# Cards round 6 USC – Emory KM

# 1NC

### 1NC

**Resolved requires affirmation of the resolution and negation of the resolution by the negative**

Parcher 1—Jeff Parcher, Former Debate Coach at Georgetown University [Feburary 2001, http://www.ndtceda.com/archives/200102/0790.html]

(1) Pardon me if I turn to a source besides Bill. American Heritage Dictionary: Resolve: 1. To make a firm decision about. 2. To decide or express by formal vote. 3. To separate something into constiutent parts See Syns at \*analyze\* (emphasis in orginal) 4. Find a solution to. See Syns at \*Solve\* (emphasis in original) 5. To dispel: resolve a doubt. - n 1. Frimness of purpose; resolution. 2. A determination or decision. (2) The very nature of the word "resolution" makes it a question. American Heritage: A course of action determined or decided on. A formal statemnt of a deciion, as by a legislature. (3) The resolution is obviously a question. Any other conclusion is utterly inconcievable. Why? Context. The debate community empowers a topic committee to write a topic for ALTERNATE side debating. The committee is not a random group of people coming together to "reserve" themselves about some issue. There is context - they are empowered by a community to do something. In their deliberations, the topic community attempts to craft a resolution which can be ANSWERED in either direction. They focus on issues like ground and fairness because they know the resolution will serve as the basis for debate which will be resolved by determining the policy desireablility of that resolution. That's not only what they do, but it's what we REQUIRE them to do. We don't just send the topic committee somewhere to adopt their own group resolution. It's not the end point of a resolution adopted by a body - it's the prelimanary wording of a resolution sent to others to be answered or decided upon. (4) Further context: the word resolved is used to emphasis the fact that it's policy debate. Resolved comes from the adoption of resolutions by legislative bodies. A resolution is either adopted or it is not. It's a question before a legislative body. Should this statement be adopted or not. (5) The very terms 'affirmative' and 'negative' support my view. One affirms a resolution. Affirmative and negative are the equivalents of 'yes' or 'no' - which, of course, are answers to a question.

**USFG should is governmental action**

Ericson, 03 (Jon M., Dean Emeritus of the College of Liberal Arts – California Polytechnic U., et al., The Debater’s Guide, Third Edition, p. 4)

The Proposition of Policy: Urging Future Action In policy propositions, each topic contains certain key elements, although they have slightly different functions from comparable elements of value-oriented propositions. 1. An agent doing the acting ---“The United States” in “The United States should adopt a policy of free trade.” Like the object of evaluation in a proposition of value, the agent is the subject of the sentence. 2. The verb should—the first part of a verb phrase that urges action. 3. An action verb to follow should in the should-verb combination. For example, should adopt here means to put a program or policy into action though governmental means. 4. A specification of directions or a limitation of the action desired. The phrase free trade, for example, gives direction and limits to the topic, which would, for example, eliminate consideration of increasing tariffs, discussing diplomatic recognition, or discussing interstate commerce. Propositions of policy deal with future action. Nothing has yet occurred. The entire debate is about whether something ought to occur. What you agree to do, then, when you accept the affirmative side in such a debate is to offer sufficient and compelling reasons for an audience to perform the future action that you propose.

**Statutory restrictions are: Overturn authority, alter the jurisdiction, limit authorization, require inter-agency consultation, or require prior notification**

KAISER 80—the Official Specialist in American National Government, Congressional Research Service, the Library of Congress [Congressional Action to Overturn Agency Rules: Alternatives to the Legislative Veto; Kaiser, Frederick M., 32 Admin. L. Rev. 667 (1980)]

In addition to direct statutory overrides, there are a variety of statutory and nonstatutory techniques that have the effect of overturning rules, that prevent their enforcement, or that seriously impede or even preempt the promulgation of projected rules. For instance, a statute may alter the jurisdiction of a regulatory agency or extend the exemptions to its authority, thereby affecting existing or anticipated rules. Legislation that affects an agency's funding may be used to prevent enforcement of particular rules or to revoke funding discretion for rulemaking activity or both. Still other actions, less direct but potentially significant, are mandating agency consultation with other federal or state authorities and requiring prior congressional review of proposed rules (separate from the legislative veto sanctions). These last two provisions may change or even halt proposed rules by interjecting novel procedural requirements along with different perspectives and influences into the process.

It is also valuable to examine nonstatutory controls available to the Congress:

1. legislative, oversight, investigative, and confirmation hearings;

2. establishment of select committees and specialized subcommittees to oversee agency rulemaking and enforcement;

3. directives in committee reports, especially those accompanying legislation, authorizations, and appropriations, regarding rules or their implementation;

4. House and Senate floor statements critical of proposed, projected, or ongoing administrative action; and

5. direct contact between a congressional office and the agency or office in question.

Such mechanisms are all indirect influences; unlike statutory provisions, they are neither self-enforcing nor legally binding by themselves. Nonetheless, nonstatutory devices are more readily available and more easily effectuated than controls imposed by statute. And some observers have attributed substantial influence to nonstatutory controls in regulatory as well as other matters.3

It is impossible, in a limited space, to provide a comprehensive and exhaustive listing of congressional actions that override, have the effect of overturning, or prevent the promulgation of administrative rules. Consequently, this report concentrates upon the more direct statutory devices, although it also encompasses committee reports accompanying bills, the one nonstatutory instrument that is frequently most authoritatively connected with the final legislative product. The statutory mechanisms surveyed here cross a wide spectrum of possible congressional action:

1. single-purpose provisions to overturn or preempt a specific rule;

2. alterations in program authority that remove jurisdiction from an agency;

3. agency authorization and appropriation limitations;

4. inter-agency consultation requirements; and

5. congressional prior notification provisions.

#### Prefer our interpretation:

#### Limits – A limited point of stasis is necessary for effective limits which provide equitable ground to both sides – this does not exclude their content but does require them to be topical

O’Donnell 2004, Timothy M. O’Donnell, Director of Debate, University of Mary Washington, 2004, “And the Twain Shall Meet: Affirmative Framework Choice and the Future of Debate”, DOC, http://groups.wfu.edu/debate/MiscSites/DRGArticles/DRGArtiarticlesIndex.htm

Given that advocates on all sides have dug in their heels, it does not take much to imagine that if the current situation continues to persist, the debate “community” will eventually splinter along ideological lines with break out groups forming their own organizations designed to safeguard their own sacrosanct approaches to debate. It has happened before. Yet, while debate has witnessed such crises in the past, the present era of discontent seemingly threatens the very existence of the activity as both a coherent, competitive enterprise and a rewarding, educational co-curricular activity. The origins of the present crisis have many contributing causes, including the advent of mutual preference judging, the postmodern, performative, and activist turns in scholarly circles, the dawn of the information revolution and its attendant technologies, as well as a growing resource disparity between large and small debate programs. There appears to be no mutually agreeable solution. Simply put, there is little consensus about what ought to be the focus of debate, or even what constitutes good debate. Moreover, there appears to be no agreement about what question the judge ought to be answering at the end of the debate. In the present milieu, these questions and many more are literally up for grabs.

The product of this disagreement has been a veritable boon for the negative. We need to look no further than the caselist from the 2004 National Debate Tournament (NDT) to witness the wide variety of strategic tools that the negative now has in its arsenal. In one or more debates at this tournament, the negative team attempted to alter the ground for evaluating the debate by criticizing: the use of problem-solution thinking (or the lack thereof), the will to control present in the affirmative’s opening speech act, the reliance on and use of the state, the illusory belief in fiat, the affirmative’s relationship to the “other,” the embracing or eschewing of policymaking, the ethics of the affirmative, the rhetoric of the affirmative, the representations of the affirmative, the debate community as a whole, the debate community’s practices, the affirmative’s style of debate, the type of evidence the affirmative used (including an over or under reliance on experts), the affirmative’s failure to focus on the body, the revolutionary or anti-revolutionary nature of the affirmative, the piecemeal (or lack there of) nature of change advocated by the affirmative, the desires emanating from the affirmative debaters and/or their opening speech act, the identify formation instantiated by the affirmative, the metaphors inspired by the affirmative, and the very act of voting affirmative. And this is only a partial list.

To make the point another way, it is quite likely that an affirmative team on the 2003-2004 college topic who advocated that the United States should cede political control over reconstruction in Iraq to the United Nations – certainly one of the most pressing issues of the day – could have made it through whole tournaments, indeed large portions of the whole season, without ever discussing the merits of U.S. policy in Iraq after the opening affirmative speech. Such a situation seems problematic at best. That the negative’s strategic arsenal has grown so large that negative teams are tempted to eschew consideration of the important issues of the day (in the case of Iraq, an issue with geopolitical repercussions that will echo for the rest of our lives) for competitive reasons seems more than problematic. In fact, it is downright tragic.

What is so tragic about all of this is that a debater could go through an entire debate career with very little effort to go beyond meta-argument or arguments about argument (i.e. debate theory). The sad fact is that, more often than not, the outcome of any given debate today hinges less on the substantive issues introduced by the affirmative’s first speech, than it does on the resolution of these meta-arguments. These so-called “framework” debates about what the question of the debate ought to be, while somewhat interesting, have little practical application to the circumstances of our times and in my judgment, at least, are less intellectually rewarding than their counterparts. In fact, in a situation where the merits of the public policy issues staked out by the year’s resolution along with the critical issues that those policies raise are no longer the focus of the debate – because the negative can shift the question – why have a resolution at all? The disastrous implications of this trend in academic debate are appearing at the very moment that the academy is being urged to take seriously the goal of educating citizens.

In a world where proponents for any one of the varied questions are equally strident in staking out their views about what the debate ought to be about, agreement seems to be impossible. To be sure, there is value in each of these views. Public policy is important. The political consequences of policies are important. The language used in constructing policies is important. The presentational aspects of policy are important. The epistemological, ontological, and ethical underpinnings of policies are important. And so on. What are we to do then in situations where advocates on all sides make more or less equally compelling claims? As an educator, I am interested in having the students that I work with ask and answer all of these questions at one time or another. As a coach, I am interested in having them have a predictable set of arguments to prepare for. Thus, the question for me is, how can we have a game in which they have such an opportunity? The argument of this essay seeks to chart a partial answer to this question. It involves staking out a compromise position that recognizes that there is value in a wide variety of perspectives and that all deserve an equal opportunity to be represented in competitive debates.

According to the Oxford English Dictionary, a framework consists of “a set of standards, beliefs, or assumptions” that govern behavior. When we speak of frameworks in competitive academic debate we are talking about the set of standards, beliefs, or assumptions that generate the question that the judge ought to answer at the end of the debate. Given that there is no agreement among participants about which standards, beliefs, or assumptions ought to be universally accepted, it seems that we will never be able to arrive at an agreeable normative assumption about what the question ought to be. So the issue before us is how we preserve community while agreeing to disagree about the question in a way that recognizes that there is richness in answering many different questions that would not otherwise exist if we all adhered to a “rule” which stated that there is one and only one question to be answered. More importantly, how do we stop talking past each other so that we can have a genuine conversation about the substantive merits of any one question?

The answer, I believe, resides deep in the rhetorical tradition in the often overlooked notion of stasis. Although the concept can be traced to Aristotle’s Rhetoric, it was later expanded by Hermagoras whose thinking has come down to us through the Roman rhetoricians Cicero and Quintillian. Stasis is a Greek word meaning to “stand still.” It has generally been considered by argumentation scholars to be the point of clash where two opposing sides meet in argument. Stasis recognizes the fact that interlocutors engaged in a conversation, discussion, or debate need to have some level of expectation regarding what the focus of their encounter ought to be. To reach stasis, participants need to arrive at a decision about what the issue is prior to the start of their conversation. Put another way, they need to mutually acknowledge the point about which they disagree.

What happens when participants fail to reach agreement about what it is that they are arguing about? They talk past each other with little or no awareness of what the other is saying. The oft used cliché of two ships passing in the night, where both are in the dark about what the other is doing and neither stands still long enough to call out to the other, is the image most commonly used to describe what happens when participants in an argument fail to achieve stasis. In such situations, genuine engagement is not possible because participants have not reached agreement about what is in dispute. For example, when one advocate says that the United States should increase international involvement in the reconstruction of Iraq and their opponent replies that the United States should abandon its policy of preemptive military engagement, they are talking past each other. When such a situation prevails, it is hard to see how a productive conversation can ensue.

I do not mean to suggest that dialogic engagement always unfolds along an ideal plain where participants always can or even ought to agree on a mutual starting point. The reality is that many do not. In fact, refusing to acknowledge an adversary’s starting point is itself a powerful strategic move. However, it must be acknowledged that when such situations arise, and participants cannot agree on the issue about which they disagree, the chances that their exchange will result in a productive outcome are diminished significantly. In an enterprise like academic debate, where the goals of the encounter are cast along both educational and competitive lines, the need to reach accommodation on the starting point is urgent. This is especially the case when time is limited and there is no possibility of extending the clock. The sooner such agreement is achieved, the better. Stasis helps us understand that we stand to lose a great deal when we refuse a genuine starting point.

How can stasis inform the issue before us regarding contemporary debate practice? Whether we recognize it or not, it already has. The idea that the affirmative begins the debate by using the resolution as a starting point for their opening speech act is nearly universally accepted by all members of the debate community. This is born out by the fact that affirmative teams that have ignored the resolution altogether have not gotten very far. Even teams that use the resolution as a metaphorical condensation or that “affirm the resolution as such” use the resolution as their starting point. The significance of this insight warrants repeating. Despite the numerous differences about what types of arguments ought to have a place in competitive debate we all seemingly agree on at least one point – the vital necessity of a starting point. This common starting point, or topic, is what separates debate from other forms of communication and gives the exchange a directed focus.

