# D6 Districts Round 1 v Emory KL

## 1NC

### 1NC CP

#### Great power war is a myth. The 1AC recreates stereotypes of fear and conflict that produce inaccurate scholarship and entrench a systemically flawed political methodology.

Kaldor 13, Mary Kaldor, professor of Global Governance at the London School of Economics and Director of the Civil Society and Human Security Research Unit, “In Defence of New Wars,” March 7, 2013, Stability, 2(1): 4, pp. 1-16, <http://www.stabilityjournal.org/article/download/sta.at/40%E2%80%8E>

The most common criticism of the ‘new wars’ argument is that new wars are not new. It is argued that the Cold War clouded our ability to analyse ‘small wars’ or ‘low-intensity wars’, that many of the characteristics of new wars associated with weak states can be found in the early modern period and that phenomena like banditry, mass rape, forced population displacement, or atrocities against civilians all have a long history. Of course this is true. Many of the features of new wars can be found in earlier wars. Of course the dominance of the East-West conflict obscured other types of conflict. But there is an important reason, which is neglected by the preoccupation with empirical claims, for insisting on the adjective ‘new’. Critics of the ‘new wars’ thesis often concede that what is useful about the analysis of ‘new wars’ is the policy implication of the argument. But this is precisely the point. The term ‘new’ is a way to exclude ‘old’ assumptions about the nature of war and to provide the basis for a novel research methodology. The aim of describing the conflicts of the 1990’s as ‘new’ is to change the way scholars investigate these conflicts and thus to change the way policy-makers and policy- shapers perceive these conflicts. Dominant understandings of these conflicts that under pin policy are of two kinds. On the one hand, there is a tendency to impose a stereotyped version of war, drawn from the experience of the last two centuries in Europe, in which war consists of a conflict between two warring parties, generally states or proto-states with legitimate interests, what I call ‘Old Wars’. This term refers to a stylised form of war rather than to all earlier wars. In such wars, the solution is either negotiation or victory by one side and outside intervention takes the form of either traditional peace, keeping in which the peace-keepers are supposed to guarantee a negotiated agreement and the ruling principles are consent, neutrality and impartiality - or traditional war-fighting on one side or the other, as in Korea or the Gulf War. On the other hand, where policy-makers recognise the short comings of the stereotypical understanding, there is a tendency to treat these wars as anarchy, barbarism, ancient rivalries, where the best policy response is containment, i.e. protecting the borders of the West from this malady. The use of the term ‘new’ is a way of demonstrating that neither of these approaches are appropriate, that these are wars with their own logic but a logic that is different from ‘old wars’ and which therefore dictates a very different research strategy and a different policy response. In other words, the ‘new wars’ thesis is both about the changing character of organised violence and about developing a way of understanding, interpreting and explaining the interrelated characteristics of such violence. As Jacob Mundy (2011) puts it, in one of the more thoughtful contributions to the debate: ‘Whether we choose to reject, embrace or reformulate concepts such as.... new wars, our justifications should not be based on claims of alleged coherence with particular representations of history Rather such concepts should be judged in terms of their ability to address the very phenomena they seek to ameliorate’. Even so, it can be argued that there are some genuinely new elements of contemporary conflicts. Indeed, it would be odd if there were not. The main new elements have to do with globalisation and technology. First of all, the increase in the destructiveness and accuracy of all forms of military technology has made symmetrical war, war between similarly armed opponents, increasingly destructive and therefore difficult to win. The first Gulf war between Iraq and Iran was perhaps the most recent example of symmetrical war a war, much like the First World War, that lasted for years and killed millions of young men, for almost no political result. Hence, tactics in the new wars necessarily have to deal with this reality. Secondly, new forms of communications (information technology, television and radio, cheap air travel) have had a range of implications. Even though most contemporary conflicts are very local, global connections are much more extensive, including criminal networks, Diaspora links, as well as the presence of international agencies, NGOS, and journalists. The ability to mobilise around both exclusivist causes and human rights causes has been speeded up by new communications. Communications are also increasingly a tool of war, making it easier, for example, to spread fear and panic than in earlier periods hence, spectacular acts of terrorism. This does not mean, as Berdal (2011) suggests, that the argument implies that all contemporary wars involve global connections or that those connections are necessarily regressive. Rather, it is an element in theorising the logic of new wars. Thirdly, even though it may be the case that, as globalisation theorists argue, globalisation has not led to the demise of the state but rather its transformation, it is important to delineate the different ways in which states are changing. Perhaps the most important aspect of state transformation is the changing role of the state in relation to organised violence. On the one hand, the monopoly of violence is eroded from above, as some states are increasingly embedded in a set of international rules and institutions. On the other hand, the monopoly of violence is eroded from below as other states become weaker under the impact of globalisation. There is, it can be argued, a big difference between the sort of privatised wars that characterised the pre-modern period and the ‘new wars’ which come after the modern period and are about disintegration. These new elements are not the reason for the adjective ‘new’, however, even though they may help to explain the evolution of new wars. The point of the adjective ‘new’ does not have to do with any particular feature of contemporary conflicts nor how well it resembles our assumptions about reality, but rather it has to do with the model of war and how the model I spell out is different from the prevailing models that underpin both policy and scholarship. It is a model that entails a specific political, economic and military logic.

#### Recreation of these stereotypes entrenches the existing power structure ensuring globalized war and structural violence

Kaldor 99, Mary Kaldor, professor of Global Governance a the London School of Economics and Director of the Civil Society and Human Security Research Unit, New & Old Wars, 1999, Stanford University Press, pg 110-111

The new wars have political goals. The aim is political mobilization on the basis of identity. The military strategy for achieving this aim is population displacement and destabilization so as to get rid of those whose identity is different and to foment hatred and fear. Nevertheless, this divisive and exclusive form of politics cannot be disentangled from its economic basis. The various political/military factions plunder the assets of ordinary people as well as the remnants of the state and cream off external assist ance destined for the victims, in a way that is only possible in conditions of war or near war. In other words, war provides a legitimation for various criminal forms of private aggrandizement while at the same time these are necessary sources of revenue in order to sustain the war. The warring parties need more or less permanent conflict both to reproduce their positions of power and for access to resources. While this predatory set of social relationships is most prevalent in the war zones, it aLso characterizes the surrounding regions. Because participation in the war is relatively low (in Bosnia, only 6.5 per cent of the population took part directly in the pros ecution of the war) the difference between zones of war and apparent zones of peace are not nearly as marked as in earlier periods. Just as it is difficult to distinguish between the political and the economic, public and private, military and civil, so it is increasingly difficult to distinguish between war and peace. The new war economy could be represented as a continuum, starting with the combination of criminality and racism to be found in the inner cities of Europe and North America and reaching its most acute manifestation in the areas where the scale of violence is greatest. If violence and predation are to be found in what are considered zones of peace, so it is possible to find islands of civility in nearly all the war zones. They are much less known about than the war zones, because it is violence and criminalitý and not normality that is generally reported. But there are regions where local state apparatuses continue to function, where taxes arc raised, services are provided and some production is maintained. There are groups who defend humanistic values and refuse the politics of particularism. The town of Tuzia in Bosnia— Herzegovina represents one celebrated example. The self-defence units created in Southern Rwanda arc another example. In isolation, these islands of civility are difficult to preserve, squeezed by the polarization of violence, but the very fragmentary and decentralized character of the new type of warfare makes such examples possible. Precisely because the new wars are a social condition that arises as the formal political economy withers, they are very difficult to end. Diplomatic negotiations from above fail to take into account the underlying social relations; they treat the various factions as though they were protostates. Temporary ceaselires or truces may merely legitimize new agreements or partnerships that, for the moment, suit the various factions. Peacekeeping troops sent in to monitor ceasefires which reflect the status quo may help to maintain a division of territory and to prevent the return of refugees. Economic reconstruction channelled through existing ‘political authorities’ may merely provide new sources of revenue as local assets dry up. As long as the power relations remain the same, sooner or later the violence will start again. Fear, hatred and predation are riot recipes for long-term viable polities. Indeed, this type of war economy is perennially on the edge of exhaustion. This does not mean, however, that they will disappear of their own accord. There has to be some alternative. In the next chapter, I will consider the possibilities for such an alternative; in particular, how islands of civility might offer a counterlogic to the new warfare.

#### The alternative is to reject the 1AC and their outdated conceptions of sovereignty and war to interrupt the cycle of acting and alter our scholarship and military logic to reject stereotypes of fear. This results in a cosmopolitan ethic.

Kaldor 05, Mary Kaldor, professor of Global Governance at the London School of Economics and Director of the Civil Society and Human Security Research Unit, “Old Wars, Cold Wars, New Wars, and the War on Terror,” International Politics, 42.4, December 2005, pg 497-498

By analysing New War in terms of social relations of warfare, we come up with a very different approach about how to deal with these type of conflicts and indeed, how to deal with terrorism in general. I don't want to suggest that terrorism is not a serious threat. On the contrary, I think it is too serious to be hijacked by fantasies of Old War. Actually, I felt the same way about Communism; nuclear weapons, in my view, prevented us from adopting a serious strategy for undermining communism; this was only possible in a détente context. I think World War II really did mark the end of Old Wars. Wars of this type are impossible; they are simply too destructive to be fought and have become unacceptable and, indeed, illegitimate. The 8-year war between Iraq and Iran was probably the exception that proved the rule. It was immensely destructive and led to a military stalemate and, at least on the Iraqi side, far from consolidating the state, it was the beginning of state disintegration, the slide into new war.New Wars deliberately violate all the conventions of Old War, as well as the new body of human rights legislation that has been built up since World War II. The key to dealing with New Wars has to be the reconstruction of political legitimacy. If Old Wars established a notion of political legitimacy in terms of the friend-enemy distinction, in New Wars the friend-enemy distinction destroys political legitimacy. So, political legitimacy can only be reconstructed on the basis of popular consent and within a framework of international law. It means supporting efforts of democratization in difficult situations or using various international tools and law to support such processes.Is there a role for military force? Yes, I believe military force has to be used to protect people and uphold the rule of law. I favour humanitarian intervention in cases of threatened humanitarian catastrophes. But that can't be done through classic war fighting. I don't have time to discuss this, but I do think that one can envisage new defensive uses of forces aimed at prevention, protection and stabilization rather than victory.Carl Schmitt would argue that there can be no political community without enemies, and that, where force is used in the name of humanity, the adversary is no longer an enemy but an outlaw, a disturber of the peace. If he is right, the future is very grim, a pervasive global New War is possible. But if we believe political communities can be held together by reason rather than fear, then there is an alternative possibility, a transformation of statehood, in which states are no longer intrinsically linked to warfare and operate within a multilateral framework. And as for the argument about humanity, we could turn it on its head. If we dub the terrorists as enemies, we give them political status; indeed, this may be what they are trying to achieve. I think it is quite a good idea to see them as outlaws and disturbers of the peace, and to use the methods of policing and intelligence rather than Old War.To conclude, what I have tried to show is that attempts to recreate Old War prevent us from dealing with the realities of today's globalized world. Indeed ideas of Old War feed into and exacerbate real New Wars taking place in Iraq and elsewhere. I call them 'new' not because they are altogether new but because we can only develop alternative strategies if we see how different they are from World War II, the Cold War or the War on Terror. I think there is a huge security gap in the world today. Millions of people live in daily fear of violence. Yet, our conceptions of security, drawn from the dominant experience of World War II, does not reduce that insecurity. Indeed, it makes it worse.

### 1NC T

The only War Power authority is the ability to MAKE MILITARY DECISIONS

Bajesky 13 (2013¶ Mississippi College Law Review¶ 32 Miss. C. L. Rev. 9¶ LENGTH: 33871 words ARTICLE: Dubitable Security Threats and Low Intensity Interventions as the Achilles' Heel of War Powers NAME: Robert Bejesky\* BIO: \* M.A. Political Science (Michigan), M.A. Applied Economics (Michigan), LL.M. International Law (Georgetown). The author has taught international law courses for Cooley Law School and the Department of Political Science at the University of Michigan, American Government and Constitutional Law courses for Alma College, and business law courses at Central Michigan University and the University of Miami.)

A numerical comparison indicates that the Framer's intended for Congress to be the dominant branch in war powers. Congressional war powers include the prerogative to "declare war;" "grant Letters of Marque and Reprisal," which were operations that fall short of "war"; "make Rules for Government and Regulation of the land and naval Forces;" "organize, fund, and maintain the nation's armed forces;" "make Rules concerning Captures on Land and Water," "raise and support Armies," and "provide and maintain a Navy." [n25](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n25) In contrast, the President is endowed with one war power, named as the Commander-in-Chief of the Army and Navy. [n26](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n26)¶ The Commander-in-Chief authority is a core preclusive power, predominantly designating that the President is the head of the military chain of command when Congress activates the power. [n27](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n27) Moreover, peripheral Commander-in-Chief powers are bridled by statutory and treaty restrictions [n28](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n28) because the President "must respect any constitutionally legitimate restraints on the use of force that Congress has enacted." [n29](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n29) However, even if Congress has not activated war powers, the President does possess inherent authority to expeditiously and unilaterally react to defend the nation when confronted with imminent peril. [n30](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n30) Explicating the intention behind granting the President this latitude, Alexander Hamilton explained that "it is impossible to foresee or to define the extent and variety of national exigencies, or the correspondent extent and variety of the means which may be necessary to satisfy them." [n31](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n31) The Framers drew a precise distinction by specifying that the President was empowered "to repel and not to commence war." [n32](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n32)

#### **Violation – the affirmative does not prohibit the ability of the President to make a military decision in one of the following areas mentioned in the topic – it merely requires a process or disclosure for the President to go through before exercising his commander and chief power**

Jean Schiedler-Brown 12, Attorney, Jean Schiedler-Brown & Associates, Appellant Brief of Randall Kinchloe v. States Dept of Health, Washington, The Court of Appeals of the State of Washington, Division 1, http://www.courts.wa.gov/content/Briefs/A01/686429%20Appellant%20Randall%20Kincheloe%27s.pdf

3. The ordinary definition of the term "restrictions" also does not include the reporting and monitoring or supervising terms and conditions that are included in the 2001 Stipulation.

Black's Law Dictionary, 'fifth edition,(1979) defines "restriction" as;

A limitation often imposed in a deed or lease respecting the use to which the property may be put. The term "restrict' is also cross referenced with the term "restrain." Restrain is defined as; To limit, confine, abridge, narrow down, restrict, obstruct, impede, hinder, stay, destroy. To prohibit from action; to put compulsion on; to restrict; to hold or press back. To keep in check; to hold back from acting, proceeding, or advancing, either by physical or moral force, or by interposing obstacle, to repress or suppress, to curb.

In contrast, the terms "supervise" and "supervisor" are defined as; To have general oversight over, to superintend or to inspect. See Supervisor. A surveyor or overseer. . . In a broad sense, one having authority over others, to superintend and direct. The term "supervisor" means an individual having authority, in the interest of the employer, to hire, transfer, suspend, layoff, recall, promote, discharge, assign, reward, or discipline other employees, or responsibility to direct them, or to adjust their grievances, or effectively to recommend such action, if in connection with the foregoing the exercise of such authority is not of a merely routine or clerical nature, but required the use of independent judgment.

Comparing the above definitions, it is clear that the definition of "restriction" is very different from the definition of "supervision"-very few of the same words are used to explain or define the different terms. In his 2001 stipulation, Mr. Kincheloe essentially agreed to some supervision conditions, but he did not agree to restrict his license.

#### Vote negative –

#### Ground – the negative should be able to say Drone Strikes, Cyber ops, troop invasion and indefinite detention good/bad – This is the core negative topic ground – they get to link turn our disad by saying we still allow authority in one of the areas.

