**FW: 1NC**

**Our interpretation is that the affirmative must defend the hypothetical enactment of a topical plan by the United States federal government.**

The USFG is the government in Washington, DC – that’s US Gov

Resolved expresses intent to implement the plan – that’s Merriam Webster

Should denotes expectation of implementation – that’s American Heritage

**A. Interpretation: the affirmative must defend the hypothetical enactment of a topical plan by the United States federal government.**

**The United States federal government is the actor defined by the resolution, not individual debaters**

**US Gov** Official Website 20**09**

http://www.usa.gov/Agencies/federal.shtml

U.S. Federal Government **The three branches of U.S. government—legislative, judicial, and executive—carry out governmental power and functions.** View a complete diagram (.PDF) of the U.S. government's branches.

**“Resolved” expresses intent to implement the plan**

**Merriam-Webster Dictionary** 19**96** [http://dictionary.reference.com/search?q=resolved, downloaded 07/20/03]

“6. **To change or convert by resolution or formal vote**; -- **used only reflexively; as, the house resolved itself into a committee of the whole**.”

**“Should” denotes an expectation of enacting a plan**

**American Heritage Dictionary 2K**

[www.dictionary.com]

3 **Used to express** probability or **expectation**

**B. Violation—the affirmative does not defend the implementation of a topical plan.**

**C. Vote negative**

**Limits—their interpretation kills limits because it creates a strategic incentive to disregard the resolution. If teams can get away with being non-topical, there’s no reason to defend the resolution. Limits are good:**

**A. Critical thinking—having a limited topic with equitable ground is necessary to foster decision-making and clash**

Steinberg & Freeley 8 \*Austin J. Freeley is a Boston based attorney who focuses on criminal, personal injury and civil rights law, AND \*\*David L. Steinberg , Lecturer of Communication Studies @ U Miami, **Argumentation and** Debate: Critical Thinking for Reasoned Decision Making pp 45-

**Debate is a means of settling differences, so there must be a** difference of opinion or a **conflict of interest before there can be a debate. If everyone is in agreement** on a tact or value or policy, **there is no need for debate:** the matter can be settled by unanimous consent. Thus, for example, **it would be pointless to attempt to debate "Resolved: That two plus two equals four,"** because there is simply no controversy about this statement. (**Controversy is an essential prerequisite** of debate. **Where there is no clash of ideas, proposals, interests, or expressed positions on issues, there is no debate. In addition, debate cannot produce effective decisions without clear identification of a question or questions to be answered.** For example**, general argument may occur about the broad topic of illegal immigration. How many** illegal immigrants **are in the United States?** What is the impact of illegal immigration and immigrants on our economy? What is their impact on our communities? Do they commit crimes? **Do they take jobs** from American workers? Do they pay taxes? Do they require social services? Is it a problem that some do not speak English? **Is it the responsibility of employers to discourage illegal immigration** by not hiring undocumented workers? Should they have the opportunity- to gain citizenship? Docs illegal immigration pose a security threat to our country? **Do illegal immigrants do work that American workers are unwilling to do?** Are their rights as workers and as human beings at risk due to their status? Are they abused by employers, law enforcement, housing, and businesses? I low are their families impacted by their status? What is the moral and philosophical obligation of a nation state to maintain its borders? **Should we build a wall on the Mexican border**, establish a national identification can!, or enforce existing laws against employers? Should we invite immigrants to become U.S. citizens? **Surely you can think of many more concerns to be addressed by a conversation about the topic area of illegal immigration. Participation in this "debate" is likely to be emotional and intense. However, it is not likely to be productive or useful without focus on a particular question and identification of a line demarcating sides in the controversy.** To be discussed and resolved effectively, **controversies must be stated clearly. Vague understanding results in unfocused deliberation and poor decisions,** frustration, and emotional distress, as evidenced by the failure of the United States Congress to make progress on the immigration debate during the summer of 2007. **Someone disturbed by the problem of the growing underclass of poorly educated, socially disenfranchised youths might observe, "Public schools are doing a terrible job!** They are overcrowded, and many teachers are poorly qualified in their subject areas. Even the best teachers can do little more than struggle to maintain order in their classrooms." That same concerned citizen, facing a complex range of issues, might arrive at an unhelpful decision, such as "We ought to do something about this" or. worse. "It's too complicated a problem to deal with." **Groups of concerned citizens worried about the state of public education could join together to express their frustrations**, anger, disillusionment, and emotions regarding the schools, **but without a focus for their discussions, they could easily agree about the sorry state of education without finding points of clarity or potential solutions. A gripe session would follow. But if a precise question is posed**—such as "What can be done to improve public education?"—**then a more profitable area of discussion is opened up simply by placing a focus on the search for a concrete solution step**. **One or more judgments can be phrased in the form of debate propositions, motions for parliamentary debate, or bills for legislative assemblies.** The statements "Resolved: That the federal government should implement a program of charter schools in at-risk communities" and "Resolved: That the state of Florida should adopt a school voucher program" more clearly identify specific ways of dealing with educational problems in a manageable form, suitable for debate. **They provide specific policies to be investigated and aid discussants in identifying points of difference. To have a productive debate, which facilitates effective decision making by** directing and **placing limits on the decision** to be made, **the basis for argument should be clearly defined. If we merely talk about "homelessness" or "abortion" or "crime'\* or "global warming" we are likely to have an interesting discussion but not to establish profitable basis for argument**. For example, **the statement "Resolved: That the pen is mightier than the sword" is debatable, yet fails to provide much basis for clear argumentation**. If we take this statement to mean that the written word is more effective than physical force for some purposes, we can identify a problem area: the comparative effectiveness of writing or physical force for a specific purpose. **Although we now have a general subject, we have not yet stated a problem. It is still too broad,** too loosely worded to promote well-organized argument. **What sort of writing are we concerned with**—poems, novels, government documents, website development, advertising, or what? **What does "effectiveness" mean** in this context? What kind of physical force is being compared—fists, dueling swords, bazookas, nuclear weapons, or what? A more specific question might be. "Would a mutual defense treaty or a visit by our fleet be more effective in assuring Liurania of our support in a certain crisis?" **The basis for argument could be phrased in a debate proposition** such as "Resolved: That the United States should enter into a mutual defense treatv with Laurania." Negative advocates might oppose this proposition by arguing that fleet maneuvers would be a better solution. **This is not to say that debates should completely avoid creative interpretation** of the controversy by advocates, **or that good debates cannot occur over competing interpretations of the controversy; in fact, these sorts of debates may be very engaging. The point is that debate is best facilitated by the guidance provided by focus on a particular point of difference, which will be outlined in the following discussion.**

**Critical thinking skills are crucial to solve world problems—the training debate provides is uniquely key. It’s a pre-requisite to applying their aff in the real world**

**Lundberg 10** - Christian O. Lundberg 10 Professor of Communications @ University of North Carolina, Chapel Hill, “Tradition of Debate in North Carolina” in Navigating Opportunity: Policy Debate in the 21st Century By Allan D. Louden, p311

The second major problem with the critique that identifies a naivety in articulating debate and democracy is that it presumes that the primary pedagogical outcome of debate is speech capacities. But **the democratic capacities built by debate are not limited to speech**—as indicated earlier, **debate builds capacity for critical thinking**, analysis of public claims, **informed decision making, and better public judgment**. **If the picture of modem political life that underwrites this critique of debate is a pessimistic view of increasingly labyrinthine and bureaucratic administrative politics, rapid** scientific and technological **change** outpacing the capacities of the citizenry to comprehend them, **and ever-expanding insular special-interest- and money-driven politics, it is a puzzling solution, at best, to argue that these conditions warrant giving up on debate**. If democracy is open to rearticulation, it is open to rearticulation precisely because **as the challenges of modern political life proliferate, the citizenry's capacities can change, which is one of the primary reasons that theorists of democracy** such as Ocwey in The Public awl Its Problems **place such a high premium on education** (Dewey 1988,63, 154). **Debate provides an indispensible form of education in the modem articulation of democracy because it builds precisely the skills that allow the citizenry to research and be informed about policy decisions that impact them**, to son rhroueh and evaluate the evidence for and relative merits of arguments for and against a policy in an increasingly infonnation-rich environment, and to prioritize their time and political energies toward policies that matter the most to them. The merits of debate as a tool for building democratic capacity-building take on a special significance in the context of information literacy. John Larkin (2005, HO) argues that one of the primary failings of modern colleges and universities is that they have not changed curriculum to match with the challenges of a new information environment. This is a problem for the course of academic study in our current context, but perhaps more important, argues Larkin, for the future of a citizenry that will need to make evaluative choices against an increasingly complex and multimediatcd information environment (ibid-). Larkin's study tested the benefits of debate participation on information-literacy skills and concluded that in-class debate participants reported significantly higher self-efficacy ratings of their ability to navigate academic search databases and to effectively search and use other Web resources: To analyze the self-report ratings of the instructional and control group students, we first conducted a multivariate analysis of variance on all of the ratings, looking jointly at the effect of instmction/no instruction and debate topic . . . that it did not matter which topic students had been assigned . . . students in the Instnictional [debate) group were significantly more confident in their ability to access information and less likely to feel that they needed help to do so----These findings clearly indicate greater self-efficacy for online searching among students who participated in (debate).... These results constitute strong support for the effectiveness of the project on students' self-efficacy for online searching in the academic databases. There was an unintended effect, however: After doing ... the project, instructional group students also felt more confident than the other students in their ability to get good information from Yahoo and Google. It may be that the library research experience increased self-efficacy for any searching, not just in academic databases. (Larkin 2005, 144) Larkin's study substantiates Thomas Worthcn and Gaylcn Pack's (1992, 3) claim that **debate in the college classroom plays a critical role in fostering the kind of problem-solving skills demanded by the increasingly rich media and information environment of modernity**. Though their essay was written in 1992 on the cusp of the eventual explosion of the Internet as a medium, Worthcn and Pack's framing of the issue was prescient: the primary question facing today's student has changed from how to best research a topic to the crucial question of learning how to best evaluate which arguments to cite and rely upon from an easily accessible and veritable cornucopia of materials. There are, without a doubt, a number of important criticisms of employing debate as a model for democratic deliberation. But cumulatively, **the evidence presented here warrants strong support for expanding debate practice** in the classroom as a technology **for enhancing democratic deliberative capacities. The unique combination of critical thinking skills, research and information processing skills, oral communication skills, and capacities for listening and thoughtful, open engagement with hotly contested issues argues for debate as a crucial component of a rich and vital democratic life**. In-class debate practice both aids students in achieving the best goals of college and university education, **and serves as an unmatched practice for creating thoughtful, engaged, open-minded and self-critical students who are open to the possibilities of meaningful political engagement and new articulations of democratic life. Expanding this practice is crucial, if only because the more we produce citizens that can actively and effectively engage the political process, the more likely we are to produce revisions of democratic life that are necessary if democracy is not only to survive, but to thrive. Democracy faces** a myriad **of challenges, including**: domestic and international **issues of class, gender, and racial justice**; **wholesale environmental destruction and the potential for rapid climate change**; emerging **threats to international stability** in the form of terrorism, intervention and new possibilities for great power conflict; **and increasing challenges of rapid globalization** including an increasingly volatile global economic structure. **More than any specific policy or proposal, an informed and active citizenry that deliberates with greater skill** and sensitivity **provides one of the best hopes for responsive and effective democratic governance, and by extension, one of the last best hopes for dealing with** the **existential challenges** to democracy [in an] increasingly complex world.

