good idea, neg if it isn’t.

#### A. Solves their offense – the impact of the K is a reason the aff is bad

#### B. Aff choice – they arbitrarily steal 9 minutes of offense, destroys the aff’s only advantage

#### Extinction 1st -

**Perm do both**

**Permutation do the plan and all non-competitive parts of the alternative**

**The alt alone is worthless to policy making – only coupling with the method of the 1AC can solve**

**Cairney 10**

(Paul, Chair in Politics and Public Policy¶ BA (Hons), MSc, PhD at Aberdeen University, “Complexity Theory in Public Policy” <http://www.psa.ac.uk/journals/pdf/5/2010/121_665.pdf>, SEH)

**Why has Complexity Theory Struggled for Attention?¶** The first difficulty with complexity theory is that it is difficult to pin down. While we¶ may find similar discussions in a wide range of texts in the literature, this may be merely¶ because it is vague. Its appeal in the sciences may be because it means different things to¶ different people, suggesting that initial enthusiasm and cross-disciplinary cooperation may be replaced by growing scepticism.¶ The second is that, **when we do pin the meaning of complexity theory down, it seems to¶ present a deterministic argument**. **The danger is that if the complex system is¶ predominantly the causal factor then we lose sight of the role that policymakers play;¶ there may be a tendency to treat the system as a rule-bound structure which leaves¶ minimal room for the role of agency.** It is tempting to contrast this picture with¶ interpretive social science which rejects the assumption of structural constraint. Rather, it¶ explores how agents perceive their decision-making environments; how they reproduce,¶ accept or challenge the structural, institutional and wider systemic constraints that they¶ appear to face when making decisions. Indeed, they may even reject terms such as¶ ‘institution’ and ‘rule’ because they imply a sense of permanence or common¶ understanding that has not been demonstrated (Bevir and Rhodes, 2003; 2006). This is¶ the essence of the study of politics, explaining why different policymakers make different¶ decisions under the same circumstances. Yet, there is perhaps good reason to resist this¶ temptation because, if the aim of complexity theory is to identify a shift in rule-bound¶ behaviour, then it could have something in common with interpretivist accounts which¶ seek to understand how agents interpret, adapt to and influence their decision-making¶ environment. This seems to be Teisman and Klijn’s (2008: 289) point when they focus¶ on agents adapting to the fitness landscape. Further, as Schneider and Bauer (2007: 6)¶ discuss, complexity theory appears to differ from the old functionalist logic of systems¶ theories that has gone out of fashion in political science. A kinder treatment of¶ complexity suggests that, so far, it has been used in public policy more to provide¶ practical advice to public managers than to inform the wider theological debates on¶ structure and agency we find in political science. I return to this theme in the next¶ section. The third is that **it is difficult to identify or define a system and separate it from its¶ environment**. For Mitleton-Kelly (2003: 30) this is not a problem because it is useful to¶ work on the assumption that there is no fixed boundary between the two. Rather, the¶ picture is one of overlapping systems or an ‘intricate web of inter-relationships’,¶ suggesting that systems as a whole engage in ‘co-evolution’. Rather than a system¶ adapting to its environment, we picture organisations influencing and being influenced by¶ the ‘social ecosystem’ which consists of other organisations (2003: 31).¶ This conclusion raises a fourth problem related to scale or perspective in complex¶ systems**. Not only do we not know what a complex system is, but we don’t know at what¶ level we should view it**. **Wider scientific accounts relate the benefit of complexity theory¶ to the ability to step back and see the system as a whole**, in much the same way that we¶ move from looking at molecules to observing the whole being. Yet, **this doesn’t guide us¶ too much, because we could still see systems at different levels, such as a healthcare¶ system or a political system or even 8an international political system** (plus authors such as¶ Mitleton-Kelly often seem to situate analysis at the organisational level). While this¶ gives us some flexibility, **it could raise a whole host of further theoretical questions (are¶ central policymakers situated within, or treated as external to, the systems they cannot¶ control?** If a country’s political system is made up of a number of other systems, does this suggest that there are super-emergent processes when systems interact with each¶ other?).¶ **The fifth is that it is difficult to know which types of policy issue or area complexity¶ theory applies to.** For example, Klijn (2008: 314) suggests that complexity theory is best¶ suited to ‘wicked problems’, suggesting that it refers primarily to issues of joined-upgovernment¶ and/ or intractable policy problems (what would this exclude?). Bovaird¶ (2008: 325) suggests that complex systems “are less likely to be found in ‘command-andcontrol’¶ environments”. This is confusing for two related reasons. First, the best¶ example in the UK of a command-and-control approach is the English NHS. Yet,¶ Kernick (2006) argues that complexity theory is well suited to explain why the NHS is¶ impervious to central control. Second, perhaps Bovaird is referring not to areas with¶ command-and-control styles, but those conducive to them. If so, there seems to be no¶ way to decide which areas are most relevant. The irony of governance, highlighted by¶ Rhodes (1997), in which successive governments have contributed to their own lack of¶ central control, knows no bounds. Perhaps the point is that the identification of¶ emergence and self-organizing behaviour is most likely in areas where the role of the¶ ‘centre’ is not strong, but this also raises further issues (below). The sixth is that, **although anti-reductionism and whole-systems approaches sound¶ attractive** (almost like a valence issue), **reductionist theories have a strong hold in¶ political science.** Indeed, **rational choice theory may represent complexity theory’s¶ poplar opposite because it seeks parsimonious results based on a reduction of the social¶ world into as few factors as possible.** This is as much a practical as a philosophical issue.¶ **While we may view the world as a complex system, we do not have the ability to study it¶ as one**. The ACF, for example, situates analysis at the level of the subsystem and¶ identifies two main processes: a process of learning within subsystems as advocacy¶ coalitions compete to define the policy problem and account for new information, and an¶ external process which may produce shocks to the system that change how the subsystem¶ operates (Sabatier and Jenkins-Smith, 1993; Weible et al, 2009). **The interesting aspect¶ of this framework is that, while from a complex systems perspective we may prefer to¶ study the system as a whole, the ACF may be no worse a way to study the process when¶ we are faced with limited resources and cognitive abilities**.¶ A final problem may be that **complexity theory complicates the study of public policy¶ without offering something new. This point seems strongest when applied to the study¶ of implementation.** For example, one case study in the PMR special issue demonstrates¶ ‘how local governments develop contrasting behaviour on the same national policy¶ impulse due to self-organizing abilities to combine adaptiveness and self referentiality’¶ (Teisman and Klijn, 2008: 296), but Teisman and Klijn do not show how this differs from¶ similar ‘bottom-up’ processes of self-selection in implementation structures (Hjern, 1981;¶ Hjern and Porter, 1982) or street-level bureaucracy (Lipsky, 1980) identified 30 years ago¶ (also compare Buuren and Gerrits’ 2008: 382 line that ‘decisions are neither the starting¶ nor the finishing points of a decision-making process’ with Barret and Fudge’s focus on¶ ‘policy in action’). Similarly, the statement that complexity theory shows us that¶ ‘managers are not the rational beings presented in many managerial handbooks (Teisman and Klijn, 2008: 297) does not seem startlingly original. We are in the very¶ familiar territory of uncertain policy effects and unintended consequences. A¶ sympathetic assessment might suggest that these points are being restated because the¶ lessons from bottom-up studies have been lost or ignored. This seems to be the tone of¶ Butler and Allan’s (2008) argument that there is no one-best-way in the delivery of local¶ services and in Kernick’s (2006: 388) criticism of the assumption of a single¶ organizational solution in the NHS (and promotion of a more meaningful dialogue¶ between those who design and those who deliver and use the service). But is there¶ anything more to complexity theory than this?