#### Limited stasis necessary for education and dialogue – absent a prepared in depth focus debate becomes meaningless

Bassham 07 (Gregory, Professor, Chair of the Philosophy Department, and Director of the Center for Ethics and Public Life – King’s College, et al., Critical Thinking: A Student’s Introduction, p. 3-10)

Critical thinking is what a college education is all about. In many high schools, the emphasis tends to be on “lower-order thinking.” Students are simply expected to passively absorb information and then repeat it back on tests. In col-lege, by contrast, the emphasis is on fostering “higher-order thinking”: the active, intelligent evaluation of ideas and information. This doesn’t mean that factual information and rote learning are ignored in college. But it is not the main goal of a college education to teach students¶ what to think.¶ The main goal is to teach students¶ how to think¶ —that is, how to become independent, self-directed think-ers and learners.¶ W¶ HAT¶ I¶ S¶ C¶ RITICAL¶ T¶ HINKING¶ ?¶ Often when we use the word¶ critical ¶ we mean “negative and fault-ﬁnding. This is the sense we have in mind, for example, when we complain about apparent or a friend who we think is unfairly critical of what we do or say. But¶ critical ¶ also means “involving or exercising skilled judgment or observation.”In this sense critical thinking means thinking clearly and intelligently. More precisely,¶ critical thinking¶ is the general term given to a wide range of cogni-tive skills and intellectual dispositions needed to effectively identify, analyze, and evaluate arguments and truth claims; to discover and overcome personal preconceptions and biases; to formulate and present convincing reasons in sup-port of conclusions; and to make reasonable, intelligent decisions about what to believe and what to do. Put somewhat differently, critical thinking is disciplined thinking governed by clear intellectual standards. Among the most important of these intellectual¶ standards are¶ clarity, precision, accuracy, relevance, consistency, logical cor-rectness, completeness,¶ and¶ fairness.¶ ¶ 1 The function of education is to teach one to think intensively and to think critically.¶ —Martin Luther King Jr.¶ The purpose which runs through all other educational purposes—the common thread of education—is the development of the ability to think.¶ —Educational Policies Commission¶ Let’s begin our introduction to critical thinking by looking brieﬂy at each of these important critical thinking standards.¶ Before we can effectively evaluate a person’s argument or claim, we need to understand clearly what he or she is saying. Unfortunately, that can be difﬁcult because people often fail to express themselves clearly. Sometimes this lack of clarity is due to laziness, carelessness, or a lack of skill. At other times it results from a misguided effort to appear clever, learned, or profound. Consider the following passage from philosopher Martin Heidegger’s inﬂuential but notoriously obscure book¶ Being and Time:¶ ¶ Temporality makes possible the unity of existence, facticity, and falling, and in this way constitutes primordially the totality of the structure of care. The items of care have not been pieced together cumulatively any more than temporality itself has been put together “in the course of time” [“mit der Zeit”] out of the future, the having been, and the Present. Temporality “is” not an¶ entity¶ at all. It is not, but it¶ temporalizes¶ itself. . . . Temporality temporalizes, and indeed it tempo-ralizes possible ways of itself. These make possible the multiplicity of Dasein’s modes of Being, and especially the basic possibility of authentic or inauthentic existence.¶ 2¶ ¶ That may be profound, or it may be nonsense, or it may be both. Whatever exactly it is, it is quite needlessly obscure. As William Strunk Jr. and E. B. White remark in their classic¶ The Elements of Style,¶ “[M]uddiness is not merely a disturber of prose, it is also a destroyer of life, of hope: death on the highway caused by a badly worded road sign, heartbreak among lovers caused by a misplaced phrase in a well-intentioned letter. . . .”¶ 3¶ Only by paying careful attention to language can we avoid such needless miscommunications and disappointments. Critical thinkers not only strive for clarity of language but also seek max-imum clarity of thought. As self-help books constantly remind us, to achieve our personal goals in life we need a clear conception of our goals and priori-ties, a realistic grasp of our abilities, and a clear understanding of the problems and opportunities we face. Such self-understanding can be achieved only if we value and pursue clarity of thought.¶ Precision¶ Detective stories contain some of the most interesting examples of critical thinking in ﬁction. The most famous ﬁctional sleuth is, of course, Sherlock Holmes, the immortal creation of British writer Sir Arthur Conan Doyle. In Doyle’s stories Holmes is often able to solve complex mysteries when the bungling detectives from Scotland Yard haven’t so much as a clue. What is the secret of his success? An extraordinary commitment to¶ precision.¶ First, by care-ful and highly trained observation, Holmes is able to discover clues that other shave overlooked. Then, by a process of precise logical inference, he is able to reason from those clues to discover the solution to the mystery. Everyone recognizes the importance of precision in specialized ﬁelds such as medicine, mathematics, architecture, and engineering. Critical thinkers also understand the importance of precise thinking in daily life. They under-stand that to cut through the confusions and uncertainties that surround many everyday problems and issues, it is often necessary to insist on precise answers to precise questions: What exactly is the problem we’re facing? What exactly are the alternatives? What exactly are the advantages and disadvantages of each alternative? Only when we habitually seek such precision are we truly critical thinkers.¶ Accuracy¶ There is a well-known saying about computers: “Garbage in, garbage out. ”Simply put, this means that if you put bad information into a computer, bad information is exactly what you will get out of it. Much the same is true of human thinking. No matter how brilliant you may be, you’re almost guaran-teed to make bad decisions if your decisions are based on false information. A good example of this is provided by America’s long and costly involve-ment in Vietnam. The policymakers who embroiled us in that conﬂict were not stupid. On the contrary, they were, in journalist David Halberstam’s oft-quoted phrase, “the best and the brightest” of their generation. Of course, the reasons for their repeated failures of judgment are complex and controversial; but much of the blame, historians agree, must be placed on false and inad-equate information: ignorance of Vietnamese history and culture, an exaggerated estimate of the strategic importance of Vietnam and Southeast Asia, false assumptions about the degree of popular support in South Vietnam, unduly optimistic assessments of the “progress” of the war, and so on. Had American policymakers taken greater pains to learn the truth about such matters, it is likely they would not have made the poor decisions they did. Critical thinkers don’t merely value the truth; they have a¶ passion¶ for accurate, timely information. As consumers, citizens, workers, and parents, they strive to make decisions that are as informed as possible. In the spirit of Socrates’ famous statement that the unexamined life is not worth living, they never stop learning, growing, and inquiring. ¶ Relevance Anyone who has ever sat through a boring school assembly or watched a mud-slinging political debate can appreciate the importance of staying focused on relevant ideas and information. A favorite debaters’ trick is to try to distract an audience’s attention by raising an irrelevant issue. Even Abraham Lincoln wasn’t above such tricks, as the following story told by his law partner illustrates: In a case where Judge [Stephen T.] Logan—always earnest and grave—opposed him, Lincoln created no little merriment by his reference to Logan’s style of dress. He carried the surprise in store for the latter, till he reached his turn before the jury. Addressing them, he said: “Gentlemen, you must be careful and not permit yourselves to be overcome by the eloquence of counsel for the defense. Judge Logan, I know, is an effective lawyer. I have met him too often to doubt that; but shrewd and careful though he be, still he is sometimes wrong. Since this trial has begun I have discovered that, with all his caution and fastidiousness, he hasn’t knowledge enough to put his shirt on right.” Logan turned red as crimson, but sure enough, Lincoln was correct, for the former had donned a new shirt, and by mistake had drawn it over his head with the pleated bosom behind. The general laugh which followed destroyed the effect of Logan’s eloquence over the jury—the very point at which Lincoln aimed. 4 Lincoln’s ploy was entertaining and succeeded in distracting the attention of the jury. Had the jurors been thinking critically, however, they would have realized that carelessness about one’s attire has no logical relevance to the strength of one’s arguments. Consistency It is easy to see why consistency is essential to critical thinking. Logic tells us that if a person holds inconsistent beliefs, at least one of those beliefs must be false. Critical thinkers prize truth and so are constantly on the lookout for inconsistencies, both in their own thinking and in the arguments and assertions of others. There are two kinds of inconsistency that we should avoid. One is logical inconsistency, which involves saying or believing inconsistent things (i.e., things that cannot both or all be true) about a particular matter. The other is practical inconsistency, which involves saying one thing and doing another. Sometimes people are fully aware that their words conﬂict with their deeds. The politician who cynically breaks her campaign promises once she takes ofﬁce, the TV evangelist caught in an extramarital affair, the drug counselor arrested for peddling drugs—such people are hypocrites pure and simple. From a critical thinking point of view, such examples are not especially interesting. As a rule, they involve failures of character to a greater degree than they do failures of critical reasoning. More interesting from a critical thinking standpoint are cases in which people are not fully aware that their words conﬂ ict with their deeds. Such cases highlight an important lesson of critical thinking: that human beings often display a remarkable capacity for self-deception. Author Harold Kushner cites an all-too-typical example: Ask the average person which is more important to him, making money or being devoted to his family, and virtually everyone will answer family without hesitation. But watch how the average person actually lives out his life. See where he really invests his time and energy, and he will give away the fact that he really does not live by what he says he believes. He has let himself be persuaded that if he leaves for work earlier in the morning and comes home more tired at night, he is proving how devoted he is to his family by expending himself to provide them with all the things they have seen advertised. 6 Critical thinking helps us become aware of such unconscious practical inconsistencies, allowing us to deal with them on a conscious and rational basis. It is also common, of course, for people to unknowingly hold inconsistent beliefs about a particular subject. In fact, as Socrates pointed out long ago, such unconscious logical inconsistency is far more common than most people suspect. As we shall see, for example, many today claim that “morality is relative,” while holding a variety of views that imply that it is not relative. Critical thinking helps us recognize such logical inconsistencies or, still better, avoid them altogether. Logical Correctness To think logically is to reason correctly—that is, to draw well-founded conclusions from the beliefs we hold. To think critically we need accurate and well supported beliefs. But, just as important, we need to be able to reason from those beliefs to conclusions that logically follow from them. Unfortunately, illogical thinking is all too common in human affairs. Bertrand Russell, in his classic essay “An Outline of Intellectual Rubbish,” provides an amusing example: I am sometimes shocked by the blasphemies of those who think themselves pious—for instance, the nuns who never take a bath without wearing a bathrobe all the time. When asked why, since no man can see them, they reply: “Oh, but you forget the good God.” Apparently they conceive of the deity as a Peeping Tom, whose omnipotence enables Him to see through bathroom walls, but who is foiled by bathrobes. This view strikes me as curious. 8 As Russell observes, from the proposition 1. God sees everything. the pious nuns correctly drew the conclusion 2. God sees through bathroom walls. However, they failed to draw the equally obvious conclusion that 3. God sees through bathrobes. Such illogic is, indeed, curious—but not, alas, uncommon. Completeness In most contexts, we rightly prefer deep and complete thinking to shallow and superﬁcial thinking. Thus, we justly condemn slipshod criminal investigations, hasty jury deliberations, superﬁcial news stories, sketchy driving directions, and snap medical diagnoses. Of course, there are times when it is impossible or inappropriate to discuss an issue in depth; no one would expect, for example, a thorough and wide-ranging discussion of the ethics of human genetic research in a short newspaper editorial. Generally speaking, however, thinking is better when it is deep rather than shallow, thorough rather than superﬁcial. Fairness Finally, critical thinking demands that our thinking be fair—that is, open minded, impartial, and free of distorting biases and preconceptions. That can be very difﬁ cult to achieve. Even the most superﬁ cial acquaintance with history and the social sciences tells us that people are often strongly disposed to resist unfamiliar ideas, to prejudge issues, to stereotype outsiders, and to identify truth with their own self-interest or the interests of their nation or group. It is probably unrealistic to suppose that our thinking could ever be completely free of biases and preconceptions; to some extent we all perceive reality in ways that are powerfully shaped by our individual life experiences and cultural backgrounds. But as difﬁ cult as it may be to achieve, basic fair-mindedness is clearly an essential attribute of a critical thinker. THE BENEFITS OF CRITICAL THINKING Having looked at some of the key intellectual standards governing critical reasoning (clarity, precision, and so forth), let’s now consider more speciﬁcally what you can expect to gain from a course in critical thinking. Critical Thinking in the Classroom When they ﬁrst enter college, students are sometimes surprised to discover that their professors seem less interested in how they got their beliefs than they are in whether those beliefs can withstand critical scrutiny. In college the focus is on higher-order thinking: the active, intelligent evaluation of ideas and information. For this reason critical thinking plays a vital role throughout the college curriculum. In a critical thinking course, students learn a variety of skills that can greatly improve their classroom performance. These skills include • understanding the arguments and beliefs of others • critically evaluating those arguments and beliefs • developing and defending one’s own well-supported arguments and beliefs Let’s look brieﬂy at each of these three skills. To succeed in college, you must, of course, be able to understand the material you are studying. A course in critical thinking cannot make inherently difﬁcult material easy to grasp, but critical thinking does teach a variety of skills that, with practice, can signiﬁcantly improve your ability to understand the arguments and issues discussed in your college textbooks and classes. In addition, critical thinking can help you critically evaluate what you are learning in class. During your college career, your instructors will often ask you to discuss “critically” some argument or idea introduced in class. Critical thinking teaches a wide range of strategies and skills that can greatly improve your ability to engage in such critical evaluations. You will also be asked to develop your own arguments on particular topics or issues. In an American Government class, for example, you might be asked to write a paper addressing the issue of whether Congress has gone too far in restricting presidential war powers. To write such a paper successfully, you must do more than simply ﬁnd and assess relevant arguments and information. You must also be able to marshal arguments and evidence in a way that convincingly supports your view. The systematic training provided in a course in critical thinking can greatly improve that skill as well. Critical Thinking in the Workplace Surveys indicate that fewer than half of today’s college graduates can expect to be working in their major ﬁ eld of study within ﬁ ve years of graduation. This statistic speaks volumes about changing workplace realities. Increasingly, employers are looking not for employees with highly specialized career skills, since such skills can usually best be learned on the job, but for employees with good thinking and communication skills—quick learners who can solve problems, think creatively, gather and analyze information, draw appropriate conclusions from data, and communicate their ideas clearly and effectively. These are exactly the kinds of generalized thinking and problem-solving skills that a course in critical thinking aims to improve. Critical Thinking in Life Critical thinking is valuable in many contexts outside the classroom and the workplace. Let’s look brieﬂ y at three ways in which this is the case. First, critical thinking can help us avoid making foolish personal decisions. All of us have at one time or another made decisions about consumer purchases, relationships, personal behavior, and the like that we later realized were seriously misguided or irrational. Critical thinking can help us avoid such mistakes by teaching us to think about important life decisions more carefully, clearly, and logically. Second, critical thinking plays a vital role in promoting democratic processes. Despite what cynics might say, in a democracy it really is “we the people” who have the ultimate say over who governs and for what purposes. It is vital, therefore, that citizens’ decisions be as informed and as deliberate as possible. Many of today’s most serious societal problems—environmental destruction, nuclear proliferation, religious and ethnic intolerance, decaying inner cities, failing schools, spiraling health-care costs, to mention just a few—have largely been caused by poor critical thinking. And as Albert Einstein once remarked, “The signiﬁcant problems we face cannot be solved at the level of thinking we were at when we created them.” Third, critical thinking is worth studying for its own sake, simply for the personal enrichment it can bring to our lives. One of the most basic truths of the human condition is that most people, most of the time, believe what they are told. Throughout most of recorded history, people accepted without ques-tion that the earth was the center of the universe, that demons cause disease, that slavery was just, and that women are inferior to men. Critical thinking, honestly and courageously pursued, can help free us from the unexamined assumptions and biases of our upbringing and our society. It lets us step back from the prevailing customs and ideologies of our culture and ask, “This is what I’ve been taught, but is it true?”

