# Cybernetics K Supplement—Wave 1—FMPS

### Notes

Thanks to Ansel Ang-Olson, Arthur Guo, Cleo Shaw, Esther Liu, George Jabren, and Rajan Sandhu for doing fantastic work!

This file is intended to supplement the starter packet cybernetics K and includes very few of the cards from that file. Here’s a brief rundown of how this file is organized:

**Topshelf:** New links and impacts, different potential alternatives, new framework angles/pieces of offense

**Blocks:** Supplements to the blocks from the original file; if a block has the same name as one from the original file, then the cards in it are simply alternatives, not necessarily replacements

**Answers:** More answers; largely organized in the aff context, but (like the aff section of the original file) also useful for neg cards against cybernetics affs, like the one in this file

**Bronze Night Aff:** A cybernetics aff! See the notes section there for more. There is not a separate neg section; a framework file is being released separately, and there are plenty of substantive answers to the aff between the answers section in this file and the starter packet file. Additionally, more material that can be used on the neg against this aff (and other K affs) will be coming from our lab in wave 2!

## Topshelf

### Link—AI—Autonomous Weapons

#### The 1AC doesn’t “escape” the violence autonomous weapons, but rather ignores that the human machine is already an automated entity – try or die for the alt

Matviyenko 15 (Svitlana Matviyenko, University of Western Ontario, “LACAN’S CYBERNETICS”A thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy The School of Graduate and Postdoctoral Studies The University of Western Ontario London, Ontario, Canada) //ansel

\*edited for gendered language

The use of “automaton” in reference to man can be traced to the work of William Cornwallis: in his Essayes of Certaine Paradoxes (1616), he compares human performance to the functioning of man-made mechanisms. “In the whole course and frame of Nature, we see that nothing is made for it selfe,” he writes and explains, “the sunne by his splendor to lighten all the world; by his warmth and heate, to cherish and comfort each livuing and vegetable thing” (G2). In such an interconnected universe of things, Cornwallis conceives the body as both attached to its surroundings and, at the same time, an autonomous system, an assemblage of interrelated parts linked by the invisible “bond of duty, of use or of service, by which it is indebted to other”: the foot to the eye, the hand to the foot, the mouth to the hand, the stomach to the mouth, the whole body to the stomach; the human beings to their dogs and to their oxen (G2-G3). “Let [~~man~~] but looke into himself,” Cornwallis wrote, “and see how his constitutiue parts are debters each to other, the soule doth quicken and giue life to the body, the body like an Automaton, doth moue and carry it selfe and the soule” (G3). Cornwallis’ depiction of the mechanism of the body as an automaton does not presume, however, that its attachment to the environment makes it what we call today an open system. Rather, it remains a system closed-on-itself, that functions independently of will, man’s conscious control, or any outside direction. In the French context, a similar intuition was expressed by Pascal, who used “automate” for “man that acts as a machine” in his posthumously published Thoughts in 1669. In this book, Pascal continued his earlier exploration of the idea of **the natural order as “a homogeneous and autonomous whole, governed by laws, agreeing with a certain model, which derives its independence from one or more other orders**,” which he identifies in Thoughts as the order of the body, the order of the mind or reason, and the order of the heart or of charity (#308, #933).

Is there any “attachment” or “connection” between an automaton and the environment? This issue was articulated by the seventeenth-century philosophers in terms or “agreement” or “correlation” between the “orders.” We can still say that, for Cornwallis, 71 the cause of automation was located both inside and outside the automated living or nonliving entity, but only in the sense that **automation** **was seen as the effect of a higher law acting upon the automated entity from the outside,** which was the same as the inner law operating within an automated entity. **Modern science’s response** to the questions raised about the relation between these orders or **systems is to “mathematicalize**” (Milner) the correspondence. The process that Lacan and, later, Jacques-Alain Miller identify as “suturing,” emerges as a mathematical technique for demonstrating the presence of determinism or, as Lacan speaks about it, a law without intention (Seminar II 295), that was supposed to ground man’s relation to the “new” world system of correlated, autonomous, and automated orders. The subject of science emerges not in the rupture between these automated inner and outer universes, but as this rupture, which, as Slavoj Žižek has noted, “involves no lived experience, consciousness, or any other predicates we usually associate with subjectivity” (597).

Let us consider Jean-Claude Milner’s summary of one of Alexandre Koyré’s theorems of modern science found at the basis of Lacan’s theory of science: M**odern science holds that there is no boundary limiting its material domain**. It supposes two things: (**a) there exists nothing material that modern science cannot treat as one of its objects** (in other words, the set of existent material objects, usually called a universe, is in principle coextensive with the set of objects of modern science); (b) **both sets are mathematically infinite** (hence the notion of the modern infinite universe as opposed to the closed world of Antiquity). (“Lacan and the Ideal of Science” 29) In other words, he argues that “**a particular expression, a particular thought are modern only insofar as they belong to a system of thought in which a mathematized empirical science is possible**” (Milner, “Lacan and the Ideal of Science” 29). This allows modern science to challenge the Euclidian conception of “space” and to articulate a theory of “place,” or analysis situs, to use the archaic name for topology, which began in the work of Leibniz. Before Leibniz, the question of space was approached by René Descartes, who already thought of it only in connection to the extended body, res extensa, or “corporeal substance,” one of the three substances of Cartesian ontology. According to Descartes, matter extends in length, breadth, or depth and it is precisely this property of matter that constitutes space: space only exists as a consequence of such extension. In his correspondence with English philosopher Henry More48 from the 1640s, Descartes agreed with him that “in the natural course of events there is no vacuum,” but he also noted that there was what could not be perceived, and reserved the full knowledge of the invisible part of the extended body for God. Despite his awareness of the divisibility of matter, Descartes posited the extended body as existing beyond the perception of man: “a body can retain its whole bodily nature without being soft or hard or cold or hot to the senses – indeed without having any perceptible quality,” he wrote; “**all matter is completely imperceptible if it is divided into parts much smaller than the particles of our nerves and the individual parts are given a sufficiently rapid movement,**” which, he noted further in the letter to More, “is in a manner circular” (Descartes, III 360, 363). Descartes’ theory of automation, however, was different from his conception of the machinic body When Descartes approached this topic in the 1640s, he offered a mechanistic conception of the body49 that, he believed, physiologically functioned in the same way for both Homo sapiens and animals, except that the latter were lacking in “thinking substance.” He conceived the movements of animals as “purely mechanical and corporeal,” depending “solely on the force of the spirits and the structure of … organs” that “can be called the corporeal soul” (III 365).50 For Descartes, animals were thus “natural automata”: …it is certain that in the bodies of animals, as in ours, there are bones, nerves, muscles, animal spirits and other organs so arranged that they can by themselves, without any thought, give rise to all the movements we observe in animals. This is very clear in convulsions, when the mechanism of the body moves despite the mind, and often moves more violently and in a more varied manner than usually happens when it is moved by the will. (Descartes, III 366) Even though human bodies could, when they were not guided by thought or their “incorporeal soul,” exhibit such behaviour, men were not automata, but machines or mechanisms. When he said, “God made our body like a machine, and he wanted it to function like a universal instrument, which would always operate in the same way in accordance with its own laws” (Descartes, V 163-164), he was not referring to human automatism, but the machinic organization of the body. As Dennis Des Chene has argued in Spirits and Clocks, the novelty of Descartes’ theory was in combining …the animal-machine with a new philosophy of nature, in which the actions of agents inferior to humans not only might but must be explained without reference to any “form” but extension or to any qualities but the modes of extension. Descartes had the formidable task of showing that the vegetative and sensitive powers of plants and animals are nothing other than the actions they exhibit by virtue of the “disposition” of their parts. (13) Thus, automata, for Descartes, were self-contained machines, closed systems; and as such, they could not be human. The openness and connectedness of the human-machine to the world was maintained by means of the non-physical res cogitans, the mental substance. By denying automata the capacity for mental functioning, he made a distinction between automation of the self-moving life or non-life forms and intelligence, an attitude which would dominate until the mid-to-late nineteenth century. At the same time, as Lorraine Daston reminds us, seventeenth- and eighteenth-century usage of the term “intelligence” …overlaps but does not coincide with its twentieth-century meaning. Both denote mental agility, particularly in problem solving and learning; but whether intelligence was inborn or acquired by education, unitary or multiple in its faculties, the property of individuals or of groups, these were oppositions which would not have been easily accommodated within the Enlightenment framework for understanding the mind. (191) Therefore, calculating machines, for example, would not qualify as “intelligent.” On the contrary, due to their automatic, or algorithmic, behavior, they were seen as the opposite of anything intelligent. The fascination with automata over the course of the eighteenth century and the beginning of the nineteenth was the fascination with the “non-intelligent” behaviour of “dummies,” especially when these human-like and other automata demonstrated their sometimes uncanny proximity to human performance.

#### A “bloodless” war between machines is impossible – the technological nature of LAWS guarantees alternatives that target non-military objectives

**Wilson 20** (Neil Wilson, Master’s at Utrecht University, “Understanding the Battle for AI in Warfare through the Practices of Assemblage: A Case Study of Project Maven”, Utrecht University, 8/2/20, <https://studenttheses.uu.nl/bitstream/handle/20.500.12932/37392/Neil%20Wilson%20MA%20Thesis%20%281%29.pdf?sequence=1&isAllowed=y>) // EL

2.1. Lethal Autonomous Weapons Systems and AI in Warfare Debate relating to Lethal Autonomous Weapons Systems (LAWS) is a mile wide but an inch deep - vast but as-yet unsubstantiated. Ample discussion surrounds the potential political, legal and moral repercussions of deploying LAWS but there is little theoretically-informed analysis of their development. Given the revolutionary potential of such technologies, there is an urgent need to rectify this imbalance. Political challenges posed by the deployment of LAWS on battlefields are numerous. Unlike nuclear weapons, LAWS would require no hard-to-obtain materials and be relatively cheap to develop, leading some to fear a global robot arms race. Even those contending that “arms race” framing risks escalating rivalries nevertheless agree on the need to manage the proliferation of these technologies. In particular, the risk of LAWS proliferating among non-state actors seeking to “level the playing field” is severe. Even among democratic states, LAWS would overcome the “bodybag” problem and thus lower the threshold for going to war. In such a scenario, however, the obvious attraction of using LAWS - a ‘bloodless’ war between machines - is misguided. A change of footsoldiers does not alter the fundamental objective of war: “imposing and enduring costs to reveal relative capability or resolve.” In the absence of human soldiers to impose costs upon, belligerents may seek alternative means to demonstrate their resolve, e.g. by targeting non-military objectives and civilians. Indeed, as drones have enabled the removal of soldiers from battlefields, the inability for enemies to directly reciprocate violence has instigated fears of “blowback” by other means. Political concerns aside, the legal questions raised by LAWS are momentous. Formal and informal rules have guided conduct in warfare for as long as it has been carried out. Over time, International Humanitarian Law (IHL) has steadily evolved to keep up with the development of new methods of warfighting, as evidenced by bans on the use of Chemical and Biological Weapons, anti-personnel landmines and blinding laser weapons. Throughout history, however, IHL has been developed under the assumption that human intelligence is guiding conduct in combat, not artificial. As existing treaties make no reference to LAWS, it is unclear if they can be banned under the current legal framework. Nevertheless, because it is impossible to confidently predict the outcomes of commands on complex AI systems, there is a possibility of LAWS running afoul of IHL. Can a robot be entrusted with the ability to discriminate between legitimate targets and civilians? If it fails, who can be held accountable? Some fear LAWS subverting the Hague Convention if they can act autonomously but not assume responsibility for the consequences. The ethics of using LAWS are fraught. At first glance, there is obvious appeal in using robots to do the “dull, dirty and dangerous” work in war as in civilian life. A robot never gets tired, stressed or traumatised. Their dispassionate nature, immune to the intoxicating effects of adrenaline, may even reduce the risk of civilian harm in conflict. From this perspective, if LAWS lessens the danger to soldiers and civilians alike, some suggest utilising them is not only judicious but an ethical imperative. Even if LAWs could perfectly adhere to IHL and reduce harm to both combatants and civilians, many question whether they should. As a simple matter of dignity, some insist that taking a human life should involve a human decision. “Delegating the decision to kill to algorithms,” according to Rosert and Sauer, “is inhumane and unacceptable under any circumstances.” A compelling argument, but potentially relativised by the fact that there are many different interpretations of human dignity and many ways it can be violated - technological or otherwise. The political, ethical and legal concerns raised are troubling but overwhelmingly speculative. Are we jumping the (autonomous) gun? Such preoccupation with the future use of killer robots may obscure meaningful debate about their present day development. A few notable contributions from Lewis, Taylor and Verbruggen are to be commended for grappling with the development of these systems, but this remains an under-theorised field. Presumably owing to its novelty, Project Maven has thus far evaded serious academic scrutiny. One notable exception comes from Suchman, however it nevertheless engages primarily with the deployment rather than development of this technology. Common to these conjectural, dystopian perspectives on the future of warfare is the assumption that if LAWS technology exists, it will be used. Not a dramatic leap of faith but nevertheless it seems prudent to question what is driving the demand for these technologies in this domain; thereby drawing the line between where we stand and where some fear we are heading. LAWS will only be deployed, presumably, if there is some strategic, operational and/or tactical need for them. Understanding this will elucidate a fuller picture of why and how they are being developed. To satisfy this curiosity, we turn to the growing field of scholarship on remote warfare.

### Link—AI—Ethics

#### The aff’s search for ethics ignores the way algorithms inevitably shape our assumptions and forward technological manipulation

**Amoore 20** (Louise Amoore, Professor of Political Geography at Durham University, “Cloud Ethics: Algorithms and the Attributes of Ourselves and Others”, *Duke University Press*, 8/30/20, <https://doi.org/10.1080/1369118X.2020.1800782>) // EL

Ethics of Algorithms At first sight, the potential for violent harm precipitated by algorithms that learn to recognize human propensities appears to be a self-evident matter for critique. Surely, one could say, the ethical terrain of the algorithm resides in the broader political landscape of rights and wrongs, good and evil. After all, one could readily identify a set of rights, already apparently registered as belonging to rights-bearing subjects, that has been contravened by algorithms that generate targets, adjudicating which people may peaceably assemble, or which people are worthy of credit or employment, and on what terms. Indeed, on this terrain of delineating the rights and wrongs of algorithmic actions is precisely where many critical voices on the harms of the algorithm have been heard. Writing in the New York Times, for example, Kate Crawford identifies machine learning’s “white guy problem,” arguing that “we need to be vigilant about how we design and train machine learning systems.”10 The dominant critical perspectives on algorithmic decisions have thus argued for removing the “bias” or the “value judgements” of the algorithm, and for regulating harmful and damaging mathematical models.11 Within each of these critical calls, the ethical problem is thought to dwell in the opacity of the algorithm and in its inscrutability, so that what Frank Pasquale has called the “black box society” is addressed through remedies of transparency and accountability.12 In sum, the rise of algorithmic power in society has been overwhelmingly understood as a problem of opaque and illegible algorithms infringing or undercutting a precisely legible world of rights belonging to human subjects. In such a framing, there is an outside to the algorithm—an accountable human subject who is the locus of responsibility, the source of a code of conduct with which algorithms must comply. To call for the opening of the black box, for transparency and accountability, then, is to seek to institute arrangements that are good, ethical, and normal, and to prevent the transgression of societal norms by the algorithm. Yet, when people gathered to protest on Baltimore streets, or when Facebook users’ data fueled the political and commercial models of Cambridge Analytica (figure I.3), legible rights to peaceable assembly or to electoral due process were not violated primarily by illegible algorithms. Rather, the means by which people could appear in a political forum, the conditions of their appearance, and the capacities they had to make a recognizable political claim in the world were subject to algorithmic regimes of what Michel Foucault calls truth telling and wrongdoing.13 In short, what matters is not primarily the identification and regulation of algorithmic wrongs, but more significantly how algorithms are implicated in new regimes of verification, new forms of identifying a wrong or of truth telling in the world. Understood in these terms, the algorithm already presents itself as an ethicopolitical arrangement of values, assumptions, and propositions about the world. One does not need to look beyond the algorithm for an outside that is properly political and recognizably of ethics. Indeed, there can be no legible human outside the algorithm and underwriting its conduct, for as John Cheney-Lippold reminds us, we are enmeshed in the data that produce each “freshly minted algorithmic truth.”14 One cannot sustain a search for codes of ethics that instill the good, the lawful, or the normal into the algorithm. Contemporary algorithms are not so much transgressing settled societal norms as establishing new patterns of good and bad, new thresholds of normality and abnormality, against which actions are calibrated. Actions one might consider harmful, as William Connolly notes, are not merely “actions by immoral agents who freely transgress the moral law” but are “arbitrary cruelty installed in regular institutional arrangements taken to embody the Law, the Good, and the Normal.”15 Amid the widespread search for new ethical arrangements for the scrutiny and regulation of algorithms, what becomes of the arbitrary harms lodged within embodied algorithmic arrangements? One could imagine a world in which the deep neural networks used in cities like Baltimore are scrutinized and rendered compliant with rules and yet continue to learn to recognize and misrecognize people and to infer intent, to generate rules from the contingent and arbitrary data of many past moments of associative life on the city streets, to refine and edit the code for future uses in unknown future places. I may feel that some notion of legible rights is protected, and yet the attributes generated from my data, in correlation with yours and others’, continue to supply the conditions for future arbitrary actions against unknown others. I draw a distinction here between ethics as code, or what Michel Foucault describes as “the code that determines which acts are permitted or forbidden,” and ethics as the inescapably political formation of the relation of oneself to oneself and to others.16 My argument is that there is a need for a certain kind of ethical practice in relation to algorithms, one that does not merely locate the permissions and prohibitions of their use. This different kind of ethical practice begins from the algorithm as always already an ethicopolitical entity by virtue of being immanently formed through the relational attributes of selves and others. My desire for a different mode of critique and ethical account is animated not by the question, How ought the algorithm be arranged for a good society?, but by the question, How are algorithmic arrangements generating ideas of goodness, transgression, and what society ought to be?

#### Algorithms can never be ethical – attempts fail to account for the relations in which they first emerged

**Amoore 20** (Louise Amoore, Professor of Political Geography at Durham University, “Cloud Ethics: Algorithms and the Attributes of Ourselves and Others”, Duke University Press, 8/30/20, <https://doi.org/10.1080/1369118X.2020.1800782>) // EL

A cloud ethics acknowledges that algorithms contain, within their spatial arrangements, multiple potentials for cruelties, surprises, violences, joys, distillations of racism and prejudice, injustices, probabilities, discrimination, and chance. Indeed, many of the features that some would like to excise from the algorithm—bias, assumptions, weights—are routes into opening up their politics. Algorithms come to act in the world precisely in and through the relations of selves to selves, and selves to others, as these relations are manifest in the clusters and attributes of data. To learn from relations of selves and others, the algorithm must already be replete with values, thresholds, assumptions, probability weightings, and bias. In a real sense, an algorithm must necessarily discriminate to have any traction in the world. The very essence of algorithms is that they afford greater degrees of recognition and value to some features of a scene than they do to others. In so doing, algorithms generate themselves as ethicopolitical beings in the world. If to have ethics is not merely to have a code prohibiting, for example, bias or assumptions, but to work on oneself via relations, then the ethicopolitics of algorithms involves investigations of how they learn to recognize and to act, how they extract assumptions from data relations, and how they learn what ought to be from relations with other humans and algorithms. To be clear, the cloud ethics I propose here does not belong to an episteme of accountability, transparency, and legibility, but on the contrary begins with the opacity, partiality, and illegibility of all forms of giving an account, human and algorithmic. To advance a cloud ethics is to engage the ungrounded politics of all forms of ethical relations. The significant new ethical challenges that algorithms seem to present to society actually manifest novel features of some profoundly old problems of the grounds for ethical action. As Judith Butler explains in her Spinoza lectures, the demand to give an account of oneself will always fall short, for “I cannot give an account of myself without accounting for the conditions under which I emerge.”19 If one assumes that the determination of an unequivocal I who acts is a necessary precondition of ethics, as Butler cautions, then this identifiable self is “dispossessed” by the condition of its emergence in relation to others. For Butler, this persistent failure to give a clear-sighted account does not mark the limit point of ethics. On the contrary, the opaque and unknowable nature of making all kinds of acting subjects is the condition of possibility of having an ethicopolitical life.20 In short, and in contrast to the equation of ethics with transparency and disclosure, ethical responsibility is sustained by conditions of partiality and opacity. My notion of a cloud ethics extends the opacity of the human subject, envisaging a plurality of venues for ethical responsibility in which all selves—human and algorithmic—proceed from their illegibility. The apparent opacity and illegibility of the algorithm should not pose an entirely new problem for human ethics, for the difficulty of locating clear-sighted action was already present. The I who forms the ethical relation was always in question and is now, with algorithms, in question in new ways. Though the mathematical propositions of algorithms cannot be made fully legible, or rendered accountable, they can be called to give accounts of the conditions of their emergence. These conditions include some relations that are identifiably between humans and algorithms—such as the selection and labeling of training data, the setting of target outputs, or the editing of code “in the wild,” for example—but others still are relations of algorithms to another algorithm, such as a classifier supplying the training data from which a neural network will learn. In all such instances of iterative learning, the significant point is that the conditions of an algorithm’s emergence—a composite of human-algorithm relations—are venues for ethicopolitics.

### Link—AI—Perception/Targeting

#### Algorithms’ superior abilities of “perception” creates rash reactionary politics

**Amoore 20** (Louise Amoore, Professor of Political Geography at Durham University, “Cloud Ethics: Algorithms and the Attributes of Ourselves and Others”, Duke University Press, 8/30/20, <https://doi.org/10.1080/1369118X.2020.1800782>) // EL

Critical accounts of the rise of algorithms have placed great emphasis on the power of algorithms to visualize, to reprogram vision, or indeed even to “see” that which is not otherwise available to human regimes of visuality. Similar to the spatial arrangement, this primacy of the visual register has also annexed what could count as the ethics and politics of algorithms. There are two curiously twinned accounts of contemporary algorithms in relation to regimes of sight and vision. The first is that algorithms operate on a plane in excess of human visibility and at scales that are inscrutable to the human. The second is that algorithms themselves have an enhanced capacity to visualize the invisible, to see, scan, and search volumes and varieties of data heretofore unavailable to human senses. Indeed, this intersection of machinic and human vision comes to the fore in the espoused ethics of public inquiries into the state’s deployment of automated algorithms for the government of the population. For example, in the UK parliamentary inquiry following the Edward Snowden disclosures of widespread automated data analysis, a peculiar kind of virtue was found in the notion that, in machine learning intelligence, “only a tiny fraction of those collected are ever seen by human eyes.” Similarly in the United States, the former director of national intelligence James Clapper likened the nsa’s algorithmic analysis of citizens’ data to a form of library in which few books are “actually read” and where the output of the system supplies “the books that we need to open up and actually read.” There is an acute problem, then, with the widespread appeal to ethical codes that regulate what algorithms or humans do or do not see. It is a problem, I suggest, with its roots in the privileging of sight and vision over other forms of making things perceptible. “Vision cannot be taken,” writes Orit Halpern in her wonderful book Beautiful Data, “as an isolated form of perception” but must be considered “inseparable from other senses.” To act and to be responsible for action, an algorithm need not “see” or “read” but need only make something or someone perceptible and available to the senses. In this book I situate the ethics and politics of algorithms within a genealogy of technologies of perception. Contemporary algorithms are changing the processes by which people and things are rendered perceptible and brought to attention. This is definitively not merely a matter of making things amenable to vision and indeed is frequently a matter of sustaining something beneath the visual register and yet perceptible. As art historian Jonathan Crary writes, “Ideas about perception and attention were transformed” alongside the historical “emergence of new technological forms of spectacle, display, projection, attention, and recording.” Understood in this way, the transformation of perception involves changes in how the perceiving subject thinks about what could be brought to attention, changes in the horizon of possibility of human action. As with the advent of the technologies of printing press, camera, or cinema, so the advent of the machine learning algorithm implies a reworking of what it means to perceive and mediate things in the world. This is not a process that is effectively captured by the idea that automated systems are undermining or superseding human forms of perception and action. To foreground instruments of perception, or what Henri Bergson terms “organs of perception,” is to breach conventional distinctions between humans and machines and acknowledge the entangled nature of all forms of perception. Bergson insists on the shared limits of perception across science and ordinary everyday experience, so that “ordinary knowledge is forced, like scientific knowledge,” to divide up time into perceptible slices, to “take things in a time broken up into particles.” Whether the organ of perception is microscope, telescope, eye, camera, or algorithm, perception is attuned to action, to the dividing up of movement into points on a trajectory so that they can be acted on. “What you have to explain,” he writes, is not “how perception arises, but how it is limited, since it should be the image of the whole, and is in fact reduced to the image of that which interests you.” Following Bergson’s insight on how an organ of perception seizes the object of interest from its environment, to consider algorithms as instruments of perception is to appreciate the processes of feature extraction, reduction, and condensation through which algorithms generate what is of interest in the data environment. Confronted by something of a moral panic surrounding the expansive volumes of “big data” and powers of surveillance of automated systems, my emphasis on practices of perception foregrounds precisely the opposing process: the reducing, distilling, and condensing of particles of interest from a whole. A defining ethical problem of the algorithm concerns not primarily the power to see, to collect, or to survey a vast data landscape, but the power to perceive and distill something for action. Algorithms function with something like an aperture—an opening that is simultaneously a narrowing, a closure, and an opening onto a scene. Let us consider, for example, an algorithm designer working in the UK defense sector, demonstrating the capacity of his deep neural network algorithms to recognize a mistaken civilian target amid a crowded data environment of drone images. He shows a slice through time as a vehicle travels away from the center of Kandahar, Afghanistan. He explains the problem for the decision: that this could be a suspect vehicle or, crucially, a school bus taking children home to villages outside the city. The algorithms had learned to recognize a school bus through training data that supplied images of predominantly yellow US-style buses. The designer explains that his algorithm is aggregated with many others to generate a single actionable output— target/no target—but to do this he must necessarily reduce and condense the patterns of interest from a volume of input data. The training data—and the humans who labeled it—have conditioned the cnn algorithm to carve out and value some objects and to discard others. In this part of Afghanistan, some of the school buses are indeed in the spatial form of a US-style school bus, but others still are open-back trucks repurposed for transporting scholars. My point is that a potential act of violence, such as a school bus wrongfully targeted by a drone strike, resides not primarily in the vertical surveilling and collecting of data, but in fact in the horizontal arraying of possible patterns of interest lodged within the algorithm itself. As an aperture instrument, the algorithm’s orientation to action has discarded much of the material to which it has been exposed. At the point of the aperture, the vast multiplicity of video data is narrowed to produce a single output on the object. Within this data material resides the capacity for the algorithm to recognize, or to fail to recognize, something or someone as a target of interest. The ethical stakes of what Mark Hansen calls “potential perceptual reconfiguration” applied to my cloud ethics necessarily involves something like a reopening of the process of the algorithm’s reduction of a multiplicity to one. What is happening in this process of condensing plural possible pathways to a single output? When an algorithm determines whether a vehicle is a military or a civilian target, or when it decides if a public protest contains latent dangerous propensities, it reduces the heterogeneity of durational time to perceive the attributes of an object and their differences of degree from other objects encountered in a past set of data. The question of what this crowd could be, what this vehicle might do, the frustrations or discomforts of the actual lived experience of waiting or gathering persist as indeterminacies in the hidden layers of the algorithm. Even within the archive of training data—sometimes just a Google ImageNet dataset of labeled images of school buses—are the residual contingencies of durational time, with all the past lived moments supplying norms and anomalies for the algorithm to learn. “My own duration, such as I live it in the impatience of waiting,” reflects Gilles Deleuze, “serves to reveal other durations that beat to other rhythms, that differ in kind from mine.” To respond to the perceptual power of the algorithm and to prize open the aperture of the single output is to trace the other durations that continue to beat in the discarded data, the multiple other potential pathways that could be mapped between fragments.

### Link—Big Data

#### Collection of “big data” manipulates human behavior and creates the new surveillance capitalism

**Kwet 21** (Michael Kwet, Yale Univeristy – Information Society Project, “People’s Tech for People’s Power: A Guide to Digital Self-Defense & Empowerment”, *Right2Know Campaign*, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748901>) // EL

Surveillance Capitalism Throughout history, surveillance systems have undermined freedom and democracy. In South Africa, surveillance has been central to systems of oppression, from the identity passes issued to indigenous people under colonialism to the reference books (dompas) administered by the apartheid government. With digital technology, the capacity for surveillance has expanded, and is being used by those with power for political, economic, and social control. South Africa is often deemed the “protest capital of the world”, and many protesters are subjected to mass and targeted surveillance. This threatens freedom of expression. Civil society activists and the poor are the most vulnerable, and they face the most violent repercussions for their political activity. Journalists, judges, politicians, whistleblowers, unions, and academics are among the many surveillance targets in recent years. Today’s surveillance is much more pervasive than in times past. A new, digitally-powered form of surveillance capitalism – the economic exploitation of society through corporate and state mass surveillance – is spreading to South Africa from abroad. This threatens our civil rights and liberties by subjecting us to a life continuously watched and recorded by states and corporations. Big Data refers to the drastic expansion of data collected about people and nature in today's digital world, and the use of computers to make sense of it by identifying patterns and correlations. Information about things such as what people like, what websites they visit, and who they are friends with has provided Big Tech corporations with data that can be used to manipulate people’s behavior with targeted advertisements and addictive features. For instance, Silicon Valley corporations are capturing market share by using “brain hacking” – the systematic exploitation of psychological vulnerabilities to hook consumers into their products and services so they will view more ads. Big Data underpins these practices, and is spreading fast across society. US-based transnational corporations, led by “GAFAM” (Google, Amazon, Facebook, Apple, Microsoft), are the centre of this brave new world. They continuously collect every little detail about us from our computers, mobile phones, and internet activities. As technology advances, they are expanding their data fiefdoms by building surveillance into household gadgets like Amazon Echo and Google Nest. Through the Internet of Things, everyday appliances like “smart” refrigerators, thermostats, trash cans, toothbrushes, and even diapers are being manufactured to collect ever more consumer data.

### Link—Cyber—Attribution

#### Legal resolution of the attribution problem is an attempt to reinscribe cyberspace within the state’s control.

Joque, 18—PhD from the European Grad School, researches philosophy, technology and media and is the visualization librarian at the University of Michigan, go blue (Justin, “Buffer Overflow: The Space and Time of Cyberwar,” *Deconstruction Machines: Writing in the Age of Cyberwar*, Chapter 1, 53-56, dml)

War and politics in this realm then begin not only to fix upon the most important nodes in various economic, legal, and military networks but also to reshape the connections and nodes of these networks to their advantage. War becomes the ability not only to occupy and control nodes or connect and disconnect parts of the network but to shape the space and networks that underlie the global battle space. Perhaps this is part of the reason that late-twentieth- and early-twenty-first-century war begins to fixate so heavily on the spectacle. It may be that, rather than war becoming a purely virtual phenomenon, war has instead taken the naming of reality itself as its object. If one can effectively intervene in the multiple networks that define the twenty-first-century globe, it may now be possible to win conflicts without even fighting them. Through these attempts to win by defining the battle, war has become actively engaged in the process of representing both the world and the ability to destroy it. In that sense, we must add a provision to Galloway’s claim: “There is one game in town: a positivistic dominant of reductive, systemic efficiency and expediency. Offering a counter-aesthetic in the face of such systematicity is the first step toward building a poetics for it, a language of representability adequate to it.”55 These dominant forces are equally invested in destroying this game, in upsetting the positivist investments of their enemies. War machines, states, and corporations are already invested in representing the complex space of these networks and in destroying both networks and their representations. The cases of Comment Crew and Stuxnet demonstrate that there is not merely a reductive system of efficiency. Rather, the powers of war and conflict are invested in both speed and slowness; pure unnamed flow and the poetics of representation; construction and destruction. Thus any resistance to these forces of war and control, while it certainly must utilize these tactics, cannot rely solely on representation and slowness against the speed and complexity of war and domination.

INTERNATIONAL LAW AND TERRITORIALITY

The speed at which these spaces are created and reconfigured creates dynamic forces that threaten to destabilize the institutions that exist within these spaces. One need only look at the difficulty that governments face in legislating and regulating networks to see how destabilizing these spaces can be. The constant reconfiguration of the technological, topological, and conceptual nature of these spaces impedes their integration into legal frameworks. For instance, the attribution problem stems from the reach and speed with which individuals can connect and disconnect from the global Internet. This particular difficulty is often taken up in legal discussions surrounding cyberwar. Although the problem of attributing attacks affects the security of systems, it is more often a political and legal problem. If it is impossible to assign responsibility for an attack convincingly, political and military responses become difficult. A number of legal solutions to both the attribution problem and this more general destabilization of quickly shifting spaces have been proposed, but many quickly run into challenges.

One potential legal remedy to the uncontrollability of networks has been to make individual nations responsible for attacks originating in their territories.56 This attempt to solve the attribution problem shifts the burden of responsibility to the countries from which attacks emanate, regardless of their political or military involvement in the attacks. Although a number of legal scholars, especially from the United States, have suggested this potential approach, their optimism is usually tempered by the admission that the vast majority of attacks traverse networks inside the United States owing to the density of well-networked (and often insecure) computers in that country.57 It seems ultimately unlikely that the United States or many other countries would actually push such an agenda on an international level, because they would then be responsible for a vast number of attacks and compromised machines. Aside from the question of whether such a solution is politically viable or would actually serve to decrease the rate of attack, it is interesting in that it attempts to reassert the geographic territoriality and responsibility of nations over the network. Moreover, these attempts mark a willingness among these authors to give up identity in favor of a new territoriality. The proponents of this plan seem so frustrated by attacks that they are willing to forgo knowing the identity of attackers (whether they are military, paramilitary, rogue agents, etc.) by assigning responsibility to those with national political control over territory.

An American legal scholar and a computer scientist, Jeremy and Ariel Rabkin, have gone so far as to suggest that the United States reintroduce the practice of issuing “letters of marque” to counter cyberattacks. Letters of marque were a practice for dealing with pirates up until the middle of the nineteenth century. With a letter of marque, a privateer would be authorized by a government to attack and capture pirate vessels. Thus, while the government did not take responsibility for the reprisal, it would offer legal protection for privateering. The notion proposed by the Rabkins would have the U.S. government offer letters of marque to domestic hackers to attack particular hackers in other countries. They are clear about the claimed benefits of privateering, both historically and contemporarily: “In practice, letters of marque often were issued to those who had learned the craft of capturing prize at sea without any government authorization. Governments issuing authorization brought these raiders under more state control in return for offering them more state protection.”58 The extent to which some scholars of cyberwar are willing to go to reassert state and territorial control over its complicated existence in cyberspace is at times astounding. This is not to suggest that an unraveling of state control over cyberspace or territory is inevitable. The opposite may be true: that we are condemned to live in a bordered, nationalized, territorial world for centuries. What is surprising about the Rabkins’ suggestion is the intensity of their response to the fear that an uncontrolled military force might grow outside of the state’s control. Rather than rethinking the relationship between state, territory, and war, they seem to reach for any legal metaphor to recapture these events in the space of law and territory. They are keenly aware that one of the effects of letters of marque is to bring privateers under some state control. They are willing to return to privateering so as to guarantee that everything falls into the state/territorial system at least to the highest degree possible.

