# Round 7—Neg vs KState KH

## 1NC

### 1nc 1

#### First off is facts—

#### Facts are meaningless. Their internal link chains are factoids, which are worse. 1ac was detrimental to the cause of their position. This is not a critique of the law.

Schlag ’13 Pierre Schlag, “Facts (The),” his blog, 1/28/2013, http://brazenandtenured.com/2013/01/28/facts-the/

But let me explain about the facts. First, notice, that the most factish of facts (apologies to Latour) are actually factoids—trivial data bits shorn of any actual narrative. CNN had it down cold: “America has had five presidents who ate fish for breakfast.” What, I ask you, could you possibly do with that qua fact? Still, Americans like facts. It was Joe Friday on Dragnet who first said, “all we want are the facts, ma’am.” Really? That’s all? I don’t think so. He was on a mission. He wanted facts on a mission. And we, the viewers, did too. So I have to say, as a preliminary matter, things already don’t look too good for the facts. Indeed, the possibility that in their most prototypical factishisness, facts are nearly useless while in their most desirable state they are on a mission—well, that’s not an auspicious start. Things get worse. In law and social science (that’s my domain limit here—I feel really cramped) facts generally function as poseurs. The facts, are nearly always posing as the truth about “what-is-actually-going-on.” Facts are frequently presented as “the-real-story” or “the bottom line.” One is no doubt supposed to conclude from this that “facts are facts”—that they are the veritable bedrock of truth. But notice that this doesn’t make any sense. Notice that the “bottom line” is an accounting metaphor. Consider that, “the real story” is an oxymoron deliberately composed of both truth and fiction. Note that “what-is-actually-going-on” is a problematic state hanging precariously on the ungrounded and notoriously unreliable reality/appearance pair. All of this is to say, that the appeal of “getting down to the facts,” (or some such thing) often rests on situating the facts in some initially alluring rhetorical space (e.g. “the real story” “the bottom line”) that turns out, upon further inspection, to be constructed of images, metaphors or fictions of questionable philosophical countenance. (See, Nietzsche, On Lies and Truth in a Non-Moral Sense) Now, it’s not that these metaphors, images or fictions turn facts into non-facts. But still, I ask you: what could be more humbling to a fact then to learn that its appeal rests upon a fiction? Not only do facts frequently function as poseurs, but, when they are at their most factish, they’re often not all that interesting. Factish facts don’t really tell you much of anything you want to know. Imagine a party. Here are some exemplary factish facts: There were 19 people at the party. 9 were women. 10 were men. While the party was happening, gravity exercised a constant force of 32 feet per second/per second. Everyone standing stayed connected to the ground. Not the greatest narrative is it? And notice here that if you stick strictly to the facts (if you admit only of truly factish facts) adding more of these little items will not markedly improve your story line. (For you editors of university press books and law review articles, please pay special attention here.) The only time facts are really interesting (remember law and social science is the domain limit) is when they’re something more than just the facts. Go back to the party. Here’s another fact: Jill left the party with Tom. This fact is more interesting. Well, mildly so. With this sort of fact, you can start imagining possible implications (amorous, murderous, whathaveyou). But note that now we’re no longer talking about “just the facts.” We’re talking about facts with implications, facts with attitude. Why then are facts ever interesting? Well, ironically it’s because they’re not functioning as “just facts,” but something more.

#### Information is uniquely dissuasive—vote neg.

Baudrillard, ’92 (Jean, *Pataphysics of Year 2000*, [online])

Outside of this gravitational pull which keeps bodies in orbit, all the atoms of meaning lose themselves or self-absolve in space. Every single atom follows its own trajectory towards infinity and dissolves in space. This is precisely what we are living in our present societies occupied with the **acceleration of all** bodies, all **messages, all processes** in all possible senses and wherein, via modern media, each event, each narrative, each image gets endowed with the simulation of an infinite trajectory. Every political, historical, cultural fact is invested with a kinetic energy which spreads over its own space and thrusts these facts into a hyperspace where they **lose all meaning** by way of an inability to attain their meaning. It is useless to turn to science-fiction: from this point on, from the here and now, through our computer science, our circuits and our channels, this particle accelerator has definitively disrupted and broken the referential orbit of things. With respect to history, the narrative has become impossible since by definition it is the **potential re-narrativization of a sequence of meaning**. Through the impulse of total diffusion and circulation **each event is liberated for itself only** — each event becomes atomized and nuclear as it follows its trajectory into the void. In order to diffuse itself *ad infinitum,* it has to be fragmented like a particle. This is the way it attains a speed of no-return, distancing it from history once and for all. Every cultural, eventual group needs to be fragmented, disarticulated to allow for its entry into the circuits, each language must be absolved into a binary mechanism or device to allow for its circulation to take place — not in our memory, but in the electronic and luminous memory of the computers. There is no human language or speech (*langage*) that could compete with the speed of light. There is no event that could withstand its own diffusion across the planet. No meaning stands a chance once offered the means of its own acceleration. There is no history that will resist the centrifugal pull of facts or its short-circuiting in real time (in the same order of ideas: no sexuality will resist its own liberation, not a single culture will foreclose its own advancement, no truth will defy its own verification, etc.). Even theory is no longer in the state of "reflecting" on anything anymore. All it can do is to snatch concepts from their critical zone of reference and transpose them to the point of no return, in the process of which theory itself too, passes into the hyperspace of simulation as it loses all "objective" validity, while it makes significant gains by acquiring real affinity with the current system. The second hypothesis, with respect to the vanishing of history, is the opposite of the first, i.e., it pertains not to the acceleration but to the slowing down of processes. This too is derived directly from physics. Matter slows the passage of time. More precisely, time seems to pass very slowly upon the surface of a very dense body of matter. The phenomenon increases in proportion to growth in density. The effect of this slowing down (*ralentissement*) will raise the wavelength of light emitted by this body in a way that will allow the observer to record this phenomenon. Beyond a certain limit, time stops, the length of the wave becomes infinite. The wave no longer exists. Light extinguishes itself. The analogy is apparent in the way history slows down as it brushes up against the astral body of the "silent majorities". Our societies are governed by this process of the mass, and not only in the sociological or demographical sense of the word, but also in the sense of a "critical mass", of going beyond a certain point of no-return. That is where the crucially significant event of these societies is to be found: the advent of their revolutionary process along the lines of their mobility, (they are all revolutionary with respect to the centuries gone by), of their equivalent force of inertia, of an immense indifference, and of the silent power of this indifference. This inert matter of the social is not due to a lack of exchanges, of information or of communication; on the contrary, it is the result of the multiplication and saturation of exchanges. It is borne of the hyperdensity of cities, of merchandise, messages and circuits. It is the cold star of the social, a mass at the peripheries of which history cools out. Successive events attain their annihilation in indifference. **Neutralized and bullet-sprayed by information**, the masses neutralise history retrospect and act as a screen of absorption. They themselves have no history, no meaning, no conscience, no desire. They are potential residues of all history, of all meaning, of all desire. By **inserting themselves into modernity**, all these wonderful things managed to invoke **a mysterious counterpart**, the misappreciation of which has unleashed all current political and social strategies. This time, it's the opposite: history, meaning, progress are no longer able to find their speed or tempo of liberation. They can no longer pull themselves out of this much too dense body which slows down their trajectory, slows down their time to the point from whereon perception and imagination of the future escapes us. All social, historical and temporal transcendence is absorbed via this mass's silent immanence. Already, political events no longer conduct sufficient autonomous energy to rouse us and can only run their course as a silent movie in front of which we all sit collectively irresponsible. That is where history reaches its end, not because of the lack of actors or participants, not due to a lack of violence (with respect to violence, there is always an increasing amount), not due to a lack of events (as for events, there will always be more of them thanks to the role of the media and information!) — but because of a slowing down or deceleration, because of indifference and stupefaction. History can no longer go beyond itself, it can no longer envisage its own finality or dream of its own end, it shrouds or buries itself in its immediate effect, it self-exhausts in special effects, it implodes in current events. Essentially, one can no longer speak of the end of history since it has no time to rejoin its own end. **As its effects accelerate, its meaning inexorably decelerates**. It will end up stopping and extinguishing itself like light and time at the peripheries of an infinitely dense mass... Humanity too, had its big-bang: a certain critical density, a certain concentration of people and exchanges that compel this explosion we call *history* and which is none other than the dispersal of dense and hieratic cores of earlier civilizations. Today, we are living an effect of reversal: we have overstepped the threshold of critical mass with respect to populations, events, information, control of the inverse process of inertia of history and politics. At the cosmic level of things, we don't know anymore whether we have reached this speed of liberation wherein we would be partaking of a permanent or final expansion (this, no doubt, will remain forever uncertain). At the human level, where prospects are more limited, it is possible that the energy itself employed for the liberation of the species (acceleration of birthrates, of techniques and exchanges in the course of the centuries) have contributed to an excess of mass and resistance that bear on the initial energy as it drags us along a ruthless movement of contraction and inertia. Whether the universe infinitely expands or retracts to an infinitely dense and infinitely small core will hinge upon its critical mass (with respect to which speculation itself is infinite in view of the discovery of newer particles). Following the analogy, whether our human history will be evolutionary or involuted will presumably depend upon the critical mass of humanity. Are we to see ourselves, like the galaxies, on a definitive orbit that distances us from each other under the impact of a tremendous speed, or is this dispersal to infinity itself destined to reach an end, and the human molecules bound to draw closer to each other by way of an inverse effect of gravitation? The question is whether a human mass that grows day by day is able to control a pulsation of this genre? Third hypothesis, third analogy. But we are still dealing with a point of disappearance, a point of evanescence, a *vanishing-point,* this time however along the lines of music. This is what I call the stereophonic effect. We are all obsessed with high fidelity, with the quality of musical "transmission" (*rendu*). On the console of our channels, equipped with our tuners, our amplifiers and our baffles, we mix, regulate and multiply soundtracks in search of an infallible or unerring music. Is this, though, still music? Where is the threshold of high fidelity beyond the point of which music as such would disappear? Disappearance would not be due to the lack of music, it would disappear for having stepped beyond this boundary, it would disappear into the perfection of its materiality, into its own special effect. Beyond this point, neither judgement nor aesthetic pleasure could be found anymore. Ecstasy of musicality procures its own end. The disappearance of history is of the same order: there too, we have gone beyond this limit or boundary where, subjected to *factual* and *information-al* sophistication, history as such ceases to exist. Large doses of immediate diffusion, of special effects, of secondary effects, of fading — and this famous Larsen effect produced in acoustics by an excessive proximity between source and receiver, in history via an excessive proximity, and therefore the disastrous interference of an event with its diffusion — create a short-circuit between cause and effect, similarly to what takes place between the object and the experimenting subject in microphysics (and in the human sciences!). All things entailing a certain radical uncertainty of the event, like excessive high fidelity, lead to a radical uncertainty with respect to music. Elias Canetti says it well: "as of a certain point", nothing is true anymore. This is also why the soft music of history escapes us, it disappears under the microscope or into the stereophony of information.

### 1nc 2

#### Next off is Apocalypse Meow—

#### The 1AC’s descriptions of an apocalypse depoliticize the human and violence against the nonhuman body—naturalizes oppressive structures

**Collard 13**—Geography Department at the University of British Columbia [modified for ableist language, modifications denoted by brackets]

(Rosemary-Claire, “Apocalypse Meow”, Capitalism Nature Socialism, 24:1, 35-41, dml)

It is an easy point to make, that apocalypse is **defined in** almost totally human terms. Although environmental apocalypticism is tied to **statistics about species loss** and habitat destruction, it is only really an apocalypse **once human beings** (**and capitalist production** for that matter) **are under threat**. Occasionally nonhuman species deemed extraordinary in some manner (usually in the degree to which either they are most ‘‘like us’’ or useful to us) may enter into the apocalyptic calculus\* dolphins that can recognize themselves in the mirror, chimpanzees that use tools. This is further evidence of apocalypticism’s anthropocentrism. Leftist critiques of apocalyptic narratives, while not necessarily incompatible with the previous point, have focused instead on **these narratives’ depoliticizing tendencies**. Swyngedouw (2010a; 2011) locates apocalypse within a general trend toward environmental populism and ‘‘post-politics,’’ a political formation **that** forecloses the political**, preventing the politicization of particulars** (Swyngedouw 2010b). He argues that populism never assigns proper names to things, signifying (following Rancie`re) an erosion of politics and ‘‘genuine democracy . . .[which] is a space where the unnamed, the uncounted, and, consequently, un-symbolized become named and counted’’ (Swyngedouw 2011, 80). Whereas class struggle was about naming the proletariat, and feminist struggles were named through ‘‘woman’’ as a political category, a defining feature of post-politics is **an** ambiguous **and** unnamed **enemy or target of concern**. As Swyngedouw (2010b; 2011) contends, the postpolitical condition **invokes a common predicament and the need for common humanity-wide action**, with ‘‘human’’ and ‘‘humanity’’ vacant signifiers and homogenizing subjects in this politics. I return to this idea soon. Over a decade earlier, Katz (1995) also argues that ‘‘apocalypticism is politically ~~disabling’’~~ [debilitating] (277). She writes: ‘‘contemporary problems are so serious that **rendering them apocalyptic** obscures their political ecology\*their sources, their political, economic and social dimensions’’ (278). Loathe to implicate ‘‘human nature’’ as one of these sources, Katz instead targets global capitalism, which is ‘‘premised on a series of socially-constructed differences that, in apocalyptic visions, take a universal character: man/woman; culture/nature; first world/third world; bourgeoisie/working class’’ (279). Towards the end of her short chapter, she remarks that ‘‘human beings are simultaneously different from and of a piece with bees’’ (280), calling subsequently for ‘‘a usable environmental politics [that] takes seriously the political responsibility implied by the difference between people and bees’’ (280). There is so much to agree with here. But Katz misses a big binary in her list: human/animal. On the other hand, she clearly if implicitly recognizes not only the productiveness of this binary and its role in environmental politics (the humans and the bees), but also the attention it deserves. The question then remains: Although according to Katz, apocalyptic politics underplays if not entirely ignores the production process, is this inherent to apocalypticism, or is there potential to train apocalypticism onto production, particularly of the human and the human/animal binary? **Neither a natural order, nor a pre-given subject position, nor a category that exists beyond politics, the human is rather** an intensely political categorywhose ongoing production is rife with violence, contestation, and hierarchy. The central mode of this production is the human/animal binary that Haraway (2008, 18) says ‘‘flourishes, lethally, in the entrails of humanism.’’ This binary is **continually** re-made **and** re-authorized **politically**, legally, scientifically, religiously, and so on. It is **the product of particular** epistemologies**,** ontologies**, and** power relations, and it also produces these same structures. The spatial, material and discursive inclusion and exclusion of animals construct the human/animal binary. Materially, animals are included in the ‘‘human’’ project as laborers, food, clothing, and so on, but are **excluded from life itself** should their dead bodies be of economic value. Animals work for us, for free, and are largely ‘‘disposable workers’’ in a manner similar to and different from the ‘‘disposable women’’ Wright (2006) observes are fundamental to the workings of capital and labor in Mexican maquiladoras. The similarity lies in how both animal laborers and these women factory workers are devalued as laborers, and this devaluing of their labor actually **contributes to the formation of value in the commodities and capital of the production network**. They are different in that of course the women are still paid\*albeit marginally\*and their labor is recognized as labor. Animals do not just labor for free. They also die for profit and power. The most obvious example of industrial meat production aside, **capitalism and the liberal state** derive significant profits **from the ability to kill**\*often in mass numbers\*wild **animals**. Killing wolves, bears, cougars, and other animals has been a predominant colonial project, with bounty often the first laws passed in the colonies. Not only domesticated but also wild animals have played and continue to play a central role, materially and symbolically, in capitalism and the formation of the nation state, as symbols, commodities, and spectacle. Discursively **animals found the human subject by virtue of their exclusion**: the human is what is not animal. This is **a juridicopolitical, ethical exclusion** that is always at the same time an inclusion. The human thus **appears to be a neurological or biophysiological product** rather than **a result of** specific histories**,** geographies**, and** social relations, between humans and also humans and animals. Certainly particular socio-natural properties do become essential to a thing’s power and geopolitical centrality (think opposable thumbs, cerebral cortexes, bipedalism, and so on). But as Huber (2011, 34, emphasis added) argues in the context of oil, ‘‘biophysical capacities are **only realizable through particular uneven social relations** of culture, history, and power.’’ Specific conditions and relations produce the human, which is entirely different than saying that humans are the same as each other or as other animals. Their differences should not be disregarded for a host of reasons, not the least of which is the political struggle various groups have made to claim both difference and not being animals. It is not my aim to ignore, then, the particularities of the human species, although I would emphasize that these particularities are not universal and are increasingly being shown to be far less particular than we imagined.