#### Limits – they justify any aff that does transparency or requires a process before implementing a particular war power, – this allows them to apply a process to any particular subsection…

1. Bidirectionality – consultation and oversight mechanisms allow aff’s to defend the status quo by only adding another hoop for the executive to jump through, dont require a fundamental change from existing policy.

### Preemption

#### Too many logical holes for this to be a real advantage – psychological bias means you should be skeptical of their risk calculus and default negative towards higher probability impacts.

Cavelty 12 (Myriam Dunn Cavelty is a faculty member of the Swiss Federal Institute of Technology Center for Security Studies, "The militarisation of cyber security as a source of global tension", http://www.academia.edu/1471717/The\_militarisation\_of\_cyber\_security\_as\_a\_source\_of\_global\_tension, Strategic Trends 2012)

There is no denying that different political,¶ economic, and military conflicts¶ have had cyber(ed) components¶ for a number of years now. Furthermore,¶ criminal and espionage activities¶ involving the use of computers happen¶ every day. It is a fact that cyber¶ incidents are continually causing¶ minor and only occasionally major¶ inconveniences: These may be in the¶ form of lost intellectual property or¶ other proprietary data, maintenance¶ and repair, lost revenue, and increased¶ security costs. Beyond the direct impact,¶ badly handled cyber attacks have¶ also damaged corporate (and government)¶ reputations and have, theoretically¶ at least, the potential to reduce¶ public confidence in the security of¶ Internet transactions and e-commerce¶ if they become more frequent.¶ However, in the entire history of¶ computer networks, there are no examples¶ of cyber attacks that resulted¶ in actual physical violence against¶ persons (nobody has ever died from¶ a cyber incident), and only very few¶ had a substantial effect on property¶ (Stuxnet being the most prominent).¶ So far, cyber attacks have not caused¶ serious long-term disruptions. They¶ are risks that can be dealt with by¶ individual entities using standard¶ information security measures, and¶ their overall costs remain low in comparison¶ to other risk categories such¶ as financial risks.¶ These facts tend to be almost completely¶ disregarded in policy circles.¶ There are several reasons why the¶ threat is overrated. First, as combating¶ cyber threats has become a highly¶ politicised issue, official statements¶ about the level of threat must also be¶ seen in the context of competition for¶ resources and influence between various¶ bureaucratic entities. This is usually¶ done by stating an urgent need¶ for action and describing the overall¶ threat as big and rising.¶ Second, psychological research has¶ shown that risk perception, including¶ the perception of experts, is highly¶ dependent on intuition and emotions.¶ Cyber risks, especially in their¶ more extreme form, fit the risk profile¶ of so-called ‘dread risks’, which are¶ perceived as catastrophic, fatal, unknown,¶ and basically uncontrollable.¶ There is a propensity to be disproportionally¶ afraid of these risks despite¶ their low probability, which translates¶ into pressure for regulatory action of¶ all sorts and the willingness to bear¶ high costs of uncertain benefit.¶ Third, the media distorts the threat¶ perception even further. There is no¶ hard data for the assumption that the¶ level of cyber risks is actually rising¶ – beyond the perception of impact¶ and fear. Some IT security companies¶ have recently warned against overemphasising¶ sophisticated attacks just¶ because we hear more about them.¶ In 2010, only about 3 per cent of all¶ incidents were considered so sophisticated¶ that they were impossible to¶ stop. The vast majority of attackers¶ go after low-hanging fruit, which are¶ small to medium sized enterprises¶ with bad defences. These types of¶ incidents tend to remain under the¶ radar of the media and even law enforcement.¶ Cyber war remains unlikely¶ Since the potentially devastating¶ effects of cyber attacks are so scary, the¶ temptation is very high not only to¶ think about worst-case scenarios, but¶ also to give them a lot of (often too¶ much) weight despite their very low¶ probability. However, most experts¶ agree that strategic cyber war remains¶ highly unlikely in the foreseeable¶ future, mainly due to the uncertain¶ results such a war would bring, the¶ lack of motivation on the part of the¶ possible combatants, and their shared¶ inability to defend against counterattacks.¶ Indeed, it is hard to see how¶ cyber attacks could ever become truly¶ effective for military purposes: It is¶ exceptionally difficult to take down¶ multiple, specific targets and keep¶ them down over time. The key difficulty¶ is proper reconnaissance and¶ targeting, as well as the need to deal¶ with a variety of diverse systems and¶ be ready for countermoves from your¶ adversary. ¶ Furthermore, nobody can be truly¶ interested in allowing the unfettered¶ proliferation and use of cyber war¶ tools, least of all the countries with¶ the offensive lead in this domain.¶ Quite to the contrary, strong arguments¶ can be made that the world’s¶ big powers have an overall strategic¶ interest in developing and accepting¶ internationally agreed norms on¶ cyber war, and in creating agreements¶ that might pertain to the¶ development, distribution, and deployment¶ of cyber weapons or to¶ their use (though the effectiveness of¶ such norms must remain doubtful).¶ The most obvious reason is that the¶ countries that are currently openly¶ discussing the use of cyber war tools¶ are precisely the ones that are the¶ most vulnerable to cyber warfare attacks¶ due to their high dependency¶ on information infrastructure. The¶ features of the emerging information¶ environment make it extremely¶ unlikely that any but the most limited¶ and tactically oriented instances¶ of computer attacks could be contained.¶ More likely, computer attacks¶ could ‘blow back’ through the¶ interdependencies that are such an¶ essential feature of the environment.¶ Even relatively harmless viruses and¶ worms would cause considerable¶ random disruption to businesses,¶ governments, and consumers. This¶ risk would most likely weigh much¶ heavier than the uncertain benefits to¶ be gained from cyber war activities.¶ Certainly, thinking about (and planning¶ for) worst-case scenarios is a¶ legitimate task of the national security¶ apparatus. Also, it seems almost¶ inevitable that until cyber war is¶ proven to be ineffective¶ or forbidden, states and¶ non-state actors who¶ have the ability to develop¶ cyber weapons will try to do¶ so, because they appear cost-effective,¶ more stealthy, and less risky than other¶ forms of armed conflict. However,¶ cyber war should not receive too much¶ attention at the expense of more plausible¶ and possible cyber problems.¶ Using too many resources for highimpact,¶ low-probability events – and¶ therefore having less resources for the¶ low to middle impact and high probability¶ events – does not make sense,¶ neither politically, nor strategically¶ and certainly not when applying a¶ cost-benefit logic.¶ Europe is not the US¶ The cyber security discourse is American¶ in origin and American in the¶ making: At all times, the US government¶ shaped both the threat perception¶ and the envisaged countermeasures.¶ Interestingly enough, there are¶ almost no variations to be found in¶ other countries’ cyber threat discussions¶ – even though the strategic¶ contexts differ fundamentally. Many¶ of the assumptions at the heart of¶ the cyber security debate are shaped¶ by the fears of a military and political¶ superpower. The US eyes the cyber¶ capabilities of its traditional rivals, the¶ rising power of China and the declining¶ power of Russia, with particular¶ suspicion. This follows¶ a conventional strategic¶ logic: The main¶ question is whether¶ the cyber dimension could suddenly¶ tip the scales of power against the US¶ or have a negative effect on its ability¶ to project power anywhere and anytime.¶ In addition, due to its exposure¶ in world politics and its military engagements,¶ the US is a prime target¶ for asymmetric attack.¶ The surely correct assumption that¶ modern societies and their armed forces¶ depend on the smooth functioning¶ of information and communication¶ technology does not automatically¶ mean that this dependence will be¶ exploited – particularly not for the majority¶ of states in Europe. The existence¶ of the cyber realm seems to lead people¶ to assume that because they have¶ vulnerabilities, they will be exploited.¶ But in security and defence matters,¶ careful threat assessments need to be¶ made. Such assessments require that¶ the following question be carefully¶ deliberated: ‘Who has an interest in¶ attacking us and the capability to do so,¶ and why would they?’ For many democratic¶ states, particularly in Europe, the¶ risk of outright war has moved far to¶ the background and the tasks of their¶ armies have been adapted to this. Fears¶ of asymmetric attacks also rank low.¶ The same logic applies to the cyber domain.¶ The risk of a warlike cyber attack¶ of severe proportions is minimal; there¶ is no plausible scenario for it. Cyber¶ crime and cyber espionage, both political¶ and economic, are a different story:¶ They are here now and will remain the¶ biggest cyber risks in the future.¶ The limits of analogies¶ Even if the cyber threat were to be¶ considered very high, the current¶ trend conjures up wrong images.¶ Analogies are very useful for relating¶ non-familiar concepts or complex ideas¶ with more simple and familiar ones.¶ But when taken too far, or even taken¶ for real, they begin to have detrimental¶ effects. Military terms like ‘cyber¶ weapons’, ‘cyber capabilities’, ‘cyber¶ offence’, ‘cyber defence’, and ‘cyber¶ deterrence’ suggest that cyberspace¶ can and should be handled as an operational¶ domain of warfare like land,¶ sea, air, and outer space (cyberspace¶ has in fact been officially recognised¶ as a new domain in US military doctrine).¶ Again, this assumption clashes¶ with the reality of the threat and the¶ possibilities for countermeasures.¶ First, calling offensive measures cyber¶ weapons does not change the fact that¶ hacker tools are not really like physical¶ weapons. They are opportunistic and¶ aimed at outsmarting the technical¶ defences. As a result, their effect is usually¶ not controllable in a military sense¶ – they might deliver something useful¶ or they might not. Also, even though¶ code can be copied, the knowledge¶ and preparation behind it cannot be¶ easily proliferated. Each new weapon¶ needs to be tailored to the system it¶ is supposed to attack. Cyber weapons¶ cannot be kept in a ‘silo’ for a long¶ time, because at any time, the vulnerability¶ in the system that it is targeted¶ at could be patched and the weapon¶ would be rendered useless.¶ Second, thinking in terms of attacks¶ and defence creates a wrong image of¶ immediacy of cause and effect. However,¶ high-level cyber attacks against¶ infrastructure targets will likely be¶ the culmination of long-term, subtle,¶ systematic intrusions. The preparatory¶ phase could take place over several¶ years. When – or rather if – an¶ intrusion is detected, it is often impossible¶ to determine whether it was¶ an act of vandalism, computer crime,¶ terrorism, foreign intelligence activity,¶ or some form of strategic military¶ attack. The only way to determine¶ the source, nature, and scope of the¶ incident is to investigate it. This again¶ might take years, with highly uncertain¶ results. The military notion of¶ striking back is therefore useless in¶ most cases.¶ Third, deterrence works if one party¶ is able to successfully convey to an-¶ other that it is both capable and¶ willing to use a set of available (often¶ military) instruments against the¶ other side if the latter steps over the¶ line. This requires an opponent that¶ is clearly identifiable as an attacker¶ and has to fear retaliation – which¶ is not the case in cyber security because¶ of the attribution problem.¶ Attribution of blame on the basis¶ of the cui bono logic is not sufficient¶ proof for political action.¶ Therefore, deterrence and retribution¶ do not work in cyberspace and¶ will not, unless its rules are changed¶ in substantial ways, with highly¶ uncertain benefits. Much of what is¶ said in China and in the US about¶ their own and the other’s cyber¶ capabilities is (old) deterrence rhetoric¶ – and must be understood as such.¶ The White House’s new International¶ Strategy for Cyberspace of 2011¶ states that the US reserves the right to¶ retaliate to hostile acts in cyberspace¶ with military force. This ‘hack us and¶ we might bomb you’ statement is an¶ old-fashioned declaratory policy that¶ preserves the option of asymmetrical¶ response as a means of deterrence,¶ even though both sides actually know¶ that following up on it is next to¶ impossible.¶ Fourth, cyberspace is only in parts¶ controlled or controllable by state¶ actors. At least in the case of democracies,¶ power in this domain is in the¶ hands of private actors, especially the¶ business sector. Much of the expertise¶ and many of the resources required¶ for taking better protective measures¶ are located outside governments. The¶ military – or any other state entity for¶ that matter – does not own critical (information)¶ infrastructures and has no¶ direct access to them. Protecting them¶ as a military mandate is impossible,¶ and conceiving of cyberspace as an¶ occupation zone is an illusion. Militaries¶ cannot defend the cyberspace of¶ their country – it is not a space where¶ troops and tanks can be deployed, because¶ the logic of national boundaries¶ does not apply.¶

**Zero risk of accidents**

**Quinlan 9** (Sir Michael Quinlan, Former Permanent Under-Secretary of State UK Ministry of Defense, Thinking About Nuclear Weapons: Principles, Problems, Prospects, p. 63-69, The book reflects the author's experience across more than forty years in assessing and forming policy about nuclear weapons, mostly at senior levels close to the centre both of British governmental decision-making and of NATO's development of plans and deployments, with much interaction also with comparable levels of United States activity in the Pentagon and the State department)

There have certainly been, across the decades **since** 19**45, many known accidents** involving nuclear weapons, from transporters skidding off roads to bomber aircraft crashing with or accidentally dropping the weapons they carried (in past days when such carriage was a frequent feature of readiness arrangements it no longer is). A few of these accidents may have released into the nearby environment highly toxic material. **None** however has entailed a nuclear detonation. Some commentators suggest that this reflects bizarrely good fortune amid such massive activity and deployment over so many years. A more rational deduction from the facts of this long experience would however be that the probability of any accident triggering a nuclear explosion is extremely low. It might be further nested that the mechanisms needed to set of such an explosion are technically demanding, and that in a large number of ways the past sixty years have seen extensive improvements in safety arrangements for both the design and the handling of weapons. It is undoubtedly possible to see respects in which, after the cold war, some of the factors bearing upon risk may be new or more adverse; but some are now plainly less so. The years which the world has come through entirely without accidental or unauthorized detonation have included early decades in **which knowledge was sketchier, precautions** were **less developed, and** weapon **designs were less ultra-safe** than they later became, as well as substantial periods in which weapon numbers were larger, deployments immure widespread arid diverse, movements more frequent, and several aspects of doctrine and readiness arrangements more tense. Similar considerations apply to the hypothesis of nuclear war being mistakenly triggered by false alarm. Critics again point to the fact, as it is understood, of numerous occasions when initial steps in alert sequences for US nuclear forces were embarked upon, or at least called for, by indicators mistaken or misconstrued. In none of these instances, it is accepted, did matters get at all near to nuclear launch—extraordinary good fortune again, critics have suggested. But the rival and more **logical inference** from **hundreds of events** stretching over **sixty years** of experience presents itself once more: that the probability of initial misinterpretation leading far towards mistaken launch **is remote**. Precisely because any nuclear weapon processor recognizes the vast gravity of any launch, release sequences have **many steps**, and human decision is **repeatedly interposed** as well as capping the sequences. To convey that because a first step was prompted the world somehow came close to accidental nuclear war is wild hyperbole, rather like asserting, when a tennis champion has lost his opening service game, that he was nearly beaten in straight sets. **History** anyway **scarcely offers any** ready **example** of major war started by accident **even before the nuclear revolution imposed an order-of-magnitude increase of caution**. In was occasion conjectured that nuclear war might be triggered by the real but accidental or unauthorized launch of a strategic nuclear-weapon delivery system in the direction of a potential adversary. No such launch is known to have occurred in over sixty years. The probability of it is therefore very low. But even if it did happen, the further hypothesis of it initiating a general nuclear exchange is far-fetched. It fails to consider the real situation of decision-makers, as pages 63-4 have brought out. The notion that cosmic holocaust might be mistakenly precipitated in this way **belongs to science fiction**.