#### Stasis key to fairness – otherwise debates have no means to engage – fairness is a necessary condition to make debate fun and enjoyable absent ground and effective preparation incentive to research positions diminishes and active engagement is vastly decreased – fair debate is an activity that ought to be encouraged because it creates equal footing to make debate possible

#### Government engagement – a point of controversy around the government allows for transformative educational value – we don’t have to role play but we should focus our demands towards institutions. The fact that one may not like the government is not a reason to disengage – its all the more reason to engage only by debating about the policy implications about the resolution is debate meaningful.

### 1NC

#### The United States federal government should utilize limited counter-measures to combat cyber-attacks that do not rise to the level of armed attacks under the law of war.

#### The United States federal government should initiate international negotiations for an international cyber-treaty to limit and define the cyber-attacks to which states may respond with force and empower states to engage in international cooperation in evidence collection and criminal prosecutions.

#### CP solves the case provides a check on risky and hair-trigger retal AND is better than Norms. But it doesn’t restrict OCOs and DOESN’T REQUIRE CONGRESSIONAL NOTIFICATION.

Hathaway et. Al 12 (Oona A. Hathaway the Gerard C. and Bernice Latrobe Smith Professor of International Law and director of the Center for Global Legal Challenges at Yale Law, Rebecca Crootof, pursuing a PhD in Law at Yale Graduate School of Arts and Sciences, Philip Levitz, Yale Law School Princeton University, Haley Nix, Research Assistant at Yale Law School Aileen Nowlan, William Perdue, Julia Spiegel (Forthcoming in the California Law Review, 2012), “THE LAW OF CYBER-ATTACK”)

B. A Cyber-Attack Treaty

Changes in domestic law and policy, such as adding extraterritorial ¶ applicability to criminal laws and planning for the use of countermeasures, are ¶ valuable legal responses to the threat of cyber-attack. Yet “cyberspace is a ¶ network of networks that includes thousands of internet service providers ¶ across the globe; no single state or organization can maintain effective cyber ¶ defenses on its own.”280 Given the transnational nature of the challenge, ¶ international cooperation is likely to be necessary to provide a solution ¶ commensurate to the problem.281

The United States has already committed itself to working “with like-minded states to establish an environment of expectations or norms of ¶ behavior, that ground foreign and defense polices and guide international ¶ partnerships.”282 While the development of international norms is useful, it ¶ will not provide governments and private actors with the clarity of a codified ¶ definition of cyber-attack or written guidelines on how states should respond to ¶ certain types of challenges. For this reason, we recommend that the ¶ international community create a multilateral agreement. The agreement ¶ should have two central features. First, it must offer a shared definition of ¶ cyber-attack and which cyber-attacks constitute armed attack—“cyber-warfare”—under the U.N. Charter.283 Second, it should offer a framework for ¶ more robust international cooperation in evidence collection and criminal ¶ prosecution of those participating in cross-national cyber-attacks. That ¶ framework should be attentive to the challenges of over-criminalization, ¶ maintaining room for individuals to use the Internet and related technologies to ¶ engage in lawful dissent. Such a treaty would serve both international aims and ¶ national interests of participating countries.284

1. Define Cyber-Attack and Cyber-Warfare

Any international resolution defining when a cyber-attack rises to the ¶ level of an armed attack should follow the effects-based approach described ¶ above.285 In other words, a cyber-conflict should be defined to escalate into a ¶ conventional conflict only if the cyber-attack causes physical injury or ¶ property damage comparable to a conventional armed attack. Although the ¶ framework of jus in bello is of limited usefulness in evaluating the lawfulness ¶ of cyber-attacks because of its ambiguities, it would not be appropriate for this ¶ definitional treaty to attempt to articulate the content of jus in bello norms for ¶ cyber-attack. Rather, the jus in bello challenges articulated above—such as ¶ proportionality of non-lethal or temporary harm and the definition of direct ¶ participation for civilians working alongside military cyber-attackers—are ¶ likely to be clarified through state practice. In any resolution or agreement on ¶ cyber-attacks, but especially in the Security Council, the international community should ensure that the accepted definition of cyber-attack does not ¶ quell legitimate dissent and other legitimate expressive activities in ¶ cyberspace.

Adopting a clear definition of cyber-warfare and cyber-attack could be ¶ concluded in the context of a comprehensive treaty or as an independent ¶ agreement in anticipation of more broad-based future cooperation. As a ¶ starting point, a defining declaration would provide predictability on the ¶ answer to the question of whether a state is initiating an armed conflict and ¶ whether retaliation in self-defense is warranted.286 A defining declaration ¶ would also provide a reference point for the extraterritorial criminal laws ¶ described in Part IV.A and would provide content that could be incorporated ¶ into a later, more comprehensive international treaty. 287

2. International Cooperation on Evidence Collection and Criminal ¶ Prosecution

The definition of cyber-warfare and cyber-attack outlined above ¶ provides a common understanding of cyber-attack that individual countries ¶ could incorporate into their own domestic criminal legislation. This strategy ¶ has been applied, for example, in the international effort to battle bribery: the ¶ OECD Bribery Convention provides a definition of bribery that state parties then integrate into national legislation forbidding the practice.288 Under the ¶ Bribery Convention, “signatories pledged to criminalize and prosecute the ¶ bribery of foreign public officials.”289 The thirty-eight state parties have passed ¶ implementing legislation.290 A defining declaration on cyber-attack could ¶ similarly provide the content for domestic criminal legislation targeting the ¶ practice.

In addition to such loose coordination, an international treaty ¶ addressing cyber-attacks should provide for more extensive cooperation among ¶ states on evidence collection and criminal prosecution of those involved in ¶ cyber-attacks. A useful starting point for building a universal treaty is the ¶ Council of Europe Convention on Cybercrime, described in Part III.B.3, which ¶ provides for harmonized regulation of a wide range of cyber-crimes, many of ¶ which might be utilized in cyber-attacks. This treaty remains largely limited to ¶ Europe (though the United States has ratified the agreement) and it does not ¶ address all cyber-attacks that a comprehensive agreement would ideally ¶ regulate.291 Nonetheless, it provides a framework from which a more ¶ comprehensive agreement might begin.

Building on the framework established in the Council of Europe ¶ Convention, the new agreement should require parties to pass domestic laws ¶ banning the cyber-attack-related conduct prohibited under the treaty, so as to ¶ harmonize laws across states. The agreement could begin with the information-sharing program suggested above, layering on additional mechanisms for ¶ fostering cooperation in identifying and stopping the sources of cyber-attacks ¶ through criminal law enforcement agencies.

Member states should also be granted access to cyber-related ¶ information that would not be available to non-members. Information sharing ¶ would not only give states an incentive to commit to limiting their resort to ¶ armed force, but it might also aid states in identifying the source of cyber-attacks. This technical challenge—a fundamental limitation of the legal ¶ framework governing cyber-attack—is essentially a problem of information. ¶ The more information that is available to states regarding sources and locations ¶ of cyber-threats, the easier it will be to prevent cyber-attacks. International ¶ cooperation in information-sharing could be an extremely valuable ¶ complement to other regulation of cyber-attack.

Finally, consistent with the Tunis Commitment292 and Agenda,293 a ¶ treaty could provide a foundation that would allow more technologically-developed countries to assist less-developed ones in responding to shared ¶ cyber threats. As the recent White House Cyberspace Strategy memo observed,

Enhancing national-level cybersecurity among developing ¶ nations is of immediate and long-term benefits [to the United ¶ States and all nations], as more states are equipped to confront ¶ threats emanating from within their borders and in turn, build ¶ confidence in globally interconnected networks and cooperate ¶ across borders to combat criminal misuse of information ¶ technologies. It is also essential to cultivating dynamic, ¶ international research communities able to take on next - generation challenges to cybersecurity.294

#### WILL and INTENT to use cyber ops can solves a china war

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

That said, the ambiguities that characterize cyberspace do not argue against exploring how deeper theories of deterrence, which transcend nuclear weapons, could be applied in some conditions—perhaps to Sino U.S. cyber war. Most classes of cyber attackers—for example, nonstate actors and rogue states with little to lose—probably cannot be deterred by the threat of cyber retaliation. The source of lesser attacks and identity of the attackers may be difficult to determine. Consequences may be more annoying than devastating. Network defense may be adequate to contain if not prevent such attacks, reducing the importance of a threat of retaliation. Thus, deterrence is neither assured nor essential for most network attacks and attackers.

Yet the fact that deterrence does not apply against every network threat does not mean it does not apply to any. Even if adequate network protection is possible against most attackers, it might not be against all. Even if many network attackers are themselves not vitally dependent on data networking and thus unlikely to be bothered by the threat of retaliation, some might be. For our purposes, cyber deterrence need not apply generally: it need only apply to Sino-U.S. cyber war.

Beyond simple logic that some cases may not prove all cases, two factors suggest that deterrence might work under some conditions. First, states that pose the largest and most damaging network threats, for which defense is least promising, may themselves be dependent on networks and thus susceptible to threats of retaliation. Second, those posing such threats are unlikely to carry them out except in a crisis or conflict, which could help identify the attacker

Generally speaking, deterrence is indicated when five conditions are

satisfied:25

■ adequate defense is infeasible or unaffordable

■ the scale of expected harm makes it important to prevent attack

■ means of powerful retaliation exist

■ the enemy has more to lose from retaliation than to gain from attacking

■ the attacker is identifiable enough to support a credible threat of retaliation.

The first two conditions make deterrence necessary; the third, fourth, and fifth make it possible.

This study finds that these conditions fit the case of Sino-American cyber war, albeit with important qualifications. The first two conditions have already been addressed. If large-scale and sustained attacks were made against strategic networks on which the United States relies—for example, those that enable financial transactions, powergrid management, telecommunications, transportation, national intelligence, or military operations—defenses are unlikely to be adequate to prevent large and lasting harm. This does not mean that efforts to defend against major network attacks are pointless; indeed, even an imperfect defense is more important against infrequent major attacks than frequent minor ones. Better defended U.S. networks may increase the adversary’s costs and difficulties and reduce its prospective gains from attack. However, for at least the days and weeks following a major attack, network defense alone cannot be counted on to avoid serious national damage.

The third condition—means of powerful retaliation—has also been addressed. The United States has the means to retaliate strongly for a Chinese attack, regardless of the scale of the attack and damage done (because there is essentially no counterforce). The same could be said for Chinese retaliation for a U.S. cyberstrike. The United States and China have ways to communicate a credible threat of retaliation, which is as much a matter of will and intent as it is of capabilities.

The fourth condition—the attacker’s vulnerability in cyberspace— has also been addressed, at least where China and the United States are concerned. Vital functions of each, as well as their economic stability, could be badly if temporarily disrupted, with lasting effects. In the Chinese case, this danger is compounded by uncertainty about how segments of the population would respond to the crisis to their material conditions and future. These dangers would be weighed against expected gains from launching a cyber attack or expected harm that might come from not doing so. The stakes for the United States could be high—for example, the loss of some forces (aircraft carriers) and failure to prevent China from forcibly gaining control of Taiwan. For China, the stakes could be even higher—a crushing defeat by the United States, failure to reunify the country, and a setback in China’s quest to become a great power. For these reasons, cyber deterrence might not work. Yet the fact that one cannot be certain that the threat of retaliation will prevent cyber attack does not argue against a cyber deterrence strategy.

#### Miscalc alone causes Extinction

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

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

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

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

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

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

#### We have a unique net benefit – short term north Korean war is inevitable without SPEEDY and CALCULATED cyber attack – traditional military systems cannot deter – we need a range of military operations.

Leed 9/16/13 Ph.D. From RAND graduate school (Maren, is senior adviser with the Harold Brown Chair in Defense Policy Studies at CSIS, where she works on a variety of defense-related issues., senior fellow and director of the New Defense Approaches Project at CSIS, where she led projects on topics as diverse as military personnel costs, the future of ground forces, reforming the military personnel system, strategic forecasting, organizing for electromagnetic spectrum control, amphibious capabilities’ contributions to deterrence and shaping missions, and service cultures.. Dr. Leed received her A.B. in political science from Occidental College and her Ph.D. in quantitative policy analysis from the RAND Graduate School. “Offensive Cyber Capabilities at the Operational Level”, http://csis.org/publication/offensive-cyber-capabilities-operational-level)

While the future defense budget remains highly uncertain, there is a broad consensus that defense resources will continue to be under pressure. At the same time, defense challenges remain complex, geographically dispersed, and can unfold at unprecedented speed. Against this backdrop, defense policymakers face a range of challenges. First, there is a continuing need to prepare U.S. military forces to operate at scale. Even if a single, large military engagement may seem unlikely (perhaps a North Korean implosion is the most plausible short-term scenario in this regard), the potential for multiple, geographically disparate operations (to include deterrence activities aimed at precluding conflict) calls for capacity across numerous military capabilities.