#### Voting neg means getting naked in front of our pets—use the ballot to express solidarity with the nonhuman through allowing for an apocalypse of the human subject—the debate round is uniquely emancipatory but the perm removes that potential

**Collard 13**—Geography Department at the University of British Columbia

(Rosemary-Claire, “Apocalypse Meow”, Capitalism Nature Socialism, 24:1, 35-41, dml)

While what counts as human shifts dramatically in time and space, what remains for the most part constant is **the animal outside that founds this category**. These are not meaningless exclusions, and in the context of environmental politics, of course, they have especially pronounced momentum and significance. The naturalization of a superior, distinct species category **enables systematically and casually inflicted death and suffering** on an inconceivable scale. What is outside the ‘‘human’’ is far more ‘‘killable,’’ like Haraway says, more easily ‘‘noncriminally put to death,’’ says Derrida, more ‘‘precarious’’ for Butler. Although Butler’s extensive work on the politics of the human has been criticized for anthropocentrism, in a recent interview (Antonello and Farneti 2009), she questions what it might mean to **share conditions of vulnerability and precariousness** with animals and the environment, and suggests it undoes **‘‘the very conceit of anthropocentrism**.’’ Such an undoing is precisely what I advocate. While an entrenched and powerful category, **the human is also** changeable **and** fluid. As Derrida (2008, 5) says, ‘‘the list of what is ‘proper’ to man always forms a configuration, from the first moment. For that very reason, it can never be limited to a single trait and is never closed.’’ The human’s contingencies, dependencies and destructive, homogenizing effects should be front and center in environmental politics. To show its strangeness is to show that it could be otherwise. Ultimately, **we might have to reconfigure subjectivity’s contours and topographies**, allow for an apocalypse of the human subject. We might have to get naked in front of our pets. ‘‘A true political space,’’ writes Swyngedouw (2010b, 194), ‘‘is always a space of contestation for those who are not-all, who are uncounted and unnamed.’’ This true political space necessarily includes\*if only by virtue of their exclusion\*animals, the ‘‘constitutive outside’’ of humanity itself. How we respond to this dynamic **ought to be a central question** of critical scholarship and philosophizing. To be a philosopher, says Deleuze in the ‘‘A for Animal’’ entry to the ‘‘abecedary’’ (L’abe´ce´daire de Gilles Deleuze 1989), ‘‘is to write in the place of animals that die.’’ This is still an imperfect way of describing my objective (for one thing, I am also interested in animals that are still alive), but it is an improvement over being a ‘‘spokesperson’’ for animals, which are often characterized as speechless and may be rendered more so having spokespeople appointed to speak on their behalf. To write in the place of animals that die seems a preferable, though still fraught, characterization. This paper is therefore written in the place of those uncounted and unnamed non-subjects of political space, the animals that die, the nonhumans, the hundreds of millions of animals that are ‘‘living out our nightmares’’ (Raffles 2010, 120): injected, tested, prodded, then discarded. **We have** denied**,** disavowed**, and** misunderstood **animals**. They are refused speech, reason, morality, emotion, clothing, shelter, mourning, culture, lying, lying about lying, gifting, laughing, crying\*the list has no limit. But ‘‘who was born first, before the names?’’ Derrida (2008, 18) asks. ‘‘Which one saw the other come to this place, so long ago? Who will have been the first occupant? Who the subject? Who has remained the despot, for so long now?’’ Some see identifying this denial as a side-event, inconsequential, even sort of silly. The belief in human superiority is firmly lodged and dear to people’s hearts and senses of themselves. It also seems a daunting task, not a simple matter of inserting the excluded into the dominant political order, which as Zˇ izˇek (1999) writes, neglects how **these very subversions and exclusions are the order’s condition of being**. But if the political is precisely, as Swyngedouw (2010b) suggests, the expansion of a specific issue into a larger universal demand against ‘‘those in power’’ (an elevation he argues is precluded by the post-political, **which** **reduces an issue to a** particular**,** contained**, and** very specific **demand**), then perhaps the universal demand we need to mobilize in the Left is humanity itself. We need to write in the place of animals that die, in the sense that our politics must undertake not only a re-writing of our histories of oppression, our constitutions, our global agreements (and who and what are included in them), but also, necessarily, **a radical reconfiguring of how subjects are positioned in relation to each other**. The human can in fact serve as the named subject of this political effort, perhaps most aptly in environmental struggles. Like Braidotti (2008, 183) argues, ‘‘sustainability is about decentering anthropocentrism.’’ It is about an ‘‘egalitarianism . . .that displaces both the old-fashioned humanistic assumption that ‘man’ is the measure of all things and the anthropocentric idea that the only bodies that matter are human’’ (183). In tackling the human category, I believe the Left **would not only be more relevant, but also could bring a** transformative sensibility **to an environmental politics** that often seems to want to blame ‘‘humankind’’ but **fails to consider precisely how this material and symbolic category remains untroubled in such misanthropy.**

### 1nc 3

#### The 1ac is inculcation within the liberal world order of all cyber space—usage of law to regulate software violence leaves unquestioned the violence innate to law itself, a “friendly violence” that still justifies acting outside the law to protect the network of cyber society.

Cox and Knahl 11. Geoff Cox Researcher in Digital Aesthetics as part of the Digital Urban Living Research Center, Aarhus University (DK). He is also an occasional artist, and Associate Curator of Online Projects, Arnolfini, Bristol (UK), adjunct faculty, Transart Institute, Berlin/New York (DE/US), Associate Professor (Reader), University of Plymouth (UK), where he is part ofKURATOR/Art and Social Technologies Research group, and Martin Knahl, Lecturer at the University of Plymouth. He is a Research Fellow at the Centre for Information Security and Network Research, “NeMe: Critique of Software Violence,” <http://www.neme.org/1300/critique-of-software-security>, May 2011

Eventually Blue Security surrendered and went out of business, expressing their reluctance (unlike the Israeli State) to take part in an ever-escalating ‘soft war’ of violence and counter-violence. The point is that security software operates double standards. It would seem that the issue of security is reducible to the challenge of managing the inherent insecurities of networked relations. In other words, the network needs to distinguish whether you are a friend or not, evoking Carl Schmitt’s notion of enmity (in The Concept of the Political, of 1927).[11](http://www.neme.org/1300/critique-of-software-security#fn11) Under contemporary neo-liberal conditions – inextricably linked to security – it is clear that liberal democracies exert a form of violence through their insistence on friendliness and participation in networks. This is the organised violence of democracy or ‘violence of participation’, as Markus Meissen puts it (2007: 26).[12](http://www.neme.org/1300/critique-of-software-security#fn12) In other words, liberal democracy exerts a form of friendly violence that doesn’t appear violent at all – such as encouraging the use of certain kinds of software. All the time the violence is exerted nonviolently under the guise of protection from violence: security.

#### This is not benign, but a liberal tactic in the racist and genocidal global civil war that justifies the destruction of the entire world.

Evans 10. Brad Evans, Lecturer in the School of Politics and International Studies at the University of Leeds and Programme Director for International Relations, “Foucault’s Legacy: Security, War, and Violence in the 21st Century,” Security Dialogue vol.41, no. 4, August 2010, pg. 422-424, sage

Imposing liberalism has often come at a price. That price has tended to be a continuous recourse to war. While the militarism associated with liberal internationalization has already received scholarly attention (Howard, 2008), Foucault was concerned more with the continuation of war once peace has been declared.4 Denouncing the illusion that ‘we are living in a world in which order and peace have been restored’ (Foucault, 2003: 53), he set out to disrupt the neat distinctions between times of war/military exceptionalism and times of peace/civic normality. War accordingly now appears to condition the type of peace that follows. None have been more ambitious in map-­ ping out this war–peace continuum than Michael Dillon & Julian Reid (2009). Their ‘liberal war’ thesis provides a provocative insight into the lethality of making live. Liberalism today, they argue, is underwritten by the unreserved righteousness of its mission. Hence, while there may still be populations that exist beyond the liberal pale, it is now taken that they should be included. With ‘liberal peace’ therefore predicated on the pacification/elimination of all forms of political difference in order that liberalism might meet its own moral and political objectives, the more peace is commanded, the more war is declared in order to achieve it: ‘In proclaiming peace . . . liberals are nonethe-­ less committed also to making war.’ This is the ‘martial face of liberal power’ that, contrary to the familiar narrative, is ‘directly fuelled by the universal and pacific ambitions for which liberalism is to be admired’ (Dillon & Reid, 2009: 2). Liberalism thus stands accused here of universalizing war in its pursuit of peace: However much liberalism abjures war, indeed finds the instrumental use of war, espe-­ cially, a scandal, war has always been as instrumental to liberal as to geopolitical thinkers. In that very attempt to instrumentalize, indeed universalize, war in the pursuit of its own global project of emancipation, the practice of liberal rule itself becomes profoundly shaped by war. However much it may proclaim liberal peace and freedom, its own allied commitment to war subverts the very peace and freedoms it proclaims (Dillon & Reid, 2009: 7). While Dillon & Reid’s thesis only makes veiled reference to the onto-­ theological dimension, they are fully aware that its rule depends upon a certain religiosity in the sense that war has now been turned into a veritable human crusade with only two possible outcomes: ‘endless war or the transformation of other societies and cultures into liberal societies and cul-­ tures’ (Dillon & Reid, 2009: 5). Endless war is underwritten here by a new set of problems. Unlike Clausewitzean confrontations, which at least pro-­ vided the strategic comforts of clear demarcations (them/us, war/peace, citizen/soldier, and so on), these wars no longer benefit from the possibility of scoring outright victory, retreating, or achieving a lasting negotiated peace by means of political compromise. Indeed, deprived of the prospect of defin-­ ing enmity in advance, war itself becomes just as complex, dynamic, adaptive and radically interconnected as the world of which it is part. That is why ‘any such war to end war becomes a war without end. . . . The project of removing war from the life of the species becomes a lethal and, in principle, continuous and unending process’ (Dillon & Reid, 2009: 32). Duffield, building on from these concerns, takes this unending scenario a stage further to suggest that since wars for humanity are inextricably bound to the global life-­chance divide, it is now possible to write of a ‘Global Civil War’ into which all life is openly recruited: Each crisis of global circulation . . . marks out a terrain of global civil war, or rather a tableau of wars, which is fought on and between the modalities of life itself. . . . What is at stake in this war is the West’s ability to contain and manage international poverty while maintaining the ability of mass society to live and consume beyond its means (Duffield, 2008: 162). Setting out civil war in these terms inevitably marks an important depar-­ ture. Not only does it illustrate how liberalism gains its mastery by posing fundamental questions of life and death – that is, who is to live and who can be killed – disrupting the narrative that ordinarily takes sovereignty to be the point of theoretical departure, civil war now appears to be driven by a globally ambitious biopolitical imperative (see below). Liberals have continuously made reference to humanity in order to justify their use of military force (Ignatieff, 2003). War, if there is to be one, must be for the unification of the species. This humanitarian caveat is by no means out of favour. More recently it underwrites the strategic rethink in contemporary zones of occupation, which has become biopolitical (‘hearts and minds’) in everything but name (Kilcullen, 2009; Smith, 2006). While criticisms of these strategies have tended to focus on the naive dangers associated with liberal idealism (see Gray, 2008), insufficient attention has been paid to the contested nature of all the tactics deployed in the will to govern illiberal populations. Foucault returns here with renewed vigour. He understood that forms of war have always been aligned with forms of life. Liberal wars are no exception. Fought in the name of endangered humanity, humanity itself finds its most meaningful expression through the battles waged in its name: At this point we can invert Clausewitz’s proposition and say that politics is the continuation of war by other means. . . . While it is true that political power puts an end to war and establishes or attempts to establish the reign of peace in civil society, it certainly does not do so in order to suspend the effects of power or to neutralize the disequilibrium revealed in the last battle of war (Foucault, 2003: 15). What in other words occurs beneath the semblance of peace is far from politically settled: political struggles, these clashes over and with power, these modifications of relations of force – the shifting balances, the reversals – in a political system, all these things must be interpreted as a continuation of war. And they are interpreted as so many episodes, fragmentations, and displacements of the war itself. We are always writing the history of the same war, even when we are writing the history of peace and its institutions (Foucault, 2003: 15). David Miliband (2009), without perhaps knowing the full political and philo-­ sophical implications, appears to subscribe to the value of this approach, albeit for an altogether more committed deployment: NATO was born in the shadow of the Cold War, but we have all had to change our thinking as our troops confront insurgents rather than military machines like our own. The mental models of 20th century mass warfare are not fit for 21st century counter-­ insurgency. That is why my argument today has been about the centrality of politics. People like quoting Clausewitz that warfare is the continuation of politics by other means. . . . We need politics to become the continuation of warfare by other means. Miliband’s ‘Foucauldian moment’ should not escape us. Inverting Clausewitz on a planetary scale – hence promoting the collapse of all meaningful distinctions that once held together the fixed terms of Newtonian space (i.e. inside/outside, friend/enemy, citizen/soldier, war/peace, and so forth), he firmly locates the conflict among the world of peoples. With global war there-­ fore appearing to be an internal state of affairs, vanquishing enemies can no longer be sanctioned for the mere defence of things. A new moment has arrived, in which the destiny of humanity as a whole is being wagered on the success of humanity’s own political strategies. No coincidence, then, that authors like David Kilcullen – a key architect in the formulation of counter-­ insurgency strategies in Iraq and Afghanistan, argue for a global insurgency paradigm without too much controversy. Viewed from the perspective of power, global insurgency is after all nothing more than the advent of a global civil war fought for the biopolitical spoils of life. Giving primacy to counter-­ insurgency, it foregrounds the problem of populations so that questions of security governance (i.e. population regulation) become central to the war effort (RAND, 2008). Placing the managed recovery of maladjusted life into the heart of military strategies, it insists upon a joined-­up response in which sovereign/militaristic forms of ordering are matched by biopolitical/devel-­ opmental forms of progress (Bell & Evans, forthcoming). Demanding in other words a planetary outlook, it collapses the local into the global so that life’s radical interconnectivity implies that absolutely nothing can be left to chance. While liberals have therefore been at pains to offer a more humane recovery to the overt failures of military excess in current theatres of operation, warfare has not in any way been removed from the species. Instead, humanized in the name of local sensitivities, doing what is necessary out of global spe-­ cies necessity now implies that war effectively takes place by every means. Our understanding of civil war is invariably recast. Sovereignty has been the traditional starting point for any discussion of civil war. While this is a well-established Eurocentric narrative, colonized peoples have never fully accepted the inevitability of the transfixed utopian prolificacy upon which sovereign power increasingly became dependent. Neither have they been completely passive when confronted by colonialism’s own brand of warfare by other means. Foucault was well aware of this his-­ tory. While Foucauldian scholars can therefore rightly argue that alternative histories of the subjugated alone permit us to challenge the monopolization of political terms – not least ‘civil war’ – for Foucault in particular there was something altogether more important at stake: there is no obligation whatsoever to ensure that reality matches some canonical theory. Despite what some scholars may insist, politically speaking there is nothing that is necessarily proper to the sovereign method. It holds no distinct privilege. Our task is to use theory to help make sense of reality, not vice versa. While there is not the space here to engage fully with the implications of our global civil war paradigm, it should be pointed out that since its biopolitical imperative removes the inevitability of epiphenomenal tensions, nothing and nobody is necessarily dangerous simply because location dictates. With enmity instead depending upon the complex, adaptive, dynamic account of life itself, what becomes dangerous emerges from within the liberal imaginary of threat. Violence accordingly can only be sanctioned against those newly appointed enemies of humanity – a phrase that, immeasurably greater than any juridical category, necessarily affords enmity an internal quality inherent to the species complete, for the sake of planetary survival. Vital in other words to all human existence, doing what is necessary out of global species necessity requires a new moral assay of life that, pitting the universal against the particular, willingly commits vio-­ lence against any ontological commitment to political difference, even though universality itself is a shallow disguise for the practice of destroying political adversaries through the contingency of particular encounters. Necessary Violence Having established that the principal task set for biopolitical practitioners is to sort and adjudicate between the species, modern societies reveal a distinct biopolitical aporia (an irresolvable political dilemma) in the sense that making life live – selecting out those ways of life that are fittest by design – inevitably writes into that very script those lives that are retarded, backward, degener-­ ate, wasteful and ultimately dangerous to the social order (Bauman, 1991). Racism thus appears here to be a thoroughly modern phenomenon (Deleuze & Guattari, 2002). This takes us to the heart of our concern with biopoliti-­ cal rationalities. When ‘life itself’ becomes the principal referent for political struggles, **power necessarily concerns itself with those biological threats to human existence** (Palladino, 2008). That is to say, since life becomes the author of its own (un)making, the biopolitical assay of life necessarily portrays a commitment to the supremacy of certain species types: ‘a race that is portrayed as the one true race, the race that holds power and is entitled to define the norm, and against those who deviate from that norm, against those who pose a threat to the biological heritage’ (Foucault, 2003: 61). Evidently, what is at stake here is no mere sovereign affair. Epiphenomenal tensions aside, racial problems occupy a ‘permanent presence’ within the political order (Foucault, 2003: 62). Biopolitically speaking, then, since it is precisely through the internalization of threat – the constitution of the threat that is now from the dangerous ‘Others’ that exist within – that societies reproduce at the level of life the ontological commitment to secure the subject, since everybody is now possibly dangerous and nobody can be exempt, for politi-­ cal modernity to function one always has to be capable of killing in order to go on living: Wars are no longer waged in the name of a sovereign who must be defended; they are waged on behalf of the existence of everyone; entire populations are mobilized for the purpose of wholesale slaughter in the name of life necessity; massacres have become vital. . . . The principle underlying the tactics of battle – that one has to become capable of killing in order to go on living – has become the principle that defines the strategy of states (Foucault, 1990: 137). When Foucault refers to ‘killing’, he is not simply referring to the vicious act of taking another life: ‘When I say “killing”, I obviously do not mean simply murder as such, but also every form of indirect murder: the fact of exposing someone to death, increasing the risk of death for some people, or, quite simply, political death, expulsion, rejection and so on’ (Foucault, 2003: 256). Racism makes this process of elimination possible**,** for it is only through the discourse and practice of racial (dis)qualification that one is capable of introducing ‘a break in the domain of life that is under power’s control: the break between what must live and what must die’ (Foucault, 2003: 255). While kill- ing does not need to be physically murderous, that is not to suggest that we should lose sight of the very real forms of political violence that do take place in the name of species improvement. As Deleuze (1999: 76) duly noted, when notions of security are invoked in order to preserve the destiny of a species, when the defence of society gives sanction to very real acts of violence that are justified in terms of species necessity, that is when the capacity to legitimate murderous political actions in all our names and for all our sakes becomes altogether more rational, calculated, utilitarian, hence altogether more frightening: When a diagram of power abandons the model of sovereignty in favour of a disciplinary model, when it becomes the ‘bio-­power’ or ‘bio-­politics’ of populations, controlling and administering life, it is indeed life that emerges as the new object of power. At that point law increasingly renounces that symbol of sovereign privilege, the right to put someone to death, but allows itself to produce all the more hecatombs and genocides: not by returning to the old law of killing, but on the contrary in the name of race, precious space, conditions of life and the survival of a population that believes itself to be better than its enemy, which it now treats not as the juridical enemy of the old sovereign but as a toxic or infectious agent, a sort of ‘biological danger’.Auschwitz arguably represents the most grotesque, shameful and hence meaningful example of necessary killing – the violence that is sanctioned in the name of species necessity (see Agamben, 1995, 2005). Indeed, for Agamben, since one of the most ‘essential characteristics’ of modern biopolitics is to con-­ stantly ‘redefine the threshold in life that distinguishes and separates what is inside from what is outside’, it is within those sites that ‘eliminate radically the people that are excluded’ that the biopolitical racial imperative is exposed in its most brutal form (Agamben, 1995: 171). The camp can therefore be seen to be the defining paradigm of the modern insomuch as it is a ‘space in which power confronts nothing other than pure biological life without any media-­ tion’ (Agamben, 1995: 179). While lacking Agamben’s intellectual sophistry, such a Schmittean-­inspired approach to violence – that is, sovereignty as the ability to declare a state of juridical exception – has certainly gained wide-­ spread academic currency in recent times. The field of international rela-­ tions, for instance, has been awash with works that have tried to theorize the ‘exceptional times’ in which we live (see, in particular, Devetak, 2007; Kaldor, 2007). While some of the tactics deployed in the ‘Global War on Terror’ have undoubtedly lent credibility to these approaches, in terms of understanding violence they are limited. Violence is only rendered problematic here when it is associated with some act of unmitigated geopolitical excess (e.g. the inva-­ sion of Iraq, Guantánamo Bay, use of torture, and so forth). This is unfortunate. Precluding any critical evaluation of the contemporary forms of violence that take place within the remit of humanitarian discourses and practices, there is a categorical failure to address how necessary violence continues to be an essential feature of the liberal encounter. Hence, with post-interventionary forms of violence no longer appearing to be any cause for concern, the nature of the racial imperative that underwrites the violence of contemporary liberal occupations is removed from the analytical arena.