Both of these attempts appear to try to reinscribe cyberspace into the space of the nation: the first simply by using the physical location of servers to inscribe cyberspace in national law and the second by treating cyberspace as analogous to the high seas and legalizing privateering. In both cases, the authors see war located on the Internet as problematic for state control. This fear testifies to a loosening of the state’s control over space, or at least the new spaces created through modern communication technologies.

This is not to say that such a process is historically unique but rather that cyberwar can be understood as part of a process of militarization creating smooth space, Deleuze and Guattari’s term for an open space across which forces are able to move uninterrupted. They define this type of space against striated space, the space of law and the state, in which one is held in place and blocked from movement. Their concepts of smooth and striated space share much with Castell’s distinction between spaces of flow and spaces of place. The distribution and configuration of these spaces are central to contemporary politics. As Deleuze and Guattari suggest, the state “does not just go from the smooth to the striated, it reconstitutes smooth space; it reimparts smooth in the wake of the striated. It is true that this new nomadism accompanies a worldwide war machine whose organization exceeds the State apparatuses and passes into energy, military-industrial, and multinational complexes.”59 This is not to suggest that these are necessarily spaces of liberation or freedom. Rather, these spaces can become the most terrifying sites of state violence. One could easily imagine that smooth spaces inhabited by pirates and privateers could be more violent than the interiors of state control. Thus we must draw a distinction between the spaces in which the state acts and spaces the state can control. These spaces that are opened for military intervention often turn into spaces in which the state acts but is ultimately unable to control and is thus forced to appropriate and integrate privateering, piracy, and other forces that exceed the state and potentially destabilize it.

The militarization of new spaces is not unequivocally on the side of expanded state control. Rather, it appears that the expansion and distortion of the space of war may ultimately undermine the state’s relation to its territory, requiring the creation of novel legal regimes or the reintroduction of old institutions, such as privateering, to reappropriate these destabilizing spaces to state control. These spaces are not frictionless networks over which the state unceasingly expands its control. It is the complexity, multiplicity, and polyvocal nature of these spaces and those systems that inhabit them that continually challenge state attempts to fix, stabilize, and manage them.

### Link—Cyber—Encryption

#### Cryptography is a double-edged sword. The aff’s attempt to completely control encryption turns against itself.

Joque, 18—PhD from the European Grad School, researches philosophy, technology and media and is the visualization librarian at the University of Michigan, go blue (Justin, “Distributed Denial of Service: Cybernetic Sovereignty,” *Deconstruction Machines: Writing in the Age of Cyberwar*, Chapter 3, 121-125, dml)

As the state summons a counterwriting against the tendencies of the universe, it increasingly risks itself in the process. As we saw in the example of Tor, it is often the war machine that takes advantage of this counterwriting against, or at least outside, the state. Both the state and the war machine have an uncertain relationship to cryptography and the ability of citizenry to write in secret. The state appears at once to promote and develop cryptography, especially as a support for modern networked-based capitalism, and at the same time it moves to undermine and defeat cryptography. Moreover, since the invention of publickey cryptography, when we speak of the desire for and promotion of cryptography, we must remember that we are referring to the ability not only to send secret messages but also to authenticate and prove one’s identity. Thus both states and war machines arrive at the public realization of the universe’s tendency toward strong cryptography in a difficult situation. If, as Foucault suggests in his lecture series Security, Population, Territory, the function of the modern state is to secure the population, the state both requires cryptography to secure digital spaces and the digital population but must then defeat cryptography to secure its physical population. The ability to guarantee secrets becomes critical for maintaining long-distance communication networks but at the same time threatens to empower secret conspiracies that would turn against the state.

To better understand what is at stake in the state’s relation to cryptography in particular, and more generally in relation to cyberwar and the militarization of networks, it is helpful to trace these developments through Foucault’s work on the state vis-à-vis its population.24 Foucault outlines three historical modes of operation of the state: sovereignty, societies of discipline, and finally, societies of security. He cautions, “There is not a series of successive elements, the appearance of the new causing the earlier ones to disappear. . .what above all changes is the dominant characteristic.”25 Still, the most contemporary in this list, security societies, has as its most notable element the creation of a population that must be secured as a whole. Foucault says of security,

Security will try to plan a milieu in terms of events or series of events or possible elements, of series that will have to be regulated within a multivalent and transformable framework. The specific space of security refers then to a series of possible events; it refers to the temporal and the uncertain, which have to be inserted within a given space. The space in which a series of uncertain elements unfold is, I think, roughly what one can call the milieu.26

To control this milieu, the state intervenes in a population that is treated as a biological entity. Norms and limits are discovered against which to measure the population. In contrast to previous forms of the state,

the milieu appears as a field of intervention in which, instead of affecting individuals as a set of legal subjects capable of voluntary actions—which would be the case with sovereignty—and instead of affecting them as a multiplicity of organisms, of bodies capable of performances, and of required performances—as in discipline— one tries to affect, precisely, a population. I mean a multiplicity of individuals who . . . essentially only exist biologically bound to the materiality within which they live.27

Security thus takes a space and a biological population that exists within that space and attempts to maintain control over the uncertain events of the milieu and the embedded population. The population, as biological entity, is measured against a norm and securitized to maintain the desired norm. This relation, between the state and a population that must be accounted for as a whole, radically changes in our contemporary era, especially under the threat of cyberwar.

The advent of cyberwar, especially with its cryptographic concerns, adds to the complexity of the state’s desire for security. As more and more of our daily activities occur online and more infrastructure is supported and made vulnerable by its connection to the global Internet, the state becomes responsible for a digital milieu and a digital population as much as it is responsible for a biological population. The state’s quest for security becomes bifurcated between a topographic and topological space, a biological population and a digital population. Cryptography bifurcates along similar lines and now fills a dual function. On one hand, cryptography has become the linchpin to security online. Without the ability to both send secure messages and identify individuals, there would exist no way to use the Internet for any but the most trivial functions. Cryptography thus becomes a requirement for security online and for the physical infrastructure connected to these digital networks. On the other hand, cryptography allows the exchange of messages across the globe beyond the watchful eyes of security agencies and militaries. Cryptography, in a sense, cuts between the war machine and the state, becoming a necessity and a threat to both.

The problem posed by cryptography is not an entirely new problem for the state. While, on one hand, it is a problem of spatiality, between topographic space and topological space and between a digital population and a biological population, it is also a problem of the relationship between the mass and the individual. Cryptography is critical for the security of the mass of online functions, for the global totality of the Internet, but an individual’s use of cryptography can easily threaten the digital or physical whole. Cryptography thus repeats a central problem Foucault outlines in relation to the rise of security and the art of government, or governmentality, as he refers to it. Foucault traces the roots of the modern security state to the Christian pastorate, which he claims to be

paradoxically distributive since, of course, the necessity of saving the whole entails, if necessary, accepting the sacrifice of a sheep that could compromise the whole. . . On the other hand, and this is the paradox, the salvation of a single sheep calls for as much care from the pastor as does the whole flock; there is no sheep for which he must not suspend all his other responsibilities and occupations, abandon the flock, and try to bring it back.28

Both the mass and the individual must be saved, and each at the expense of the other. For Foucault, the pastoral problematic does not stumble upon an already constituted individual who is opposed to the mass it constitutes; rather, the pastorate “is a form of individualization that will not be acquired through the relationship to a recognized truth, [but] will be acquired instead through the production of an internal, secret, and hidden truth.”29 The Christian pastorate constructs both an individual and mass that come to be diametrically opposed and require salvation both through and against the other.

Foucault goes on to say that as this system of pastoral power is adopted by the state, its logic disregards the problem of the mass and the individual.30 Thus, for Foucault, the state as an institution of governmentality does away with the problem of the mass and the individual. It decides clearly on the side of the mass at the expense of the individual. But he also notes that as the state becomes a more liberal institution and its aims become “a matter of insuring that the state only intervenes to regulate, or rather to allow the well-being, the interest of each to adjust itself in such a way that it can actually serve all,”31 the issue of this relation between mass and individual is maintained as an aporetic concern of the state. We see it arise precisely in the relation between the state, cryptography, and its defenses against cyberwar. The whole requires cryptography to function in a digital world, but the individual’s access to cryptography threatens the whole. At the same time, the individual, as potential threat to the mass, must somehow be barred from full access to digital security. The paradox the Christian pastorate stumbles upon returns as a key aspect of the apparatus of security. Moreover, even if the state were to find an optimal balance between the two, the war machine’s attempts to both secure its own systems and disrupt the security of enemy systems further destabilize any technopolitical balances.

### Link—Cyber—Securitization

#### The aff’s hypersecuritization of cybersecurity stems from itself – disasters of cyber systems happen as a result of their initial investment

**Hansen & Nissenbaum 9** (Lene Hansen & Helen Nissenbaum, IR scholar and Professor at University of Copenhagen & Professor of Information Science at Cornell Tech, “Digital Disaster, Cyber Security, and the Copenhagen School”, International Studies Quarterly, Volume 53, Issue 4, 12/2/9, <https://academic.oup.com/isq/article/53/4/1155/1815351?login=false>) // EL

Hypersecuritization The first concept, hypersecuritization, has been introduced by Buzan (2004:172) to describe an expansion of securitization beyond a ‘‘normal’’ level of threats and dangers by defining ‘‘a tendency both to exaggerate threats and to resort to excessive countermeasures.’’ This definition has an objectivist ring to it in that to identify ‘‘exaggerated’’ threats implies that there are ‘‘real’’ threats that are not exaggerated. Moreover, the question of whether a securitization is seen as ‘‘exaggerating’’ concerns the degree to which it is successful (unsuccessful securitizations are seen as ‘‘exaggerating’’) and is not part of the grammatical specificities of sectors. Thus we suggest to drop the ‘‘exaggerated’’ from the definition of hypersecuritization and to apply it to the cyber sector to identify the striking manner in which cyber security discourse hinges on multi-dimensional cyber disaster scenarios that pack a long list of severe threats into a monumental cascading sequence and the fact that neither of these scenarios has so far taken place. All securitizations do of course have an element of the hypothetical in that they constitute threats that must be countered, and thus mobilize an ‘‘if-then’’ logic, but what distinguishes hypersecuritizations from ‘‘mere’’ securitization is their instantaneity and inter-locking effects (Denning 1999:xiii). This combination draws critically from the securitization of the network (Deibert 2002), yet the power of hypersecuritization stems not only from a securitization of the network itself, but from how a damaged network would cause societal, financial, and military break-down hence bringing in all other referent objects and sectors. Securitizations always mobilize the specter of the future to some extent, but most nevertheless articulate the past as a legitimating reference that underscores the gravity of the situation. Looking to the Cold War, the logic of nuclear deterrence relied upon projections of a nuclear exchange that had not taken place, yet there were the devastations of Hiroshima and Nagasaki to be used as a yardstick for what nuclear war would imply. Cyber securitizations on the other hand have no similar history of founding incidents to base themselves on but try to conjure historical analogies such as ‘‘electronic Pearl Harbors’’ (Bendrath 2003:50).7 The combination of cascading disasters and the absence of a prior incident of that magnitude creates a crucial ambiguity within cyber security discourse. The extreme reliance on the future and the enormity of the threats claimed at stake makes the discourse susceptible to charges of ‘‘exaggeration,’’ yet the scale of the potential catastrophe simultaneously raises the stakes attached to ignoring the warnings.8 Turning the absence of prior incidences in the opposite direction, the difficulty of saying that it could not happen also creates a powerful space for the projection of the (im)possible. The hypersecuritization of the entire network in cyber security creates an obvious resemblance to environmental security discourse where the fate of the planet is claimed at stake. Both discourses also emphasize irreversibility: once a species is extinct or a digital system gone, they can never be recreated in full. Yet, there are also crucial differences between the two discourses. First, the speed of the threat scenarios differ with cyber security gaining its power from the instantaneity of the cascading effects whereas environmental security usually allows for a gradual accumulation of threats and dangers until a certain threshold may be reached and events accelerate. This establishes different modalities of urgency and hence different spaces for political intervention.9 Second, there is a crucial difference in terms of the possibility of visualizing threats, and hence for how securitizing actors communicate to their audiences (Williams 2003). The digital, networked character of cyber security—and the absence of prior disasters—is hard to represent through images, whereas environmental security discourse may mobilize for example endangered and extinct species as well as melting ice caps and forests devastated by acid rain or clear-cutting.

#### Cybersecurity logics are false – threats stem from unpredictability of cyber itself which the aff reproduces

**Hansen & Nissenbaum 9** (Lene Hansen & Helen Nissenbaum, IR scholar and Professor at University of Copenhagen & Professor of Information Science at Cornell Tech, “Digital Disaster, Cyber Security, and the Copenhagen School”, International Studies Quarterly, Volume 53, Issue 4, 12/2/9, <https://academic.oup.com/isq/article/53/4/1155/1815351?login=false>) // EL

Securitizing Digital Systems: The Referent Objects of Cyber Security The history of cyber security as a securitizing concept begins with the disciplines of Computer and Information Science. One, if not the first, usage of cyber security was in the Computer Science and Telecommunications Board’s (CSTB) report from 1991, Computers at Risk: Safe Computing in the Information Age which defined ‘‘security’’ as the ‘‘protection against unwanted disclosure, modification, or destruction of data in a system and also [to] the safeguarding of systems themselves’’ (CSTB 1991:2). Security comprised technical as well as human aspects and ‘‘it has significant procedural, administrative, physical facility, and personnel components’’ (CSTB 1991:17). Crucially, threats to cyber security do not only arise from (usually) intentional agents, but also from systemic threats. These systemic threats, defined by Hundley and Anderson (1995 ⁄ 1996:232) as ‘‘cyberspace safety’’ stems from the inherent unpredictability of computers and information systems which by themselves ‘‘create unintended (potentially or actually) dangerous situations for themselves or for the physical and human environments in which they are embedded.’’ Threats arise from software as well as hardware failures and cannot be corrected through perfecting digital technology and programming; there is, in short, an inherent ontological insecurity within computer systems (Edwards 1996:290–2; Denning 1999:12). ‘‘Computer security’’ would not, however, in most cases by itself qualify as a security concept according to the Copenhagen School. As Helen Nissenbaum points out, the majority of computer scientists adopt a technical discourse that is focused on developing good programs with a limited number of (serious) bugs and systems that are difficult to penetrate by outside attackers. In the move from ‘‘computer security’’ to ‘‘cyber security,’’ this technical discourse is linked to the securitizing discourse ‘‘developed in the specialized arena of national security’’ (Nissenbaum 2005:65). ‘‘Cyber security’’ can, in short, be seen as ‘‘computer security’’ plus ‘‘securitization.’’ In the 1991 CSTB report it is argued that ‘‘We are at risk’’ and in a remarkable mobilization of securitizing prose that ‘‘Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb.’’ No major attacks have been launched so far, but it is a key element of securitizing discourse to argue that if action is not undertaken then serious incidents will materialize in the near future, thus ‘‘there is reason to believe that our luck will soon run out’’ (CSTB 1991:7–8). The constitution of a much too complacent audience that does not realize the magnitude of these dangers is another key staple of securitizing discourse, and the CSTB laments that ‘‘Very few individuals not professionally concerned with security … have ever been directly involved in or affected by a computer security incident. … most people have difficulty relating to the intricacies of malicious computer actions’’ (CSTB 1991:159–61). Eleven years later, most Americans have been exposed to (scares of) computer viruses, worms, and hackers, yet the Board complains that in spite of the reports produced over the past years, ‘‘not much has changed with respect to security as it is practiced.’’ As the threats to cyber security have increased while the countermeasures have not, ‘‘our ability and willingness to deal with threats have, on balance, changed for the worse’’ (CSTB 2002:2). In another attempt to stress the urgency and wake up policy makers and the broader public, the report is titled Cybersecurity Today and Tomorrow: Pay Now or Pay Later. A similar tone is struck a year later in the so-far most authoritative and comprehensive statement of US cyber security policy: President Bush’s The National Strategy to Secure Cyberspace which opens by asserting that ‘‘In the past few years, threats in cyberspace have risen dramatically.’’ Although a large-scale cyber attack has not yet taken place, this is no time to ‘‘be too sanguine’’ as ‘‘the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving’’ (The National Strategy 2003:viii). Key to understanding the potential magnitude of cyber threats is the networked character of computer systems. These networks ‘‘control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, and radars’’ (The National Strategy 2003:6–7) and attacks—or ‘‘cyberdisasters’’—would ‘‘compromise systems and networks in ways that could render communications and electric power distribution difficult or impossible, disrupt transportation and shipping, disable financial transactions, and result in the theft of large amounts of money’’ (CSTB 2002:6). Although not necessarily directly connected, the magnitude and simultaneity of these attacks would have cascading effects and thus networked consequences for referent objects beyond networks themselves. Networked computers have also dissolved the traditional boundary protecting the territorial nation state, ‘‘the infrastructure that makes up cyberspace—software and hardware—is global in its design and development’’ and cyber attackers may operate at a distance obfuscating ‘‘their identities, locations, and paths of entry’’ (The National Strategy 2003:7; Yould 2003). To give an indication of how an attack transgresses territorial boundaries, RAND’s ‘‘The Day After… in Cyberspace II’’ exercise in 1996 drew up a list (Anderson and Hearn 1996:4–5) including electronic looting of European and American banks by (unspecified) Russians, software computer viruses causing financial havoc and plane and train crashes, power grid fall-outs at airbases, malfunctioning of ATMs and news broadcasts, and stock market manipulation. RAND’s scenario shows aptly how cyber security discourse moves seamlessly across distinctions normally deemed crucial to Security Studies: between individual and collective security, between public authorities and private institutions, and between economic and political-military security. The private sector’s fear of hackers stealing large sums of money, intellectual property owner’s worry that file sharing compromises their rights and revenues (Nissenbaum 2005:68), and public, private, and civil society scares that bugged software and computer viruses will have damaging consequences produce a powerful blending of private-economic and public-national security concerns. Not only are large parts of the networks, hardware, and software privately produced and owned and thus governed by financial considerations, but the security logics of the economic and the cyber sector have crucial similarities. The economic sector is also ‘‘rich in referent objects, ranging from individuals through classes and states to the abstract and complex system of the global market itself’’ (Buzan et al. 1998:100), and in liberal economies instability and risk taking is built into the logic of capitalism itself. The modern economic system is, like the cyber network, constituted by trans-border flows, and authority and sovereignty is more ambiguously located than in traditional national-military security. It is in both sectors often difficult to identify where an attack originated, and with the global reach of the Internet⁄world economy, tricky questions of responsibility and enforcement are continuous sources of fraught cross-border and international treaty negotiations. That said, cyber security does not fully mirror the economic sector either: its securitizing potential exceeds that of the economic sector as strictly defined (Buzan et al. 1998:116–7) and this in turn allows—or is an indication of—a much stronger link to national military security. Cyber security is not left to the liberal market, but implies a complex constellation of public-private responsibility and governmental authority. Drawing upon the individual-collective resolution laid out above, the government consistently holds the private sector co-responsible for cyber security: not only does the latter own major parts of the computer network, it also possesses the knowledge—‘‘In general, the private sector is best equipped and structured to respond to an evolving cyber threat’’ (The National Strategy 2003:ix). Mobilizing civil liberties discourse further invokes a crucial balance between the public and the private that should not be violated: ‘‘The federal government should likewise not intrude into homes and small businesses, into universities, or state and local agencies and departments to create secure computer networks’’ (The National Strategy 2003:11). To the government this allows for a distribution of the financial and political burden and it strategically engages critics who point to privacy violations. To the private sector, these securitizations boost its calls for the protection of intellectual property rights, for vigilant prosecution of cyber crimes, and for combating digital anonymity (Nissenbaum 2005:68). Negotiation of the boundaries between the public and the private and between the economic and the political thus couples the network-fragmentation implied by ‘‘cyber’’ with an understanding of business and government as sharing the same goal. At the same time the political center still constitutes the private sector as responsible for major parts of the digital realm. This academic and policy discourse articulates in sum a wide array of threats to government, business, individuals, and society as a whole perpetuated by hackers, criminals, terrorists, commercial organizations, and nations that adopt cyber strategies for financial, ideological, political, or military gain (Hundley and Anderson 1995 ⁄ 1996:232). Yet obviously not all political or societal actors concur with the manner in which official American cyber security discourse has attempted to keep the public-private and individual-state resolutions in place. As Ronald J. Deibert (2002) and Diana Saco (1999) have argued, cyber security is a terrain on which multiple discourses and (in)securities compete.6 Privacy advocates and cyber libertarians point to governmental violations of personal security (Saco 1999), and authoritarian (and not so authoritarian) regimes securitize transborder information flows as threats to regime ⁄state security and national (societal) identity in a way that expands the threat-referent object constellation considerably (Deibert 2002). The question is therefore how we incorporate this complexity into our theoretical framework without loosing the sense of cyber security discourse as a distinct phenomenon? Deibert (2002) argues that cyber security is constituted through four separate discourses with distinct referent objects, threats, policy options, and world orders: national security, state security (comprising external threats to state sovereignty as well as internal threats to regime security), private security, and network security, and Saco holds that national and personal security compete (Saco 1999:270, 286). We agree with Deibert that cyber security should be theorized as a sector where multiple discourses may be found, yet we think that understanding this multi-discursivity as arising from competing articulations of constellations of referent objects, rather than separate referent objects, better captures the securitizing and political dynamic of the field. To see cyber security discourse as fragmenting along the lines of distinct referent objects downplays the ways in which cyber security discourse gains its coherence from making connections between referent objects rather than operating at separate tracks. Particularly crucial in the case of cyber security is the linkage between ‘‘networks’’ and ‘‘individual’’ and human collective referent objects. Thus it is not the case that a private security discourse constitutes the individual as its referent object, but rather that ‘‘the individual’’ of this discourse is linked to societal and political referent objects. Take the example of post-September 11 battles between governmental discourses legitimizing digital surveillance and data-mining through securitizing reference to the War on Terror and citizen groups fighting this legislation through reference to basic civic liberties and privacy issues. These are not two separate discourses with unrelated referent objects, but competing articulations of the appropriate individual-state contracts of the liberal state (Saco 1999:271). Moreover, it is not fully clear from Deibert’s and Saco’s accounts whether private security discourse operates through the political rather than the semantic modality of security. This does not mean that cyber ‘‘privacy’’ cannot be securitized, but this has to be mediated through a collective referent object, either a political-ideological one, questioning the appropriateness of the individual-state balance, and⁄ or a national-societal one, mobilizing the values held to be the core of the community’s identity. Similarly, a securitization of the network cannot, and does not, stop at the network itself: it is the implications of network break-downs for other referent objects, ‘‘society,’’ ‘‘the regime,’’ or ‘‘the economy’’ (which is, again, in turn linked to ‘‘state’’ and ‘‘society’’) that makes cyber securitization a plausible candidate for political and media attention. Securitization works in short by tying referent objects together, particularly by providing a link between those that do not explicitly invoke a bounded human collectively, such as ‘‘network’’ or ‘‘individual,’’ with those that do. Contestation and multidiscursivity is thus found between competing articulations of linked referent objects as well as by tracing the potential internal instability of each discourse.

### Link—Death?

#### Foucault kindly and shyly, in his style, tells Deleuze: you know, I must confess to you that the word “desire” disgusts me. I would prefer to use the word “pleasure,” would you agree? Deleuze does not agree at all.

Bifo 20 (Franco “Bifo” Berardi, founder of the famous Radio Alice in Bologna and an important figure in the Italian Autonomia movement, is a writer, media theorist, and social activist, “Desire, Pleasure, Senility, and Evolution”) // ‘ansel’

This essay is short and inconsistent. It grew out of a talk I gave at the e-flux conference “Art After Culture” in June 2019. When I was invited to speak, the subject I proposed was: “Desire, Pleasure, Evolution.” I will begin with a few things about those topics, but will move on to other things, namely senility and evolution.

So, desire and pleasure. I recently discovered that somewhere—I don’t remember exactly where—Gilles Deleuze recounts the story of an exchange between himself and Michel Foucault. Before leaving the house of Deleuze, Foucault kindly and shyly, in his style, tells Deleuze: you know, I must confess to you that the word “desire” disgusts me. I would prefer to use the word “pleasure,” would you agree?

Deleuze does not agree at all. He absolutely disdains the word “pleasure.” Actually, in a lecture he delivered in Vincennes in 1973, Deleuze said something along the lines of: Plaisir, quel horrible et atroce mot. Qu’est-ce que ça signifie? Le décharge? (Pleasure, what a horrible, atrocious word. What does it mean? Discharge?)

This discussion between the two is revealing of a dimension of desire as discussed by Deleuze and Félix Guattari that has always escaped me. During my years in Paris in the late ’70s, I first came to realize that desire is the engine that mobilizes social energies, but I did not consider at all the distinction between desire and pleasure. It wasn’t until just last year that I understood the difference, while reading about that exchange between Deleuze and Foucault.

Of course, one can find an explication of the difference in **Jean Baudrillard, the real wise man of the Parisian scene** of the ’70s and ’80s. Baudrillard says: desire, yes okay, the desire for beautiful things, but beware that the entire history of capitalism is based on permanent desire.

Now, in my old age I have come to (painfully) appreciate the difference between desire and pleasure, and I understand that **capitalism is**, in fact, **based on an endless postponement of pleasure, and simultaneously on the permanent excitement of desire**. Virtual capitalism—what I call **semiocapitalism**—**is an intensification of both these conditions**, postponing pleasure and exciting desire.

Another catalyst for my realization of how they differ is feeling physically, personally that growing old essentially means losing the ability to access certain spheres of pleasure, while desire continues undisturbed. Beyond my personal experience, and its suggestion of a larger condition, there is something more interesting, and more disturbing, in the relationship between the two. This relationship—between the permanent burning of desire and the inaccessibility, the unattainability of pleasure—has something to do with the present historical moment of transition, the present step in human evolution.

Why are older people so nervous? Cantankerous even? I don’t even know the meaning of this word, but it sounds right. Why are old people so malignant?

I have two answers. The first has to do with the disappearance of neurons and synapses in old age: the reduction in the ability to process information, the loss of subtlety, the loss of definition in the relationship between sensibility and experience. The second is that we—**we** humans, old humans in particular—**tend to cling to life because we think it is our private property. This life is mine, and I don’t want to lose this property**.

The denial of death is deeply inscribed in the modern mind. As the world’s white population grows old, this has provoked something resembling a social psychosis, an aggressive grasping among the old for all that is left: naked life, putrescent life.

At the end of his beautiful book The Order of Time, Carlo Rovelli writes that **the fear of death is a mistake of evolution**. It is an error provoked by the inability to think the world without one’s own presence within it, an inability to think the world without me. Modern culture emphasizes the individual in continuous competition with other individuals, and consequently erases a sense of community among people. Thus, it has turned death into something that cannot be thought, said, or psychically elaborated. Death is systematically denied, which in turn leaves the individual alone in an infinite desert of sadness, and ultimately unable to see the continuity among the individual and the community, among me and you.

Furthermore, modern capitalism is based on an idolatry of energy. It is based on an obsession with growth, expansion, productivity, acceleration—futurist obsessions that have made senility unthinkable.

Why am I writing about these strange and slightly scary subjects? Why am I talking about senility and death? Of course, the main reason is that they are my problems. But, believe me, they’re not my problems alone. They are two of the main problems of humankind in the present. The denial of death, linked to the idolatry of energy and expansion, has turned decline and un-growth into purely negative tendencies, and frugality into scarcity. So, in this sense, **life has become a paranoid fight against the passage of time**.

I strongly believe that senescence is the (unseen or unfathomed) key to understanding the present historical conundrum, just as decline is simultaneously the problem and the solution to the late-modern crisis.

Firstly, we can surmise that this situation is due to demographic reasons. Senility now tends to be the condition of most of the Western population, and not only of the Western population. While the African population grows exponentially, while the populations in the Middle East and on the Indian subcontinent steadily grow, Western dominators and aggressors are ageing, they are losing energy, and most of all, they are losing the innocent faith in the future that belongs mostly to younger people.

The demographic gap between the population explosion in much of the South and the decline in the North is probably one of the central reasons for contemporary racism and aggressiveness. Old people have transferred their declining potency to the machines, and the war machine is in motion as a permanent menace against those oppressed in the South, the colonized people who try to migrate towards the declining Northern lands. This is why we must consider the crucial problem of senility if we want to understand anything at all about what is happening in the social, cultural, and political spheres.

#### Time oppresses me I fall

And I slide on my knees

My hands feel the night

Farewell streams of light

All that remains for me now is the shadow

The dregs the blood

I await the strike of the bell

Where screaming

I entered the shadow.

* Georges Bataille

Bifo 20 (Franco “Bifo” Berardi, founder of the famous Radio Alice in Bologna and an important figure in the Italian Autonomia movement, is a writer, media theorist, and social activist, “Desire, Pleasure, Senility, and Evolution”) // ‘ansel’

I recently read Staying with the Trouble by Donna Haraway. When I read Haraway, I don’t understand everything, but I understand the essentials. She says, in an ironic and beautiful way, that today there are two reactions to technology. On one side, there are the techno-optimists, who believe that technology will save humanity, the planet, and the environment. On the other side are the techno-apocalyptics, who say no way, technology will destroy everything. Haraway takes a different stance: she instead tells us to keep calm. She says that it isn’t a tragedy that the human race is doomed to disappear.

Extinction is the new buzzword on the political scene nowadays. Look at the enormous demonstrations organized by children in Sweden, in Germany, in Italy, everywhere in the world. Millions of children marched on March 15, 2019. Their message is about extinction. They don’t have a political problem. They simply say: it’s time to panic. And look at Extinction Rebellion. It’s the first time in human history, as far as I know, that extinction has become the core concern of a political protest movement.

I would not focus on rebelling against extinction. Can one even rebel against extinction? I don’t think so. You can deal with extinction. You have to deal with extinction. Extinction, by the way, is not the worst thing that one can imagine for the future. The worst thing imaginable is the war that will lead to extinction—not death, but the long-lasting agony that financial capitalism has prepared for humankind. This is the real danger. Extinction is not so bad, if we compare it to capitalism.

After quoting Haraway, I want to quote the French philosopher and psychoanalyst Catherine Malabou. She says that psychoanalysis has undergone a shift from the analysis of sex and language to neurology. The fields of sex and language have long been the focus of psychoanalytic theory and therapy. But when we speak of Alzheimer’s and Parkinson’s, or of panic attacks and depression, we can see that they’re not just problems related to sex and language. They concern the physical dimensions of neurology. It’s neurology nowadays that is at stake. It’s the brain, not the mind. Or better yet: not only the mind, but also the brain. Malabou, taking up this thread, writes of trauma and neuroplasticity.

Evolution must be rethought from scratch, from the point of view of the relationship between desire and pleasure. Pleasure is the goal, the aspiration. Over the past forty years, I forgot about pleasure because I was obsessed with desire, but now I understand that **the way out of capitalism** is the opposite: the way out is not desire, it is pleasure. And **how can the brain find a new balance of pleasure** in the present? This is the problem that we are going to face in the coming years, in the coming decade.

I want to dedicate this inconsistent essay to a friend who died in May 2019. The name of this friend is Nanni Balestrini. Nanni was a poet, a novelist, and most of all a recombiner. He is the first poet in history of humankind who never wrote a single word. He refused the dirty work of writing words. He asked: Why should I do that? Why should I spend my time writing words? I’m a poet. I don’t write words. I take signs from the infosphere, from the daily conversations of people in the subway, from newspapers, from advertisements. His activity, he said, was to recombine. **Recombination is also our task**, and we should take a cue from him. But the question is: the recombination of what? The recombination of meaning, of language, of desire, of pleasure. **Poetry is the consistent and intentional recombination of what exists, with the aim of creating what does not yet exist.**

### Link—Diplomacy

#### Our interpretation evinces the new era of geopolitics – the figure of the diplomat is no longer the representative of nation-states, but rather collectivizes epistemological production. Our understanding of IR formulates a new diplomat that promotes a planetarization based around technodiversity.

Guinard et al 20 (Martin, curateur in charge of conferences and publications, LUMA Arles; Bruno Latour, a French philosopher, anthropologist and sociologist; Ping Lin, e-flux editors; “Editorial: You and I Don’t Live on the Same Planet” December 2020) //ansel is hungry

On the occasion of the Taipei Biennial 2020 and together with the Taipei Fine Arts Museum (TFAM), this special issue of e-flux journal will also be available to read in Chinese in 2021. Titled “You and I Don’t Live on the Same Planet,” the issue deals with an increasingly pressing situation: people “around” the world no longer agree on what it means to live “on” earth—to such a radical extent that the foundational material and existential categories of “earth” and “world” are profoundly destabilized. It was often said at the beginning of Trump’s time in office that he had no coherent strategy. But today we can see that, on the contrary, he had an extremely coherent strategy that unfolded over four years without fail: privatization, deregulation, and isolating the US from any international project. The message of this strategy was clear: “You and I don’t live on the same planet.” What becomes of politics when opposing parties are taken as aliens occupying separate earths altogether? It is as if the question no longer concerns different visions of the same planet, but the composition and shape of several planets in conflict with one another. Pluralism has taken a much more explicit ontological shape, as if we are literally living on different earths—and earths that are at war with each other, as the essay in this issue “Coping with Planetary Wars” explores.  
  
Successive “world orders” have treated planet earth as a fairly homogeneous place where different kinds of resources, different kinds of interests, and different kinds of sovereignties are all unified by one homogenous and overarching concept of Nature. This issue explores the consequences of what Eduardo Viveiro de Castro calls a shift from multiculturalism to “multinaturalism.” As we approach a series of tipping points, we simultaneously witness a division between those who seem to have abandoned planet earth, those who try to make it more habitable, and those whose cosmology never fit within the ideals of the globalizing project in the first place.  
  