Second, there is a need for strategic depth, or the ability to respond to challenges that could arise almost anywhere on the globe, potentially at speeds unable to be met by traditional military platforms if they are not already in the vicinity. Third, there is the need for a broader range of tools across the diplomatic and military space to respond to challenges arising from weakening state authority, the dispersion of political power, and the diffusion of lethality across a wide range of actors.

The implications of these challenges are significant. Absent sufficient numbers, traditional military systems will have difficulty meeting both the scale and depth requirements of the future. Compressed timelines are leading to the development of highly specialized, and very expensive, niche platforms or military systems. And approaches to address the gap between national and popular interests remain traditional and limited: special operations forces or intelligence capabilities that cannot be easily scaled.

Cyber tools can have numerous attributes that are well aligned to this environment. From a life cycle cost perspective, they can compare very favorably to other weapons systems. All have research and development costs; space programs and traditional platforms also have large production and deployment costs, whereas for cyber weapons these are minimal. Cyber and space weapons have very low operations and maintenance costs, while these can be substantial for traditional weapons systems. In sum, the cost curve for all weapons is initially steep, but it likely falls off quickly for cyber weapons, then space, then traditional platforms.

At least some cyber weapons also have the potential to scale dramatically; a single algorithm could disable a whole class of adversary systems, for example. They can operate at the speed of light, providing a timeliness that is increasingly necessary but difficult to achieve with shrinking inventories of far-flung traditional platforms. Perhaps even more importantly, cyber weapons can have unparalleled versatility. They can operate across the full range of military operations, from engagement to high-end warfare. Because their effects can be reversible, they are well suited to all phases of operation, from shaping the environment through intense warfare through reconstruction. When employed against a specific weapon system, they can counter it at multiple points in time, from early in development (e.g., causing reliability problems) to decisions about employment (disabling even one weapon can introduce doubt about the entire class of weapons in a way that kinetic strikes cannot), up to post-launch or firing. This versatility offers at least one set of capabilities that can operate in the transition space between diplomacy and military action, as well as more squarely in the military domain.

#### Nuclear war

Kline 13—Comment Editor and Writer @ National Post [Jesse Kline (Master of Journalism degree from the University of British Columbia), “Deterrence is the best way to prevent war with North Korea,” National Post, April 9, 2013, pg. http://fullcomment.nationalpost.com/2013/04/09/jesse-kline-deterrence-is-the-best-way-to-prevent-war-with-north-korea/]

Another day, another provocation from North Korea. Last week the reclusive regime threatened to launch a nuclear strike against the United States, blocked South Korean workers from entering the Kaesong industrial complex and evacuated the Russian and British embassies, warning Western diplomats the country could not ensure their safety in the event of war. This week, the North has reportedly moved missile launchers to its east coast and threatened to shut down the industrial complex it jointly operates with the South. On Tuesday it warned1 foreigners to get out of South Korea because of the threat of "thermonuclear war." This all sounds bad, but there's little reason to panic, so long as the Obama administration makes it abundantly clear that any act of war will result in the full might of the U.S. military bearing down on North Korea.

Ever since the Korean War ended in 1953, the Kim regime has been bringing the peninsula to the brink and then backing off once the international community agrees to concessions. This is especially true any time South Korea elects a new president or conducts war games with the United States—two events that have taken place in recent weeks.

Appeasement seemed like a viable option until it became apparent that the North was developing weapons of mass destruction. As it turned out, constantly giving in to the North Koreans failed to stop them from developing a nuclear weapon and only encouraged the regime to continue playing games with the international community.

The North keeps playing these game because it works. By ratcheting up the rhetoric against the U.S. and South Korea, Kim Jong-Un is able to keep his population in a constant state of fear—always worried about the enemy at the gates. He is also able to shore up support from the military and justify spending money on defence instead of feeding the population, while pressuring the international community into giving aid to the cash-strapped country.

Kim Jong-Un is moving the world to the brink of war only because past experience has shown that he'll get something out of it. The truth is that there is very little chance of North Korea deliberately starting a conflict, as the regime is surely aware that it would be crushed by the American army in a head-to-head conflict.

The U.S. has put South Korea under its nuclear umbrella—i.e., a first strike against the South would trigger an American second strike. Barack Obama has also done a fairly good job of not showing weakness in the face of North Korean aggression by continuing joint war games with the South and flying nuclear-capable bombers to the peninsula. The only real threat of war occurs if either side trips up. And by preparing his forces for war, Kim Jong-Un has created a situation in which one wrong move by edgy soldiers guarding the demilitarized zone could ignite the tinder box.

Yet there is no reason to believe that standard deterrence mechanisms will not work in this situation. During the Cold War there was a very real threat of nuclear war between the United States and the Soviet Union, but it was prevented largely because of deterrence programs such as MAD (Mutually Assured Destruction). Other nuclear-armed rivals such as India and Pakistan have also prevented war using the same principals.  Kim Jong-Un may appear crazy, but there's no indication that he has a death wish.

However, as former U.S. secretary of state Henry Kissinger once said, "Deterrence requires a combination of power, the will to use it, and the assessment of these by the potential aggressor. Moreover, deterrence is the product of those factors and not the sum. If any one of them is zero, deterrence fails."

The North Koreans are betting that the American publicare in no mood for war, following Iraq and Afghanistan. And although war should be prevented at all costs, there probably would be support in the U.S. for the kind of fight the Americans are best at: Go in, kick ass and get out—nation building be damned. Flying B-2 bombers to Korea indicated that Washington was in no mood for games, but the announcement Sunday that the Pentagon will be delaying a planned missile test sends the opposite signal.

In order for deterrence to work, Washington has to be abundantly clear that any act of war will provoke a swift, and deadly, American response. And that any nuclear weapon—detonated anywhere in the world—using North Korean technology will result in Washington turning Pyongyang into a wasteland.

So long as Kim Jong-Un and his cronies believe there is a real and credible threat from the United States, there is very little to worry about. Cancelling planned displays of American firepower and not being explicit about U.S. support for countries such as South Korea and Japan, will only embolden North Korea—making the powder keg more likely to blow.

#### Restrictions cause IBC which wrecks cyber deterrence – causes major cyber war

Kramer et. al 12 (Franklin D. Kramer is a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He served as the assistant secretary of defense for international security affairs from 1996 to 2001. Stuart H. Starr is also a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He concurrently serves as the president of the Barcroft Research Institute. Larry Wentz is a senior research fellow in the Center for Technology and National Security Policy at the National Defense University., “Cyberpower and National Security”, p. 318)

No cyber deterrence strategy can hope to be airtight to prevent all minor attacks. However, a strategy can increase the chances that major cyber attacks can be prevented; this could protect the United States and its allies not only from a single major attack but also from serial cyber aggressions and resulting damage. A worthwhile goal of a cyber deterrence strategy would be to transform medium-sized attacks into low-probability events and to provide practically 100 percent deterrence of major attacks.

A cyber deterrence strategy could contribute to other key defense activities and goals, including assurance of allies, dissuasion, and readiness to defeat adversaries in the event of actual combat. The goal of dissuading adversaries is crucially important. Thus far, the United States has not been noticeably forceful in stating its intentions to deter major cyber attacks and, if necessary, to respond to them with decisive force employing multiple instruments of power. Meanwhile, several countries and terrorist groups are reportedly developing cyber attack capabilities. Dissuasion of such activities is not an easy task: it requires investment in technical capabilities as well as building an internal consensus to employ these capabilities. If some of these actors can be dissuaded from entering into cyber competition with the United States and its allies, the dangers of actual cyber aggression will diminish.

How would a cyber deterrence strategy operate, and how can its potential effectiveness be judged? Deterrence depends on the capacity of the United States to project an image of resolve, willpower, and capability in sufficient strength to convince a potential adversary to refrain from activities that threaten U.S. and allied interests. As recent experience shows, deterrence can be especially difficult in the face of adversaries who are inclined to challenge the United States and otherwise take dangerous risks. In cases of failure, deterrence might well have been sound in theory but not carried out effectively enough to work. The aggressions of Saddam Hussein, Slobodan Milosevic, and al Qaeda might not have been carried out had these actors been convinced that the United States would respond with massive military force. These aggressions resulted because of a failure to communicate U.S. willpower and resolve, not because the attackers were wholly oblivious to any sense of restraint or self-preservation, nor because the logic of deterrence had lost its relevance.

#### Escalation of conflict is inevitable without speedy OCOs

Gjetlen 13 (Tom Gjelten is a correspondent for NPR., January / February, “First Strike: US Cyber Warriors Seize the Offensive”, [http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive)](http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive)\)

In the aftermath of the Stuxnet revelations, discussions about cyber war became more realistic and less theoretical. Here was a cyberweapon that had been designed and used for the same purpose and with the same effect as a kinetic weapon: like a missile or a bomb, it caused physical destruction. Security experts had been warning that a US adversary could use a cyberweapon to destroy power plants, water treatment facilities, or other critical infrastructure assets here in the United States, but the Stuxnet story showed how the American military itself could use an offensive cyberweapon against an enemy. The advantages of such a strike were obvious. A cyberweapon could take down computer networks and even destroy physical equipment without the civilian casualties that a bombing mission would entail. Used preemptively, it could keep a conflict from evolving in a more lethal direction. The targeted country would have a hard time determining where the cyber attack came from.

In fact, the news that the United States had actually developed and used an offensive cyberweapon gave new significance to hints US officials had quietly dropped on previous occasions about the enticing potential of such tools. In remarks at the Brookings Institution in April 2009, for example, the then Air Force chief of staff, General Norton Schwartz, suggested that cyberweapons could be used to attack an enemy’s air defense system. “Traditionally,” Schwartz said, “we take down integrated air defenses via kinetic means. But if it were possible to interrupt radar systems or surface to air missile systems via cyber, that would be another very powerful tool in the tool kit allowing us to accomplish air missions.” He added, “We will develop that—have [that]—capability.” A full two years before the Pentagon rolled out its “defensive” cyber strategy, Schwartz was clearly suggesting an offensive application.

The Pentagon’s reluctance in 2011 to be more transparent about its interest in offensive cyber capabilities may simply have reflected sensitivity to an ongoing dispute within the Obama administration. Howard Schmidt, the White House Cybersecurity Coordinator at the time the Department of Defense strategy was released, was steadfastly opposed to any use of the term “cyber war” and had no patience for those who seemed eager to get into such a conflict. But his was a losing battle. Pentagon planners had already classified cyberspace officially as a fifth “domain” of warfare, alongside land, air, sea, and space. As the 2011 cyber strategy noted, that designation “allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests.” That statement by itself contradicted any notion that the Pentagon’s interest in cyber was mainly defensive. Once the US military accepts the challenge to fight in a new domain, it aims for superiority in that domain over all its rivals, in both offensive and defensive realms. Cyber is no exception. The US Air Force budget request for 2013 included $4 billion in proposed spending to achieve “cyberspace superiority,” according to Air Force Secretary Michael Donley.

It is hard to imagine the US military settling for any less, given the importance of electronic assets in its capabilities. Even small unit commanders go into combat equipped with laptops and video links. “We’re no longer just hurling mass and energy at our opponents in warfare,” says John Arquilla, professor of defense analysis at the Naval Postgraduate School. “Now we’re using information, and the more you have, the less of the older kind of weapons you need.” Access to data networks has given warfighters a huge advantage in intelligence, communication, and coordination. But their dependence on those networks also creates vulnerabilities, particularly when engaged with an enemy that has cyber capabilities of his own.

“Our adversaries are probing every possible entry point into the network, looking for that one possible weak spot,” said General William Shelton, head of the Air Force Space Command, speaking at a CyberFutures Conference in 2012. “If we don’t do this right, these new data links could become one of those spots.”

Achieving “cyber superiority” in a twenty-first-century battle space is analogous to the establishment of air superiority in a traditional bombing campaign. Before strike missions begin against a set of targets, air commanders want to be sure the enemy’s air defense system has been suppressed. Radar sites, antiaircraft missile batteries, enemy aircraft, and command-and-control facilities need to be destroyed before other targets are hit. Similarly, when an information-dependent combat operation is planned against an opposing military, the operational commanders may first want to attack the enemy’s computer systems to defeat his ability to penetrate and disrupt the US military’s information and communication networks.

Indeed, operations like this have already been carried out. A former ground commander in Afghanistan, Marine Lieutenant General Richard Mills, has acknowledged using cyber attacks against his opponent while directing international forces in southwest Afghanistan in 2010. “I was able to use my cyber operations against my adversary with great impact,” Mills said, in comments before a military conference in August 2012. “I was able to get inside his nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations.”

Mills was describing offensive cyber actions. This is cyber war, waged on a relatively small scale and at the tactical level, but cyber war nonetheless. And, as DARPA’s Plan X reveals, the US military is currently engaged in much larger scale cyber war planning. DARPA managers want contractors to come up with ideas for mapping the digital battlefield so that commanders could know where and how an enemy has arrayed his computer networks, much as they are now able to map the location of enemy tanks, ships, and aircraft. Such visualizations would enable cyber war commanders to identify the computer targets they want to destroy and then assess the “battle damage” afterwards. Plan X would also support the development of new cyber war architecture. The DARPA managers envision operating systems and platforms with “mission scripts” built in, so that a cyber attack, once initiated, can proceed on its own in a manner “similar to the auto-pilot function in modern aircraft.” None of this technology exists yet, but neither did the Internet or GPS when DARPA researchers first dreamed of it.