**B. Creativity—thinking “inside the box” forces teams to be creative about their positions and come up with innovative solutions. Absent constraints, debate becomes boring and stale**

Intrator 10 (Intrator, David, President of The Creative Organization and musical composer, October 22, 2010, “Thinking Inside The Box: A Professional Creative Dispels A Popular Myth”, Training, http://www.trainingmag.com/article/thinking-inside-box) FS

**One of the most pernicious myths about creativity, one that seriously inhibits creative thinking and innovation, is the belief that one needs to “think outside the box.”** As someone who has worked for decades as a professional creative, **nothing could be further from the truth. This** a **is** view **shared by the vast majority of creatives, expressed** famously **by** the **modernist designer Charles Eames when he wrote, “Design depends largely upon constraints.” The myth of thinking outside the box stems from a fundamental misconception of what creativity is**, and what it’s not. In the popular imagination, creativity is **something weird and wacky.** The creative process is magical, or divinely inspired. But, in fact, **creativity is** not about divine inspiration or magic. It’s **about problem-solving, and by definition a problem is a constraint**, a limit, a box. One of the best illustrations of this is the work of **photographers**. They create by excluding the great mass what’s before them, choosing a small frame in which to work. Within that tiny frame, literally a box, they uncover relationships and establish priorities. What makes creative problem-solving uniquely challenging is that you, as the creator, are the one defining the problem. You’re the one choosing the frame. And **you alone determine what’s an effective solution**. **This can be quite demanding,** both intellectually and emotionally. **Intellectually, you are required to establish limits, set priorities**, and cull patterns and relationships from a great deal of material, much of it fragmentary. More often than not, this is the material you generated during brainstorming sessions. At the end of these sessions, you’re usually left with a big mess of ideas, half-ideas, vague notions, and the like. Now, chances are you’ve had a great time making your mess. You might have gone off-site, enjoyed a “brainstorming camp,” played a number of warm-up games. You feel artistic and empowered. **But to be truly creative**, you have to clean up your mess, organizing those fragments into something real, something useful, something that actually works. That’s the hard part. It takes a lot of energy, time, and willpower to make sense of the mess you’ve just generated. It also can be emotionally difficult. **You’ll need to throw out many ideas you originally thought were great, ideas you’ve become attached to, because they simply don’t fit into the rules you’re creating as you build your box.** You can always change the rules, but that also comes with an emotional price. Unlike many other kinds of problems, with creative problems there is no external authority to which you can appeal to determine whether you’re on the right track, whether one set of rules should have priority over another, or whether one box is better than another. There is no correct answer. Better said: There might be a number of correct answers. Or none at all. The responsibility of deciding the right path to take is entirely upon you. That’s a lot of responsibility, and it can be paralyzing. So it’s no wonder that the creative process often stalls after the brainstorming in many organizations. Whereas generating ideas is open-ended, and, in a sense, infinitely hopeful, having to pare those ideas down is restrictive, tedious, and, at times, scary. The good news, however, is that understanding the creative process as problem-solving is ultimately liberating. For one, all of **those** left-brainers **with well-honed rational skills will find themselves far more creative than they ever thought**. They’ll discover their talents for organization, abstraction, and clarity are very much what’s required to be a true creative thinker. **Viewing creativity as problem-solving also makes the whole process far less intimidating**, even though it might lose some of its glamour and mystery. Moreover, **since creative problems are open to rational analysis, they can be broken down into smaller components that are easier to address.** Best of all, **the very act of problem-solving, of organizing and trying making sense of things, helps generate new ideas.** Paradoxically, **thinking within a box may be one of the most effective brainstorming techniques there** is. That may be what Charles Eames meant when he added, “I welcome constraints.” Without some sort of structure to your creative thinking, you’re just flailing about. For a while you might feel like you’re making progress, generating a great mess of ideas that might hold some potential. But to turn those ideas into something truly innovative, your best bet is to build your box and play by the rules of your own creation.

#### We co-opt their offense –game rules inspire pedagogical transformation

Armstrong 2K

(Paul B., Dean and Professor of Literature at Brown University, New Literary History, 31: 211–223, “The Politics of Play: The Social Implications of Iser’s Aesthetic Theory”)

The contradictory combination of restriction and openness in how play deploys power is evident in Iser’s analysis of “regulatory” and “aleatory” rules. Even the regulatory rules, which set down the conditions participants submit to in order to play a game, “permit a certain range of combinations while also establishing a code of possible play. . . . **Since** these **rules limit the text game without producing it, they are regulatory but not prescriptive. They do no more than set the aleatory in motion,** and the aleatory rule differs from the regulatory in that it has no code of its own” (FI 273). **Submitting to the discipline of regulatory restrictions is both constraining and enabling because it makes possible certain kinds of interaction that the rules cannot completely predict or prescribe in advance**. Hence the existence of aleatory rules that are not codiﬁed as part of the game itself but are the variable customs, procedures, and practices for playing it. Expert facility with aleatory rules marks the difference, for example, between someone who just knows the rules of a game and another who really knows how to play it. Aleatory rules are more ﬂexible and open- ended and more susceptible to variation than regulatory rules, but **they** too **are characterized by a contradictory combination of constraint and possibility, limitation and unpredictability,** discipline and spontaneity. **As a rule-governed but open-ended activity, play provides a model for deploying power in a nonrepressive manner that makes creativity and innovation possible not in spite of disciplinary constraints but because of them**. Not all power is playful, of course, and some restrictions are more coercive than enabling. **But thinking about the power of constraints on the model of rules governing play helps to explain the paradox that restrictions can be productive rather than merely repressive.** Seeing constraints as structures for establishing a play-space and as guides for practices of exchange within it envisions power not necessarily and always as a force to be resisted in the interests of freedom; **it allows** imagining the **potential for power to become a constructive social energy that can animate games of to-and-fro exchange between participants whose possibilities for self-discovery and self-expansion are enhanced by** the **limits shaping their interactions.**

#### C. Fairness—they cause debate breakdown—if it’s too hard to be neg, no one will play—empirics prove

Robin Rowland, University of Kansas, “Topic Selection in Debate,” AMERICAN FORENSICS IN PERSPECTIVE, ed. D.Parson, 1984, p. 53-54.

The first major problem identified by the work group as relating to topic selection is the decline in participation in the National Debate Tournament (NDT) policy debate. As Boman notes: There is a growing dissatisfaction with academic debate that utilizes a policy proposition. Programs which are oriented toward debating the national policy debate proposition, so-called “NDT” programs, are diminishing in scope and size.4 This **decline in** policy **debate is tied**, many in the work group believe, **to excessively broad topics**. The most obvious characteristic of some recent policy debate topics is extreme breath. A resolution calling for regulation of land use literally and figuratively covers a lot of ground. Naitonal debate topics have not always been so broad. Before the late 1960s the topic often specified a particular policy change.5 The move from narrow to **broad topics** has had, according to some, the effect of **limit**ing **the number** of students **who participate** in policy debate. First, **the breadth of the topics has all but destroyed novice debate**. Paul Gaske argues that because the stock issues of policy debate are clearly defined, it is superior to value debate as a means of introducing students to the debate process.6 Despite this advantage of policy debate, Gaske belives that NDT debate is not the best vehicle for teaching beginners. The problem is that **broad** policy **topics terrify novice debaters**, especially those who lack high school debate experience. **They are unable to cope with the breadth** of the topic **and** experience “negophobia,”7 the **fear** of **debating negative**. As a consequence, the educational advantages associated with teaching novices through policy debate are lost: “Yet all of these benefits fly out the window as rookies in their formative stage quickly experience humiliation at being caugh without evidence or substantive awareness of the issues that confront them at a tournament.”8 The ultimate result is that fewer novices participate in NDT, thus lessening the educational value of the activity and limiting the number of debaters or eventually participate in more advanced divisions of policy debate. In addition to noting the effect on novices, participants argued that broad topics also discourage experienced debaters from continued participation in policy debate. Here, the claim is that **it takes so much** times and **effort** to be competitive **on a broad topic that students** who are concerned with doing more than just debate **are forced out of the activity**.9 Gaske notes, that “broad topics discourage participation because of insufficient time to do requisite research.”10 **The final effect may be that entire programs** either **cease functioning** or shift to value debate as a way to avoid unreasonable research burdens. Boman supports this point: “It is this **expanding** necessity of evidence, and thereby **research**, which **has created a competitive imbalance** between institutions that participate in academic debate.”11 In this view, it is the competitive imbalance resulting from the use of broad topics that has led some small schools to cancel their programs.

**Flex DA**

**Executive flexibility is key deterrence**

**Bradbury 11** (Steven – partner @ Dechert, LLP, “The Developing Legal Framework for Defensive and Offensive Cyber Operations” March 2011, Cybersecurity: Law, Privacy, and Warfare in a Digital World, Harvard National Security Journal, Vol. 2)

Conclusion. So here’s my thesis: To my view, **the lack of clarity on certain of these issues under international law means that with respect to those issues, the President is free to decide, as a policy matter, where and how the lines should be drawn on the limits of traditional military power** in the sphere of cyberspace. For example, that means that within certain parameters, **the President could decide when and to what extent military cyber operations may target computers located outside areas of hot fighting that the enemy is using for military advantage**. And when a cyber attack is directed at us, **the President can decide, as a matter of national policy, whether and when to treat it as an act of war**. The corollary to all this is that **in situations where the customs of war,** in fact, **are not crystallized**, **the lawyers at the State Department and the Justice Department shouldn’t make up new red lines** — **out of some aspirational sense of what they think international law ought to be** — **that end up putting dangerous limitations on the options available to the United States**. Certainly, the advice of lawyers is always important, especially so where the legal lines are established or firmly suggested. **No one would contend that the laws of war have no application to cyber operations or that cyberspace is a law free zone**. **But it’s not the role of the lawyers to make up new lines that don’t yet exist in a way that preempts the development of policy**. 14 In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention on cyberwarfare — perhaps a kind of arms control agreement for cyber weapons. **I believe there is no foreseeable prospect that that will happen. Instead, the outlines of accepted norms and limitations in this area will develop through the practice of leading nations**. And **the policy decisions made by the United States in response to particular events will have great influence in shaping those international norms**. I think that’s the way we should want it to work.