**Linearity might not be true but complexity isn’t 100% true either**

Gorka et al 12

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

These competing views of America’s national security concerns indicate an important and distinctive characteristic of today’s global landscape: **prioritization is simultaneously** very **difficult and very important** for the United States. **Each of these threats and potential threats**—**al Qaeda, China, nuclear proliferation, climate change, global disease, and so on**—**can conjure up a worstcase scenario that is immensely intimidating.** Given the difficulty of combining estimates of probabilities with the levels of risk associated with these threats, **it is challenging to establish priorities.** Such **choices and trade-offs are** **difficult, but not impossible**. 30 In fact, **they are the stock-in-trade of the strategist and planner**. **If the U**nited **S**tates **is going to respond proactively and effectively to today’s international environment,** **prioritization is the key first step**—**and** **precisely the opposite reaction** **to the** **complacency and undifferentiated fear that the** **notion of unprecedented complexity encourages**. **Complexity suggests a maximization of flexibility and** **minimization of commitment**; **but prioritization** **demands wise allotment of resources** **and attention in a way that** **commits American power and effort** **most effectively and efficiently**. Phrased differently, **complexity induces deciding not to decide**; **prioritization encourages deciding which decisions matter most.** **Today’s world** **of** **diverse threats** characterized by uncertain probabilities and unclear risks **will** **overwhelm us** **if the specter of complexity seduces us into** either **paralysis or paranoia**. Some **priorities need to be set** if the United States is to find the resources to confront what threatens it most. 31 As Michael Doran recently argued in reference to the Arab Spring, “the United States must train itself to see a large dune as something more formidable than just endless grains of sand.”32¶ **This is not to deny the possibility of** **nonlinear phenomena, butterfly effects, self-organizing systems** that exhibit patterns in the absence of centralized authority, **or emergent properties**. 33 If anything, **these hallmarks of complexity theory remind strategists of the importance of revisiting key assumptions in light of new data and** allowing for **tactical flexibility** in case of unintended consequences. **Sound strategy requires hard choices and commitments,** **but it need not be inflexible**. **We can prioritize without being procrustean.** **But a model in which everything is potentially relevant is a model in which** **nothing is**.

#### Epistemic uncertainty isn’t a voting issue: imaging scenarios, even if unlikely or flawed is a pre requisite to good analysis – the aff isn’t a research paper, just dismiss poorly constructed impacts

Wimbush, 08

Director of the Center for Future Security Strategies

(S. Enders, senior fellow at the Hudson Institute and the author of several books and policy articles, “A Parable: The U.S.-ROK Security Relationship Breaks Down”, Asia Policy, Number 5 (January 2008), 7-24)

What if the U.S.-ROK security relationship were to break down? This essay explores the alternative futures of such a scenario. Analyzing scenarios is one technique for trying to understand the increasing complexity of strategic environments. A scenario is an account of an imagined sequence of events. The intent of a scenario is to suggest how alternative futures might arise and where they might lead, where conflicts might occur, how the interests ofdifferent actors might be challenged, and the kinds of strategies actors might pursue to achieve their objectives. Important to keep in mind is that scenarios arenothing more than invented, in-depth stories—stories about what different futures could look like and what might happen along plausible pathways to those futures. The trends and forces that go into building a scenario may be carefully researched**,** yet a scenario is not a research paper. Rather, it is a work of the imagination. As such, scenarios are, first, tools that can help bring order to the way analysts think about what might happen in future security environments; second, scenarios are a provocative way of revealing possible dynamics of future security environments that might not be apparent simply by projecting known trends into the future. Scenarios are particularly useful in suggesting where the interests and actions of different actors might converge or collide with other forces, trends, attitudes, and influences. By using scenarios, to explore the question “what if this or that happened?” in a variety of different ways, with the objective of uncovering as many potential answers as possible, analysts can build hedging strategies for dealing with many different kinds of potential problems. Though they may choose to discount some of these futures and related scenarios, analysts will not be ignorant of the possibilities, with luck avoiding having to say: “I never thought about that.”