#### Cyber deterrence is the only way to tranition away from nuclear deterrence

Kallberg & Lowther 12 (Jan Kallberg phD University of Texas at Dallas, Adam Lowther is a defense analyst at the Air Force Research Institute. "The Return of Dr. Strangelove: How austerity makes us stop worrying and love the bomb…and cyber war" International Affairs Forum online (2012). <http://works.bepress.com/jan_kallberg/3>)

Throughout history, adversaries have taken steps toward each other that escalated quickly because they underestimated the options and determination of the other based on the presence of resources of war at hand. Because of this, it is important that America is clear about its intentions and capability. The current “no first use” doctrine of the United States is flawed in that it does not strike fear into the hearts of our adversaries by promoting strategic ambiguity. Because it establishes clear red lines, adversaries are encouraged to push the United States to the edge, which is clearly established in policy. It may also be an unwise policy when cyber deterrence reaches maturity.

The United States is the only nation that has used nuclear arms at war when it eradicated two Japanese cities at the end of World War II. None have yet to employ the nuclear option in cyberspace. America is, after all, the only nation that has used nuclear weapons—credibility that should not be frittered away. For any potential adversary, it is a lethal fact. It might not color the minds of the current American leadership, but it influences foreign leaders. Deterrence relies upon will and capability. If the United States can no longer deter with conventional forces; cyber attack is restrained by international law and military doctrine; international sanctions are ineffective; and coalition building is beyond financial reach; nuclear deterrence becomes the primary upholder of strategic deterrence. When austerity removes other strategically deterring options and the United States is left with nuclear deterrence, Dr. Strangelove and his doomsday machines (cyber and nuclear) can make their triumphal return.

America’s ability and willingness to wage all-out war is validated by strategic deterrent patrols, bombers sitting on alert, launch-ready missiles, and an offensive cyber-geddon capability. With these assets ready to reach global targets, deterrence is upheld. No matter whether we want it, believe it, like it, or imagine it, federal austerity will force radical change in the nation’s defense posture, which is likely to lead to a greater reliance on nuclear and cyber arms.

#### Deterrence based off of nuclear weapons makes nuclear war inevitable

Beljac 09 [Dr Marko Beljac, ‘9. PhD at Monash University and he has taught at the University of Melbourne. “The Case for Minimum Nuclear Deterrence,” Science and Global Security, 7-24-09,[\*\*http://scisec.net/?p=154\*\*](http://scisec.net/?p=154).]

**Nuclear war can best be seen** as a form of risk externality. **Nuclear weapon states must recognize that** nuclear deterrence carries with it a certain probability or risk that an exchange may result due to accidental or inadvertent use.Despite this risk states nonetheless calculate that **nuclear weapons** serve to **promote state policy** and are thereby prepared to bare this risk. However, from the perspective of society as a whole this risk is far too large given the consequences **that are associated with nuclear weapons employment**. During the Cuban Missile Crisis President Kennedy reportedly exclaimed that the risk of war was one third to even. Khrushchev must have known he was taking a huge risk in sending nuclear missiles to Cuba. These risks were taken despite the potential consequences. Attempts have been made to quantify this risk, for instance Ian Bellany draws a link between the number of weapon states in a strategic complex and the probability of accidental use. The quantification of risk is necessarily imprecise; the doomsday clock might well be our best measure. But there does seem to be an intuitive relationship between deterrence and safety. This relationship has been borne out by more empirically minded analysis by Scott Sagan and Bruce Blair. **The greater the salience that a state places upon deterrence,** for example **by maintaining high alert postures, the less safe do nuclear weapons become**. Pakistan reportedly does not mate warheads with delivery vehicles. However, in an acute crisis we would expect that for Rawalpindi deterrence would trump safety and this policy would be abandoned by the Army high command. This would increase the risk of inadvertent use. **Every improvement in the effectiveness** and doctrinal scope of deterrence **adds to the risk of accidental exchange because opposing states** would need to react accordingly to maintain the effectiveness of their deterrence postures**.** **The greater the scope of deterrence the greater the risk of use given the inevitable strains and frictions of international relations.** If nuclear weapons are to deter everything then anything can escalate to nuclear war.

### 1NC Case

#### Their description of conflict is innacurate – cyber capability take forever to execute preemption doesn’t immediately “escalate” or “go kinetic”

Lewis 10/10/13 (James Andrew Lewis, Ph.D. in international Politics from the University of Chicago, is a senior fellow and director of the Technology and Public Policy Program at CSIS, where he writes on technology, security, and the international economy, Special to the Washington Post, “On the offense in the cyberspace arms race”, <http://www.registercitizen.com/lifestyle/20131010/on-the-offense-in-the-cyberspace-arms-race>)

There is no fairy dust when it comes to offensive cyber-capabilities. In the movies, a hacker types wildly on a laptop for a few seconds and turns off a city's lights. In fact, a serious attack can take months to plan, probing the target network and developing code tailored to damage, disrupt or destroy. Attacks have several stages: conducting reconnaissance to identify the target's vulnerabilities, breaking in, delivering the software "payload" and then "triggering" it — all without being detected. The most damaging cyberattacks — such as Stuxnet, which destroyed centrifuges used by the Iranian nuclear program — are still a high art. Only the United States, Britain, China, Russia and Israel possess the necessary skills, but many others want them.

Offensive cyber-capabilities provide real military advantage. This is why most leading military powers are developing them. Publicly available information shows 46 countries with military cyber-programs, and 12 countries acknowledging offensive cyber-capabilities in 2012 (up from four in 2011). Other countries have military programs but don't admit to them.

Unlike the United States, most countries say very little about their military doctrine. Most of them blend war-fighting and covert action in their cyber-war planning. Each nation's plans for offensive cyber-operations reflect their different military strategies. The Russians combine political action with cyber-strikes on command networks and critical infrastructure to cripple opponents at the start of conflict. The Chinese focus on quickly disabling U.S. military systems and have systematically hacked into just about every weapon related to U.S. plans for an "Air-Sea Battle" in Asia. Iran will attack energy infrastructure and considers cyber a way to score against a distant and once-invulnerable foe. North Korea's attacks are driven by its internal politics and dislike of the South.

There have been only a handful of true cyberattacks. Russia and China are hyperactive in cyber-espionage, but are cautious about offensive use and avoid actions that could trigger a violent response. Iran and North Korea are more aggressive and are improving their cyber-capabilities. Iran attacked Saudi Aramco, destroying data on 30,000 hard drives. North Korea did something similar to South Korean banks. The worry is that either country will miscalculate in its use of cyberattacks and stumble into a larger conflict.

Jihadis, anarchists and other non-state actors don't have real cyberattack capabilities. This is not much of a comfort because acquiring attack capabilities is becoming easier. The trend in information technology is commoditization — products get smaller, cheaper and more powerful. Cyberattack is being commoditized and cyber-crime provides innovative tools (such as the one Iran used against Aramco). Jihadis prefer the drama and violence of bombs to cyberattack, but that may change. The Syrian Electronic Army has only basic skills but could use its ties to Russian and Iranian hackers to improve. The global trend is increased capabilities and more attackers.

For the United States, offensive cyber-capabilities provide a new way to attack. The recently leaked Presidential Policy Directive 20 set the rules for "offensive cyber operations." Only the president can approve a cyber-operation likely to result in "significant consequences" that could result in the loss of life or a damaging reaction, although the defense secretary or the head of the U.S. Cyber Command can take independent action in an emergency. The United States could relax the requirement for presidential approval — similar to the presidential authorization needed to use nuclear weapons — as technology improves, but offensive cyber-capabilities are still too new, with too many unknown risks, to let anyone but the president make a decision with potentially profound consequences for the nation.

# 2NC

### Turns Case

#### Outweighs their mechanism

Laura Young, Ph.D., Purdue University Associate Fellow, June 2013, Unilateral Presidential Policy Making and the Impact of Crises, Presidential Studies Quarterly, Volume 43, Issue 2

During periods of crisis, the time available to make decisions is limited. Because the decision-making process is often arduous and slow in the legislative branch, it is not uncommon for the executive branch to receive deference during a crisis because of its ability to make swift decisions. The White House centralizes policies during this time, and presidents seize these opportunities to expand their power to meet policy objectives. Importantly, presidents do so with limited opposition from the public or other branches of government (Howell and Kriner 2008). In fact, despite the opposition presidents often face when centralizing policies, research shows policies formulated via centralized processes during times of crisis receive more support from Congress and the American people (Rudalevige 2002, 148-49). For several reasons, a crisis allows a president to promote his agenda through unilateral action. First, a critical exogenous shock shifts attention and public opinion (Birkland 2004, 179). This shift is a phenomenon known as the “rally round the flag” effect (Mueller 1970). The rally effect occurs because of the public's increase in “its support of the president in times of crisis or during major international events” (Edwards and Swenson 1997, 201). Public support for the president rises because he is the leader and, therefore, the focal point of the country to whom the public can turn for solutions. Additionally, individuals are more willing to support the president unconditionally during such times, hoping a “united front” will increase the chance of success for the country (Edwards and Swenson 1997, 201). As a result, a crisis or focusing event induces an environment that shifts congressional focus, dispels gridlock and partisanship, and increases positive public opinion—each of which is an important determinant for successful expansion of presidential power (Canes-Wrone and Shotts 2004; Howell 2003). In other words, a crisis embodies key elements that the institutional literature deems important for presidential unilateral policy making. The president's ability to focus attention on a particular issue is also of extreme importance if he wishes to secure support for his agenda (Canes-Wrone and Shotts 2004; Edwards and Wood 1999; Howell 2003; Neustadt 1990). The role the media play is pivotal in assisting a president in achieving such a result because of its ability to increase the importance of issues influencing the attention of policy makers and the priorities of viewers. Although it is possible a president can focus media attention on the policies he wishes to pursue through his State of the Union addresses or by calling press conferences, his abilities in this regard are limited, and the media attention he receives is typically short lived (Edwards and Wood 1999, 328-29). High-profile events, on the other hand, are beneficial because they allow the president to gain focus on his agenda. This occurs because the event itself generates attention from the media without presidential intervention. Thus, the ability of crises to set the agenda and shift media and public attention provides another means for overcoming the constraints placed upon the president's ability to act unilaterally. Finally, Rudalevige finds support that a crisis increases the success of presidential unilateral power even if the policy process is centralized. A crisis allows little time to make decisions. As a result, “the president and other elected officials are under pressure to ‘do something’ about the problem at hand” (2002, 89, 148). Because swift action is necessary, presidents rely on in-house advice. As a result, the policy formation process is centralized, and the president receives deference to unilaterally establish policies to resolve the crisis. During a crisis, the president has greater opportunity to guide policy because the event helps him overcome the congressional and judicial obstacles that typically stand in his way.2 This affords the president greater discretion in acting unilaterally (Wildavsky 1966). It is possible the institutional make-up of the government will align so that the president will serve in an environment supportive of his policy decisions. It is also likely a president will have persuasive powers that enable him to gain a great deal of support for his policy agenda. An event with the right characteristics, however, enhances the president's ability to act unilaterally, regardless of the institutional make-up of government or his persuasive abilities.

### Link – Nukes

#### US is lowering its nuclear weapons roles as cyber ops capabilities grow

Cimbala 12 (Stephen J. Cimbala 2011. Professor of Political Science at Penn State, “Chasing Its Tail Nuclear Deterrence in the Information Age”, <http://www.au.af.mil/au/ssq/2012/summer/cimbala.pdf>)

Faced with exigent threats, states with cyber capabilities will be tempted to employ them to good efect. For example, imagine a replay of the Cuban missile crisis between a future Russia and the United States, with Rus­ sia having deployed nuclear-capable missiles and/or warheads into South Ossetia. Or, to lip the example, hypothesize a NATO missile defense installation deployed to protect Tbilisi or Kiev, supported by short- and medium-range ballistic missiles as a trip wire. One can expect that cyber operations of the information-technical type (attacking enemy systems and networks) as well as the information-psychological variety (inluenc­ ing public opinion among foreign and domestic audiences, including elites and general publics) will commend themselves to peacetime and crisis political leaders and their military advisors.27

The larger context for cyber operations and nuclear deterrence also in­ volves the possible adoption of minimum deterrence force postures and the deployment of missile defenses by the United States and NATO or perhaps others. Minimum deterrence might appeal to the United States and to Russia under very favorable political conditions, including a re­ think of European and central Eurasian territory as a uniied security community instead of as a ight club. In this regard, the United States and NATO phased adaptive approach to missile defenses offers the choice between cooperative security and Cold War retro approaches to arms con­trol. Regardless the outcome of the imbroglio over EPAA, US plans for a global missile defense system will include technology transfers and secu­ rity cooperation with regional allies in Europe, the Middle East, and Asia. Prospective US opponents in those regions may therefore cultivate both nuclear deterrence and information operations as means for antiaccess and area denial (A2/AD) deterrence and defense.

Nuclear deterrence in the Cold War was something sui generis that grew from a way station for coping with new weapons and new threats into an all-purpose solvent for problems of military strategy. Nuclear weapons remain alive and menacing in the twenty-irst century, but they are presently and prospectively circumscribed by new contexts. One of these contexts is the coexistence of information warfare or military cyber operations and nuclear deterrence.

### 2NC Overview

#### Only KINETIC war escalates

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)

The direct effects of some cyberattacks may be easily reversible. (Reversibility means that the target of the attack is restored to the operating condition that existed prior to the attack.) For example, turning off a denial-of-service attack provides instant reversibility with no effort on the part of the attacked computer or its operators. If backups are available, an attack on the integrity of the operating system may take just a few minutes of reloading the operating system. Many effects of kinetic attacks are not as easy to reverse.34

#### No cyber attack – mutual restraint

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

The absence of major cyber attacks on critical U.S. networks may mean that subtle deterrence is already working. Perhaps China has chosen not to move from computer network exploitation to computer network attack out of fear of U.S. retaliation. In any case, the Chinese evidently have not found themselves in circumstances in which the advantages of disrupting or degrading U.S. strategic networks would outweigh the risks of retaliation, political condemnation, or economic sanction. China and the United States have not had a serious confrontation since President Clinton sent two aircraft carriers into the Taiwan Strait to signal U.S. willingness to defend Taiwan. One can speculate about whether a crisis of that order today would produce a Chinese cyber attack.