**Only offensive capabilities will suffice**

Jarno **Limnéll** October 9 **2012** “Offensive Cyber Capabilities Need to be Built and Exposed Because of Deterrence”, <http://www.infosecisland.com/blogview/22534-Offensive-Cyber-Capabilities-Need-to-be-Built-and-Exposed-Because-of-Deterrence.html>

**Within the next** couple of **years the world will experience** more **intentionally executed and demonstrated cyberattacks** while the development of offensive cyberweapons will become fiercer and publicly more acceptable.¶ Today, **cyber capabilities are essential for nation-states** and armed forces **that want to be treated as credible players.** Cyberspace, the fifth dimension of warfare, has already become an important arena of world politics, especially since we are living in a time in which the lines between war and peace have blurred. **The digital world has become a domain where strategic advantage can be either lost or won.¶ To succeed in the cyber domain is not merely a question of defense**, even if we would like to think of it that way – at least not for the nation-states. Naturally, defense capabilities have to be as preventive as possible in order to reduce the effectiveness of the adversary´s – whoever it might be –cyber attack. However, despite the best defensive efforts, intrusions will occur. In the cyber domain, you must also be resilient, i.e. have the ability to withstand attacks and failures, to mitigate harm, more so than what is needed in other domains. **Creating cyber defense capabilities and resilience are fairly easy for the public to accept. But they are not enough. Deterrence is** also **needed, that is, the capabilities and policies to convince others not to launch a cyber attack against you. Deterrence will only be effective if you can build and demonstrate offensive cyber capabilities**. To put it clearly: **cyber offensive capabilities are an essential element for nation-states to succeed in the current and future reality of both international and security policies. Defense, resilience, and offense contribute to a country’s overall ability** to protect itself. You need them all.¶ From nuclear to cyber deterrence¶ **Deterrence theory was developed in the 1950s**, primarily to address the new strategic challenges posed by nuclear weapons. During the Cold War, nuclear deterrence was able to keep the United States and the Soviet Union in check. **Nuclear deterrence was the art of convincing an enemy not to take a specific action** by threatening it with intolerable punishment or unacceptable failure. **The theory worked well.**¶ Based on that logic, **cyber deterrence should play a similar role in the digitalized world**. However, the anonymity, the advantage of attacks, and the global reach and interconnectedness greatly reduce the efficiency of cyber deterrence. At the same time, there are suspicion and rumors surrounding the kind of capabilities others have and how they are already using those capabilities.¶ In the kinetic world, it is much simpler to evaluate an opponent’s capabilities. It is typically quite easy to accurately estimate how many tanks, interceptors, or submarines a given country possesses. Countries also openly expose their arsenal, in military parades for example, or their operational skills, by organizing large military exercises. **In the logic of deterrence, even more important than having the actual capability is the perception of having that capability**.

**Only deterrence can solve future cyber attacks**

**Kramer 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 U**nited **S**tates **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 U**nited **S**tates **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 U**nited **S**tates **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.

**Rolli: 1NC**

**The aff confuses perception and intensity and treats speed as a problem of phenomenology. Using examples like the feeling of driving a car they claim this sense of speed generates an anxiety about our exposure to contingency. But the Glezos evidence is wrong. Its account of perception is atomistic, reductionist, and assumes that sense data corresponds to ideas. This is anthropomorphic.The Deleuzian account of intensity to which it refers is pre-personal and cannot be experienced and only contemporary technology’s ability to abstract allows us to map it.**

Marc **Rölli**, Professor of Philosphy at Fatih University, “Deleuze on Intensity Differentials and the Being of the Sensible,” Deleuze Studies Volume 3, June, **2009**. P. 28-29

**Let us look again at the foundations of** the empiricist theory of **perception**. **We know that it is supposed to facilitate the realisation of a programme that founds and checks over all knowledge through reference to immediate experience**. Hume introduces ‘**perception’ as the generic term for facts of experience** in general and **distinguishes two types of perception** according to their degree of intensity: **impressions and ideas**. Impressions for their part divide into impressions of sensation and impressions of reflection. In addition Hume emphasises that there are not only simple impressions, but also (from the simple ones) compound impressions and ideas. **This** addition is important because it complicates the dependency relationships of the two types of impression to one another. Hume’s fundamental **empiricist proposition**, which **is** generally **known** **as the copy-principle,** frankly **maintains ‘that all our simple ideas in their first appearance are derived from simple impressions, which are correspondent to them, and which they exactly represent**’¶ (Hume 1978: 4). **The prototype-copy relation can therefore only be established on the level of simple perceptions.** This is fundamentally significant because the empiricist analysis of abstract ideas depends on being able to reduce ideas to impressions and can only elicit their truth content in this way. In this context we have the principle of difference as formulated by Hume, which states that ‘whatever objects are different are distinguishable, and that whatever objects are distinguishable are separable by the thought and imagination’ (Hume 1978: 18). Associations of ideas cannot combine the latter in such a way that they merge together or are made inseparable: precisely their ‘independent separability’ makes possible their empiricist justification in the first place.¶ It has often enough been pointed out that for Deleuze the **atomistic premises of the theory of perception and the corresponding copy theory are not feasible** and force us to look back at the distinction between phenomenological and naturalistic aspects of Hume’s empiricism. The atomistic premises then give way to the central thesis to which Deleuze adheres, which says **that sensual intensities are genetic elements that actualise themselves in extensity as an extensive magnitude**. However, **they are concealed by perceived qualities that ascribe themselves to some persistent object constituting itself within the same given framework** (that is, in the corresponding space-time actualisation relations). Formulated in empiricist terminology, **this thesis maintains that sense impressions are first to be understood as pre-individual sense data and only begin to stabilise themselves as associatively bundled and organised moments of perception in the order of visible objects. The postulated displacement within the empiricist field of concepts reveals itself only after a requisite appraisal in terms of immanent criteria.**

**Moreover, the aff’s relation to contingency is problematic- contingency doesn’t produce a tragic sense of experience where we can’t grasp or know anything about the future - a position that results in strict utopianism or pessimism- but something to manage. We must take what tools we can because the contingency of ecological crisis and the excesses of socio-technological assemblages risk devastation. Economic planning, quantitative data mining, and cybernetic operations are essential to the struggle. Managing contingency and navigating the devastating effects of contingency are different. The aff ends the later.**

Alex **Wiliams** **and** Nick **Srnicek**, PhD Candidates in International Relations at the London School of Economics, “#ACCERLATE MANIFESTO for an Acceleration Politics,” May 14, **2013**, <http://criticallegalthinking.com/2013/05/14/accelerate-manifesto-for-an-accelerationist-politics/>

6. Given the enslave­ment of tech­nos­cience to cap­it­al­ist object­ives (espe­cially since the late 1970s) **we surely do not yet know what a mod­ern tech­noso­cial body can do**. **Who amongst us fully recog­nizes what untapped poten­tials await in the tech­no­logy which has already been developed**? **Our wager is that the true trans­form­at­ive poten­tials of much of our tech­no­lo­gical and sci­entific research remain unex­ploited, filled with presently redund­ant fea­tures (or pre- adaptations) that, fol­low­ing a shift bey­ond the short- sighted cap­it­al­ist socius, can become decisive**.¶ 7. **We want to accel­er­ate the pro­cess of tech­no­lo­gical evol­u­tion**. But **what we are arguing for is not techno- utopianism. Never believe that tech­no­logy will be suf­fi­cient to save us. Neces­sary, yes, but never suf­fi­cient without socio- political action**. **Tech­no­logy and the social are intim­ately bound up with one another, and changes in either poten­ti­ate and rein­force changes in the other**. Whereas the techno- utopians argue for accel­er­a­tion on the basis that it will auto­mat­ic­ally over­come social con­flict, our pos­i­tion is that tech­no­logy should be accel­er­ated pre­cisely because it is needed in order to win social conflicts.¶ 8. **We believe that any post- capitalism will require post- capitalist plan­ning. The faith placed in the idea that, after a revolu­tion, the people will spon­tan­eously con­sti­tute a novel socioeco­nomic sys­tem that isn’t simply a return to cap­it­al­ism is naïve at best, and ignor­ant at worst**. To fur­ther this, **we** **must develop both a cog­nit­ive map of the exist­ing sys­tem and a spec­u­lat­ive image of the future eco­nomic system**.¶ 9. To do so, **the left must take advant­age of every tech­no­lo­gical and sci­entific advance made pos­sible by cap­it­al­ist soci­ety**. We declare that **quan­ti­fic­a­tion is not an evil to be elim­in­ated, but a tool to be used in the most effect­ive man­ner pos­sible**. **Eco­nomic mod­el­ling is** — simply put — **a neces­sity for mak­ing intel­li­gible a com­plex world.** **The 2008 fin­an­cial crisis reveals the risks of blindly accept­ing math­em­at­ical mod­els on faith, yet this is a prob­lem of ille­git­im­ate author­ity not of math­em­at­ics itself.** The tools to be found in **social net­work ana­lysis, agent- based mod­el­ling, big data ana­lyt­ics, and non- equilibrium eco­nomic mod­els, are neces­sary cog­nit­ive medi­at­ors for under­stand­ing com­plex sys­tems like the mod­ern eco­nomy**. **The accel­er­a­tion­ist left must become lit­er­ate in these tech­nical fields**.¶ 10. **Any trans­form­a­tion of soci­ety must involve eco­nomic and social exper­i­ment­a­tion**. The Chilean Pro­ject Cyber­syn is emblem­atic of this exper­i­mental atti­tude — fus­ing advanced cyber­netic tech­no­lo­gies, with soph­ist­ic­ated eco­nomic mod­el­ling, and a demo­cratic plat­form instan­ti­ated in the tech­no­lo­gical infra­struc­ture itself. Sim­ilar exper­i­ments were con­duc­ted in 1950s – 1960s Soviet eco­nom­ics as well, **employ­ing cyber­net­ics and lin­ear pro­gram­ming in an attempt to over­come** the **new prob­lems** faced by the first com­mun­ist eco­nomy. That both of these were ulti­mately unsuc­cess­ful can be traced to the polit­ical and tech­no­lo­gical con­straints these early cyber­net­i­cians oper­ated under.¶ 11. **The left must develop soci­o­tech­nical hege­mony: both in the sphere of ideas, and in the sphere of mater­ial plat­forms. Plat­forms are the infra­struc­ture of global soci­ety**. They estab­lish the basic para­met­ers of what is pos­sible, both beha­vi­our­ally and ideo­lo­gic­ally. In this sense, **they embody the mater­ial tran­scend­ental of soci­ety: they are what make pos­sible par­tic­u­lar sets of actions, rela­tion­ships, and powers**. While much of the cur­rent global plat­form is biased towards cap­it­al­ist social rela­tions, this is not an inev­it­able neces­sity. **These mater­ial plat­forms of pro­duc­tion, fin­ance, logist­ics, and con­sump­tion can and will be repro­grammed and reformat­ted towards post- capitalist ends.**

**This results in war, crisis, and extinction democracy can’t solve.**

Alex **Wiliams** **and** Nick **Srnicek**, PhD Candidates in International Relations at the London School of Economics, “#ACCERLATE MANIFESTO for an Acceleration Politics,” May 14, **2013**, <http://criticallegalthinking.com/2013/05/14/accelerate-manifesto-for-an-accelerationist-politics/>