This state of division flies in the face of many twentieth-century strategies of political ecology—especially the principle that the high stakes of political ecology justify bypassing the tedious process of negotiation and deliberation typical for political action. Unanimity was supposed to rally the masses in a strong revolutionary push to “save the planet.” However, for the last forty years, we have seen that ecology does not unify. Instead, ecology divides. It divides the generations who will deal with its failures from those who will escape its consequences; it divides the regions already affected by climate disasters from those that are protected; within each region, it divides the classes that suffer disproportionately from decisions made by other classes; furthermore, it divides each one of us at the personal level: for each decision we face, we know there are cascades of unintended consequences that make it hard to distinguish the right actions from the wrong ones. What Bruno Latour has elsewhere called the “New Climatic Regime” poses problems at every magnitude of scale and blurs the classical political cartography.1 As Chun-Mei Chuang writes in this issue: “Our place is neither conservative nor progressive. It is molecular and planetary.”  
  
To characterize this new spatial configuration, Dipesh Chakrabarty offers a brief history of ways of conceiving of the planets, while Eduardo Viveiros de Castro and Déborah Danowski explore the consequences of the turn from a philosophy of history to a philosophy of space, epitomized by the dismantling of the Axial Age thesis.2  
  
In which direction should we go once these divisions are established and assumed? The objective here is to try to imagine procedures that would allow these incommensurable worlds not so much to “dialogue”—which is not sufficient for the enormous differences in ways of inhabiting the world—but to enter into diplomatic negotiations.  
  
The diplomacy that is evoked here does not lie within the existing framework of nation-states, which have, to say the least, many limitations with regard to the New Climate Regime. At the international level, the various UN Conferences of the Parties (COPs) have shown only moderate efficacy. The state may be relevant for choosing whether to shift away from coal or to impose regulations prohibiting the consumption of single-use plastics, but when it comes to managing “trans-boundary hazards” or reducing CO2 produced outside a state’s borders, **a framework other than that of the nation-state and intergovernmental negotiations needs to be imagined**. In this issue, John Tresch, through his research on “cosmograms,” searches for a representation of this space to be invented, while Erika Balsom looks at how documentary cinema can depict those encounters at the “third register.”  
  
As Adam Tooze argues in his essay, diplomacy must be understood here as a mode of negotiation in a world without arbiters, without a higher authority capable of regulating the actions of the various collectives concerned. Of course, being horizontal rather than vertical in its mode of operation does not mean that there is no balance of power.  
  
Taiwan is perfectly positioned to explore this theme. Due to its particular exclusion from the international order, the Taiwanese government has constantly created innovative ways of asserting its existence. For example, in the 1990s it funded the University of the African Future, an elite pan-African university in Senegal whose history is traced in this issue by artists and curators Hamedine Kane, Stéphane Verlet-Bottéro, Olivia Anani, and Lou Mo. But Taiwan is also a place where geological power is felt: an island that trembles, where erosion is severe and typhoons common, and which does not escape the problems of dependence on coal and extractivism. In short, Taiwan is the ideal place to explore geopolitics in both senses of the word: geological and political.  
  
It is on the basis of the cleavages arising from this new geopolitics that a new form of diplomacy can be formulated. As Isabelle Stengers writes in this issue, the statement “‘we are divided’ should first be understood … in an active sense, pointing to what divides us, that is, to what has destroyed the feeling of interdependence as an operative political affect.” In this sense, **the figure of the diplomat is changing**: it is no longer a representative of a state, but **rather an investigator of collective dependencies who has the capacity to help these collectivities formulate their obligations towards what must be maintained**. In other words, the diplomat is an “epistemic messenger,” as Paul B. Preciado writes in this issue. What remains to be explored is how to set up such collectives and how to grant oneself the right to represent them.  
  
**When one world vampirically preys upon the resources of another, diasporas may play the mediating role of stitching together torn geographies**, as Nadia Yala Kisukidi proposes. She emphasizes the modalities of living in several worlds at the same time rather than assigning a place-based identity to diasporas. By exploring this form of geopolitics, Kisukidi traces a path away from the “poor dialectic” that binds France and the Democratic Republic of the Congo. For Yuk Hui, **the figure of the diplomat mutates into that of the “knowledge producer,” promoting a planetarization based on a diversity of ways to understand technology**. A new appreciation of technodiversity might help us break out of the global hegemony within which planetarization has become stuck. And with a concern that this situation may result in new forms of “techno-molecular colonialism,” Achille Mbembe draws the contours of an ethic that is not based on a “diaphanous universalism,” but on “commonality and incalculability” among the living.  
  
Relying on a more traditional definition of inter-state diplomacy, Pierre Charbonnier urges ecological discourse to change its moralist tone and develop a realpolitik approach. The author sees China’s announcement that it will achieve carbon neutrality by 2060 as a way of asserting its power on the international stage. An undemocratic ecology is on the march. Such a context can be instructive for European environmental movements advocating ecological justice by consensus in ways that limit their ability to defend concrete interests.  
  
Even with such a “realist” approach to the situation, can we truly envisage negotiating with everyone? As the well-known doctrine goes, “You can’t negotiate with terrorists.” But what of the state-subsidized terror of preventing legal abortion? Preciado identifies a set of countries, from the US to Afghanistan, that shares a set of repressive policies on abortion. The diplomacy to be invented in this case must be one that incorporates the logic of resistance, otherwise the opponents of this techno-patriarchal bloc will lose all their leverage.

Adam Tooze, for his part, wants to clarify the modalities that make it possible to speak between opposing camps: one cannot negotiate with the hyper-privileged who abandon earth to fly towards “planet escape.”3 An irresponsible project that places so little value on the lives of the masses can only be a crime against humanity, whose adequate response is not diplomatic (horizontal) negotiation, but a hierarchically organized (vertical) trial. According to Tooze, the growing concern about a world that may become uninhabitable makes ecology less a question of superior metaphysical force than an increasingly credible cause. Tooze concludes: “Let us look for every chance for ‘diplomatic encounters.’ But let us reckon with the pervasive force of the emergency that our instruments so clearly register and let us not ignore complementary action” in the realm of traditional politics

### Link—DOD

#### The DOD technologizes war and expands it across the globe while enabling it to boomerang home in the form of domestic repression.

**Wilson 20**( Neil, Masters in Conflict Studies and Human Rights and Utrecht University, “Understanding the Battle for AI in Warfare through the Practices of Assemblage: A Case Study of Project Maven”, Section 6.3, CS)

Examining the practices of antipolitics and reassembly in this context reveal a new form for the Military-Technological Complex. Bridging the divide between the material power of the DoD and social power of civil society, a new breed of “defence-tech” companies like Anduril have carved out a niche as bespoke contractors. Having drawn engineering talent from both traditional defence companies and Silicon Valley, they exclusively but openly court defence contracts, invoking a discourse of patriotism without risking the alienation of a wider consumer market. The ease and speed with which they began providing this work speaks to the significant power of the DoD and, in turn, the resilience of the Military-Technological Complex as an assemblage. Underlying this entire process is a constant tension between the predominantly compulsory power of the DoD and the predominantly productive power of civil society. Sizeable contracts provide a compelling material incentive for many tech companies to provide the technologies sought by the DoD, but are in conflict with the ethical pitfalls publicised by civil society. In some ways, each mimics the other. As the DoD has adopted a discourse of patriotism to assuage ethical concerns, civil society has underlined the material risk to businesses with large consumer markets seen to be enabling these developments in warfare. As a result, the civil-military industrial divide appears more porous than ever, raising valuable questions about contemporary warfare. Project Maven exemplifies a certain fluidity, in that its technologies were originally developed for the consumer market, weaponised by the DoD for drone footage analysis, and are now being “re-legitimised” through their transfer back into the civilian sphere for humanitarian and public health purposes. Such a process arguably reflects a late-modern - or liquid modern - blurring of the boundaries between war and peace, military and civilian, public and private. A blurring civil-military distinction in this regard must be understood in the context of a geographically and temporally expanding militarism observed in the rise of “unending” and “everywhere” wars. Similarly, in Graham’s conceptualisation of the “battlespace” of cities, he observes it “has no front and no back and no start or end… the concept… thus works by collapsing convention al military-civilian binaries.” Common to these suggestions that conventional ties between war, space and time are coming undone, however, is a focus on their practice. The ascendancy of the Military-Technological Complex suggests that the nebulous expansion of warfare across space and time not only pertains to how it is practiced but also how its means are developed and procured. It is not a stretch to suggest that this expansion, in turn, risks normalising new imaginations of violence. And given that “violence needs to be imagined in order to be carried out,” one wonders where this normalisation may lead. Conceptualising the Military-Technological Complex as an assemblage is particularly appropriate in the context of liquid modernity. Absent of rigid, ‘arboretic’ structures, it takes shape in a manner consistent with Bauman’s interpretation of sociality, “spreading rhizomically and sprouting formations of varying degree of durability, but invariably unstable, hotly contested and devoid of foundation to rely on.” Fluidity of formation and re-formation in this regard, however, should be regarded as “a feature of state power, not a bug.” Instead of the state standing separately to the private sphere, it is intimately embedded within it and continually reproducing its power through it. Lastly, directly relevant to this “undoing” of conventional warfare and fluidity of the military-civilian divide is Foucualt’s ‘boomerang’, which suggests the practices - and technologies - of peripheral subjugation inevitably return to the centre. Or, as Marx suggested, the scenario of “war [being] developed earlier than peace.” Indeed, many have noted the ways in which the United States’ war on terror has already “come home to roost” in the form of widespread surveillance and militarised police forces. One of the most overt and egregious examples can be seen in the recent use of an MQ-9 Predator drone for surveilling Black Lives Matter protests in Minneapolis. It is not known whether this drone was utilising the technologies developed in Project Maven. But nor is it hard to imagine.

### Link—Hacking

#### Hacking is a corporate tool used to control social realities – it’s intrinsic nature to the cybernetic system means the alternative is the only option

**Burkart 19** (Patrick Burkart, Asistant professor in the Department of Communication @ Texas A&M, “Why Hackers Win: Power and Distribution in the Network Society”, University of California Press, 2019, <https://www.academia.edu/38287801/Why_Hackers_Win_Power_and_Disruption_in_the_Network_Society?from=cover_page>) // EL

Contemporary geopolitics are in flux as their norms shift and institu- tions realign. Information increasingly is employed as both hard and soft power in struggles that cross the social and technical boundaries of long-standing networks. These struggles are central to what we term the “Network Society.”1 Why Hackers Win: Power and Disruption in the Network Society examines the pressures that have driven global law and policy into ambiguous territory. While many popular and scholarly accounts posit hacking as a means to wobble the trajectory of late capi- talism, we argue the inverse is true. Hacking (offensively through exploits and defensively through cybersecurity) extends and deepens state and corporate proclivities to control social realities. We define “hacking” as unauthorized trespass, breach, or bypass of “trusted sys- tems” for purposes of surveillance and potential theft, manipulation, or destruction of information.2 These systems are based on communica- tion networks in which service providers and users must be authenti- cated to access goods and services. Therefore, user trust in their secu- rity and reliability is essential.3 We focus on the hacking of trusted systems—and not other kinds of readily accessible systems—because the template for their protection has been refined in key areas of law, technology, and society. We posit hacking as a generalized symbolic medium, like power and money, which can be collected and mobilized to influence communica- tion systems. In the process hacking affords opportunities to bypass exist- ing law and policy through force. Our purpose in Why Hackers Win is to examine hacking as a corporate and state strategy for managing risk. Ulrich Beck claims that “being at risk is the way of being and ruling in the world of modernity; being at global risk is the human condition at the beginning of the twenty-first century” (2006, 330). Given the immense complexity of the Network Society, state and corporate actors seek greater self-awareness and certainty. Hacking enables these actors to seek out their blind spots in online boundaries and activities. This knowl- edge is valuable for maintaining systems and exposing risks. Hacking (offensively through exploits or defensively through cybersecurity) reflects common social impulses to survey, to measure, to model, and to predict. While hacking often is viewed as essentially disruptive to social structures, we argue the inverse is true. States and corporations seek to maintain their standing and seek competitive advantage through hacking campaigns. The creation of markets for exploits and cybersecurity also affords new opportunities to develop and exchange commodities. Conse- quently, to preserve national-security prerogatives and develop global markets for hacking technologies, states have resisted legal regimes to contain hacking by institutions—even as they have enacted draconian laws against hacking by individuals. We find that hacking and cybersecurity reinforce and accelerate each other in trusted systems. While ostensibly antagonistic, both increasingly share a common grounding in intellectual property. For hackers the value of hacking victims, or “data subjects,” is not so much in their personally identifiable information, which is gathered and com- modified by trusted systems. Instead, hackers exploit the “intellectual property” that gathers and commodifies this information within these systems to squeeze revenues through phishing and fraud. A secondary value is that hacking provides data for valuing insurance products and refining cybersecurity products already in use. In turn, cybersecurity offers possibilities for developing intellectual property in the military and civilian sectors, particularly in software and services. Both private security firms and state military and police forces claim to have evolved cybersecurity and cyber warfare into a “science,” in which knowledge and expertise are increasingly institutionalized in higher education and corporate management. Both markets and militaries view offensive hacking techniques (intrusion software like malware and botnets) and defensive countermeasures as new opportunities to generate power and money and manage risk. Much like the “dual-use” nature of exploits themselves and consist- ent with other domains in the Network Society, the boundaries between private and public are blurred and indeterminate. In the neoliberal era the economic system has assumed more and more responsibility for allocating risk through the market function of pricing, and the state has turned more areas of social welfare over to markets in an elaborated process of risk management and deregulation.4 Similarly, states increas- ingly outsource both hacking and cybersecurity as a means of manag- ing risk. Internet service providers perform state surveillance by proxy, and states (including the United States) frequently employ independent spyware and hacking firms to supplement their operations. Innovations such as insurance against corporate hacking and identity theft also reflect the commodification of hacking risks. When these responsibili- ties are outsourced to the market, risks are distributed in patterns that can reinforce social inequalities. The economy provides markets for risk management, but “with the economic exploitation of the risks it sets free, industrial society produces the hazards and the political potential of the risk society” (Beck 1992b, 23). Through all these means hacking represents an interface between technical code (the structure of trusted systems), legal code (the laws that govern their access and use), and social code (their impact on soci- ety, particularly in terms of privacy and sanctioned activity). As a grow- ing portion of the global economy is based in digital trusted systems, we find a proportional growth in the vulnerabilities inherent to these systems: the buggy software, the unprotected account access, and the availability of personally identifying information to others on the inter- net. Although hacking ostensibly undermines their own security, corpo- rations and states paradoxically use hacking for gain. Hacking can suit a broad spectrum of purposes, including gathering intelligence, managing crises, and accumulating competitive advantages over rivals. Some “exfiltration” hacks have successfully stolen data such as business plans, while some failed episodes have landed spies in jail (Landau 2013). The “hack-back,” an attempt by victims of cyberattacks to get into the hack- er’s computer, can try to ascertain the fallout from the initial breach, as well as knowledge about any new schemes and risks of future breaches. While examining abuses of power through computer vulnerabilities and exploits, we have not found “master conspiracies” of surveillance and espionage, or even a systematic imposition of will, in coordinated hack- ing campaigns. Instead, we see a proliferation of agents contributing to offenses and defenses played in long games and embedded in global net- works. In our view hacking has become a mundane, “business as usual” application of force for many enterprises. The development of hacking and cybersecurity together also fore- grounds paradoxes for social systems. Hacking is now integrated into state and corporate activities, especially where business or security interests are invested in maintaining trusted systems. Organizations may hack for advantages over rivals by exploiting vulnerabilities in trusted systems. At the same time organizations may hack their own trusted systems or invite others to hack them (sometimes called penetration testing or “pen testing”) for purposes of cybersecurity. “Red Team v. Blue Team” exercises take pen testing to active warfare levels— one team trying to break in while the other defends. (In cybersecurity gospel “Red team ALWAYS wins eventually. Blue just holds on as long as they can.”) “Red teaming” is embraced and institutionalized by the U.S. Department of Defense, where “in the cyber world, offense and defense stemmed from the same tools and techniques” (Kaplan 2016, 260). In all these scenarios hacking activity provides recursive knowledge about trusted systems and the communication systems in which they are embedded. In turn, these reflexive processes can exercise coercive force in these systems. Whether or not they encounter defenses, an exploit delivered through the right attack vector can contribute to cybernetic feedback loops within systems. These loops appear to be generated with increasing frequency, as hacking campaigns (or cyberat- tacks) proliferate together with mass data breaches. Our approach to technology foregrounds the role of human agents and institutions in communication. We argue that technologies are socially constructed rather than deterministic and autonomous. Not- withstanding the impact of technological change on the economy and society, even our most powerful technologies do not operate independ- ently of human controls such as market exchange, law, policy, and cul- tural norms. Why Hackers Win takes a sociological perspective on hack- ing, viewing it as one of many activities that constitute communication in social systems. If we view the cybernetic arena as a social system, hacking serves to differentiate the components of this system, which then adapts accordingly. The system as a whole is reconfigured, with consequences for political, economic, and legal systems, among others. Hacking and its codependent, cybersecurity, therefore contribute to encoding communication in social systems rather than undermining them. This idea is informed by Jürgen Habermas’s (1984, 1987) theory of communicative action and his dualistic “system and lifeworld” analysis of modern societies. Accordingly, hacking is related to digital piracy as a means of cultural reproduction (Burkart 2011, 2014). In the absence of a tightly regulated market for cybersecurity and component exploits, hacking has greater freedom to “steer” interactions between states, markets, and laws. If the legal system were to suppress the proliferation of commercial hacking tools and spyware, the risks perpetuated by cyber insecurity might improve. But the legal system is not designed to do this; in fact, it contributes to systemic risk by enabling legal or gray markets for vulnerabilities. We argue that the conjoining of intellectual property and cyber defense in copyright law and policy adds additional levels of risk for society as a whole. **This is in part because hacking and data breaches are not just episodic bugs; rather, they are routine and institutionalized features of the system.** The growth of cybersecurity software and related industries also impact these institutions and rou- tines, contributing social effects in the process. Although social-technical systems for media, business and finance, and defense are increasingly globalized, the nation-state still provides the basis for law and policy governing hacking. But the coherence and continuity of law and policy within nation-states can fall on a contin- uum from anarchic to totalitarian. Hacking therefore illustrates “gov- ernance in areas of limited statehood” (Risse 2013). The relative depend- ence or independence of hacking on law and policy can turn on a variety of factors. Why Hackers Win addresses cases where new laws on hacking have conflicted with both received policy traditions and emer- gent policy regimes and where hacking still occupies legal gray areas. Judicial review is not fully incorporated into many decision-making processes; broad categories of hacking remain the privilege of the state and therefore are exempted from the rule of law. Even hacking by pri- vate firms may be absolved by the state (such as when telecommunica- tions carriers received retroactive immunity from illegal wiretapping violations).5 Secrecy and self-regulation are the rule for states and firms, with little concern for values and norms for personal privacy. Numerous national and international legal systems have categorized piracy and hacking as cybercrimes, which has intertwined their history and led us to consider them as distinct but related aspects of communica- tive social action. As with piracy, the conflicts surrounding trusted sys- tems center on issues of ownership and control, based on the right to share private property or exclude others from access. It remains as unlikely today as it did in 2006, when we wrote Digital Music Wars, that a universal standard for digital-rights management will be adopted by even a single industry. But the reprising of digital-rights–management models for managing cybersecurity risks and the securitization of intellectual property in military cybersecurity policy suggest that guidelines for ntellectual-property theft will dominate discourse over how to define and prioritize cyber threats. We also anticipate that enterprises depend- ent on trusted systems will employ technology practices, legal activities, and political lobbying to strengthen pecuniary rights at the expense of the public good. However unjust they may be, “consumption norms” already have gelled for trusted systems—along with their bases in sur- veillance and intellectual property (Burkart 2010, 2014). In the aggregate of digital dirty tricks and the attack vectors that enable them, we find an unfolding, alternative history of technological development and its impact on society. We conclude our study with a reflection on the overt and covert applications of hacking and cybersecurity by states and cor- porations and the importance of research and activist groups in drawing attention to these activities. Without their efforts the question of who is responsible for guarding the public interest in the Network Society seems to answer itself: no one. The development of hacking and its dou- ble star, cybersecurity, offers another example of how ostensibly resistant technologies and practices may be contained, controlled, and repurposed to suit the instrumental purposes of state and corporate power.

#### Hacking is integral to digital capitalism – corporations lie to achieve surveillance

**Burkart 19** (Patrick Burkart, Asistant professor in the Department of Communication @ Texas A&M, “Why Hackers Win: Power and Distribution in the Network Society”, University of California Press, 2019, <https://www.academia.edu/38287801/Why_Hackers_Win_Power_and_Disruption_in_the_Network_Society?from=cover_page>) // EL

growth hacks The extent of corporate espionage (or “corporate intelligence”) through hacking is unknown, although Fortune 500 companies use it to maintain defenses against IP theft (Bailey 2016).19 As a byproduct of “digital capitalism” (Schiller 2000), hacking markets flourish at numerous levels (Burkart and McCourt 2017). In addition to markets for exploits and packaged cyber-defense tools, other “growth areas” include insurance against corporate hacking and identity theft (whether these insurance products add or reduce risk is another question). Markets for risk can diminish trust in social and sociotechnical systems, resulting in what Jürgen Habermas (1975) terms a “legitimation crisis.” Although attempts to offload risk have worked for now, we can already see how legitimation problems in cybercrime law and policy are converging with escalating social risk toward catastrophe. As Ulrich Beck proposes, “risk is not synonymous with catastrophe. Risk means the anticipation of the catastrophe. Risks concern the possibility of future occurrences and developments; they make present a state of the world that does not (yet) exist. Whereas every catastrophe is spatially, temporally and socially determined, the anticipation of catastrophe lacks any spatiotemporal or social concreteness” (2009, 9). We address the institutional shaping of social norms in the next chapter. Three cases, in which transnational corporations hacked trusted systems to engage in deceptive and anticompetitive behavior, illustrate the way in which “growth hacks”—a Silicon Valley euphemism “that describes breaking legal or moral rules in a quest for scale” (Roberts 2017)—have migrated from start-up culture to big business. We distinguish growth hacks from “deep hacks” (see chapter 2), which can emanate from outside the marketplace and which reverberate through the systems of technology, law, and society. The first example of a growth hack involves Uber Technologies, which secretly built the Greyball and Hell software tools into its drivers’ smartphone app, enabling the company to operate in markets where its services had been restricted. Uber’s Android rider app “phoned home” to send sensitive user data back to the company (Khandelwal 2014). News Corporation (News Corp) hacked voice-mail accounts and intercepted private communications to generate sensationalized stories for its News of the World tabloid newspaper—which it then tried to cover up. Finally, Volkswagen’s software hack was created to mask excessive emissions by their diesel vehicles, in clear violation of environmental protection rules in the United States and abroad, even as the company sued researchers who had discovered a way to hack its vehicle’s locks. These examples illustrate the ways in which corporations have relied on hacks of trusted systems as a standard business tactic while sometimes using antihacking law to slow discovery of vulnerabilities in their own systems.20 Uber has a particular “reputation for ruthlessness” (Estes 2017). Its business model, based on a trusted-system software platform shared by drivers and users, uses real-time surveillance to match rides more efficiently than taxicabs. To expand into areas where its operations were prohibited, in 2014 the company surreptitiously added the Greyball function to its smartphone app for riders. Greyball allowed Uber to identify and evade potential authorities through practices such as “geofencing,” in which a digital map would locate city government offices and enable drivers to avoid riders from those areas. Besides deceiving regulators, Greyball also allowed Uber to survey social media and mine credit card databases to identify and flag potential government or police employees (Isaac 2017, A1). Another module on the driver app, known by Uber executives and engineers as “Hell,” allowed the company “to track drivers using its biggest competitor in the US, Lyft, and to monitor which of Lyft’s drivers also drove for Uber” (Cook and Price 2017). The Hell and Greyball programs exploited the surveillance features of smartphones on both sides of its platform—driver and rider—to seek anticompetitive advantage in labor markets for drivers and to evade government regulations. Although these deceptive growth hacks contributed to Uber’s business plan by adding scale to its overall market, they also added to a growing list of legal problems (including sexual harassment and antilabor practices) attributed to Uber’s former management. As of this writing, the company is under investigation by the U.S. Department of Justice for Greyball and by the FBI for both the Greyball and Hell initiatives. But Uber remains “unrepentant.” The firm’s response to getting caught deploying Greyball was to denigrate the public investigators and law enforcement who caught them, while at the same time implying that Uber was entitled to pursue hacking its employees’ and customers’ phones as a proprietary business strategy. It employed a classic hacking rationale to protect its trusted system (its private property) from trespass (theft): “This program denies ride requests to users who are violating our terms of service, whether that’s people aiming to physically harm drivers, competitors looking to disrupt our operations, or opponents who collude with officials on secret ‘stings’ meant to entrap drivers,” an Uber spokesperson stated (Estes 2017). Uber was itself breached, as evidenced in May 2014, when two sellers on the anonymous Tor network offered thousands of Uber usernames and passwords that would allow buyers to log in and book rides (Gibbs 2015b). Uber first issued a denial, but in November 2017 the company admitted that it had hidden the breach, in which fifty-seven million driver and rider accounts were stolen from a third-party server, for over a year. After paying a $100,000 ransom, Uber tracked down the hackers and pushed them to sign nondisclosure agreements forbidding them to tell regulators or users that the information was stolen. The company then concealed the ransom by calling it a “bug bounty,” in which hackers are hired to test the security of systems (Isaac, Benner, and Frenkel 2017, B1; Larson 2017b). Yet, as the New York Times noted, “The issue is not legally clear cut. Laws concerning bug bounties are ambiguous. The Justice Department weighed into bug disclosure programs for the first time in July and largely left it to organizations to decide what access they will authorize for hackers and what they can do with the data. . . . Breach disclosure laws also differ state to state. The state laws most relevant to Uber’s case require disclosure if names are exposed in with driver’s license numbers in a ‘breach of security’” (Perlroth and Isaac 2018, A1).21 At News Corp illicit hacking teams appear to have operated regularly under the direction of its board of directors and subsidiaries, depending on the business needs of the day. To bolster readership of News Corp’s well-known tabloids, its journalists have turned to innovative means of gathering information, including brute-force password hacking of voice-mail boxes to access and delete messages. One voicemail box belonged to a teenage UK girl at the center of a missing person’s case, who was later discovered murdered; others belonged to victims of 9/11. A former News of the World employee (Paul McMullan, deputy features editor) offered a wildly bent rationale for his team’s illegal phone hacking. He claimed that surveillance and privacy violations are necessary to acquire exclusive sources for any story: “Phone hacking is a perfectly acceptable tool, given the sacrifices we make, if all we’re trying to do is get to the truth. . . . Privacy is for pedos” (qtd. in Lyall 2011). By 2017 News Corp’s newspapers had settled with more than a thousand phone-hacking victims (Ruddick 2017). That same year News Corp’s News Group apologized in court to a former British intelligence official whose computer had been infected with eBlaster spyware by a “private investigations” firm operating under News Group’s direction (2017a). The legal record strongly suggests that hacking for business advantage is normal operation in News Corp’s TV distribution division as well. Although the company claims to have disproved all allegations of illegal hacks, their extensive computer hacking, including that in the service of “predatory piracy” (Sauer and Tepper 2008), has been traced to roughly 1997. Four separate lawsuits, accusing News Corp firms of hacking copy-protection schemes, revealed a News Corp team dedicated specifically to developing such “black ops” in support of its DirecTV operations. Following a 2011 shareholder action against the company, a court found News Corp’s subsidiary NDS guilty of hacking Vivendi and Echostar TV smart cards and recruiting hackers to distribute counterfeit NagraStar cards to pirate Dish Network signals, beginning in 1997. Specifically, NDS “was accused by satellite company EchoStar of illegally extracting software code from competitors’ cards and posting the information online, allowing hackers to create counterfeit cards that could be used to intercept television programming. A federal jury found that NDS’s practices were illegal and the court subsequently granted EchoStar an injunction preventing NDS from intercepting its satellite signal” (Pilkington 2011). NDS won on appeal to the U.S. Ninth Circuit Court in 2010 and eventually collected $18 million from EchoStar. But in the testimony a witness claimed to have been paid more than $20,000 in cash concealed in CD and DVD players from HarperCollins (a News Corp division) to “develop a pirating program to make DirecTV more secure, not to sabotage rival systems” (Zetter 2008). Researchers have noted that News Corp’s News America Marketing division “has been the subject of five lawsuits alleging anti-competitive behavior . . . [forcing] the company to pay out more than $650 million in settlements to three competitors” (Longstreth and Hals 2011). One suit involving a competitor, Floorgraphics, claimed that “on at least eleven separate occasions between October 2003 and January 2004, News intentionally, knowingly and without authorization breached FGI’s secure computer system and repeatedly accessed, viewed, took and obtained [Floorgraphics’] most sensitive and private information concerning its past and upcoming advertising and marketing programs” (Edwards 2009).22 News America Marketing settled the lawsuit by purchasing Floorgraphics’ contracts midtrial, before the company had finished presenting its case. The claims involving News Corp cluster around breaches of trusted systems, for corporate espionage (theft of intellectual property), hacking news makers and public officials, and circumventing digital-rights management (conditional access controls for competitors’ satellite TV channels). Their pattern begins with News Corp–owned (or majority-owned) companies instigating hacks against competitors, continues with defensive litigation, and typically resolves with a corporate takeover, settlement, or (in the case of News of the World) restructuring.23 As UK regulators evaluate the Murdoch dynasty as “fit and proper” in News Corp’s bid for total ownership of Sky (Sweney 2017), its hacking victims have undermined News Corp’s claims that its standards and practices are, to use British military parlance, tickety-boo. Volkswagen’s software hack enabled cars marketed as “clean diesel” vehicles to “pass” emissions tests despite dirty exhausts, and its discovery triggered international regulatory reforms for car emissions. Installed inside the car, Volkswagen’s defeat device informed the emissions-testing computer when a testing cycle was activated and changed the vehicle’s emissions accordingly. Researchers at West Virginia University discovered cars with hacked chips emitted pollutants almost forty times what was allowed by U.S. regulations (Glinton 2015). After pleading guilty to federal fraud and conspiracy charges, Volkswagen paid $15 billion in fines for software installed in cars made from 2009 to 2015 (McCarthy 2017). It also agreed to compensate individual owners and repair all affected models. An engineer pled guilty to participating in the scheme and was sentenced to a forty-month prison sentence in 2016. New York and Massachusetts attorneys general have pursued a civil case against Volkswagen, claiming that “this was a widespread conspiracy involving many, many people,” including the company’s CEO, who resigned when the scandal went public (Isidore 2016). At the time of this writing, German authorities arrested and held the CEO of Volkswagen’s Audi branch for over three months in an ongoing criminal investigation into emissions-test cheating. With the discovery of its “defeat devices,” Volkswagen found itself on the wrong side of its own hack. But Volkswagen was not charged with creating and deploying defeat devices; it was instead charged with conspiracy to defraud the United States and its customers and to violate the Clean Air Act. However, two years prior to the emissions-hack revelations, Volkswagen sued Flavio Garcia, a computer science security researcher at the University of Birmingham (and his team), to prevent disclosure of a vulnerability in the antitheft system of some Volkswagen vehicles, including high-end sports cars. In this case Volkswagen asked the UK government to censor research findings that the wireless autoignition system was easily hackable by thieves or others with criminal intent. The lawsuit prevented Garcia and his team from presenting their findings at the USENIX Security Conference in Washington, DC, in August 2013 (Trotman 2013).24 Publication of the research (Garcia, Verdult, and Ege 2013) was delayed two years by the suit but was soon followed by a new paper, whose findings were even more serious (Garcia et al. 2016): “Volkswagen left not only its ignition vulnerable but the keyless entry system that unlocks the vehicle’s doors, too. And this time, they say, the flaw applies to practically every car Volkswagen has sold since 1995.” These cars numbered about a hundred million units. With Volkswagen’s security system disclosed as a potential attack vector, the company faces extensive recalls and repairs and possibly other large expenditures related to the vulnerability (although none are reported at the time of this writing). The hack used a cheap, off-the-shelf microcomputer kit (called an Arduino). The suit against the Birmingham researchers raised concerns that the company may have known about the security vulnerability for years. The chip manufacturer that served Volkswagen and other companies noted that VW’s chip uses “a legacy security algorithm, introduced 18 years ago. . . . Our customers are aware” (Greenberg 2016). The UK court’s 2013 order against Flavio Garcia’s team quashed the news of the vulnerabilities and placed an embargo on their publication. The ruling reduced VW’s short-term financial risk in the conflict but potentially increased security risks to the public through vulnerabilities that were known but unfixed for at least two years. These three cases of corporate “growth hacks” are known through their failures; we must ask how many other cases –successful or not— have gone undiscovered and unreported. Each company has offered a unique response to its resulting public-relations nightmare. Volkswagen launched advertisements titled, “Keeping Your Promises” with the tagline, “It’s more than just a car. It’s keeping your promises” (Slater 2016), a campaign seemingly designed to exploit audience ignorance or shortterm memory loss. News Corp’s Rupert Murdoch (sort of) apologized to the family of the dead thirteen-year-old girl whose voice mail was hacked: “As the founder of the company, I was appalled to find out what happened” (“Murdoch Begins” 2011). Uber claimed to have deployed Greyball in charity, “because it was ‘deeply concerned that its driverpartners would be penalized financially’ or otherwise for their driving” (“Uber Faces” 2017). The cases of Uber, News Corp, and Volkswagen share a corporate realpolitik: turnabout is fair play when hacking is part of corporate strategy. Hack your customers, your employees, your competitors, your regulators, and, if expeditious, retaliate if you’re hacked. Deny, disclaim, or even cover up as needed, and offer a counternarrative for plausible deniability. Use antihacking law to your advantage if others find bugs in your trusted systems. None of these cases demonstrates negligence as clearly as they demonstrate hubristic anticompetitiveness. As giant corporations caught abusing trust, their growth hacks add social risk, complexity, and extra layers of secrecy and suspicion to the economy, politics, and the law. They signify the impetus to manipulate trusted systems, a form of “soft power,” to compete for advantage. A hacker’s successful exploit of a trusted system is not the sort of news willingly shared by a company whose reputation and business depends on that system. News of hacking cases bubbles up from industry trade magazines, hacker forums, security email listservs, and other sources removed from the business pages of newspapers and magazines. Hacking tools and techniques allow states and corporations to manipulate sociotechnical systems for advantage, sometimes illegally through outright fraud but more commonly through legal “gray zones.” Nurtured by legal fictions, aporias, and other vagaries, hacking can blur the boundaries between military and corporate intelligence programs, between national and international legal systems, and between corporations and clients. Hacking can catalyze changes in multiple domains and across related subsystems, often in a “cascading” fashion that can escalate the scale of their effects (Landau 2013, 160). Since interconnected networks increasingly are essential to the state’s political and economic functions, they are considered to be among the state’s strategic defense interests. Yet national legal regimes are riddled with inconsistencies that reduce their effectiveness in coordinating social systems and may even exacerbate social risks of hacking.