### Truncated Decisions Good

#### Truncated decision making k2 solve offensive cyber operations are necessary to deter future attacks – the impact is military and economic strength

Schmitt 6/6/13 (Gary Schmitt co-directs the Marilyn War Center for Security Studies at the American Enterprise Institute, “How to meet the threat from China's army of cyber guerrillas, <http://www.foxnews.com/opinion/2013/06/06/how-to-meet-threat-from-china-army-cyber-guerrillas/#ixzz2bPr59xoZ>)

The reality is, the Chinese government is engaged in a form of warfare—new to be sure in its technological aspects but not new in the sense that cyber attacks harm our relative military strength and damage the property (intellectual and proprietary) of citizens and companies alike.

So far, the American government’s response has largely been defensive, either talking to the Chinese about establishing new, agreed-upon “rules of road” for cyberspace or working assiduously to perfect new security walls to protect government and key private sector computer systems.

Although neither effort should be abandoned, they are no more likely to work than, say, before World War II, the Kellogg-Briand Pact could outlaw war and the Maginot Line could protect France from an invading Germany.

This last point is especially important. When it comes to cyberspace, according to Cyber Command head and director of the National Security Agency, General Keith Alexander, those on the offensive side of the computer screen–that is, those hacking into or compromising computer systems–have the advantage over those on the defensive side who are trying to keep systems secure. Walls have always been breached and codes broken.

Moreover, attempts to beef up security are complicated by the fact that our own cyber warriors are undoubtedly reluctant to provide those charged with protecting systems here at home with the latest in their own capabilities.

In addition to increasing the chance such information might leak by expanding the number of persons in the know, efforts to use that information to plug our own vulnerabilities can inadvertently alert a potential adversary on the very backdoors American would want to save for using in a future crisis or conflict.

All of which leads to the conclusion that to stem the tide of harmful cyber attacks by the Chinese (or, for that matter, Iran, Russia or North Korea), there has to be a cyber response on America’s part that deters continued cyber aggression.

Reprisals that are proportionate, in self-defense and designed to stop others from such behavior falls well within the bounds of international law as traditionally understood.

Nor is it the case that such reprisals should be limited to responding to government-on-government cyber attacks. The U.S. government has always understood that it has an affirmative duty to protect the lives and property of its citizens from foreign aggression and, in times both past and current, this has meant using American military might.

That need not be the case here, however. Indeed, one advantage of the cyber realm is the wide variety of options it offers up for reprisal that can inflict economic harm without causing loss of life or limb.

The good news is that the U.S. government has been gradually beefing up its offensive cyber capabilities.

Indeed, a little over a month ago in open testimony before the House Armed Services Committee, Gen. Alexander said that he created thirteen new teams that would go on the offensive if the nation were hit by a major cyber attack. And new reports coming out of the Pentagon indicate that the Joint Chiefs would like to empower geographic combatant commanders to counter cyber attacks with offensive cyber operations of their own.

These are necessary steps if we hope to create a deterrent to Chinese cyber aggression; however, they are not sufficient.

The threat posed by China’s army of cyber “guerrillas” is constant, is directed at both the U.S. government and the private sector, and ranges from the annoying to the deadly serious.

A truly adequate response would require meeting the Chinese challenge on all these fronts. And no amount of summitry between the American and Chinese leaders is likely to substitute for the cold, hard fact that, when it comes to Chinese misbehavior, upping the cost to Beijing is a necessary first step to reclaiming the peaceful potential of the newest of the “great commons,” cyberspace.

#### Speed key – k2 legit threat we’re impact turning that too.

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

In this light, resorting to cyber war only in response to cyber attack would add legitimacy to the threat and act of retaliation and thus strengthen deterrence. Given its myriad other forms of power and its dependence on vulnerable networks, the United States should favor such a norm. However, networks have become so integral to military operations, for the United States and China alike, that the United States is highly unlikely to foreswear attacks on networks that enable operations of the PLA.

### AT: Stevnson

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

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

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

#### Deterrence is the only stable foundation for the international system—internal link turns self-fulfilling prophesy

Lupovici 08 (Amir, Post-Doctoral Fellow Munk Centre for International Studies, Why the Cold War Practices of Deterrence are Still Prevalent: Physical Security, Ontological Security and Strategic Discourse, [http://www.cpsa-acsp.ca/ papers-2008/Lupovici.pdf](http://www.cpsa-acsp.ca/papers-2008/Lupovici.pdf))

Since **deterrence** can become part of the actors’ identity, it **is** also **involved in the** actors’ **will to achieve ontological security, securing the actors’ identity and routines. As McSweeney explains, ontological security is “the acquisition of confidence in the routines of daily life**—the essential **predictability of interaction through which we feel confident in knowing what is going on** and that we have the practical skill to go on in this context.” **These routines become part of the social structure that enables and constrains the actors’ possibilities** (McSweeney, 1999: 50-1, 154-5; Wendt, 1999: 131, 229-30). Thus, **through** the emergence of the **deterrence** norm and the construction of deterrence identities, the **actors create an intersubjective context and intersubjective understandings that in turn affect their interests and routines**. In this context, **deterrence** strategy and deterrence **practices are better understood by** the actors, and therefore **the** continuous **avoidance of violence** is more easily achieved. Furthermore, within such a context of **deterrence** relations, rationality is (re)defined, clarifying the appropriate practices for a rational actor, and this, in turn, **reproduces** this **context and** the actors’ **identities**. Therefore, the **internalization of deterrence** ideas **helps** to **explain how actors** may **create** more **cooperative practices and break away from the** spiral of **hostility** that is **forced** and maintained **by the** identities that are attached to the **security dilemma, and which lead to mutual perception of the other as an** aggressive **enemy**. As Wendt for example suggests, in situations **where states are restrained from using violence—such as MAD (mutual assured destruction)—states not only avoid violence, but** “ironically, may be **willing** to **trust each other enough to take on collective identity”. In such cases if actors believe that others have no desire to engulf them, then it will be easier to trust them** and to identify with their own needs (Wendt, 1999: 358-9). In this respect, the norm of deterrence, the trust that is being built between the opponents, and the (mutual) constitution of their role identities may all lead to the creation of long term influences that preserve the practices of deterrence as well as the avoidance of violence. Since a basic level of trust is needed to attain ontological security,21 the existence of it may further strengthen the practices of deterrence and the actors’ identities of deterrer and deterred actors. In this respect, I argue that for the reasons mentioned earlier, the practices of deterrence should be understood as providing both physical and ontological security, thus refuting that there is necessarily tension between them. Exactly for this reason I argue that Rasmussen’s (2002: 331-2) assertion—according to which MAD was about enhancing ontological over physical security—is only partly correct. Certainly, **MAD should be understood as providing ontological security; but it also allowed for physical security, since,** compared to previous strategies and doctrines, **it was all about decreasing the physical threat of nuclear weapons**. Furthermore, **the ability to increase** one dimension of **security** helped to enhance the other, since it **strengthened the actors’ identities and created more stable expectations of avoiding violence**.

#### Other states have the capability and a convergence of factors make use inevitable

Denmark et al. 10 (Abraham M. Denmark is a Fellow at the Center for a New American Security.¶ Chris Evans is a Senior Consultant at Delta Risk Consulting.¶ Robert D. Kaplan, a National Correspondent for The Atlantic and a Senior Fellow at the Center for a¶ New American Security, is writing a book on the Indian Ocean.¶ Jason Healey is the Washington D.C. Office Director for Delta Risk Consulting.¶ Frank Hoffman wrote his chapter when he was a Fellow at the Foreign Policy Research Institute and¶ the Potomac Institute for Policy Studies. He now works for the Department of the Navy.¶ Oliver Fritz is the Assistant Director of Strategic Planning at Headquarters, U.S. Air Force.¶ Lt Col Kelly Martin (USAF) is a Senior Military Fellow at the Center for a New American Security.¶ Dr. James Mulvenon is Vice-President of Defense Group Inc.’s Intelligence Division and Director¶ of DGI’s Center for Intelligence Research and Analysis.¶ Dr. Greg Rattray is a Partner at Delta Risk Consulting, is Chief Internet Security Advisor at the Internet¶ Corporation for Assigned Names and Numbers (ICANN), and is a member of the Cyber Conflict Studies¶ Association Board.¶ Eric Sterner is a Fellow at the George C. Marshall Institute., “Contested Commons:¶ The Future of American Power¶ in a Multipolar World”, pdf)

The cyber commons today is a complex and anarchic environment lacking effective international¶ agreements. Currently state and non-state actors¶ are able to hack, intrude, corrupt and destroy data¶ with relative impunity. While economic and technological necessity have allowed for the creation¶ of standards and protocols to enable consistent¶ communication, security in the cyber commons¶ is often self-provided by users rather than by a¶ central authority.

At the same time, the increasing use of the Internet¶ and other aspects of the cyber commons by¶ advanced states to manage domestic infrastructure¶ creates new strategic vulnerabilities that adversaries cannot ignore. For example, sustained power¶ outages or catastrophic breakdowns in transportation systems could result in significant physical¶ damage and casualties, not to mention severely¶ disrupting crucial economic, military and social¶ activities. More disturbingly, attacks against these¶ systems are technologically feasible. 23

The distributed and interactive nature of cyberspace, combined with the low cost of computing¶ devices, has lowered the threshold for actors to¶ operate with great effect in cyberspace. Actors¶ do not necessarily have to build complex weapons systems, like the Joint Strike Fighter, in order¶ to leverage the benefits of cyberspace. Instead,¶ accessibility and anonymity have created an¶ environment in which smaller organizations and¶ political actors, especially those who seek to hide¶ from retribution in other environments, can¶ achieve a disproportional increase in capabilities¶ to conduct their operations and disrupt those of¶ adversaries. The ease of achieving anonymity on¶ the Internet also facilitates the rapid orchestration¶ of operations across wide geographic areas with¶ less chance of tipping off adversaries that disruptive attacks are imminent. The Madrid bombers,¶ for example, reportedly used “a program downloaded from the Internet by which text messages¶ could activate mobile phones simultaneously” to¶ set off multiple explosions. 24 A 2005 Washington¶ Post article noted that al Qaeda “has become the¶ first guerrilla movement in history to migrate from¶ physical space to cyberspace.” 25

Cyberspace has changed the dynamic of political¶ and military competition, as states may be able to¶ compete aggressively in cyberspace while still being¶ deficient in other measurements of national power.¶ Weak adversaries can use cyberspace to exploit¶ vulnerabilities of their more powerful adversaries and, for instance, steal intellectual property¶ from advanced states. Just as the expansion of¶ global maritime trade required the development of¶ colonies, naval fleets and their supporting infrastructures, cyberspace will require political and¶ military measures to protect economic and informational interests. The United States will have to¶ learn how to protect its cyberspace presence in a¶ cost-effective fashion.

Indeed, using the cyber commons to achieve rapid¶ strategic impact has become a tool for non-state¶ actors. Organized criminal activity, Internet posting of terrorist videos of beheadings and malicious¶ disruption on a global scale can all spread rapidly. 26 Cyberspace has multiplied opportunities¶ for small groups to achieve large effects by getting¶ their message to a global audience. This increases¶ their geographic base for acquiring resources,¶ whether through voluntary contributions or illicit activity. In the future, these groups will use¶ cyberspace as a place where guerilla campaigns,¶ orchestrated dispersal and surreptitious disruption¶ can occur. The challenge for the United States is to¶ create a recognizable signature in cyberspace that¶ renders such nefarious groups vulnerable to retaliation and future deterrence.

Cyberspace offers opportunities for disrupting¶ and crippling even the largest state opponents¶ through new methods of attack. The disruptive¶ attacks against U.S. and South Korean government¶ and economic sites in early July 2009 illustrate¶ this. While the actors behind the attack remain¶ unknown, it is known that they utilized a botnet of tens of thousands of computers based on¶ a long-known vulnerability to network security¶ protocols. 27

Although the major threat to the openness of¶ the global commons stems from its anarchic and¶ decentralized nature, several state and non-state¶ actors are developing the capability to challenge¶ U.S. and international access to the cyberspace.

Russia • reportedly has developed a robust ability¶ to deny its adversaries access to cyberspace. 28 In¶ April 2007, during an imbroglio surrounding the¶ removal of a Soviet-era monument, the websites¶ of the Estonian Parliament, ministries, media¶ outlets, and banks were attacked and defaced.¶ While the Estonian government immediately¶ blamed Russia for the attack, they could not¶ definitively link it to Moscow. 29 Georgia faced¶ similar attacks during its war with Russia over¶ South Ossetia in 2008. 30

China • reportedly has developed several types¶ of computer network operations. According to¶ a Pentagon report, China’s military has “established information warfare units to develop¶ viruses to attack enemy computer systems and¶ networks, and tactics and measures to protect¶ friendly computer systems and networks.” 31¶ Indeed, according to the Pentagon, China’s¶ military has integrated these sorts of strikes into¶ its exercises, using them as first strikes against¶ enemy networks.

Al Qaeda • apparently has developed plans to¶ target key businesses, government agencies,¶ financial markets and civil infrastructure¶ using cyberspace. 32

### AT: Pan

#### We’re not essentializing, there is no one nature to china, but in the context of cyber space the lack of LOAC doctrine makes escalation uniquely likely – there are divides in leadership etc. our arg is super nuanced.