At the begin­ning of the second dec­ade of the Twenty- First Cen­tury, **global civil­iz­a­tion faces a new breed of cata­clysm**. These com­ing apo­ca­lypses ridicule the norms and organ­isa­tional struc­tures of the polit­ics which were forged in the birth of the nation- state, the rise of cap­it­al­ism, and a Twen­ti­eth Cen­tury of unpre­ced­en­ted wars.¶ 2. **Most sig­ni­fic­ant is the break­down of the plan­et­ary cli­matic sys­tem**. In time, **this threatens the con­tin­ued exist­ence of the present global human pop­u­la­tion**. Though this is the most crit­ical of the threats which face human­ity, **a series of lesser but poten­tially equally destabil­ising prob­lems exist along­side and inter­sect with it. Ter­minal resource deple­tion,** espe­cially in water and energy reserves, **offers the pro­spect of mass star­va­tion**, **col­lapsing eco­nomic paradigms, and new hot and cold war**s. Con­tin­ued fin­an­cial crisis has led gov­ern­ments to embrace the **para­lyz­ing death spiral policies of aus­ter­ity,** privat­isa­tion of social wel­fare ser­vices, mass unem­ploy­ment, and stag­nat­ing wages. Increas­ing auto­ma­tion in pro­duc­tion pro­cesses includ­ing ‘intel­lec­tual labour’ is evid­ence of the sec­u­lar crisis of cap­it­al­ism, soon to **render it incap­able of main­tain­ing cur­rent stand­ards of liv­ing for even the former middle classes of the global north**.¶ 3. In con­trast to these ever- accelerating cata­strophes, **today’s polit­ics is beset by an inab­il­ity to gen­er­ate the new ideas and modes of organ­isa­tion neces­sary to trans­form our soci­et­ies to con­front and resolve the com­ing anni­hil­a­tions**. **While crisis gath­ers force and speed, polit­ics with­ers and retreats. In** this para­lysis of the polit­ical ima­gin­ary, the future has been cancelled.¶ 4. Since 1979, **the hege­monic global polit­ical ideo­logy has been neo­lib­er­al­ism, found in some vari­ant through­out the lead­ing eco­nomic powers**. In spite of the deep struc­tural chal­lenges the new global prob­lems present to it, most imme­di­ately the credit, fin­an­cial, and fiscal crises since 2007 – 8, **neo­lib­eral pro­grammes have only evolved in the sense of deep­en­ing**. This con­tinu­ation of the neo­lib­eral pro­ject, or neo­lib­er­al­ism 2.0, has begun to apply another round of struc­tural adjust­ments, most sig­ni­fic­antly in the form of encour­aging new and aggress­ive incur­sions by the private sec­tor into what remains of social demo­cratic insti­tu­tions and ser­vices. This is in spite of the imme­di­ately neg­at­ive eco­nomic and social effects of such policies, and the longer term fun­da­mental bar­ri­ers posed by the new global crises.¶ 5. **That the forces of right wing gov­ern­mental, non- governmental, and cor­por­ate power have been able to press forth with neo­lib­er­al­isa­tion is at least in part a res­ult of the con­tin­ued para­lysis and inef­fec­tual nature of much what remains of the left**. Thirty years of **neo­lib­er­al­ism have rendered most left- leaning polit­ical parties bereft of rad­ical thought, hol­lowed out, and without a pop­u­lar man­date**. At best they have respon­ded to our present crises with calls for a return to a Keyne­sian eco­nom­ics, in spite of the evid­ence that the very con­di­tions which enabled post- war social demo­cracy to occur no longer exist. We can­not return to mass industrial- Fordist labour by fiat, if at all. Even the neo­so­cial­ist regimes of South America’s Bolivarian Revolu­tion, whilst heart­en­ing in their abil­ity to res­ist the dog­mas of con­tem­por­ary cap­it­al­ism, remain dis­ap­point­ingly unable to advance an altern­at­ive bey­ond mid- Twentieth Cen­tury social­ism. Organ­ised labour, being sys­tem­at­ic­ally weakened by the changes wrought in the neo­lib­eral pro­ject, is scler­otic at an insti­tu­tional level and — at best — cap­able only of mildly mit­ig­at­ing the new struc­tural adjust­ments. But with no sys­tem­atic approach to build­ing a new eco­nomy, or the struc­tural solid­ar­ity to push such changes through, for now labour remains rel­at­ively impot­ent. The **new social move­ments** which emerged since the end of the Cold War, exper­i­en­cing a resur­gence in the years after 2008, have been sim­il­arly unable to devise a new polit­ical ideo­lo­gical vis­ion. Instead they **expend con­sid­er­able energy on internal direct- democratic pro­cess and affect­ive self- valorisation over stra­tegic effic­acy**, and fre­quently pro­pound a vari­ant of neo- primitivist loc­al­ism, as if to oppose the abstract viol­ence of glob­al­ised cap­ital with the flimsy and eph­em­eral “authen­ti­city” of com­munal immediacy.¶ 6**. In the absence of a rad­ic­ally new social, polit­ical, organ­isa­tional, and eco­nomic vis­ion the hege­monic powers of the right will con­tinue to be able to push for­ward their narrow- minded ima­gin­ary, in the face of any and all evid­ence**. At best, **the left may be able for a time to par­tially res­ist some of the worst incur­sions**. But this is to be Canute against an ulti­mately irres­ist­ible tide. **To gen­er­ate a new left global hege­mony entails a recov­ery of lost pos­sible futures, and indeed the recov­ery of the future as such**.

**Our alternative is to endorse accelerationism. This is distinct from the aff in two ways: 1) it not merely accepts the tragic condition of an ateological future, but actively embraces the experimental potential of techno-capitalism and 2) it reinvents collective projects of criticism, evolution, and adaptation that the aff shuts down in its skeptical objections to cyberoperations. We believe in ateleogical contingency, but this requires openness to the very forms of control and politics they dislike**

Alex **Wiliams** **and** Nick **Srnicek**, PhD Candidates in International Relations at the London School of Economics, “#ACCERLATE MANIFESTO for an Acceleration Politics,” May 14, **2013**, <http://criticallegalthinking.com/2013/05/14/accelerate-manifesto-for-an-accelerationist-politics/>

22. We need to revive the argu­ment that was tra­di­tion­ally made for post- capitalism: not only is **cap­it­al­ism** an unjust and per­ver­ted sys­tem, but it **is also a sys­tem that holds back pro­gress. Our tech­no­lo­gical devel­op­ment is being sup­pressed by cap­it­al­ism, as much as it has been unleashed. Accel­er­a­tion­ism is the basic belief that these capa­cit­ies can and should be let loose by mov­ing bey­ond the lim­it­a­tions imposed by cap­it­al­ist soci­ety**. The move­ment towards a sur­pass­ing of our cur­rent con­straints must include more than simply a struggle for a more rational global soci­ety. We believe it must also include recov­er­ing the dreams which trans­fixed many from the middle of the Nine­teenth Cen­tury until the dawn of the neo­lib­eral era, of the quest of Homo Sapi­ens towards expan­sion bey­ond the lim­it­a­tions of the earth and our imme­di­ate bod­ily forms. These vis­ions are today viewed as rel­ics of a more inno­cent moment. Yet they both dia­gnose the stag­ger­ing lack of ima­gin­a­tion in our own time, and offer the prom­ise of a future that is affect­ively invig­or­at­ing, as well as intel­lec­tu­ally ener­gising. After all, **it is only a post- capitalist soci­ety, made pos­sible by an accel­er­a­tion­ist polit­ics, which will ever be cap­able of deliv­er­ing on the promis­sory note of the mid- Twentieth Century’s space pro­grammes, to shift bey­ond a world of min­imal tech­nical upgrades towards all- encompassing change**. **Towards** a time of col­lect­ive self- mastery, and **the prop­erly alien future that entails and enables. Towards a com­ple­tion of the Enlight­en­ment pro­ject of self- criticism and self- mastery, rather than its elimination.¶** 23. **The choice facing us is severe: either a glob­al­ised post- capitalism or a slow frag­ment­a­tion** towards prim­it­iv­ism, per­petual crisis, **and plan­et­ary eco­lo­gical collapse.¶** 24. **The future needs to be con­struc­ted.** It has been demol­ished by neo­lib­eral cap­it­al­ism and reduced to a cut- price prom­ise of greater inequal­ity, con­flict, and chaos. This col­lapse in the idea of the future is symp­to­matic of the regress­ive his­tor­ical status of our age, rather than, as cyn­ics across the polit­ical spec­trum would have us believe, a sign of scep­tical matur­ity. **What accel­er­a­tion­ism pushes towards is a future that is more mod­ern — an altern­at­ive mod­ern­ity that neo­lib­er­al­ism is inher­ently unable to gen­er­ate. The future must be cracked open once again, unfasten­ing our hori­zons towards the uni­ver­sal pos­sib­il­it­ies of the Outside.**

**Case:**

**Their uniqueness claim is wrong-institutions and the executive are effectively dealing with social acceleration now**

**GSN 2013**

(Global Solutions Networkm “Global Problem Solving in an Era of Big Data”, <http://gsnetworks.org/global-problem-solving-in-an-era-of-big-data>)

**With the right tools and the right training, global solution networks can also harness this vast cloud of data to develop more analytical approaches to problem solving**. For example**, GSNs can use pervasive computing and the data it generates to revolutionize our ability to model the world and all of its systems**, **giving us new insights into social and natural phenomena** and the ability to forecast trends like climate change with greater accuracy. The DC-based World Resources Institute (**WRI**), for example, **maintains** Global Forest Watch (**GFW**), **a global watchdog network that improves transparency and accountability in forest management decisions by increasing the public’s access to information** on forestry developments around the world. Within minutes, an interested researcher can detect changes in forest coverage, see the location and duration of a forestry company’s logging concessions, look up local forestry laws and regulations, and check whether the logging companies have paid their taxes. Most information can be easily navigated using a visual map interface that taps into a combination of satellite imagery, national forest data sets and “on-the-ground” reports. More advanced users can download geographical data from their warehouse and manipulate it for their own analyses using third party apps like Google Earth. **The big data will revolutionize the practice of global problem solving and even alter the basic skill set required to participate effectively in global public policy debates.** A collection of data scientists working with the UN Global Pulse team in New York, for example, is convinced that **data driven analysis and real-time reporting is on the cusp of transforming the way solution networks and development institutions respond to a wide range of critical issues.** Analyzing Tw

itter messages, for instance, can give an early warning of a spike in unemployment, price rises and disease. In fact, research found that surges in online mentions of rice prices accurately captured price increases several months before official reports. **If the Global Pulse team is successful in building effective tools for collecting, analyzing and visualizing data, their contributions could allow UN projects and policies to move faster, adapt to changing circumstances and be more effective, helping to lift more communities out of poverty and even save lives.** Indeed, for global solution networks, **the big data revolution will create tremendous opportunities to develop new knowledge and inform action with credible data.** But there will also be deep challenges in coming to grips with the infrastructure and tools required to take advantage of big data.