#### Their cyberattack arguments are produced from the scholarship of paranoia – this justifies unending threat construction and elimination of those threats

Hart 11 (Catherine, Masters in Communications at Simon Fraser U, "Mobilizing the Cyberspace Race: the Securitization of the Internet and its Implications for Civil Liberties," Cyber-Surveillance in Everyday Life: An International Workshop \* May 12-15, 2011 \* University of Toronto, <http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Hart-Mobilizing-the-Cyberspace-race.pdf>)

In this paper I seek to explore the way in which the increasing regulation of networked computing through digital controls and surveillance is being justified using a securitizing discourse. I argue that the dominant frame of ‘cybersecurity’ has become one based on national security, due to the potentially debilitating effect that a breakdown of the network would have on society, the economy, the military, and government. This understanding caused President Obama, during his 2008 presidential campaign, to declare the U.S. information infrastructure a ‘strategic asset,’ a move which positions the Internet as a significant issue for the military (Clarke, 2010, 116). Within the Copenhagen School’s perspective on International Security Studies, this is known as a ‘securitizing move’; an attempt to frame something as essential to national security. I seek to examine the application of this securitizing discourse to networked computing and its development into an issue of ‘cybersecurity’ over the past three U.S. administrations. To do this, I will apply the Copenhagen School’s framework to each administration’s official policy on cybersecurity, in order to assess whether the securitization is successful, and what impact proposed responses may have on civil liberties. Securitization: A Framework for Analysis A securitization is a speech act which constitutes a ‘referent object’, in this case the state, as threatened in its very existence, and therefore necessitates urgent action (Buzan et al, 1998). The analysis of this process of “securitization” in networked computing involves a three-part process: the identification of a discourse of national security within discussions of networked computing, evidence of the acceptance of this discourse by an audience, and the promotion or uptake of restrictive responses aimed at increasing security. The first part of the process, the mobilization of an existing discourse of national security, relies upon the understanding that “the very utterance of ‘security’ is more than just saying or describing something but the performing of an action,” with the potential to create a new reality (Stritzel, 2007, 362). This is a prominent feature of framing, which Edelman explains allows “the character, causes, and consequences of any phenomenon [to] become radically different as changes are made in what is prominently displayed, what is repressed and especially in how observations are classified” (as cited in Entman, 1993, 54). Therefore scholars of securitization are not concerned with the validity of an asserted threat; their focus, rather, is the action that is facilitated as a result of the acceptance of the validity of a threat. Buzan explains that [s]tates, like people, can be paranoid (constructing threats where none exist) or complacent (ignoring actual threats). But since it is the success (or not) of the securitization that determines whether action is taken, that side of threat analysis deserves scrutiny just as close as that given to the material side. (Buzan, 2006, 1102) The second stage in the process concerns the likelihood that this discourse will be accepted by a wider audience than those advancing the securitization. The ability of an actor to successfully securitize an issue is highly dependent on their position. Security has, to some degree, been institutionalized, as is the case with the military, and therefore “some actors are placed in positions of power by virtue of being generally accepted voices of security, by having the power to define security” (Buzan et al, 1998, 31). Government cybersecurity policy would therefore seem to be an ideal vehicle to mobilize and perhaps also legitimize a securitizing move. Policy represents an administration’s official standpoint on an issue which is understood to be a problem, and proposes solutions based on technical knowledge and research. However, as public policy scholar Frank Fischer explains, [f]rom the social constructivist perspective... the social and political life under investigation is embedded in a web of social meanings produced and reproduced through discursive practices. Politics and public policy are understood to take shape through socially interpreted understandings, and their meanings and the discourses that circulate them are not of the actors’ own choosing or making. (2003, 13) Public policy therefore contains both a persuasive and a responsive element; it seeks to justify a chosen course of action which is based upon socially interpreted understandings of ‘national security’. To use the Copenhagen School’s terms, it is both part of the securitizing move, employing a discourse of security, but by its very existence, demonstrates the success of the securitizing move because the issue has been taken seriously enough to warrant an official standpoint and planned response. Assessing how far securitization in policy promotes national security above all other considerations, including civil liberties, is the third part of the process. By applying a framework of security to an event, it is understood that the issue is one of urgency, and, in the words of Buzan et al, “if the problem is not handled now it will be too late, and we will not exist to remedy our failure” (1998, 26). According to the Copenhagen School's approach, “[t]he invocation of security has been the key to legitimizing the use of force, but more generally it has opened the way for the state to mobilize, or to take special powers, to handle existential threats” (ibid, 21). If a securitization is successful, an audience will tolerate violations of rules that would otherwise have to be obeyed, for example the restriction of free speech, or freedom from unreasonable search and seizure. By its very definition, a framework selectively calls attention to certain aspects of reality, and therefore ignores or omits others (Entman, 1993, 54). A security framework privileges security above all other concerns, sometimes to the detriment of civil liberties. It is commonly understood that to attain security, a little freedom must be given up, but how much freedom is under debate. It is not yet clear whether the security arguments of the U.S. military, the intelligence community, and more hawkish members of government will result in the hypersecuritization of cyberspace—to use Barry Buzan's term for the mobilization of exaggerated threats and excessive countermeasures (2004, 172)—or whether a more measured view, taking into account civil liberties and the positive potential of the Internet, will win out.

#### No impact to cyber war – rationality checks.

Fox 11 <Stuart. “Why Cyberwar is Unlikely” July 2, 2011. http://www.securitynewsdaily.com/830-cyberwar-unlikely-deterrence-cyber-war.html>

Even as more and more countries invest in the idea of cyberwarfare, cyberspace remains largely peaceful insofar as actual war is concerned. In the two decades since cyberwar first became possible, there hasn't been a single event that politicians, generals and security experts agree on as having passed the threshold for strategic cyberwar. In fact, the attacks that have occurred have fallen so far short of a proper cyberwar that many have begun to doubt that cyberwarfare is even possible. The reluctance to engage in strategic cyberwarfare stems mostly from the uncertain results such a conflict would bring, the lack of motivation on the part of the possible combatants and their shared inability to defend against counterattacks. Many of the systems that an aggressive cyberattack would damage are actually as valuable to any potential attacker as they would be to the victim. The five countries capable of large-scale cyberwar (Israel, the U.S., the U.K., Russia and China) have more to lose if a cyberwar were to escalate into a shooting war than they would gain from a successful cyberattack. "The half-dozen countries that have cyber capability are deterred from cyberwar because of the fear of the American response. Nobody wants this to spiral out of control," said James Lewis, senior fellow and director of technology and public policy at the Center for Strategic and International Studies in Washington, D.C. "The countries that are capable of doing this don't have a reason to," Lewis added. "Chinese officials have said to me, 'Why would we bring down Wall Street when we own so much of it?' They like money almost as much as we do." Deterrence plays a major factor in preventing cyberwar. Attacks across the Internet would favor the aggressor so heavily that no country has developed an effective defense. Should one country initiate a cyberattack, the victim could quickly counter-attack, leaving both countries equally degraded, Lewis told InnovationNewsDaily. Even if an attacker were to overcome his fear of retaliation, the low rate of success would naturally give him pause. Any cyberattack would target the types of complex systems that could collapse on their own, such as electrical systems or banking networks. But experience gained in fixing day-to-day problems on those systems would allow the engineers who maintain them to quickly undo damage caused by even the most complex cyberattack, said George Smith, a senior fellow at Globalsecurity.org in Alexandria, Va. "You mean to tell me that the people who work the electrical system 24 hours a day don't respond to problems? What prevents people from turning the lights right back on?" Smith told SecurityNewsDaily. "And attacks on the financial system have always been a non-starter for me. I mean, [in 2008] the financial system attacked the U.S.!" Of course, just because political, technological and economic concerns have prevented cyberwar thus far does not mean the situation cannot change. Some analysts believe that the cost of getting caught flatfooted by a cyberattack more than justifies investing in protection against future threats. "The situation could change," said Sami Saydjari, chairman of Professionals for Cyber Defense, a organization formed to "advocate, advise and advance sound cyber defense policy for the United States of America." "For example, if we ended up in a shooting war with China, for whatever reason, they have a capability to take out our infrastructure," Saydjari said. "We don't want them to be able to do that. We don't want our enemies to even have the potential to do that, even if they currently have no incentive to do so." And then there's the issue of terrorism. Undeterred by possible counterattack and unencumbered by economic and political ties, terrorist groups make the most feared attackers in a hypothetical cyberwar. "One day we're going to wake up and find that Al Qaeda or one of these more extreme groups will get this capability. That's what I worry about," Lewis said. "They don't have this capability now. There’s some indication that they know about the black market. But it's like them trying to acquire any other advanced weapon system." But so far, there's no evidence that any terrorist group plans on launching a cyberattack against the U.S. In fact, there's not really any evidence that any country plans on initiating cyberwar against any other country in the near future. For the last 20 years, and into the foreseeable future, it's remained all quiet in the cyber front. "I would give people who say there's an enormous cyber threat the benefit of the doubt. But I've been hearing this for close to twenty years now," said Martin Libicki, a senior policy analyst in cyber issues for the RAND Corporation in Santa Monica, Calif. "Twenty years after Kitty Hawk, airplanes were an integral part of warfare," Libicki said. "By comparison, cyberwar hasn't advanced nearly as quickly."

#### There is no risk of great power conflict – operations are difficult to conduct.

Dunlap 12 (Charles J. Dunlap Jr, American Bar Association, Patriots Debate: Contemporary Issues in National Security, Lawless Cyberwar? Not If You Want To Win") 12

The threat of cyberwar is certainly an extremely serious one, but surely not a greater peril than is nuclear war. Yet at least insofar as the U.S. military is concerned, nuclear operations *can* be made amenable to the law.35 In other words, if our survival does not require abandoning the rule of law with respect to nuclear weapons, there is certainly no reason to do so in the cyber realm.  Does Baker nevertheless believe that the United States is so vulnerable to catastrophic cyber attack that the nation must reject any legal limits in its cyber response?  If, indeed, the United States were as vulnerable to catastrophic attack as Baker would have us believe, al Qaeda or some extremistgroup certainly would have launched one by now. In point of fact,although cyber crime may be extensive, militarily significant cyber attacks apparently are not so easy to conduct as Baker seems to think.In reporting the rejection of cyber weaponry as a means of dismantling ibyan air defenses, *The New York Times* noted that:  While popular fiction and films depict cyberattacks as easy to mount—only a few computer keystrokes needed—in reality it takes significant digital snooping to identify potential entry points and susceptible nodes in a linked network of communications systems, radars and missiles like that operated by the Libyan government, and then to write and insert the proper poisonous codes.36  Obviously, if cyber weaponry is technically difficult for the world’s foremost military to use even against a third-world power such as Libya, one may reasonably infer that it is markedly more difficult to use against a sophisticated first-world power, even for a peer or near peer of that power.

#### Cyber-wars don’t escalate – redundancy in the system reduces the threat

Posner 11 (Gary Becker and Richard Posner, 8/7/11 The Becker-Posner Blog, "The Challenge of Cyber Warfare - Posner")

Although at present defense against cyber warfare is very difficult, and indeed seemingly ineffectual, a pooling of the civilized world’s computer expertise in an international effort to secure computer networks and databases against online espionage and (especially) sabotage, as well as to create redundancy in such networks and databases that would enable their essential functions to be maintained even after a large-scale cyber attack, would certainly be a worthwhile undertaking. There are indications of cooperation between the United States and close allies such as the United Kingdom and Israel. Let us hope that international cooperation in cyber defense is expanded and adequately financed.

#### Cyber-aggression doesn’t escalate- damage is contained

**Gartzke ’12** [Erik A. Gartzke, Associate Professor of Political Science at UC San Diego, PhD in International Relations from Iowa, “The Myth of Cyberwar,” <http://dss.ucsd.edu/~egartzke/papers/cyberwar_12062012.pdf>]

Beyond questions of means and motive, two basic features make cyber warfare different from other¶ types of conflict. First, the bulk of damage contemplated by cyberwar is in all likelihood temporary.¶ The assumption among many cyber-pessimists that the potential for creating harm is sufficient to¶ make cyber space a suitable substitute for, or at least an alternative to, terrestrial conflict is simply¶ incorrect. Shutting down the power grid, or preventing communication could be tremendously¶ costly, but most such damage can be corrected quickly and with comparatively modest investment¶ of tangible resources. Regardless, damage of this type is sunk. Losses experienced over a given time¶ interval cannot be recovered whatever one's reactions and so should not have much direct impact on subsequent policy behavior. Harm inflicted over the internet or through any other medium¶ will matter politically when it involves changes to the subsequent balance of power, or when it¶ indicates enemy capabilities that must be taken into account in future plans. Precisely because¶ cyberwar does not involve bombing cities or devastating armored columns, the damage inflicted¶ will have a short-term impact on targets.10 To accomplish meaningful objectives, cyber attacks¶ must contribute to other aspects of a more conventional war effort. In order to affect the long-term¶ balance-of-power, for instance, cyberwar must be joined to other, more traditional, forms of war.¶ Temporary damage can be useful in two circumstances. First, compromising or incapacitating¶ networks might afford an enemy valuable tactical, or even strategic, advantages. An opponent that¶ cannot shoot, move, resupply or communicate will be easier to defeat. However, this still requires¶ the advantaged party to act through some medium of combat to seize the initiative. Notions that¶ cyber attacks will themselves prove pivotal in future war are reminiscent of World War I artillery¶ barrages that cleared enemy trenches, but which still required the infantry and other arms to achieve¶ a breakout. Whether an actor can benefit from cyberwar depends almost entirely on whether the¶ actor is willing and able to combine a cyber attack with some other method | typically kinetic¶ warfare | that can convert temporary advantages achieved over the internet into a lasting blow.¶ Internet attacks thus offer an assailant a \soft kill" that is valuable only when attackers intend and¶ prosecute follow-on attacks with traditional military force to permanently weaken an enemy.11¶ The notion of a devastating surprise attack is a particularly baroque aspect of cyberwar paranoia, and is certainly frightening to the degree that such scenarios are accurate. However, the idea¶ of a surprise attack over the internet is in fact extremely misleading and relies on a fundamental¶ misconception of the role of internet-based aggression. It has seldom been the case in modern times¶ that any one element of combat proves pivotal. Instead, it is the ability to combine elements into¶ a complex whole that increasingly distinguishes adept utilization of military force (Biddle 2004).¶ The archetype of modern, combined arms warfare is the blitzkreig, where the lethality and¶ effectiveness of conventional military violence is enhanced by actions designed to disrupt the enemy's military and civilian infrastructure. An important element of blitzkreig was the use of terror¶ weapons, such as the Ju 87 “Stuka” dive bomber, to sow panic, mobilizing enemy populations¶ to flood roads and railways, thereby crippling infrastructure needed by the defense. Yet, fear is¶ temporary and in the absence of substance, quickly subsides. The Stukas were effective only as long¶ as Germany held other military advantages over its enemies. Unless threatened with immediate¶ invasion, the terror role of the Stuka was largely redundant. Stukas contributed little to Germany's¶ attempt to subdue the United Kingdom, for example. Stuka units experienced heavy casualties¶ against a competent air defense and had to be removed from service in the Battle of Britain. The¶ hubris of Luftwa e commander Goring in promising victory while exploiting only a single domain¶ (the air) was precisely that he exaggerated the independent effect of a new technology on war.¶ There is no reason to believe that cyberwar will be any more useful as an isolated instrument¶ of coercive foreign policy. An attack that causes temporary harm will inevitably be followed by¶ countermeasures and heightened vigilance, as has happened for example in Estonia in the aftermath of the 2007 attacks. For cyber aggression to have lasting effects, a virtual attack must be¶ combined with physical intervention. Knocking out communications or power infrastructure could¶ cause tremendous disruption, but the ability to quickly recover from such attacks implies that the¶ consequences in terms of the balance of national power would be negligible. The need to follow¶ virtual force with physical force in order to achieve lasting political effects suggests that the application of cyber warfare independent of conventional forms of warfare will be of tertiary importance in¶ strategic and grand strategic terms. If one cannot foresee circumstances where physical aggression¶ is plausible independent of cyberwar, then cyberwar is also unlikely to constitute a critical threat.