#### Refuse the mapping of the liberal sovereign model onto the network. The ethos of hacking is an ethical injunction—computer piracy replaces the standard place of the protest, us the ballot to represent such a clogging of the machine

Cox and Knahl 11. Geoff Cox Researcher in Digital Aesthetics as part of the Digital Urban Living Research Center, Aarhus University (DK). He is also an occasional artist, and Associate Curator of Online Projects, Arnolfini, Bristol (UK), adjunct faculty, Transart Institute, Berlin/New York (DE/US), Associate Professor (Reader), University of Plymouth (UK), where he is part ofKURATOR/Art and Social Technologies Research group, and Martin Knahl, Lecturer at the University of Plymouth. He is a Research Fellow at the Centre for Information Security and Network Research, “NeMe: Critique of Software Violence,” <http://www.neme.org/1300/critique-of-software-security>, May 2011

When no other choice is possible, software violence might be the answer – replacing the strike in the form of software that Deleuze anticipated when he claimed: ‘Computer piracy and viruses, for example, will replace strikes and what the nineteenth century called “sabotage” (“clogging” the machinery).’ (1990) There are many examples of artists and activists working in this way through direct action and hacking. Hackers, crackers,[13](http://www.neme.org/1300/critique-of-software-security" \l "fn13) or system intruders are generally understood as those who attempt to penetrate security systems on remote computers, but this is a pejorative use of the term. In general it simply refers to a person who was capable of creating hacks, or demonstrating technical virtuosity (Levy 1984). The ethical principles of hacking reflect these concerns:

Access to computers – and anything that might teach you something about the way the world really works – should be unlimited and total.  
Always yield to the Hands-On Imperative!

All information should be free.

Mistrust authority – promote decentralization.

Hackers should be judged by their acting, not bogus criteria such as degrees, age, race, or position.

You can create art and beauty on a computer.

Computers can change your life for the better.

Don’t litter other people’s data.

Make public data available, protect private data.[14](http://www.neme.org/1300/critique-of-software-security#fn14)

In keeping with these principles, it should be stated that most hackers condemn attacks against communication systems. In 1999, the Chaos Computer Club joined an international coalition of hacker groups (including the Cult of the Dead Cow)[15](http://www.neme.org/1300/critique-of-software-security" \l "fn15) to condemn the use of networks as battlegrounds in their declaration for ‘info peace’: ‘DO NOT support any acts of “Cyberwar”. Keep the networks of communication alive. They are the nervous system for human progress.’[16](http://www.neme.org/1300/critique-of-software-security#fn16)

An excellent example of non-violent direct action is the FloodNet tactical software developed in 1998 by the Electronic Disturbance Theater.[17](http://www.neme.org/1300/critique-of-software-security#fn17) The FloodNet implementation is based on Java applets that assists in the execution of virtual sit-ins or online civil acts of disobedience, and offered as a tool to enable protestors to effectively shut down web servers of target institutions, by flooding them with requests. The requests are automatically reloaded at high frequencies to cause an excessive amount of traffic on the server so that other users are not able to access the website. It further enables users to post statements to a targeted site by transmitting them to the server’s log files:

‘By the selection of phases for use in building the “bad” urls , for example using “human\_rights” to form the url “http://www.xxx.gb.mx/human\_rights”, the FloodNet is able to upload messages to server error logs by intentionally asking for a non-existent url. This causes the server to return messages like “human\_ rights not found on this server.” This works because of the way many http servers process requests for web pages that do not exist. FloodNet’s Java applet asks the targeted server for a directory called, in this example, “human\_rights”, but since that directory doesn’t exist, the server returns the familiar “File not Found” or “Error 404” message, recording the bad request. This is a unique way to leave a message on that server.’ (Stalbaum)[18](http://www.neme.org/1300/critique-of-software-security" \l "fn18)

The tactic follows the hacker sensibility in opening up existing security vulnerabilities in the system. As ever, power continues to produce its own vulnerability but the question of violence is more unsettling and paradoxical. For some hackers, the ethical practices of free software represent a move away from the use of violence.[19](http://www.neme.org/1300/critique-of-software-security#fn19) However what this essay has tried to establish is how violence is simply unavoidable and is inherent to the socio-technical structures of networks. In addition, insecurity is promoted by a burgeoning security industry that creates both awareness and fear regarding perceived insecurity,[20](http://www.neme.org/1300/critique-of-software-security#fn20) intensifying the dependency of users on its software and at the same time engendering a growing ambivalence even amongst security professionals who recognise that ‘security causes its own type of harm’.[21](http://www.neme.org/1300/critique-of-software-security#fn21)

The actions of software dissidents can be seen to extend network forms of antagonism and the justification of certain means that constitute violence – further evoking Benjamin’s essay. Moreover, software is necessarily violent even when it appears nonviolent.

### solvency

#### The plan can never solve—this evidence is the bee’s knees. Bzzzzz.

**Fatovic 9**—Director of Graduate Studies for Political Science at Florida International University [added the word “is” for correct sentence structure—denoted by brackets]

(Clement, *Outside the Law: Emergency and Executive Power* pg 1-5, dml)

But the problem for any legal order is that law aims at fixity in a world beset by flux. The greatest challenge to legally established order comes not from the resistance of particular groups or individuals who object to any of its substantive aims but from the unruliness of the world itself. The stability, predictability, and regularity sought by law eventually runs up against **the unavoidable instability, unpredictability, and irregularity of the world**. Events constantly threaten to disrupt and destabilize the artificial order established by law. Emergencies-sudden and extreme occurrences such as the devastating terrorist attacks of September 11, an overwhelming natural disaster like Hurricane Katrina, a pandemic outbreak of avian flu, a catastrophic economic collapse, or a severe food shortage, to name just a few-dramatize **the limitations of the law** in dealing with unexpected and incalculable contingencies. Designed for the ordinary and the normal, law cannot always provide for such extraordinary occurrences in spite of its aspiration to comprehensiveness. When such events arise, the responsibility for formulating a response usually falls to the executive.

The executive has a unique relationship to the law and the order that it seeks, especially in a liberal constitutional system committed to the rule of law. Not only is the executive the authority most directly responsible for enforcing the law and maintaining order in ordinary circumstances, it is also the authority most immediately responsible for restoring order in extraordinary circumstances. But while the executive is expected to uphold and follow the law in normal times, **emergencies** sometimes **compel the executive to** exceed the strict letter of the law. Given the unique and irrepressible nature of emergencies, the law often provides **little effective guidance**, leaving executives to their own devices. Executives possess special resources and characteristics that enable them to **formulate responses more** rapidly**,** flexibly**, and** decisively **than can legislatures, courts, and bureaucracies**. Even where the law seeks to anticipate **and** provide **for emergencies by** specifying the kinds of actions **that** public **officials are permitted or required to take**, **emergencies create** unique opportunities **for the executive to** exercise an extraordinary degree of discretion. And when the law seems to be inadequate to the situation at hand, executives often claim that it [is] necessary to **go beyond its dictates** by consolidating those powers ordinarily exercised by other branches of government or **even by expanding the range of powers ordinarily permitted**. But in seeking to bring order to the chaos that emergencies instigate, executives who take such action also **bring attention to** the deficiencies of the law **in maintaining order**, often with serious consequences for the rule of law.

The kind of extralegal action that executives are frequently called upon to take in response to emergencies **is** deeply problematic **for liberal constitutionalism**, which gives pride of place to the rule of law, both in its self-definition and in its standard mode of operation. If emergencies test the limits of those general and prospective rules that are designed to make governmental action limited and predictable, that is because **emergencies are** largely unpredictable **and** potentially limitless.1 Yet the rule of law, which has enjoyed a distinguished position in constitutional thought going back to Aristotle, has always sought to place limits on what government may do by substituting the arbitrariness and unpredictability of extemporary decrees with the impartiality and regularity of impersonal rules promulgated in advance. The protection of individual freedom within liberal constitutionalism has come to be unimaginable where government does not operate according to general and determinate rules.2 The rule of law has achieved primacy within liberal constitutionalism because it is considered vital to the protection of individual freedom. As Max Weber famously explained of the modern bureaucratic state, legitimacy in the liberal state is not based on habitual obedience to traditions or customs sanctified by time or on personal devotion to a charismatic individual endowed with superhuman gifts but on belief in the legality of a state that is functionally competent in administering highly impersonal but "rational rules." 3 In fact, its entire history and aim can be summed up as an attempt to curtail the kind of discretionary action associated with the arbitrary "rule of men"-by making government itself subject to the law.