### Link—Humanitarianism

#### Thinking is over. Hello calculation. The global computational turn renders the affs attempts to retract international imperialism a farce of modern technocapitalism. Empire no longer operates through traditional statecraft or <insert affs mechanism> but rather through the ontopolitics of adaptive design, a recourse to remote management and interconnected digitized finance as a means of simultaneously eliminating and recreating precarity. This design principle is the zeitgeist of late modernity and makes global interventions and security crises inevitable.

Duffield 19 (Mark Duffield is Professor Emeritus and former Director of the Global Insecurities Centre, University of Bristol, and an Honorary Professor at the Humanitarian and Conflict Response Institute, University of Manchester., Post-Humanitarianism: Governing Precarity Through Adaptive Design) //ansel

The War on Terror imposed limitations. Compared to the 1970s and 1980s, humanitarian agencies found their political room for manoeuvre significantly restricted (BOND, 2003). At the same time, despite agency growth and extensive efforts to professionalise relief work, there was little commensurate increase in effectiveness (Fiori et al., 2016). Growing risk aversion and **recourse to** **remote management**, moreover, **created problems of distancing** and loss of familiarity (Healy and Tiller, 2014). Distracted by debt-fuelled uncertainty, rather than an indignant citizenry, Western publics now present as so many disillusioned, ironic spectators (Chouliaraki, 2013). Diplomatic influence has also declined (Mair, 2013). While NGOs lay claim to a ‘nongovernmental’ status, direct action thrived when **donor sovereignty** was, paradoxically**, still able to cast a shadow**. Given the refugee crisis, few can today contemplate the wretched state of ‘official’ humanitarianism without some disquiet. Despite what we may wish or demand, however, it is unlikely that significant improvement will occur any time soon. But to then conclude that humanitarianism is dead would be a mistake. While autonomous international direct action lies buried in the rubble of the West’s urbicidal wars, a new optimistic, less direct but technologically updated humanitarianism has confidently stepped forth. More de-risked and requiring less professional expertise than the labour-intensive direct engagement of the past, it is a cheaper Western humanitarianism designed for connectivity rather than circulation. Often called humanitarian innovation (ALNAP, 2009; Betts and Bloom, 2014), a feature of **this new humanitarianism is its enthusiastic embrace of adaptive design** (Ramalingam et al., 2014; HPG, 2018). Moreover, unlike autonomous direct action, which reached its peak in the late 1980s**, humanitarian innovation sits comfortably with private partners and corporate sponsorship** (Zyck and Kent, 2014), **a** necessary **recalibration given its dependence upon what can be called the computational turn** – that is, since the 1990s, **the seamless penetration of commercial information and communication technologies, software platforms, automating apps and screen interfaces into all aspects of personal, social, national and international life** tout court. **Humanitarian innovation is politically safe, logoed, glitzy and smart**. Besides establishment acceptance, humanitarian innovation draws positivity from its disavowal of past failures and commitment to a future of ‘failing-forward in a spirit of honesty’ (HPG, 2018: 132). Transparency regarding current systemic ‘pathologies’ like **institutionalising selfinterest** or neglecting the agency of the disaster-affected (ibid.: 22–3) **is part of the self-cleansing necessary to birth a humanitarianism** 2.0. This paper, however, questions whether humanitarian innovation can be any more effective than the past relief efforts it now disavows. Rather than system failure, just as important is that the world has changed. Societies are more fragmented and unequal than before (Piketty, 2014). International space has striated into fast, slow and stopped lanes (Brown, 2010) as debt, precarity and anger have flourished (Mishra, 2017). **Rather than correcting past mistakes, humanitarian innovation is embarked on a wholly different project**. **It is helping create the systems and structures to govern global precarity**. **Important here is its privileging of the design principle over** the need for, or even **the possibility of, political change**. Design Not Politics **The computational turn and societal dependence on digital technologies has changed the way the world is understood and the status of humans within it** (Chandler, 2018). The privileging of the design principle is central to this change. **Besides the spatial shift from circulation to connectivity, an ontological, epistemological and methodological translation has also taken place** (Duffield, 2018). While anticipating late-modernity, the spirit of 1970s direct humanitarian action was fabricated from a deductive process of knowledge formation framed by narratives of history, causation and reciprocity. Reflecting the rise to dominance of a cybernetic episteme, **this register has been replaced by a reliance on inductive mathematical data and machine-thinking for sense-making** (Rouvroy, 2012). **Thinking has been transformed into calculation** (Han, 2013).1 The current dominance within the academy of empiricism and behaviourism reflects this change in world-experience. What is often called post-humanism (Braidotti, 2013) brings several contemporary positivist stands together. These include the new empiricism, speculative realism and actor network theory. Posthumanist thought draws on process-oriented behavioural ontologies of becoming. These privilege individuals understood as cognitively limited by their unmediated relationship with their enfolding environments (Galloway, 2013; Chandler, 2015**). An individual’s ‘world’ reduces to the immediate who, where and when of their changing network connections and disconnections**. The overlap here with neoliberalism’s necessarily ignorant subject is returned to below. Importantly, the pure factuality of **a post-humanist existence casts doubts on the distinction between a lived reality and a wider world**, **a distinction that is central to knowledge and the narrative of history**. **Without this separation there is no space**, as it were, **for a political commons of contrasting life-chances, contestation and critique that is essential if we are to successfully share the world with Others**. In its absence, as Bruno Latour approvingly argues, the whole becomes smaller than the sum of its parts (Latour et al., 2012). **Rather than a shared world of circulation, we have the endless personalised and separate worlds of connectivity**. Post-humanism problematises the possibility of a shared or collective politics. Indeed, Latour (Latour, 2008) goes further in suggesting that **design has now replaced politics**. Building on his earlier rejection of grand narratives and critique (Latour, 2004), Latour claims that since encountering the scale of the ecological crisis, we are all now designers rather than modernisers. Across a wide arc of operational discourse, empathetic design attitudes reflecting such feminine sentiments as ‘attachment, precaution, entanglement, dependence and care’ have all but replaced earlier, more masculine Promethean commitments to ‘emancipation, detachment, modernization, progress and mastery’ (Latour, 2008: 2). **In place of political change**, **Latour asserts the primacy of a conservative design-based ontopolitics**. That is, the need to accept and work with the world as is – rather than how it ought to be. In celebrating the positive demand for empathy, humility and resilience, **adaptive design supplants the call for systemic change**. This conservatism 16 is an example of how a progressive neoliberalism (Fraser, Journal of Humanitarian Affairs (2019) 1/1 Downloaded from manchesteropenhive.com at 04/06/2019 01:04:08AM via free access 2017) is dissolving and sapping the powers of resistance (Han, 2010). **The excessive positivity of adaptive design, its endless willingness to happily fail-forward into the future, suits the economic logic of late-capitalism**.2 To draw this out, it is necessary to first review the latter’s greatest achievement. **Global Precarity A characteristic of late-modernity, at least in relation to the global North**,3 is what Nikolas Rose has called the ‘death of the social’ (Rose, 1996). This demise is usually equated with the roll-back of the welfare state. Originally meant as a collective insurance-based shield against market forces, since the 1980s the welfare state has been residualised through means-testing, privatisation, cuts and the politics of austerity. Companies and businesses, however, have also shed their former social-democratic responsibilities (Boltanski and Chiapello, 2005). Jobs for life, intergenerational career structures, apprenticeships, subsidised canteens, social clubs, sports facilities and company pensions have disappeared. In the mid twentieth century, for the white working class at least, welfarism together with a Fordist employment culture provided a high degree of protection against market forces. Indeed, this was a defining political feature of the West’s racial- and gender-inflected Cold War socialdemocratic settlement (Streeck, 2017). Over the last two or three decades, driven by the neoliberalism of the conservative counter-revolution, this social protection has largely evaporated. Insurance- and company-based social protection has historically been limited or absent in the global South. Late-modern precarity begins here first (Munck, 2013). Encouraged by the imposition of structural adjustment, the South’s informal economies began to rapidly expand from the end the 1970s, absorbing the surplus population thrown off as public-sector employment and services contracted (Cornia, 1987). Moving to catch up, so to speak, by the 1990s a ‘post-social’ economy was consolidating in the global North. While marked differences remain, **the North and South have drawn together around the economic logic of precarity**. In the latter, fuelled by jobless growth, for several decades a selfreproducing informal sector has been by far the largest employer and supplier of goods and services (Meagher, 2016). **For the North, precarity has taken the form of the disappearance of ‘good’ jobs as the casualisation of work has increased**. This includes the growth of insecure, poorly paid temporary work and marginal forms of selfemployment (TUC, 2017). Wages have stagnated, and social mobility stalled. Moreover, it is widely accepted that today’s young no longer enjoy the life chances of their parents (Corlett, 2017). Given this downturn, living the dream has meant a massive expansion of debt financing (Streeck, 2017). The acceleration of economic informality in the global South has been matched by the residualisation of market protection in the North. As this conjuncture suggests, the greatest achievement of late-capitalism has been to author an expanding post-social global precariat. While progressive neoliberalism celebrates the exchange of ‘nanny-state’ security for a contingent freedom to consume (Boltanski and Chiapello, 2005), latecapitalism is fraught with contradictions. Reversing a hitherto world-historical trend, since the ‘long boom’ ended in the 1970s there has been a secular decline in the rate of profit. Every recovery from the periodic business cycle has, from this period, been feebler than the last (Brenner, 2006). Recovery from the 2008 financial crisis, for example, has been the weakest and most prolonged on record (Streeck, 2017). Reflecting the realities of the downturn, the new freedom to consume has, to a remarkable degree, been unequally distributed (OECD, 2008; Oxfam, 2016). Precarity is a by-product of the long downturn. It emerges at that historic moment when the economy becomes a site of permanent emergency (Streeck, 2011). A human surplus coexists with the ‘jobless’ growth resulting from the systemic urge to deepen automation at a time of declining profitability (Smith, 2017). **Within a post-social world, risk and security have been individuated**. Compared to the normative welfare systems of the past, **a new disaggregated and personalised biopolitics has emerged**. If biopolitical regimes could be likened to animal species, the welfare state catered for the herd. Today, it is the turn of the predator. 4 Rather than share risk, there is a new emphasis on individual responsibility. In the global North, the downturn has spawned a narcissistic culture of bodily fitness, healthy lifestyles and making good choices, while **in the South, a post-humanitarian ethic has disaggregated, medicalised and reduced precarity to the basic nutritional, energy, health, sanitation, education, financial and psychic requirements needed to maintain bodily functioning** (Jaspars, 2015). Everywhere, **resilience**, **or the injunction to endlessly adapt before unmediated market and environmental forces, has become the zeitgeist of late modernity** (Evans and Reid, 2014). As the uncertainty of active unemployment becomes the global work norm, the chronically poor and the disaster-affected have blurred. In an unmediated relationship with their environments, they are both subject to permanent emergency. They constantly change place and, at a time when economy and disaster have blurred, from a post-humanitarian perspective, they become indistinguishable. Since resilience is now equally required of the poor and exposed – as well as the ‘first Post-Humanitarianism 17 Downloaded from manchesteropenhive.com at 04/06/2019 01:04:08AM via free access responders’ – the traditional distinction between developmental and humanitarian relief has also lost its meaning. Disasters are developmental; so development has been set the task of re-wilding a post-social world. **Within the economic logic of precarity, however, the global South has a special place**. Able to utilise the relatively unregulated conditions existing there (Hosein and Nyst, 2013), rather than eradicating poverty, **the role of humanitarian innovation is to experiment, trial and anticipate the means to govern an emerging global precariat** (Jacobsen, 2015). In particular, the challenge is to sustain precarity in the sub-prime conditions of the South by optimising its social reproduction. Having devoured, since the 1970s, the last areas of economic and institutional autonomy still outside of itself (Sloterdijk, 2013), other than profitably recycle the precarity it now produces in abundance, so to speak, late-capitalism has no other future.

### Link—Innovation\*\*\*

#### \*\*\*Note while prepping: These cards also serve as DOD links

#### The affirmative’s need for militaristic innovation upholds the drive for capital investment in harmful technologies

**Wilson 20** (Neil Wilson, Master’s at Utrecht University, “Understanding the Battle for AI in Warfare through the Practices of Assemblage: A Case Study of Project Maven”, Utrecht University, 8/2/20, <https://studenttheses.uu.nl/bitstream/handle/20.500.12932/37392/Neil%20Wilson%20MA%20Thesis%20%281%29.pdf?sequence=1&isAllowed=y>) // EL

4.1.1. Military-Technological Complex “To overcome challenges to our military superiority,” declared the US Secretary of Defense Chuck Hagel in 2014, “we must change the way we innovate, operate, and do business.” Noticing tides of change lapping at his feet, Hagel recognised that new ways of war required new ways of business. From his perspective, the problem of AI in defence was one of access: the technology existed, but was out of reach of the DoD. Cooperation with new industrial partners would be essential to developing these new technologies and, in turn, maintaining American military superiority. To understand why the Department of Defense needed to forge new alignments with industry, it helps to consider previous practices of military research and development (R&D) and their (un)suitability for purpose. In the post-WWII era, a “Military Industrial Complex” emerged among the civilian industrial conglomerates (e.g. Boeing and General Motors). Simultaneously, significant public investments into military R&D boomed and led to several technologies now commonplace in the civilian sphere, such as GPS. In fact, this cross-pollination of public funding and technological innovation between the military and civilian spheres transformed Silicon Valley’s from a “landscape of fruit orchards into a hub of electronics production and innovations.” At the conclusion of the Cold War, the Military-Industrial Complex lost its raison d’etre. Fifty-five billion dollars of acquisitions and mergers followed, as many engineering companies parted with their defence businesses, consolidating the defence industry into five “titans.” Concurrently, DoD procurement practices became cumbersome and convoluted, resulting in $46bn wasted between 2001 and 2011 on weapons systems that never entered production. Most acquisition programes took years or even decades to reach the battlefield. Tightening belts and a slow production line blunted the technical edge of the Military-Industrial Complex. Today, most R&D investments are dominated by the private sector. By 2014, when Hagel announced the Third Offset Strategy, it was clear that digital technologies were the future of defence. As the leader of Project Maven Jack Shanahan noted, “the future battlespace is constructed of not only ships, tanks, missiles, and satellites, but also algorithms, networks, and sensor grids.” Hagel obliquely referred to LAWS with his warning that the US army “could one day go into battle confronting a range of advanced technologies that limit our freedom of maneuver.” Deputy Secretary of Defense Bob Work, by contrast, was more explicit: “10 years from now if the first person through a breach isn't a fricking robot, shame on us” Moreover, the official DoD directive on LAWS declared its intention to develop autonomous weapons with “appropriate levels of human judgment” that would satisfy “the law of war, applicable treaties, weapon system safety rules, and applicable rules of engagement.” From this, it appears the problem was perceived not in the technology itself but in developing it to a certain standard. It could not do so alone. Technological innovation took centre stage in the Third Offset Strategy but would require new actors, by Hagel’s own admission: “[The] DoD no longer has exclusive access to the most cutting-edge technology or the ability to spur or control the development of new technologies the way we once did. So we will actively seek proposals from the private sector… those firms and academic institutions outside DoD’s traditional orbit.” Technology companies, by contrast, were not as public in their intentions of working with the DoD. Despite Silicon Valley’s government-funded roots, its radically different working culture of “disruption” and willingness to “fail fast, fail often” were institutionally alien to the DoD. Beyond these normative issues, many technology companies regarded the Pentagon as too small a customer to work with, especially given the bureaucracy involved. Similarly, the huge sets of training data required to make useful machine-learning algorithms are hard to come by for defence purposes. Notably, well before Project Maven was even established, Google was making significant inroads in robotics development but appeared unwilling to work with the Pentagon, however it was unclear whether this was driven by ideological or market considerations. Nevertheless, it was clear that for many tech companies the problem was perceived in a technical manner similar to the DoD: the issue was not necessarily developing the technology but establishing the partnerships.

#### Innovation is unsustainable – the DOD’s pursual of the private industry and dismissal of technological expertise proves their sole intent is capitalist superiority

**Wilson 20** (Neil Wilson, Master’s at Utrecht University, “Understanding the Battle for AI in Warfare through the Practices of Assemblage: A Case Study of Project Maven”, Utrecht University, 8/2/20, <https://studenttheses.uu.nl/bitstream/handle/20.500.12932/37392/Neil%20Wilson%20MA%20Thesis%20%281%29.pdf?sequence=1&isAllowed=y>) // EL

4.2.1. Military-Technological Complex From the Third Offset Strategy, AI technologies were clearly considered imperative to maintaining American military strength. Incapable of mandating cooperation between private industry and the military, however, the DoD had to rely on persuasion rather than coercion to acquire the technologies it sought. Accordingly, the “solution” for the DoD appeared to be becoming better in building relationships with contractors. And so it began courting tech companies with new contracting processes. In April 2015, then-Secretary of Defense Ash Carter delivered a speech at Stanford University - the first visit to Silicon Valley from a Secretary of Defense in twenty years. Centred around innovation, the speech culminated in the announcement of the Defense Innovation Unit Experimental (DIUx). This new DoD body, located in Silicon Valley (“a nexus of innovation”), would work to “strengthen existing relationships and build new ones; help scout for new technologies; and help function as a local interface for the department.” In addition to the DIUx, the Defense Innovation Advisory Board (DIB) was established the following year. This collection of Silicon Valley luminaries, chaired by Eric Schmidt (formerly of Alphabet Inc., the parent company to Google), were assembled to provide the Pentagon access to “the brightest technical minds focused on innovation.” Drawing industry voices like Schmidt into the assemblage suggested that with the right expertise, the challenges of developing AI for defence could be overcome. The role of the DIB in legitimising the DoD’s endeavours in this field will be elaborated in the following chapter: authorising knowledge & managing failures. Forging alignments with tech companies accelerated dramatically in 2017 with the creation of the Algorithmic Warfare Cross Functional Team (AWCFT). Better known as Project Maven, the AWCFT sought “to accelerate DoD's integration of big data and machine learning… to tum the enormous volume of data available to DoD into actionable intelligence and insights at speed” Specifically, its goal of automating the “Processing, Exploitation and Dissemination [PED] for Tactical Unmanned Aerial Systems” meant using Machine Learning to automatically analyse drone footage for objects of interest, freeing up human analysts for higher-level work. It is important to note that those leading Project Maven in the DoD were not selected on the basis of technological expertise but their skill in building relationships. Although the role of Google was not public at this early stage, a public “industry day” hosted by the DoD in October 2017 was attended by more than 300 industry and academic partners - a clear sign of DoD enthusiasm for forging alignments with the tech industry. Beyond the concrete goals of Maven, it had an important underlying purpose as a “pathfinder” mission, the “spark that kindles the flame front of artificial intelligence across the rest of the [Defense] Department,” according to its leader Lt. Gen. Jack Shanahan. Its founding memo emphasised agility: “after successful sprints in support of Intelligence, Surveillance, Reconnaissance (ISR) PED, the AWCFT will prioritize the integration of similar technologies into other defense intelligence mission areas” (emphasis added). The Pentagon was thus framing the solution as being to move faster and work closer with industry in adopting and integrating algorithmic technologies. For the DoD, then, just as the “problem” of integrating AI technologies was a logistical one, the proposed solution was equally practical. Initiatives like the DIUx, DIB and Project Maven indicated that with enough energy and skill, it could forge the necessary alignments with tech companies to acquire these technologies. Elements gathering around the problem of AI in defence from this perspective were thus already crystallising as its solution - closer cooperation.

### Link—Remote Warfare

#### The affirmative’s obsession with the efficiency of remote warfare mystifies conflict into a “war without bodies” entrenching a cycle of violence

**Wilson 20** (Neil Wilson, Master’s at Utrecht University, “Understanding the Battle for AI in Warfare through the Practices of Assemblage: A Case Study of Project Maven”, Utrecht University, 8/2/20, <https://studenttheses.uu.nl/bitstream/handle/20.500.12932/37392/Neil%20Wilson%20MA%20Thesis%20%281%29.pdf?sequence=1&isAllowed=y>) // EL

2.2. Remote Warfare The best indication of warfare’s near future can be found in its recent past. With this in mind, LAWS can be contextualised by the ascendancy of “remote warfare.” Defined as “a strategy of countering threats at a distance, without the deployment of large military forces,” remote warfare takes a variety of forms, including the use of technological (e.g. drones) or physical (e.g. partner forces, private military contractors) proxies. By considering remote warfare from strategic-political and tactical-technological perspectives, LAWS can be considered a natural continuation of technologically-enabled warfighting among risk-averse Western states. The technologies of remote warfare - particularly drones - cannot be fully understood without attending to the strategic and political impetus for their use. “Stand-off” warfighting runs deeper than any single technology. At the turn of the millennium, Ignatieff’s analysis of the “Virtual War” in Kosovo noted that Precision-Guided Munitions (PGMs) promised “speedy, risk-free victory.” Contemporaneously, others noted the ascendancy of of “riskless x warfare” and “risk-transfer militarism” establishing a trend towards the asymmetrical deployment of force in Western Military operations. Patterns of risk-aversion among Western forces observed at the turn of the millennium have since accelerated. A combination of past failures, budgetary constraints, and increased political and popular scrutiny mean Western militaries exercise even greater caution in their troop deployments today. Risk-aversion has not precluded military engagement entirely, but has prompted states to consider alternative means of projecting influence without committing large ground forces. In his conceptualisation of “vicarious warfare,” Waldman therefore notes the pre-eminence of delegating force (to proxies and partner forces) and danger-proofing personnel (through airstrikes and remotely-piloted weapons systems) in contemporary military interventions. Delegation and danger-proofing respectively constitute the social and material forms of mitigating risk to US troops. Similar dynamics have been observed among other NATO members. Put simply, the strategic appeal of remote warfare is perceived as efficiency: risking less and achieving more. From a tactical perspective, the efficiency engendered by remote warfare was made possible by technological innovation. For this reason, a burgeoning field of scholarship has emerged around the technologies of remote warfare, particularly drones - “the most visible application of the information age to contemporary warfare.” Chamayou’s seminal treatise on Drone Theory takes an expansive look at the political, ethical and legal implications of drone warfare, concluding that “remote war is a war of human machines against the human body… one side loses people; the other side loses toys.” While this analysis does consider the human impact of this technology, it remains overwhelmingly focused on the drone itself. Some argue this “fetishisation” of drone technologies (predominantly by military actors but also in academia) mystifies their human relations. Myopic focus on technologies alone thus risks presenting a false image of “war without bodies.” Scholars of remote warfare are not alone in their tendency to perceive technology deterministically. Despite the centrality of technology to IR, its study too-often assumes it is either entirely controlled by humans or distinctly separate from human agency. In line with Latour’s concept of the Black Box, “technical work is made invisible by its own success,” leaving us unaware of its broader significance. As Flusser quipped, however, “technology has become too serious a matter to be left to technicians.” There is thus a need to apprehend the complex socio-technical systems that produce and are served by technologies. Or, as Hoijtink and Leese invite, to “render them political” and consider “the politics that go into technology, as well as the politics that emanate from technology.” In such socio-technical systems, accounting for the interaction of humans, technologies and structures invites analysis of how agency and power may be produced, distributed and transformed.

### Link—Security Cooperation

#### Security cooperation misses the point. War is transitioning – now operates through the computational redisclosure of the battlefield and predictive preemptive systems

Dyer-Witheford and Matviyenko 2019—associate professor of information and media studies at the University of Western Ontario; assistant professor of communication at Simon Fraser University (Nick and Svitlana, *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*) //ansel

What this reach grasps is the “datified subject” (Cheney-Lippold 2017, 35), that is to say, the identity constituted for individuals by their activity on digital networks. This is not to suggest an entire virtual translation of the person into the network but rather the collection of digital identifiers that converge on, add to, overlay, interpenetrate, and, in some contexts, supplant the multiple social codes and indicators of which corporeal individuality is composed. There is now an extensive literature on the various corporate and state “profiling machines” (Elmer 2004) that assemble and ascribe identities from the traces of digital searching, liking, browsing, shopping, chatting, and navigating, and, indeed, from the mere act of carrying location-transmitting mobile phones. And there is a similar series of investigations into the “black boxes” (Pasquale 2015; see also Amoore 2013; Finn 2017) of algorithmic processes that, from the accumulation of “big data,” predict future activities—and of the many biases and errors that enter this process (O’Neill 2016). This literature highlights the paradox that the mass volumes of big data enable increasingly precise, personalized mapping of an individualized “data subject” (Bauman et al. 2014) according to its conformity or deviation from a series of patterns. We will follow this idea through three different registers in which war touches the “datified subject”: battlefield intelligence, civilian surveillance, and digital propaganda, focusing particularly on examples from the United States. Shawn Powers and Michael Jablonski (2015, 81) observe that origins of data profiling lie in intelligence operations, where mosaic theory, the idea that “one can piece discrete bits of information together to predict the likely intentions or actions of others,” has been a core idea. Early in the so-called war on terror, mosaic theory was applied at the CIA’s black sites and U.S. military’s detention centers at Guantánamo, Bagram, and Kandahar, where captives were often held and interrogated solely on the basis of association with other suspects (Pozen 2005). The idea that big data can generate an “individualization” of war has become increasingly prominent in cyberwar doctrine. In 2014, Charles Dunlap, a retired U.S. major general (and one of the several authors who invoke the pseudoTrotsky aphorism we started with), suggested that anticipations of cyberwar as a series of “apocalyptic” infrastructure attacks might be less important than the “hyperpersonalization of war” based on data profiles. The possibility that particularly excited him was that of targeting specific members of an opponent’s forces, “primarily the leadership cadre but also critical technicians and experts,” with the primary example being the use of drones, both for information gathering and attack delivery from the skies over Afghanistan, Iraq, Pakistan, Yemen, and Somalia.

### Link—Undersea Cables

#### Their threat toward undersea cable systems is exaggerated and a form of fearmongering

**Bueger 21** (Christian Bueger, Professor of International Relations at the University of Copenhagen, “Protecting hidden infrastructure: The security politics of the global submarine data cable network”, *Contemporary Security Policy*, 3/29/21, <https://www-tandfonline-com.proxy.lib.umich.edu/doi/pdf/10.1080/13523260.2021.1907129?needAccess=true>) // EL

Cable security and the problem of threat inflation While the control and security of submarine communication infrastructure were a core issue and part of the security calculations during the two World Wars as well as the Cold War (Hills, 2002; Smith, 2018), in the post-Cold War environment such concerns were less prevalent. The uncontested U.S. naval hegemony and the primacy of non-state threats moved such issues to the margins. The new discourse on the protection of critical infrastructures influenced by the concerns over transnational terrorism of the 2000s did not change this substantially. It is only in the early 2010s, that scholars such as Sechrist (2012), Ross (2014), or Martinage (2015) called attention to the security of the submarine cable network. Since then, a number of studies have documented the relevance of cables for national and international security. Anchored in the wider geopolitical, strategic, and military discourses of the North Atlantic security community, contributors are concerned about the rise of hybrid warfare, the perceived hostility of Russia’s foreign policy, the fear of a large-scale cyber-attack, and the growing technical sophistication of terrorist groups. The focus of such studies is hence the vulnerability of the cable network emanating from deliberate attacks. Observations of Russian submarine activities in territorial waters and in proximity to cable routes, that became public in 2015, triggered much of this debate (Hicks et al., 2016, pp. 3–4). This raised concerns that the Russian navy might tap into the cables for espionage and surveillance, temper with or even cut them as part of a hybrid warfare campaign. Schaub et al. (2017, p. 37) stress that “cables and nodes would be prime targets in a hybrid warfare campaign” instigated by Russia. A former Supreme Allied Commander at the North Atlantic Treaty Organization (NATO) suggests that this seems obvious, as “in the case of heightened tensions, access to the underwater cable system represents a rich trove of intelligence, a potential major disruption to an enemy’s economy and a symbolic chest thump for the Russian Navy” (Stavridis, 2016). Similarly, a report by the British think tank Policy Exchange emphasizes that “whether from terrorist activity or an increasingly bellicose Russian naval presence, the threat of these vulnerabilities being exploited is growing” (Sunak, 2017, p. 5). Others suggest that undersea cables are inherently susceptible to attacks from non-state violent groups and terrorism, since their location is usually public, cables tend to be highly concentrated geographically and the level of technical expertise and resources required to damage them are limited (Martinage, 2015; Matis, 2012; Sunak, 2017). These studies are supplemented by governmental reports that examine and assess threats to the undersea cable network. NATO’s military leadership for instance warned that the Russian navy is threatening the undersea cable network (Birnbaum, 2017). It is, nevertheless, not clear whether NATO believes Russia has the capability or the intention of attacking cable networks (Hinck, 2017). In order to mitigate the threats to the undersea cable network, above studies situate cable security in the context of national security strategies and call for a military response. Increased naval patrols, surveillance activities and other measures of deterrence are the proposed responses (Martinage, 2015; Matis, 2012; Sunak, 2017). Other proposals concern national focal points, public-private coordination and the creation of cable protection zones (Davenport, 2015; Martinage, 2015; Schaub et al., 2017; Sunak, 2017). However, neither scholars nor public officials have provided much detailed information about the substance of a Russian or terrorist threat to the cable infrastructure. Hinck (2017), for instance, diagnoses a general lack of information regarding any threats to the undersea cable network, particularly when it comes to the alleged Russian intentions, plans and activities. So far, no intentional hostile disruptions to the submarine cable infrastructure have been reported publicly. The scenarios underpinning the threat discourse hence seem to be built not on prior incidents but on overall assessments of the geopolitical landscape. Arguably, this implies that the threat scenarios could be exaggerated and point to a substantial risk of threat inflation and fearmongering.

### Impact—Algorithmic Warfare

#### Algorithmic warfare expands mass techno-inflicted violence across the globe and risks nuclear extinction.

Johnson, 18—Professor, Environmental History, Loyola University Chicago (Benjamin, “Coded Conflict: Algorithmic and Drone Warfare in US Security Strategy,” Journal of Military and Strategic Studies, Volume 18, Issue 4, dml)

The notion that people can be killed ‘incorrectly’ represents the dominant concern in military appropriation of civilian technologies and replicates the same troubling issue that is identified by post-colonial critiques of drone warfare: that implicitly there is a ‘correct’ and therefor ethical way to kill people at all. However, even the post-colonial focus on how surveillance and kill targets are ‘Othered’ and the violence encountered through that process is only part of a larger set of issues raised by the focus on algorithmic warfare. Given that security discourse is beginning to re-emphasize the importance of long-term interstate competition and a security strategy predicated on information-decision cycle dominance through algorithmic superiority, the implications posed go beyond the violence of surveillance and killing.

For one, the increasing militarization of everyday life supports the normalization of drones and weapons, which in turn legitimates their use in regimes of violence. This in and of itself is not a departure from the liberal way of war but a strengthening of its underlying rationality – that peace must be secured through force.

Second, while the focus has also been on the role of algorithms in shaping autonomous weapons without the perceived ethics of a human consciousness (which itself is a problematic position), the implications of algorithmic decision making go much farther than autonomous weapons. The most recent security strategy rhetoric, which defines its adversarial advantage in terms of decision-making cycles, shares a similar but amplified form of the game-theoretic rationality that underpinned Cold-War thinking under the rubric of ‘mutually assured destruction’ (MAD). However, unlike MAD, which theoretically maintained a balance of power (however uncomfortable) between the US and USSR, the new logic of decision cycle advantage has been combined with an equal shift towards a rhetorical need for weapons that exist below the threshold of non-use (whether because of their destructive capability or cost). While the National Defense Strategy states an overall strategy of interaction “below the level of armed conflict,”131 there is a troubling scenario presented when decision making is theoretically collapsed into the instantaneous without humans necessarily ‘in the loop.’132 Combined with a rhetorical stance that has emphasized a need for new weapons and a modernized nuclear arsenal with ‘small-yield’ warheads, which are argued to introduce a measure of ‘limit’ and tactical capability within US nuclear deterrence,133 the expansion and normalization of algorithmic violence seems a likely future for societies across the globe. Dillon and Reid have already alluded to the possibilities encountered in this environment. They argue that:

endless war is underwritten here by a new set of problems [because] 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 defining 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 [...].134

This is not to suggest that the future looks like the totalitarian and apocalyptic scenarios of fiction. However, the ‘unending’ and ‘everywhere’ war does imply, following Focault’s interest in the continuation of war once peace has been declared, that the spatial and temporal parameters of conflict are increasingly escaping even the foggiest notion that peace and war are inseparable. Shaw has argued that failing to conceive of artificial intelligence in terms of its behavioural agency (which is implicitly limited to humans) fails to consider how artificial intelligence and robots will transform the global political order independent of their instrumental use by.135 At its most seemingly innocuous end in terms of the spectrum of possibilities encountered, the set of issues posed suggest that war and security will increasingly become a routinized, normalized and indeed biopolitical in terms of its structure for even the smallest processes of everyday life across multiple spaces. At the other end of this spectrum towards the seemingly impossible nightmare scenarios encountered in fiction, algorithmic warfare is posed to extend the liberal rationality of ‘peace through force’ into the realm of totalitarianism and the threat of mass techno-inflicted violence across the globe.

Conclusion

The notion that war is now ‘never-ending’ has a two-fold dimension. The first is that in order to retain advantage over one’s opponents, one must be continuously adapting and innovating, especially as those opponents are able to play ‘catch-up’ at an increasing speed. The second dimension is that, as a consequence of the first dimension, the life-worlds of individuals and societies will be increasingly subjugated to a particular militarized and securitized logic of adaptation and innovation, such that human life itself risks being lost to totalitarian governance or even total destruction. This of course is a dramatization of the latent possibilities in a ‘permanent’ and ‘everywhere’ war. However, as a great deal of research has shown, these latent possibilities are already actual realities for an increasing number of people across the globe. Thus, the potential consequences of these dramatic possibilities should not be discounted.