#### No great power draw-in

**Gelb ’10** (President Emeritus of the Council on Foreign Relations, 2010 (Leslie, former senior official in the U.S. Defense Department and State Department, Foreign Affairs, November/December Foreign Affairs 2010)

Also reducing the likelihood of conflict today is that there is **no arena** in which the vital interests of great powers seriously clash. Indeed, the most worrisome security threats today--rogue states with nuclear weapons and terrorists with weapons of mass destruction--**actually tend to unite the great powers more than divide them**. In the past, and specifically during the first era of globalization, major powers would war over practically nothing. Back then, they fought over the Balkans, a region devoid of resources and geographic importance, a strategic zero. **Today, they are unlikely to shoulder their arms over almost anything, even the highly strategic Middle East. All have much more to lose than to gain from turmoil in that region**. To be sure, great **powers such as China and Russia will tussle with one another for advantages, but they will stop well short of direct confrontation.** **To an unprecedented degree**, the **major powers now need one another to grow their economies, and they are loath to jeopardize this interdependence by allowing traditional military and strategic competitions to escalate into wars**. In the past, U.S. enemies--such as the Soviet Union--would have rejoiced at the United States' losing a war in Afghanistan. Today, the United States and its enemies share an interest in blocking the spread of both Taliban extremism and the Afghan-based drug trade. China also looks to U.S. arms to protect its investments in Afghanistan, such as large natural-resource mines. More broadly, no great nation is challenging the balance of power in either Europe or Asia. Although nations may not help one another, they rarely oppose one another in explosive situations.

### China

#### Their assertion that American executive restraint can spur Chinese change is an orientalist fantasy organized around an idealized western subject.

Pan 2013

Chengxin, Senior Lecturer in International Relations, Deakin University, Australia, Knowledge, Desire and Power in Global Politics Western Representations of China’s Rise, pg. 123-124

As well as perplexed by its false premises, the notion of the 'China opportunity' itself is often vaguely defined. If it means that China will become more like 'us\*, that only raises more questions than answers: Who. for example, is 'us'? This popular collective 'we', as noted earlier, is inherently heterogeneous and constantly contested. As a result, there is no single Western self for China to emulate, nor is there a commonly agreed Western norm for China to follow. Despite much focus on 'bringing China into the international community', Johnston and Ross acknowledge that there has been little attempt to establish 'who constitutes this community and what are the shared global norms and rules\*. To provide a remedy, they call for the creation of an ambitious "score-card\* to 'assess China's commitment to global norms, rules and institutions across time, across other states and across issue areas'.86 And on the score-card, Johnston and Evans include a key criterion in terms of 'whether Chinese behavior complies with US interests as American political and military leaders define them". Explicit as this benchmark may sound, what remains unclear is which American political and military leaders actually define what, given that 'American leaders\* are far from a homogeneous entity Further complicating the issue is the debate over 'genuine learning' versus "strategic adaptation'. Some define 'genuine learning' as 'genuine (if often incremental) transformation of elite perceptions'- but the problem remains as to what is meant by 'genuine\*. For example, does evidence of policy change qualify as genuine learning? Jack S. Lew argues that policy change is not a necessary criterion, but Iain Johnston argues that it is.89 Granted that it is, we are still unclear whether policy change refers to 'humane governance' or 'the end of the one party system\*. David Lampton believes that it should be the former. Bui for James Mann, 'more humane governance' is no political change at all, as it is little more than 'a new euphemism for acceptance of China's existing one-party system'.90 For some, though both the precise meaning and measurement of China's convergence may be messy and elusive, what really matters is that both China and the West have begun to share a common interest in engagement and integration. For example, both seem to agree that China is an opportunity for the world Both sides stress the importance of China becoming a responsible stakeholder. Bill Clinton observed first hand that Jiang Zemin shared his desire to integrate China into the world community.91 But there is more to such apparent convergence than meets the eye. Despite some of the common vocabulary in use, there has been a lack of common meaning on those terms. As Lampion observes, both the US and China 'can agree about being responsible powers as a general proposition but fall out over what the content of "responsibility" may specifically be'.92 Consequently, the two sides often talk at cross-purposes. When they do seem to agree on some common meanings, common meanings do not necessarily translate into consensus. Quite the contrary, 'a common meaning", as Charles Taylor explains, 'is very often the cause of the most bitter lack of consensus". ' This point has not been lost on Thomas Friedman In a BBC documentary he made the point that "What is most unsettling about China to Americans is not their communism, it is their capitalism'.94 Furthermore, granted that the West and China could settle on a common goal for the time being, that goal could turn out to be a moving target over time. Surely not all Western expectations of China are inherently elusive. Yet the problem is that as China takes one modest step forward, it often invites the expectation of another, always one step ahead of China. In this sense, the West's normative goal of changing China is not a need, but a demand. In the words of Slavoj Zizek, 'every time the subject gels the object he demanded, he undergoes the experience of "This is not that!" Although the subject "got what he asked for." the demand is not fully satisfied'.95

#### Turns the case --- Historically, the demand for Chinese policy reform causes miscalculation and military conflict.

Pan 2013

Chengxin, Senior Lecturer in International Relations, Deakin University, Australia, Knowledge, Desire and Power in Global Politics Western Representations of China’s Rise, pg. 144

In this context, through its "China fantasy'" offshoot, the 'China opportunity’ paradigm is partly responsible for the hardline turn in Western approach to China. Herein lies the danger of this China paradigm and its strategy of 'constructive engagement". Engagement, as Jean A. Garrison points out, 'rests on the dangerous hope for regime change in China... This "hope"' raises expectations among certain constituencies that make presidents susceptible to political backlash when progress is not forthcoming".107 What we are witnessing today is in large degree a product of such political backlash, which, if unchecked, could launch US-China relations on a dangerous path of spiralling confrontation. In fact, such a path has been well-trodden in history. A cursory look at past Sino-Western interactions reveals that their clashes were not just due to their conflicting interests or diverging values per se, but also due to the recurring volatile dynamics of mutual hope and subsequent mutual disillusionment. Though no bilateral relationship can be free from the fluctuation of hope and disenchantment, in their dealing with China, the West in general and the US in particular have been especially prone to the pendulum cycle of paternalistic hope and 'rightful' disillusionment, with the end of each such cycle frequently marked by prolonged estrangement and open hostility.108 '

#### No risk of China offensive cyber operation - globalization means it not in their self-interest

Chou 2/8/11 (Ella, Graduate Student in Regional Studies at Harvard Law, "US-China Cyber War Scenario in the Eyes of a Chinese Student" The Atlantic)

In this equation, intent ranges from zero to 100% (100% meaning the country is willing to devote all capability to one mission). Even if China's capability in the cyber arena is increasing, it does not make it a threat to U.S. national security if China does not have the intent to use that capability in an attack against the United States. It would hardly be surprising to learn that China, like all countries with such capabilities, is engaged in cyber espionage. But real or threatened attacks against either U.S. military or the civilian infrastructure would not be in China's interests for a variety of reasons: the negative effects on trade which would have a direct impact on its volatile migrant labor population, the international backlash that would destroy its hard-earned position in the international organizations in which it has strong interests, not to mention the danger of confronting the full weight of U.S. military.

#### Interdependence checks cyber war with China

Austin and Gady 2012(Greg, professorial fellow at the EastWest Institute and senior visiting fellow in the department of War Studies at King’s College London, and Franz-Stefan, associate and foreign policy analyst at the EastWest Institute, "Cyber Detente Between the united States and China: Shaping the Agenda", http://www.ewi.info/system/files/detente.pdf)

That said, the two countries’ economies, though very different in many respects, are each highly dependent on a global Internet and shared communications platforms and hardware. While the Chinese economy is not as dependent on the Internet as the U.S., economy is, the difference between the two is fast shrinking. China’s export-driven economy and its trade in financial services make it as vulnerable to cyber attack as the United States. This interdependence—despite occasional outbursts of confrontational rhetoric coming from both Beijing and Washington— can be leveraged to promote stability in bilateral relations. In fact, this is already happening. We can think of this interdependency as a bal-ance of cyber power. If one accepts that both governments make rational calculations, than this new interconnectedness can be exploited to make conflict less likely. In today’s interconnected, digitalized world, the “opportunity cost” associated with embarking on a confrontational course will deter both parties from engaging in open hostile actions. This of course does not preclude cyber espionage, intellectual property theft, or even what some analysts have called the “long game,” i.e. the slow and gradual infiltration of strategically significant economic ICT systems by hackers on both sides.

#### Interdependence is amplified in cyber war—the potential impacts prevent any potential conflict

Austin and Gady 2012(Greg, professorial fellow at the EastWest Institute and senior visiting fellow in the department of War Studies at King’s College London, and Franz-Stefan, associate and foreign policy analyst at the EastWest Institute, "Cyber Detente Between the united States and China: Shaping the Agenda", http://www.ewi.info/system/files/detente.pdf)

China and the United States do have a com-plementary interest in cooperating on many aspects of cybersecurity. The most significant argument to support a claim for cooperation in China’s international behavior in cyberspace is mutual dependence among the major economic powers (including China, the United States, Japan and the European Union) in the economic sphere, in a situation where trillions of dollars of transactions occur through networked digital communications each day. In speaking of the U.S.’s economic reliance on digital networks and systems, former Director of National Intelligence Mike McConnell observed in 2010: “The United States economy is $14 trillion a year. Two banks in New York City move $7 trillion a day. On a good day, they do eight trillion... All of those transactions are massive reconciliation and accounting. If those who wish us ill, if someone with a different world view was successful in attacking that information and destroying the data, it could have a devastating impact, not only on the nation, but the globe.” 31 The cost to global economic stability would likely be very high if there were a major confrontation between China and the United States. Sustained or repeated interruptions in connectivity, corruption of transaction data, or deletion of commercial records on a large scale could have major negative repercus-sions for the global economy. Whether confidence after such attacks could be restored remains an open question. These costs would be so high that they should at least dampen if not fully deter states from resorting to cyber war. Cyberspace only amplifies traditional interdependence in trade.

#### No epistemology for Chinese militarism – the biggest internal link to US-China war is the way the US understands itself – their supposed experts are structurally unable to come to terms with the role of self-knowledge in producing China policy

Pan 4 (Chengxin, Department of Political Science and International Relations, Faculty of Arts, Deakin University, Discourses Of ‘China’ In International Relations: A Study in Western Theory as (IR) Practice, p. 255-256)

For example, as I pointed out in Chapter 5, the ‘China threat’ as conceived by Richard Bernstein, Ross Munro, Richard Betts, and Thomas Christensen, has been derived less from an ‘objective’ examination of China’s military capabilities, strategic posture, or actual foreign behaviour, and more from a (neo)realist conception of China as an aggressive, threatening entity in an unremittingly anarchic system. This conception, in turn, is derived from an entrenched understanding of the Western/American self as the rational orderer of the system, an understanding which has long been passed as the universal reality of world politics per se. The neorealist John Mearsheimer sums up this perspective well in proposing that: If… China becomes not only a leading producer of cutting-edge technologies but also the world’s wealthiest great power, it would almost certainly use its wealth to build a mighty military machine. For sound strategic reasons, moreover, it would surely pursue regional hegemony, just as the United States did in the western hemisphere during the nineteenth century. So if Chinese relative power grows substantially, one should expect it to attempt to dominate Japan and South Korea, as well as other regional actors, by building military forces that are so powerful that those other states would not dare challenge it. One should also expect it to develop its own version of the Monroe Doctrine, directed at the United States; just as the United States has made it clear to distant great powers that they are not allowed to meddle in the western hemisphere, China will make it clear that American interference in Asia is unacceptable [emphases added].12 This is a typical example of Western discourse allowing no room for an understanding of China outside the parameters of Western self-perception, an argument that, as I illustrated in Chapter 6, is equally applicable to the (neo)liberal perspective. In this latter context, for example, Western efforts to report and depict the Tiananmen uprising of 1989 as a ‘pro-democracy’ movement relied on ‘pro-Western’ interpretations of the movement’s motives, interpretations not easily attached to the event. It is as if the Tiananmen movement would make little sense were it not a specific example of the worldwide democratic wave to become more like ‘us.’ Thus, setting out to know the specifically different society called ‘China,’ both realist and liberal discourses have invariably ended up ‘discovering’ the same world everywhere, a world essentially of their own making. The very notion that ‘we’ know for sure how China will behave in international relations and what China’s ‘real goal’ is (even before the Chinese themselves know it) brings home this kind of ‘objective’ knowledge of others as narcissistic, modernist self-imagination. This self/Other construction, as I pointed out in Chapter 2, is particularly evident in regard to the U.S., whose dominant self-imagination has been essential to both the formation of its knowledge of others and to its often violent foreign policy trajectory in global politics based upon that knowledge.

#### No US-China war

**Rosecrance et al ‘10** (Richard, Political Science Professor @ Cal and Senior Fellow @ Harvard’s Belfer Center and Former Director @ Burkle Center of IR @ UCLA, and Jia Qingguo, PhD Cornell, Professor and Associate Dean of School of International Studies @ Peking University, “Delicately Poised: Are China and the US Heading for Conflict?” Global Asia 4.4, <http://www.globalasia.org/l.php?c=e251>)

**Will China and the US Go to War?** If one accepts the previous analysis, the answer is “no,” or at least not likely. Why? First, despite its revolutionary past, **China has** gradually **accepted the US-**led **world** order **and become a status quo power.** It has joined most of the important inter-governmental international organizations. It has subscribed to most of the important international laws and regimes. It has not only accepted the current world order, it has become a strong supporter and defender of it. China has repeatedly argued that the authority of the United Nations and international law should be respected in the handling of international security crises. China has become an ardent advocate of multilateralism in managing international problems. And China has repeatedly defended the principle of free trade in the global effort to fight the current economic crisis, despite efforts by some countries, including the US, to resort to protectionism. To be sure, there are some aspects of the US world order that China does not like and wants to reform. However, it wishes to improve that world order rather than to destroy it. Second, **China** has **clearly rejected** the option of **territorial expansion.** It argues that territorial expansion is both immoral and counterproductive: immoral because it is imperialistic and counterproductive because it does not advance one’s interests. China’s behavior shows that instead of trying to expand its territories, **it has been trying to settle** its border **disputes through negotiation**.