The apparent primacy of law in liberal constitutionalism has led some critics to **question its capacity to deal with emergencies**. Foremost among these critics is German political and constitutional theorist Carl Schmitt, who concluded that liberalism is incapable of dealing with the "exception" or "a case of extreme peril" that poses "a danger to the existence of the state" without resorting to measures that contradict and undermine its commitments to the rule of law, the separation of powers, the preservation of civil liberties, and other core values.4 In Schmitt's view, liberalism is wedded to a "normativistic" approach that seeks to regulate life according to strictly codified legal and moral rules that not only **obscure the "decisionistic" basis of all law** but also **deny the role of** personal decision-making **in the** interpretation**,** enforcement**, and** application **of law**. 5 Because legitimacy in a liberal constitutional order is based largely on adherence to formal legal procedures that restrict the kinds of actions governments are permitted to take, actions that have not been specified or authorized in advance **are simply ruled out**. According to Schmitt, the liberal demand that governmental action always be controllable **is** **based on the naive belief that the world is thoroughly calculable**. 6 If it expects regularity and predictability in government, it is because it understands the world in those terms, **making it** oblivious **to the problems of contingency**. Not only does this belief that the world is subject to a rational and predictable order make it difficult for liberalism to justify actions that stand outside that order, it also **makes it difficult for liberalism** even to acknowledge emergencies when they do arise. But Schmitt's critique goes even further than this. When liberal constitutionalism does acknowledge the exception, its commitment to the rule of law forces it to choose between potential suicide if it adheres strictly to its legalistic ideals and undeniable hypocrisy if ignores those ideals? Either way, the argument goes, **emergencies expose the inherent shortcomings and weaknesses of liberalism**.

It is undeniable that the rule of law occupies a privileged position within liberal constitutionalism, but it is a mistake to identify liberal constitutionalism with an excessively legalistic orientation that renders it incapable of dealing effectively with emergencies. Schmitt is correct in pointing out that liberal normativism seeks to render government action as impersonal and predictable as possible in normal circumstances, but the history of liberal 'I· constitutional thought leading up to the American Founding reveals that its main proponents recognized the need to supplement the rule of law with a personal element in cases of emergency. The political writings of John Locke, David Hume, William Blackstone, and those Founders who advocated a strong presidency indicate that many early liberal constitutionalists were **highly attuned** to the limitations of law in dealing with events that disrupt the regular order. They were well aware that rigid adherence to the formalities of law, both in responding to emergencies and in constraining the official who formulates the response, **could undermine important substantive aims and values**, thereby sacrificing the ends for the means.

Their reflections on the chronic instability and irregularity of politics reveal an appreciation for the **inescapable**-albeit temporary-**need** for the sort of discretionary action that the law ordinarily seeks to circumscribe. As Locke explained in his classic formulation, that "it is impossible to foresee, and so by laws to provide for, all Accidents and Necessities, that may concern the publick means that the formal powers of the executive specified in law must be supplemented with "prerogative," the "Power to act according to discretion, for the publick good, without the prescription of the Law, and sometimes even against it." 8 Unlike the powers of the Hobbesian sovereign, which are effectively absolute and unlimited, the exercise of prerogative is, in principle, limited in scope and duration to cases of emergency. The power to act outside and even against the law **does not mean that the executive is "above the law”**—morally or politically unaccountable—**but it does mean that** executive power isultimately irreducible to law**.**

#### the President will manipulate procedures to keep Congress in the dark

**Dycus 10** – Professor at Vermont Law School, (Stephen 8/11/, “Congress’s Role in Cyber Warfare,” <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>)

In 1991, in response to the Iran-Contra Affair, Congress adopted a measure directing the President to keep the congressional intelligence committees “fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity.”25 The term “intelligence activity” expressly includes “covert actions,”26 which additionally require a written finding by the President that they are “necessary to support identifiable foreign policy objectives of the United States and [are] important to the national security of the United States.”27 Intelligence activities are also understood to include “all activities that elements of the Intelligence Community are authorized to conduct pursuant to [Executive Order No. 12,333],” the executive charter for such activities.28 The “intelligence community” includes the Office of the Director of National Intelligence, CIA, NSA, other Defense Department intelligence components, and other federal intelligence elements,29 which are authorized to engage in, inter alia, intelligence collection and analysis and “activities to protect against international terrorism . . . and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents.”30 This broad mandate certainly encompasses many U.S. efforts to defend against cyber attack and to employ cyber weapons offensively. By this definition, most preparations for and conduct of cyber warfare should be reported to the intelligence committees as “intelligence activities.” It is significant that the reporting requirement in the 1991 law is not limited to agencies within the intelligence community. ¶

Yet this legislation provides no guarantee that Congress will receive the information it needs to play a meaningful role in the development or execution of cyber warfare policy. It is not known, for example, precisely what it means for the intelligence committees to be “fully and currently” informed, what kinds of intelligence activities are regarded as “significant” enough to report, or who decides.31 Other sections of the 1991 law call on all agencies involved in intelligence activities, not just the President, to keep the intelligence committees informed about those activities, but only “[t]o the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters.”32 The “due regard for” language might be invoked to keep Congress in the dark. ¶ Under the 1991 law, “covert actions,” those with respect to which “it is intended that the role of the United States Government will not be apparent or acknowledged publicly,”33 need only be reported to a small group of legislators known as the “Gang of Eight,”34 and then only in a “timely fashion,” a term not defined by statute.35 Characterization of U.S. planning and execution of electronic warfare as “covert” could enable reporting to the smaller group, making it more difficult for Congress to play a significant role.36 Moreover, any reporting might be delayed indefinitely.37

### advantage

#### Cyber war infeasible—this evidence is the cat’s meow

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

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

#### their invocation of the cyber threat makes it happen - linear impact to debate

Gady, 13 [senior fellow at the EastWest Institute, where he was a program associate and founding member of the Worldwide Cybersecurity Initiative, “Shaky Cyber Trigger Fingers”, Franz-Stefan,

http://www.ewi.info/shaky-cyber-trigger-fingers-0

Project Syndicate recently featured EWI’s Franz-Stefan Gady’s “Shaky Cyber Trigger Fingers,” where he and co-author Alexander Klimburg argue that increased public awareness of cyber threats may actually be increasing tensions in cyberspace. Their article: A media storm centered on the “emerging cyber threat” has turbocharged the public debate on cyber security in the United States – and raised the stakes in bilateral relations with China. While wider public awareness of the cyber threat should be welcomed, the increasingly strident discourse may not help alleviate tensions in cyberspace. In the medium term, it might even increase the risk of serious cyber conflict. A recent report by the US Department of Defense employs the strongest language yet to implicate China’s government and military in cyber espionage, including on computer systems owned by the US government. The report also warns that, for those targeted by such activities, distinguishing between espionage and preparations for serious cyber attacks is virtually impossible. What the report does not mention is that this ambiguity has another important implication: a serious cyber conflict could easily be triggered by accident. This means that China’s alleged incursions are not the only threat; America’s increasingly forceful position on cyber espionage could inadvertently trigger a cyber war. After all, actions about cyberspace can be misunderstood just as easily as activities in cyberspace. In this context, the US government should tread lightly. While invoking the specter of cyberattacks may help to mobilize domestic support for security legislation, it may also increase the likelihood of a major cyber conflict. As another recent report from the US Department of Defense suggests, a cyber war could be catastrophic: military aircraft could be grounded, or, in an extreme scenario, parts of America’s nuclear arsenal could be compromised. Civilians would suffer considerably in such a “permanently degraded cyber environment,” which could include the collapse of energy and utility services. The lights might not simply go out; they could remain off for a long time. While such an apocalyptic scenario is unlikely to occur, it cannot be ruled out, especially given that a cyber conflict, unlike most conventional military conflicts, can be initiated unintentionally, taking even the party responsible by surprise. Such “inadvertent escalation” can stem from a pattern of imprudent operational behavior, for example, or from persistent strategic miscalculation. Given that national cyber security usually involves at least 5-6 government departments or ministries, along with a vast array of state and non-state actors, most operational tasks are conducted with minimal oversight. In other words, senior government officials do not always know what is occurring at the operational level – or understand how provocative or misleading it may be. While accusations of insufficient oversight over hackers’ activities have been leveled specifically at China, the challenge of tracking potentially disruptive cyber activities extends to all current and future cyber powers. At the same time, governments must contend with significant strategic challenges, which vary according to national conditions. For example, US law hampers the federal government’s ability to protect critical infrastructure and key resources from cyber attacks. While recent legislative proposals like the Cyber Information Security and Protection Act (CISPA) may help to improve the situation, their impact remains to be seen. The US, increasingly confident in its ability to identify and strike back at any cyber assailant, has so far evaded legal obstacles by focusing on deterrence. But this approach is effective only if would-be attackers have at least a basic understanding of America’s capabilities. Fortunately for the US, the media are helping to fill this gap with a steady stream of revelations on the subject. Deterrence, however, carries significant escalation risks. By instilling fear in its adversaries, deterrence can goad governments – even those that are not directly involved in current cyber standoffs – into reckless or unpredictable behavior. Although recent officials US statements have been directed primarily at China and Russia, they have motivated governments worldwide to build their own offensive cyber capabilities. While there is a small possibility that stronger language from the US will lead China to curb its alleged cyber-espionage activities, the more likely outcome will be akin to a cyber arms race, with an increasing number of countries striving to become cyber powers in their own right. More than 40 countries now have some sort of military-intelligence cyber capability, and with the proliferation of offensive cyber capabilities, inadvertent escalation will become increasingly likely.

#### No extinction

Wynne Parry 11, 2/2/11, Live Science Staff Writer, “Article: Theory About Mammals and Fungus Explains Bat Plague”, <http://www.livescience.com/11705-theory-mammals-fungus-explains-bat-plague.html>

Even highly virulent infectious disease does not cause extinctions – because as population density decreases, so does transmission, and the remaining individuals are more resistant. In addition, at the end of the Cretaceous, dinosaurs weren't the only ones to be decimated. Marine animals were affected, as were many species of flowering plant, according to Douglas Robertson, of the Cooperative Institute for Research in Environmental Sciences at the University of Colorado. "It is not even vaguely plausible that all these extinctions, let alone just the various dinosaur species extinctions, were all caused by some pathogen," Robertson wrote in an e-mail.

#### The medicalization of political discourses directly underwrites a reproduction of security discourse to eliminate the diseases and the filthy

**Campbell, 2008**

(David, Prof. of International Politics @ the University of Newcastle, *Writing Security: United States Foreign Policy and the Politics of Identity*, Revised Edition, University of Minnesota Press, ISBN 0-8166-3144-1, Pg. 81-82)

However one might begin to fathom the many issues located within those challenges, our current situation leaves us with one certainty: because we cannot escape the logic of differentiation, **we are often tempted by the logic of defilement. To say as much is not to argue that we are imprisoned within a particular and permanent system of representations.** To be sure, **danger is often represented as disease, dirt, or pollution.** As one medical text argues: "Disease is shock and danger for existence."32 Or as Karl Jaspers maintains: "Disease is a general concept of non-value which includes all possible negative values."33 But **such concerns have less to do with the intrinsic qualities of those conditions than the modernist requirements of order and stability: "Dirt offends against order. Eliminating it is not a negative moment, but a positive effort to organize the environment."**34 One might suggest that **it is the extent to which we want to organize the environment—the extent to which we want to purify our domain— that determines how likely it is that we represent danger in terms of dirt or disease. Tightly defined order and strictly enforced stability, undergirded by notions of purity, are not a priori conditions of existence; some order and some stability might be required for existence as we know it** (i.e., in some form of extensive political community), **but it is the degree of tightness, the measure of strictness, and the extent of the desire for purity that constitute danger as dirt or disease.** But **the temptation of the logic of defilement as a means of orienting ourselves to danger has more often than not been overpowering, largely because it is founded on a particular conceptualization of "the body";** in its use since at least the eighteenth century, this conceptualization demands purity as a condition of health and thus makes the temptation to defilement a "natural" characteristic. **This has endowed us with a mode of representation in which health and cleanliness serve the logic of stability, and disorder is rendered as disease and dirt.** In the eighteenth century, when state forms were becoming the most prevalent articulations of extensive political community, these modes of representation began to take a new turn that intensified the capacity of representations of disease to act as discourses of danger to the social.

In France, a number of notions that would be fundamental to the medicalization of society materialized around the time of the Revolution. Including the myth of a clergy-like national medical profession and the supposition that pacific republics would be totally free of disease, these notions altered the conception of medicine and changed the functioning of the body politic metaphor. In this context, Foucault argues, **medicine shifted from simply being an ensemble of practices for curing ills to a concern with the knowledge of the healthy, nonsick, and model man.**35 In association with a more widespread intellectual shift from juridical discourses that promulgated natural rules to a concern with codes of normalization, **this development meant that medicine reoriented its principal focus from that which was healthy to that which was normal. In this context, "when one spoke of the life of groups and societies, of the life of the race, or even of the 'psychological life/ one did not think first of the internal structure of the organized being, but of the medical bipolarity of the normal and thepathological."**36 **This development did not mean that representations of danger ceased to function in terms of disease, dirt, or some other form of defilement. Rather, it meant that just as "the body" functioned as a trope for the social, "disease" now functioned as a trope for the pathological in opposition to the normal.**

While the bipolarity of normal/pathological appears to derive its authority as a regulative ideal for society from its medical origins, this fact should not obscure the contested and problematic nature of such an understanding within the practice of medicine. Although the common effect of this bipolarity is to assume that "normal" refers to natural or desired health marked by the complete absence of disease, there have been many debates within medicine concerning the extent to which disease itself is something of a biological norm.37 That is, few if any people are marked by the complete absence of ailments or physical problems, and most surveys show that large numbers of people who live in a perfectly happy and satisfactory way possess physiological characteristics that depart markedly from statistical averages and would be a source of ill health to some.38 As a result, a medical conclusion would be that "if the normal does not have the rigidity of a fact of collective constraint but rather the flexibility of a norm which is transformed in its relations to individual conditions, it is clear that the boundary between the normal and the pathological becomes imprecise."39 Most important, **the variability inherent in physiological norms, and their subsequent lack of universality, means that the imputation of a clear distinction between health and disease—which is the regulative desire of the bipolarity of normal/pathological in the political realm—is an understanding effected by a social and cultural logic. It is not something mandated by medical knowledge.** In consequence, proclaims Canguilhem: "Pathological constants have a repulsive and strictly conservative value."40

#### Fear is an environment – the multiplication of simultaneous threats to our reality merely creates an atmospheric compression that makes even peace an unescapable fearful accident

Virilio and Richard ‘12 (Paul, French Thinker and Architect, and Bertrand, *The Administration of Fear*, pp. 42-45)

And yet, when we are afraid, that is not what we are afraid of... There are many intermediate, more prosaic fears (jobs, health, security) that take the place of what we should really be afraid of, which is that the world is becoming, as you describe it, unlivable, compressed, shrunk by speed. And the worst part is that we still want even more speed and instantaneity. What does it mean? My task, as you know, is to focus on the fear that is hidden by the ideology of progress. The hothouse effect of the siege mentality, the claustrophobia of masses of individuals under siege are the phenomena that draw and require my attention. During the Second World War, an American journalist entered the Warsaw Ghetto and noticed that the windows were open in the middle of winter even though the inhabitants were burning their furniture to keep warm. When he expressed his surprise, people there replied: “You wouldn't want us to have to close our windows too.” This is the siege mentality: foreclosure. The growing atmospheric pressure caused by global warming is joined by dromospheric pressure, the tension created by speed in our daily lives and work. At the intersection between the environment and our ways of life, we can find fears that are related to socio-economic contexts. On this topic, how can we not think of the wave of suicides that swept France Telecom at the beginning of winter in 2009-20 10? And the scale! How can we not see that fear has been administered, in the strict meaning of the term, by instant interactivity, in particular in the functions that relate to real-time communications? The acceleration of reality has had a considerable impact on social rhythms and has started to wreak havoc. The notion of arrhythmia that I also mentioned earlier is obvious in the slogan "Time to move," the management program implemented within France Telecom to ensure the permanent mobility among its executives. The rhythms of the past were tied to seasons, the liturgical calendar, Sunday holidays, the Sabbath; they have been pushed aside in favor of 24/7. "For what reason should we stop people from working on Sunday? The world is changing," is the refrain we now hear. With the rural exodus in the 19th century and the urban exodus that is beginning (since a number of Western cities have seen a decline in the net migration rate), with the change from an artisanal rhythm to an industrial rhythm to a postindustrial rhythm characterized by logics of synchronization, we are now experiencing firsthand the loss of the sociopolitical rhythmology that has always governed human beings. Temporal compression, as it is technically called, is an event that concretely modifies everyone's daily life at the same time. In the face of this acceleration of daily life, fear has become an environment, even in a time of peace. We are living in the accident of the globe, the accident of instantaneousness, simultaneity and interactivity that have now gained the upper hand over ordinary activities.