As a brief summary of the expansive discussion made above, this article has argued that drone and algorithmic warfare are an expression of and an indivisible tool for the ‘never-ending’ war that is now propelling US security strategy rhetoric. These technologies and the never-ending war itself are not ‘new’ in the sense that there is a clean break between the conflicts of yesterday and today. However, modern warfare is not the same either. Rather, these technologies and the rationalities that underpin them are part of a much larger set of practices that are historically rooted with linkages to the Cold War, the World Wars, and even to the Napoleonic Wars, but have increasingly penetrated the lives of everyone in new and complex ways. In this respect, drone and algorithmic warfare represent a particular configuration of a simultaneous evolution in technological capability and an acute faith in that capability to mitigate the risks of uncertainty, which paradoxically appear to be increasing as a result of globalized networks. Fukuyama’s ‘end of history’ it seems gave birth to the very conditions that are undermining its own stability. While the policies and technologies associated with counter-terrorism have formed and will undoubtedly continue to form a major part of this security environment, the return of ‘great power competition’ entails much wider implications stemming from an intensified focus on distance and autonomy. If the recent US security strategy is to serve as an indicator for where history will go, it will be a race to not only decide more than the ‘Other’, whoever that may be, but to know, decide and, if necessary, strike faster – to essentially collapse the spectrum of domains and dominate a singular domain of space-time. To accomplish this may require a totalizing endeavor not dissimilar to the complete and total mobilization of society needed to wage the World Wars, the culmination of total war. However, unlike the blurring of the civilian and military spheres along with the mass mobilization of labour and industrial capacity, total war in the ‘never-ending’ sense implies that it will happen in the networks and minutia of everyday life, perhaps without us even knowing it.

### Impact—China War

#### **Cybernetic capitalism makes US-china war so inevitable**

Dyer-Witheford and Matviyenko 19—associate professor of information and media studies at the University of Western Ontario; assistant professor of communication at Simon Fraser University (Nick and Svitlana, *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*) //ansel

These companies’ collaborations with the U.S. security apparatus include their acquiescence to the NSA PRISM surveillance program, an episode they are now energetically attempting to live down. It also includes their lucrative provision of services to U.S. military and intelligence agencies, ranging from massive data storage and processing facilities (Amazon and Google) to space-based “geospatial visualization services” (Google) to “wearable tech” for the armed services (Apple) as well as surveillance systems for the private military contractors that now constitute the sizable penumbra of Pentagon operations (Alexander 2015; Gregg 2017; Levine 2014a, 2014b).8 This reciprocity also involves the “revolving door” between high-level Silicon Valley and Pentagon managers and their shared culture of global “problem-solving” think tanks, typified by Google’s Jigsaw, and a willingness to censor internet material at the behest of the U.S. government, once only sporadically disclosed but now in full swing after the 2016 election hacking scandal (Assange 2014; Levine 2014c; Greenwald 2017b). Yet the United States has cyberwar vulnerabilities. Paradoxically, these result from its historically advantageous “home game” (Segal 2016; 35) advantage: a highly networked military and economy susceptible to hacker attack. This problem is intensified by the neoliberal form of capitalism the United States champions. Free market zealotry is at once governmentally embraced and on occasion makes it difficult for the U.S. state to enforce cybersecurity provisions on private capital, around issues ranging from the reporting of cyberattacks to mobile phone encryption. **It is largely in reaction to U.S. strengths and weaknesses that Russia and China have developed their own capacities and strategies**. In particular, rather than seeing cyberwar as a distinct sphere of military operations, it is for these nations’ military forces subsumed within a larger category of “information warfare” that comprehends forms of psychological operations and propaganda. This orientation, taken together with the different historic levels and paths of technological development, has led to distinctive approaches to conflict in cyberspace.

The People’s Republic of China (PRC) was until recently the main object of popular U.S. cyberwar anxieties: depictions of transpacific wars fought with digital weapons abound in both fictional entertainments and serious political scenarios (Singer and Cole 2015; McCoy 2017). Yet although China’s digital policies and practices have been presented in the most ominous terms in U.S. media, they may be as much a sign of weakness as of strength (Lindsay 2014; Lindsay, Cheung, and Reveron 2015). An important factor driving the leaders of the Chinese Communist Party to open their country to the world market at the end of the 1970s was the perception of massive and intensifying technological backwardness vis-à-vis the West. As the PRC confronts the question of whether, in the global market, it will be an economic “head servant” (Hung 2009) to the United States or risk conflict over issues of trade and political dominance in the Pacific, this awareness shapes China’s concept of cyberwar. Thus, for the Chinese state, a major concern is, notoriously, maintenance of ideological control over a population perceived as vulnerable to terrorism, to separatism, and to “foreign influences” of the sort projected by U.S. digital “soft power.” This control is exercised through the elaborate and continually evolving apparatus of digital censorship, surveillance, and preemption shorthanded as the “Great Firewall of China.” This system combines blackouts of proscribed websites, algorithmic filtering and monitoring of email, and interventions by internet militias (the so-called Fifty Cent Army, named for the alleged pay rate for each posting) or bureaucrats to divert or disrupt controversial discussions with pro-government cheerleading with digital surveillance of, and attacks on, overseas sites and groups attempting to evade censorship (Lindsay, Cheung, and Reveron 2015; Klimburg 2017). Administered via the collaboration of private-sector internet service providers with state authorities, the system has been characterized by a changing, erratic enforcement that by its very uncertainty increases the risk to dissenters. The Firewall, which has undoubtedly contributed to China’s unenviable record of large-scale imprisonment of social activists and journalists, has been a frequent target of Western criticisms for violations of internet freedom, though these have subsided somewhat post-Snowden. China’s possible larger plans for an extensive “social credit” system based on monitoring of internet practices and “scoring” of social and perhaps political behavior would represent the logical consolidation of this system (Economist 2016a).

The overlap between issues of hard and soft power in a cyberwar context is demonstrated by what Bratton (2016, 112) terms the “Sino-Google war.” Between 2002 and 2010, Google was involved in protracted and complex disputes with the PRC over that state’s internet censorship. These intensified when, in 2006, Google set up a Google China subsidiary, headquartered in Beijing. After oscillating between compliance and noncompliance, and having suffered highly sophisticated hacking attacks, which the NSA offered to help counter (Levine 2014b), Google China closed its mainland office in 2010 and, though it continued operating from Hong Kong, now holds only a tiny share of China’s search activity. **This episode can be interpreted in several ways: as a clash between internet freedom and authoritarianism (the version favored by Western politicians, internet pundits, and media); as an intercapitalist dispute between Google and China’s major domestic, and state-championed, search enterprise, Baidu; or, as Bratton describes it, as a collision between rival concepts of the internet’s relation to the state, one giving the former primacy over the latter, the other reversing that priority.**

Although there is something to be said for all these perspectives, they overlook the one Bratton explicitly rejects: “superpower” conflict. Yet the period of the “Sino-Google war” was one of mounting tensions between the United States and China, including the unfolding aftermath of China’s earlier capture of a U.S. spy plane (Hersh 2010); American accusations of large-scale digital espionage, both economic and military, by Chinese hackers (Segal 2016); NSA “implants” in the networks of China’s giant telecommunications company (Hsu 2014); and widespread expectations that Sino-American tensions could trigger the first full-scale cyberwar (expectations still widely held, even if Russia has lately publicly supplanted China as an object of U.S. suspicions). In this context, it is hardly surprising that the issue of a giant U.S. internet company not only skirting China’s Great Firewall but also amassing massive information about China’s data subjects, and establishing itself as gateway to global networks, was extraordinarily tense.9

### Impact—Dark Pure War

#### The expansion of war beyond physicality enables dark pure war against the planet.

Towns, 19—associate professor in Communication and Media Studies, Carleton University (Armond, “(Dark) Pure War: Virilio, the Cinematic, and the Racial,” Media Theory, Vol. 3, No. 2, 145-160, dml)

In Pure War, Paul Virilio argued that war continued beyond the physicality of the battlefield. Outside of the violence of the fight lay a violence of industrial production toward the conditions for war. Put differently, pure war signified the new ways that war was now acted out ‘in infinite preparation’ (Virilio, 2008: 29). Pure war indicated the always already active preparation for war by the state, even when war was not being physically waged.

One could say that a cornerstone of Virilio’s research has been media’s relation to unending war. A central component of pure war, for example, is information, or the gathering of data to surveil and police populations that are always under the watchful eye of the war machine. Interestingly, Virilio concerns himself less with the racial implications of those who are open to surveilling and policing and more with the expansion of policing and surveilling as practices that are applicable to ‘everyone’. Yet, his examples of war have racial undertones that he often does not fully investigate: the Vietnam War, the Iraq War, and the Italo-Ethiopian War, to name a few, all creep toward the pure war. Even as Virilio (2002) acknowledged the racial implications of the Second World War, he had less to say about the recognition that the Nazis pulled their racialized strategies of death for the European Jewish population from the US state’s approach to black and indigenous people (Whitman, 2017). Each of these wars, between white and nonwhite people or between white and white people in relation to those who could never fully be white, suggest that the wars that Virilio found most interesting were not race neutral.

What can Virilio provide for a media studies of race? I argue that Virilio’s work on pure war can be reinterpreted as a ‘dark pure war’, concerned with a militaristic, unending war against nonwhite populations. It is a dark pure war, one that structures the colony and the metropole, that lays the foundation for pure war. Dark pure war is not necessarily ‘black’ in the racialized sense, even as it often functions that way. Instead, it is black in the ‘blackening’ sense, in what Kumi Silva (2010) calls the ‘identification’ of nonwhite bodies as open to state violence. Thus, pulling from Virilio and Simone Browne’s (2015) Dark Matters, a dark pure war outlines the centrality of race to the continuance of war, even as race is the purposefully forgotten genesis of such war. This is not Michel Foucault’s (2003) ‘race war’, as Europe is not the central locale from which such war occurs. Rather, dark pure war is inseparable from Euro-American imperial, capitalistic expansionism (colonialism and racial slavery) as militarized projects toward the maintenance of white life and the conditions of black death, ad infinitum.

Virilio’s work has been called, rightly in my opinion, ‘wild and aphoristic’ (Sharma, 2013). Yet, I want to say that what Virilio may point toward is an investigation of the centrality of technologies to racialization processes. Surveillance studies (which has long investigated race) and media philosophy (which has been slower to discuss race) are put into conversation with one another here. I advance the concept of dark pure war in three sections. I start by delineating the connections between war, cinema, and information that Virilio argued were important. I then move into outlining the darkness of pure war, particularly by outlining the racialized components of contemporary policing and surveillance. I conclude by calling for a rethinking of ‘dromology’, one that moves toward including the multi-symbolic capacity of ‘race’ in discussions of war.

The Perceptions of War: Vision and the Cinematic

In War and Cinema, Virilio argued that the history of war was both theatrical and a history of transforming perceptual fields, whereby vision was increasingly the site of power. As such, the rifle’s gunsights and the camera came together to situate the world as a field of vision that could be measured, calculated, and shot. For Virilio, film functioned as a pedagogical tool, one that involved an increasing sensorial detachment from film itself. Virilio’s example is the famous myth of an audience in Paris watching a film of a moving locomotive filling the screen causing the people in the cinema to believe the train was going to drive over them:

[In] fact it was the precision of the camera-shot which first created audience panic at the Lumières’ ‘motion demonstrations’ of the train’s arrival at la Ciotat, when everyone felt that they risked being crushed or injured by the train. This kind of fear, akin to the sense of speed that people seek on roller coasters, did not disappear but simply became more pernicious as the audience learnt to control its nervous reactions and began to find death amusing (Virilio, 1989: 39-40).

What Virilio pointed to was a transformation in perception: film produced images of objects, thus, perceptually distancing audiences from said objects, to a point where there would no longer be a need to panic at the sight of an oncoming train in a cinema. There have been a few attempts to debunk the myth of whether or not the audience was actually sent running at the sight of the train (Cooper, 2016; Grundhauser, 2016), but the fact still stands: ‘film is now second nature to us, but it was utterly shocking not much more than a century ago’ (Cooper, 2016).

Cinemas were ‘training camps’, bonding ‘people together in the face of death agony, teaching them to master the fear of what they did not know – or rather, as Hitchcock put it, of what did not exist’ (Virilio, 1989: 40). In short, cinema readied people for ‘the artificial horizon of a screen or a monitor capable of permanently displaying the preponderance of the media perspective, the relief of the “tele-present” event taking precedence over the three dimensions of the volume of the objects or places here present’ (Virilio, 2006: 66). This training did not occur overnight, but involved multiple media forms that all worked toward perceptual transformation. As such, more than cinema, Virilio is interested in the ‘cinematic’, which included and exceeded cinema, proper; he tried to track the link between cinema, war, and later ‘vision machines’, such as television, CCTV, smart devices, and drone strikes, assuring us that ‘Components of a cinematic machine have been in use over many centuries: forms of projection, moving images, immobile voyages, and visionary illuminations’ (Crary, 2009: 13). The cinema, television, and war all worked together toward distancing audiences from objects, for Virilio.

Virilio’s work on cinema also adds much to those interested in studying the Web and information. In the wake of the atom bomb, Virilio warned of a second bomb, the ‘information bomb’, which is important for pure war. Whereas the atom bomb was a war of movement, the information bomb was a war of knowledge and speed, signifying a war ‘won’ by the increasing speed of interactivity in real time. Such a bomb included and exceeded cinema, and essentially structured computer screens and the Web – both media developed during and after the Second World War, and very much because of it. This is a trajectory of transformations that cannot be said to have origins in cinema, but were representative of the impact of the cinematic:

We’re still here in the domain of cinematic illusion, of the mirage of information precipitated on the computer screen what is given is exactly the information but not the sensation; it is the apatheia, this scientific impassibility which makes it so that the more informed man is the more the desert of the world expands around him, the more the repetition of information (already known) upsets the stimuli of observation, overtaking them automatically, not only in memory (interior light) but first of all in the look, to the point that from now on it’s the speed of light itself which limits the reading of information and the important thing in electronic information is no longer the storage but the display (Virilio, 2009: 56).

For Virilio, then, the shift from ‘tele-vision’ to ‘tele-surveillance’ reflected the demands of capitalism and war. Whereas tele-vision held ‘the task of informing or entertaining the mass of viewers’ (Virilio, 2006: 59), the new tele-vision, or the ‘tele-surveillance’, was concerned with ‘exposing and invading of individuals’ domestic space, like a new form of lighting, which is capable of revolutionizing the notion of neighborhood unit, or of a building or district’ (Virilio, 2006: 59). The drone strike, then, could pinpoint a ‘target’s’ location, whether indoors or outdoors.

Thus, tele-surveillance spoke to a ‘dromology,’ a ‘speed politics’, or a politics of instantaneousness, sparked by the increasing need to entertain, monitor, and prepare others for their own monitoring. Further, it replicated the waging of war on people at a distance: ‘Making information resonate globally, which is necessary in the age of the great planetary market, is in many ways going to resemble the practices and uses of military intelligence, and also political propaganda and its excesses’ (Virilio, 2006: 62). Likewise, this spoke to what many have called a ‘slow violence’, one that disproportionately impacts the Global South (Nixon, 2011; Parikka, 2017), as a space largely viewed solely as a waste station of the Global North. War is a continual process that does not end when the last round is fired, but is also carried out via the circulation of information and propaganda in ways that penetrate architecture without necessarily physically destroying a building’s structural integrity.

Dark Pure War: Surveillance and the Racial

Pure war is the continuance of war after the physicality of war is over and done; now, information functions toward the continuance of war, as a preemptive strike against enemies: ‘But war doesn’t really end, as Virilio noted, it just accelerates, approximating ever more closely to its pure form’ (Wark, 2018). Information is now a central component of war, whereby ‘Not only is architecture vulnerable to bombs, it proves defenseless against information, passing through the doors and walls of our homes, rearranging the space and time we imagine we live within’ (Wark, 2018). Indeed, ‘the capability of war without war manifests a parallel information market of propaganda, illusion, dissimulation’ (Der Derian, 2002: viii).

To rethink Virilio’s pure war as dark pure war requires thinking about not only how information is weaponized toward war’s continuance, but also the presumed racial neutrality associated with both war and information. Thus, race is the underexamined, overlooked element of Virilio’s theory. Like discussions of dark matter in physics, Browne’s employment of ‘dark matter’ is meant to point toward the ‘unseen and unperceived’ elements of antiblackness in the surveillant practices of contemporary society. She argues that ‘rather than seeing surveillance as something inaugurated by new technologies, such as automated facial recognition or unmanned autonomous vehicles (or drones)’ (Browne, 2015: 8), we can instead think about ‘surveillance in and of black life as a fact of blackness’ (Browne, 2015: 6). Thus, Browne connects surveillance theory to a dark history concerned with the measurement of bodies to see their ‘intentions’, a dark history often underexamined in surveillance studies. That history is scientific racism:

Anthropometry, or Bertillonage, was introduced in 1883 by Alphonse Bertillon as a system of measuring and then cataloguing the human body by distinguishing one individual from another for the purposes of identification, classification, and criminal forensics. This early biometric information technology was put to work as a “scientific method,” alongside the pseudo-sciences of craniometry (the measurement of the skull to assign criminality and intelligence to race and gender) and phrenology (attributing mental abilities to the shape of the skull, as the skull was believed to hold a brain made up of individual organs) (Browne, 2015: 112).

What Browne points toward is a question unasked by Virilio: what if the ‘fact of blackness’ is the structuring necessity for the new technologies of surveillance themselves? This would require that we rethink pure war as a dark pure war, which is to say that pure war holds race as central, while never acknowledging its importance to the maintenance of war.

What if we thought about Virilio’s pure war as a racial condition in the US? In short, what if we were to rearticulate WEB Du Bois’ (1994) question of, ‘How does it feel to be a problem’, as a racialized question of war? The end of the US Civil War and the end of racial slavery marked the structure of pure war as a condition, rather than a contingency, of black life. Another way to say this is that white people went to war with each other over the right to own our black bodies in the US Civil War, and it presumably ended in 1865. Yet, the replication of racial violence, what Saidiya Hartman (2008) calls the ‘afterlife of slavery’, has yet to end for black people; instead, racial violence is fundamental to what it means to be black (and white) in the US. Jim Crowism, ghettoization, deindustrialization, white flight, mass incarceration, and gentrification are remnants of dark pure war. They are post-war answers to how to deal with a ‘problem’; to call for their end is to call for the end to what many cannot let go of: whiteness. Further, with race at its center, this entails that black people are not the only ones affected by dark pure war, but are part of dark pure war’s larger assemblage.

What Virilio pointed toward, then, was that cinema and war were necessarily interconnected and assistants in the perceptual transformations that readied populations for their own continual surveillance; and just as important, such forms of surveillance have been tested on people of color prior to their implementation on the larger society. This is what Browne refers to as the ‘unseen and unperceived’ component of dark matter and what I call dark pure war: it is the necessity of the black body as an always already surveillable, commodified object, one that can normalize even the contemporary surveillance of people’s information online.

### Impact—Dystopia

#### Dystopia outweighs everything.

Harel and Brownsword, 19—law professor at the Hebrew University of Jerusalem AND Professor in Law at King's College London (Alon and Roger, “Law, liberty and technology: criminal justice in the context of smart machines,” International Journal of Law in Context, Volume 15, Special Issue 2, June 2019, pp. 107-125, dml) [language modifications denoted by brackets]

Famously, Stephen Hawking (2018, p. 188) remarked that ‘the advent of super-intelligent AI would be either the best or the worst thing ever to happen to humanity’. At best, smart machines, smart policing and smart cities of the kind contemplated by Elizabeth Joh might signal the end of crime; but, at worst, we can imagine various dystopian futures where the existential and agential threats presented by AI have been realised. Given, in James Bridle's (2018, p. 2) words, that our technologies are complicit in ‘an out-of-control economic system that immiserates many and continues to widen the gap between rich and poor; the collapse of political and societal consensus across the globe resulting in increasing nationalisms, social divisions, ethnic conflicts and shadow wars; and a warming climate, which existentially threatens us all’, then Vincent Chiao might well be right in claiming that the turn to smart technology might not be the smartest [best] way of trying to achieve the end of crime.

In this collection, our contributors have not highlighted concerns of an existential nature. Nevertheless, we might fear that, in our quest for crime-free societies, for greater safety and well-being, we will develop and embed ever more intelligent devices to the point that there is a risk of the extinction of humans – or, if not that, then a risk of humanity surviving ‘in some highly suboptimal state or in which a large portion of our potential for desirable development is irreversibly squandered’ (Bostrom, 2014, p. 281, note 1; see also Ford, 2015). Our contributors have not yet recommended that we should follow the example of Samuel Butler's Erewhonians who, fearful for their liberty, destroyed their machines (Butler, 1872) – and who also, of course, inverted conventional wisdom by punishing those who fell ill while, by contrast, treating in hospital and sympathising with those who committed crimes such as forging cheques, setting property on fire or robbing with violence. Yet, the beauty of Erewhon is that, to some present-day readers – particularly readers who are familiar with, say, Harari's Homo Deus (2016) 15 or Häggerström's Here be Dragons (2016) – the practices of the Erewhonians might seem to be anything but benighted. Is it so ridiculous to think that, with the acceleration in technological development, machines might become much smaller and smarter, capable of reproducing themselves, communicating with one another and displaying various degrees of intelligence (if not consciousness as humans experience it) and agency? Most importantly, which policy would be the more crazy [imprudent]: to disregard machines as a threat to the human condition or to treat the threat as sufficiently serious to warrant at least some precautionary measures – albeit perhaps not precaution on the scale exercised by the Erewhonians, who destroyed ‘all the inventions that had been discovered for the preceding 271 years’ (Butler, 1872, p. 260)?

Such, however, are not the most explicit concerns of our contributors. Rather, the concerns expressed by Bowling and Iyer, by Lynskey and by Macdonald, Correia and Watkin relate to our agential interests and, in particular to our interests in privacy, in the fair collection and processing of our personal data and in access to (and the integrity of) the informational eco-system. Increasingly, it is being recognised that such interests are ‘contextual’ not only in the sense that their demands might vary from one context to another, but in the more fundamental sense that we have a common interest in a context that enables our self-development (Hu, 2017; Brincker, 2017). This is nicely expressed in a paper (discussing data governance) from the Royal Society and British Academy:

‘Future concerns will likely relate to the freedom and capacity to create conditions in which we can flourish as individuals; governance will determine the social, political, legal and moral infrastructure that gives each person a sphere of protection through which they can explore who they are, with whom they want to relate and how they want to understand themselves, free from intrusion or limitation of choice.’ (Royal Society and British Academy, 2016, p. 5)

With data being gathered, in both the public and the private sector, on an unprecedented scale (Vaidhyanathan, 2011; Galloway, 2017), we might treat such dataveillance as compromising the conditions for self-development and agency (Pasquale, 2015). Moreover, we might fear that, where data are used to train smart machines that sift and sort citizens (as mooted by the Chinese social credit system) (Chen and Cheung, 2017), then, in Glen Greenwald's (2014, p. 6) words, this could be the precursor to a truly dystopian ‘system of omnipresent monitoring and control’.

Finally, there is the subtle and insidious way in which smart machines might compromise the conditions for moral development. If we accept that the fundamental aspiration of any moral community is that its members should try to do the right thing, then this presupposes a process of moral reflection and action that accords with one's moral judgment. Of course, this does not imply that each agent will make the same moral judgment or apply the same reasons. A utilitarian community is very different to a Kantian community; but, in both cases, these are moral communities and it is their shared aspiration to do the right thing that is the lowest common denominator (Brownsword, 2013; 2018a). Arguably, liberty – in the sense of having the practical option of doing both the right thing and the wrong thing – is critical to moral community. On the East coast, where crime is rife and where prudential reasoning dominates, the moral project is poorly realised; but it is at least a community with moral possibilities and with room for moral improvement. By contrast, in the well-ordered technologically managed West coast, if the possibility of moral community is lost, then, as Beyleveld and Brownsword emphasise, this should certainly give us pause about the direction of travel in the criminal justice system.

The ability to do the right thing also hinges not only on individual deliberation, but also on public moral deliberation. The automated processes designed to disable crime also typically mute and disable public moral deliberation. If behaviour that previously was condemned and prohibited has become impossible to engage in (due to technological innovations), we are less likely to debate its justifiability. We will never know whether speed limits are justified unless some people violate them; we can never know whether certain restrictions on movement promote the public interest if such restrictions are enforced perfectly by using technological innovations. In other words, automated processes do not only erode individual moral sensibilities; they also erode public moral deliberation.

### Impact—Entropy

#### Technical systems are entropic - makes collapse inevitable.

Featherstone, 17 [Mark Featherstone Senior Lecturer in Sociology at Keele University. “Planet Utopia: Utopia, Dystopia, and Globalisation,” February 17, 2017]//Townes

This is exactly what Baudrillard (2012) means when he writes of ecstatic communication, which communicates nothing but the fact of communication itself, and Serres (1983) reflects upon when he explains that all technical systems point towards entropy, noise, and the black depths of the universe. What this means is that the absolute security of the market, the realisation of Platonic form in the financial utopia that led Ben Bernanke and others to speak of the great moderation, is also Badiou’s (2006) void, the black screen, the moment the numbers no longer seem to add up or make sense. For mathematician Benoit Mandelbrot (2004) the connection between these two moments, the point of total securitisation and the black screen of nonsense, runs through the accumulation of an endless number of small events that come together to create a systemic tipping point. In his view these small deviations occur because the logic of financial securitisation is fundamentally flawed. In his work on the unpredictability of markets he asks, for example, what happens when the trade in derivatives and options starts to feed back into the valuation of stocks and shares to such an extent that price becomes absolutely distorted? What happens when it becomes clear that probability is incapable of predicting the future because it is based on calculations premised on the fantasy that what has happened in the past will continue to happen in the future? Thus Mandelbrot’s (2004) point is that probability theory is ineffective in a highly complex system because there are too many variables and too many interactions to be able to base prediction about the future in an assessment of the past. In this way his fractal theory, which he names in reference to the Greek fractus that means ‘to break’, presents a picture of systemic uncertainty, unpredictability, and potential collapse that contradicts the standard picture of cybernetic economy where calculation and the ability to hedge against fluctuation enables the maintenance of stability and order.

### Impact—Horizontal Escalation

#### Horizontal escalation is more likely than vertical escalation.

Joque, 18—PhD from the European Grad School, researches philosophy, technology and media and is the visualization librarian at the University of Michigan, go blue (Justin, “Buffer Overflow: The Space and Time of Cyberwar,” *Deconstruction Machines: Writing in the Age of Cyberwar*, Chapter 1, 65-66, dml)

In one sense, this military investment in “metaphysical control” and new battle spaces is a continuation of ancient strategies of deception, sabotage, and manipulation, but still this contemporary explication seems to mark a qualitatively new level of abstraction and expansiveness. As DiNardo and Hughes, two military historians and theorists, have warned, this focus on a metaphysical battle space marks a military– strategic investment in the complete inversion of the Clausewitzean formula in which politics is war by other means.70 In a 1995 article in Airpower Journal, they worry that the military focus on information warfare and subduing the enemy outside of traditional fighting lends itself to a complete military intervention into politics and civilian life. Chun’s insight that software functions as ideology is thus important in another regard: both software and ideology, along with law and economics, become sites of intervention that risk their symbolic functioning being turned against them.71

Although war spills over into all aspects of everyday life, it is decidedly not total war. It is almost the opposite: a war so constrained and reserved that it nearly goes unnoticed. As is argued in Unrestricted Warfare, growing global interlinkages, including international law, the shared biosphere, a highly connected global economy, and the threat of global thermonuclear war, serve to constrain many global actors. This is not to suggest that these constraints are always or even often effective or that they are positive forces, but they add additional costs that complicate political and military calculuses. All of these serve to put political limits on military options. Instead of vertical escalations of conflict to ever more violence, we are witnessing a horizontal escalation to ever more varied modes of conflict. As war spreads, it escalates horizontally and strategists attempt to open new domains. Thus “fighting” begins to look little like previous conflicts. For instance, the existence of both domestic and international law opens the possibility that one force would be able to limit another force’s strategic options by litigation (a strategy occasionally referred to as lawfare).72 These global interconnections have raised the cost of military escalation, often forcing states to fight within specified rules and domains for fear of upsetting the global order and unleashing potentially more destructive forces or disconnections from global spaces of flow.

Rather than a completely accessible global battle space where war would rage unhindered, we are witnessing the growth of a metaconflict where strategists, legal experts, and public relations experts are constantly attempting to define and constrain war for each side’s strategic advantage. The concept of war has now become part of war itself. As Qiao and Wang argue, the means to contemporary victory in war involve combining limited ends with unlimited means. They are careful to say that this is not total war. Rather, it is a war that weighs means and is not afraid to use any of them, but always to achieve limited rather than total ends. This must be at least part of what Virilio calls “pure war,” or elsewhere the “race to the absolute essence of war”73 as military goals become increasingly limited while strategy expands infinitely, culminating in “the war with zero deaths for the military, but also zero victories in political terms.”74 Rather than an all-out war, we are witnessing with the rise of cyberwar a war that spills outside the bounds of traditional warfare while remaining vertically constrained. This is not to say that these conflicts cannot become horribly violent; for the further afield these interventions stray, the more they may be likely to spiral out of control.

### Impact—Interventions

#### The global north maintains power through digital management and algorithmic biopolitics – they cause exploitation and interventions

* How alt resolves? Exploitation happens not because of simply digital capitalism, but rather because of the way that we view Africa through technical metaphysics that calculates its utility
* Maybe a better aff card because it describes emerging tech broadly

Oppegaard 22 (Doctoral Research Fellow, Department of Sociology and Human Geography at [University of Oslo](https://twitter.com/UniOslo), “The promise and peril of the digital economy”) //ansel is tired

How digital capitalism, despite often being framed as potential growth engine, exploits the already marginalized and reproduces inequalities and power-relations between Africans.

digital technologies enable new ways of organizing the production of services, unconstrained by spatial distances. By making it possible to carry out a service from everywhere in the world, digitalization has facilitated the increased fragmentation and outsourcing of services that were previously constrained by the need for geographic proximity between buyer and seller. The digitalization of the economy is at the same time giving rise to new forms of work and new ways of organizing labor processes—across the globe.

In The Digital Continent: Placing Africa in Planetary Networks of Work, Mohammed Amir Anwar and Mark Graham explore the development and organization of digital labor—defined as “work activities involving the paid manipulation of digital data by humans through [information and communication technologies] such as mobile phones, computers, laptops, etc.”—in Africa. They argue that African workers are playing an increasingly central role in digital capitalism by training “**artificial intelligence” and machine learning algorithms**, tagging images, and performing customer services, design tasks, **data management**, and so on. Thus, Anwar and Graham argue that digital capitalism is—despite rarely being mentioned—increasingly “made in Africa.” The aim of their book is to make both African workers and Africa as a core location in the digital economy visible.

Based on extensive fieldwork in five countries—Ghana, Kenya, Nigeria, South Africa, and Uganda—Anwar and Graham first argue that digitalization has made African countries lucrative destinations for offshoring services. They explore two such cases: “business process offshoring,” where a firm outsources non-core functions to specialized subcontractors, and the “remote gig economy,” composed of service tasks (such as writing, transcription, search engine optimization, and so on) mediated and coordinated by digital platforms and carried out by individual workers for customers who can be located anywhere. Second, they show how the African labor force is increasingly drawn into the digital economy, as workers who struggle to find employment in the “analog” sector of the economy turn to digital labor to make a living. This, Anwar and Graham argue, raises concerns for employment protections, social rights, and working conditions on digital platforms.

Anwar and Graham intervene in a prominent narrative promoted by governments, the World Bank, development organizations, and consulting firms that frames digitalization and information and communication technologies as “technological fixes” that will create jobs, reduce poverty, improve productivity, and lead to economic growth in Africa. Although digitalization and the fragmentation and outsourcing of production processes has integrated Africa into global production networks, Anwar and Graham argue that “Africa continues to be locked into a value-extractive position in the global economy.” Rather than a frictionless and “flat” global economy, Anwar and Graham’s analyses show how digitalization amplifies existing inequalities and power relations; in Africa, digital production is primarily characterized by poorly remunerated tasks at the bottom of the value chain that do not, in practice, represent economic improvements for workers.

For some segments of the population, such as university-educated workers unable to capitalize on their credentials, the digital economy provides an important lifeline. On the one hand, these forms of work provide a certain flexibility and autonomy. Workers are often able to, at least partially, set their own schedules. On the other hand, however, digital labor can also contribute to precarity, as contracts are usually short, working hours long, and social benefits and labor rights irregular or lacking. This is, Anwar and Graham argue, partially a result of workers being classified as self-employed independent contractors, the piece-rate model of compensation, and the ease with which digital firms can transfer tasks to another worker, company, or continent.

In addition, Anwar and Graham highlight the so-called “algorithmic management” used in these digital business models. Digitalization, they argue, is not only a tool for capital’s expansion into new localities, markets, and industries—digital technologies also enable managers to exert new forms of control over workers and labor processes. The authors term this form of management “digital Taylorism,” a digital manifestation of the Taylorist principles of detailed surveillance, meticulous control over labor process, disassembly of the production process, and “deskilling” every task to improve productivity and lower the costs of labor power. While the notion of “digital Taylorism” highlights platform capital’s control over workers and labor processes, it might neglect a key feature of “algorithmic management”: its strategic use of freedom and flexibility. While Taylor’s “scientific management” instructed workers on how each particular task should be performed, digital platforms usually allow workers to choose when they want to work, what tasks they want to do, and how they want to do them—partially in an effort to avoid being classified as their employers. Moreover, worker evaluation occurs through rating systems, with workers being sanctioned with moves like “deactivation” or firing if their average rating falls below a certain threshold. Thus, “algorithmic management” might be seen as representing a mode of management and control diverging from the core principles of Taylorism.

Furthermore, it is important to emphasize the ways in which workers assert agency and resist capital’s control, as Anwar and Graham do in detail. Drawing on the notion of “hidden transcripts,” they theorize labor agency not solely in organized and collective action, finding that digital workers in Africa exert individual agency through everyday practices and strategies of “resilience, reworking, and resistance.”

The Digital Continent is a very well-researched and well-written book. Anwar and Graham build on an impressively rich empirical material, mixing statistics and excerpts from interviews to give readers a proper understanding of workers’ lives, struggles, and aspirations. The presentation jumps eloquently between theoretical discussions, explications of labor geography concepts, and empirical investigations, producing thorough and thought-provoking analyses. This is particularly true for the final chapter, where the authors discuss measures for building a fairer global economy and world of work.

As a researcher studying platform work in the Norwegian transportation industry, the similarities between the working conditions, biographies, and experiences of the workers I interview in Oslo and the workers I met in The Digital Continent is striking. They are drawn from similar segments of the labor force and express the same ambivalence toward the real economic opportunities—combined with precarious working conditions—offered by the digital business models. Despite the field’s recent emphasis on how digital business models are being “embedded” in local social, political, and economic contexts, these models seem to create surprisingly similar outcomes in very different parts of the world. This puzzle might suggest that although digital labor platforms have to adjust to local conditions, regulations, and so on, they also function as technological and global capitalist machines, exporting the same employment model and “algorithmic management” from Silicon Valley (where they are usually designed) to every corner of the world, creating similar outcomes for workers regardless of their different contexts while also taking advantage of local specificities. This highlights Anwar and Graham’s conclusion that the fight for a fair digital economy has to be global.