 Through persistent efforts, China has concluded quite a number of border agreements in recent years. As a result, most of its land borders are now clearly drawn and marked under agreements with its neighbors. In addition, China is engaging in negotiations to resolve its remaining border disputes and making arrangements for peaceful settlement of disputed islands and territorial waters. Finally, **even on** the question of **Taiwan**, which China believes is an indisputable part of its territory, **it has adopted** a policy of **peaceful reunification**. A country that handles territorial issues in such a manner is by no means expansionist. Third, **China has relied on trade** and investment **for** national welfare and **prestige, instead of** military **conquest.** And like the US, Japan and Germany, China has been very successful in this regard. In fact, so successful that **it** really **sees no other option than** to continue on **this path to prosperity**. Finally, after years of reforms, China increasingly finds itself sharing certain basic values with the US, such as a commitment to the free market, rule of law, human rights and democracy. Of course, there are still significant differences in terms of how China understands and practices these values. However, at a conceptual level, Beijing agrees that these are good values that it should strive to realize in practice. A Different World It is also important to note that certain changes in international relations since the end of World War II have made the peaceful rise of a great power more likely. To begin with, the emergence of nuclear weapons has drastically reduced the usefulness of war as a way to settle great power rivalry. By now, all great powers either have nuclear weapons or are under a nuclear umbrella. If the objective of great power rivalry is to enhance one’s interests or prestige, the sheer destructiveness of nuclear weapons means that these goals can no longer be achieved through military confrontation. Under these circumstances, countries have to find other ways to accommodate each other — something that China and the US have been doing and are likely to continue to do. Also, globalization has made it easier for great powers to increase their national welfare and prestige through international trade and investment rather than territorial expansion. In conducting its foreign relations, the US relied more on trade and investment than territorial expansion during its rise, while Japan and Germany relied almost exclusively on international trade and investment. China, too, has found that its interests are best served by adopting the same approach. Finally, the development of relative pacifism in the industrialized world, and indeed throughout the world since World War II, has discouraged any country from engaging in territorial expansion. **There is less and less popular support for using force to address even legitimate concerns** on the part of nation states. Against this background, efforts to engage in territorial expansion are likely to rally international resistance and condemnation. Given all this, is the rise of China likely to lead to territorial expansion and war with the US? The answer is no.

**Economics and relations prevent China-Taiwan war**

**Rosenberg 9** (David, Professor of Political Science – Middlebury College and Research Fellow at the Research School of Pacific and Asian Studies – Australian National University, “Dire Straits: Competing Security Priorities in the South China Sea”, The Asia-Pacific Journal, 3-20, http://japanfocus.org/-David-Rosenberg/1773)

**There is a** curious **pattern of accommodation** **in PRC-Taiwan relations**. On the one hand, the PRC views Taiwan as a renegade province while Taiwan views the mainland with cultural empathy but political disdain. **On many South China Sea** **issues**, however, **they are** often **in agreement. They have not had any direct confrontations** in the South China Sea. They make the same claims, use the same definitions, baselines, and maps in stating their interests in the region. There is even some direct cooperation between China and Taiwan on technical issues. Beyond these governmental links, **there are very substantial corporate and personal links between China and Taiwan**. Taiwanese firms have invested over US $100 billion on the mainland, more than any other country. Much of this involves the relocation of Taiwanese industries to the Shanghai-Suzhou and Fujian areas. To a large extent, **Taiwan's continued economic prosperity is tied to reintegration with the mainland**. **These** economic **links** of investment and trade **are reinforced by** **millions of personal visits** as well as mail and email correspondence. Bonds of marriage also strengthen these ties. Nearly 10% of Taiwanese men marry mainland brides, further tying migrant generations to ancestral origins. These deeply-rooted, long-term economic and demographic trends provide a counterbalance to the often strident political clashes. The longer and broader the cross-Strait engagement, the better the prospects for peaceful coexistence. Unfortunately, the cross-Strait issue has become immersed in domestic politics in Taiwan and China. The recent spate of threats and counter-threats over Taiwan's status is linked to maneuvering among domestic political forces seeking popular support. For example, in March 2005, after China passed its anti-secession law, there were widespread protest demonstrations in Taiwan led by Prime Minister Chen Shui-bian's Democratic Progressive Party (DPP). Soon after, a large delegation of Taiwan's main opposition party, the Kuomintang (KMT, Nationalist Party), visited the mainland to encourage trade and political dialogue with China and to pay respects to the memorial shrine of Sun Yat-sen, KMT's founder. This, in turn, was followed in early April by the visit of right-wing Taiwan Solidarity Union party leaders to the Yasukuni shrine, the Japanese war memorial in Tokyo. Clearly issues of national identity and national sovereignty can generate volatile reactions. The big danger across the Taiwan Strait is that misunderstanding and miscalculation, fueled by distrust, xenophobia, and opportunism, may lead to escalating conflict. Senior leaders on both sides of the Strait are beginning to realize the potential consequences if instability erupts into violence. Hu Jintao has recently been signaling that he advocates a long-term policy of stability for eventual reunification. Chen Shui-bian has recently dropped his independence demands. Several Southeast Asian leaders have opposed Taiwan's independence; most explicitly, Singapore's Prime Minister, Lee Hsien Loong. Lee bluntly stated, "If Taiwan goes for independence, Singapore will not recognize it. In fact no Asian country will recognize it. China will fight. Win or lose, Taiwan will be devastated." The prospect of a **military confrontation** between the mainland and Taiwan **is unlikely**, in part **because the consequences** of such a conflict **would be extremely destructive for both sides.** Diplomatic efforts are needed to avoid even this remote risk. In the March/April 2005 issue of Foreign Affairs, Kenneth Lieberthal offered a useful proposal to change the focus of negotiations over "independence" and "reunification" to a pragmatic question: what is needed to achieve long-term stability and peaceful coexistence between China and Taiwan? What confidence building measures are needed to reassure security strategists that defensive military developments are not offensive? What legal and administrative means are necessary to resolve routine conflicts that will inevitably occur as commercial and civil relations thicken? The current U.S. attempts to help Taiwan "contain" China and to mobilize support in its global war on terrorism threaten to complicate if not weaken regional security developments. As Ronald Montaperto notes, "the almost daily manifestations of Chinese economic power, the effort to demonstrate commitment to the 'new' principle that the economic development of individual nations is inseparable from the development of the region as a whole, and the broad perception within the region that the Chinese are willing to engage actively in multilateral, cooperative policies have combined to provide Beijing with an unprecedented measure of influence and even clout."[6] The **Beijing** regime **is obsessed with economic stability**, because it fears that a severe downturn would trigger social and political upheaval. **The last thing it wants is a military confrontation with its biggest trading partner**, the United States, or with Japan or Taiwan, each of which are major trade and investment partners. It may go on playing the nationalist card over Taiwan to curry domestic political favor, but **there has been** **no massive military build-up** **and there is no plausible threat of impending war**. [7] To the contrary, China is investing heavily in creating a regional security framework to pursue its domestic development. The U.S. goal of achieving genuine regional maritime security would best be served through cooperation with China -- one of its most important creditors, suppliers, and markets -- rather than confrontation.

## 2NC Kaldor

### 2NC – Alt

#### This debate round matters – critical interrogation of our war policy and adaptation to “new wars” is critical to create a new form of scholarship that is predicated on local, national, and global scholarship external from the status quo security apparatus.

Kaldor 13, Mary Kaldor, professor of Global Governance at the London School of Economics and Director of the Civil Society and Human Security Research Unit, “In Defence of New Wars,” March 7, 2013, Stability, 2(1): 4, pp. 1-16, <http://www.stabilityjournal.org/article/download/sta.at/40%E2%80%8E>

The debate about new wars has helped to refine and reformulate the argument. The debate about Clausewitz has facilitated a more conceptual interpretation of new wars, while the debate about data has led to the identification of new sources of evidence that have helped to substantiate the main proposition. The one thing the critics tend to agree is that the new war thesis has been important in opening up new scholarly analysis and new policy perspectives, which, as I have stressed, was the point of the argument (Newman 2004; Henderson and Singer 2002). The debate has taken this further. It has contributed to the burgeoning field of conflict studies. And it has had an influence on the intensive policy debates that are taking place especially within the military, ministries of defence and international organisations the debates about counter-insurgency in the Pentagon, for example, or about human security in the European Union and indeed about non-traditional approaches to security in general. What is still lacking in the debate is the demand for a cosmopolitan political response. In the end, policing, the rule of law, justice mechanisms and institution-building depend on the spread of norms at local, national and global levels, and norms are constructed both through scholarship and public debate. If we are to reconceptualise political violence as ‘new war’ or crime and the use of force as cosmopolitan law enforcement rather than war-fighting, then we have to be able to challenge the claims of those who conceptualise political violence as ‘old war’, and this can only be done through critical publicly-engaged analysis.

#### Globalization and collective security are inevitable, but our method and justification for how we should engage those structures is founded in our scholarship. Alt is a prerequisite and any risk of a link means you vote neg.

Kaldor 99, Mary Kaldor, professor of Global Governance a the London School of Economics and Director of the Civil Society and Human Security Research Unit, New & Old Wars, 1999, Stanford University Press, pg 123-124

The failure to take seriously alternative sources of power displays a myopia about the character of power and the relationship between power and violence. An effective response to the new wars has to be based on an alliance between international organizations and local advocates of cosmopolitanism in order to reconstruct legitimacy. A strategy of winning hearts and minds needs to identify with individuals and groups respected for their integrity. They have to be supported, and their advice, proposals, recommendations need to be taken seriously. There is no standard formula for a cosmopolitan response; the point is rather that, in each lsocal situation, there has to be a process involving these individuals and groups through which a strategy is developed. The various components of international involvement — the use of troops, the role of negotiation, funds for reconstruction — need to be worked out jointly. This argument also has implications for the way in which political pressure from the above is exerted on political and military leaders to reach agreement or to consent to peacekeeping forces. Typical methods include the threat of air strikes or economic sanctions, which have the consequence of identifying the leaders with the population instead of isolating them, treating them as representative of ‘sides’, as legitimate leaders of states or proto-states. Such methods can easily be counterproductive, alienating the local population and narrowing the possibilities of pressure below. There may be circumstances in which these methods are an appropriate strategy and others where more targeted approaches may be more effective — arraigning the leaders as war criminals so that they Cannot travel, exempting Cultural communication so as to support civil society, for example. The point is that local cosmopolitans can provide the best advice on what is the best approach; they need to be consulted and treated as partners.

### 2NC – Framework GENERAL

#### Fourth, we don’t preclude the 1AC or the possibility of policy focus, we just think that methodology is a prior question – means they don’t have offense. But even if they win policy simulation is good that makes the kritik more important – ethical and methodological questions are critical to avoid policy failure

McAllister et al 12 – School of Planning, Architecture and Civil Engineering Queen’s University Belfast (Keith, with Liu Ping Hui and Stephen McKay, “Evidence and Ethics in Infrastructure Planning”, International Journal of Applied Science and Technology Vol. 2 No. 5; May 2012, dml)

Lack of transparency on matters of policymaking and decision taking raise more ethical questions than answers. There was a definitive disinclination by key respondents to answer on such matters, inferring a reluctance to engage in fearless speech (Foucault, 1983). Nonetheless, such is the importance of these questions that those who provide leadership and wield power must be cognisant of the ramifications of not upholding the ethical standards and principles of legitimacy which justify their position. The professional-political relationship in decision taking is masked in shadow, though this investigation has yielded knowledge inferring that ethical dilemmas face planning practitioners on a daily basis, albeit that most do not perceive it to be a serious issue, as one respondent put it “it‟s just part of the job”.

Such perceptions undermine the ethos upon which the profession is founded and must be redressed. Rudimentary knowledge means that only speculation is possible on the dynamic which is located at the hub of policymaking and decision taking, therefore only those interacting at the foci of power truly understand how outputs emerge from interactive discursive processes. The evidence from this investigation did, however, indicate that cognisance must not just be taken of the professional-political relationship but the professional-professional relationship in the wider planning context. While the sample is admittedly small, there is clearly an issue to address with regard to the impact of power on professional ethics. Professionals, whatever their rank, have a responsibility to dissent (Marcuse, 1976) and it is disconcerting to think that where organisational legitimacy (Tilling, 2004) is taken as read, power-laden structures (Tewdwr-Jones and Allmendinger, 1998) may be conducive to the development of an inherent fear to express opinion as it might damage how, at best, they are perceived by their superiors or, at worst, impede career development.

While specifically testing the integrity of professional practitioners is almost impossible, it is vitally important that those who influence decisions at locations where power is wielded hold true to the ethical principles underpinning the profession. Failure to do so will ultimately lead to a catastrophic breakdown of societal approval (Kapland and Ruland, 1992) of the planning profession. Such a scenario may ultimately be conducive to the development and implementation of inappropriate policies and strategies which contribute to the demise of the environment which we strive to protect. Evidence from other jurisdictions suggests that the new infrastructure paradigm for operational practice is generally well placed to face such challenges in terms of “expertise and knowledge” (Sheridan, 2010, p. 10). The findings from this investigation suggest that commissioners and inspectors in the wider planning context are perceived as having the ethical robustness to distance themselves from challenges presented by powerbrokers; and the inherent nature of the approach is such that, unlike advocates who tactically manipulate knowledge or flagrantly misrepresent the truth, commissioners are programmed to use a balance sheet approach underpinned by impartiality (Marcuse, 1976). The task for the IPC commissioners is to remain cognisant of such ethical challenges and match the expectations achieved by their counterparts in other planning decision making arenas.

### A2 perm do both

#### Third, thinking that we can resist the structures of imperialism while endorsing problematic policies and world views ensures that we become amoral political subjects bound to imperial empathy. Any inclusion of the plan coopts the alternative and makes it a footnote.

Abbas 10, Asma Abbas, Professor and Division Head in Social Studies, Political Science, Philosophy at the Liebowitz Center for International Studies at Bard College at Simon’s Rock, Liberalism and Human Suffering: Materialist Reflections on Politics, Ethics, and Aesthetics, London: Palgrave Macmillan, pg. Pg. 38-39/

The dizzying back and forth between professed Kantians and Humeans blurs the fact that, regardless of whether morality is anchored interior to the acting subject or determined by the effects of the actions of the subject as they play out in the outside world, the unit of analysis is quite the same. Thus, when touchy liberals desire better attention to the fact of human pain and suffering, they manage to talk about cruelty where, ironically, cruel actions are derivatives of cruel agents and the victim’s suffering is just fallout. Besides this shared inability to dispel the primacy of the agent and the perpetrator in favor of the sufferer of pain, the rift between Kant and Hume is deceptive in another way. In terms of historical evolution, the current status of cruelty betrays a fetish of the active agent. It is no accident that the terms “good” and “evil” require a focus on cruelty and its infliction, leaving untouched the suffering of cruelty. Moral psychology ends up being the psychology of cruelty, which is amoral question, and hence of those who cause it. In the same frame, suffering is never a moral, let alone political or legal, question unless amoral agent with a conscience has caused it. All sufferers automatically become victims in the eyes of politics and law when “recognized.” Suffering is thus relevant as a political question only after it is a moral one, when it is embodied and located in a certain way, when it surpasses arbitrary thresholds. It is one thing to claim that liberalism, whether empiricist or idealist, cannot overcome its subject-centeredness even in its moments of empathy for the “victim.” It is another to understand the stubborn constitution of the agent at the helm of liberal justice and ask what makes it so incurable and headstrong and what the temperament of this stubbornness might be: is it pathetic, squishy, helplessly compassionate, humble, philanthropic, imperialist, venomous, neurotic, all of the above, or none of these? Not figuring out this pathos is bound to reduce all interaction with liberal assertions to one or another act of editing or “correcting” them. Inadvertently, all protests to liberalism tread a limited, predictable path and will be, at some point, incorporated within it. Liberalism’s singular gall and violence is accessed every time a resistance to it is accommodated by liberalism. Think, for instance, not only of how often liberals affirm their clumsiness and mediocrity in speaking for the other’s suffering but also of how quickly its antagonists—purveyors of many a righteous anti-representational politics—“make space” for the voice of others without challenging the (liberal, colonizing) structures that determine and distribute the suffering and speaking self, and the suffering and speaking other, to begin with. This protest leaves unquestioned what it means to speak for one’s own, or others’, suffering and whether there are other ways of speaking suffering that problematize these as the only options.