**No impact – speed increases resilience.**

**Thrift, University of Oxford geography professor, 2004**

[Nigel, “But Malice Aforethought: Cities and the Natural History of Hatred Centre of Contemporary Culture of Barcelona” <http://www.cccb.org/rcs_gene/malice_aforethought.pdf>, p.5-6, accessed 9-30-13, TAP]

Recently, this general hum of activity has been powered up by information technology. True, **the speed and ¶ interconnectedness of information and communications technology may have produced new vulnerabilities ¶ but, generally speaking, information and communications technology has probably made cities more robust ¶ by adding more degrees of redundancy.** Simple things like risk analysis and other institutionalised forms of ¶ diligence, booking systems, etc. have made the business of maintenance and repair easier to carry out and, ¶ indeed, is beginning to automate at least some of this activity (as in, for example, the instance of machines ¶ that send messages that they are breaking down). **More to the point, in situations of breakdown, whether epic or mundane, the humble mobile phone has extended the city’s interactivity and adaptability in all kinds ¶ of ways and may well have been the most significant device to add to a city’s overall resilience by adding an ¶ extra thread to the urban knot. In addition, all kinds of knowledges of maintenance and repair which are ¶ heavily dependent upon information and communications technologies are coming to the fore, all the way ¶ from logistics to disaster planning itself** (which, in certain senses, is a branch of logistics).

**I want to argue that this activity constitutes an urban technological unconscious which helps to keep cities as predictable objects in which things turn up as they are meant to, regularly and predictably** (THRIFT, ¶ 2004a). **Modern Western cities are in many ways mass engineerings of time and space and this engineering ¶ increasingly involves working with very small spaces** (of the order of millimetres) **and times** (of the order of ¶ milliseconds). **At this scale, this means working on the structure of anticipation, producing a comforting ¶ sense of regularity and a corresponding** (and probably amplified historically) **sense of annoyance when ¶ things do not play out exactly as it is intended that they should. In a sense, speed has produced a new ¶ landscape of anticipation**. Some commentators see this landscape as a threat, likely to institute a new ¶ «dromocracy». I am more ambivalent. It seems to me that **it offers possibilities too, and not least in ¶ providing rapid reaction to problems large and small. Indeed, as information technology systems come in ¶ which are based on continuous updating of information, some degree of capacity to track and trace and the ¶ ability to forecast forward in a very limited way** (for example, through profiling systems), **so it seems to me ¶ that cities will add another landscape to their repertoire, one which works a few seconds or minutes or, in ¶ extreme cases, hours ahead of the present and which will add markedly to their resilience**. Of course, there ¶ is a new repertoire of risk associated with this landscape of foresight but whether it is that much larger than ¶ many other developments remains to be seen. Computer systems are vulnerable to attack just like any other ¶ system but **it is** also **important to remember the continuous amount of repair and maintenance which goes ¶ into these systems anyway and reactions to attacks by worms or viruses are rapidly being incorporated into ¶ this burgeoning structure**.

**Their theory can’t describe military technology**

**Thommesen, 3**

(PhD Student-Center, University of Denmark, “Virilio: From Space to Time, From Reality to Image,” http://www.ephemerajournal.org/contribution/virilio-space-time-reality-image)

It seems appropriate to close this review by returning once more to the issue of technology and warfare, which has resumed actuality with two recent hi-tech wars. It will also provide an opportunity to explain his method. Leaving aside the idea of society being shaped by military logic, one might question whether **Virilio exaggerates the significance of technology in warfare**, that is, whether he accepts at face value the picture presented by the proponents of televised high-precision missile systems. Without being an expert in military history, I seem to remember that those bombs were never quite as smart and precise as announced by military spokesmen. And it has also been argued that at least the more recent war in Afghanistan was not won from the air but depended quite largely on ground personnel (at a mere 'relative speed'4). Furthermore, the example of automatic defence systems also seems to show that he echoes the optimistic arguments about the potential for Artificial Intelligence. He accepts that this degree of automatization - not only in warfare, but also **as a general tendency** - is a realistic vision, **while the fact is that research in AI has failed to deliver for decades**. (On other hand it is a relief that he does not simply argue that AI is impossible due to phenomenological insights). Thus, while Virilio offers a critical antidote to the choir of IT evangelists, i.e. the idea of us all getting together in the global village (which he explicitly criticizes), he may be criticized for a similar tendency to **attribute too much importance to the isolated factor of Technology**. And perhaps this critique could be extended to his method in general, that is, dying to read signs of the future in various contemporary events without resorting to any elaborate empirical study, picking out convenient examples without over-zealous attention to then actual representativity - a method Brugger and Petersen (1994) label 'archaeology of the future\*. On the other hand, those may be exactly the conditions and risks involved in trying to grasp the future: the intention is to identify future tendencies rather than merely describe contemporary reality. Although the critique of his empirical 'method' should not be completely silenced, neither should critique silence the observations of an analytical and somewhat cynical 'visionary'. I certainly find many of his ideas and arguments inspiring for further study, without having to subscribe to all of his theses.

## 2NC

**The affs turn to creative engagements with democracy as their glezos evidence says “we *will have to develop new structures…allow us to engage with accelerationism in a democratic way*.” But this is exactly the problem. The ateological contingency of the future means that no options can be taken off the table. Democratic responses are coopted, compromised and insufficient in themselves. Distributing agency requires a complement of sovereign planning and control. Their reliance on democracy is a fetish or wounded attachment insufficient to the intensities and singularities of technological society. Even executive action can take part in creativity engagements with the future.**

Alex **Wiliams** **and** Nick **Srnicek**, PhD Candidates in International Relations at the London School of Economics, “#ACCERLATE MANIFESTO for an Acceleration Politics,” May 14, **2013**, <http://criticallegalthinking.com/2013/05/14/accelerate-manifesto-for-an-accelerationist-politics/>

12. **We do not believe that dir­ect action is suf­fi­cient to achieve any of this**. **The habitual tac­tics** of march­ing, hold­ing signs, and estab­lish­ing tem­por­ary autonom­ous zones r**isk becom­ing com­fort­ing sub­sti­tutes for effect­ive suc­cess.** “**At least we have done some­thing” is the ral­ly­ing cry of those who priv­ilege self- esteem rather than effect­ive action.** **The only cri­terion of a good tac­tic is whether it enables sig­ni­fic­ant suc­cess or not.** **We must be done with fet­ish­ising par­tic­u­lar modes of action. Polit­ics must be treated as a set of dynamic sys­tems, riven with con­flict, adapt­a­tions and counter- adaptations, and stra­tegic arms races. This means that each indi­vidual type of polit­ical action becomes blun­ted and inef­fect­ive over time as the other sides adapt. No given mode of polit­ical action is his­tor­ic­ally invi­ol­able.** Indeed, over time, **there is an increas­ing need to dis­card famil­iar tac­tics as the forces and entit­ies they are mar­shalled against learn to defend and counter- attack them effect­ively.**

**It is in part the con­tem­por­ary left’s inab­il­ity to do so which lies close to the heart of the con­tem­por­ary malaise**.¶ 13. **The over­whelm­ing priv­ileging of democracy- as- process needs to be left behind**. **The fet­ish­isa­tion of open­ness, hori­zont­al­ity, and inclu­sion of much of today’s ‘rad­ical’ left set the stage for inef­fect­ive­ness. Secrecy, ver­tic­al­ity, and exclu­sion all have their place as well in effect­ive polit­ical action** (though not, of course, an exclus­ive one).¶ 14. Demo­cracy can­not be defined simply by its means — not via vot­ing, dis­cus­sion, or gen­eral assem­blies. **Real demo­cracy must be defined by its goal — col­lect­ive self- mastery. This is a pro­ject which must align polit­ics with the leg­acy of the Enlight­en­ment, to the extent that it is only through har­ness­ing our abil­ity to under­stand ourselves and our world bet­ter** (our social, tech­nical, eco­nomic, psy­cho­lo­gical world) **that we can come to rule ourselves. We need to posit a col­lect­ively con­trolled legit­im­ate ver­tical author­ity in addi­tion to dis­trib­uted hori­zontal forms of social­ity, to avoid becom­ing the slaves of either a tyr­an­nical total­it­arian cent­ral­ism or a capri­cious emer­gent order bey­ond our con­trol. The com­mand of The Plan must be mar­ried to the impro­vised order of The Network.**

#### The two are incompatible-they operate at different speeds- introducing the hesitations of relentless horizontalism builds in failure from the beginning.

Alex Wiliams and Nick Srnicek, PhD Candidates in International Relations at the London School of Economics, “#ACCERLATE MANIFESTO for an Acceleration Politics,” May 14, 2013, <http://criticallegalthinking.com/2013/05/14/accelerate-manifesto-for-an-accelerationist-politics/>

We believe the most import­ant divi­sion in today’s left is between those that hold to a folk polit­ics of loc­al­ism**,** dir**­**ectaction**,** and relent­less hori­zont­al­ism, and those that out­line what must become called an accel­er­a­tion­ist polit­ics at ease with a mod­ern­ity of abstrac­tion, com­plex­ity, glob­al­ity, and tech­no­logy. The former remains con­tent with estab­lish­ing small and tem­por­ary spaces of non- capitalist social rela­tions, eschew­ing the real prob­lems entailed in facing foes which are intrins­ic­ally non- local, abstract, and rooted deep in our every­day infra­struc­ture. The fail­ure of such polit­ics has been built- in from the very begin­ning. By con­trast, an accel­er­a­tion­ist polit­ics seeks to pre­serve the gains of late cap­it­al­ism while going fur­ther than its value sys­tem, gov­ernance struc­tures, and mass patho­lo­gies will allow.¶ 2. All of us want to work less. It is an intriguing ques­tion as to why it was that the world’s lead­ing eco­nom­ist of the post- war era believed that an enlightened cap­it­al­ism inev­it­ably pro­gressed towards a rad­ical reduc­tion of work­ing hours. In The Eco­nomic Pro­spects for Our Grand­chil­dren (writ­ten in 1930), Keynes fore­cast a cap­it­al­ist future where indi­vidu­als would have their work reduced to three hours a day. What has instead occurred is the pro­gress­ive elim­in­a­tion of the work- life dis­tinc­tion, with work com­ing to per­meate every aspect of the emer­ging social factory.¶ 3. Cap­it­al­ism has begun to con­strain the pro­duct­ive forces of tech­no­logy, or at least, dir­ect them towards need­lessly nar­row ends. Pat­ent wars and idea mono­pol­isa­tion are con­tem­por­ary phe­nom­ena that point to both capital’s need to move bey­ond com­pet­i­tion, and capital’s increas­ingly ret­ro­grade approach to tech­no­logy. The prop­erly accel­er­at­ive gains of neo­lib­er­al­ism have not led to less work or less stress. And rather than a world of space travel, future shock, and revolu­tion­ary tech­no­lo­gical poten­tial, we exist in a time where the only thing which devel­ops is mar­gin­ally bet­ter con­sumer gad­getry. Relent­less iter­a­tions of the same basic product sus­tain mar­ginal con­sumer demand at the expense of human acceleration.¶ 4. We do not want to return to Ford­ism. There can be no return to Ford­ism. The cap­it­al­ist “golden era” was premised on the pro­duc­tion paradigm of the orderly fact­ory envir­on­ment, where (male) work­ers received secur­ity and a basic stand­ard of liv­ing in return for a life­time of stul­ti­fy­ing bore­dom and social repres­sion. Such a sys­tem relied upon an inter­na­tional hier­archy of colon­ies, empires, and an under­developed peri­phery; a national hier­archy of racism and sex­ism; and a rigid fam­ily hier­archy of female sub­jug­a­tion. For all the nos­tal­gia many may feel, this régime is both undesir­able and prac­tic­ally impossible to return to.¶ 5. Accel­er­a­tion­ists want to unleash lat­ent pro­duct­ive forces. In this pro­ject, the mater­ial plat­form of neo­lib­er­al­ism does not need to be des­troyed. It needs to be repur­posed towards com­mon ends. The exist­ing infra­struc­ture is not a cap­it­al­ist stage to be smashed, but a spring­board to launch towards post- capitalism.