### Impact—Manifest Destiny

#### Mission accomplished – to Manifest Destiny is to reach across the world in favor of the white economy – baiting humanity into capital under the neo-human automaton. The incongruity between Western individuation and the neo-human automaton births the self-destructive swarm on path to extinction

Franco ‘Bifo’ Berardi. 2021. Franco "Bifo" Berardi is an Italian communist philosopher, theorist and activist in the autonomist tradition, whose work mainly focuses on the role of the media and information technology within post-industrial capitalism. Berardi has written over two dozen published books, as well as a number of essays and speeches. “Manifest Destiny”. Ill Will. September 2nd, 2021. <https://illwill.com/manifest-destiny> //GJ

Mission Accomplished

I am curious to see how the upcoming twentieth anniversary celebrations of the Islamist attack on the Manhattan towers unfolds. Perhaps there will be no celebrations. European newspapers will not write: "we are all Americans," like they did the day Bush declared war on Afghanistan. In fact, America has lost.

While the defeat in Vietnam was a national drama, the Afghan defeat does not scratch the American conscience because the American population is incapable of seeing failure because of the epidemic of dementia that grips it.

The defeat in Vietnam was not terminal; the defeat in Afghanistan is. While still the greatest military power of all times, the United States no longer has one essential thing: itself. There is no longer the United States of America, there are at least two, and they are in fierce struggle. So, as fires consume an ever-widening area of territory and converge on its megacities, as psychotic shootings remain a daily occurrence, the country no longer has a governing government and never will again.

Osama bin Laden’s victory is now final, and the victories of all the great leaders of past history pale in comparison. Bin Laden has defeated the two greatest powers of all time: the USSR and the USA. What happened to the Soviet Union after the Afghan defeat is well known. We are now waiting to see what will happen to the United States, and it is legitimate to hope that the effects will be equally definitive. American society is irreparably split, engaged in a headlong process of social, cultural and psychic disintegration. The civil war is not political, but daily, molecular, omnipresent.

Can we hope, then, that the collapse of American power will restore humans to the human?

I'm afraid not, because this collapse comes too late: America has already largely completed its mission, which was not to establish the kingdom of democracy, as they told us, but to destroy mankind.

John Sullivan coined the expression Manifest Destiny to define the civilizing mission of the American idealists (but weren’t the leaders of the SS, the propagators of the joy of the German superior race, also idealist?). That mission was to bring freedom into the world, or more realistically to transform human life into a mere articulation of the absolute domination of capital.

The stages of this process: primitive accumulation based on slavery and on genocide. Constant intensification of the productivity of workers through the systematic dehumanization of social relations.

That mission is accomplished.

While some big companies (Big Pharma, Amazon, big finance) are making unprecedented profits today, and increasing their earnings every day, psychosis takes over the collective mind, depression is rampant, freely available weapons of war kill unfortunates every day, wages are decreasing, working conditions are increasingly precarious, and in the meantime the forests burn and the cities are hopeless traps.

The purpose of the American wars was not to win. It was to destroy the conditions of life, and to reduce the living to insane ghosts like those who now roam the metropolises of the world. So the neo-human automaton will thrive.

In 1992 the first summit on climate change was held in Rio de Janeiro. On that occasion, the American president, George Bush senior, declared that "the standard of living of Americans is not negotiable."

The standard of living of Americans consists in consuming four times more energy than the average inhabitants of the planet. It consists of psychopathic bulimia that produces obesity and acquisitive aggression.

It consists of consuming meat in insane quantities. And so on.

Consumerism and commercial advertising were perhaps the most decisive contributions to the destruction of the conditions of livability of the planetary environment, as the extermination of the human is intrinsic to the neo-human character of Puritan Protestantism from which the idea of ​​the Manifest Destiny was born. The digital automaton is the accomplishment of this American Dream.

The Swarm

In the twenty-first century, the manifest destiny of the USA has turned into the cancellation of conjunctive impurity, the full realization of the project of integral digitization and connection of the biological within the neo-human flow.

The integral automation project is now underway, but due to a surprising joke (fate is cynical and cruel), it will not be the Westerners that will enjoy it (so to speak).

What is more likely is that the beneficiary of this accursed bonanza will be a nation both more patient and less individualistic, with a people who tends to operate as if in the mode of a unified cognitive organism, and whose vocabulary is not anchored in that most deceptive of words: "freedom."

In pre-capitalist history, technics developed as a structured and functional mode of objects handled by man. In the course of the modern evolution of the capitalist mode of production, however, technology has been transformed into an operational framework within which man is forced to act, and from which he is not permitted to leave.

Following Heidegger, the Chinese thinker Yuk Hui sees in the concept of Gestell or ‘enframing’ the keystone of that transformation whereby technics becomes a key player in the mutation of humanity into a cognitive Automa. Technology establishes Gestalten (structured forms) within which human action is increasingly pre-ordered, to the point of operating like a swarm.

This technological mutation, which found its laboratory in California and which took the West as its field of experimentation, established the "neo human" model of a formatted, compatible, and connected man. Society becomes a swarm in which the movements of individuals are guided by a single brain, on which individual brains depend.

But the experimental automaton is only partially operative in the West, for reasons that are bound up with the cultural and cognitive peculiarities of the individuation process in the Western sphere: the common cognitive basis, linked to language learning, is thin, and resistance to the swarm-model is high.

The automaton seems to work much better in the sphere of ideographic languages, namely China, because the process of individuation is based on a twofold common cognitive basis: the learning of spoken language and the ideographic transcription. The Chinese mind is more easily integrated thanks to the different characteristics of the identification process (language acquisition, double neural molding, easy adhesion to the swarm model).

Cashing-In on Devastation

Sangihe is one of the countless islands of the Indonesian archipelago. The island was once home to a blue bird. It seemed as if the bird had all but disappeared, when it was recently discovered that he still hops in the forests. But there is not only the sparrow, there are also some tens of thousands of people living on the island. Fishermen, gatherers, craftsmen, teachers, students.

Some time back, a Canadian company obtained a concession on half of the subsoil because it was recently discovered that there is gold. Until recently, Indonesian state law prohibited extraction from the subsoil of the islands, but last year international pressure led to the abolition of that law. Extraction is now legal, and the Canadian company that owns the exploitation rights is coming forward to enforce its rights.

This story — documented in a BBC video you can find here — is by no means a new one. It has been like this for a few hundred years: white predators arrive in any place on earth, they discover that they can extract a mineral that has value for the white economy (perhaps a useless mineral like gold, loaded with immense religious significance, to the point that it can be considered the totem of that superstitious belief known as "economics”). The white predators destroy everything, they subject the humans who inhabit the territory to an excruciating pace of work in return for which they give them a salary, a car, a house with all the essential accessories of that mousetrap in which salaried workers are accustomed to dwelling. By now they have destroyed almost everything, so now the world has begun to burn, and will certainly burn, until the human race is erased, except perhaps a few specimens that will manage to escape aboard shuttles into outer space, where they will spend the rest of their sad days in cages floating around in the void.

But some islands of the planet earth have not yet been totally captured by the exterminators, because they are too remote. For example, Sangihe.

To the question: “what will you gain by carrying out your project” (cutting down the forests, drilling the ground, extracting the ore that economic superstition considers precious)? the bald peaceful representative of the mining company replies with a good laugh: “Millions and millions of dollars. When we are at full capacity we plan to extract thousands of ounces a month in a few years."

And there will be work for five thousand people. Five thousand people will be able to stop fishing, build useful objects for the community, study, and will finally go a few hundred meters underground eight hours a day in exchange for a salary that allows them to have a car, to replace their home with a mousetrap and so on.

The story left an impression on me, because it contains nearly everything you need to know about modernity in four and a half minutes of film. The destruction of life, pleasure, beauty, affection, joy, sunrise, sunset, food, breath, in exchange for a car, a salary, and lung cancer — in a word: the economy.

After five centuries there are still places on which such Western ‘care’ has not been imposed. Forests are burning, rivers are overflowing, wars are multiplying, depression is rampant, but somewhere, progress has not yet arrived. Let's bring it there quickly, before the show is over.

It's a matter of years now. Extinction is no longer a distant prospect, but an issue that concerns the present generation, the same one that cannot even go to school because there is a mysterious virus. Before being swallowed by the rapidly spreading apocalypse, we must not neglect to drag the poor inhabitants of Sangihe into it, since they have not yet enjoyed the fruits of Western progress.

This progress finds in the United States of America its vanguard and its symbol.

### Impact—Meltdowns

#### Technospheric breakdown causes global nuclear meltdowns—extinction.

Nadesan ’14 [Majia; September 13; professor of communication at ASU, their interdisciplinary research examines the ethical implications of societal governing logics and risk-management strategies; “The Nuclear Energy Paradigm Collides with Earth Changes and Technospheric Breakdown,” The Millenium Report, themillenniumreport.com/2014/09/will-fukushima-become-an-extinction-level-event]

As Technospheric Breakdown Accelerates, Nuclear Power Generation Mishaps will Increase and Intensify

There is really no way around this eventuality. As all the nuclear power plants age, they will succumb to the micro-stresses which inevitably occur in such an ever-deteriorating environment. Most people are unaware of the true depth and breadth of technospheric breakdown since it is a concept rarely taken up by academia or the media. The following excerpts provide a wider perspective of this unavoidable byproduct of the Industrial Revolution.

Technospheric breakdown is something that occurs everywhere around the globe, 24/7, without interruption, and with tremendous repercussions. Let’s start with anything that has been manufactured in the factories of the modern world or built on the surface of the Earth. Simply put, everything is in the constant state of breaking down, degeneration, deterioration.

What does this really mean when we say that every bridge is slowly breaking down, every road is in greater disrepair with each passing day, every reservoir is gradually degrading, every office building, every factory, every school, every home, etc. most of which adhered to very low building standards in the first place?

What does it mean when the infrastructure for every sewer system, municipal water division, electrical grid, airport, railway station, etc. is in a slow but sure process of degrading and breaking down. So, unfortunately, is every nuclear power plant across the planet. (Cosmic Convergence)

What makes this ongoing process of physical degradation so insidious is that it almost always occurs subliminally. Through a gathering array of various forces throughout post-modern civilization, there does exist a sort of conspiracy of circumstances which has greatly magnified the effects of technospheric breakdown. The completed marriage between the industrial base of the Western powers and the financial class throughout the world has guaranteed that this slow motion collapse will continue unabated. How so?

Because so many corporate decisions are made according to their impact on the bottom line, many inferior nuclear power plants have been constructed around the globe. Likewise, because the mega-banks and investment houses are now dictating to a financially-strapped Nuclear Energy Industry, substandard nuclear reactors have been designed, engineered and continue to be put into operation across the planet. One only has to take a close look at the websites dedicated to decommissioned nuclear reactors or cold shutdowns or partially closed nuclear power plants or emergency actions taken at various nuclear power generation sites to grasp just how precarious a position the entire industry is currently in.

Unknown to even many of the nuclear engineers who address these issues ‘in the office’, or who fix the cascade of problems at nuke plants themselves, is the notion of slow motion, subclinical, pernicious technospheric breakdown. It often manifests in ways where cause and effect cannot be easily established because of some of the unseen forces produced by atomic fission. With that said, it should be noted that a chapter could easily be dedicated to this particular issue alone, so significant is it to the future of nuclear power generation

Then there is the problem of nuclear wastes and natural rights, yes?

No one has articulated this point better than Albert Bates in his definitive essay entitled The Karma of Kerma: Nuclear Wastes and Natural Rights (Bates, A.K., 1988)

This extremely lucid and illuminating, sober and sane treatment of the greatest ongoing environmental disaster of our times lays bare the most basic legal and human rights issues which converge around the production, treatment and storage of nuclear wastes. Were the governments of the world to read and take to heart its simple and straightforward thesis, the current incarnation of nuclear energy production would have been abandoned years ago:

The disposal of radioactive substances in a manner that anticipates their eventual partial release into the human environment imposes a health burden upon future generations that cannot be justified by any moral or legal rationale. Like an irresistible force meeting an immovable object, the concept of the greater good for the many in the present generation runs against the concept of the inalienable rights of each individual in future eras. At present, in matters involving nuclear power, our governmental agencies have taken the side of the irresistible force. But when federal agencies venture to tread beyond of the scope of the foundation principles with which the federal government was fashioned, they endanger more than human lives. At risk in the nuclear waste debate are long-held concepts of ordered liberty. (Bates A. K., 1988)

Fukushima has illustrated exactly why this elegantly stated legal concept of human rights and moral imperative is so pertinent to the public discourse. When massive amounts of radioactive wastewater are dumped into the Pacific Ocean, not only human life will be adversely affected. Marine life has been negatively impacted in ways that will take decades to observe and comprehend. The outright destruction of the environment in and around Fukushima and the Pacific Ocean must also be considered in any meaningful assessment of collateral damage.

Perhaps even more than Chernobyl, Fukushima has allowed the global community to view the whole event through the lens of legal responsibility and ethical outcomes so that new international standards can be written and implemented regarding nuclear waste conveyance and disposal. If nothing else, this discussion has raised awareness about the most nagging issue concerning the NEP. Whereas the human rights aspect confers the legal right to not be contaminated by nuclear radiation has barely been addressed by those responsible for it consequences, it now enjoys a prominent place throughout the worldwide debate.

Accidents and mishaps, manmade and natural disasters happen. Things are fixed fairly quickly in this postmodern age, and life goes on. Whether these events occur in a full-blown war zone or in the wake of a hurricane, the affected population usually does everything it can to rebuild and move on.

However, when these events take place in or near nuclear power plants, life doesn’t just go on. It often stops. Depending on the circumstances and seriousness of a nuclear event, sometimes life stops in that area for a long time.

Our civilization has now been given three unmistakable wakeup calls since the advent of the nuclear power generation era. First there was Three Mile Island in Pennsylvania, then there was Chernobyl in the Ukraine, and lastly the world is still reeling from the specter of possibilities which are presented by Fukushima.

Surely it is not by chance that these three flagrant examples of nuclear Perfect Storms occurred around the globe affecting major nations and populations centers. Each of these disasters has served to wake up whole swaths of humanity to the dangers and risks which are associated with the current Nuclear Energy Paradigm. To ignore, or deny, or refute the obvious lessons which all three nuclear catastrophes have given to humankind would be folly of the highest order.

The global impact of Fukushima, which has disseminated radionuclides (radioactive contaminants) by air and by way of the largest of the seven seas, stands as dramatic testimony to all that can go wrong — seriously wrong — with the current nuclear energy business model and method of power generation. Can it get any worse than Fukushima? That we are compelled to even ask this question speaks volumes about the true state of the affairs on that 25 square mile patch of land and contiguous sea which surround the Fukushima Daiichi nuclear disaster site.

Given this inescapable testament of nuclear folly, it is now incumbent upon the community of nations to rally around the obvious necessity of terminating the current form of the Nuclear Energy Paradigm. Why? Because when a “China Syndrome” occurs anywhere in the world, it will inevitably affect the entire planet. In other words, an INES Level 7 (Wikipedia, International Nuclear Event Scale) nuclear catastrophe does not respect borders. Nor does it discriminate between the young and old, healthy and sick, or those who live close to ground zero from those who live far away.

Therefore, any nation that chooses to set up a nuclear energy-producing operation from this point forward has an inviolable responsibility to its neighbors, as it does to the rest of the world. Likewise, those nations have a moral obligation to proceed in a manner that guarantees its neighbors will not be exposed to the consequences of its nuclear accidents, even when they are caused by duel natural disaster events as we saw at Fukushima.

Just as Europe was contaminated with radiation from Chernobyl (Yablokov, A.V., 2009), and North America has been contaminated from Fukushima, it is understood that once a nuclear catastrophe spirals out of control, the genie of radioactive contamination cannot be put back in the bottle. The entire Pacific Rim, in fact, has varying degrees of exposure to the radioactive waste water being conveyed by the ocean from Fukushima, as does the Western Hemisphere to seaborne radioactive isotopes like Cesium-137 and airborne isotopes such as Iodine-131(Center for Marine and Environmental Radiation).

Consequently, Japan is responsible for the damage wrought to the largest ocean on Earth. Have they acknowledged this? Have they approached the nations both near and far which have been affected by their cavalier and irresponsible approach to siting reactors up and down their seismic shorelines? Has the United Nations even addressed this extremely important issue known as national accountability? Or territorial sovereignty?

Conclusion

It doesn’t get very much more weighty than the ‘fallout from Fukushima’. All of the affected nations have been curiously silent on this issue. It is almost as though a conspiracy of silence has descended upon the concerned countries because of how unpredictable and intractable the nuclear containment problems have been at the Daiichi plant.

At the end of the day the current race of humanity will look back on the Fukushima Nuclear Disaster as the defining moment for both the industry and the underlying paradigm. If they haven’t already, the various stakeholders will be forced to re-evaluate the integrity of their nuclear enterprises around the globe. Hopefully, they will begin to take aggressive preemptive measures to address whatever needs to be addressed at every nuclear site still in operation.

If a decisive response is not formulated and implemented on a global scale, in light of the hard lessons learned from Fukushima, the current planetary civilization will be compelled to face up to these fatal flaws in most unpleasant ways, which will continue to manifest with each major Earth change. In a similar way, the inherent defects of the NEP will only be accentuated as technospheric breakdown accelerates. The profound and fundamental shortcomings which pervade the entire nuclear energy industry can no longer be hidden or ignored.

### Alt—Cloud Ethics

#### The alternative is cloud ethics, which chooses an episteme of opacity over cybernetic transparency.

**Amoore 20** (Louise Amoore, Professor of Political Geography at Durham University, “Cloud Ethics: Algorithms and the Attributes of Ourselves and Others”, Duke University Press, 8/30/20, <https://doi.org/10.1080/1369118X.2020.1800782>) // EL

In this book I propose a different way of thinking about the ethicopolitics of algorithms. What I call a cloud ethics is concerned with the political formation of relations to oneself and to others that is taking place, increasingly, in and through algorithms. My use of the term cloud here is not confined to the redefined sovereignties and technologies of a “cloud computing era,” as understood by Benjamin Bratton and others, but refers to the apparatus through which cloud data and algorithms gather in new and emergent forms. The cloud in my cloud ethics is thus closer to that envisaged by John Durham Peters, for whom clouds are media in the sense that they are “containers of possibility that anchor our existence and make what we are doing possible.” To consider algorithms as having ethics in formation is to work with the propensities and possibilities that algorithms embody, pushing the potentials of their arrangements beyond the decisive moment of the output. A cloud ethics acknowledges that algorithms contain, within their spatial arrangements, multiple potentials for cruelties, surprises, violences, joys, distillations of racism and prejudice, injustices, probabilities, discrimination, and chance. Indeed, many of the features that some would like to excise from the algorithm—bias, assumptions, weights—are routes into opening up their politics. Algorithms come to act in the world precisely in and through the relations of selves to selves, and selves to others, as these relations are manifest in the clusters and attributes of data. To learn from relations of selves and others, the algorithm must already be replete with values, thresholds, assumptions, probability weightings, and bias. In a real sense, an algorithm must necessarily discriminate to have any traction in the world. The very essence of algorithms is that they afford greater degrees of recognition and value to some features of a scene than they do to others. In so doing, algorithms generate themselves as ethicopolitical beings in the world. If to have ethics is not merely to have a code prohibiting, for example, bias or assumptions, but to work on oneself via relations, then the ethicopolitics of algorithms involves investigations of how they learn to recognize and to act, how they extract assumptions from data relations, and how they learn what ought to be from relations with other humans and algorithms. To be clear, the cloud ethics I propose here does not belong to an episteme of accountability, transparency, and legibility, but on the contrary begins with the opacity, partiality, and illegibility of all forms of giving an account, human and algorithmic. To advance a cloud ethics is to engage the ungrounded politics of all forms of ethical relations. The significant new ethical challenges that algorithms seem to present to society actually manifest novel features of some profoundly old problems of the grounds for ethical action. As Judith Butler explains in her Spinoza lectures, the demand to give an account of oneself will always fall short, for “I cannot give an account of myself without accounting for the conditions under which I emerge.” If one assumes that the determination of an unequivocal I who acts is a necessary precondition of ethics, as Butler cautions, then this identifiable self is “dispossessed” by the condition of its emergence in relation to others. For Butler, this persistent failure to give a clear-sighted account does not mark the limit point of ethics. On the contrary, the opaque and unknowable nature of making all kinds of acting subjects is the condition of possibility of having an ethicopolitical life. In short, and in contrast to the equation of ethics with transparency and disclosure, ethical responsibility is sustained by conditions of partiality and opacity. My notion of a cloud ethics extends the opacity of the human subject, envisaging a plurality of venues for ethical responsibility in which all selves—human and algorithmic—proceed from their illegibility. The apparent opacity and illegibility of the algorithm should not pose an entirely new problem for human ethics, for the difficulty of locating clear-sighted action was already present. The I who forms the ethical relation was always in question and is now, with algorithms, in question in new ways. Though the mathematical propositions of algorithms cannot be made fully legible, or rendered accountable, they can be called to give accounts of the conditions of their emergence. These conditions include some relations that are identifiably between humans and algorithms—such as the selection and labeling of training data, the setting of target outputs, or the editing of code “in the wild,” for example—but others still are relations of algorithms to another algorithm, such as a classifier supplying the training data from which a neural network will learn. In all such instances of iterative learning, the significant point is that the conditions of an algorithm’s emergence—a composite of human-algorithm relations—are venues for ethicopolitics. In a discussion on the impossibility of the transparent algorithm, the brilliant and generous scholar of black studies and machine learning Ramon Amaro once said, “Well what would it be if we even could open it? It’s just math.” Of course, he intended the comment as a provocation, but mathematics is never only “just math,” as Amaro’s work vividly shows. To reflect on the conditions of an algorithm’s emergence is also to consider how, as mathematical knowledge forms, algorithms have achieved the status of objective certainty and definiteness in an uncertain world. Ludwig Wittgenstein observed mathematical propositions to be “given the stamp of incontestability,” a mark of the “incontrovertible” and an “exemption from doubt” that other propositions, such as “I am called,” are not afforded. For Wittgenstein, mathematics as practice—like all other language games—is concerned with particular uses of propositions, where “what a proposition is, is in one sense determined by the rules of sentence formation, and in another sense by the use of the sign in the language game.” His concern is that the mathematical proposition has achieved a particular status of certainty in an otherwise uncertain world, so that it becomes “a hinge on which your dispute can turn.” For Wittgenstein, the mathematical proposition should be regarded as no less doubtful or uncertain than the “empirical propositions” otherwise made about the world. Indeed, Wittgenstein’s point is to address mathematical propositions as empirical actions that are “in no way different from the actions of the rest of our lives, and are in the same degree liable to forgetfulness, oversight and illusion.” Following Wittgenstein, the use of mathematical propositions is profoundly social and, in my reading, ethicopolitical. An algorithm is formulated through a series of truth claims about its match to the world, and yet, in its use in the world it is as prone to forgetfulness, oversight, misrecognition, and illusion as any other language game. Algorithms such as those used to detect latent social unrest in the city may appear in the world as Wittgenstein’s “hinge on which your protest can turn” in the most direct sense that the hinge delimits and circumscribes the arc of the politics of protest. But the algorithm as hinge does not merely mark the limit point of resistance; rather, it presents something as a singular optimal output, when it is actually generated through multiple and contingent relations. My cloud ethics considers the algorithmic hinge to be akin to Karen Barad’s scientific apparatus, which decides what matters in the world, what or who can be recognized, what can be protested, and which claims can be brought. Understood in this way, the algorithm is not the hinge as an incontrovertible axis, exempted from doubt, on which all social, political, and economic life turns. “The hinge point,” as Foucault differently identifies, can also be the point of “ethical concerns and political struggle,” as well as the point of “critical thought against abusive techniques of government.”

### Alt—Ecological Ethics

#### Vote neg for a reorientation of human agency towards a co-evolutionary assemblage with technology.

Sy Taffel 19 - Senior Lecturer in Media Studies and co-director of the Political Ecology Research Centre at Massey University, PhD at the University of Bristol. “Digital Media Ecologies.” Google Books. Oct 2019. [https://www.bloomsbury.com/us/digital-media-ecologies-9781501349263/,](https://www.bloomsbury.com/us/digital-media-ecologies-9781501349263/)AG

Given the current forecasts for the Anthropocene, an ecological ethics emphasizes the urgent need for modifying current practices. As Cubitt (2005: 59) astutely observes, ‘Techne is the only route through which we can now sense the world, most especially the part of the world’s conversations which are not conducted in wavelengths we can hear, see or otherwise comprehend.’ Without contemporary information-processing technologies, humans would not have sufficiently developed understandings of looming ecological crises to enact urgent calls to action. This is exemplified by the fact that when considering climatic trends, we are addressing global datasets with durations measured in decades and centuries – a temporal scale far slower and a spatial scale far larger than those readily perceptible to humans.

We can only understand climate change via technological mediations which allow us to see enduring trends within noisy, chaotic and complex global climatic systems. This technocultural assemblage includes satellites that measure tropospheric temperatures, thermal drills that can extract 3-kilometre-deep ice cores from polar regions and the storage facilities that preserves these geological artefacts, and the supercomputers that are used to simulate climatic futures. Ecological ethics, then, must not advocate abandoning mediation and technology as a means of retreating to a romanticized past but instead requires reorienting modes of production and consumption towards ecologically beneficial outcomes. Only through repurposing technics along ecological lines – creating commonwealth rather than commodities – are potential solutions to ecological crises likely to become visible; there exists no option to return to a pre-industrial state before technics supposedly altered the harmonious ‘balance of nature’, as is commonly suggested by conservationist and deep ecological discourses.

Applying such an ethics to contemporary media practices means considering the ways in which media systems at varying scales create novel connections and forms of commons and public good, and at the same time involve the usage of energy and materials which close off other avenues via their ecological costs. Ecological ethics is based on praxis rather than pure reason, encouraging experimentation and creative interventions designed to produce positive biopolitical impacts. It entails realizing that while there are detrimental consequences stemming from currently produced technologies, there are bifurcation points whereby the agential capacities of assemblages afford meaningful positive changes to be made to these systems by using theoffending technologies. This is not hypocrisy, but does require a praxis that abandons an idealistic purity.

At the level of content, this means exploring how information flows have created the commodified economy of attention, problematic discourses of Big Data and the context of communicative capitalism, while investigating how ideology, cognitive frames and cognitive dissonance act as brakes which prevent subjects from altering opinions and effecting change. At the level of software, this entails considering issues surrounding licensing, software development and the types of freedom maintained by the free software movement, alongside issues surrounding surveillance, user privacy and the contemporary movement towards the commodification of web protocols as evidenced within HTML5. Within the realm of hardware, this involves examining the flows of energy and matter which comprise and maintain the physical architecture of the network society, considering the material impacts that these flows have on ecological systems at every stage in the life cycle of microelectronics devices. Across all scales this additionally requires an examination of the multiple ways that powerful actors seek to utilize existing and novel hierarchies to perpetuate privileged positions and technocultural systems that are currently leading us towards social and ecological catastrophe.

Media ecology suggests that an experimental praxis with various commons-orientated projects across the scales of content, software and hardware is necessary if ecologically resilient and equitable alternatives are to supplant current practices of mediation. While openness is often proclaimed to be the defining characteristic of commons-based peer-to-peer systems, media ecology follows Bauwens in arguing that openness alone is not enough to guarantee ecologically beneficial outcomes. Alongside openness, projects require commitments to social solidarity and ecological resilience if they are to escape reterritorialization.

Rather than an abstract mode of thought, ecological ethics emphasizes embodied acts of engagement as a method of becoming-ethical. Praxis additionally forms a model which resists contemporary processes of proletarianization, which sees knowledge becomes embodied within technologies, constituting an industrialization of memory and the externalization of communal knowledge into corporate technics. Without some degree of knowledge and experience regarding the complex and distributed processes of mediation which are increasingly central to contemporary life, we have little agency to affect and alter these assemblages along eco-ethical lines. Ecological ethics contends that such knowledge is derived from material practices rather than abstract speculation; following Deleuze, we do not know what a digital assemblage can do, but through experimentation we can produce forms and practices that can help to realize change. ‘Make a rhizome. But you don’t know what you can make a rhizome with, you don’t know which subterranean stem is effectively going to makea rhizome, or enter a becoming, people your desert. So experiment’ (Deleuze and Guattari 1982: 277). We cannot exhaustively know the capacities of systems in advance of this practical activity, so the process of activism, of creating projects, itself opens up points of critical instability and forms lines of flight that can lead to more equitable and resilient futures.

This does not, however, imply that such knowledge leads to mastery and control. Indeed, a basic comprehension of complex systems entails realizing that unilateral control is impossible. Unlike humanist accounts of agency which relegate technics and nature to the status of Cartesian automata, systems which are teleologically bound to particular pathways, media ecology contends that agency is a distributed property, existing throughout assemblages, rather than being an innate quality applying to one particular type of node. While forms of agency differ between varying types of actor, the diverse examples explored in this text have tried to elucidate numerous ways that nonhuman actants realize differential forms of agency.

Understanding the multiplicity of nonhuman agencies at play in technological systems – those associated with algorithms, codecs, file formats, operating systems, minerals, metals and energy supplies – has been posited as key to understanding ways that these ensembles, along with humans, work together to form media ecologies. Improving our understandings of the media systems we are entangled with entails comprehending various forms of nonhuman agency, how they manifest and what kinds of selection pressures they apply to the evolution of technical ensembles. Stiegler’s account of the human as being fundamentally defined by its co-evolutionary relationships with technologies, which form an exteriorized mode of distributed and collective memory is useful here, insofar as it reminds us that ‘we’ do not exist outside of our technical support systems and suggests that the varying agencies which technologies mobilize produce divergent ethical and political imperatives. This goes beyond claims that ‘technology is society made durable’ (Latour 1990), which suggests that society precedes technology (which allows the former to endure), rather than there being a mutually constitutive co-evolution of technology and society.

### Alt—Digital Socialism

#### Vote negative for movements of digital socialism

**Kwet 21** (Michael Kwet, Yale Univeristy – Information Society Project, “People’s Tech for People’s Power: A Guide to Digital Self-Defense & Empowerment”, *Right2Know Campaign*, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748901>) // EL

Let us begin this chapter with a simple observation: no country will ever become wealthy when the critical infrastructure powering its economy is owned and controlled by foreign corporations. South Africa’s modern history arises from a European-led invasion by the Dutch East India Company, who stole the land and brutally exploited the indigenous people for profit. Critical infrastructure and resources – railroads, mines, industrial equipment, housing, and land – were dominated by white settlers at the expense of the African people. White authorities also waged psychological and conceptual warfare on the population through the imposition of colonial interpretations of religion, culture, and political economy. Bantu education sought to instill passivity and acceptance of race and class-based inequality. Today, US-based corporations are colonising digital technology. Instead of taking over the land, they are colonising critical digital infrastructure and human knowledge. They seek to own the world’s knowledge and culture (intellectual property), the material infrastructure (cloud server farms, transoceanic cables, and other hardware), the code powering computers (software), and information about people and nature (data). Converting knowledge into private property is foundational to their system of domination. When Big Tech corporations do share knowledge, it is done in ways beneficial to themselves. Google and Facebook, for example, are happy to “open source” some of their artificial intelligence software (e.g. Tensor Flow and PyTorch) because they use it to monetise Big Data surveillance.xviii Yet if their access to surveillance data were shut out by new technologies and privacy laws, they would close off much of their “open source” technology and increase the share of proprietary code in the software market. The problem we face today is digital capitalism and authoritarianism, not simply surveillance capitalism. As I previously wrote in the Mail & Guardian, the Fourth Industrial Revolution (4IR) narrative claims Big Data, intellectual property, centralised clouds, the Internet of Things, “smart” cities littered with surveillance, automation, algorithmic decision-making, Big Tech corporations, and surveillance capitalism are the way of the future. A creation of the ultra-capitalist World Economic Forum (WEF), the 4IR concept is an elite construct which serves a useful purpose at the periphery of empire by steering inquiry about tech into the WEF agenda. Like the colonial missionaries of past, they preach a new religion, the 4IR, as the saviour of society. Not surprisingly, the tools they promote are the tools of the masters: corporate ownership, intellectual property, centralised clouds, Big Data surveillance, the profit incentive, and private production for the market. This will not work for the common person. As Audrey Lorde put it, “the master’s tools will never dismantle the master’s house”. The threat of proprietary technology – and the selective sharing of knowledge by corporations – was captured by Archbishop Desmond Tutu, who stated in 2007: Freedom is an ongoing process, and not an end in itself … We are not shy to use the word freedom, and do so in contexts where its importance is not always recognised. In a digital world, there are many threads to a hard-won liberty. There are those who take our ideas and lock them up for business gain. There are those who will take the fruits of the human mind and lock them up, dishing them out to us in meted amounts for a fee that locks most of our people out. And there are laws that are reserved for business reasons and changed to rob society of its own rights ... To paraphrase Edmund Burke, who said, ‘the only thing necessary for the triumph of those who take away our freedom in the digital world is for organisations [like universities] to do nothing.’ But there are people, like our keynote speakers … who are not content to do nothing. Indeed, there is a whole movement that is rapidly gaining momentum worldwide arising out of the work of people like Free Software Foundation founder Richard Stallman, creating socially responsible businesses out of the very freedoms that we are talking about. Free Software and Open Source, Free and Open Resources for Education, new ways to create and share cultural artifacts such as music, writing, and art – all of these are changing the world for the better. Unfortunately, intellectuals who believe themselves to be "critical" of Big Tech have formulated a liberal imperialist narrative called the "techlash" that fails to address digital colonialism. These USEurocentric "critics", drawn from elite Western university and media outlets, ignore the centrality of property and the Free Software Movement. Much like the Sullivan Principles during apartheid,xix their solutions offer minor reforms that maintain US interests, such as weak privacy laws, "competitive markets" created through antitrust, and corporate ownership of the digital ecosystem. The "techlash" extends Francis Fukuyama's "end of history" to tech, where nothing fundamentally different can occur other than what we have seen in the West. If we are going to create a society that prioritises freedom and equality, we will have to develop a new framework to restructure the digital ecosystem. This requires more than the array of Free Software technologies outlined in this guide. We must also have supportive laws, critical education, and a grassroots movement to counter digital colonialism and replace it with a democratic digital commons owned and controlled directly by the people. There is no way around this. Laws like POPIA are designed to safeguard surveillance capitalism. This can be seen in its provisions that allow Big Data surveillance to flourish with mild restrictions said to “protect” your privacy. Under POPIA, exemptions include data processed for national security, such as “defense or public safety”, instances in which “the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject”, and instances where the processing provides “a clear benefit to the data subject or third party that outweighs … interference with [their] privacy”. The “public interest” includes “national security”, “the prevention, detection and prosecution of offences”, “important economic and financial interests of a public body”, and “historical, statistical or research activity” (as well as the “special importance of the interest in freedom of expression”). POPIA also allows people to “consent” to Big Data surveillance through terms and conditions, defined as “any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.” Yet we know that nobody can read these terms and conditions, even if they wanted to. One study showed that the average person would have to spend about 76 working days per year to read the Terms and Conditions of the websites they visit. Google South Africa sent me about 20,000 words of “terms and conditions” covering the Google technologies used in South African schools. Users can either “consent” to Google’s data processing, or they can’t use its technologies at all. Forcing people to endure surveillance just to visit a website, join a social network, or use a weather app, on the basis that they “consent” is unjust. Yet POPIA does not appear to prohibit this “take it or leave it” surveillance society. Digital capitalism has a business model crisis. It concentrates and extracts wealth, cedes authoritarian control over digital experiences to transnational corporations unaccountable to the public, and subjects users to surveillance, advertising, and manipulation. If it moves to a “pay-for-ethicaltreatment” model, it will generate class inequality, especially for the poor who have no disposable income. In a commons-based system of digital socialism, knowledge is free and open for all to consume, modify, and share. Free Software, interoperability, federated services, and decentralisation tools provide the public with the means to own and control their experiences. To support the global commons, production and maintenance of digital technology and culture could be paid for by the rich through progressive taxation and heavy taxes on Big Tech corporations. This requires a Tech New Deal that transforms the digital ecosystem from a profit-seeking enterprise into a publicly funded global commons. A movement for digital socialism dovetails with efforts to build an environmentally sustainable global economy based on wealth redistribution and equality, not limitless growth. Many of the core technologies powering the digital revolution were funded by the state, including computers, the internet, and GPS. The state also supports the education of computer scientists and engineers. Research and development institutions like the CSIR could help develop decentralisation technologies like FreedomBox instead of surveillance systems like Cmore. University researchers could work on voice assistants like Almond, which does not spy on its users, as they are doing at Stanford University. With enough funds from taxes, talented developers could be awarded comfortable middle-class salaries to work on public interest technologies, instead of joining exploitative institutions like Google and Microsoft, who pay researchers a few million rand per year. As noted in previous chapters, government policy can require the use of People’s Tech in schools, universities, and the public sector; protect user privacy; and teach people about tech freedom. But none of this will occur without you. Technology corporations have concentrated enormous sums of wealth into the hands of a few, and they will not give it up without a serious fight. It doesn’t help that elected representatives are tempted to exploit corporate tech for their own surveillance and control. Nhlanhla Mabaso, a champion of Free Software, headed the Open Source Centre – since renamed the Meraka Institute – at the CSIR. (“Meraka” is Sotho for “open grazing land”.) In a research interview, Mabaso told me some of his colleagues argue the government’s Free and Open Source Software policy preference means “open source is law” in South Africa. Efforts by Mabaso and his peers once aimed to undermine the power of corporations like Microsoft from colonising the South African tech ecosystem. Decades earlier, anti-apartheid activists protested against the use of computers from tech corporations like IBM to facilitate the apartheid system. They eventually forced IBM to withdraw its business operations from South Africa. During the struggle against apartheid education, Zwelakhe Sisulu asserted: We are not prepared to accept any ‘alternative’ to Bantu Education which is imposed from above. This includes American or any other imperialist alternatives designed to safeguard their selfish interests in the country, by promoting elitist and divisive ideas and values which will ensure foreign monopoly exploitation continues. Only through democratic institutions and committees could students, parents, and teachers take control of their own education. “We are fighting for the right to self-determination in the education sphere as in all other spheres … It has become a struggle of the whole community with the involvement of all sections of the community”, Sisulu said. In the neoapartheid era, a new wave of US tech transnationals are pushing oppressive products into the country once again. A People's Tech movement to kick Big Tech out of Africa could form a critical part of the global protests against the enduring legacy of racism and colonialism. Activists across the world could unite to form a targeted boycott, divestment, and sanctions (BDS) movement centered on Big Tech corporations and their supporters in the United States. South African communities are tasked to build a digital ecosystem that the people own and control, so they are not subjects of American or any other imperialist powers. People’s Tech for People’s Power, a holistic solution based on a Free and Open Source technology commons, socialist legal solutions, people's education, subsidies for public interest technology, and a vigorous grassroots movement, is urgently needed to avert disaster and build a truly democratic and egalitarian society.