#### Fourth, reject every instance – perequisite to political reformation

Galli 10, Carlo Galli, Professor of Political Philosophy at the Univeristy of Bologna, Politics Spaces and Global War, trans. Adam Sitze, p. 188

Rather than denying the theoretico-political novelty of Global War, ratherthan closing our eyes to the fact that Global War radically challengesmodern political philosophy and its categories, and rather than continuing to believe that globalization is not the horizon that determines ourexperience today, our task is to begin to think the novelties, the paradoxes and the aporiac of globalization. We must ask ourselves about its possibilities—not in order to stabilize it, for that would be impossible—but in order to imagine routes within it that would make for a less tumultuous crossing of the sea the world has become.If we do not want to make the mistake of applying old remedies to new illnesses, or to wander ¡n vain in our own smug conceptuality (which has become nothing but ineffectual jargon), we must remember that we scholars need to apply a mix of good sense, humility and theoretical radicalism.This will give us a renewed capacity for observation and analysis, Political philosophy should not institute itself primarily as a public elaboration of criteria of judgment, or as the rational production of a set of guiding values to be put into practice; it should not seek to be a discourse internalto the City. Before it takes on these tasks, it must first begin the radical deconstruction of its own concepts; it must clear the rubble of the Modern off the ground—for today, that rubble hinders more than it helps.

### A2 Negative State Action

#### Thinking that we can reform the state only marginalizes and coopts the voices of the oppressed. We have to completely reject the system.

Nayar 99 Copyright (c) 1999 Transnational Law & Contemporary Problems Transnational Law & Contemporary Problems Fall, 1999 9 Transnat'l L. & Contemp. Probs. 599. “SYMPOSIUM: RE-FRAMING INTERNATIONAL LAW FOR THE 21ST CENTURY: Orders of Inhumanity” Jayan Nayar (Ph. D from the University of Cambridge, Professor of International Development Law and Human Rights and the University of Warwick) cylab.info/u/JQ/texts/Nayar-\_Orders\_of\_Inhumanity.doc)

Thus, just as the aspirations of most anti-colonial elite leaderships were infused with the colonizer's visions of human progress--the languages of "statehood," of "modernization," of "institution building, and the like--so too now the languages of the elites of "civil society" reflect the terrain as demarcated by contemporary world-orderists. Development, democracy, human rights, NGO "networks," even "education" and "law," are all contemporary slogans that are repeated in the hope of a progressive civilizational movement toward human emancipation. And increasingly, these "transnational," even "global," languages of human emancipation are formulated and articulated within professional sites of resistance and activism that stand as mirrors of ordering institutions; for the government committee there are the NGO forums, for the ministerial conference there is the "alternative" conference of civil society delegates, for the business/corporate coalition with government there are the similar NGO partnerships. The play of critique and legitimization, of compromise and cooperation, of review and reformulation, is thereby enabled, taking on a [\*625] momentum and a rationale of its own, becoming an activity of grand proportions where the activity itself becomes a reason for, and object of perpetuation. To be outside of these circles of "communication" is deemed to be without "voice," which is for the critic, an unacceptable silencing. To be inside these circles, however, entails a constant torment of co-option, betrayal and appropriation of voice.

### A2 Security good

#### Justifications of security and threat construction enforce colonialism and prop up imperialism

Nayar 99 Copyright (c) 1999 Transnational Law & Contemporary Problems Transnational Law & Contemporary Problems Fall, 1999 9 Transnat'l L. & Contemp. Probs. 599. “SYMPOSIUM: RE-FRAMING INTERNATIONAL LAW FOR THE 21ST CENTURY: Orders of Inhumanity” Jayan Nayar (Ph. D from the University of Cambridge, Professor of International Development Law and Human Rights and the University of Warwick) cylab.info/u/JQ/texts/Nayar-\_Orders\_of\_Inhumanity.doc

"Security" is another bulwark of the "new world-order." This is not surprising, for "development" requires the creation of conditions that facilitate its implementation and that ensure the obedience, if not the subservience, of those to be "developed." Security, as a motive for ordering, has been a useful distraction for this purpose, as is demonstrated by its transformation from a precept of coexistence to a common cause of globalization. From its very conception, the current framework of international order, constructed through the United Nations Charter, had as its fundamental rationale the creation of conditions of security. Born out of the expressed aspirations of the Atlantic Charter n26 amid the early phases of the Second World War, the postwar UN Charter begins with words that were intended to resonate generations down the line: "We the Peoples of the United Nations Determined to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind. . . ." n27 [\*613] With these visions of an order freed from the madness of states in conflict, there was created a basis for collective responsibility in the preservation of peace--the collective security regime under the supervision of the Security Council, and particularly, its "Permanent Members," as stipulated in Chapter VII of the UN Charter. n28 Many further refinements to these high ideals have since been made as the post-UN Charter world-order evolves. With the end of formal colonialism, attention was transferred in the 1960s and 1970s to the perceived importance of elaborating on principles of non-aggression and non-intervention. The 1980s and 1990s have seen a reversal of enthusiasms, however, as interest is being increasingly expressed, especially within "Western" states, for a more "collective" undertaking of responsibility in matters of security. This includes the forwarding of arguments in favor of "humanitarian intervention" in cases of "internal" conflicts. n29 These trends in the changing outlook on "security" and its relationship to "sovereignty" have continued, and have recently resulted in the formation of a permanent International Criminal Court to bring to justice perpetrators of "genocide," "war crimes" and "crimes against humanity." n30 Ever so gradually, it seems, the "new world-order" is moving away from the statist pillars of sovereignty and domestic jurisdiction to a globalist notion of collective rights and responsibilities. Yet, as the following two observations on the nature of the global "security" landscape demonstrate, the realities of ordering that have flowed from reiterations of the commitment to non-violence have failed to establish a legacy of security for the majority of the global population: The period since 1945 may be regarded as a long peace only in the restricted sense that there has been no war between major powers. In other respects, and for much of the world, it has been a period of frequent wars. . . . By one estimate, between 1945 and 1989 there were 138 wars, resulting in some 23 million deaths. . . . All 138 wars were fought in the Third World, and many were fuelled by weapons provided by the two major powers [the United States and the Soviet Union] or their allies. n31 The twentieth-century is a period of history which, in the words of anthropologist Marvin Harris, has seen "a war to end all wars followed by a war to make the world safe for [\*614] democracy, followed by a world full of military dictatorships." We were then promised a New World-order as the reward for agreeing to the Gulf War, as the end of the Cold War gave way to a seemingly endless series of intra-state wars which the international community is unwilling or unable to bring to order. n32 Once again, from the perspective of the ordered, the order of security has proved to be the ideological weapon for the systematic infliction of violence. It is not so much the order of security that is of interest here, but rather, the ordering which takes place in its guise. And with the passing of history, so has the legitimizing claim for the necessity of violent ordering for "security" purposes--fascism, colonialism, communism, capitalism (depending on the ideological orientation of the claimant), terrorism (particularly of the Islamic bent). There is always an enemy, sometimes internal, sometimes external, threatening the well-being of the people. The languages of nationalism and sovereignty, of peace and collective security, constructed to suit whichever threat happens to be in fashion, are passionately employed; the anarchy that is a Hobbesian state of nature is always the prophesied consequence of the lack of order that is impending. And the price that the "ordered" has to pay for all this "security" in the post-colonial, new world-order?: the freedom of those who order to be violent! From a "nationalist" standpoint, the rhetoric would insist that the security of the state is paramount, all else flowing from it. By this perspective, the state, that prize which was (re)gained from the colonial epoch, that jewel to be protected by the international order of "collective security," becomes the expression of the dignity of the "people," no questions asked. n33 From the anti-colonial struggle, from independence, the reasoning flows naturally, it seems, that the State is to be preserved from any challenge. The police, the military, and the secret service, purportedly given sight and hearing by the eyes and the ears of "the people," are the trophies of "independence." Overnight, the term "freedom fighter" is banished from the vocabulary of the state, the notion of the "terrorist" becomes its replacement. Overnight, the revolution is terminated, with "counter-revolution" becoming [\*615] the label for any attempt to challenge the new status quo. Overnight, supposedly, the basic structures for freedom from violence are achieved--the condition of "security" that must be preserved is attained. Of course, the post-colonial state could not construct this security alone. In the spirit of the new "co-operation," where security is a global concern, the contribution by the "international community," providing the basic instruments of and training for security, proves essential. n34 From this "internationalist," arguably now, global, perspective, this "freedom to be violent" is a selective freedom, however. In some cases--in Turkey, Mexico, Burma, and until recently, in Indonesia, for example--the preserve of the state to "secure" its jurisdictional space is maintained, even encouraged, if not supported. In others--Kosovo and Iraq, for example--this "freedom to be violent" is denounced with the force of righteousness that automatically flows from the labeling of actions as "genocide," "crimes against humanity," "ethnic cleansing," or "holocaust." Most other cases, however, remain largely outside of global vision--Angola, Sierra Leone, Tibet, and Liberia being examples--where the sensitivities of morality are little disturbed by the apparent inconsequentiality of the deaths, pain and fear, the insecurity, of those sectors of humanity. Why this discrepancy in the international community's moral judgment on violence and "insecurity"? It may be that no "development" stakes presently exist for the international community with regard to the fate of these nameless, faceless wretches; they are so deemed unworthy of a starring role in the real-life dramas of prime-time television. Media hype and its feeding of the fixation of the arm-chair audience who are the ratings-figures that inform the corporate media of "newsworthiness" notwithstanding, the reality of insecurity is that it is a localized experience. No amount of editorial juxtapositioning of "shots" of suffering is able to capture fear and pain. "Insecurity" is beyond "order;" it either exists as an experiential reality or it does not. And where it does exist, it exists as a result of relationships of violence. Issues of complicity here warrant little air-time. Less compelling are revelations that distant suffering is not often the result of depravities "out there," but rather, the outcome of "securities" enforced on [\*616] "our" behalf. In this respect, I wonder for whom projections of order are (re)articulated at timely intervals. Is it for the secure who need reassurance to dissuade the suspicions within their conscience, or for the insecure whose very bodies and minds are the material "subjects" and objects of the very real effects of the ordering that is violence?

#### Vote neg on ethics – colonialism must be rejected in every instance, ZERO risk of good repesentations with a risk link.

Shaikh 07, Nermeen Shaikh, senior fellow at Asia Source, “Interrogating Charity and the Benevolence of Empire,” 2007, Development 50, Palgrave-Journals

It would probably be incorrect to assume that the principal impulse behind the imperial conquests of the 18th and 19th centuries was charity. Having conquered large parts of Africa and Asia for reasons other than goodwill, however, countries like England and France eventually did evince more benevolent aspirations; the civilizing mission itself was an act of goodwill. As Anatol Lieven (2007) points out, even 'the most ghastly European colonial project of all, King Leopold of Belgium's conquest of the Congo, professed benevolent goals: Belgian propaganda was all about bringing progress, railways and peace, and of course, ending slavery'. Whether or not there was a general agreement about what exactly it meant to be civilized, it is likely that there was a unanimous belief that being civilized was better than being uncivilized—morally, of course, but also in terms of what would enable the most in human life and potential. But what did the teaching of this civility entail, and what were some of the consequences of changes brought about by this benevolent intervention? In the realm of education, the spread of reason and the hierarchies created between different ways of knowing had at least one (no doubt unintended) effect. As Thomas Macaulay (1935) wrote in his famous Minute on Indian Education, We must at present do our best to form a class who may be interpreters between us and the millions whom we govern; a class of persons, Indian in blood and colour, but English in taste, in opinions, in morals, and in intellect. To that class we may leave it to refine the vernacular dialects of the country, to enrich those dialects with terms of science borrowed from the Western nomenclature, and to render them by degrees fit vehicles for conveying knowledge to the great mass of the population. This meant, minimally, that English (and other colonial languages elsewhere) became the language of instruction, explicitly creating a hierarchy between the vernacular languages and the colonial one. More than that, it meant instructing an elite class to learn and internalize the culture—in the most expansive sense of the term—of the colonizing country, the methodical acculturation of the local population through education. As Macaulay makes it clear, not only did the hierarchy exist at the level of language, it also affected 'taste, opinions, morals and intellect'—all essential ingredients of the civilizing process. Although, as Gayatri Chakravorty Spivak points out, colonialism can always be interpreted as an 'enabling violation', it remains a violation: the systematic eradication of ways of thinking, speaking, and being. Pursuing this line of thought, Spivak has elsewhere drawn a parallel to a healthy child born of rape. The child is born, the English language disseminated (the enablement), and yet the rape, colonialism (the violation), remains reprehensible. And, like the child, its effects linger. The enablement cannot be advanced, therefore, as a justification of the violation. Even as vernacular languages, and all habits of mind and being associated with them, were denigrated or eradicated, some of the native population was taught a hegemonic—and foreign—language (English) (Spivak, 1999). Is it important to consider whether we will ever be able to hear—whether we should not hear—from the peoples whose languages and cultures were lost? The colonial legacy At the political and administrative levels, the governing structures colonial imperialists established in the colonies, many of which survive more or less intact, continue, in numerous cases, to have devastating consequences—even if largely unintended (though by no means always, given the venerable place of divide et impera in the arcana imperii). Mahmood Mamdani cites the banalization of political violence (between native and settler) in colonial Rwanda, together with the consolidation of ethnic identities in the wake of decolonization with the institution and maintenance of colonial forms of law and government. Belgian colonial administrators created extensive political and juridical distinctions between the Hutu and the Tutsi, whom they divided and named as two separate ethnic groups. These distinctions had concrete economic and legal implications: at the most basic level, ethnicity was marked on the identity cards the colonial authorities introduced and was used to distribute state resources. The violence of colonialism, Mamdani suggests, thus operated on two levels: on the one hand, there was the violence (determined by race) between the colonizer and the colonized; then, with the introduction of ethnic distinctions among the colonized population, with one group being designated indigenous (Hutu) and the other alien (Tutsi), the violence between native and settler was institutionalized within the colonized population itself. The Rwandan genocide of 1994, which Mamdani suggests was a 'metaphor for postcolonial political violence' (2001: 11; 2007), needs therefore to be understood as a natives' genocide—akin to and enabled by colonial violence against the native, and by the new institutionalized forms of ethnic differentiation among the colonized population introduced by the colonial state. It is not necessary to elaborate this point; for present purposes, it is sufficient to mark the significance (and persistence) of the colonial antecedents to contemporary political violence. The genocide in Rwanda need not exclusively have been the consequence of colonial identity formation, but does appear less opaque when presented in the historical context of colonial violence and administrative practices. Given the scale of the colonial intervention, good intentions should not become an excuse to overlook the unintended consequences. In this particular instance, rather than indulging fatuous theories about 'primordial' loyalties, the 'backwardness' of 'premodern' peoples, the African state as an aberration standing outside modernity, and so forth, it makes more sense to situate the Rwandan genocide within the logic of colonialism, which is of course not to advance reductive explanations but simply to historicize and contextualize contemporary events in the wake of such massive intervention. Comparable arguments have been made about the consolidation of Hindu and Muslim identities in colonial India, where the corresponding terms were 'native' Hindu and 'alien' Muslim (with particular focus on the nature and extent of the violence during the Partition) (Pandey, 1998), or the consolidation of Jewish and Arab identities in Palestine and the Mediterranean generally (Anidjar, 2003, 2007).