### Accidents Defense 2NC

#### FIRST, No risk of Accidents for US or Russia

Dr. Leonid **Ryabikhin et all** (Executive Secretary, Committee of Scientist for Global Security and Arms Control; Senior Fellow, EastWest Institute), General (Ret.) Viktor Koltunov (Deputy Director, Institute for Strategic Stability of Rosatom), and Dr. Eugene Miasnikov (Senior Research Scientist, Center for Arms Control, Energy and Environmental Studies) “De-alerting: Decreasing the Operational Readiness of Strategic Nuclear Forces” Discussion paper presented at the seminar on “Re-framing De-Alert: Decreasing the Operational Readiness of Nuclear Weapons Systems in the U.S.-Russia Context” in Yverdon, Switzerland, 21-23 June 200**9**. http://www.ewi.info/system/files/RyabikhinKoltunovMiasnikov.pdf

Most of the experts define de-alerting as implementing some reversible physical changes in a weapon system that would significantly increase time between the decision to use the weapon and the actual moment of its launch. The proponents of this concept consider it as one of the ways to maintain strategic stability. They provide the following arguments in support of this concept. Radical changes have occurred in US-Russian relations. Russia and the United States are building strategic partnership relationship. In such situation the high alert readiness of strategic offensive forces targeted at each other does not correspond to the character of our relations. Strategic nuclear forces high alert readiness in combination with a concept of launch-on-warning strike increases the risk of “accidental” nuclear war (as a result of mistakes in the C3I system, inadequate situation analysis, mistaken decision-making, unauthorized action of personnel or even terrorists, provocation from the “third” states or non-state actors, etc.); False signals about missile attacks obtained from early warning system that may trigger an accidental launch. This assumption was very popular when the Russian early warning system was weakened as a result of collapse of the Soviet Union. Analysis of the above arguments shows, that they do not have solid grounds. Today Russian and U.S. ICBMs are not targeted at any state. High alert status of the Russian and U.S. strategic nuclear forces has not been an obstacle for building a strategic partnership. The issue of the possibility of an “accidental” nuclear war itself is hypothetical. Both states have developed and implemented constructive organizational and technical measures that practically exclude launches resulting from unauthorized action of personnel or terrorists. Nuclear weapons are maintained under very strict system of control that excludes any accidental or unauthorized use and guarantees that these weapons can only be used provided that there is an appropriate authorization by the national leadership. Besides that it should be mentioned that even the Soviet Union and the United States had taken important bilateral steps toward decreasing the risk of accidental nuclear conflict. Direct emergency telephone “red line” has been established between the White House and the Kremlin in 1963. In 1971 the USSR and USA signed the Agreement on Measures to Reduce the Nuclear War Threat. This Agreement established the actions of each side in case of even a hypothetical accidental missile launch and it contains the requirements for the owner of the launched missile to deactivate and eliminate the missile. Both the Soviet Union and the United States have developed proper measures to observe the agreed requirements.

#### More Proof: Missiles default to hitting oceans.

Walter B. **Slocombe**, J.D. Harvard Law, Former Under Secretary of Defense for Policy and Senior advisor for the Coalition Provisional Authority in Baghdad, 21-23 June 20**09**, “De-Alerting: Diagnoses, Prescriptions, and Side-Effects\*” Discussion paper presented at the seminar on “Re-framing De-Alert: Decreasing the Operational Readiness of Nuclear Weapons Systems in the U.S.-Russia Context” in Yverdon, Switzerland http://www.ewi.info/system/files/Slocombe.pdf

Moreover, in recent years, both the US and Russia, as well as Britain and China, have modified their procedures so that even if a nuclear-armed missile were launched, it would go not to a “real” target in another country but – at least in the US case - to empty ocean. In addition to the basic advantage of insuring against a nuclear detonation in a populated area, the fact that a missile launched in error would be on flight path that diverged from a plausible attacking trajectory should be detectable by either the US or the Russian warning systems, reducing the possibility of the accident being perceived as a deliberate attack. De-targeting, therefore, provides a significant protection against technical error.5

**Cyber war infeasible**

**Clark**, MA candidate – Intelligence Studies @ American Military University, senior analyst – Chenega Federal Systems, 4/28/’**12** (Paul, “The Risk of Disruption or Destruction of Critical U.S. Infrastructure by an Offensive Cyber Attack,” American Military University)