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

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

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

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

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

U.S. Experience with the LOAC

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

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

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

The Tallinn Manual and Emerging Cyber Norms

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

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

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

#### Our depictions of China are accurate

Blumenthal et al 11 ( Dan Blumenthal is a current commissioner and former vice chairman of the U.S.-China Economic and Security Review Commission, where he directs efforts to monitor, investigate, and provide recommendations on the national security implications of the economic relationship between the two countries. “Avoiding Armageddon with China” http://shadow.foreignpolicy.com/posts/2011/09/06/avoiding\_armageddon\_with\_china?wpisrc=obinsite)

The balancing and hedging strategy should involve options to avoid what Traub rightfully describes as "Armageddon." We call for a myriad of conventional options short of striking the nuclear-armed PRC, in the hope that such a strategy enhances deterrence in the first place and avoids Armageddon should deterrence fail. The strategy aims to slow escalation rather than quicken it. The idea of a self-fulfilling prophecy -- of turning China into an enemy by treating it as one -- is like a unicorn; it is a make believe creature that still has its believers. The United States has done more than any other country to "turn China into a friend" by welcoming it into the international community. Alas, China has not fulfilled this U.S. "prophesy of friendship." Instead China has built what all credible observers call a destabilizing military that has changed the status quo by holding a gun to Taiwan's head even as Taiwan makes bold attempts at peace, by claiming ever more territory in the South China Sea, and by attempting to bully and intimidate Japan. Traub asks whether our allies and partners will be willing to participate in an "anti-Chinese coalition," as he describes it. As the paper says, all allies, partners, and potential partners are already modernizing their militaries in response to China. And they will continue to do so regardless of whether the U.S. pursues what Traub would see as an "anti-China" strategy. Even laid-back Australia has plans to double its submarine fleet -- it is not doing so to defend against Fiji. The paper argues that it is time for the United States to offer more serious assistance so that matters do not get out of hand. A strong U.S. presence and commitment to the region's security can help avoid a regional nuclear arms race, for example. The United States can be a force multiplier by providing the intelligence, surveillance, and reconnaissance that only Washington possesses, and by training, and equipping our allies and friends. This strategy is one way of beginning to put Asia back in balance as China changes the status quo. Not doing so, we fear, would lead to Armageddon.

### AT: Deterrence will fail

#### Doesn’t matter

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

Of course, deterrence might fail, a large attack might occur, and the United States might be unable to identify the attacker with enough confidence to retaliate. In that case, deterrence might be weakened for the future. But this is no reason for the United States to forego the advantages of deterrence against a Chinese (or other) strategic cyber attack. The same reasoning can be applied to the Chinese as they consider how to restrain the United States from such attacks on China.

6–5 depicts notionally why deterrence may work even with a lack of certainty about the identity of an attacker. As the likelihood of attri-bution increases, the side attacked (“retaliator”) grows increasingly confident of retaliating against the actual attacker. Meanwhile, the attacker loses confidence that it will not be identified and thus escape retaliation. The attacker does not know for certain how likely it is to be identified or how confident the attacked side must be before deciding to retaliate. Assuming that retaliation would be extremely punishing—outweighing the gains of attacking—the attacker is unlikely to depend on not being identified or the attacked side will retaliate only if absolutely sure of the attacker’s identity.

### 2NC Other Speed Bad

#### Unconstrained speed is key

LI 09 J.D. candidate, Georgetown University Law Center [Zheyao Li, “War Powers for the Fourth Generation: Constitutional Interpretation in the Age of Asymmetric Warfare,” 7 Geo. J.L. & Pub. Pol'y 373 2009 WAR POWERS IN THE FOURTH GENERATION OF WARFARE]

A. The Emergence of Non-State Actors

Even as the quantity of nation-states in the world has increased dramatically since the end of World War II, the institution of the nation-state has been in decline over the past few decades. Much of this decline is the direct result of the waning of major interstate war, which primarily resulted from the introduction of nuclear weapons.122 The proliferation of nuclear weapons, and their immense capacity for absolute destruction, has ensured that conventional wars remain limited in scope and duration. Hence, "both the size of the armed forces and the quantity of weapons at their disposal has declined quite sharply" since 1945.123 At the same time, concurrent with the decline of the nation-state in the second half of the twentieth century, non-state actors have increasingly been willing and able to use force to advance their causes. In contrast to nation-states, who adhere to the Clausewitzian distinction between the ends of policy and the means of war to achieve those ends, non-state actors do not necessarily fight as a mere means of advancing any coherent policy. Rather, they see their fight as a life-and-death struggle, wherein the ordinary terminology of war as an instrument of policy breaks down because of this blending of means and ends.124 It is the existential nature of this struggle and the disappearance of the Clausewitzian distinction between war and policy that has given rise to a new generation of warfare. The concept of fourth-generational warfare was first articulated in an influential article in the Marine Corps Gazette in 1989, which has proven highly prescient. In describing what they saw as the modem trend toward a new phase of warfighting, the authors argued that: In broad terms, fourth generation warfare seems likely to be widely dispersed and largely undefined; the distinction between war and peace will be blurred to the vanishing point. It will be nonlinear, possibly to the point of having no definable battlefields or fronts. The distinction between "civilian" and "military" may disappear. Actions will occur concurrently throughout all participants' depth, including their society as a cultural, not just a physical, entity. Major military facilities, such as airfields, fixed communications sites, and large headquarters will become rarities because of their vulnerability; the same may be true of civilian equivalents, such as seats of government, power plants, and industrial sites (including knowledge as well as manufacturing industries). 125 It is precisely this blurring of peace and war and the demise of traditionally definable battlefields that provides the impetus for the formulation of a new. theory of war powers. As evidenced by Part M, supra, the constitutional allocation of war powers, and the Framers' commitment of the war power to two co-equal branches, was not designed to cope with the current international system, one that is characterized by the persistent machinations of international terrorist organizations, the rise of multilateral alliances, the emergence of rogue states, and the potentially wide proliferation of easily deployable weapons of mass destruction, nuclear and otherwise. ///////MARKED AT/////////

B. The Framers' World vs. Today's World The Framers crafted the Constitution, and the people ratified it, in a time when everyone understood that the state controlled both the raising of armies and their use. Today, however, the threat of terrorism is bringing an end to the era of the nation-state's legal monopoly on violence, and the kind of war that existed before-based on a clear division between government, armed forces, and the people-is on the decline. 126 As states are caught between their decreasing ability to fight each other due to the existence of nuclear weapons and the increasing threat from non-state actors, it is clear that the Westphalian system of nation-states that informed the Framers' allocation of war powers is no longer the order of the day. 127 As seen in Part III, supra, the rise of the modem nation-state occurred as a result of its military effectiveness and ability to defend its citizens. If nation-states such as the United States are unable to adapt to the changing circumstances of fourth-generational warfare-that is, if they are unable to adequately defend against low-intensity conflict conducted by non-state actors-"then clearly [the modem state] does not have a future in front of it.' 128 The challenge in formulating a new theory of war powers for fourthgenerational warfare that remains legally justifiable lies in the difficulty of adapting to changed circumstances while remaining faithful to the constitutional text and the original meaning. 29 To that end, it is crucial to remember that the Framers crafted the Constitution in the context of the Westphalian system of nation-states. The three centuries following the Peace of Westphalia of 1648 witnessed an international system characterized by wars, which, "through the efforts of governments, assumed a more regular, interconnected character."' 130 That period saw the rise of an independent military class and the stabilization of military institutions. Consequently, "warfare became more regular, better organized, and more attuned to the purpose of war-that is, to its political objective."' 1 3' That era is now over. Today, the stability of the long-existing Westphalian international order has been greatly eroded in recent years with the advent of international terrorist organizations, which care nothing for the traditional norms of the laws of war. This new global environment exposes the limitations inherent in the interpretational methods of originalism and textualism and necessitates the adoption of a new method of constitutional interpretation. While one must always be aware of the text of the Constitution and the original understanding of that text, that very awareness identifies the extent to which fourth-generational warfare epitomizes a phenomenon unforeseen by the Framers, a problem the constitutional resolution of which must rely on the good judgment of the present generation. 13 Now, to adapt the constitutional warmarking scheme to the new international order characterized by fourth-generational warfare, one must understand the threat it is being adapted to confront. C. The Jihadist Threat The erosion of the Westphalian and Clausewitzian model of warfare and the blurring of the distinction between the means of warfare and the ends of policy, which is one characteristic of fourth-generational warfare, apply to al-Qaeda and other adherents of jihadist ideology who view the United States as an enemy. An excellent analysis of jihadist ideology and its implications for the rest of the world are presented by Professor Mary Habeck. 133 Professor Habeck identifies the centrality of the Qur'an, specifically a particular reading of the Qur'an and hadith (traditions about the life of Muhammad), to the jihadist terrorists. 134 The jihadis believe that the scope of the Qur'an is universal, and "that their interpretation of Islam is also intended for the entire world, which must be brought to recognize this fact peacefully if possible and through violence if not."' 135 Along these lines, the jihadis view the United States and her allies as among the greatest enemies of Islam: they believe "that every element of modern Western liberalism is flawed, wrong, and evil" because the basis of liberalism is secularism. 136 The jihadis emphasize the superiority of Islam to all other religions, and they believe that "God does not want differing belief systems to coexist."' 37 For this reason, jihadist groups such as al-Qaeda "recognize that the West will not submit without a fight and believe in fact that the Christians, Jews, and liberals have united against Islam in a war that will end in the complete destruction of the unbelievers.' 138 Thus, the adherents of this jihadist ideology, be it al-Qaeda or other groups, will continue to target the United States until she is destroyed. Their ideology demands it. 139 To effectively combat terrorist groups such as al-Qaeda, it is necessary to understand not only how they think, but also how they operate. Al-Qaeda is a transnational organization capable of simultaneously managing multiple operations all over the world."14 It is both centralized and decentralized: al-Qaeda is centralized in the sense that Osama bin Laden is the unquestioned leader, but it is decentralized in that its operations are carried out locally, by distinct cells."4 AI-Qaeda benefits immensely from this arrangement because it can exercise direct control over high-probability operations, while maintaining a distance from low-probability attacks, only taking the credit for those that succeed. The local terrorist cells benefit by gaining access to al-Qaeda's "worldwide network of assets, people, and expertise."' 42 Post-September 11 events have highlighted al-Qaeda's resilience. Even as the United States and her allies fought back, inflicting heavy casualties on al-Qaeda in Afghanistan and destroying dozens of cells worldwide, "al-Qaeda's networked nature allowed it to absorb the damage and remain a threat." 14 3 This is a far cry from earlier generations of warfare, where the decimation of the enemy's military forces would generally bring an end to the conflict. D. The Need for Rapid Reaction and Expanded Presidential War Power By now it should be clear just how different this conflict against the extremist terrorists is from the type of warfare that occupied the minds of the Framers at the time of the Founding. Rather than maintaining the geographical and political isolation desired by the Framers for the new country, today's United States is an international power targeted by individuals and groups that will not rest until seeing her demise. The Global War on Terrorism is not truly a war within the Framers' eighteenth-century conception of the term, and the normal constitutional provisions regulating the division of war powers between Congress and the President do not apply. Instead, this "war" is a struggle for surviva and dominance against forces that threaten to destroy the United States and her allies, and the fourth-generational nature of the conflict, highlighted by an indiscernible distinction between wartime and peacetime, necessitates an evolution of America's traditional constitutional warmaking scheme. As first illustrated by the military strategist Colonel John Boyd, constitutional decision-making in the realm of war powers in the fourth generation should consider the implications of the OODA Loop: Observe, Orient, Decide, and Act. 44 In the era of fourth-generational warfare, quick reactions, proceeding through the OODA Loop rapidly, and disrupting the enemy's OODA loop are the keys to victory. "In order to win," Colonel Boyd suggested, "we should operate at a faster tempo or rhythm than our adversaries." 145 In the words of Professor Creveld, "[b]oth organizationally and in terms of the equipment at their disposal, the armed forces of the world will have to adjust themselves to this situation by changing their doctrine, doing away with much of their heavy equipment and becoming more like police."1 46 Unfortunately, the existing constitutional understanding, which diffuses war power between two branches of government, necessarily (by the Framers' design) slows down decision- making. In circumstances where war is undesirable (which is, admittedly, most of the time, especially against other nation-states), the deliberativeness of the existing decision-making process is a positive attribute. In America's current situation, however, in the midst of the conflict with al-Qaeda and other international terrorist organizations, the existing process of constitutional decision-making in warfare may prove a fatal hindrance to achieving the initiative necessary for victory. As a slow-acting, deliberative body, Congress does not have the ability to adequately deal with fast-emerging situations in fourth-generational warfare. Thus, in order to combat transnational threats such as al-Qaeda, the executive branch must have the ability to operate by taking offensive military action even without congressional authorization, because only the executive branch is capable of the swift decision-making and action necessary to prevail in fourth-generational conflicts against fourthgenerational opponents.

### AT: It’ll Escalate

#### China would get crushed

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

The Chinese should be aware that U.S. cyber attacks on increasingly important and exposed Chinese C4 ISR networks could derail their strategy, such as by damaging their ability to track, target, and attack U.S. carriers near, en route to, or at standoff range from China. Before long, U.S. cyber attacks could be as devastating to Chinese operations as Chinese cyber attacks could be to U.S. operations. A paradox—and potential trap—awaits Chinese military strategy: the more prepared PLA forces are to carry out informationized operations, the more vulnerable the PLA is to U.S. cyber war. In the context of Sino-U.S. conventional war, cyber war could leave China no better off and possibly worse off. Instead of complementing China’s growing antiaccess capabilities, cyber war could undermine their effectiveness. While this scenario depends on a number of assumptions about the cyber war capabilities and vulnerabilities of both sides, the Chinese have to consider it.

### AT: Accident

#### No launch on warning

Ford ‘8 (Senior Fellow and Director of the Center for Technology and Global Security at the Hudson Institute, and formerly U.S. Special Representative for Nuclear Nonproliferation, and Principal Deputy Assistant Secretary of State, Christopher, “Dilemmas of Nuclear Force “De-Alerting”” 10/7, http://www.hudson.org/files/documents/De-Alerting%20FINAL2%20%282%29.pdf)

• It is *not* true that current forces are bound to destabilizing “hair-trigger” launch assumptions, though for deterrent purposes U.S. and Russian forces likely both go to considerable trouble to maintain the *option* of launching at least *some* forces immediately. Rather, nuclear force postures aim to provide national leaders with as much information and decision-making time – and therefore flexibility – as possible in all circumstances. This includes also trying to ensure the option of riding out an attack while retaining a credible second-strike retaliatory force, which is quite the *opposite* of a launch-on-warning posture.