#### The world is becoming a global concentration camp with accidents constantly growing in scale. The final catastrophe – absolute nuclear annihilation – is becoming inevitable and the aff makes it worse through their reliance on tech and communication to resolve their impacts

Hutchings 8 (Kimberly Hutchings, Professor and Department Head of International Relations at the London School of Economics and Political Science, 2008, “Apocalyptic times” in *Time and world politics: thinking the present*, Manchester University Press)

Virilio develops an extensive vocabulary to capture his vision of chronopolitics (2000: 109). But the most telling of the terms he uses is 'globalitarian', in which the concepts of 'globalisation' and 'totalitarianism' are fused (2000: 10-11). Here his arguments are strongly reminiscent of Arendt's account of totalitarianism (Arendt, 1986). Globalisation is totalitarian because it both homogenises and fragments the human condition. It homogenises it by destroying the spaces between individuals that condition the possibility of political judgement and action. There is no plurality of perspective in globalitarian time, and therefore no democratic engagement. Instead we have a politics (or non-politics) of collectivist emotion, of immediate gut reaction to simultaneously experienced events, in which there is no possibility of mediation (Virilio, 2005: 33). Globalisation fragments the human condition because it destroys the common location in which political community can be sustained, leaving individuals with nothing but the commitment to their own material, instant gratification, which feeds into a logic of instrumentality and technical control, and extends into all bodily as well as spiritual domains of existence (2000: 66). Like Arendt, Virilio is also clear that people are at least partly responsible for their own globalitarian plight. He argues that we are complicit with the projects of control and surveillance that have spilled over from war into all spheres of human existence. **We should**, he suggests, **be thinking about how to control this new temporality, rather than letting it control us.** But his arguments make it difficult to see how this could be possible. A crucial question arises at this precise instant in history: can one democratise ubiquity, instantaneity, omniscience and omnipresence, which are precisely the privileges of the divine, or in other words, of autocracy? (2002: 134) One strand of Virilio's thought can be traced back to Rousseau or, more generally, the romantic and conservative critiques of modernity that have deplored the effects on society and politics of mass society and materialism, from Burke to Arendt. However, there is another strand of his argument that is strongly technologically determinist. The first strand of argument permits the possibility of the invention or reinvention of **alternative spatio-temporal conditions for politics that might allow politics** (and thereby humanity) to take priority over war or technological innovation. It is this first strand that leads Virilio to deny that he is a purveyer of doom, and identify himself instead as a political actor (2005: 100). But the second strand of argument sees the fate of humanity as technologically determined, from the point at which politics becomes possible to the point at which it ceases to exist. If one defines politics in terms of particular kinds of spatio-temporal conditions that can no longer apply, then the answer to Virilio's 'crucial question' has to be in the negative. It is in this mode that Virilio writes of the earth as 'the colony, the camp of the great ordeal' (2000: 131) or our lives as a 'labyrinth for laboratory animals' (1997a: 73). However, there is another twist to Virilio's narrative. His grim vision of the **earth as a global concentration camp** is not the only possible ending, the end of chronos as such is also possible: if interactivity is to information what radioactivity is to energy, then we are confronted with the fearsome emergence of the **'Accident to end all accidents'**, an accident which is no longer local and precisely situated, but global and generalised. (2000: 134) Inherent in every form of chronos are different possibilities of accidental catastrophe, from the train wreck to **nuclear holocaust**. The accident undoes the power of control inherent in different technologies, but is also only possible because of them. For the first time, however, in the era of electro-magnetic proximity**, this 'undoing' threatens to undo the human species altogether, if not immediately then certainly in the longer term** (Armitage, 2000a: 44). In the contemporary era, the project of technical control is confronted for the first time in pure form with the potentially **wholly catastrophic consequences** of its own power on a number of fronts **economically and biopolitically as well as militarily**. The idea of 'accident' encompasses not just the possibility of another Chernobyl, but more broadly any of the unintended consequences of new technologies. For Virilio this includes **the possibility of world economic collapse**, which follows from the technologies that **enable a single world market and the gradual replacement of humanity itself by its virtual counterparts**. In this respect, **the road to hell is most certainly paved with good intentions**, since the technologies enabling the world market or cloning or cyber-sex were set up to serve rather than to destroy human interests. And so, we have seen the emergence of a third anthropological type over the twentieth century: **the exterminator**. Not so much the butcher of a terrorism that has turned suicidal, the looming shadow of the lost soldier of the wars of days gone by; more the kind of butcher who ingeniously **offers the means of putting an end to the world** and to its embedded humanity every possible means, including economic, technical and scientific **all the while being intimately persuaded of bringing Progress, as superior civilization.** (2005: 79) Virilio extends his argument about the accident to encompass more generally the implications of a world in which fear of the consequences of loss of control matches the scale of devastation that technologies of control have made possible. In this kind of world, he argues, there is a **tendency for the declaration of a 'state of emergency' to become widespread, and for pre-emptive action to be seen as the appropriate response** to unexpected events. He interprets the US response to the events of 9/11 in these terms (2005: 74).

## 2NC

LOOK AT ALL THESE CARDS JOE READ

### cyber k

#### Our interpretation is that the internet ought to be free.

Deibert 2k3(Ronald, “Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace” Millennium - Journal of International Studies 2003 32: 501)

Of course, problems of access to policy forums for civil society organisations are not unique to the ICT sector. But, one area where civic networks may have the upper hand that civil society organisations working in other policy sectors do not is in terms of the influence on the very environment of the Internet itself. Since its beginnings, the Internet’s architecture has been shaped not only by states and corporations but also by the distributed base of users themselves. Indeed, networks of skilled individuals have been responsible for some of the most revolutionary Internet technologies, from open source/free software platforms to P2P networks and encryption systems. The Internet’s saving grace may lay in the resources of its millions of users spread around the world, especially as those networked individuals harness their creativity to politically defined goals. Having been turned on and energised by the distributed potential of digital-electronic communications, these skilled individuals and groups are almost impossible to turn off. The term used to describe this combination of politically motivated, grassroots technology development is ‘hacktivism’.91 Inspired by the original definition of the term hacker, ‘exploring the details of programmable systems and how to stretch their capabilities’,92 hacktivists have developed technologies in three key areas: anticensorship and freedom of speech, privacy, and Internet security. Some of these technologies are developed by ad hoc groups of hackers and activists, others by small companies. The scope of these technologies ranges from small, simple scripts and programs to highly developed P2P network protocols, steganography tools, and advanced software development. Hacktivists gather around major Internet forums, like Slashdot, monitoring policy developments and offering technical solutions.93 One of the more interesting hacktivist groups is Hacktivismo, an offshoot of one of the Internet’s oldest and most well known hacker groups, the Cult of the Dead Cow.94 Hacktivismo may at first appear to be a typically sophomoric club of computer enthusiasts, but closer inspection reveals a more serious agenda. Hacktivismo’s Declaration takes as its starting point the principles and purposes enshrined in Article 19 of the Universal Declaration of Human Rights regarding freedom of speech. Its board of advisers includes a high profile human rights advocate and renowned Internet lawyer. But it is the network of technology programmers that gives Hacktivismo its clout and credibility. In recent years, Hacktivismo has been responsible for several privacy and security enhancing technologies designed to allow citizens in repressive states to surf around censorship and surveillance.95 Hacktivismo is by no means alone. Hacktivist tools have sprouted all over the Internet in increasing numbers, and increasingly with the financial support of major international foundations. With nearly every government attempt to censor online communications, hacktivists create and distribute tools to get around them. As soon as a corporation comes up with the latest method of protecting digital copyright, hacktivists are there to crack the code**.** Although this movement is still multi-directional and politically immature, it can be seen as a potentially formidable check on attempts to re-exert control over the Internet’s distributed, open architecture.96 Generally speaking, theories of globalisation, global civil society, and transnational networks have assumed a continuing trajectory of increasingly open and distributed communications. This in turn is gradually diminishing the power of the state while fuelling the rise of what James Rosenau aptly called ‘sovereignty-free actors’. As the analysis above suggests, that assumption can no longer be taken for granted. Although the properties of the Internet may very well have been biased towards openness and decentralisation in the past, it is important to remember that the Internet is not a fixed medium that will remain unchanged into the future and as it changes, so too will its consequences. The Internet is, rather, a complex mix of technological systems in constant evolution, morphing in response to the pressures and technological choices of powerful actors able to influence its overall architecture.97 States — especially powerful ones like the United States — still constitute one of those major actors. For those concerned with deepening and expanding the prospects for global democratic governance and the flourishing of global civil society in the context of an emerging single world polity, the evolving nature or architecture of the communications infrastructure should be, therefore, of vital concern. For all its many faults and digital divides, it is the Internet that is providing the means by which an increasing number of citizens around the world can and will deliberate, debate, and ultimately have an input into the rules of the game by which they are governed. While at one time the Internet, and in particular its characteristically liberal environment, could be taken for granted by civil society actors, that time has now passed. Aformidable set of social forces is pushing regulations and technologies that, whatever their individual aims, collectively have the effect of taking that open, liberal architecture in a decidedly different direction. Global citizen networks must now become dynamic participants in the politics of Internet design, or risk having the power source for their activities increasingly unplugged. To do so, however, IR theorists — interested in and normatively in favour of opening up spaces for alternative voices, grassroots democracy, and global democratic governance to flourish — will have to pay greater attention to the material foundations upon which global communications take place. Doing so means qualifying notions of ‘ideas all the way down’ and ‘worlds of our making’ to acknowledge the extent to which material factors of communication, albeit socially constructed,98 present a formidable set of real constraints on the realm of the possible.99 Quite naturally, those interested in such topics have been concerned primarily with moving away from older positivist-materialist notions of state interaction to concerns about the circulation of ideas, the framing role of discourses, and processes of legitimation. But communication does not take place in a vacuum. It is anchored within and shaped by the material properties of the communications environment. It is with some small measure of optimism then that one can look upon recent developments in the area of civic networks and Internet governance. Among the converging interests of NGO users, privacy advocates, computer scientists, and grassroots media, one can detect the emergence of a kind of ‘epistemic community’. Although principles have nowhere been formally codified, a constellation of values brings these groups together to help give shape to a common agenda. Bolstering this transnational social movement is the powerful ammunition of politically motivated research and development of civic technologies that feed into, and give concrete shape to, the Internet’s basic structural design. Those material constraints, embedded in code, may in the long run provide the most important constitutional mechanisms to ensure that a communications infrastructure supports, rather than detracts from, the ongoing project of global democratic governance.

#### Cyber activism is comparatively MORE IMPORTANT to creating the possibility of peace online than judicial reform

Deibert 2k3(Ronald, “Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace” Millennium - Journal of International Studies 2003 32: 501)

Accompanying electronic surveillance has been the largely undebated militarisation of cyberspace. A great deal of attention has focused on the question of cyberterrorism, particularly in the wake of 9/11 and fears of potential terrorist use of electronic networks.55 While some see the possibility of an ‘electronic Pearl Harbour’ being unleashed by terrorists, skilled individuals and non-state actors, many others believe these fears are largely overdrawn and ignore the redundancies built into the architecture of the Internet as well as the relatively low pay-off for groups whose ultimate aim is violence.56 In spite of the alarm, there are no empirical examples of cyber-terrorism to date, unless the term is used so broadly as to encompass politically motivated hacks on websites and occasional inconveniences caused by denial of service attacks. Rather than tools of mass destruction, threats from terrorist actors employing the Internet appear to bode little more than periodic disruptions to Internet traffic.57 Whatever the ultimate nature of the threat, the debate has largely obscured a potentially more serious development: the quiet expansion and adoption of offensive information warfare capabilities by states. The military use of cyberspace operates on a new terrain, presenting many thorny legal and moral questions concerning the targeting of civilian infrastructures, and the boundaries between an armed assault, a probe, the collection of information, and the dissemination of propaganda.58 Theory has definitely trailed behind practice in this case.59 As in most areas of military capabilities, the United States leads the cyber arms race. The development of cyber-war tools can be seen as a natural evolution of the so-called Revolution in Military Affairs (RMA), the latter defined as a major change in the nature of warfare brought about by the innovative use of new technologies and organisational structures related to them; from advanced computing and communications technologies to remote sensors.60 Going back further, its roots can be found in the use of propaganda and psychological warfare techniques and electronic jamming that date to the Second World War: electromagnetic pulse bombs (EMPs), and the insertion of malicious codes and secret back doors in software for intelligence purposes during the Cold War. While much of these techniques were kept clandestine, the United States has recently acknowledged that offensive cyber-war is an official element of strategic doctrine.61 The United States’ military now openly employs computer hackers, develops advanced Trojan horses, viruses, and worms, and has used techniques of cyber-propaganda and other sophisticated ‘psychological operations’ leading up the conflict in Iraq.62 It is not alone. Dozens of countries around the world have either debated or adopted offensive cyber-war capabilities, including China, Russia, Taiwan, Israel, the United Kingdom, Australia, and Canada. The number of documented state cyber-war has risen in recent years as well. In spite of the greater penetration of these technologies in advanced industrialised countries, many of the more prominent examples of information warfare have occurred in the developing world.63 It is, of course, well known that radio networks were employed by Tutsi militia to incite genocidal violence against Hutus in Rwanda. Later, the Rwandan military regularly eavesdropped on insecure United Nations and humanitarian NGOs’ communications networks, and in at least one case used the intelligence to hunt down and kill Hutu refugees.64 During the Russian campaign against Chechnya in the mid-1990s, Chechen commanders made efficient use of mobile phone networks and eavesdropped on insecure Russian radio networks to organise devastatingly successful military strikes. In 2000, an ‘inter-fada’ erupted between Israeli and Lebanese hackers as each bombarded the other’s networks in distributed denial of service attacks. In the 2002 reoccupation of Palestine by the Israeli Defence Forces (IDF), the IDF systematically targeted the communications and information infrastructure of the Palestinian Authority and other civil society groups in tactics ranging from removing hard drives to disabling telephone switchboards.65 What are the concerns for global civic networks of the militarisation of cyberspace? In some respects, the threats may be exaggerated. Just as networked redundancies and distributed security practices constrain the potential ramifications of cyber-terrorism, there may be natural limits to the type of havoc states can wreak on the global communications infrastructure. There are also rational, as well as technological, constraints. Much like the deterrent effect of nuclear weapons, states that are home to private corporations with assets spread transnationally throughout the world face strong financial incentives to preserve the security and seamless functioning of global communications networks that are the sinews of hyper-capitalism. These constraints should not be overdrawn, however. Rational choice models of costs and benefits do not always translate neatly into the equations drawn for the use of force internationally. And even targeted attacks on infrastructures can cause enormous disruptions to the flows of information worldwide, as several recent worms and viruses have demonstrated. More broadly for global democratic governance, however, is a theoretical question about the proper constitutive relationship between military and civilian spheres in liberal democratic polities; particularly as these bear on questions concerning the design of the public sphere. The Internet is much more than a simple appendage to other sectors of world politics — it is the forum or commons within which civic communications will take place. Preserving this commons from militarisation **is** as essential to global democratic governance **as is** the judicial restraint on force **in domestic political spheres**. Given the race by states to develop offensive information warfare capabilities, and its potentially destructive and unforeseeable consequences, has the time come for a kind of cyberspace ‘arms control’? If so, what might that look like and how might it emerge?66 Though not described in terms of arms control per se, the following section offers a survey of the prospects.