The Department of **Homeland Security worries** that **our critical infrastructure and key resources** (CIKR) **may be exposed**, both directly and indirectly, **to** multiple **threats because of** CIKR **reliance on** the global **cyber infrastructure**, an infrastructure that is **under routine cyberattack by a “spectrum of malicious actors**” (National Infrastructure Protection Plan 2009). **CIKR** in the extremely large and complex U.S. economy **spans multiple sectors including** agricultural, finance and banking, dams and water resources, public health and emergency services, **military** and **defense**, transportation and shipping, **and energy** (National Infrastructure Protection Plan 2009). The disruption and destruction of public and private infrastructure is part of warfare, without this infrastructure conflict cannot be sustained (Geers 2011). Cyber-attacks are desirable because they are considered to be a relatively “low cost and long range” weapon (Lewis 2010), but **prior to** the creation of **Stuxnet**, the first cyber-weapon, **the ability to disrupt and destroy critical infrastructure through cyber-attack was theoretical. The movement of an offensive cyber-weapon from conceptual to actual has forced the U**nited **S**tates **to question whether offensive cyber-attacks are a significant threat** that are able to disrupt or destroy CIKR to the level that national security is seriously degraded. It is important to understand the risk posed to national security by cyber-attacks to ensure that government responses are appropriate to the threat and balance security with privacy and civil liberty concerns. **The risk** posed **to CIKR from cyber-attack can be evaluated by measuring the threat from cyber-attack against the vulnerability of a** CIKR **target and the consequences of** CIKR **disruption.** As the only known cyber-weapon, **Stuxnet has been thoroughly analyzed** **and used as a model for predicting future cyber-weapons. The U.S. electrical grid**, a key component in the CIKR energy sector, is a target that **has been analyzed for vulnerabilities** and the consequences of disruption predicted – **the electrical grid has been used in multiple attack scenarios** including a classified scenario provided to the U.S. Congress in 2012 (Rohde 2012). Stuxnet will serve as the weapon and the U.S. electrical grid will serve as the target in **this risk analysis** that **concludes that there is a low risk of disruption or destruction of critical infrastructure** from a an offensive cyber-weapon **because of the complexity of the attack path, the limited capability of non-state adversaries to develop cyber-weapons, and the existence of multiple methods of mitigating** the cyber-**attacks.** To evaluate the threat posed by a Stuxnet-like cyber-weapon, the complexity of the weapon, the available attack vectors for the weapon, and the resilience of the weapon must be understood. The complexity – how difficult and expensive it was to create the weapon – identifies the relative cost and availability of the weapon; inexpensive and simple to build will be more prevalent than expensive and difficult to build. Attack vectors are the available methods of attack; the larger the number, the more severe the threat. For example, attack vectors for a cyberweapon may be email attachments, peer-to-peer applications, websites, and infected USB devices or compact discs. Finally, the resilience of the weapon determines its availability and affects its usefulness. A useful weapon is one that is resistant to disruption (resilient) and is therefore available and reliable. These concepts are seen in the AK-47 assault rifle – a simple, inexpensive, reliable and effective weapon – and carry over to information technology structures (Weitz 2012). The evaluation of **Stuxnet** identified **malware** that **is** “**unusually complex and large” and required code written in multiple languages** (Chen 2010**) in order to complete** a variety of **specific functions contained in a “vast array” of components** – **it is one of the most complex threats ever analyzed by Symantec** (Falliere, Murchu and Chien 2011). **To be successful, Stuxnet required a high level of technical knowledge across multiple disciplines**, **a laboratory with** the **target equipment configured for testing, and a foreign intelligence capability to collect information on the target network and attack vectors** (Kerr, Rollins and Theohary 2010). **The malware also needed careful monitoring and maintenance** because it could be easily disrupted; as a result **Stuxnet** was developed with a high degree of configurability and **was upgraded multiple times in less than one year** (Falliere, Murchu and Chien 2011). **Once introduced into the network, the** cyber-**weapon** then **had to utilize four known vulnerabilities and four unknown vulnerabilities**, known as zero-day exploits, **in order to install itself and propagate** across the target network (Falliere, Murchu and Chien 2011). **Zero-day exploits are incredibly difficult to find** and **fewer than twelve out of** the **12,000,000 pieces of malware** discovered each year **utilize zero-day exploits** and this rarity makes them valuable, **zero-days can fetch** $50,000 to **$500,000 each on the black market** (Zetter 2011). The **use of four rare exploits in a single piece of malware is “unprecedented”** (Chen 2010). Along with the use of four unpublished exploits, **Stuxnet** also **used the “first ever” programmable logic controller** rootkit, a Windows rootkit, antivirus evasion techniques, **intricate process injection routines, and other complex interfaces** (Falliere, Murchu and Chien 2011) all **wrapped up in “layers of encryption** like Russian nesting dolls” (Zetter 2011) – including custom encryption algorithms (Karnouskos 2011). As the **malware** spread across the now-infected network it **had to utilize** additional **vulnerabilities in** proprietary Siemens industrial control **software** (ICS) **and hardware** used to control the equipment it was designed to sabotage. **Some of these** ICS **vulnerabilities were** published but some were **unknown and required such a high degree of inside knowledge** **that there was speculation that a Siemens employee had been involved in the malware design** (Kerr, Rollins and Theohary 2010). The **unprecedented technical complexity of** the **Stuxnet** cyber-weapon, along with the extensive technical and financial resources and foreign intelligence capabilities required for its development and deployment, **indicates** that the **malware was likely developed by a nation-state** (Kerr, Rollins and Theohary 2010). Stuxnet had very limited attack vectors. When a computer system is connected to the public Internet a host of attack vectors are available to the cyber-attacker (Institute for Security Technology Studies 2002). Web browser and browser plug-in vulnerabilities, cross-site scripting attacks, compromised email attachments, peer-to-peer applications, operating system and other application vulnerabilities are all vectors for the introduction of malware into an Internetconnected computer system. **Networks that are not connected to the public internet are “air gapped,”** a technical colloquialism to identify a physical separation between networks. **Physical separation from the public Internet is a common safeguard for sensitive networks including** classified **U.S. government networks. If the target network is air gapped, infection can only occur through physical means – an infected disk or USB device** that **must be physically introduced** into a possibly access controlled environment and connected to the air gapped network. The first step of the Stuxnet cyber-attack was to initially infect the target networks, a difficult task given the probable disconnected and well secured nature of the Iranian nuclear facilities. **Stuxnet was introduced via a USB** device to the target network, **a method that suggests that the attackers were familiar with the configuration of the network** and knew it was not connected to the public Internet (Chen 2010). This assessment is supported by two rare features in Stuxnet – having all necessary functionality for industrial sabotage fully embedded in the malware executable along with the ability to self-propagate and upgrade through a peer-to-peer method (Falliere, Murchu and Chien 2011). **Developing an understanding of the target network** configuration **was a significant and daunting task based on** Symantec’s **assessment that Stuxnet repeatedly targeted** a total of **five different organizations over nearly one year** (Falliere, Murchu and Chien 2011) **with physical introduction** via USB drive **being the only available attack vector.** The final factor in assessing the threat of a cyber-weapon is the resilience of the weapon. There are **two** primary **factors** that **make Stuxnet non-resilient**: the **complexity of the weapon and the complexity of the target. Stuxnet** was highly customized for sabotaging specific industrial systems (Karnouskos 2011) and **needed a large number of very complex components and routines** in order to increase its chance of success (Falliere, Murchu and Chien 2011). The **malware required eight vulnerabilities** in the Windows operating system **to succeed** and therefore would have failed if those vulnerabilities had been properly patched; four of the eight vulnerabilities were known to Microsoft and subject to elimination (Falliere, Murchu and Chien 2011). **Stuxnet also required** that two drivers be installed and required **two stolen security certificates for installation** (Falliere, Murchu and Chien 2011); driver installation would have failed if the stolen certificates had been revoked and marked as invalid. Finally, the configuration of systems is ever-changing as components are upgraded or replaced. **There is no guarantee that the network that was mapped for vulnerabilities had not changed in the months**, or years, **it took to craft Stuxnet** and successfully infect the target network. **Had specific components** of the target hardware **changed** – the targeted Siemens software or programmable logic controller – **the attack would have failed. Threats are less of a threat when identified**; this is why zero-day exploits are so valuable. **Stuxnet went to great lengths to hide its existence** from the target and utilized multiple rootkits, data manipulation routines, and virus avoidance techniques to stay undetected. The malware’s actions occurred only in memory to avoid leaving traces on disk, it masked its activities by running under legal programs, employed layers of encryption and code obfuscation, and uninstalled itself after a set period of time, all efforts to avoid detection because its authors knew that detection meant failure. **As a result of the complexity of the malware, the changeable nature of the target network, and the chance of discovery**, **Stuxnet is not a resilient system.** **It is a fragile weapon that required an investment of time and money** to constantly monitor, reconfigure, test and deploy **over the course of a year. There is concern,** with Stuxnet developed and available publicly, **that the world is on the brink of** a storm of **highly sophisticated** Stuxnet-derived **cyber-weapons which can be used by hackers, organized criminals and terrorists** (Chen 2010). As former counterterrorism advisor Richard Clarke describes it, there is concern that the technical brilliance of the United States “has created millions of potential monsters all over the world” (Rosenbaum 2012). Hyperbole aside, technical knowledge spreads. **The techniques behind cyber-attacks are “constantly evolving and making use of lessons learned over time**” (Institute for Security Technology Studies 2002) and the **publication of the Stuxnet code may make it easier** to copy the weapon (Kerr, Rollins and Theohary 2010). **However**, this is something of a zero-sum game because **knowledge works both ways** **and cyber-security techniques are also evolving**, and “understanding attack techniques more clearly is the first step toward increasing security” (Institute for Security Technology Studies 2002). **Vulnerabilities are discovered and patched, intrusion detection and malware signatures are expanded and updated, and monitoring and analysis** processes and methodologies **are expanded and honed.** **Once the element of surprise is lost, weapons and tactics are less useful**, this is the core of the argument that “uniquely surprising” **stratagems like Stuxnet are single-use**, **like Pearl Harbor and the Trojan Horse**, the “very **success** [of these attacks] **precludes** their **repetition**” (Mueller 2012). **This** paradigm **has already been seen in** the “son of Stuxnet” malware – named **Duqu** by its discoverers – that is based on the same modular code platform that created Stuxnet (Ragan 2011). **With** the **techniques used by Stuxnet now known**, other **variants** **such as Duqu are being discovered and countered by security researchers** (Laboratory of Cryptography and System Security 2011). It is obvious that **the effort required to create, deploy, and maintain Stuxnet and its variants is massive and it is not clear that the rewards are worth the risk and effort.** Given the location of initial infection and the number of infected systems in Iran (Falliere, Murchu and Chien 2011) it is believed that Iranian nuclear facilities were the target of the Stuxnet weapon. **A significant amount of money and effort was invested in** creating **Stuxnet but** yet **the expected result** – assuming that this was an attack that expected to damage production – **was minimal at best.** Iran claimed that **Stuxnet caused only minor damage**, probably at the Natanz enrichment facility, the Russian contractor Atomstroyeksport reported that no damage had occurred at the Bushehr facility, and an unidentified “senior diplomat” suggested that Iran was forced to shut down its centrifuge facility “for a few days” (Kerr, Rollins and Theohary 2010). **Even the most optimistic estimates believe that Iran’s nuclear enrichment program was only delayed by months**, or perhaps years (Rosenbaum 2012). The actual damage done by Stuxnet is not clear (Kerr, Rollins and Theohary 2010) and the primary damage appears to be to a higher number than average replacement of centrifuges at the Iran enrichment facility (Zetter 2011). Different targets may produce different results. The Iranian nuclear facility was a difficult target with limited attack vectors because of its isolation from the public Internet and restricted access to its facilities. **What is the probability of a successful attack against the U.S. electrical grid** and what are the potential consequences should this critical infrastructure be disrupted or destroyed? An attack against the electrical grid is a reasonable threat scenario since **power systems are “a high priority target for military and insurgents**” and there has been a trend towards utilizing commercial software and integrating utilities into the public Internet that has “increased vulnerability across the board” (Lewis 2010). **Yet** the **increased vulnerabilities are mitigated by** an **increased detection and deterrent capability** that has been “**honed over many years of practical application” now that power systems are using standard, rather than proprietary and specialized, applications and components** (Leita and Dacier 2012). The **security of the** electrical **grid is also enhanced by increased awareness after a smart-grid hacking demonstration in 2009 and the identification of the Stuxnet malware** in 2010; as a result **the public and private sector are working together in an “unprecedented effort” to establish robust security guidelines** and cyber security measures (Gohn and Wheelock 2010).

### Cyberattacks- Speed

#### Speed in cyberspace doesn’t cause escalation – their impacts are hype.

Valeriano, Lecturer in Social and Political Sciences at the University of Glasgow, and Maness, Ph.D. candidate at the University of Illinois at Chicago, 11-21-12

(Brandon and Ryan, “The Fog of Cyberwar,” http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar?page=show, accessed 12-16-12, CMM)

In mid-2010, thousands of centrifuges, enriching uranium at Iranian nuclear research facilities, spun out of control. The instruments were mysteriously reprogrammed to operate faster than normal, pushing them to the breaking point. Iranian computer systems, however, inexplicably reported that the centrifuges were operating normally. This incident, it was later revealed, was the work of the infamous Stuxnet computer worm, presumed to be the creation of the United States and Israel, and one of the most sophisticated cyberweapons to date. The infiltration was initially thought to have set back Iran’s suspected nuclear weapons program three to five years, although current estimates are in the range of two years to a few months.¶ Stuxnet was followed by the Flame virus: a new form of malware that infiltrated several networks in Iran and across the Middle East earlier this year. Flame copied text, recorded audio, and deleted files on the computers into which it hacked. Israel and the United States are again the suspected culprits but deny responsibility.¶ These two attacks generated substantial buzz in the media and among policymakers around the world. Their dramatic nature led some experts to argue that cyberwarfare will fundamentally change the future of international relations, forcing states to rethink their foreign policy. In a speech to the New York business community on October 11, 2012, U.S. Defense Secretary Leon Panetta expressed fear that a cyber version of Pearl Harbor might take the United States by surprise in the near future. He warned that the U.S. government, in addition to national power grids, transportation systems, and financial markets, are all at risk and that cyberdefense should be at the top of the list of priorities for President Barack Obama’s second term.¶ The Stuxnet and Flame attacks, however, are not the danger signs that some have made them out to be. First of all, the viruses needed to be physically injected into Iranian networks, likely by U.S. or Israeli operatives, suggesting that the tactic still requires traditional intelligence and military operation methods. Second, Stuxnet derailed Iran’s nuclear program for only a short period, if at all. And Flame did nothing to slow Iran’s nuclear progression directly, because it seems to have been only a data-collection operation.¶ Some cyberattacks over the past decade have briefly affected state strategic plans, but none has resulted in death or lasting damage. For example, the 2007 cyberattacks on Estonia by Russia shut down networks and government websites and disrupted commerce for a few days, but things swiftly went back to normal. The majority of cyberattacks worldwide have been minor: easily corrected annoyances such as website defacements or basic data theft -- basically the least a state can do when challenged diplomatically.¶ Our research shows that although warnings about cyberwarfare have become more severe, the actual magnitude and pace of attacks do not match popular perception. Only 20 of 124 active rivals -- defined as the most conflict-prone pairs of states in the system -- engaged in cyberconflict between 2001 and 2011. And there were only 95 total cyberattacks among these 20 rivals. The number of observed attacks pales in comparison to other ongoing threats: a state is 600 times more likely to be the target of a terrorist attack than a cyberattack. We used a severity score ranging from five, which is minimal damage, to one, where death occurs as a direct result from cyberwarfare. Of all 95 cyberattacks in our analysis, the highest score -- that of Stuxnet and Flame -- was only a three.¶ To be sure, states should defend themselves against cyberwarfare, but throwing vast amounts of money toward a low-level threat does not make sense. The Pentagon estimates it spent $2.6 to $3.2 billion on cybersecurity in fiscal year 2012. And it is likely that such spending will only increase. The U.S. Air Force alone anticipates spending $4.6 billion on cybersecurity in the next year. Even if the looming “fiscal cliff” guts the Defense Department’s budget, Panetta has made clear that cybersecurity will remain a top funding priority. At a New York conference on October 12, 2012, he described the United States as being in a “pre-9/11 moment” with regards to cyberwarfare and said that the “attackers are plotting,” in reference to the growing capabilities of Russia, China, and Iran.¶ Of the 20 ongoing interstate rivals in our study, China and the United States cybertargeted each other the most. According to our study, Beijing attacked U.S. assets 18 times and Washington returned fire twice. Two notable attacks were the 2011 Pentagon raid, which stole sensitive files from the Defense Department, and the 2001 theft of Lockheed Martin’s F-35 fighter-jet schematics. These attacks get only a moderate severity score because they targeted specific, nonessential state documents and were not intended to affect the general public. Over the same time span, India and Pakistan targeted each other 11 times (India five times, Pakistan six), as did North and South Korea, with North Korea being the aggressor ten times and South Korea launching one return attack. These ranged from minor incidents, such as Pakistan defacing an Indian government website, to more serious ones, such as North Korea stealing sensitive state documents from South Korea.¶ Israeli-Iranian tensions have risen in recent months, but despite all the talk, this conflict is not playing out in the cybersphere. There were only eight cyberattacks between these states from 2001 to 2011, four launched by Israel, four by Iran. Although Stuxnet and Flame were more severe, Iranian attempts to disrupt government websites have not been very sophisticated. And Israel’s near-insistence on an armed conventional attack proves that even the most sophisticated cyberattacks are not changing state behavior.¶ Cyberattacks are rare, and when they do occur, states are cautious in their use of force. A