#### Risk framing motivates new social movements and re-democratizes politics

Borraz, ‘7

[Olivier Borraz, Centre de Sociologie des Organisations, Sciences Po-CNRS, Paris, Risk and Public Problems, Journal of Risk Research Vol. 10, No. 7, 941–957, October 2007, p. 951]

These studies seem to suggest that risk is a way of framing a public problem in such a way as to politicize the search for solutions. This politicization entails, in particular, a widening of the range of stakeholders, a reference to broader political issues and debates, the search for new decision- making processes (either in terms of democratization, or renewed scientific expertise), and the explicit mobilization of non-scientific arguments in these processes. But if this is the case, then it could also be true that risk is simply one way of framing public problems. Studies in the 1990s, in particular, showed that a whole range of social problems (e.g., poverty, housing, unemployment) had been reframed as health issues, with the result that their management was transferred from social workers to health professionals, and in the process was described in neutral, depoliticized terms (Fassin, 1998). Studies of risk, on the contrary, seem to suggest that similar social problems could well be re-politicized, i.e., taken up by new social movements, producing and using alternative scientific data, calling for more deliberative decision-making procedures, and clearly intended to promote change in the manner in which the state protects the population against various risks (health and environment, but also social and economic). In other words, framing public problems as risks could afford an opportunity for a transformation in the political debate, from more traditional cleavages around social and economic issues, to rifts stemming from antagonistic views of science, democracy and the world order.

The burden of proof is on the negative to prove we are wrong – simply pointing out the 1AC seems fishy is poor scholarship and doesn’t rise to an sufficient reason to reject us.

Yudkowsky 6

Eliezer Yudkowsky, Research Fellow at the Singularity Institute for Artificial Intelligence that has published multiple peer-reviewed papers on risk assessment. Cognitive biases potentially affecting judgment of global risks Forthcoming in Global Catastrophic Risks, eds. Nick Bostrom and Milan Cirkovic. August 31, 2006.

Every true idea which discomforts you will seem to match the pattern of at least one psychological error. Robert Pirsig said: “The world’s biggest fool can say the sun is shining, but that doesn’t make it dark out.” If you believe someone is guilty of a psychological error, then demonstrate your competence by first demolishing their consequential factual errors. If there are no factual errors, then what matters the psychology? The temptation of psychology is that, knowing a little psychology, we can meddle in arguments where we have no technical expertise – instead sagely analyzing the psychology of the disputants. If someone wrote a novel about an asteroid strike destroying modern civilization, then someone might criticize that novel as extreme, dystopian, apocalyptic; symptomatic of the author’s naive inability to deal with a complex technological society. We should recognize this as a literary criticism, not a scientific one; it is about good or bad novels, not good or bad hypotheses. To quantify the annual probability of an asteroid strike in real life, one must study astronomy and the historical record: no amount of literary criticism can put a number on it. Garreau (2005) seems to hold that a scenario of a mind slowly increasing in capability, is more mature and sophisticated than a scenario of extremely rapid intelligence increase. But that’s a technical question, not a matter of taste; no amount of psychologizing can tell you the exact slope of that curve. It’s harder to abuse heuristics and biases than psychoanalysis. Accusing someone of conjunction fallacy leads naturally into listing the specific details that you think are burdensome and drive down the joint probability. Even so, do not lose track of the real- world facts of primary interest; do not let the argument become about psychology. Despite all dangers and temptations, it is better to know about psychological biases than to not know. Otherwise we will walk directly into the whirling helicopter blades of life. But be very careful not to have too much fun accusing others of biases. That is the road that leads to becoming a sophisticated arguer – someone who, faced with any discomforting argument, finds at once a bias in it. The one whom you must watch above all is yourself. Jerry Cleaver said: “What does you in is not failure to apply some high-level, intricate, complicated technique. It’s overlooking the basics. Not keeping your eye on the ball.” Analyses should finally center on testable real-world assertions. Do not take your eye off the ball.