#### Absent recognizing the importance of the figure of the hacker, their policy is doomed to failure—this evidence is from a policy expert

Rosenzweig, 12 [ Copyright (c) 2012 I/S: A Journal of Law & Policy for the Information Society I/S: A Journal of Law and Policy for the Information Society Fall, 2012 I/S: A Journal of Law and Policy for the Information Society 8 ISJLP 393 LENGTH: 7722 words NAME: Paul \* BIO: \* Principal, Red Branch Consulting PLLC; Carnegie Fellow in National Security Journalism, Medill School of Journalism, Northwestern University (2011); Professorial Lecturer in Law, George Washington University. The author served as Deputy Assistant Secretary for Policy in the Department of Homeland Security from 2005-09. Portions of this article will appear in the forthcoming book Cyberwarfare: How Conflicts in Cyberspace are Challenging American and Changing the World (Santa Barbara: Praeger, 2012, p. lexis]

IV. Conclusion If the question about cyberspace is: "What is our policy making apparatus most likely to misunderstand or get wrong?" the answer, I fear, is quite a lot. Not because policy makers in Washington are ill-meaning, or venal, or even unintelligent. But rather, I fear, because they are confronting a new reality to which they have yet to adapt. The sausage making process of policy development inside sovereign governments is slow and encrusted with hierarchical restrictions. It lacks the pace and capacity to keep up with the ever-changing environment of the Internet. Worse, policy makers continue to think of the Internet as just another tool-sort of like a telephone, but quicker. But the things that "everybody knows" are changing every day. Until we come to grips with the ubiquity and rapidity of the Internet and the fundamental way in which the Internet creates asymmetries that empower the individual to the disadvantage of the nation-state, we won't really build good cyber policy. It's a daunting task-but no easier for putting off to the future.

#### Focus on top down executive regulation solutions reinforces a notion of sovereignty that is unitary that marginalizes alternative political formations—choose the model of Edward Snowden rather than the congressional representative

Buell 13. John Buell, columnist for The Progressive Populist, adjunct professor at Cochise College, “Nationalism, Tech Giants, and Spy States,” The Contemporary Condition August 10, 2013 <http://contemporarycondition.blogspot.com/2013/08/nationalism-tech-giants-and-spy-states.html> accessed September 4, 2013

That's is one reason it is hard today to remain aloof from politics. But for those who seek to do so the message is just as clear. If the Internet has progressive possibilities, their realization will not be automatic. Today a countersubversive culture nurtures and is nurtured by an evolving alliance of high tech giants, government bureaucrats (whom Smith calls securecrats), the older more established military industrial complex and powerful private corporations that benefit from close ties to the state, including especially the oil  and investment banking community.

If the most repressive outcomes are to be avoided, the best course might be an evolving counter-coalition that would emerge from moral and historical critiques of and alternative to the countersubversive tradition. In Emergency Politics, Honig argues that the very focus on the question of the rules that should govern declarations of emergency and the protections that can be revoked in emergencies reinforce a notion of sovereignty as unitary and top down. Thus they "marginalize forms of popular sovereignty in which action in concert rather than institutional governance is the mark of democratic power and legitimacy." Unitary and decisive sovereignty committed to its own invulnerability is "most likely to perceive crisis where there may only be political conflict and to respond...with antipolitical measures."

The best answer lies not merely in challenging the constitutional status of this surveillance state but in building a political coalition that embodies the forms of popular sovereignty of which Honig speaks. This would include labor, consumer and environmentalist critiques of and alternatives to the role of the state and markets in fostering inequality. It would be attentive to the possibilities and risks of the social media and the limits of its own interventions in these.  The coalition might advance more democratic forms of enterprise and media as well as decentralized and more sustainable forms of energy production and transportation.  And in an era where hyper nationalism erodes so many democratic impulses, cross border initiatives in the interest of widespread access to an open Internet with robust privacy protections would be paramount. (Let's hope that) Edward Snowden's travels (in a world dominated by the state passport and surveillance system) helps to highlight the stake citizens of many lands have in a democratic Internet but a more exploratory and democratic polity

#### Our interpretation is that the internet ought to be free.

Deibert 2k3(Ronald, “Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace” Millennium - Journal of International Studies 2003 32: 501)

Of course, problems of access to policy forums for civil society organisations are not unique to the ICT sector. But, one area where civic networks may have the upper hand that civil society organisations working in other policy sectors do not is in terms of the influence on the very environment of the Internet itself. Since its beginnings, the Internet’s architecture has been shaped not only by states and corporations but also by the distributed base of users themselves. Indeed, networks of skilled individuals have been responsible for some of the most revolutionary Internet technologies, from open source/free software platforms to P2P networks and encryption systems. The Internet’s saving grace may lay in the resources of its millions of users spread around the world, especially as those networked individuals harness their creativity to politically defined goals. Having been turned on and energised by the distributed potential of digital-electronic communications, these skilled individuals and groups are almost impossible to turn off. The term used to describe this combination of politically motivated, grassroots technology development is ‘hacktivism’.91 Inspired by the original definition of the term hacker, ‘exploring the details of programmable systems and how to stretch their capabilities’,92 hacktivists have developed technologies in three key areas: anticensorship and freedom of speech, privacy, and Internet security. Some of these technologies are developed by ad hoc groups of hackers and activists, others by small companies. The scope of these technologies ranges from small, simple scripts and programs to highly developed P2P network protocols, steganography tools, and advanced software development. Hacktivists gather around major Internet forums, like Slashdot, monitoring policy developments and offering technical solutions.93 One of the more interesting hacktivist groups is Hacktivismo, an offshoot of one of the Internet’s oldest and most well known hacker groups, the Cult of the Dead Cow.94 Hacktivismo may at first appear to be a typically sophomoric club of computer enthusiasts, but closer inspection reveals a more serious agenda. Hacktivismo’s Declaration takes as its starting point the principles and purposes enshrined in Article 19 of the Universal Declaration of Human Rights regarding freedom of speech. Its board of advisers includes a high profile human rights advocate and renowned Internet lawyer. But it is the network of technology programmers that gives Hacktivismo its clout and credibility. In recent years, Hacktivismo has been responsible for several privacy and security enhancing technologies designed to allow citizens in repressive states to surf around censorship and surveillance.95 Hacktivismo is by no means alone. Hacktivist tools have sprouted all over the Internet in increasing numbers, and increasingly with the financial support of major international foundations. With nearly every government attempt to censor online communications, hacktivists create and distribute tools to get around them. As soon as a corporation comes up with the latest method of protecting digital copyright, hacktivists are there to crack the code**.** Although this movement is still multi-directional and politically immature, it can be seen as a potentially formidable check on attempts to re-exert control over the Internet’s distributed, open architecture.96 Generally speaking, theories of globalisation, global civil society, and transnational networks have assumed a continuing trajectory of increasingly open and distributed communications. This in turn is gradually diminishing the power of the state while fuelling the rise of what James Rosenau aptly called ‘sovereignty-free actors’. As the analysis above suggests, that assumption can no longer be taken for granted. Although the properties of the Internet may very well have been biased towards openness and decentralisation in the past, it is important to remember that the Internet is not a fixed medium that will remain unchanged into the future and as it changes, so too will its consequences. The Internet is, rather, a complex mix of technological systems in constant evolution, morphing in response to the pressures and technological choices of powerful actors able to influence its overall architecture.97 States — especially powerful ones like the United States — still constitute one of those major actors. For those concerned with deepening and expanding the prospects for global democratic governance and the flourishing of global civil society in the context of an emerging single world polity, the evolving nature or architecture of the communications infrastructure should be, therefore, of vital concern. For all its many faults and digital divides, it is the Internet that is providing the means by which an increasing number of citizens around the world can and will deliberate, debate, and ultimately have an input into the rules of the game by which they are governed. While at one time the Internet, and in particular its characteristically liberal environment, could be taken for granted by civil society actors, that time has now passed. Aformidable set of social forces is pushing regulations and technologies that, whatever their individual aims, collectively have the effect of taking that open, liberal architecture in a decidedly different direction. Global citizen networks must now become dynamic participants in the politics of Internet design, or risk having the power source for their activities increasingly unplugged. To do so, however, IR theorists — interested in and normatively in favour of opening up spaces for alternative voices, grassroots democracy, and global democratic governance to flourish — will have to pay greater attention to the material foundations upon which global communications take place. Doing so means qualifying notions of ‘ideas all the way down’ and ‘worlds of our making’ to acknowledge the extent to which material factors of communication, albeit socially constructed,98 present a formidable set of real constraints on the realm of the possible.99 Quite naturally, those interested in such topics have been concerned primarily with moving away from older positivist-materialist notions of state interaction to concerns about the circulation of ideas, the framing role of discourses, and processes of legitimation. But communication does not take place in a vacuum. It is anchored within and shaped by the material properties of the communications environment. It is with some small measure of optimism then that one can look upon recent developments in the area of civic networks and Internet governance. Among the converging interests of NGO users, privacy advocates, computer scientists, and grassroots media, one can detect the emergence of a kind of ‘epistemic community’. Although principles have nowhere been formally codified, a constellation of values brings these groups together to help give shape to a common agenda. Bolstering this transnational social movement is the powerful ammunition of politically motivated research and development of civic technologies that feed into, and give concrete shape to, the Internet’s basic structural design. Those material constraints, embedded in code, may in the long run provide the most important constitutional mechanisms to ensure that a communications infrastructure supports, rather than detracts from, the ongoing project of global democratic governance.

#### Cyber activism is comparatively MORE IMPORTANT to creating the possibility of peace online than judicial reform

Deibert 2k3(Ronald, “Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace” Millennium - Journal of International Studies 2003 32: 501)

Accompanying electronic surveillance has been the largely undebated militarisation of cyberspace. A great deal of attention has focused on the question of cyberterrorism, particularly in the wake of 9/11 and fears of potential terrorist use of electronic networks.55 While some see the possibility of an ‘electronic Pearl Harbour’ being unleashed by terrorists, skilled individuals and non-state actors, many others believe these fears are largely overdrawn and ignore the redundancies built into the architecture of the Internet as well as the relatively low pay-off for groups whose ultimate aim is violence.56 In spite of the alarm, there are no empirical examples of cyber-terrorism to date, unless the term is used so broadly as to encompass politically motivated hacks on websites and occasional inconveniences caused by denial of service attacks. Rather than tools of mass destruction, threats from terrorist actors employing the Internet appear to bode little more than periodic disruptions to Internet traffic.57 Whatever the ultimate nature of the threat, the debate has largely obscured a potentially more serious development: the quiet expansion and adoption of offensive information warfare capabilities by states. The military use of cyberspace operates on a new terrain, presenting many thorny legal and moral questions concerning the targeting of civilian infrastructures, and the boundaries between an armed assault, a probe, the collection of information, and the dissemination of propaganda.58 Theory has definitely trailed behind practice in this case.59 As in most areas of military capabilities, the United States leads the cyber arms race. The development of cyber-war tools can be seen as a natural evolution of the so-called Revolution in Military Affairs (RMA), the latter defined as a major change in the nature of warfare brought about by the innovative use of new technologies and organisational structures related to them; from advanced computing and communications technologies to remote sensors.60 Going back further, its roots can be found in the use of propaganda and psychological warfare techniques and electronic jamming that date to the Second World War: electromagnetic pulse bombs (EMPs), and the insertion of malicious codes and secret back doors in software for intelligence purposes during the Cold War. While much of these techniques were kept clandestine, the United States has recently acknowledged that offensive cyber-war is an official element of strategic doctrine.61 The United States’ military now openly employs computer hackers, develops advanced Trojan horses, viruses, and worms, and has used techniques of cyber-propaganda and other sophisticated ‘psychological operations’ leading up the conflict in Iraq.62 It is not alone. Dozens of countries around the world have either debated or adopted offensive cyber-war capabilities, including China, Russia, Taiwan, Israel, the United Kingdom, Australia, and Canada. The number of documented state cyber-war has risen in recent years as well. In spite of the greater penetration of these technologies in advanced industrialised countries, many of the more prominent examples of information warfare have occurred in the developing world.63 It is, of course, well known that radio networks were employed by Tutsi militia to incite genocidal violence against Hutus in Rwanda. Later, the Rwandan military regularly eavesdropped on insecure United Nations and humanitarian NGOs’ communications networks, and in at least one case used the intelligence to hunt down and kill Hutu refugees.64 During the Russian campaign against Chechnya in the mid-1990s, Chechen commanders made efficient use of mobile phone networks and eavesdropped on insecure Russian radio networks to organise devastatingly successful military strikes. In 2000, an ‘inter-fada’ erupted between Israeli and Lebanese hackers as each bombarded the other’s networks in distributed denial of service attacks. In the 2002 reoccupation of Palestine by the Israeli Defence Forces (IDF), the IDF systematically targeted the communications and information infrastructure of the Palestinian Authority and other civil society groups in tactics ranging from removing hard drives to disabling telephone switchboards.65 What are the concerns for global civic networks of the militarisation of cyberspace? In some respects, the threats may be exaggerated. Just as networked redundancies and distributed security practices constrain the potential ramifications of cyber-terrorism, there may be natural limits to the type of havoc states can wreak on the global communications infrastructure. There are also rational, as well as technological, constraints. Much like the deterrent effect of nuclear weapons, states that are home to private corporations with assets spread transnationally throughout the world face strong financial incentives to preserve the security and seamless functioning of global communications networks that are the sinews of hyper-capitalism. These constraints should not be overdrawn, however. Rational choice models of costs and benefits do not always translate neatly into the equations drawn for the use of force internationally. And even targeted attacks on infrastructures can cause enormous disruptions to the flows of information worldwide, as several recent worms and viruses have demonstrated. More broadly for global democratic governance, however, is a theoretical question about the proper constitutive relationship between military and civilian spheres in liberal democratic polities; particularly as these bear on questions concerning the design of the public sphere. The Internet is much more than a simple appendage to other sectors of world politics — it is the forum or commons within which civic communications will take place. Preserving this commons from militarisation **is** as essential to global democratic governance **as is** the judicial restraint on force **in domestic political spheres**. Given the race by states to develop offensive information warfare capabilities, and its potentially destructive and unforeseeable consequences, has the time come for a kind of cyberspace ‘arms control’? If so, what might that look like and how might it emerge?66 Though not described in terms of arms control per se, the following section offers a survey of the prospects.