### Alt—Governable Stacks

#### Vote negative to pursue insurgent governable stacks that reassemble the technical layers of the cybernetic episteme in ways that fractally spill up to align with radical struggles across the globe.

Schneider, 22—assistant professor of media studies at the University of Colorado Boulder (Nathan, “Governable Stacks against Digital Colonialism,” tripleC 20 (1): 19-36, 2022, dml)

The spinning wheel remains a cipher and a site of conflict, an everyday technology summoned to a contest over the meaning of democracy. Despite having political ties with Gandhi’s assassin, the Hindu nationalist prime minister Narendra Modi promotes homespun cloth and has done photo-ops operating a spinning wheel. Modi has meanwhile shuttered boards that gave artisans a voice in policy under the slogan “Minimum Government and Maximum Governance” (Vincent 2020). The technology itself does not guarantee self-governance, but it can be the symbolic base from which ever-enlarging acts of self-governance defeat an empire.

In the spirit of the technological cipher I propose the pursuit of “governable stacks”: an orientation toward ungovernable organising under digital colonialism.

The geek-colloquial meaning of stack, in the most relevant sense, is a set of interoperating hardware and software. Benjamin H. Bratton (2016, xvii) goes further, describing the stack as “a new architecture for how we divide the world into sovereign spaces”. Its layers come with intersecting relations of dependency, along with emergent freedoms. A stack might include all that enables one to use a social media service, for instance: the server farms, the corporation that owns them, its investors, the software the servers run on, the secret algorithms that analyse one’s data, the mobile device, its accelerometer sending biometric data to the server farm, the network provider, the backdoor access for law enforcement, and so on. The layers of a stack might further include the sun or coal powering it, the wars fuelled by rare-earth mining, and the mythologies and rituals that dictate what people in it will tolerate. Each layer is in fact multiple layers, and layers build on each other.

Before governable stacks were the topic of this article, they were an experience for me, particularly through an organisation in which I have been an anecdotal participantobserver for a decade. May First Movement Technology (mayfirst.coop) is a cooperative that provides web hosting, cloud services, and public education for a 850-strong membership composed largely of activist organisations in the United States and Mexico (Lopez et al. 2007). Through the tools May First offers, I have been able to move much of my daily computing away from companies that surveil and extract into servers I co-own and govern, running commons-based software. I have formed relationships with the people who maintain these services and participated in decision-making over bilingual conference calls and online ballots. I learn about new tools from fellow members, and we sponsor events that teach people outside our membership how to challenge the power of big tech in their lives and their communities. Akin to the slow food movement, this is slow computing (Schneider 2015), its pace measured not by bandwidth or processing speed but by the attention to the social dimensions of everyday practice.

While Silicon Valley elites escape to phone-free retreats (Marantz 2019) and agonise about their children’s exposure to screens (Bowles 2018), May First offers no such “abhorrence of machinery” (Chaplin 1966, 373). It does not accept the false choice between addictive, surveillance-addled apps and a fantasy of returning to some blissful innocence. Instead, members share technologies that do what they need and that they can reasonably control. These technologies, and the self-governance we surround them with, are our stack. May First does not demand that you ‘learn to code’, or otherwise trade traditional knowledge for digital expertise. For me, being part of a governable stack like May First has unlocked political possibilities. The experience motivated years of working to build governable stacks elsewhere, because I know that it can be done. I poured myself into developing alternative ownership models like “platform cooperatives” (Schneider 2018) and “exit to community” (Mannan and Schneider 2021) that are better suited to making tech governable. With time, ungovernable stacks have come to feel like foreign lands. I may use them, but they never feel like home.

Governable stacks are cyborg assemblages of inter-operating technology, in symbiosis with human relationships (Haraway 1991; Puar 2012). Those relationships organise power, in partnership with the technology more than through domination over it. We learn with each other, and we learn with the machines, which take on life of their own – through their own intelligence, or that which we affectionately project onto them. In the sense of Grace Lee and Jimmy Boggs’s dialectical humanism, governable stacks invite the people who use them to change their relationship with technologies, to imagine different sorts of technologies, and to be changed themselves.

Perhaps governability can be achieved by reconfiguring tools that already exist; perhaps it is necessary to make new ones. Tiziana Terranova (2014), who has proposed the complementary idea of a “red stack”, writes that insurgent stacks become “new platforms through a crafty bricolage of existing technologies, the enactment of new subjectivities through a detournement of widespread social media literacy”. Older technologies may be better suited to this than newer ones (Maxigas and Latzko-Toth 2020). Even the colonial platforms can be repurposed – as the Algerian writer Kateb Yacine said of the French language – as spoils of war. The lifeblood of the governable stack is not any claim to innovation but the self-governance that flows through it. What emerges from there is the point.

The Guifi.net community Internet network in Catalonia (guifi.net) became the condition of possibility for a suite of “community cloud” services deployed through it (Selimi et al. 2015). FairTEC (fairtec.io) combines into one product a stack of preexisting services across three European countries: a sustainably manufactured smartphone, a non-commercial operating system, a cooperative telecom, and a cooperative phone rental company. The developers of the CommonsCloud (commonscloud.coop) see their shared technology as only one layer of a larger community stack, which also includes “social” and “discursive” layers – the context and substance of their self-governance. Layers form over time, too. Governable stacks of the past lurk in the archaeology of colonial systems through legacies like Indymedia, an activist social network whose participatory servers and software prefigured the corporate “Web 2.0” (Pickard 2006). Indymedia itself drew from decades of organising among activist communityradio stations, particularly in Latin America (Ruiz Martinez 2021). There can be no one governable stack – only many, whose archipelagos of commoning enable each other and give rise to more.

Technologists seeking alternative visions have often gravitated to the Free Software and Open Source movements, which employ creative licensing to enable the sharing of accessible and modifiable code. These movements have been successful in terms of the sheer volume of widely used software in their commons. But their emphasis on the freedoms of individual users, as well as of corporations, has privileged those with the technical know-how to take advantage. The software commons has spawned operating systems that fly in military jets and databases that aid in the imprisonment of asylum seekers (Ehmke 2020). In the name of freedom, too, developers have harboured sexism and other forms of exclusionary culture (SSL Nagbot 2016). Governable stacks should prioritise community accountability alongside individual freedom.

Another emerging strategy for challenging digital colonialism has come from within. Employees at Silicon Valley giants have achieved reforms by organising against certain ethical outrages at their workplaces (Tarnoff 2020). Yet there are limits to what these campaigns are likely to achieve, since these workers are invested – often literally, through stock options – in the basic business models of their employers. Employees’ actions can present the impression that their protest cleanses the colonial tools they produce. Governable stacks do not seek merely to improve the occupier. “Decolonization is not an ‘and’”, as Tuck and Yang (2012) put it. “It is an elsewhere” (36).

Experiences with governable stacks introduce us to possible elsewheres. The spinning wheel was an elsewhere, the invention of a democratic India. May First Movement Technology is an elsewhere for its members, who in turn become part of its learning and evolving. Collectives, families, and movements can assemble and adjust their stacks over time, wherever possible seeking to make their technological lives ever more governable. I next turn to strategies to guide the process of doing so.

5. Governable Strategy

May First is infinitesimally small by the standards of the tech economy. “Goldman Sachs doesn’t care if you’re raising chickens”, as the political theorist Jodi Dean (2011) has said. It’s a reminder for anyone tempted to see too much potential in personal practices, technological or otherwise. But spinning wheels are small, too, and they helped drive away the British Empire.

adrienne maree brown (2017) credits Grace Lee Boggs for helping her see that (her emphasis) “what we practice at the small scale sets the patterns for the whole system”. She explains this in a chapter called “Fractals”, which recalls how she shifted her activism to better reflect her political values in daily practice. Fractals are mathematical phenomena, frequent in nature, whose patterns at smaller scales repeat at larger scales. They are appealing and widely used as a metaphor, being both mathematically precise in theory and conveniently vague when applied to human affairs. Those like brown and Boggs who apply fractal-talk to politics exercise a kind of faith. To make good on that faith, there must some linkage, some strategy, that connects self-governance from the scale of small communities to the larger societies those community seek to transform. There was a fractal in the free maroons of Saint-Domingue who stormed down from their mountains into combat with French troops so the whole island could be free.

There was a fractal in the spinning wheel on the Indian National Congress flag, extending from a traditional practice to an eventual industrial policy. These chickens came to roost because they were part of a strategy that involved organised confrontation with colonial power. Self-governing became a challenge, a threat. In even small experiments, governable stacks can begin to normalise the otherwise elusive fact that better ways of organising technology are possible. Carefully chosen practices sever habits of dependency on the systems we seek to resist.

It is an uncomfortable matter of fact that nowhere has been so successful a counterweight to the power of Silicon Valley as China. The country has not only barred certain data-colonising companies with its ‘Great Firewall’ but has cultivated comparably ubiquitous Internet firms, using comparably invasive colonial practices to produce platforms that are at once hyper-capitalist and dominated by state interests (Chu 2017; Hong 2017). And yet China’s policy of sovereignty shows that dependence on hostile stacks is not inevitable.

Rather than trading one colonial power for another, Western Europe has sought a high road in demanding privacy regulations and investments in commons-based technology (Lemley 2020). Projects such as the Sovereign Cloud Stack (scs.community) seek to supplant reliance on corporate walled gardens with globally replicable, locally deployed tools. Several European governments have adopted and funded free/open-source software like the Matrix (matrix.org) messaging protocol and NextCloud (nextcloud.com), a file-sharing platform. Countries far from the power centres, like Uganda and Lebanon, have experimented with imposing taxes on the use of foreign social media (Boxell and Steinert-Threlkeld 2019). Although such efforts have been widely perceived as acts of repression more than solidarity, similar policies could be used for different goals. Echoing the Cold War-era Non-Aligned Movement among countries caught between the United States and the Soviet Union, some have been calling for a “digital non-aligned movement” that asserts many diverse sovereignties against the duelling forces of Silicon Valley and Shenzhen (Freuler 2020; Mejias 2020).

Sovereignty need not be solely the purview of nation states. The discourse of digital sovereignty has been particularly important among indigenous communities whose members are used to seeing their pre-digital sovereignty effaced; they have developed governable stack-layers such as tribal broadband lines (Blackwater 2020), cryptocurrencies (Tekobbe and McKnight 2016), data governance (Carroll et al. 2020), and linguistic autonomy (Pinto 2018). Amelia Winger-Bearskin (2020) draws on the Haudenosaunee practice of wampum agreements to propose “ethical dependencies” in software; these would encode and enforce certain commitments up and down the stack. Laying claim to collective sovereignty is central to such practices. Glen Sean Coulthard (2014) challenges the “colonial politics of recognition” – when people accept their colonisers’ definition of their sovereignty, rather than their own – to insist on more autonomous forms of self-determination. He describes how tribal nations can produce sovereignty through “community-scale activities” such as cooperatives and assemblies in everyday life (68). The indigenous organiser Berta Cáceres, before her murder by Honduran paramilitaries, denounced the pseudo-democracy of political representatives but affirmed the “decisive” democracy possible through poor people’s movements (Castellanos and Pine 2020).

Sovereignty can occur at levels ranging from the network backbone to last-mile connections, up through the hardware and software of devices, to the collaboration tools in the cloud. Sovereignty looks like a user-owned cooperative or a city providing connectivity, or like Douglass (douglass.io), an operating system whose apps take their names from icons of Black liberation. The tech publication The Markup has paid a “privacy tax” by developing its own software that protects user data rather than adopting the standard surveillance-based offerings (Angwin 2020). For Archive of Our Own (archiveofourown.org), a fan-run fandom repository, sovereignty puts creators in control of how they publish and protects their work against copyright overreach. What makes technology sovereign is when its stewards are the people who depend on it, protected from outside control by any legal or extra-legal means available. The data, the algorithms, and the interfaces are for their users, rather than acting surreptitiously against them.

5.2. Democracy

The other side of sovereignty is participatory democracy – its guarantor and its everyday practice. Here we resist the temptation of autocratic vanguardism by designing governable stacks to be accountable and alive. The style of democracy may be that of the Debian operating system, a constitutional republic of coders (debian.org/devel/constitution), or like the Ethical Source Movement’s vision of many collectives deciding on the ethical limits of how their software can be used (ethicalsource.dev). Digital democracy is beginning to have dedicated tools – from smaller-group decisions on Loomio (loomio.org) to the scale of cities or countries through Barcelona’s Decidim (decidim.org) or Polis (pol.is), which is employed by the government of Taiwan (Stempeck 2020). Platform cooperatives practice democracy at the level of the company, such as at Stocksy United (stocksy.com), co-owned by artists in dozens of countries (Schneider 2018). On a network scale, the federated social network Mastodon was able to counteract an incursion by the alt-right platform Gab, as it did earlier with Islamic State accounts – through self-organised activity by server administrators and app developers (Caelin 2020). Countering hate speech doesn’t need to depend on the might of a global monopoly; it can be tangible and empowering.

Practices of local democracy from the Global South have been migrating into governable online tools. Participatory budgeting practices originating from Porto Alegre, Brazil (Cabannes 2004), have appeared in apps like Cobudget (cobudget.co) and Decidim. A founder of an experimental political party in Argentina, Partido Red, has applied the same logic of “liquid democracy” to a blockchain-based governance platform, Democracy Earth (democracy.earth). Mexico City’s 2016 exercise in crowdsourcing its constitution has been studied as a model around the world.

Digital democracy has the potential to evolve rapidly and creatively. People can participate in far more rapid and fine-grained ways than was possible when the prevailing regimes of corporate and state governance first appeared. Organisational designs that work well could become part of a governance commons, enabling other groups to adopt, adapt, and share them back into the common pool (Schneider et al. 2021). In this way, small-scale accountability can spread, and it can creep into larger and larger kinds of communities, demonstrating that colonial control was never necessary. The more we demand and practice the arts of self-governing, the harder we are for someone else to govern.

5.3. Insurgency

The spinning wheel stood for household autonomy, but it was also defiance against British rule. Governable stacks must be similarly insurgent. Some of the earliest online social media emerged through Indymedia’s coverage of anti-capitalist protests. Twitter has its roots in technology for coordinating street protests (Costanza-Chock 2020, Chapter 3). While investors and accelerators receive frequent credit for innovation, insurgency is just as much a source of it.

Insurgency might mean challenging government subpoenas of member data, as May First has done, or facilitating leaks about abuses of power. Resistance might take the form of what the Catalan Integral Cooperative calls “economic disobedience” (cooperativa.cat/economic-disobedience), which includes refusing to pay unjust taxes or interest. Insurgents might choose not to submit the data of a friendship to the social graphs of colonial platforms, or to actively deceive those platforms, just as the Tor network (torproject.org) disguises its users’ locations. Like Copwatch groups or the Driver’s Seat Cooperative (driversseat.sco), insurgents can do data collection on the colonisers, sousveillance from below (Browne 2015).

To the extent that establishing the expansionist, slaveholding republic of the United States was also an anticolonial conflict, it relied on self-governance as resistance. The colonists organised through a Continental Congress, which extracted lessons from the Haudenosaunee nations – yes to confederation, no to matriarchal authority – to prefigure a future government. After independence, Alexis de Tocqueville (1840/2006) observed how the flourishing of civic associations energised the politics of the fledgling republic. Successful poor people’s struggles against the country’s wealthy elites, from the 19th-century Populists (Goodwyn 1978) to the 20th-century movements for Black power (Nembhard 2014), grew out of tangible collective organising in labour unions and cooperatives.

Insurgents might use colonial platforms for education and organising. They might spread viral messages and enjoy themselves. But if they have governable stacks to go back to, they are more than just subjects. They are maroons, with swamps and forests of their own.

### Alt—Radical Nonpreference

#### We must turn to the question of the dream in politics and the question of politics in dreaming. The alternative is radical nonpreference – a radical formulation of subjectivity that dwells in the gap between individualism and individualization to create new collectivites and embrace the contingency of the world.

Gray and Eloff, 22—School of Philosophy at North-West University (Chantelle and Aragorn, “Fabulation in a Time of Algorithmic Ecology: Making the Future Possible Again,” *Technology, Urban Space and the Networked Community*, Chapter 5, 105-133, SpringerLink, dml) //ansel recut [pharmakon=something which is both poison and cure simultaneously]

The answer to our problems does not lie in primitivism or any other return to a (mythical) better past. We are here; we need to find ways to deal with now if we are to rescue the future. The answer, equally, does not solely lie in reform. Rather, we need to ask what we want our societies to look like—and here we can look to the past for some ideas without returning to it. **In short, we need to foster new forms of collectivity in the maze of individualism and individualisation**. This requires radical new formulations of subjectivity that take into account our contemporary situation. Like Bartleby, it might consist of a preference not to, which is neither refusal nor acceptance: it simply “posits an impossibility” (Deleuze 1997, 71). **This impossibility or nonpreference produces a tension, an ambiguity that creates a path for escaping the neurosis of the world**. That is, the little fissure it creates gives way to a mapping of trajectories away from subjugated groups and towards new types of group subjects that do not merely concede to the present, either in terms of an eschatology of techno-singularitarianism or hikimomori-style withdrawal. For Guattari, this involves processes of resingularisation, where singularisation refers to a self-organizing process that at its most basic level concerns bringing together ensembles of diverse components (material/semiotic; individual/collective), that is, assemblages … that deploy their own intrinsic references (inventing relations with the outside as well), and the analysis of their effects (especially transformations) on the formation of subjectivity beyond the individuated subject and prefabricated versions of ~~him/her~~. [them](Genosko 2001, 129)

Far from the homophile groups of online life, this requires, as Guattari foresaw, an injection of heterogeneity where individuals can be confronted with ideas dissimilar from their own and opportunities to talk this through rather than reactively cancelling 27 someone. It requires forms of offline life that nurture transgenerational, intergenerational, interpersonal, personal and pre-personal long-circuits in order to reach the Neganthropocene, a place of dreams. As Stiegler puts it: we must turn to the question of the dream in politics and the question of the politics of dreaming—where dreams would be the resource of any neganthropogenesis, that is, any exosomatic organogenesis such that it would preserve its future by maintaining its noetic capacity. (Stiegler 2019, 162)

**These new social practices** of liberation—yes, **of dreaming—cannot be based on new hierarchical relations**. Instead, one of the main goals needs to be the creation of new alliances, a transversal politics, “that confers to these initiatives a character of living subjectivation and irreplaceable experience, that ‘is worth being lived’, that ‘gives meaning to life’” (Guattari and Negri 2010, 125). In short, we are looking for health. Interestingly, for Deleuze and Guattari, as for Nietzsche before them, health is not opposed to illness; rather it is the “immanent process whereby illness brings about its own autocritique and self-overcoming” (Tynan 2010, 155). The illness of our time therefore needs to be transmuted in order to create new ways of living again—and this is of course the schizoanalytic practice. The aim is to see our current algorithmic articulations as a pharmakon—that, precisely, is Bartleby’s stance. It is a productive paradox, an affirmation of life and the future, rather than a negation of it. Importantly, though, it is only with the pharmakon that knowledge takes care of the pharmakon … **the whole manifold of life-knowledge—which passes through rituals as well as habitus, trades and forms of worship** [cultes] that are found in any society insofar as it consists in a social cohesion that is a collective individuation, cultivating, through these always diverse pathways, the organic and organological solidarity in which it consists. (Stiegler 2019, 224)

The individualist, individualising societies we currently find ourselves in have not only lost their means of tertiary protention, but a memory of what a society is and can be: that which allows the development and co-creation of individual and social freedom; where material goods are produced in order to meet the physical needs of everyone in a society, rather than satisfy the insatiable requirements of capitalism; where free and equal social relationships are fostered so that people can flourish mentally and emotionally and, in turn, develop their ethical and creative capacities.28 If this is the basis of our society, algorithms would have a very different function and that, we hold, is more important than reform.

### Framework—Epistemology Key—cybersecurity

#### Cybersecurity is an assemblage of knowledge and power. Their interpretation functions as cybernetic obfuscation to hide its operations.

Dyer-Witheford and Matviyenko 2019—associate professor of information and media studies at the University of Western Ontario; assistant professor of communication at Simon Fraser University (Nick and Svitlana, *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*) //ansel

These definitional debates are not abstract semantic disputes. As Robert Kaiser (2015) argues, since 2000, **cyberwar** has named **an emergent “knowledge power assemblage,” mobilizing institutional powers**, lavish budgets, and lucrative career paths. **It has become the core of a discursive “resonance machine,” with its own “catalyzing agents,**” **“shimmering points” of elaboration, refinement and subtle discrimination, and “centers of calculation,” focused around the materialization of a “new policy object**” (Kaiser 2015, 11–20). In 2009, after tortuous bureaucratic infighting between competing governmental departments and military agencies, **the Pentagon created a Cyber Command to conduct operations** in a “cyberdomain” now deemed as important as land, sea, air, and space. This is a logic being duplicated within national security states around the world. **The observation that cyberwar has now become extremely handy for acquiring big funds for research and militarization** (Rid 2013) is true, but, with a self-validating circularity, the cyberwar apparatuses built on this promotional discourse not only speak but also prepare and act. **Public knowledge of** these **cyberwar acts is**, however, limited and **distorted**; if **the new cyberwar complexes are** in one way new “**assemblages of knowledge and power**,” **they are also assemblages of power, nonknowledge and antiknowledge**, **military factories of ignorance** and obfuscation. War always involves secrets, but **cyberwars are** exceptionally **deeply cloaked**. As Michael Kenney (2015, 117) observes, “**cyber-warfare is** typically **a covert form of statecraft**. Herein lies much of [its] utility as a weapon: states can attack their adversaries without declaring war against them.” **If there is one cyberwar cliché more common than “you may not be interested in cyberwar,” it is a redo of Clausewitz’s “fog of war” as “fog of cyberwar”** (Valeriano and Maness 2012; Canabarro and Borne 2013; Rantapelkonen and Salminen 2013). **Digital war is a veritable fog machine**, because operations are usually conducted covertly and are often intended to confuse; hacks are hidden from view and, when discovered, are laden with misdirection; signals intelligence implodes into infoglut. Apparently incriminating traces of hacking tools left at the site of a digital breach may be intentional false flags and what looks like a singular exploit actually a chain of attacks by different actors “piling on” to a discovered system vulnerability. Is a hacking exploit that leaves as a signature the name of the founder of the Soviet secret service a careless, or cavalier, disclosure of national responsibility—or a blatant red herring? As of today, it can be said that all, or nearly all, obvious indicators pointing to a potential responsible party, such as time, specifics of code, politics or other motifs, and cybertactics, can be manufactured to point in a wrong direction. In investigating cyberwar, conspiracy theory is methodologically mandatory. However, not only attribution of attacks but also **the distinction between attacks and accidents becomes highly problematic**; **“fog of war” (ignorance) and “friction of war” (mishap) intermingle**. **Cyberwar thus tends to “obliterating proof** ” (Filiol 2011, 260), sometimes **by producing too many proofs,** “incessant **fluctuations” of proofs**, to use Claude Shannon’s phrase for noise, or, in the words of W. Ross Ashby ([1963] 1966), “**variety [that] can destroy variety**.”

Cybersecurity experts argue that, given sufficient time, it is indeed possible to make a reasonable determination of responsibility for cyberattacks. This process can involve analyzing technical details, such as the design of malware payload or “IP addresses, email addresses, domain names, and small pieces of text” used in the attack; comparing the modus operandi of hackers with the known profiles gathered from other cases; and assessing the likely reasons for an intrusion—but even then, verification is a matter of degree of certainty rather than a binary yes or no answer (Rid and Buchanan 2016). In this book, we often necessarily rely on such “balance of probability” interpretations, but with an awareness that **cyberwar is a weaponization of information that always threatens to destroy truth**. It is, as Justin Joque (2018, “Foreword”) writes, **a force of “machinic deconstruction” that constantly threatens “to sweep away any belief in security.**” We write also knowing that, in “a world where it is not clear who is hacking whom” (Ridgeway 2017), the attribution of cyberwar activity can itself become a tactic setting up an adversary for sanctions and retaliation. Academic interpretation, too, can be weaponized; those who stare into the abyss of cyberwar soon find it staring back at them.

### Framework—Gaming Bad

#### Abstracting the managerialism of the game is important to high school debate – the autonomy, portable skills, and perspective of debaters are at risk – reject their technocratic managerialism hidden under technology terminology and game-like features

Christo Sims, 20. Associate Professor in the Department of Communication and an Affiliated Faculty member in Science Studies and Ethnic Studies at the University of California, San Diego. His most recent book, *Disruptive fixation: school reform and the pitfalls of techno-idealism* (Princeton University Press, 2017), is the winner of the 2018 Best Book Award from the Communication, Information Technology, and Media Sociology section of the American Sociological Association. “Pedagogic Fixation.” *The digital age and its discontents: Critical reflections in education*, Chapter 10, 196-199. //GJ

Repairing Idealism

Part of the answer to the question I just posed has to do with the occluding effects of fixations. As I have been arguing, reformers tend to fix their imagination and attention on aspects of the world they can foreseeably transform in morally sanctified ways with their seemingly innovative remedies; correspondingly, they tend to overlook and take for granted whatever they cannot so easily control and transform with these newly available means. As we have seen, the school’s designers did not have the power to change many of the factors that structured canonical pedagogic practices. The state and the Department of Education, rather than the school’s designers, determined much of the curriculum, as well as funding for student–teacher ratios, the allocation of space and many other resource provisions. The built environments that they inhabited—consisting of multiple similar classrooms, each of which had been designed for a single educator teaching several dozen students—were inherited and built with canonical models of schooling in mind. Additionally, the school had to be able to interoperate with other schools in the broader New York City schooling system, as well as with colleges and universities. Part of its mandate involved receiving and delivering students in age-graded cohorts and producing standardized outcome metrics that made students and educators legible, hence differentiable, in processes of social selection and managerial oversight that extended beyond the space of the school. Reformers and educators had to comport themselves to these more entrenched strictures, and they deliberated how to do so, but reformers, in particular, did not tend to see such practices as central to what their project was all about.

How so?

For one, despite their professed student-centred ethos, more widespread and deeply sedimented ideological edifices about age relations and developmental temporalities helped reformers and educators downplay aspects of their pedagogic practices that were particularly at odds with their ideals. As sociologists of childhood and youth have documented, modernist practices of disciplining and controlling children and young people are legitimized, and hence often taken for granted, in part because of a more general tendency among adults to infantilize children and young people, a tendency that emerged alongside broader historical changes in the social and cultural organization of age relations (Zelizer 1985; Qvortrup 1994; James, Jenks & Prout 1998; Corsaro 2005). Figuring children as particularly underdeveloped and vulnerable is especially common in figured worlds that take the care and development of children and young people as their raison d’être. There were too many of these infantilizing practices to enumerate, but the reformer’s previous comment that the students couldn’t handle recess in the gym is one such example. Additionally, some educators routinely addressed the students with labels that positioned them as immature and inexperienced because of their age—terms such as boys and girls—and one educator even reminded the students that they were being addressed with these terms because they had not yet proven themselves worthy of a more mature and autonomous status. More commonly, educators routinely subjected students to didactic lessons on topics that students were presumed not to know, but were, in fact, quite knowledgeable about. One such episode was a school-wide assembly in which educators made students perform small skits in which they acted out norms for polite social etiquette, such as how to hold the door open for someone and how to acknowledge the act with the phrase ‘thank you’. Students already knew about these normative conventions, even if they sometimes did not enact them, in part, I believe, to demonstrate their autonomy from adult-imposed strictures. As we will see in the next chapter, these sorts of infantilizing practices produce conditions for oppositional behaviour, especially for subordinates who can gain status among their peers by demonstrating resistance to supervisory power.5

Additionally, experienced reformers and educators routinely made a distinction between practices of control and practices of care, the former of which they classified as classroom management and the latter of which they classified as pedagogical or learning activities. In practice, classroom management and pedagogic practices were one and the same, with purportedly caring pedagogic practices taking forms that helped sustain authorities’ control in crowded conditions. Yet, experienced reformers and educators tended to classify management practices as a separate but necessary precondition for administering pedagogic practices, and the latter was widely seen as beneficial for all students and hence as morally caring. For experienced reformers and educators, classroom-management practices seemed to be understood as a necessary, sometimes ugly, but also fairly mundane aspect of being a professional educator. And, if anything, experienced reformers and educators seemed to see those of us who were newer to their figured worlds—such as reformers who came from the worlds of technology design, as well as myself—as a bit naïve. As I spent more and more time in the school, I often got the sense that learning how to discipline and control students was treated by experienced educators as a sort of sub rosa aspect of being an experienced member of their figured world. Indeed, new reformers and educators became more experienced old-timers in part by learning to make the distinction between classroom management and pedagogic practices, as well as by learning how to be comfortable exercising power over young people. Perhaps recalling their own experiences as novice teachers and knowing that I was new to middle school as an adult, several of the experienced educators would make comments to me such as, ‘Teaching is crazy, right?’ after I witnessed an educator deploy a variety of rather domineering disciplinary techniques in an attempt to corral and pacify students. When I agreed, I felt as if I was beginning to be let into their club, in part by treating the exercise of power over young people as a normal, and even skillful, aspect of being an experienced educator.

While less-experienced reformers seemed to share my sense that many of these disciplinary practices were odd, if not unsettling, the division of labour in the philanthropic intervention also made it easier for these reformers to downplay and overlook the extent to which their project involved exercising coercive and disciplinary techniques on those it was designed to help. At the Downtown School, there was a fairly sharp and spatialized division of labour between the people who designed and supported the intervention and those who implemented it. By and large, the school’s design team spent little time managing everyday life at the school, even though they held considerable power over those who did. The founders of the school spent increasingly little time in the school as the project aged, and the practitioners who did spend their days in the school were split between, on the one hand, a group of game designers and curriculum designers who were largely responsible for crafting the school’s innovative pedagogy and, on the other hand, teachers and administrators who enacted the designers’ pedagogic scripts, managed students and were charged with keeping the school running. It was the school’s philanthropic backers, its game and curriculum designers, and its founders who remained the most enthusiastic about the school and its innovative philanthropic potential, and yet they also had comparatively little responsibility for, as well as less exposure to, its quotidian functioning. Additionally, those of us who were newer to educational reform were able to treat canonical practices of discipline and control as respectfully belonging to the world of professional educators. For example, one of the school’s founders, a media technology designer, noted to me that they also found educators’ classroom-management practices curious, but then quickly distanced themselves from the remarkability of such practices by suggesting that they were an oddity of what professional educators do.