### A2 No Link

Gregory 11. Derek Gregory, professor of geography at the University of British Columbia, “The Everywhere War,” he Geographical Journal, Vol. 177, No. 3, September 2011, pg. 246

The question is a good one, but it needs to be directed outwards as well as inwards. For the United States is also developing an offensive capacity in cyberspace, and the mission of CYBERCOM includes the requirement ‘to prepare to, and when directed conduct, full-spectrum military cyberspace opera- tions in order to enable actions in all domains’. This is a programmatic statement, and there are difficult con- ceptual, technical and operational issues to be resolved. The concept of the ‘cyber kill-chain’ has already made its appearance: software engineers at Lockheed Martin have identified seven phases or ‘border-crossings’ in cyberspace through which all advanced persistent intrusions must pass so that, con- versely, blocking an attack at any one of them (dislo- cating any link in the kill-chain) makes it possible ‘to turn asymmetric battle to the defender’s advantage’ (Croom 2011; Holcomb and Shrewsbury 2011). The issues involved are also ethical and legal. Debate has been joined about what constitutes an armed attack in cyberspace and how this might be legally codified (Dipert 2010; Nakashima 2010), and most of all about how to incorporate the protection of civilians into the conduct of cyber warfare. In the ‘borderless realm of cyberspace’ Hughes (2010, 536) notes that the boundary between military and civilian assets – and hence military and civilian targets – becomes blurred, which places still more pressure on the already stressed laws of armed conflict that impose a vital distinction between the two (Kelsey 2008). Pre- paring for offensive operations includes developing a pre-emptive precision-strike capacity, and this is – precisely – why Stuxnet is so suggestive and why Shakarian (2011) sees it as inaugurating ‘a revolution in military affairs in the virtual realm’. Far from ‘carpet bombing’ cyberspace, Gross (2011) describes Stuxnet as a ‘self-directed stealth drone’ that, like the Predator and the Reaper, is ‘the new face of twenty- first century warfare’. Cyber wars will be secret affairs, he predicts, waged by technicians ‘none of whom would ever have to look an enemy in the eye. For people whose lives are connected to the targets, the results could be as catastrophic as a bombing raid but would be even more disorienting. People would suffer, but [they] would never be certain whom to blame.’¶ Contrapuntal geographies¶ I have argued elsewhere that the American way of war has changed since 9/11, though not uniquely because of it (Gregory 2010), and there are crucial continuities as well as differences between the Bush and Obama administrations: ‘The man who many considered the peace candidate in the last election was transformed into the war president’ (Carter 2011, 4). This requires a careful telling, and I do not mean to reduce the three studies I have sketched here to a single interpretative narrative. Yet there are connections between them as well as contradictions, and I have indicated some of these en route. Others have noted them too. Pakistan’s President has remarked that the war in Afghanistan has grave consequences for his country ‘just as the Mexican drug war on US borders makes a difference to American society’, and one scholar has suggested that the United States draws legal authority to conduct military operations across the border from Afghanistan (including the killing of bin Laden, codenamed ‘Geronimo’) from its history of extra-territorial opera- tions against non-state actors in Mexico in the 1870s and 1880s (including the capture of the real Geronimo) (Margolies 2011). Whatever one makes of this, one of the most persistent threads connecting all three cases is the question of legality, which runs like a red ribbon throughout the prosecution of late modern war. On one side, commentators claim that new wars in the global South are ‘non-political’, intrinsically predatory criminal enterprises, that cartels are morphing into insurgencies, and that the origins of cyber warfare lie in the dark networks of cyber crime; on the other side, the United States places a premium on the rule and role of law in its new counterinsurgency doctrine, accentuates the involvement of legal advisers in targeting decisions by the USAF and the CIA, and even as it refuses to confirm its UAV strikes in Pakistan provides arguments for their legality.¶ The invocation of legality works to marginalise ethics and politics by making available a seemingly neutral, objective language: disagreement and debate then become purely technical issues that involve matters of opinion, certainly, but not values. The appeal to legality – and to the quasi-judicial process it invokes – thus helps to authorise a widespread and widening militarisation of our world. While I think it is both premature and excessive to see this as a transformation from governmentality to ‘militariality’ (Marzec 2009), I do believe that Foucault’s (2003) injunction – ‘Society must be defended’ – has been transformed into an unconditional imperative since 9/11 and that this involves an intensifying triangulation of the planet by legality, security and war. We might remember that biopolitics, one of the central projects of late modern war, requires a legal armature to authorise its interven- tions, and that necropolitics is not always outside the law. This triangulation has become such a common- place and provides such an established base-line for contemporary politics that I am reminded of an inter- view with Zizek soon after 9/11 – which for him marked the last war of the twentieth century – when he predicted that the ‘new wars’ of the twenty-first century would be distinguished by a radical uncertainty: ‘it will not even be clear whether it is a war or not’ (Deich- mann et al. 2002).

HANSEN AND NISSENBAUM 2009 (Lene, Associate Professor, Director of the Ph.d. Program, Department of Political Science, University of Copenhagen. AND\*\*\* Helen, Professor, New York University, Media, Culture, and Communication & Computer Science, Digital Disaster, Cyber Security, and the Copenhagen School, International Studies Quarterly (2009) 53, 1155–1175)

 As in most academic fields, computer scientists have disagreed on the likelihood of different forms of attacks, and since the field is also cloaked in military or business secrecy, the ‘‘normal’’ follower of these debates learns ‘‘that much is withheld or simply not known, and estimates of damage strategically either wildly exaggerated or understated’’ (Nissenbaum 2005:72). These fluctuations also facilitate a coupling of radical threats with techno-utopian solutions.11 The National Strategy (2003:35) for instance couples a series of securitizations with an exuberant faith in the development of ‘‘highly secure, trust-worthy, and resilient computer systems. In the future, working with a computer, the Internet, or any other cyber system may become as dependable as turning on the lights or the water.’’ Leaving aside that for the majority of the world’s poor, and even for the impoverished American, turning on the light or water may not be entirely dependable, this echoes a technological utopianism that sidesteps the systemic, inherent ontological insecurity that computer scientists consistently emphasize. It also invokes an inherent tension between disaster and utopia as the future of cyber security. The constitution of expert authority in cyber technifications invokes furthermore the tenuous relationship between ‘‘good’’ knowledge and ‘‘bad’’ knowledge, between the computer scientist and the hacker. The hacker, argues Nissenbaum (2004), has undergone a critical shift in Western policy and media discourse, moving from a previous subject position as geeky, apolitical, and driven by the boyish challenge of breaking the codes to one of thieves, vandals, and even terrorists.12 Although ‘‘hackers’’ as well as others speaking on behalf of ‘‘hacktivista’’—the use of hacking for dissident, normatively desirable purposes— have tried to reclaim the term (Deibert 2003), both official and dissident discourse converge in their underscoring of the general securitization of the cyber sector insofar as past political hacker naivety is no longer possible. The privileged role allocated to computer and information scientists within cyber security discourse is in part a product of the logic of securitization itself: if cyber security is so crucial it should not be left to amateurs. Computer scientists and engineers are however not only experts, but technical ones and to constitute cyber security as their domain is to technify cyber security. Technifications are, as securitizations, speech acts that ‘‘do something’’ rather than merely describe, and they construct an issue as reliant upon technical, expert knowledge, but they also simultaneously presuppose a politically and normatively neutral agenda that technology serves. The mobilization of technification within a logic of securitization is thus one that allows for a particular constitution of epistemic authority and political legitimacy (Huysmans 2006:6–9). It constructs the technical as a domain requiring an expertise that the public (and most politicians) do not have and this in turn allows ‘‘experts’’ to become securitizing actors while distinguishing themselves from the ‘‘politicking’’ of politicians and other ‘‘political’’ actors. Cyber security discourse’s simultaneous securitization and technification work to prevent it from being politicized in that it is precisely through rational, technical discourse that securitization may ‘‘hide’’ its own political roots.13 The technical and the securitized should therefore not be seen as opposed realms or disjunct discursive modalities, but as deployable in complex, interlocking ways; not least by those securitizing actors who seek to depoliticize their discourses’ threat and enemy constructions through linkages to ‘‘neutral’’ technologies. A securitization by contrast inevitably draws public attention to what is done in the name of security and this provides a more direct point of critical engagement for those wishing to challenge these practices than if these were constituted as technical.

Pan 4 (Chengxin, Department of Political Science and International Relations, Faculty of Arts, Deakin University, Discourses Of ‘China’ In International Relations: A Study in Western Theory as (IR) Practice, p. 255-256)

For example, as I pointed out in Chapter 5, the ‘China threat’ as conceived by Richard Bernstein, Ross Munro, Richard Betts, and Thomas Christensen, has been derived less from an ‘objective’ examination of China’s military capabilities, strategic posture, or actual foreign behaviour, and more from a (neo)realist conception of China as an aggressive, threatening entity in an unremittingly anarchic system. This conception, in turn, is derived from an entrenched understanding of the Western/American self as the rational orderer of the system, an understanding which has long been passed as the universal reality of world politics per se. The neorealist John Mearsheimer sums up this perspective well in proposing that: If… China becomes not only a leading producer of cutting-edge technologies but also the world’s wealthiest great power, it would almost certainly use its wealth to build a mighty military machine. For sound strategic reasons, moreover, it would surely pursue regional hegemony, just as the United States did in the western hemisphere during the nineteenth century. So if Chinese relative power grows substantially, one should expect it to attempt to dominate Japan and South Korea, as well as other regional actors, by building military forces that are so powerful that those other states would not dare challenge it. One should also expect it to develop its own version of the Monroe Doctrine, directed at the United States; just as the United States has made it clear to distant great powers that they are not allowed to meddle in the western hemisphere, China will make it clear that American interference in Asia is unacceptable [emphases added].12 This is a typical example of Western discourse allowing no room for an understanding of China outside the parameters of Western self-perception, an argument that, as I illustrated in Chapter 6, is equally applicable to the (neo)liberal perspective. In this latter context, for example, Western efforts to report and depict the Tiananmen uprising of 1989 as a ‘pro-democracy’ movement relied on ‘pro-Western’ interpretations of the movement’s motives, interpretations not easily attached to the event. It is as if the Tiananmen movement would make little sense were it not a specific example of the worldwide democratic wave to become more like ‘us.’ Thus, setting out to know the specifically different society called ‘China,’ both realist and liberal discourses have invariably ended up ‘discovering’ the same world everywhere, a world essentially of their own making. The very notion that ‘we’ know for sure how China will behave in international relations and what China’s ‘real goal’ is (even before the Chinese themselves know it) brings home this kind of ‘objective’ knowledge of others as narcissistic, modernist self-imagination. This self/Other construction, as I pointed out in Chapter 2, is particularly evident in regard to the U.S., whose dominant self-imagination has been essential to both the formation of its knowledge of others and to its often violent foreign policy trajectory in global politics based upon that knowledge.

## 2NC Preemption

### 2NC – turns

#### Cyber-threats are completely hypothetical, causes preemption and loss of civil liberties – turns case

Hart 11 (Catherine Hart is a masters student in communications at Simon Fraser University, "Mobilizing the Cyberspace Race: the Securitization of the Internet and its Implications for Civil Liberties", Cyber-Surveillance in Everyday Life: An International Workshop, May 12-15, 2011)

The key component of a securitization is that a dire threat is posed to the referent object which¶ will ultimately result in its destruction. An existential threat to the nation is usually posed in¶ terms of a threat to sovereignty. Critical infrastructures and the computer networks which¶ connect them must therefore not simply be understood as important to the functioning of the¶ nation, but essential. Critically, Buzan et al suggested in 1998 that cybersecurity was a failed¶ securitization because, in their view, a cyber attack would not cause cascading effects throughout¶ society, but rather would only be felt within the computer field (1998, 25). Nissenbaum and¶ Hansen questioned this view in 2009, as networked computing has become increasingly¶ embedded in all areas of society, and in fact Rachel E. Yould suggests that “IT may be the¶ common underlying factor upon which all security sectors are destined to converge” (as cited in¶ Hansen & Nissenbaum, 2009, 1157). CF illustrates this existential threat well, stating “the nation¶ is so dependent on our infrastructures that we must view them through a national security lens.¶ They are essential to the nation’s security, economic health, and social well being. In short, they¶ are the lifelines on which we as a nation depend” (PCCIP, 1997, 11).¶ The NSSC refers to digital infrastructure as “essential to our economy, security, and way of life”¶ (DHS, 2003, iii) and therefore aims to “reduce our Nation’s vulnerability to debilitating attacks¶ against our critical information infrastructures or the physical assets that support them” (viii).¶ The existential threat is legitimized by references to traditional threats to national security, such¶ as war and terrorism. This is important because the cyber-threat is entirely hypothetical, as is the¶ case in any securitization. Buzan et al explain that security arguments “are about the future,¶ about alternative futures—always hypothetical—and about counterfactuals. A security argument¶ always involves two predictions: What will happen if we do not take "security action’... and what¶ will happen if we do” (1998, 32). Drawing parallels with past examples to justify a security¶ action, and to threaten disaster if no action is taken, gives legitimacy to the argument that a¶ government should act pre-emptively, rather than wait for disaster to strike. To this end, CF¶ draws comparisons between a “cyber attack” and attacks using chemical, biological, and nuclear weapons (PCCIP, 1997, 14), and all three documents invoke the public memory of specific past¶ attacks or threats to the security of the U.S., from Pearl Harbour to the Cold War to the¶ Oklahoma City bombings and 9/11. The links between the 9/11 terrorist attacks and potential¶ future cyber attacks are, unsurprisingly, drawn most clearly in the NSSC, which was written as a¶ component of the National Strategy for Homeland Security, part of the regulation responding to¶ the terrorist attacks of September 11, 2001. A clear but largely imaginary link is drawn between¶ the terrorist attacks and potential future cyber attacks in the following statement:¶ [u]ntil recently overseas terrorist networks had caused limited damage in the United¶ States. On September 11, 2001, that quickly changed. One estimate places the increase in¶ cost to our economy from attacks to U.S. information systems at 400 percent over four¶ years. While those losses remain relatively limited, that too could change abruptly (DHS,¶ 2003, 10).¶ The imperative to act sooner rather than later is then emphasized by the line, “[c]yber attacks can¶ burst onto the Nation’s networks with little or no warning and spread so fast that many victims¶ never have a chance to hear the alarms” (DHS, 2003, 7). This is consistent with Nissenbaum and¶ Hansen’s identification of the establishment of a complacent audience that is unaware of the¶ impending danger, which is another key trope of securitizing discourse (2009, 1161). This logic¶ can be used to persuade policy-makers of the greater good that can be accomplished by placing¶ restrictions on the Internet, even if doing so potentially infringes on civil liberties. As Arnold¶ Wolfers explains, ‘national security’ is an ambiguous concept for which there are different¶ understandings. This will therefore prompt different responses, which could be “praised for their¶ self-restraint and the consideration which this implies for values other than security [or] they¶ may instead be condemned for being inadequate to protect national values” (Wolfers, 1952, 501).¶ It is perhaps better to err on the side of caution, and support more restrictive policies, than to be¶ seen as having risked national security and a repeat of the physical and psychological damage of¶ 9/11.