### 2AC Nietzsche

#### 1. FRAMEWORK—The aff is a normative statement. Vote aff if plan is a good idea, neg if it isn’t.

A. Solves their offense –the impact of the K is a reason the aff is bad.

B. Aff choice – they arbitrarily steal 9 minutes of offense, destroys the aff’s only advantage.

#### Their refusal to engage in politics is the ultimate form of ressentiment.

**Saul Newman (postdoctoral fellow at Macquarie University). “Anarchism and the Politics of Ressentiment.” Theory and Event 4:3. 2000.**

**Can this paradoxical relationship of reflection and opposition be seen as a form of *ressentiment* in the Nietzschean sense? I would argue here that, although there are differences, the Manichean relationship of opposition between the human subject and political power that is found in anarchism obeys the general logic of ressentiment described above. This is for two reasons. Firstly, as we have seen, ressentiment is based on the moral prejudice of the powerless against the powerful -- the revolt of the 'slave' against the 'master'. We can see this moral opposition to power clearly in anarchist discourse, which pits the essentially 'moral' and 'rational' human subject against the essentially 'immoral' and 'irrational' quality of political power. It is evident in the opposition of natural to artificial authority that is central to anarchism. Secondly, ressentiment is characterized by the fundamental need to identify oneself by looking outwards and in opposition towards an external enemy. Here, however, the comparison to anarchism is not so clear-cut. For instance, one could conceivably argue that anarchist subjectivity and ethics -- the notion of mutual aid and assistance -- is something that develops independently of political power, and that therefore it does not need an oppositional relationship with the State in order to define itself. However, I would suggest that although anarchist subjectivity does develop in a 'natural' system which is radically exterior to the 'artificial' system of political power, it is precisely through this assertion of radical exteriority that ressentiment emerges. Anarchism subscribes to a dialectical logic, according to which the human species emerges from an 'animal-like' state, and begins to develop innate moral and rational faculties in a natural system. However the subject finds this development impeded by the 'irrational', 'immoral' power of the State. Thus the subject cannot achieve his full human identity as long as he remains oppressed by the State. This is why, for Bakunin: "The State is the most flagrant negation...of humanity." The realization of the subject is always stultified, deferred, put off, by the State. This dialectic of Man and State suggests that the identity of the subject is characterized as essentially 'rational' and 'moral' only in so far as the unfolding of these innate faculties and qualities is prevented by the State. Paradoxically the State, which is seen by anarchists as an obstacle to the full identity of man, is, at the same time, essential to the formation of this incomplete identity. Without this stultifying oppression, the anarchist subject would be unable to see itself as 'moral' and 'rational'. His identity is thus complete in its incompleteness. The existence of political power is therefore a means of constructing this *absent fullness.* I would argue, then, that anarchism can only posit the subject as 'moral' and 'rational' in opposition to the 'immorality' and 'irrationality' of political power. In the same way the identity of the 'slave' is consolidated as 'good' by opposing itself to the identity of the 'master' which is 'evil'. Nietzsche would see in this an attitude of ressentiment par excellence.**

Their link evidence says that blaming it on the other bad – we blame it on the US president, no reason we will enact violence against him.

#### Our impacts aren’t constructed until they prove it.

Yudkowsky 6 – Eliezer Yudkowsky, Research Fellow at the Singularity Institute for Artificial Intelligence that has published multiple peer-reviewed papers on risk assessment. Cognitive biases potentially affecting judgment of global risks Forthcoming in Global Catastrophic Risks, eds. Nick Bostrom and Milan Cirkovic. August 31, 2006.

Every true idea which discomforts you will seem to match the pattern of at least one psychological error. Robert Pirsig said: “The world’s biggest fool can say the sun is shining, but that doesn’t make it dark out.” If you believe someone is guilty of a psychological error, then demonstrate your competence by first demolishing their consequential factual errors. If there are no factual errors, then what matters the psychology? The temptation of psychology is that, knowing a little psychology, we can meddle in arguments where we have no technical expertise – instead sagely analyzing the psychology of the disputants. If someone wrote a novel about an asteroid strike destroying modern civilization, then someone might criticize that novel as extreme, dystopian, apocalyptic; symptomatic of the author’s naive inability to deal with a complex technological society. We should recognize this as a literary criticism, not a scientific one; it is about good or bad novels, not good or bad hypotheses. To quantify the annual probability of an asteroid strike in real life, one must study astronomy and the historical record: no amount of literary criticism can put a number on it. Garreau (2005) seems to hold that a scenario of a mind slowly increasing in capability, is more mature and sophisticated than a scenario of extremely rapid intelligence increase. But that’s a technical question, not a matter of taste; no amount of psychologizing can tell you the exact slope of that curve. It’s harder to abuse heuristics and biases than psychoanalysis. Accusing someone of conjunction fallacy leads naturally into listing the specific details that you think are burdensome and drive down the joint probability. Even so, do not lose track of the real- world facts of primary interest; do not let the argument become about psychology. Despite all dangers and temptations, it is better to know about psychological biases than to not know. Otherwise we will walk directly into the whirling helicopter blades of life. But be very careful not to have too much fun accusing others of biases. That is the road that leads to becoming a sophisticated arguer – someone who, faced with any discomforting argument, finds at once a bias in it. The one whom you must watch above all is yourself. Jerry Cleaver said: “What does you in is not failure to apply some high-level, intricate, complicated technique. It’s overlooking the basics. Not keeping your eye on the ball.” Analyses should finally center on testable real-world assertions. Do not take your eye off the ball.

#### Permutation: do both

#### The interdependency between political action and personal thought is unavoidable in reaching the goals of both projects. Criticisms that try to deny our attempts to correct social injustices traps theory in the exclusions it attempts to cure. And the perm solves the resentiment and oppression impacts.

William Connolly. Identity/Difference. 1991. Page 33-34.

The most general (and idealistic) idea is to subdue the politics of generalized resentment by moving on two fronts—first, by removing social injustices that exclude a large variety of constituencies from the material and cultural life of the whole and, second, by criticizing modes of existential resentment that intensify social dogmatism with respect to identity, responsibility, and otherness. These two "fronts" are neither separable nor fully harmonious within this vision. They are interdependent in that a politics of freedom cannot make much progress on either without making some on both. They enter into strife in that each can easily become a staging area for infringements upon the other. In the chapters that follow I try to keep one eye on the first front while attending most closely to the second. This more or less reverses the emphasis I have followed in the past.