### AT: Futurism bad

#### Debates about future crises are critical to social movements that pressure governments to address existential risks

Fuyuki **Kurasawa**, December **2004**. Professor of Sociology, York University of Toronto. “Cautionary Tales: The Global Culture of Prevention and the Work of Foresight,” Constellations 11.4, Ebsco.

In the twenty-first century, the lines of political cleavage are being drawn along those of competing dystopian visions. Indeed, one of the notable features of recent public discourse and socio-political struggle is their negationist hue, for they are devoted as much to the prevention of disaster as to the realization of the good, less to what ought to be than what could but must not be. The debates that preceded the war in Iraq provide a vivid illustration of this tendency, as both camps rhetorically invoked incommensurable catastrophic scenarios to make their respective cases. And as many analysts have noted, the multinational antiwar protests culminating on February 15, 2003 marked the first time that a mass movement was able to mobilize substantial numbers of people dedicated to averting war before it had actually broken out. More generally, given past experiences and awareness of what might occur in the future, given the cries of ‘never again’ (the Second World War, the Holocaust, Bhopal, Rwanda, etc.) and ‘not ever’ (e.g., nuclear or ecological apocalypse, human cloning) that are emanating from different parts of the world, the avoidance of crises is seemingly on everyone’s lips – and everyone’s conscience. From the United Nations and regional multilateral organizations to states, from non-governmental organizations to transnational social movements, the determination to prevent the actualization of potential cataclysms has become a new imperative in world affairs. Allowing past disasters to reoccur and unprecedented calamities to unfold is now widely seen as unbearable when, in the process, the suffering of future generations is callously tolerated and our survival is being irresponsibly jeopardized. Hence, we need to pay attention to what a widely circulated report by the International Commission on Intervention and State Sovereignty identifies as a burgeoning “culture of prevention,”3 a dynamic that carries major, albeit still poorly understood, normative and political implications. Rather than bemoaning the contemporary preeminence of a dystopian imaginary, I am claiming that it can enable a novel form of transnational socio-political action, a manifestation of globalization from below that can be termed preventive foresight. We should not reduce the latter to a formal principle regulating international relations or an ensemble of policy prescriptions for official players on the world stage, since it is, just as significantly, a mode of ethico-political practice enacted by participants in the emerging realm of global civil society. In other words, what I want to underscore is the work of farsightedness, the social processes through which civic associations are simultaneously constituting and putting into practice a sense of responsibility for the future by attempting to prevent global catastrophes. Although the labor of preventive foresight takes place in varying political and socio-cultural settings – and with different degrees of institutional support and access to symbolic and material resources – it is underpinned by three distinctive features: dialogism, publicity, and transnationalism. In the first instance, preventive foresight is an intersubjective or dialogical process of address, recognition, and response between two parties in global civil society: the ‘warners,’ who anticipate and send out word of possible perils, and the audiences being warned, those who heed their interlocutors’ messages by demanding that governments and/or international organizations take measures to steer away from disaster. Secondly, the work of farsightedness derives its effectiveness and legitimacy from public debate

////////////MARKED AT ////////////////

and deliberation. This is not to say that a fully fledged global public sphere is already in existence, since transnational “strong publics” with decisional power in the formal-institutional realm are currently embryonic at best. Rather, in this context, publicity signifies that “weak publics” with distinct yet occasionally overlapping constituencies are coalescing around struggles to avoid specific global catastrophes.4 Hence, despite having little direct decision-making capacity, the environmental and peace movements, humanitarian NGOs, and other similar globally-oriented civic associations are becoming significant actors involved in public opinion formation. Groups like these are active in disseminating information and alerting citizens about looming catastrophes, lobbying states and multilateral organizations from the ‘inside’ and pressuring them from the ‘outside,’ as well as fostering public participation in debates about the future. This brings us to the transnational character of preventive foresight, which is most explicit in the now commonplace observation that we live in an interdependent world because of the globalization of the perils that humankind faces (nuclear annihilation, global warming, terrorism, genocide, AIDS and SARS epidemics, and so on); individuals and groups from far-flung parts of the planet are being brought together into “risk communities” that transcend geographical borders.5 Moreover, due to dense media and information flows, knowledge of impeding catastrophes can instantaneously reach the four corners of the earth – sometimes well before individuals in one place experience the actual consequences of a crisis originating in another. My contention is that civic associations are engaging in dialogical, public, and transnational forms of ethico-political action that contribute to the creation of a fledgling global civil society existing ‘below’ the official and institutionalized architecture of international relations. The work of preventive foresight consists of forging ties between citizens; participating in the circulation of flows of claims, images, and information across borders; promoting an ethos of farsighted cosmopolitanism; and forming and mobilizing weak publics that debate and struggle against possible catastrophes. Over the past few decades, states and international organizations have frequently been content to follow the lead of globally- minded civil society actors, who have been instrumental in placing on the public agenda a host of pivotal issues (such as nuclear war, ecological pollution, species extinction, genetic engineering, and mass human rights violations).

# 1NR

**Judicial means a decision by a court**

WEST’S LAW 08 [West's Encyclopedia of American Law, edition 2. <http://legal-dictionary.thefreedictionary.com/judicial>]

Relating to the courts or belonging to the office of a judge; a term pertaining to the administration of justice, the courts, or a judge, as in judicial power.

A judicial act involves an exercise of discretion or an unbiased decision by a court or judge, as opposed to a ministerial, clerical, or routine procedure. A judicial act affects the rights of the parties or property brought before the court. It is the interpretation and application of the law to a particular set of facts contested by litigants in a court of law, resulting from discretion and based upon an evaluation of the evidence presented at a hearing.

Judicial connotes the power to punish, sentence, and resolve conflicts.

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

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.

**Their strategy of opening up to radical uncertainty goes too far in decentering provisional communal identities necessary for politics in a world of speed---minimal guidelines don’t stifle becoming or entrench predictability---they are necessary to help pluralism flourish**

David McIvor 10, research associate at the Kettering Foundation, The Politics of Speed: Connolly, Wolin, and the Prospects for Democratic Citizenship in an Accelerated Polity, Polity (2011) 43, 58–83

So, what is the point? Connolly does not describe or define it in this essay. However, judging by the rest of Connolly's work, we might say that the point is akin to the “moment” in Nietzsche's description of the rift in time,57 or Arendt's “present” in her re-telling of Kafka's parable in Between Past and Future.58 The “point” is the conjunctive of a fraught struggle between the forces of fundamentalization and pluralization; it is the joint or center of a “tense balance” between “the claims of regularity, predictability, and commonality” and “those of experimentalism, artistry, and becoming.”59 Speed becomes dangerous, then, when it tilts us against ethico-political interventions on behalf of individual and collective plurality. When the world moves so fast that we cannot resist nostalgia or overcome ressentiment, we are past this “point,” and will henceforth require more intense micro-political efforts to recalibrate our attentiveness to becoming and flux.

Yet there is another and perhaps a more damning way in which Connolly might be missing the point. As quoted above, Connolly finds that those who “recoil from speed” are nostalgic for a slower temporality and find themselves supporting frozen hierarchies in the pursuit of a predictable, slow world. Yet it is also possible to level similar charges against Connolly himself: those who recoil from slow time may align themselves with a tendency in late-modern capitalism that tears asunder the possibilities of democratic negotiations born from attachment to place, vocation, and familiar others.60 This goes well beyond the decline of social capital and the chilling specter of the lone bowler. It is by now well known that rapid vocational mobility leads to lower rates of political and civic participation.61 Yet these declines are themselves part of a growing skepticism towards public institutions as such, a trend that feeds demand for exclusive and positional goods and further entrenches class-based inequalities.62 Moreover, Sheldon Wolin's worry about the normalization of incessant change is that increasing restraints on personal freedom and public life will be accepted by a society habituated to adaptation (“becoming”?). Connolly's recoil from the normalizing pressures of democratic collective identity may perversely support what Wolin calls the “triumph of contemporaneity and of its accomplice, forgetting or collective amnesia.”63 The sobering implication is not only that democratic practices and habits will desiccate, but that their loss will not be recognized or mourned.

Connolly's recoil from collective identity also keeps him from fully appreciating the implications of his calls for “self-experimentation” on “virtual registers” via “fugitive experiences of unconscious performance.”64 Connolly provides two examples of this virtual register: a “violinist who escapes … the slowness of consciousness by getting lost in the imperatives of performance” and a “point guard clearing his mind of clutter as he dribbles down the middle of the court so the ball can be delivered to a shooter at the right instant with exactly the right bounce in a movement too fast and precise to be entrusted to the slow time of consciousness.”64 However, while these rapid maneuvers may take place in “fast time,” they are absolutely dependent on extensive training and practice (i.e. slow time). Maybe Dylan had it right: “the slow one now will later be fast.” Connolly acknowledges this fact but does not seem to recognize how it compromises (or at the very least complicates) his larger argument about speed and democracy.65 Again, recent work on flexible capitalism has shown that “success” in late-modernity (i.e. economic advancement) is negatively correlated with attachment to one's company, locality, or craft.66 Yet this same work has shown that success within these parameters leaves individuals less capable of accepting ambiguity and generously relating to others—the very foundations of Connolly's normative model for agonistic citizenship.67 This in turn feeds the demand for positional and exclusive goods as consumers prefer flexible accommodations and products to the arduous labors of collective negotiation and public action.

Perhaps, then, we are already past the point when social acceleration yielded beneficent consequences for democratic politics. It seems that theorists who care about the prospects of democracy in late-modernity must insist that certain habits are important enough to be cultivated and practiced in slow time. For just as it takes training to become a violinist or point guard, so, too, is training required to become a citizen of a complex, multilayered, and temporally desynchronized polity. Connolly downplays the possibility that slow time practices and habits may in fact serve pluralization; in the process he has overestimated the salutary impact of speed and obscured the difficulties of negotiating these accelerated tempos without a foot (or more) in slow time. While Connolly accuses Wolin and other “self-proclaimed democrats” of “freezing actors into stone,” his work threatens to leave us endlessly spinning and dancing like a toy top: moving fast but going nowhere.

Wolin: Democratic Citizenship as a Fugitive Experience

A society … caught in the frenzy of rapid change has difficulty knowing how to think about the consequences of loss, especially of things widely shared … rapid change not only blunts the collective conscience but dims the collective memory.

—Sheldon Wolin, Democracy Incorporated

Connolly argues that we should embrace speed for the work it does on our cultural/political selves. Sheldon Wolin, on the other hand, has argued that to adopt the accelerated rhythms of culture and economy would be to accept an anti-political ethos inherent to those systems, and turn democratic praxis into largely irrelevant shadow boxing.68 The dispute over speed and democracy, however, conceals another (more fundamental) disagreement between Connolly and Wolin. Unlike Connolly and Shapiro, who posit an ontological and political tendency towards settled identity, which then aggressively protects itself against the threat of its own denied difference, Wolin argues that commonality is “fugitive and impermanent.”69 For Connolly, political identities are always occupied territories, which are justly subject to disruption. For Wolin, it is difference that is stable, and democracy is concerned not with the disturbance but the discovery of “artificial” commonality. Political identities are fleeting phenomena, and similarity is not (only) a violent imposition on becoming but a pre-condition for democratic power and justice.70 Put slightly differently, if Connolly's philosophy seems unconsciously indebted to Freud's pleasure principle, then Wolin's unstated political ontology more closely resembles the death drive.

Democratic power, then, is fugitive, but it is still possible for ephemeral moments of collective action to protest the limits of the institutional order and reveal possibilities for new modes of political practice and being. This action takes place despite intransigent heterogeneity—different constituencies valuing different outcomes at different times through different means. Fugitive democracy (“the carrier of commonality”) is the temporary suspension of this heterogeneity in the interests of collective power.71 These exceptional points in time—Wolin identifies the early months of the Free Speech Movement at Berkeley as paradigmatic—disrupt a managed system of elite rule on behalf of widely-shared grievances.72 Whereas Connolly values democratic theory and praxis insofar as they disrupt and pluralize homogenous and hegemonic conceptions of time, culture, and place, Wolin values a “discordant” democracy that “affirms the value of limits.”73 Wolin certainly locates discourses of political identity in desperate need of disturbance—specifically those that emphasize an a-political model of “managed democracy” and a de-mobilized citizenry content with the pursuit of commodious living in a glaringly inegalitarian polity.74 His anxiety about postmodern discourses of disturbance is that they align with a certain tendency within “inverted totalitarianism” that thrives on a perpetually mobile—yet never mobilized—populace. Wolin therefore dismisses the “flashy but empty” discordance of “latter-day Nietzscheans” because it affirms pure becoming rather than a space of appearances in which common problems can find redress through the concerted efforts of ordinary men and women.75

Democratic citizenship, on the other hand, is a “discordant” but limit-affirming experience that compels individuals to identify and address problems they share in common with others. As Wolin puts it, “being a citizen involves doing the best one can to take part in common tasks, the deliberations that define them, and the responsibilities that follow. As a way of existence it lives in the ebb-and-flow of everyday activities, responsibilities, and relationships.”76 Wolin refers to the experience of membership in a democratic assemblage as “incorporation,” which suggests that one becomes “an integral part of some stable grouping and accept(s) it as the principle identity of individuals and the primary object of their loyalty.”77 However, it is crucial to note that Wolin's model of incorporation does not imply the elimination of differences within the body politic. Some differences may be bracketed in the interests of collective power, but Wolin does not imagine that these differences will thereby fail to matter or exist. For him, citizenship practices are the means by which we come into contact with different viewpoints, preferences, and lifestyles. The model here is less that of Rousseau's general will than a will to generality, an aspiration of “commonality amid difference.”77