#### No cyber-war- attacks fail and don’t escalate

**Gartzke ’12** [Erik A. Gartzke, Associate Professor of Political Science at UC San Diego, PhD in International Relations from Iowa, “The Myth of Cyberwar,” <http://dss.ucsd.edu/~egartzke/papers/cyberwar_12062012.pdf>]

There is a problem with the growing consensus of impending cyber apocalypse, however: it is¶ far from clear that conflict over the internet can actually function as war. Discussions of cyberwar¶ commit a common fallacy of arguing from opportunity to outcome, rather than considering whether¶ something that could happen is at all likely, given the motives of those who are able to act.¶ Cyber pessimism rests heavily on capabilities (means), with little thought to a companion logic of¶ consequences (ends). Much that could happen in the world fails to occur, largely because those¶ capable of initiating action discern no benefit from doing so. Put another way, advocates have yet¶ to work out how cyberwar actually accomplishes the objectives that typically sponsor terrestrial¶ military violence. Absent a logic of consequences, it is difficult to believe that cyberwar will prove as devastating for world affairs and for developed nations in particular as many seem to believe.¶ This essay assesses the salience of the internet for carrying out functions commonly identified with terrestrial political violence. War is fundamentally a political process, as Clausewitz¶ (1976[1832]) famously explained. States, groups and individuals threaten harm to deter or compel,¶ generating influence through the prospect of damage or loss. Military violence can also be exercised¶ to alter or maintain the balance of power and to resist or impose disputed outcomes. The internet¶ is generally an inferior substitute to terrestrial force in performing the functions of coercion or conquest. Cyber \war" is not likely to serve as the final arbiter of competition in an anarchical world¶ and so should not be considered in isolation from more traditional forms of political violence.2¶ In¶ fact, the capacity for internet coercion is limited by the same factors that make cyberwar appear¶ at first to be so intimidating. For threats or demands to prove effective, targets must believe both¶ that an attack is likely to follow from noncompliance, and that the attack is destined to inflict¶ unacceptable harm. Yet, as I detail here, the need to apprise targets of internet vulnerabilities in¶ order to make cyber threats credible contrasts with the secrecy needed to ensure an effective attack.¶ Since it is difficult to share operational details of planned attacks without compromising military¶ effectiveness, cyberwar must be practiced more often than threatened. Here too, however, there are¶ critical limitations to what can be achieved via the internet. It is one thing for an opponent to idle¶ a country's infrastructure, communications or military capabilities. It is quite another to ensure¶ that the damage inflicted translates into a lasting shift in the balance of national capabilities or¶ resolve. Cyber attacks are unlikely to prove particularly potent in grand strategic terms unless they¶ are accompanied by terrestrial military force or other actions designed to capitalize on temporary¶ weakness effected over the internet. Perpetrators must therefore be prepared to exploit windows of¶ opportunity generated by internet attacks through other modes of combat. Otherwise, there are few¶ compelling reasons to initiate cyberwar in the first place. The chief beneficiaries of cyberwar are thus¶ less likely to be weak or rising powers than those states that already possess important terrestrial¶ military advantages. Conceived of in this way, the internet is less a revolution in military a airs¶ than it is yet another set of technologies that extend existing disparities in power and influence.

#### No cyber war

**Libicki 8-14**-13 [Martin C. Libicki, Ph.D. in economics, M.A. in city and regional planning, University of California, Berkeley; S.B. in mathematics, Massachusetts Institute of Technology, Senior Management Scientist at RAND, “Don't Buy the Cyberhype,” <http://www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype>]

These days, most of Washington seems to believe that a major cyberattack on U.S. critical infrastructure is inevitable. In March, James Clapper, U.S. director of national intelligence, ranked cyberattacks as the greatest short-term threat to U.S. national security. General Keith Alexander, the head of the U.S. Cyber Command, recently characterized “cyber exploitation” of U.S. corporate computer systems as the “greatest transfer of wealth in world history.” And in January, a report by the Pentagon’s Defense Science Board argued that cyber risks should be managed with improved defenses and deterrence, including “a nuclear response in the most extreme case.”¶ Although the risk of a debilitating cyberattack is real, the perception of that risk is far greater than it actually is. No person has ever died from a cyberattack, and only one alleged cyberattack has ever crippled a piece of critical infrastructure, causing a series of local power outages in Brazil. In fact, a major cyberattack of the kind intelligence officials fear has not taken place in the 21 years since the Internet became accessible to the public.¶ Thus, while a cyberattack could theoretically disable infrastructure or endanger civilian lives, its effects would unlikely reach the scale U.S. officials have warned of. The immediate and direct damage from a major cyberattack on the United States could range anywhere from zero to tens of billions of dollars, but the latter would require a broad outage of electric power or something of comparable damage. Direct casualties would most likely be limited, and indirect causalities would depend on a variety of factors such as whether the attack disabled emergency 911 dispatch services. Even in that case, there would have to be no alternative means of reaching first responders for such an attack to cause casualties. The indirect effects might be greater if a cyberattack caused a large loss of confidence, particularly in the banking system. Yet scrambled records would probably prove insufficient to incite a run on the banks

## 2NC China

### A2 no reps

#### HOLD THEM ACCOUNTABLE TO THE 1AC – discourse constructs what we determine to be true and establishes hierarches within socio-politcal spaces.

Patricia Hill Collins 90 (Patricia Hill, Distinguished University Professor of Sociology at the University of Maryland, College Park, Former head of the Department of African American Studies at the University of Cincinnati, and the past President of the American Sociological Association Council, Black Feminist Thought: Knowledge, Consciousness and the Politics of Empowerment, p. 62-65)

A second component of the ethic of caring concerns the appropriateness of emotions in dialogues. Emotion indicates that a speaker believes in the validity of an argument. Consider Ntozake Shange’s description of one of the goals of her work: "Our [Western] society allows people to be absolutely neurotic and totally out of touch with their feelings and everyone else’s feelings, and yet be very respectable. This, to me, is a travesty I’m trying to change the idea of seeing emotions and intellect as distinct faculties." The Black women’s blues tradition’s history of personal expressiveness heals this either/or dichotomous rift separating emotion and intellect. For example, in her rendition of "Strange Fruit," Billie Holiday’s lyrics blend seamlessly with the emotion of her delivery to render a trenchant social commentary on southern lynching. Without emotion, Aretha Franklin’s cry for "respect" would be virtually meaningless. A third component of the ethic of caring involves developing the capacity for empathy. Harriet Jones, a 16-year-old Black woman, explains to her interviewer why she chose to open up to him: "Some things in my life are so hard for me to bear, and it makes me feel better to know that you feel sorry about those things and would change them if you could." Without her belief in his empathy, she found it difficult to talk. Black women writers often explore the growth of empathy as part of an ethic of caring. For example, the growing respect that the Black slave woman Dessa and the white woman Rufel gain for one another in Sherley Anne William’s Dessa Rose stems from their increased understanding of each other’s positions. After watching Rufel fight off the advances of a white man, Dessa lay awake thinking: "The white woman was subject to the same ravishment as me; this the thought that kept me awake. I hadn’t knowed white mens could use a white woman like that, just take her by force same as they could with us." As a result of her newfound empathy, Dessa observed, "it was like we had a secret between us." These components of the ethic of caring: the value placed on individual expressiveness, the appropriateness of emotions, and the capacity for empathy-pervade African-American culture. One of the best examples of the interactive nature of the importance of dialogue and the ethic of caring in assessing knowledge claims occurs in the use of the call-and-response discourse mode in traditional Black church services. In such services both the minister and the congregation routinely use voice rhythm and vocal inflection to convey meaning. The sound of what is being said is just as important as the words themselves in what is, in a sense, a dialogue of reason and emotion. As a result it is nearly impossible to filter out the strictly linguistic-cognitive abstract meaning from the sociocultural psychoemotive meaning. While the ideas presented by a speaker must have validity (i.e., agree with the general body of knowledge shared by the Black congregation), the group also appraises the way knowledge claims are presented. There is growing evidence that the ethic of caring may be part of women’s experience as well. Certain dimensions of women’s ways of knowing bear striking resemblance to Afrocentric expressions of the ethic of caring. Belenky et al. point out that two contrasting epistemological orientations characterize knowing: one an epistemology of separation based on impersonal procedures for establishing truth and the other, an epistemology of connection in which truth emerges through care. While these ways of knowing are not gender specific, disproportionate numbers of women rely on connected knowing. The emphasis placed on expressiveness and emotion in African-American communities bears marked resemblance to feminist perspectives on the importance of personality in connected knowing. Separate knowers try to subtract the personality of an individual from his or her ideas because they see personality as biasing those ideas. In contrast, connected knowers see personality as adding to an individual’s ideas and feel that the personality of each group member enriches a group’s understanding. The significance of individual uniqueness, personal expressiveness, and empathy in African-American communities thus resembles the importance that some feminist analyses place on women’s "inner voice." The convergence of Afrocentric and feminist values in the ethic of caring seems particularly acute. White women may have access to a women’s tradition valuing emotion and expressiveness, but few Eurocentric institutions except the family validate this way of knowing. In contrast, Black women have long had the support of the Black church, an institution with deep roots in the African past and a philosophy that accepts and encourages expressiveness and an ethic of caring. Black men share in this Afrocentric tradition. But they must resolve the contradictions that confront them in searching for Afrocentric models of masculinity in the face of abstract, unemotional notions of masculinity imposed on them. The differences among race/gender groups thus hinge on differences in their access to institutional supports valuing one type of knowing over another. Although Black women may be denigrated within white-male-controlled academic institutions, other institutions, such as Black families and churches, which encourage the expression of Black female power, seem to do so, in part, by way of their support for an Afrocentric feminist epistemology. The Ethic of Personal Accountability An ethic of personal accountability is the final dimension of an alternative epistemology. Not only must individuals develop their knowledge claims through dialogue and present them in a style proving their concern for their ideas, but people are expected to be accountable for their knowledge claims. Zilpha Elaw’s description of slavery reflects this notion that every idea has an owner and that the owner’s identity matters: "Oh, the abominations of slavery! ... Every case of slavery, however lenient its infliction and mitigated its atrocities, indicates an oppressor, the oppressed, and oppression." For Elaw abstract definitions of slavery mesh with the concrete identities of its perpetrators and its victims. African-Americans consider it essential for individuals to have personal positions on issues and assume full responsibility for arguing their validity. Assessments of an individual’s knowledge claims simultaneously evaluate an individual’s character, values, and ethics. African-Americans reject the Eurocentric, masculinist belief that probing into an individual’s personal viewpoint is outside the boundaries of discussion. Rather, all views expressed and actions taken are thought to derive from a central set of core beliefs that cannot be other than personal. "Does Aretha really believe that Black women should get ‘respect, or is she just mouthing the words?" is a valid question in an Afrocentric feminist epistemology. Knowledge claims made by individuals respected for their moral and ethical connections to their ideas will carry more weight than those offered by less respected figures. An example drawn from an undergraduate course composed entirely of Black women which I taught might help to clarify the uniqueness of this portion of the knowledge validation process. During one class discussion I asked the students to evaluate a prominent Black male scholar’s analysis of Black feminism. Instead of severing the scholar from his context in order to dissect the rationality of his thesis, my students demanded facts about the author’s personal biography. They were especially interested in concrete details of his life, such as his relationships with Black women, his marital status, and his social class background. By requesting data on dimensions of his personal life routinely excluded in positivist approaches to knowledge validation, they invoked concrete experience as a criterion of meaning. They used this information to assess whether he really cared about his topic and drew on this ethic of caring in advancing their knowledge claims about his work. Furthermore, they refused to evaluate the rationality of his written ideas without some indication of his personal credibility as an ethical human being. The entire exchange could only have occurred as a dialogue among members of a class that had established a solid enough community to employ an alternative epistemology in assessing knowledge claims. The ethic of personal accountability is clearly an Afrocentric value, but is it feminist as well? While limited by its attention to middle-class, white women, Carol Gilligan’s work suggests that there is a female model for moral development whereby women are more inclined to link morality to responsibility, relationships, and the ability to maintain social ties. If this is the case, then African-American women again experience a convergence of values from Afrocentric and female institutions. The use of an Afrocentric feminist epistemology in traditional Black church services illustrates the interactive nature of all four dimensions and also serves as a metaphor for the distinguishing features of an Afrocentric feminist way of knowing. The services represent more than dialogues between the rationality used in examining bible texts and stories and the emotion inherent in the use of reason for this purpose. The rationale for such dialogues involves the task of examining concrete experiences for the presence of an ethic of caring. Neither emotion nor ethics is subordinated to reason. Instead, emotion, ethics, and reason are used as interconnected, essential components in assessing knowledge claims. In an Afrocentric feminist epistemology, values lie at the heart of the knowledge validation process such that inquiry always has an ethical aim. Alternative knowledge claims in and of themselves are rarely threatening to conventional knowledge. Such claims are routinely ignored, discredited, or simply absorbed and marginalized in existing paradigms, Much more threatening is the challenge that alternative epistemologies offer to he basic process used by the powerful to legitimate their knowledge claims. If the epistemology used to validate knowledge comes into question, then all prior knowledge claims validated under the dominant model become suspect. An alternative epistemology challenges all certified knowledge and opens up the question of whether what has been taken to be true can stand the test of alternative ways of validating truth. The existence of a self-defined Black women’s standpoint using an Afrocentric feminist epistemology calls into question the content of what currently passes as truth and simultaneously challenges the process of arriving at the truth.

### 2NC – China Link

#### The affirmatives China cybersecurity threat is constructed

Cavelty 12 (Myriam Dunn Cavelty is a faculty member of the Swiss Federal Institute of Technology Center for Security Studies, "The militarisation of cyber security as a source of global tension", http://www.academia.edu/1471717/The\_militarisation\_of\_cyber\_security\_as\_a\_source\_of\_global\_tension, Strategic Trends 2012)

Second, the main cyber ‘enemy’ in¶ the form of a state has been singledout:¶ There is an increase in allegations¶ that China is responsible for cyber espionage¶ in the form of high-level penetrations¶ of government and business¶ computer systems, in Europe, North¶ America, and Asia. Because Chinese¶ authorities have stated repeatedly that¶ they consider cyberspace a strategic¶ domain and that they hope that mastering¶ it will equalise the existing military¶ imbalance between China and the¶ US more quickly (see Chapter 1 in this¶ publication), many US officials readily¶ accuse the Chinese government¶ of perpetrating deliberate and targeted¶ attacks or intelligence-gathering¶ operations. However, because of the¶ attribution problem, these allegations¶ almost exclusively rely on anecdotal¶ and circumstantial evidence. Not only¶ can attackers hide, it is also impossible¶ to know an attacker’s motivation¶ or to know a person’s affiliation or¶ sponsorship, even if the individuals¶ were known. Therefore, attacks and¶ exploits that seemingly benefit states¶ might well be the work of third-party¶ actors operating under a variety of¶ motivations. At the same time, the¶ attribution challenge also conveniently¶ allows state actors to distance themselves¶ officially from attacks.

### 2NC – AT: Predictions

#### No epistemology advantage – predictions are based on terrible evidence

Cavelty 12 (Myriam Dunn Cavelty is a faculty member of the Swiss Federal Institute of Technology Center for Security Studies, "The militarisation of cyber security as a source of global tension", http://www.academia.edu/1471717/The\_militarisation\_of\_cyber\_security\_as\_a\_source\_of\_global\_tension, Strategic Trends 2012)

Putting a number to the cost of any¶ specific malware is a very tricky thing.¶ Attempts to collect significant data or¶ combine them into statistics have failed¶ due to insurmountable difficulties in¶ establishing what to measure and how¶ to measure it. Numbers that are floating¶ around are usually ¶ more or less educated¶ ‘guesstimates’, calculated¶ by somehow adding downtime of machines¶ and the cost for making them¶ malware-free. The same problem applies¶ to Stuxnet. Shortly after the worm was¶ discovered, Symantec estimated that¶ between 15,000 and 20,000 systems¶ were infected. These numbers increased¶ the longer the worm was known. Siemens¶ on the other hand reported that¶ the worm had infected 15 plants with¶ their SCADA software installed, both in¶ and out of Iran. In the end, Symantec¶ set both the damage and the distribution¶ level of the malware to medium.