The thinking that refuses to engage the second front can often be identified through its unwillingness to explore necessary injustices in its own ideals. An unnecessary injustice is an undeserved injury done to some that can be re moved within the existing order of things. A systemic injustice is an undeserved injury not removable in the existing order. A necessary injustice is an undeserved injury that cannot be entirely eliminated without the introduction of an-other injustice. Perspectives on theory and life that do not come to terms with systemic and necessary injustices in their own ideals have, according to the perspective endorsed here, concealed the pool of existential resentment that animates them. Of course, whether and when this is so is always contestable, as is the more general perspective through which the issue is posed." But still, this perspective provides a timely test to pose to oneself in one's most rhapsodic theoretical moments: what injustice may I be concealing in my ideal so that I can dream my dream of a world without injustice?

The best perm card ever written

The interdependency between political action and critical theory is unavoidable in reaching the goals of both projects. Criticisms that try to deny our attempts to correct social injustices traps theory in the exclusions it attempts to cure.

William Connolly. Identity/Difference. 1991. Page 33-34.

The most general (and idealistic) idea is to subdue the politics of generalized resentment by moving on two fronts—first, by removing social injustices that exclude a large variety of constituencies from the material and cultural life of the whole and, second, by criticizing modes of existential resentment that intensify social dogmatism with respect to identity, responsibility, and otherness. These two "fronts" are neither separable nor fully harmonious within this vision. They are interdependent in that a politics of freedom cannot make much progress on either without making some on both. They enter into strife in that each can easily become a staging area for infringements upon the other. In the chapters that follow I try to keep one eye on the first front while attending most closely to the second. This more or less reverses the emphasis I have followed in the past.¶ The thinking that refuses to engage the second front can often be identified through its unwillingness to explore necessary injustices in its own ideals. An unnecessary injustice is an undeserved injury done to some that can be re moved within the existing order of things. A systemic injustice is an undeserved injury not removable in the existing order. A necessary injustice is an undeserved injury that cannot be entirely eliminated without the introduction of an-other injustice. Perspectives on theory and life that do not come to terms with systemic and necessary injustices in their own ideals have, according to the perspective endorsed here, concealed the pool of existential resentment that animates them. Of course, whether and when this is so is always contestable, as is the more general perspective through which the issue is posed." But still, this perspective provides a timely test to pose to oneself in one's most rhapsodic theoretical moments: what injustice may I be concealing in my ideal so that I can dream my dream of a world without injustice?

####  Only the plan affirms life – embracing the struggle against our genetic predisposition towards violence through resisting nuclear war is key

Barash and Lipton, 1985

David P., Professor of Psychology at the University of Washington (Seattle) and Judith Eve, psychiatrist at the Swedish Medical Center in Washington, “The Caveman and the Bomb” p.261-267