#### Absent recognizing the importance of the figure of the hacker, their policy is doomed to failure—this evidence is from a policy expert

Rosenzweig, 12 [ Copyright (c) 2012 I/S: A Journal of Law & Policy for the Information Society I/S: A Journal of Law and Policy for the Information Society Fall, 2012 I/S: A Journal of Law and Policy for the Information Society 8 ISJLP 393 LENGTH: 7722 words NAME: Paul \* BIO: \* Principal, Red Branch Consulting PLLC; Carnegie Fellow in National Security Journalism, Medill School of Journalism, Northwestern University (2011); Professorial Lecturer in Law, George Washington University. The author served as Deputy Assistant Secretary for Policy in the Department of Homeland Security from 2005-09. Portions of this article will appear in the forthcoming book Cyberwarfare: How Conflicts in Cyberspace are Challenging American and Changing the World (Santa Barbara: Praeger, 2012, p. lexis]

IV. Conclusion If the question about cyberspace is: "What is our policy making apparatus most likely to misunderstand or get wrong?" the answer, I fear, is quite a lot. Not because policy makers in Washington are ill-meaning, or venal, or even unintelligent. But rather, I fear, because they are confronting a new reality to which they have yet to adapt. The sausage making process of policy development inside sovereign governments is slow and encrusted with hierarchical restrictions. It lacks the pace and capacity to keep up with the ever-changing environment of the Internet. Worse, policy makers continue to think of the Internet as just another tool-sort of like a telephone, but quicker. But the things that "everybody knows" are changing every day. Until we come to grips with the ubiquity and rapidity of the Internet and the fundamental way in which the Internet creates asymmetries that empower the individual to the disadvantage of the nation-state, we won't really build good cyber policy. It's a daunting task-but no easier for putting off to the future.

#### Focus on top down executive regulation solutions reinforces a notion of sovereignty that is unitary that marginalizes alternative political formations—choose the model of Edward Snowden rather than the congressional representative

Buell 13. John Buell, columnist for The Progressive Populist, adjunct professor at Cochise College, “Nationalism, Tech Giants, and Spy States,” The Contemporary Condition August 10, 2013 <http://contemporarycondition.blogspot.com/2013/08/nationalism-tech-giants-and-spy-states.html> accessed September 4, 2013

That's is one reason it is hard today to remain aloof from politics. But for those who seek to do so the message is just as clear. If the Internet has progressive possibilities, their realization will not be automatic. Today a countersubversive culture nurtures and is nurtured by an evolving alliance of high tech giants, government bureaucrats (whom Smith calls securecrats), the older more established military industrial complex and powerful private corporations that benefit from close ties to the state, including especially the oil  and investment banking community.

If the most repressive outcomes are to be avoided, the best course might be an evolving counter-coalition that would emerge from moral and historical critiques of and alternative to the countersubversive tradition. In Emergency Politics, Honig argues that the very focus on the question of the rules that should govern declarations of emergency and the protections that can be revoked in emergencies reinforce a notion of sovereignty as unitary and top down. Thus they "marginalize forms of popular sovereignty in which action in concert rather than institutional governance is the mark of democratic power and legitimacy." Unitary and decisive sovereignty committed to its own invulnerability is "most likely to perceive crisis where there may only be political conflict and to respond...with antipolitical measures."

The best answer lies not merely in challenging the constitutional status of this surveillance state but in building a political coalition that embodies the forms of popular sovereignty of which Honig speaks. This would include labor, consumer and environmentalist critiques of and alternatives to the role of the state and markets in fostering inequality. It would be attentive to the possibilities and risks of the social media and the limits of its own interventions in these.  The coalition might advance more democratic forms of enterprise and media as well as decentralized and more sustainable forms of energy production and transportation.  And in an era where hyper nationalism erodes so many democratic impulses, cross border initiatives in the interest of widespread access to an open Internet with robust privacy protections would be paramount. (Let's hope that) Edward Snowden's travels (in a world dominated by the state passport and surveillance system) helps to highlight the stake citizens of many lands have in a democratic Internet but a more exploratory and democratic polity

#### The 1ac is an exercise in post-panoptic power that thrives on its invisibility—they make the whole of cyberspace into a potential virtual camp as there can be no outside its liberal regulation

Diken and lausten 2k3(Bulent, Carsten “Zones of indistinction - security, terror, and bare life” <http://www.lancs.ac.uk/fass/sociology/papers/diken-laustsen-zones-of-indistinction.pdf>)

Control is digital, it translates everything into the logic of codes and passwords, and thus transgresses the duality of mass and individual. “Individuals become ‘dividuals,’ and masses become samples, data, markets, or ‘banks’” (Deleuze 1995: 180). Focusing on biosurveillance methods through access to tissues, fluids and images available from the body itself, control transforms “the body into a password” (Lyon 2001: 75). Post-panoptic power can interpellate the subject in absentia through electronic lists (see Poster 1996). Regulating a fluid and endlessly divisible, fractal, “multitude” rather than “peoples”, control produces a hybrid, metastable subjectivity that no longer corresponds to stable identities of the disciplinary society (Hardt & Negri 2000: 331-2). In this sense control brings with it an infinite intensification of discipline in a smooth space devoid of enclosures; control is discipline without walls, a mobile form of discipline that regulates humans and non-humans “on the move” (Lyon 2001: 63). Nomadism was once a critical tool against discipline, a “line of flight” out of the panopticon, but control society captures nomadic “war machines”, accommodating them for its own purposes (see Deleuze & Guattari 1987: 387). Moving from “exceptional discipline” to “generalized surveillance” (Foucault 1977: 209), control extends the logic of the camp. With intensified and direct biopolitical access to bare life, control “knows no outside” (Hardt & Negri 2000: 413). Its logic transgresses the binary logic of the inside/outside distinction for it is a “decentered and deterritorializing apparatus of rule” (Hardt & Negri 2000: xii). Modern discipline had played upon the distinction between inside and outside; post-modern control, in contrast, constitutes an “ou-topia”, a non-place (Hardt & Negri 2000: 190). When there is no outside left, the zone of indistinction opened up by the camp becomes the smooth space of control, a generalized space of indistinction. Which turns discipline itself into a simulacrum: in control society “prisons are there to hide that it is the social in its entirety, in its banal omnipresence, that is carceral” (Baudrillard 1994: 12). The city as a complex technological artifact illuminates the logic of control. Systems of control are urban phenomena; cities constitute nodal points in mobile societies of surveillance, and even cyberspaces are congested “around conventional urban areas” (Lyon 2001: 53-4). Yet this is misleading because the “conventional city” no longer exists. The contemporary city is no longer founded on the divide between its “intramural” population and the outside; “it no longer has anything to do with the classical oppositions of city/country nor centre/periphery” (Virilio 1997: 382, 390). The city of control is an immanent space, a reticular ou-topia, sharing with all other networks a “fibrous, thread-like, wiry, stringy, ropy, capillary character that is never captured by the notions of levels, layers, territories, spheres, categories, structure, systems” (Latour 1996: 370). It is Rem Koolhaas’ fractal “generic city”, which “cannot be measured in dimensions” (Koolhaas 1995: 1251). With Derrida, the city of control cannot be Whole; with Baudrillard, it cannot be Real; and with Virilio, it cannot be There (see Koolhaas 1995: 967).

#### Timeframe based try or die calculations justify the invocation of speed as a political ontology, which destroys their ability to limit war powers.

Vivian 13. Bradford Vivian, Professor of Communication and Rhetorical Studies at Syracuse University, “Times of Violence,” Quarterly Journal of Speech Published online: 27 Mar 2013 pg. 1

The ways that authoritative institutions invoke and order time as a means of consolidating and expressing power often engender violence. Conflicting interpreta- tions of holy writ and spiritual obligation have incited bloody religious persecutions and armed conflicts for centuries. Slavoj Zizek contends that secular (not only religious) regimes justify radical police or military action by invoking apocalyptic senses of time: ‘‘Apocalyptic time is the time of the end of time, the time of emergency, of the state of exception when the end is nigh.’’2 States of exception in liberal-democratic nations are also times of exception: executive authorities exercise unprecedented forms of violence both within and without national borders by citing as justification allegedly temporary episodes of state emergency.3

#### The ballot is the choice of Edward Snowden—will your ballot imply complacency or using your situated position to build a network of popular insurrection?

Connolly 13. William Connolly, Krieger-Eisenhower professor of political science at Johns Hopkins, “‘The East’ and Corporate Terrorism,” The Contemporary Condition, July 7, 2013 <http://contemporarycondition.blogspot.com/2013/07/the-east-and-corporate-terrorism.html>, accessed September 4, 2013

Eventually Sarah develops a strategy of public expose and activism that draws some sustenance from her two identities and resists the traps each sets for her. I will let that part unfold when you watch the film. Is it enough?  Probably not. Could more of us participate in such acts to augment the potential they hold? Yes, we could. Many of us are what Michel Foucault called “specific intellectuals”, people with special knowledges and skills because of the work we do in law firms, medical practices, college teaching, blog writing, pharmaceutical companies, intelligence agencies, the media, school boards, churches, geological research, corporate regulatory agencies, and so on, endlessly. Each of us has specific modes of strategic information and critical skill linked to our role assignments. We can expose horrendous practices, as Snowden has done recently. We can also support others who do so as we seek to build a critical assemblage of public insurrection together.

#### this is a form of software violence that can SOLVE THE AFF by acting VIOLENTLY only against the sovereign’s ability itself to act violently on the web, leaking or hacking the USFG’s ability to use cyber operations

Cox and Knahl 11. Geoff Cox Researcher in Digital Aesthetics as part of the Digital Urban Living Research Center, Aarhus University (DK). He is also an occasional artist, and Associate Curator of Online Projects, Arnolfini, Bristol (UK), adjunct faculty, Transart Institute, Berlin/New York (DE/US), Associate Professor (Reader), University of Plymouth (UK), where he is part ofKURATOR/Art and Social Technologies Research group, and Martin Knahl, Lecturer at the University of Plymouth. He is a Research Fellow at the Centre for Information Security and Network Research, “NeMe: Critique of Software Violence,” <http://www.neme.org/1300/critique-of-software-security>, May 2011

In addition to ‘systemic violence’, there is symbolic violence embodied in language itself – not simply as an incitement to a violent action or in the ways that language reflects social domination (e.g. ‘man-made’ language) or heavy critique in general – but in the way that it produces meaning more fundamentally. For instance, in saying that ‘a fundamental violence exists in this “essencing” ability of language’ (2008: 58), Slavoj Zˇizˇek is making reference to Hegel’s observation that there is something inherently violent in the capacity of language to represent a thing – an act equivalent to its symbolic death. In the realm of software, programming languages are even more overtly violent – not simply representing a thing but enacting it. In other words, if source code says something and does something at the same time, it symbolises and enacts violence on the thing. It literally executes it.

In writing these words on a computer, violence and counter-violence is demonstrated in the choice of software and operating systems. Software development is limited through force. Violence is exerted against information that wants to be free. In what Angela Mitropoulos refers to as the ‘softwar’ (2007) proprietary software commits violence against users, all the time forcing users to pay and upgrade regularly when there are viable free alternatives. Mitropoulos is more specifically referring to the issue of intellectual property and related conflicts over sharing digital content, such as those over P2P file sharing. The perpetrator in this case breaks a number of basic principles inherent to digital media processes where files can be freely copied and shared, and furthermore legislates to normalise this contrary way of working. The moral ambiguities of software licenses and duplicities of the law are clear, and at the heart of all contractual agreements. To break a contract is to activate the threat of violence enforced by the law, whereas the greater violence has already been committed and gone unpunished. This is the basis for the piracy ethic, in stealing back what was already stolen in the first place.

On the relation between violence and social transformation, Benjamin refers to Georges Sorel’s essay ‘Reflections on Violence’ (1915) to expose the distinction between violence and force (1996: 245-6).[22](http://www.neme.org/1300/critique-of-software-security#fn22) Sorel points to the failure of parliamentary democracy to deliver its promises and to the principle of counterviolence, not only through strikes but through revolution. The point is that under certain conditions violence becomes force, as ‘pure means’.[23](http://www.neme.org/1300/critique-of-software-security#fn23) The consequences of the disruption of means and ends are political, as Agamben confirms: ‘Politics is the sphere neither of an end in itself nor of means subordinated to an end; rather, it is the sphere of a pure mediality without end intended as the field of human action and of human thought.’ (2000: 116)

In Benjamin’s ‘Critique of Violence’, the concept of pure means invokes the potential for ‘pure immediate violence’ – human action that neither makes nor preserves law, but is outside of the law. The idea of ‘pure violence’ does not apply to any violent action in itself, but in its relation to external conditions. The present is seized from the impure violence of history in what Benjamin describes as the ‘real state of emergency’ (Wohlfarth 2009: 14).[24](http://www.neme.org/1300/critique-of-software-security#fn24) The paradox of Benjamin’s position is in drawing together proletarian violence (informed by Marxism) with the theology of divine violence represented by Judaic Messianism – where redemption is provided by ‘pure divine violence’. So rather than promote terrorist violence, or as necessary means justified by ends, he calls for: ‘collective political action that is lethal not to human beings, but to the humanly created mythic powers that reign over them’ (Buck-Morss 2003: 33). The concept of pure, divine violence is a violence that appears to come from nowhere – from beyond the law – in which ‘killing is neither a crime nor a sacrifice’ according to programming languages are even more overtly violent – not simply representing a thing but enacting it. In other words, if source code says something and does something at the same time, it symbolises and enacts violence on the thing. It literally executes it.

With software, pure means opens up vulnerabilities in the system as a practice of creating insecurity. If no one will protect us from the violence of security, there is no option but to release ‘pure softwar’ – as resistance to the mythic powers that regulate our systems.

#### only the alternative can stop validating tools of cyber-securitization and use them against the elites who would dominate our ability to use the internet

Cox and Knahl 11. Geoff Cox Researcher in Digital Aesthetics as part of the Digital Urban Living Research Center, Aarhus University (DK). He is also an occasional artist, and Associate Curator of Online Projects, Arnolfini, Bristol (UK), adjunct faculty, Transart Institute, Berlin/New York (DE/US), Associate Professor (Reader), University of Plymouth (UK), where he is part ofKURATOR/Art and Social Technologies Research group, and Martin Knahl, Lecturer at the University of Plymouth. He is a Research Fellow at the Centre for Information Security and Network Research, “NeMe: Critique of Software Violence,” <http://www.neme.org/1300/critique-of-software-security>, May 2011

The background to this line of thinking draws upon Walter Benjamin’s 1921 essay ‘Critique of Violence’.[1](http://www.neme.org/1300/critique-of-software-security#fn1) For Benjamin, the issue is not whether violence is a means to a just or unjust end (a critique of ‘just ends’) but whether violence can be a moral means in itself. As he puts it, ‘a more exact criterion is needed, which would discriminate within the sphere of means themselves, without regard for the ends they serve’ (1996: 236).[2](http://www.neme.org/1300/critique-of-software-security#fn2) Rather than simply reconciling just ends by a justification of the means, or vice versa, the ‘Critique of Violence’ essay focuses on the realm of means, or more precisely: ‘the question of the justification of certain means that constitute violence’ as Benjamin puts it (1996: 237). As far as the State is concerned, violence exercised by individuals, or its legal subjects, is a threat to the legal system that serves to justify its own use of violence. Legal ends appear to be only achievable by legal power. The law uses violence for legal ends that the law itself has decided. For instance, and as an agent of State authority, police violence is legitimated as both law-making and law-preserving – and indeed all violence is a means of law-making and law-preserving according to Benjamin. This indicates the law’s ‘monopoly on violence’ as he puts it, in not simply preserving legal ends but more importantly in preserving the law itself. It also affirms the threat of actions that are outside of the law, to the law itself, and why they must be contained.