s with conventional and nuclear conflict, some of the principles of deterrence and mutually assured destruction apply. Any aggressor in cyberspace faces the acute threat of blowback: having techniques replicated and repeated against the initiator. Once developed, a cyberweapon can easily be copied and used by a tech-savvy operative with access to a critical system such as the Defense Department’s network, which foreign-government hackers have had success infiltrating.¶ Far from making interstate cyberwarfare more common, the ease of launching an attack actually keeps the tactic in check. Most countries’ cyberdefenses are weak, and a state trying to exploit an adversary’s weakness may be similarly vulnerable, inviting easy retaliation. An unspoken but powerful international norm against civilian targets further limits the terms of cyberwarfare.¶ The United States and other responsible powers should restrain their use of the tactic in order to avoid escalation. Attacks such as Flame and Stuxnet are dangerous because they break down the standard of mutually beneficial restraint. These attacks caused little damage in the end, but they still may have encouraged other states to bulk up their own capabilities. The main danger is that one state will overuse the tactic and push other states to do the same.¶ There is also concern that some countries will overreact to the cyberthreat by clamping down on the freedoms that make the Internet an open and dynamic space. A paranoid government might be tempted to develop extreme defenses, such as a kill switch, that would allow it to shut down all incoming and outgoing cybertraffic. Such a drastic step would have a chilling effect on society, creating more problems than it would solve. This is yet another reason why international standards and communication are crucial.¶ Cooperation on the cyberwar threat originated in an unlikely place: Estonia. A tiny country with a population of just over one million, it has become a global leader in promoting cyberspace rules and norms that keep states, democratic and autocratic alike, in line. Estonia was thrust into the spotlight after the 2007 cyberattack by and subsequent widespread international condemnation of Russia. Instead of lashing out against its attacker, the small state sought a world forum to discuss its case; since then, it has hosted the International Conference on Cyber Conflict four times. This conference is an outcropping of NATO and hosts countries such as the United States, Canada, the United Kingdom, France, Germany, and Italy.¶ The gatherings have successfully promoted the adoption of norms and modes of restrained behavior in cyberspace. Developments include the agreement that territorial sovereignty applies to a state’s cyberspace, and that cyberwarfare is covered by Article 51 of the UN Charter, which allows a state to take action in response to an attack. Along these same lines, cyberattacks are now being categorized on an intensity scale to help determine what a proper international response might be.

## 1NR

#### Government is not the people

Costello and Thomas 2K

(George A. and Kenneth R., Congressional Research Service, The Constitution of the United States of America: Analysis and Interpretation, http://caselaw.lp.findlaw.com/data/constitution~preamble/#annotations)

Article Text I Annotations We the People of the United States. in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America. Annotations PURPOSE AND EFFECT OF THE PREAMBLE Although the preamble is not a source of power for any department of the Federal Government, 1 the Supreme Court has often referred to it as evidence of the origin, scope, and purpose of the Constitution. 2 "Its true office," wrote Joseph Story in his COMMENTARIES, "is to expound the nature and extent and application of the powers actually conferred by the Constitution, and not substantively to create them. For example, the preamble declares one object to be, 'to provide for the common defense.'

#### Even if words have no absolute meaning, it’s possible to assign them meaning—evaluate language situationally—terms have a particular meaning in the context of debate

**Knops**, Sociology – University of Birmingham, ‘**7**

(Andrew, “Debate: Agonism as Deliberation – On Mouffe's Theory of Democracy,” Journal of Political Philosophy, Vol. 15, Iss. 1, March)

As Pitkin explains, Wittgenstein's version of language suggests that we learn terms through practice. The traditional account of language learning views it as the process of associating a term, for example a name, with a particular object or picture of that object in our heads. We can then apply that name when we encounter the object again. We associate a definition with that name, and it becomes a label for the object. While language can be learned and used in this way, Wittgenstein argues that this is a very limited account, which only explains a small section of what we use language to do. What about learning the words ‘trust’, ‘spinster’ or ‘envy’? He therefore develops a more comprehensive account of language learning which sees it as a particular practice. We learn to use a particular phrase in a particular context. Having heard its use in a context before, we hear it repeated in similar circumstances. We therefore learn to associate it with aspects of those circumstances, and to reproduce and use it in those circumstances for ourselves. So, for example, the (polite!) child learns that “Please may I have the marmalade?” results in the person who uttered it being passed the marmalade. They make the same sounds, and they are themselves passed the marmalade. They later learn that “Please may I have the jam?” leads to their being passed the jam. Finally, they understand that “Please may I have x?” will lead to their being given whatever they choose to substitute for x. This example is helpful because it shows how the meaning of a word can be refined through its use. It may be that a child initially only associates “Please may I have . . .” with marmalade. It is only when the same words are used to elicit the passing of another object – in our example, jam – that they associate it with that other object, and then eventually, after several iterations, with any object. This process may also involve them using the phrase, and projecting it into new contexts of their own. It may also, of course, involve them making mistakes, which are then corrected. Because words are developed through repeated use in this way, they rarely have settled meanings. By applying them to new contexts, we can use them to focus on different aspects of meaning. Pitkin suggests the example of ‘feed the monkey’ and ‘feed the meter’. Prior to such application, however, we may only have had a vague idea of the word's meaning, gathered through past usage. In most, if not all, cases this process is ongoing. So words are learned through a kind of ‘training’ or ‘practice’, and learning or understanding a word is an activity that involves using the word in the correct situation. It is not a case of applying a clear-cut rule to a definite situation. Because words develop through practices and their use in particular situations, and in many cases we continue to develop their meaning through such use, very rarely will a term have a single, fixed meaning. Rather, Wittgenstein argues, the different situations in which such a general term is used are like separate language games. Just like moves in a game, words that have meaning when used in one situation may be meaningless when used in another. For example, we cannot talk of ‘checking the King’ in football. While there are connections between games, they are linked like members of a family: some share the same colour eyes, others the same shape of nose, others the same colour hair, but no two members have all the same features. Wittgenstein also uses the analogy of an historic city to show how language builds up. While some areas may be uniform, many have been added to higgledy-piggledy, with no clear pattern over how streets are laid out, or which run into which. Wittgenstein therefore argues that it is impossible to assimilate the operation of all language to a single model, such as the ‘picture theory’ or label model of meaning. Different language games have different rules, and we can only discover these by investigating particular practices of use in specific cases. However, Wittgenstein concedes that there must be some kind of regularity to our use of words. Without some form of consistency, we could not know that our use of a word in a new context was supposed to indicate or evoke a similar context in which the word had been used in the past. That words do so, Wittgenstein argues, is due to their basis in activity– they are used by us in certain situations – and that such use is grounded ultimately in activities that are *shared* by groups of us, or all of us. Cavell sums this up well when he says: We learn and teach words in certain contexts, and then we are expected, and expect others, to be able to project them into further contexts. Nothing insures that this projection will take place, just as nothing insures that we will make, and understand, the same projections. That on the whole we do is a matter of our sharing routes of interest and feeling, modes of response, senses of humour and of significance and of fulfilment, of what is outrageous, of what is similar to what else, what a rebuke, what forgiveness, of when an utterance is an assertion, when an appeal, when an explanation – all the whirl of organism Wittgenstein calls ‘forms of life’. These forms of life are not so much constituted by, but constitute, language. They serve as its ‘ground’. Therefore, although the process of explaining a term, and of reasoning in language, may continue up to a point, it will always come to an end and have to confront simple agreement in activity, ways of going on, or forms of life. Mouffe sees this account as ruling out the possibility of rational consensus. Following Tully, she argues that the fact that arguments are grounded in agreement in forms of life, which constitute a form of practice marking the end point of explanation or reasons, means that all attempts at rational argument must contain an irrational, practical element. Neither is it possible to suggest, as she accuses Peter Winch of doing, that we can see forms of life as some underlying regularity, which argument or reasoning can then make explicit. Again with Tully, she contends that the ‘family resemblance’ or ‘historic city’ analogy for the development of language shows it to be far too varied and idiosyncratic for such an account. Yet I would like to argue that Wittgenstein's theory as characterised above does not rule out rational argument, and the possibility of consensus, at least in principle. Wittgenstein himself characterises the offering of reasons as a kind of ‘explanation’. This much is granted by Tully. Explanations are requested by someone unfamiliar with a practice, who would like to understand that practice. Wittgenstein sees this as a completely legitimate use of language and reason. This is not surprising, as this process of explanation is precisely the form of language learning that he sets out. A person uses a term based on their understanding of its use from their past experiences. This projection either meets with the predicted response, or a different one. If the latter, the person modifies their understanding of the term. It is only when we go further, and assume that there can be an explanation for every kind of confusion, every kind of doubt, that we get into trouble. But this is precisely not what a deliberative theory of reasoning holds. A deliberative theory of reasoning models communicative reason – reason used to develop mutual understanding between two or more human beings. To this extent, the truths that it establishes are relative, though intersubjective. They hold, or are useful for, the collectivity that has discursively constructed them. They do not claim to be objective in an absolute sense, although the concept can be extended, in theory, to cover all people and hence to arrive as closely as possible to the notion of an absolute. The process that Habermas calls ‘practical discourse’ and the process that Wittgenstein calls ‘explanation’ are basically one and the same. Both are synonyms for deliberation. Habermas sees the essentially rational nature of language as the capacity for a statement to be rejected, in the simplest case with a ‘no’. It is with this response that the request for reasons, latent in all rational statements, is activated. If we widen the sense of rejection meant by Habermas beyond the paradigm case of the utterance of a ‘no’ to the broader case of a failure to elicit an expected response, we can see the similarities between Habermas’ notion of deliberation and Wittgenstein's concept of explanation. Like Wittgenstein, Habermas sees ‘normal’ language use as taking place against a backdrop of conventionally shared meanings or understandings. It is only when this assumption breaks down, when the response differs from what was expected, that deliberation is required. Shared understandings and usage are established anew, through a dialogical sharing of reasons, or explanations, which repairs the assumption that we do use these words in similar ways.