Fortunately, whatever genetic imperatives operate in Homo sapiens, they are unlikely to extend directly to nuclear weapons, any more than a tendency for body adornment necessarily leads to a Christian Dior necktie or a New Guinea penis sheath. The general patterns that char­acterize today's nuclear Neanderthal are, in fact, general, nonspecific. They may incline us to a degree of saber rattling that seems likely to trouble the world in one way or another as long as we and the world persist, but these patterns don't require that the saber be nuclear. On this level the nuclear Neanderthal doesn't even have to play "as if": We are called on to behave not as if we had free will regarding the renun­ciation of nuclear weapons and nuclear war, but to act in accord with that free will, which we assuredly have. That is honest empowerment indeed. Teilhard de Chardin wrote about the "Omega point" at which human beings become conscious of their own evolution and, hence, of them­selves. He called for a recognition of unity and connectedness, with our speciesborn on this planet and spread over its entire surface, coming gradually to form around its earthly matrix a single, major organic unity, enclosed upon itself; a single, hypercomplex, hyperconcentrated, hyperconscious arch-molecule, coextensive with the heavenly body on which it is born.9 In overcoming the Neanderthal mentality we could finally become hu­man, or perhaps even more than this, at last able to answer affirmatively the question: Is there intelligent life on earth? As poet and novelist Nikos Kazantzakis pleaded, "Let us unite, let us hold each other tightly, let us merge our hearts, let us create for Earth a brain and a heart, let us give a human meaning to the superhuman struggle."'° Something has spoken to me in the night, burning the tapers of the waning year; something has spoken in the night, and told me I shall die, I know not where. Saying: "To lose the earth you know, for greater knowing; to lose the life you have, for greater life; to leave the friends you loved, for greater loving; to find a land more kind than home, more large than earth—Whereupon the pillars of this earth are founded, toward which the conscience of the world is tending—a wind is rising and the rivers flow." THOMAS WOLFE 11 For the existentialists the essence of humanity is in saying no—no to injustice, to murder, to the absurd and dehumanizing universe itself But the ultimate existential tragedy is that in the long run, saying no cannot succeed. Each of us will eventually die, and this looming inevitability makes our lives absurd. By our very aliveness we are therefore embarked on a hopeless campaign, which may yield some victories, but only tem­porary ones. Like a cosmic poker game, we are playing against the house, but in this game the house never loses; even if we are briefly ahead, we cannot cash in our chips and go home winners. There is no other place to go. At the close of The Plague, Albert Camus lets us inside the thoughts of Dr. Rieux, who had courageously battled a typhoid epidemic in a North African city. Just as the plague has finally been overcome, and the survivors were celebrating in the streets, Dr. Rieux understood that the tale he had to tell could not be one of a final victory. It could be only the record of what had had to be done, and what assuredly would have to be done again in the never-ending fight against terror and its relentless onslaughts, despite their personal afflictions, by all who, while unable to be saints but refusing to bow down to pestilences, strive their utmost to be healers. And, indeed, as he listened to the cries of joy rising from the town, Rieux remembered that such joy is always imperiled. He knew what those jubilant crowds did not know but could have learned from books: that the plague bacillus never dies or disappears for good; that it can lie dormant for years and years in furniture and linen-chests; that it bides its time in bedrooms, cellars, trunks, and bookshelves; and that perhaps the day would come when, for the bane and the enlightening of men, it would rouse up its rats again and send them forth to die in a happy city.12 But effectiveness per se is not the issue. The rats may come again, and with them the plague, just as every person now alive must some day die. The real question—for would-be post-Neanderthals no less than for existential thinkers—concerns the obligation of human beings in the face of such a world. "In everlasting terms—those of eternity," wrote Thomas Wolfe, "there is no greater wisdom than the wisdom of Ecclesiastes, no acceptance finally so true as the stern fatalism of the rock. Man was born to live, to suffer, and to die, and what befalls him is a tragic lot. There is no denying this in the final end." Nonetheless, he concludes, we must "deny it all along the way." Although admitting the "stern lesson of acceptance," which calls for acknowledging the "tragic under-weft of life into which man is born, through which he must live, out of which he must die," Wolfe described his intention, "having accepted it, to try to do what was before me, what I could do, with all my might."13 Camus went farther. According to Greek mythology, Sisyphus had been condemned to spend eternity rolling an enormous rock up a steep hill; when the rock neared the top, it would roll back down, and Sisyphus would have to start again. In "The Myth of Sisyphus," Sisyphus serves not only as a metaphor for humanity but, as Camus sees it, as a model as well. His struggle is not only self-defining, but also ennobling. More­over, Camus concludes that Sisyphus is happy. There are some important differences between Sisyphus and Dr. Rieux, and the post-Neanderthal. For one thing, Dr. Rieux could afford to lose many battles and even many patients, just as Sisyphus can tolerate the constant victory of gravity. Sisyphus, after all, is crushed neither mentally nor literally by his stone; no matter how many people die from a plague, some survive. Dr. Rieux will never eradicate the plague; his glory comes from his fighting on in the face of that knowledge. Sisyphus will never succeed in his labor; his happiness comes from his self-defi­nition, knowing his futility. Unlike them, however, we are not doomed to failure. Before beginning their combat the Roman gladiators used to face the spectators in the Coliseum and announce, "We who are about to die salute you." Two thousand years later the poet W. H. Auden updated their credo: "We who are about to die demand a miracle." Like the gladiators, Auden was concerned about the end of his life, what Kurt Vonnegut calls "plain old death." And to overcome plain old personal death, nothing less than a bona fide miracle in the theological sense will do. We can say no to personal death and an absurd universe all we like, but in the end, like Rieux and Sisyphus, we are bound to lose. The good news, however, is that the other kind of death—the mass, meaningless annihilation that would come with nuclear war—is not inevitable. Unlike the overturning of personal death, no divine intervention is required. Unlike the eruption of a volcano or the brewing of a hurricane, nuclear war is a man-made problem, with man- and woman-made solutions. Unlike Auden and the gladiators, we have a precious and unique op­portunity: We can say no to our Neanderthal mentality, to our genes. We are the only creatures on earth who can do this. We have this op­portunity because our genes whisper to us, they do not shout. They can be stubborn, but they can be persuaded, cajoled, bribed, or, if necessary, simply overruled and strong-armed into submission. Dr. Rieux learned in a time of pestilence that "there are more things to admire in men than to despise." Similarly, the whole can be greater than the sum of its parts, if we choose to be. We can be greater than the sum of our genes. If that is our decision, evolution can't do a thing about it. Making that decision is the supreme test of our humanity, our greatest challenge and our most sublime opportunity. Nonetheless, war touches a deep chord in most human beings, and the decision to say no will not be an easy one. Sigmund Freud com­mented that prohibitions and taboos by their very existence strongly suggest a preexisting desire to perform the prohibited act, otherwise there would be no need