An exception to this is the right to strike, conceded by the State in recognition of the inevitability of antagonism in human societies. Yet to strike is an active refusal to work, the withdrawal of actions, a non-action, and is not necessarily violent. Where violence is more easily discernible is that the motivation to strike in the first place is to escape from the violence imposed on the worker by the employer. This position is in keeping with Trotsky, in his essay ‘Terrorism’ of 1911, who considers arguments against the use of violence to be a hypocrisy in that the entire state apparatus and its laws, police, and army are nothing but an apparatus for capitalist terror:

‘Our class enemies are in the habit of complaining about our terrorism. What they mean by this is rather unclear. They would like to label all the activities of the proletariat directed against the class enemy’s interests as terrorism. The strike, in their eyes, is the principal method of terrorism. The threat of a strike, the organisation of strike pickets, an economic boycott of a slave driving boss, a moral boycott of a traitor from our ranks – all this and much more they call terrorism. If terrorism is understood in this way as any action inspiring fear in, or doing harm to, the enemy – then of course the entire class struggle is nothing but terrorism.’ (1987)

The right to strike translates as the right to use a form of violence to attain certain ends, and the State reserves the right to counter this with violence.[3](http://www.neme.org/1300/critique-of-software-security#fn3) Trotsky points to the glaring paradox of a value system that argues for the ‘absolute value of human life’ and at the same time sacrifices millions of people in wars. On the one hand violence is seen to be inadmissible, and yet on the other, inexceptional circumstances it is seen to be necessary – in a ‘shift from the moral high ground to raw self-interest’ (Buck-Morss 2003:

Much the same paradox applies in the contemporary ‘war on terror’, as the state of emergency becomes the justification for the erosion of citizen’s rights and freedoms that were hard won. The duplicity is evident in the way those deemed a danger to national security can be taken into custody and detained in ways that erase individual human rights, turning them into a ‘noncitizen’ such that ‘bare life reaches its maximum indeterminacy’ (Agamben 2005: 4). The way the State suspends and withdraws its guarantee of protection and legal entitlement is a condition of contemporary power, and this is discussed in depth in Giorgio Agamben’s State of Exception (2005). Extending Carl Schmitt’s Politische Theologie of 1922 that established the contiguity between sovereignty and the state of exception, Agamben argues that the state of exception, although described as a provisional measure in exceptional circumstances, has become the working paradigm of modern government.[5](http://www.neme.org/1300/critique-of-software-security#fn5)Under this logic, State power uses violence against an identifiable enemy so that its use of power appears legitimate despite the active contradiction with its own legal and natural laws. When the required ends cannot be guaranteed by the legal system alone, the repressive state apparatus further intervenes ‘for security reasons’ (Benjamin 1996: 243). Security marks the exception, in other words.

Software Violence

Software running over networks is a manifestation of ideology, and connectivity remains a security threat beyond its purely technical functionality. This is what Alexander Galloway and Eugene Thacker, in The Exploit, describe as the new ‘network-network symmetry’ of power, in which control is distributed relatively autonomously in horizontal organisational locales and at the same time into rigid vertical hierarchies or directed commands (2007). This description is a socio-technical truism of course, and one that supports their claim that networks and sovereignty are not incompatible. Indeed together they are exceptional and are always related as ‘sovereignty-in-networks’. Correspondingly, the recommendation to those developing oppositional tactics is to take advantage of the vulnerabilities in networks by exploiting power differentials that exist in the system. This is precisely what software developers and malware (malicious software) authors have discovered, as they exploit vulnerable operating systems, internet service and security software.

To add detail here: Internet violence is propagated through various means such as the use of viruses, spam, click fraud, phishing, and ‘botnets’ (collections of software robots, or bots, that run autonomously).[6](http://www.neme.org/1300/critique-of-software-security#fn6)

#### And the aff’s legal approach only serves to normalize the state of exception – by creating a legal framework for the deployment of offensive cyberoperations, the affirmative legitimizes their ‘legal’ military use

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).

#### The 1ac is an exercise in post-panoptic power that thrives on its invisibility—they make the whole of cyberspace into a potential virtual camp as there can be no outside its liberal regulation

Diken and lausten 2k3(Bulent, Carsten “Zones of indistinction - security, terror, and bare life” <http://www.lancs.ac.uk/fass/sociology/papers/diken-laustsen-zones-of-indistinction.pdf>)

Control is digital, it translates everything into the logic of codes and passwords, and thus transgresses the duality of mass and individual. “Individuals become ‘dividuals,’ and masses become samples, data, markets, or ‘banks’” (Deleuze 1995: 180). Focusing on biosurveillance methods through access to tissues, fluids and images available from the body itself, control transforms “the body into a password” (Lyon 2001: 75). Post-panoptic power can interpellate the subject in absentia through electronic lists (see Poster 1996). Regulating a fluid and endlessly divisible, fractal, “multitude” rather than “peoples”, control produces a hybrid, metastable subjectivity that no longer corresponds to stable identities of the disciplinary society (Hardt & Negri 2000: 331-2). In this sense control brings with it an infinite intensification of discipline in a smooth space devoid of enclosures; control is discipline without walls, a mobile form of discipline that regulates humans and non-humans “on the move” (Lyon 2001: 63). Nomadism was once a critical tool against discipline, a “line of flight” out of the panopticon, but control society captures nomadic “war machines”, accommodating them for its own purposes (see Deleuze & Guattari 1987: 387). Moving from “exceptional discipline” to “generalized surveillance” (Foucault 1977: 209), control extends the logic of the camp. With intensified and direct biopolitical access to bare life, control “knows no outside” (Hardt & Negri 2000: 413). Its logic transgresses the binary logic of the inside/outside distinction for it is a “decentered and deterritorializing apparatus of rule” (Hardt & Negri 2000: xii). Modern discipline had played upon the distinction between inside and outside; post-modern control, in contrast, constitutes an “ou-topia”, a non-place (Hardt & Negri 2000: 190). When there is no outside left, the zone of indistinction opened up by the camp becomes the smooth space of control, a generalized space of indistinction. Which turns discipline itself into a simulacrum: in control society “prisons are there to hide that it is the social in its entirety, in its banal omnipresence, that is carceral” (Baudrillard 1994: 12). The city as a complex technological artifact illuminates the logic of control. Systems of control are urban phenomena; cities constitute nodal points in mobile societies of surveillance, and even cyberspaces are congested “around conventional urban areas” (Lyon 2001: 53-4). Yet this is misleading because the “conventional city” no longer exists. The contemporary city is no longer founded on the divide between its “intramural” population and the outside; “it no longer has anything to do with the classical oppositions of city/country nor centre/periphery” (Virilio 1997: 382, 390). The city of control is an immanent space, a reticular ou-topia, sharing with all other networks a “fibrous, thread-like, wiry, stringy, ropy, capillary character that is never captured by the notions of levels, layers, territories, spheres, categories, structure, systems” (Latour 1996: 370). It is Rem Koolhaas’ fractal “generic city”, which “cannot be measured in dimensions” (Koolhaas 1995: 1251). With Derrida, the city of control cannot be Whole; with Baudrillard, it cannot be Real; and with Virilio, it cannot be There (see Koolhaas 1995: 967).

#### Timeframe based try or die calculations justify the invocation of speed as a political ontology, which destroys their ability to limit war powers.

Vivian 13. Bradford Vivian, Professor of Communication and Rhetorical Studies at Syracuse University, “Times of Violence,” Quarterly Journal of Speech Published online: 27 Mar 2013 pg. 1

The ways that authoritative institutions invoke and order time as a means of consolidating and expressing power often engender violence. Conflicting interpreta- tions of holy writ and spiritual obligation have incited bloody religious persecutions and armed conflicts for centuries. Slavoj Zizek contends that secular (not only religious) regimes justify radical police or military action by invoking apocalyptic senses of time: ‘‘Apocalyptic time is the time of the end of time, the time of emergency, of the state of exception when the end is nigh.’’2 States of exception in liberal-democratic nations are also times of exception: executive authorities exercise unprecedented forms of violence both within and without national borders by citing as justification allegedly temporary episodes of state emergency.3

#### The ballot is the choice of Edward Snowden—will your ballot imply complacency or using your situated position to build a network of popular insurrection?

Connolly 13. William Connolly, Krieger-Eisenhower professor of political science at Johns Hopkins, “‘The East’ and Corporate Terrorism,” The Contemporary Condition, July 7, 2013 <http://contemporarycondition.blogspot.com/2013/07/the-east-and-corporate-terrorism.html>, accessed September 4, 2013

Eventually Sarah develops a strategy of public expose and activism that draws some sustenance from her two identities and resists the traps each sets for her. I will let that part unfold when you watch the film. Is it enough?  Probably not. Could more of us participate in such acts to augment the potential they hold? Yes, we could. Many of us are what Michel Foucault called “specific intellectuals”, people with special knowledges and skills because of the work we do in law firms, medical practices, college teaching, blog writing, pharmaceutical companies, intelligence agencies, the media, school boards, churches, geological research, corporate regulatory agencies, and so on, endlessly. Each of us has specific modes of strategic information and critical skill linked to our role assignments. We can expose horrendous practices, as Snowden has done recently. We can also support others who do so as we seek to build a critical assemblage of public insurrection together.

## 1NR

### apocalypse meow

#### recognizing and resolving this is an ethical priority and only the alt solves the aff—star this card

**Swyngedouw 13**—Professor of Geography at the University of Manchester

(Erik, “Apocalypse Now! Fear and Doomsday Pleasures”, Capitalism Nature Socialism, 24:1, 9-18, dml)

Against this cynical stand, the third, and for me proper, leftist response to the apocalyptic imaginary is twofold and cuts through the deadlock embodied by the first two responses. To begin with, the revelatory promise of the apocalyptic narrative **has to be fully rejected**. In the face of the cataclysmic imaginaries **mobilized to assure that the apocalypse will NOT happen** (if the right techno-managerial actions are taken), the only reasonable response is ‘‘Don’t worry (Al Gore, Prince Charles, many environmental activists . . ..), you are really right, **the environmental apocalypse** WILL not only happen, it has already happened**,** IT IS ALREADY HERE**.**’’ **Many are** already living **in the post-apocalyptic interstices of life,** whereby the fusion of environmental transformation and social conditions, render life ‘‘bare.’’ The fact that the socio-environmental imbroglio has already passed the point of no return has to be fully asserted. The socio-environmental Armageddon is already here for many; it is not some distant dystopian promise mobilized to trigger response today. Water conflicts, struggles for food, environmental refugees, etc. testify to the socio-ecological predicament that choreographs everyday life for the majority of the world’s population. Things are already too late; they have always already been too late. There is no Arcadian place, time, or environment to return to, no benign socio-ecological past that needs to be maintained or stabilized. Many already live in the interstices of the apocalypse, albeit a combined and uneven one. **It is only within** **the realization of** the apocalyptic reality of the now **that a new politics might emerge**. The second gesture of a proper leftist response is to **reverse the order between** the universal **and** the particular that today dominates the catastrophic political imaginary. This order maintains that salvaging the particular historical-geographical configuration we are in depends on re-thinking and re-framing the humanenvironment articulation in a universal sense. We have to change our relationship with nature so that capitalism can continue somehow. Not only does this argument to preserve capitalism **guarantee the prolongation of the combined and uneven apocalypse of the present**, it forecloses considering fundamental change **to the actually existing unequal forms** of organizing the society-environment relations. Indeed, the apocalyptic imaginary is one that generally still holds on to a dualistic view of nature and culture. The argument is built on the view that humans have perturbed the ecological dynamic balance in ways inimical to human (and possibly non-human) long-term survival, and the solution consists broadly in bringing humans (in a universal sense) back in line with the possibilities and constraints imposed by ecological limits and dynamics. A universal transformation is required in order to maintain the present. And this can and should be done through managing the present particular configuration. This is the message of Al Gore or Prince Charles and many other environmental pundits. A left socio-environmental perspective has to insist that we need to transform this universal message into a particular one. The historically and geographically specific dynamics of capitalism have banned an external nature radically to a sphere beyond earth. On earth, there is no external nature left. It is from this particular historical-geographical configuration that **a radical politics of transformation has to be** thought **and** practiced. Only through thetransformation of the particular socio-ecological relations of capitalism can a generic egalitarian, free, and common re-ordering of the human/non-human imbroglios be forged. Those who already recognized the irreversible dynamics of the socio-environmental imbroglio that has been forged over the past few centuries coined a new term to classify the epoch we are in. ‘‘Welcome to the Anthropocene’’ became a popular catch-phrase to inform us that we are now in a new geological era, one in which humans are co-producers of the deep geological time that hitherto had slowly grinded away irrespective of humans’ dabbling with the surface layers of earth, oceans, and atmosphere. Noble prize-winning chemist Paul Crutzen introduced ‘‘the Anthropocene,’’ coined about a decade ago as the successor name of the Holocene, the relatively benign geo-climatic period that allegedly permitted agriculture to flourish, cities to be formed, and humans to thrive (Crutzen and Stoermer 2000). Since the beginning of industrialization, so the Anthropocenic argument goes, humans’ increasing interactions with their physical conditions of existence have resulted in a qualitative shift in geo-climatic acting of the earth system. The Anthropocene is nothing else than the geological name for capitalism WITH nature. Acidification of oceans, biodiversity transformations, gene displacements and recombinations, climate change, big infrastructures effecting the earth’s geodetic dynamics, among others, resulted in knotting together ‘‘natural’’ and ‘‘social’’ processes such that humans have become active agents in co-shaping earth’s deep geological time. Now that the era has been named as the Anthropocene, we can argue at length over its meaning, content, existence, and possible modes of engagement. Nonetheless, it affirms that humans and nature are co-produced and that the particular historical epoch that goes under the name of capitalism forged this mutual determination. The Anthropocene is just another name for insisting on Nature’s death. This cannot be unmade, however hard we try. The past is forever closed and the future\* including nature’s future\*is radically open, up for grabs. Indeed, the affirmation of the historical-geographical co-production of society WITH nature radically politicizes nature, makes nature enter into the domain of contested socio-physical relations and assemblages. **We cannot escape ‘‘producing nature’’**; rather, it forces us to make choices about what socio-natural worlds we wish to inhabit. It is from this particular position, therefore, that the environmental conundrum ought to be approached so that a qualitative **transformation of BOTH society AND nature has to be envisaged**. This perspective moves the gaze from thinking through a ‘‘politics of the environment’’ to ‘‘politicizing the environment’’ (Swyngedouw 2011; 2012). The human world is now an active agent in shaping the non-human world. This extends the terrain of the political to domains hitherto left to the mechanics of nature. The non-human world becomes ‘‘enrolled’’ in a process of politicization. **And that is precisely what needs to be** fully endorsed. The Anthropocene opens up a terrain whereby different natures can be contemplated and actually co-produced. And the struggle over these trajectories and, from a leftist perspective, the process of the egalitarian socio-ecological production of the commons of life is precisely what our politics are all about. **Yes, the apocalypse is** already here**, but do not despair,** **let us fully endorse the** emancipatory possibilities **of apocalyptic life**. Perhaps we should modify the now over-worked statement of the Italian Marxist Amadeo Bordiga that ‘‘if the ship goes down, the first-class passengers drown too.’’ Amadeo was plainly wrong. Remember the movie Titanic (as well as the real catastrophe). A large number of the first-class passengers found a lifeboat; the others were trapped in the belly of the beast. Indeed the social and ecological catastrophe we are already in is not shared equally. While the elites fear both economic and ecological collapse, the consequences and implications are highly uneven. The elite’s fears are indeed only matched by the actually existing socio-ecological and economic catastrophes many already live in. The apocalypse is combined and uneven. **And it is within this reality that** political choices have to be made andsides taken**.**