for the prohibition: "What no human soul desires, there is no need to prohibit; it is automatically excluded. The very em­phasis of the commandment Thou Shalt Not Kill makes it certain that we spring from an endless ancestry of murderers, with whom the lust for killing was in the blood, as possibly it is to this day with ourselves." He also emphasized that wars occur because nations, like individuals, "still obey their immediate passions far more readily than their inter­ests,"14 a succinct summary of the plight of today's Neanderthal. Prior to World War I especially, the making of war was generally considered a laudable activity. Admiration and often adulation flowed to such men as Alexander, Achilles, Caesar, Charlemagne, Frederick the Great, Napoleon, and Robert E. Lee. The first masterpiece of Western literature (Homer's Iliad) and the first histories (Herodotus' account of the Persian Wars, and Thucydides' study of the Peloponnesian War) focused on war. Western culture is by no means unique in its glorification of war, as witness the cultures of ancient Africa, Mexico, and Fiji. Ac­cordingly, "the war against war," as William James pointed out, "is going to be no holiday excursion or camping party."15 The fact is that war and sanctified violence have had a powerful and persistent appeal cross‑culturally, although not in all cultures, and throughout human history. Thus, as James said, war has come to be seen as "preserving our ideals of hardihood," a supreme test of human effectiveness, the most de­manding and, hence, for many people, the most rewarding activity of which they are capable. It is revealing that whereas "war" exists in the plural, "peace" is conceived only in the singular. (A similar pattern obtains in other lan­guages as well.) We have the War of the Roses, the Napoleonic wars, the Maori wars, World Wars I and II, and so on, but only one peace, despite the fact that there must have been as many different kinds of peace as different kinds of wars. As with the Eskimos, who are said to have eleven words for what in English we simply call "snow," or the Bedouin, who have more than one hundred words for "camel," human beings distin­guish carefully among whatever is important to them. For countless generations the human Neanderthal has been obsessed with war, and indifferent to peace, even slightly bored with it. When and if peace becomes as appealing as war, perhaps then we shall focus on it, identi­fying its varieties and nuances. Words signifying normalcy, like "peace," "health," and "sanity," have lagged behind their pathological counter­parts; thus, we know more about diseases than about wellness. Yet, as the holistic health movements are demonstrating, in order to practice preventive medicine, it is necessary to define, describe, and validate the state of wellness before one can act effectively to preserve it. Much of war's appeal, according to William James, comes from its aura of extremis, embodying the most dangerous and strenuous of human struggles, and hence becoming strangely ennobling despite (or in part, because of) its extraordinary horror. The contemplation of war, the prep­aration for war, and in many cases even the fighting of war is something that most Neanderthals find compelling, exciting, and even fun. Accord­ing to James, this gut-level attraction "cannot be met effectively by mere counter-insistency on war's expensiveness and horror. The horror makes the thrill; and when the question is of getting the extremist and supremist out of human nature, talk of expense sounds ignominious." He therefore proposed a "substitute for war's disciplinary function"—his now-famous Moral Equivalent of War, suggesting a peacetime conscription which would not so much overcome the Neanderthal mentality as bypass it with a bit of social ju jitsu, sublimating dangerous human urges into constructive activity.16 In a sense, the Peace Corps was a practical example of James's con­ception; but a real peace corps can be fashioned only when peacemaking becomes recognized as an acceptable and active verb, and when peace takes its rightful place at our own core. Ironically, in a world society that is increasingly intolerant of personal violence, that forbids murder, assault, even the threat of physical abuse, and in which fistfights and even bullying are grossly out of place, in diplomatic parlors, war and the threat of war remain acceptable. Rather than finding a moral equivalent of war, we have collectively made war itself into a morally acceptable form of violence such that societies can contemplate and plan actions that would be unacceptable if undertaken by its individual members. Those old Neanderthal cravings are still alive and well, running just beneath the surface, needing only the slightest provocation to erupt, even in the most sophisticated and presumably civilized societies. Just let some Americans be taken hostage in Iran, or a Korean airliner violate Soviet airspace, and suddenly the cavemen are at it again and the old predictable tribal bellowing resumes. Homo, called sapiens, is all but drowned in an atavistic avalanche of anger, distrust, and intolerance. The structures of peace, built up with such care and needing such nurturance, seem woefully delicate and fragile before the crude, easily evoked Neanderthal onslaught. But here we note Theodore Roethke's observation, "In a dark time, the eye begins to see." Perhaps by thinking, feeling, and believing, we can see through our Neanderthal mentality, and forge a new awareness where we confront our limitations and our strengths, able to bend, but nonetheless to resist and not to break. A major impediment to this awareness has been our ignorance that the Neanderthal mentality even exists. There is also the double irony of pessimism—the assumption that the Neanderthal mentality, under the alias of "human nature," is un­changeable. Insofar as it succeeds, this assumption is a triumph for the Neanderthal mentality and, moreover, a self-fulfilling prophecy. It is also seductive; it leaves each of us free to go ahead with his or her own little life, all the while treading on unstable slopes, heedless of the danger. "The challenge to humans in our time is whether they can become aroused not just over small but over larger dangers," observed Norman Cousins. "Whether they can perceive universal problems as well as per­sonal ones, whether they can become as concerned over their survival as a species as they are over their jobs."" This arousal is growing, in part because the overriding universal problem is increasingly perceived as an intensely personal one, because it threatens the deepest personal values of every human being, and also because it demands a committed personal response. Perhaps we shall have the final laugh after all, and perhaps the laugh will be on evolution. In giving so much autonomy to the bodies they create, the genes of Homo sapiens have unwittingly sewn the seeds of their own overthrow (not the seeds of their destruction, for that would mean our own demise as well). It is precisely—and only—by overthrowing our genes, by taking the unprecedented step and saying no to their dangerous and insistent whisperings, that we can preserve them, along with everything else. By saying no to that aspect of our genes, we say yes to life, to love, and to hope, and even to the continuation of those troublesome genes themselves. There is no better time. "At this moment," wrote Albert Camus, when each of us must fit an arrow to his bow and enter the lists anew, to reconquer, within history and in spite of it, that which he owns already, the thin yield of his fields, the brief love of this earth, at this moment when at last a man is born, it is time to forsake our age and its adolescent furies. The bow bends; the wood complains. At the moment of supreme tension, there will leap into flight an unswerving arrow, a shaft that is inflexible and free.18 Maybe in the long run we shall all laugh together, as through our negation of the Neanderthal mentality we arrive at a new affirmation, a higher level of life, its most exalted accomplishment. This will be the point at which, while unable to be saints but refusing to bow down to universal murder, we resolve to overcome the Neanderthal mentality and thereby transcend, if not overcome, our biology itself.

#### Perm do the alternative- It literally is us –

Stefan Ramaekers. “Teaching to Lie and Obey: Nietzsche and Education.” Journal of Philosophy of Education 35.2, 2001.

In *Beyond Good and Evil*, Nietzsche says about education:

Parents involuntarily make something like themselves out of their children – they call that “education”; no mother doubts at the bottom of her heart that the child she has borne is thereby her property, no father hesitates about his right to subject it to *his own* ideas and notions of worth.

In view of the importance Nietzsche attaches to obedience, to being embedded, one should not be surprised that he considers initiating the child into a particular constellation of arbitrary laws to be a natural part of her education. For the child, education means, at least in the early stages, being subordinated to a particular view of what is worth living for, and being introduced into a system of beliefs. Education consists in teaching the child to see and to value particular things, to handle a perspective: to lie. The argument goes even further. In view of Nietzsche's perspectivism one must now say that not initiating the child into a perspective, not teaching him to lie is educationally speaking not even an option: the child makes himself familiar with a perspective he cannot ignore since this is the precondition for making sense of anything and exploring the unfamiliar. Put differently, because of the necessity of being embedded a human being is molded into a particular shape that he cannot do without.

 My understanding of Nietzsche is consequently at variance with any understanding which arguments for a radical individualism and takes the individual to be the point of reference of all values and truths. Johnston, for example, tilts the scales too strongly towards the individual as a self-affirming autonomous agent and hence disregards the epistemologically and ethically constitutive importance of the individual embeddedness for what she affirms as true and valuable. He even claims that the individual put forward by Nietzsche is the antithesis of the social realm. For Nietzsche, Johnston writes, “there is no question of a reconciliation between the realms of the individual and the social.” Referring to Dewey, he makes it look as if the Nietzschean individual can withdraw herself from social embeddedness since she apparently has no need to refer her own action to that of others. Adopting a thoroughly Nietzschean stand on education therefore requires, in Johnston's opinion, a break with education conceived as a matter of “making familiar with” and of being initiated into a particular cultural inheritance, that is as a matter of socialization in the rich sense. In consequence education becomes essentially *self-education*.

#### Rejecting ethical norms means the will-to-power reigns supreme – guarantees extinction

Fasching 1993 (Darrell J., Professor of Religious Studies at University of South Florida, The Ethical Challenge of Auschwitz and Hiroshima, Pp. 28-29)

Our modern technological civilization offers us seemingly infi­nite utopian opportunities to recreate ourselves (e.g., genetic engi­neering, behavioral engineering) and our societies (social engineer­ing) and our world (chemical engineering, atomic engineering). But having transcended all limits and all norms, we seem bereft of a normative vision to govern the use of our utopian techniques. This normlessness threatens us with demonic self-destruction. It is this dark side of technical civilization that was revealed to us not only at Auschwitz and but also at Hiroshima. Auschwitz represents a severe challenge to the religious traditions of the West: to Christians, because of the complicity of Christian‑ity in the anti-Judaic path that led to Auschwitz renders its theological categories ethically suspect; to Jews, because their victim status presses faith in the God of history and in humanity to the breaking
point. But the path to Auschwitz, and from Auschwitz to Hiroshima, represents a challenge, equally severe, for the scientific and technical, secular culture of the Enlightenment. We do not seem to have fared any better under a secular ethic than we did under a religious one. Indeed we have fared worse. Genocide it seems is a unique product of the modern secular world and its technically competent barbarians. Auschwitz stands for a demonic period in modern Western civi‑lization in which the religious, political and technological develop‑ments converged to create a society whose primary purpose was the most efficient organization of that entire society for the purpose of exterminating all persons who were regarded as aliens and strangers—especially the Jews. The Nazi vision of the pure Aryan society repre‑sents a utopian vision of demonic proportions—a vision that inspired an apocalyptic revolutionary program of genocide. It reveals at once both a time of "The Death of God" in the Nietzschean sense and yet the resurgence of religion, that is, a demonic religiosity that creates a new public order in which all pluralism is eliminated from the public square and in which virtually nothing is sacred—not even human life. The period of the Holocaust stands as prophetic warning to a technological civilization that has no other norm than the will to power. If Auschwitz embodies the demonic use of technology against targeted populations to commit genocide, Hiroshima and Nagasaki represent the last such use of technology. For with the coming of Nuclear warfare, technology has outstripped human intentionality so that if the bomb is ever used again, genocide will be transformed into collective suicide or omnicide—the destruction of all life. Having ene­mies is a luxury no community on the face of the earth can any longer afford. If there is a next time, it will not matter who is right and who is wrong, we shall all perish in the flames. Auschwitz and Hiroshima suggest that the millennium which brought us the utopian age of progress threatens to bring itself to an abrupt apocalyptic conclusion. The age of the bomb seems to have shattered and restructured the millennial myth. No longer can we imagine that apocalypse will be followed by utopia. The myth of unfolding stages seems to have broken apart into an absolute Either-Or: either Apocalypse or Utopia. Not wishing to face the terror of the first option we enthusiastically (although uneasily) embrace the second. Through a somewhat forced utopian euphoria we try to repress the prophetic warnings of Ausch­witz and Hiroshima which remind us that a normless world will inevitably end in apocalyptic self-destruction.