Finally, and as noted earlier, the school’s isomorphic drift was partially obscured and discounted because many of these familiar features had been recoded with terminology borrowed from technology design, especially game design. This terminology downplayed the ways in which educators not only remade canonical practices, but also controlled others through those practices. All these dynamics help explain how reformers and educators were able to reconcile tensions and contradictions between the project’s ideals and its acts. All have the effect of occluding, normalizing, translating and generally downplaying the ways in which the school’s pedagogic activities were shot through with the very techniques that reformers aimed to disrupt. Yet, practices that occlude, distort and overlook do not adequately account for how reformers and educators also manage to maintain and repair their sense that a philanthropic intervention is both cutting-edge and morally sanctified. Oversights can help such fixations persist, but they do not provide experiences that renew a collective sense of moral optimism. The maintenance and revitalization of such feelings depend on the collective accomplishment, and ritualized valorization, of what I call sanctioned counter-practices.

#### The Game fails – constrains autonomy and it’s motivated by institutions with their own incentives – autocorrect for the guise of debate’s purpose under the game

Christo Sims, 20. Associate Professor in the Department of Communication and an Affiliated Faculty member in Science Studies and Ethnic Studies at the University of California, San Diego. His most recent book, *Disruptive fixation: school reform and the pitfalls of techno-idealism* (Princeton University Press, 2017), is the winner of the 2018 Best Book Award from the Communication, Information Technology, and Media Sociology section of the American Sociological Association. “Pedagogic Fixation.” *The digital age and its discontents: Critical reflections in education*, Chapter 10, 187-189. //GJ

Designing Beneficial Experiences

As discussed previously, the Downtown School’s most distinctive innovation was to try to redesign the pedagogic activities of schooling as if they were an engaging and beneficent game. Like the reformers’ spatial fixations, this pedagogic fixation partially arose through processes that problematized not only conventional schooling, but also modernist state institutions more generally. Like many other social reformers who have been inspired by the seemingly dynamic organizations and work cultures of Silicon Valley, the designers and backers of the Downtown School problematized reformers of the past for creating organizations that were hierarchical, rigidly scripted and, hence, controlling. These previous attempts at social and organizational engineering were seen as inhibiting, rather than enhancing, the capacities of the people who worked in bureaucratic organizations, as well as the people those organizations claimed to serve. By contrast, games appeared to offer an inspiring alternative model for how experts and managers could design and organize experiences for others. Game design, and experience design more generally, appeared to offer a way for experts and managers to craft activities that were organized and goal-driven, but also flexible, improvizational, creative and even fun. Most importantly, doing so would allow experts to redesign activities that benefited people in ways that more Tayloristic approaches to organizing activity did not. Games and experience design, proponents argued, would help unleash people’s inherent creative capacities and would thus amplify innovation, learning and personal satisfaction.

Of particular interest to the reformers who designed the Downtown School was the work of the sociolinguist James Paul Gee, who had written an influential book on the educational potential of video games (2003). Gee had also received large grants from one of the philanthropic foundations that was sponsoring the Downtown School, and he served as an advisor on the project. By turning pedagogic activities into a game, the school’s designers hoped to overcome conventional schooling’s emphasis on tightly scripted and obedient behavior, as well as its related reliance on surveillance and coercive disciplinary techniques, which, as we know from Foucault (1977), are not features unique to schools. According to Gee and the school’s founders, well-designed games would allow students to actively and creatively explore a ‘problem space’ that became incrementally more difficult as the players progressed and their skills developed. Moreover, these games would provide students with a context for their activity and, thus, with resources for constructing personal meanings and emotional investments in their school-based activities. By taking on the identity of the game’s characters, students would not only be motivated to participate in schooling, but they would also produce beneficial personal transformations, conceptualized as learning, as they did so.

The vignette at the opening of this chapter begins to illustrate how the Downtown School’s designers tried to implement this hopeful vision of pedagogic activity. Near the beginning of a trimester, the teacher in each course would introduce a ‘mission’ for that course. These episodes, which typically lasted for 20 to 30 minutes, were meant to introduce students to the designed game world that would frame the students’ schoolwork in that course for the trimester. The designed game worlds would consist of characters that did not belong to the school and who needed the students’ help. For example, the sock puppets described in the vignette at the opening of this chapter needed the students’ help so that their houses would stop falling down. In another class, a set of fictional characters needed the students’ help decoding messages in order to solve a mystery about a missing character. In still another class, professional editors at the transnational media conglomerate Pearson supposedly needed students’ help designing educational comics and so on. Guided by teachers, students would interact with these non-school characters through Skype phone calls, video chats, recorded videos, blogs, e-mails, physical letters and other telecommunications. In practice, these episodes were a noticeable break from conventional classroom activities and, as evinced in the opening vignette, many students did appear to be alert and engaged when they occurred, much as the reformers had hoped.

But when considered in terms of the school’s everyday routines, a very different picture of the school’s pedagogic practices begins to emerge. Most noticeably, these unconventional and less-scripted moments were rather fleeting and negligible compared to the abundance of conventional, highly scripted schooling activities. After brief episodes in which students communicated with characters from the designed game worlds, daily life would quickly return to familiar school routines in which managers, here teachers, issued subordinates a near constant succession of fine-grained commands. In the vignette just described, the sock puppets assigned the students paper worksheets that could be completed as homework if they did not finish them in class. In the school’s math class, which had been framed as a code-breaking academy, one of the students’ first challenges was to take a paper and pencil test on fractions. In class after class, a common pattern emerged: after an unconventional and improvizational exchange with characters from the designed game worlds, educators returned to conventional schooling practices with familiar power relations and adult-scripted activities, but these schooling practices had been relabeled as if they were part of the game.

Consider, for example, how the school’s designers attempted to transform the familiar disciplinary practices of hierarchical observation, normalizing judgments and examinations (Foucault 1977). According to the school’s designers, their goal was to help all students become masters in the school’s various knowledge domains. Much like a video game, students would get feedback rather than grades, and progress would be measured in terms of moving through various stages and levels in the game. Moreover, this feedback would supposedly come from within the designed game worlds. Instead of teachers assessing students, characters in the designed game worlds would supposedly evaluate students’ work. The above-mentioned paper-and-pencil test for the code-breaking academy is an example of this sort of symbolic transformation of a familiar disciplinary technique. The teacher presented the test as if it were an entrance exam to the code-breaking academy, but it was also a formative assessment for the school’s educators. Moreover, the feedback students received on their various assignments did not use letter grades or points out of 100, as is done in conventional schools, but it was still organized on a linear scale with five ranked categories—master, senior, apprentice, novice and pre-novice—each of which also had the equivalent of pluses and minuses—Level 1, Level 2 and Level 3. The labels had changed, but the underlying practices had not. The school’s designers envisioned a similar transformation in how they organized the curriculum. All students were required to take the same five courses, and they had little say over what they were expected to learn in each course. While the reformers referred to these courses as domains and assigned imaginative new labels to each one, the content of these courses was defined mostly by state standards and to a lesser degree the school’s designers and educators. One course covered New York State’s standards for sixth-grade science education, another class focused on the state standards for math education, another combined social studies and English and language arts, and another course blended physical fitness with what educators referred to as ‘socioemotional learning’. The school’s most unconventional course focused entirely on media production, which in the school’s first year consisted of game design. The reformers also tried to incorporate what they referred to as ‘21st-century literacies’ within these domains, which in the school’s first year consisted of teamwork, systems thinking and time management. Each domain was supposed to focus on these literacies, as well as the state-mandated content. In any case, students had no voice in shaping the curriculum, despite reformers’ claims to be student-centred.

#### The Game is a control technique – the notion of educational narrative, time, and script contradict the pedagogic fixation of academia.

Christo Sims, 20. Associate Professor in the Department of Communication and an Affiliated Faculty member in Science Studies and Ethnic Studies at the University of California, San Diego. His most recent book, *Disruptive fixation: school reform and the pitfalls of techno-idealism* (Princeton University Press, 2017), is the winner of the 2018 Best Book Award from the Communication, Information Technology, and Media Sociology section of the American Sociological Association. “Pedagogic Fixation.” *The digital age and its discontents: Critical reflections in education*, Chapter 10, 191-196. //GJ

Overflowing and Retrofitting

Not long after the school opened, it became evident that the school’s game-like pedagogy did not have the motivational powers that the school’s designers had hoped. Almost immediately after the school opened, many school leaders, teachers and parents worried that students were out of control. Some students talked back, made fun of the designed game characters, ignored or played with directives from teachers and generally asserted themselves in ways that made it difficult for teachers to stick to the scripted activities that they, game designers and curriculum designers had jointly crafted. Students were exercising their creativity and agency, but not in the ways in which the school’s designers had anticipated or desired. Instead, students were transforming the reformers’ carefully designed activities towards their own interests and sensibilities. Here, for example, is a snippet from my field notes not long after the school opened:

We’re lined up in the hallway waiting for Sarah [the teacher] to take us to the gym. Before heading up the stairs Sarah reminds us of the procedures we’re supposed to follow after we arrive: place our bags and jackets against the wall, run three laps around the perimeter of the gym, then get in a big circle and quietly wait for her instructions.

Sarah goes on to tell us about the main activity for the day. She tells us we’re going to split into two lines and play a game with basketballs. Troy shouts out, ‘Knockout!’ Several other students follow his lead and also shout out ‘Knockout.’ Sarah ignores them and starts explaining what we’re going to do: a student at the front of one line will shoot the basketball, then the person from the front of the other line will rebound the ball and give it to the next person in the shooting line. Each student will then go to the end of the opposite line and the process will repeat.

‘That’s not Knockout,’ Troy says.

Sarah says that this is what we’ll be ‘playing’ today. Troy counters that Knockout is more fun.

Sarah responds by telling Troy, ‘When you grow up and become a teacher then you can have everyone play Knockout.’ Sarah also reminds the students that gym was part of their grade.

Rake blurts out, ‘Who knew so much fun stuff would be part of our grade?’

Sarah tells him to, ‘Knock off the attitude.’

A similar dynamic played out in every class: when students tried to question or bend reformers’ and educators’ scripted activities, educators corrected them and tried to compel their participation in the school’s version of fun. Many educators equated student resistance with personal disrespect or with spoiling the fun of the group. For example, when one of the students called out, ‘This is so fake!’ as the teacher showed students a blog message that had supposedly been written by a master game designer, the teacher snapped back, ‘Stop ruining it for everyone!’ Similar tensions played out in all classes, especially at the beginning of the year.

Reformers’ and educators’ concerns about control also extended beyond the pedagogic activities of classrooms. As just mentioned, the school’s designers had allocated 45 minutes for lunch and recess, which they roughly split into two equal time blocks. At the beginning of the year students could more or less do what they liked during recess so long as they hung out in a designated classroom or the gym, both of which were monitored by adults. The students who hung out in the gym produced a heterogeneous assortment of activities that often bled into one another. Students moved around noisily and fluidly, many improvizational games emerged, and participants moved in and out of various activities, changing their own course and the course of the activities in the process. Some students shot basketballs, some played with jump ropes, others did cartwheels, some roamed the perimeter of the gym and others hung out with friends in small groups. Many students moved between activities and social groups and there was no clear overarching plan or structure, perhaps suggesting opportunities for breaking down preconceptions about class, gender and race.

However, some of the school’s designers and educators worried that this arrangement was too chaotic, noisy and out of control. As one of the school’s designers mentioned to me as we watched the students play during recess, ‘[I don’t know if they [the students] can handle this. I could hear them from the street when I went to get lunch.’ These moments of concern evince the dilemmas that contemporary institutional reformers face as they try to reconcile, on the one hand, their aspiration to design activities that promote creativity, agency and transformations towards self-realization among an intervention’s intended beneficiaries and, on the other hand, the more instrumental mandate to control, measure and develop those persons into particular idealized subjects.

While these dilemmas could theoretically be moments in which reformers questioned their assumptions, and particularly the enduring yearning to create apolitical and philanthropic mechanisms for learning, the dominant tendency was to engage in a different sort of fixation: the school’s designers and educators quickly searched for resources that would stabilize the project against the unanticipated turbulence of students’ unsanctioned behaviour. In response to students’ resistance to the adult-scripted activities—all of which evinced the student-centred agency that reformers championed—the school’s designers, leadership and educators quickly attempted to establish the authority of school adults in order to regain control of students and hence their project. Ironically, they mostly did so by retrofitting the project with the very techniques of discipline and control that were common at the conventional schools against which they had defined their project and themselves.

In several classrooms, desks were rearranged from inward-facing clusters of five desks—an arrangement which put some students’ backs towards the teacher, but also allowed for easier peer communications during student-driven project work—into sequential rows that all faced the teacher at the front of the room. Further, educators intensified their efforts to orchestrate a seamless flow of adult-scripted activities, even during moments when students had previously enjoyed some autonomy, such as recess and the brief passing period between classes. Within a week after one of the school’s designers expressed concern that students might not be able to handle recess in the gym, educators introduced adult-scripted activities for recess in the gym. Half the gym was organized into a football game administered by one of the educators. In the other half of the gym, students were allowed to organize their own smaller games, so long as they remained relatively quiet and spatially contained. Most students who did not play football stopped going to the gym after these changes, and some social divisions among students, notably gender divisions, became more spatially calcified during recess. During passing periods, which educators saw as moments when they could lose control, teachers introduced a script in which they organized students into quiet, forward-facing, single-file lines before they left a classroom. After such a line was formed—which could take some time—teachers marched students down the hallway to their next class, where they then waited quietly against a wall until the next teacher allowed them to enter. All teachers introduced this script at the same time, about a month into the school year. Further, in the middle of the fall, all the educators established a pedagogic script where they directed students to begin a silent, individual, teacher-defined task for five minutes immediately upon entering a new classroom.

In addition to extending practices of surveillance and control to spaces and periods where students had previously experienced some autonomy, educators also intensified their grip in domains where they had already been exerting their authority, albeit in the obscured ways discussed in the past section. In classrooms, educators not only continued to define and enforce scripted activities for students, but in a Tayloristic fashion instructors started breaking down these scripts into ever-smaller step-by-step procedures. In many classes, educators accompanied these fine-grained scripts with techniques intended to facilitate a heightened awareness of ‘clock time’ (Thompson 1967) among students. While modernist institutions have long emphasized clock time, this orchestration became more fine-grained and explicit than I expected. The reformers referred to their focus on clock time as 21st-century literacy called time management, but time management typically had a lot to do with classroom management, in which students ironically had little say over how they managed their time. Many educators saw clocks and timers as a useful way to keep students on task during scripted activities, as well as when they transitioned between these activities. What educators facilitated was a near-constant awareness among students of how much clock time they had left or had spent on a given task. When directing students to do a scripted activity, educators would almost always tell the students how much time they had for the activity. Many would use their laptops to project a digital countdown timer for the activity onto the whiteboard at the front of the class, which functioned as a continuous animation of clock time slipping away. Many educators also wore stopwatches around their necks and routinely referred to their stopwatches as they called out how much time was left before the scripted activity ended. Educators expected students to be in their assigned seats and listening for the next directive when a timer ended.

Not only were these references to clock time much more pervasive and evident than I had anticipated, but they somewhat surprisingly had the ‘gamifying’ effect of adding a sense of urgency and competition to what were otherwise rather trivial and boring tasks. The approaching termination of the timer could turn an otherwise boring and scripted activity into a race against the clock, and as timers approached zero you could sense a palpable rise in the energy of the students, an emotional rush that I also felt when I participated in these rote routines. Several teachers even punctuated the end of a countdown timer with the visualization and sound of a large explosion, further adding to a sense of excitement, even though the tasks that we were completing were often quite rote and meaningless. This rush against the clock was sometimes reinforced by a manufactured sense of competition among students and classes. For example, at one point during the year, an educator made a game out of how quickly students could line up quietly before entering his classroom. He taped a large piece of butcher paper on the wall outside his classroom and wrote how many seconds it took for each class to line up quietly before being admitted into the room. This went on for several weeks as classes competed against each other to see which class could be the most disciplined, until the winning class had achieved a time of less than four seconds.

Of course, these processes for creating order and discipline were in glaring contradiction to the reformers’ pedagogic fixations—which purported to cultivate student agency, creativity, improvizational problem-solving capacities and so forth—and yet, seemingly paradoxically, the designers of the school were often complicit in the introduction of these highly scripted practices. What is more, many of these techniques were either replicates, if not enhancements, of the techniques used in the more traditional schools against which the reformers had contradistinguished themselves. In keeping with DiMaggio and Powell’s (1983) notion of ‘mimetic isomorphism’, many of these canonical management techniques were introduced either by reformers and educators who had worked at other schools or by representatives from the Downtown School’s School Support Organization (SSO), the latter of which was meant to replace school boards within New York City’s autonomy for accountability exchange. And the techniques were introduced in a coordinated and standardized fashion across the entire school, often right after the school’s weekly professional development session. Here, for example, is a portion of an e-mail that one of the school’s leaders sent to the school’s faculty and staff; in it, the leader explicitly calls on educators to tighten their scripting of students’ behaviour:

During [our professional development period] we discussed the importance of the directions we give students. Are directions given both orally and in writing or are they only being delivered orally? Are they broken down into small steps or are there many steps embedded in narrative? Every lesson at The Downtown School thoughtfully considers what students are being asked to do. Please remember to review how you are asking them to do it.

This purposeful import and deployment of canonical disciplinary practices raises the curious question of how reformers managed to reconcile their practices with their ideals. In the words of Bennett Berger (2004), who studied similarly wide gaps between ideals and acts in his study of a group of countercultural communards in northern California, such reconciliation requires a lot of ideological work.

### Framework—Political Economy Key

#### Political economy is the necessary starting point for altering our relationships with technology.

**Hall 21** – Professor of Education and Technology, Research Associate in the Centre for Computing and Social Responsibility at De Montfort University. “Venturing Beyond the Imposition of a Postdigital, Anti-human Higher Education.” Springer link. Apr 2021. https://link.springer.com/chapter/10.1007/978-3-030-65592-1\_4, AG

4 In, Against, and Beyond the Digital

There is a material history of the relationship between technology, institutions, cultures, and practices. In analysing this material history, the idea of the postdigital has been framed in terms of: interaction, complexity, and social change; digital subservience to the idea of the social; digital transparency enabling issues-based dialogue; the stagnation of positivist, digital discourses; the digital reproduction of relationships of power; the decoding of relationships of power through digital transparency; and a focus upon the platform rather than the tool (Cormier et al. 2019; Jandrić et al. 2018).

At issue has been how to reimagine the idea of the human inside systems predicated upon: complexity-for-innovation; a social terrain defned around productive value; obfuscation of the ways in which algorithmic control is coded; the control of certain forms of public data and their presentation; ongoing techno-determinist readings of progress; and the subservience of life under platforms that mediate and quantify existences. This reimagining matters because, systemically and productively, the only space for radical imagination appears to be in the further, ongoing digital colonisation of the body and the self, as a means of reproducing value (Berardi 2009; Lazzarato 2014). This process is limited precisely because the spacetime of life is bounded by competition between digitally enabled humans.

In this bounded space-time, individuals, groups, or States attempt to break or harness specifc technologies for particular political ends (Watters 2021). Such contestation is amplifed at the boundary between the human and the development of convergence technologies, based on the integration of 5G cellular networks, tokenomics and forms of blockchain, machine augmentation, sentiment analysis, biotechnologies, and so on. Interactions at these boundaries then enforce human–machine intersections with digital, monopoly capitalism in the form of Google, Microsoft, Amazon, Facebook, and Apple, and the rise of alternate geopolitical rivals, in particular from China. As a result, the postdigital realities of HE, and teaching, learning, and researching inside its institutions, are framed by the techno-colonisation of what it means to be human from a variety of intersecting structures and processes (Peters 2020).

Thus, the idea of the postdigital needs to be discussed in relation to its potential to act as a dystopian pivot for the convergence of the personal/the person and a range of technologies (cognitive, biological, nano-). The terrain of aspiration is shaped through the exploitation of the fesh and of the mind, the augmentation enabled by technology, and the ongoing expropriation of what it means to be human. These moments of exploitation, expropriation, and extraction are rooted in wider, intersectional injustices, grounded in the separation of politics and economics, denying the potential for a reintegrated political economy that radically reimagines society (Hall 2018). As a result, social reproduction cannot be viewed beyond the lens of capital, and technology cannot be viewed beyond the ways in which it expands the feld of accumulation.

Part of the issue is the apparent monopolisation of digitally enhanced expertise, in relation to crises and their mitigation, by institutions of higher learning. Either private investment in institutions or state-sponsored privatisation for the creation of infrastructures like universities in which private investment can take hold disables populations from imagining futures that do not emerge from experts, technocrats, or technologists. Moreover, beyond business-as-usual, the postdigital institution has no political content. Thus, in the separation of HE institutions from their publics, except through exploitative labour and study conditions, contracts, licences, rents, or modes of knowledge transfer, there is a weakening of political imagination. Disciplinary separations, competition between subjects and institutions, technologies for monitoring and audit, each reinforce a value-driven, human-digital reality.

At issue is whether it is possible to work against this reality and the multiple differential and unjust ways in which it is experienced. This requires a new political economy, which seeks to reduce the space and time required for the production of self-suffciency and widen the base for autonomous existence. Might the very automation, or human–machine augmentation and symbiosis, demanded and developed by capital to discipline and control labour make possible an exodus from the society of capitalist work? As surplus time arises as an outcome of automation, new, radical possibilities for disposing of that time beyond the universe of value might be discussed. This requires a re-connection with the ideas of being human, knowing the plurality of humanity, and acting or doing in humane ways. This includes a reimagination of the relationship between humans and the digital in the name of dignity, in order to recover autonomy for the self beyond being a factory for value. That factory and the inhumanity that it breeds must be decomposed as a starting point.

### Framework—Optimization DA

#### Optimization DA: Framework functions as an attempt to optimize our processing power in the digital age, which quantifies the self.

Theo Hug 21. Professor at the University of Innsbruck, Department of Media, Society and Communication. “Five Theses on (Dis)Comfort in the Educational Cultures of Digitality.” 2021. <https://www.ceeol.com/search/article-detail?id=1028699> //GJ

Thesis 2: Operative fictions of optimizing processes of learning and education correspond with poorly reflected assumptions of mathematization and of the computability of the world

Notions of optimizing processes and methods to quantify the self and others are not inventions of the digital age. From choosing a lubricant for the first rotating fixed wheels to choosing efficient neural networks in machine-learning programs, narratives and leitmotifs of optimization have been diversified and developed. An end to these traditions is not in sight, on the contrary: Computer network technologies have made available processing capacities without which developments in structural sciences and their manifold technological applications would not have been possible.

The frictions between encultured medial constellations of the twentieth century and the emerging new socio-technical configurations of the twenty-first century also affect the key topics of education, especially growing up, learning and teaching. The “optimizing spirit” (Leineweber & Wunder, 2021) that pervades the rhetoric of digitalization makes some people hope for a chance to overcome the “technological deficiency” (Luhmann & Schorr, 1982) and others worry in view of certain fuzzy ideas of applying rational measurement models to the data-driven management of learning and development processes. No matter if a narrow or broad concept of technology is taken as a starting point, or if referring to a technological deficiency is generally deemed to be out-of-place or misleading with respect to the postulates of human dignity and the development of autonomy: The increasingly refined and partly automated measuring methods open up widened scopes of calculating, monitoring, manipulating and controlling, up to re-educating entire population groups.

These enhanced and sometimes de-limited scopes at the interfaces of quantitative-empirical education research, education policy and education economy may prove of value in some regards as “operative fictions” (Schmidt, 2006, p. 4). On the other hand, in the course of becoming reality, the fantasies of optimization occasionally mutate into paradoxes of optimization (Wolf & Thiersch, 2021) – not least when the polymorphism of pedagogical “logics” is consistently interpreted and assessed in the light of machine-, market- or media logics and the self-similarity of the process dynamics does not come into view anymore. The tendencies towards rationalism of disposition are not linked to a particular rationality or version of rationalism. They concern all forms of rationalism, which characteristically tend to absolutize the determination of starting positions, assessment modalities, means, purpose, or procedures and authorities for the deliberate production of behaviors or specific circumstances (cf. Hug et al., 2007). To what an extent the algorithmic rationality opens up new scopes in this context cannot be answered at this point. The discussion of “generative realities” (Löffler, 2019) as calculated, predictable and controlled realities has only just begun.

Such tendencies can be found in the algorithm-based timing of learning technology and the AI-based production of specific qualification effects. They do not only run counter to the obstinacy of open-ended educational processes. They also contradict education-related uncertainty principles. Furthermore, they correspond with ideas that processes of learning and communication are predictable on the basis of calculations and formally schematized competency elements, without consistently considering the human capacities to differentiate between sense and nonsense, to spontaneously depart from rules in the action process, and to creatively connect Phantasie und Kalkül (Schneider, 1992). And what is more, a discomfort with the optimization discourses stems from these discourses’ lack of reflection when it comes to the limits of mathematical languages (Frey, 1967), algorithmic rationality (Mersch, 2019), and the computability of the world (Pietsch et al., 2017).

## Blocks

### AT: Academy Fails

#### The academy can be reimagined towards a reengagement of human relation with cybernetic realities.

**Hall 21** – Professor of Education and Technology, Research Associate in the Centre for Computing and Social Responsibility at De Montfort University. “Venturing Beyond the Imposition of a Postdigital, Anti-human Higher Education.” Springer link. Apr 2021. https://link.springer.com/chapter/10.1007/978-3-030-65592-1\_4, AG

Composting the Anti-human University

Marx (1867/1976: 547) argued that machinery is ‘a more hideous form [for] exploiting labour-power’, reducing the worker into ‘a part of the specialised machine’, and both reducing wages and breeding ‘helpless dependence upon the factory as a whole’. The concrete realities of the HE terrain described as postdigital are of struggle against the discipline of commodity production and exchange and for humane cultures and practices. Some of these struggles are noted above, as students, teachers, and their communities push the boundaries of education for another world. However, being against a system places bodies and identities at-risk of being disciplined.

Curle (1973: 8–9) emphasised the need for a new education, which demands ‘an alien form of society’ that values the human, or our shared humanity. This is the possibility of personal evolution, or ‘higher-awareness (awareness-identity)’, formed inside a counter-system of education rooted in altruism (or #solidarity). This counter-system has echoes of Gramsci’s work on hegemony and counter-hegemony, rooted in acknowledging, analysing, and abolishing power, in both formal and informal settings. For Curle (1973: 10), such a counter-system would have higher levels of (social) awareness (beyond value). It would be grounded in awarenessidentity (social connections against-and-beyond the market), and as such be altruistic and empathetic with peaceful relations that are based on cooperative and egalitarian democracy.

In addressing how education relates to the creation of such a counter-system, Curle (1973: 17) diagnosed that we need to reveal the reality of the system as is, in order to demonstrate how hegemony rests on making particular lives intolerable or invisible. As a result, it becomes possible to prefgure other ways of knowing how to live, as a process that is generative, iterative, and educative (Amsler 2015). In revealing how life inside the postdigital University or college is reproduced forvalue, and the lived experiences of those made marginal inside this system, it becomes possible to discuss the values upon which living might be organised.

This reimagines the University as a pedagogical project that begins from humans and their society as it is embedded and reproduced in nature. It is a ‘sacred’ project, grounded in ‘the practice of freedom’ (hooks 1994: 13). Such practice is learning and teaching not as algorithmically or cybernetically managed and fnessed, rather as a process, integrated with the souls of students and teachers, and in symbiosis with ‘the necessary conditions where learning can most deeply and intimately begin’.

This idea of symbiosis and necessary conditions is critical in thinking about venturing beyond the universe of value, which reproduces itself through dialectical pro cesses that are technologically enriched. As has been noted, Marx (1867/1976: 473) described the dialectical relationship between technologies and forms of production, relations to nature, particular social relations, mental conceptions of the world, labour processes, arrangements for governance and regulation, and the conduct of daily life. At issue is whether and how to take these relationships as they form the necessary conditions for capitalist reproduction, and to move beyond their hegemonic description of the world.

Here, French et al. (2020) describe composting as a metaphor for re-engaging humans with the conditions inside which they reproduce their world. A starting point is a thick dialogue grounded in lived experiences of exploitation, expropriation, and extraction, in this case emerging from ‘stories of displacement, dispossession, dislocation, disclosure/enclosure, discomfort/comfort, and binaries’. In engaging with the realities of settler colonialism, these authors identify hegemonic structures, pathologies, and methodologies as ‘invasive, ongoing, and invisible’, and which scrub existing human relations of any meaning. They argue the need to compost anger, grief, and trauma, as a process of unearthing and breaking down distortions, and thereby creating ‘a garden of truth-telling’ (French et al. 2020). Composting serves ‘as a rich metaphor for our experiential approach to documenting our stories and building relationships with one another, with our ancestors and with land, because it is itself a relational process that repeats and is enriched with every churning of the soil’.

The process of composting centres humanity and feelings, stories, histories, relationships, cultures, and lands. Through a deep engagement with truth-telling, it seeks to begin from suffering and apparent hopelessness, in order to cultivate alternative ways of being, knowing, and acting in the world. Engaging with this struggle in educational contexts requires refection on the realities of the time required for truth-telling, alongside individual fallibilities and personal limitations, and potential for paralysis when faced by overwhelming, structural crises and forms of power (Tuck and McKenzie 2015).

Yet, in the desire to curate and cultivate ways of living more humanely, those who labour in postdigital HE might usefully seek to grapple with Tuck’s (2018) question: ‘how shall we live?’. In a technologically enriched, interconnected set of environments, inside which individual behaviours and actions are increasingly cybernetically tracked and controlled, and inside which legitimacy is judged in relation to systemic norms, this question is both imperative and revolutionary. This is more so because the idea of composting the world as it is speaks to a system that needs to decompose and lives that need to be fertilised in new ways, lest they wither or remain unfulflled. Against the morbid realities of HE, and of living and studying in the shadow of value, this is a starting point for reimagining the relationship between humans and their technologies, and how they are integrated in institutions, cultures and practices.

### AT: Liberalism Good—Fascism

#### We straight turn this. They empower fascism by tricking liberalism into believing it can sustain itself.

Franco ‘Bifo’ Berardi. 2021. Franco "Bifo" Berardi is an Italian communist philosopher, theorist and activist in the autonomist tradition, whose work mainly focuses on the role of the media and information technology within post-industrial capitalism. Berardi has written over two dozen published books, as well as a number of essays and speeches. “Manifest Destiny”. Ill Will. September 2nd, 2021. <https://illwill.com/manifest-destiny> //GJ [this card references self-harm]

One might be forgiven for thinking that America is dead.

The country does not have a president. Biden, if he ever existed, has been annihilated by the disaster of the retreat. This country does not have one people but two, and they are at war with each other. The allies are melting away and, last but not least, China is winning the diplomatic battle and also the economic competition.

All this is true, but you should not forget a non irrelevant detail: America is also a techno-military complex (Google and the Pentagon and so on) in possession of a destructive power capable of razing the planet and eliminating mankind not once but many times over, and it is acquiring the ability to evacuate a small minority of humans from planet Earth towards no one knows where.

The Afghan defeat marks the turning point in a process of disintegration of the West whose signals have accumulated over the past two decades.

Here I use the word West to mean a geopolitical entity that corresponds to the Judeo-Christian cultural world (and therefore includes Russia itself).

Perhaps capitalism is eternal, a hypothesis to be verified if we have the time, but I don't think we will. The West does not. And unfortunately, the techno-military complex that the West has at its disposal, and which continues to feed despite its ability to overkill, does not respond to the logic of politics, but is an automatism that responds to a logic of deterrence. Once upon a time deterrence was bipolar and symmetrical, but after the collapse of the USSR it has a multipolar, asymmetrical and therefore interminable dynamic. Furthermore, the techno-military complex is also an economic power that must produce war in order to reproduce itself.

This is why we should not be too pleased with the collapse of the West: the crumbling of the West will not be an (almost) peaceful process, as was the collapse of the Soviet Empire between 1989 and '91.

Before collapsing, the West could erase the world not because of political reasons, (the political brain is evidently affected by necrosis), but because of a chain of technical, military and psychological automatic reactions.

Think of Italy: despite being a second-tier military power, the country where I live has only 15 anti-fire aircrafts, while it has 716 fighter aircrafts. What do we do with this disproportionate arsenal? Why is Italy investing a huge amount in a fighter plane called Tempest, along with Germany and England, while the effects of Covid are destroying the welfare of many?

Can you tell me why?

Now, after yet another defeat that the West (NATO, the US, Europe) has suffered in a conventional war, it is naive to think that the West is giving up on war. The West, therefore, will soon be led into unconventional warfare.

Capitalism is no longer able to allow the reproduction of mankind; expansion has reached its peak. Capitalist valorization is now essentially achieved through the extraction of physical and nervous resources that are on the verge of exhaustion, and through the destruction of the planetary physical environment and the collective brain. At this point, I see two diverging perspectives: the dissolution of capitalism followed by the creation and spread of autonomous, egalitarian and frugal communities.

Or war. More likely: both perspectives at the same time.

What is certain, however, is the inability of the West to accept what is now its manifest destiny: decline, dissolution, disappearance.

Nazi-Liberal Suprematism

The collapse of the West is linked to processes that we can now pick out with the naked eye: the first is the growing infertility of the peoples of the north of the world (in 50 years the fertility of males of the Northern hemisphere has dropped by 52%). Whether it is due, as Sarah Swan argues in her recent book Count Down, to the spread of microplastics in the food chain, and to hormonal disorders caused by these microplastics, or whether it is due to the more or less conscious choice of women not to give birth to victims of rapidly spreading global fire, does not matter. The white dominators of the planet are senescent and tend to disappear.

The second process is the emergence of anti-Western capitalist powers (China) which for reasons inscribed in the psycho-cognitive formation have been more easily adaptable to the dynamics of the digital swarm with which Western individualism conflicts. (See in this regard Yuk Hui’s book Cosmotechnics, published by the MIT Press).

The third is the mental crisis, the self-contempt and the suicidal drive of the white population, unable to cope with the great migration, a consequence of colonization and wars, that is undermining the global order.

(Perhaps it would be worth rereading and updating some of Mao Tse Tung's and Lin Piao's considerations on the peripheries surrounding and strangling the center).

The European population, defending white privilege tooth and nail, is incapable of dealing with migration. Europeans refuse to recognize the need for a restitution of stolen resources, and fear a “great replacment” by non-white people. This is why neo-reactionary movements of nationalism and racism are on the rise in Europe.

According to Achille Mbembe,

Ultranationalism and racial supremacy ideologies are experiencing a global renaissance. The idea of ​​an essential human similarity has been replaced by the notion of difference, taken as anathema and prohibition ... Concepts such as the human, the human race, the human race or humanity mean almost nothing, even if contemporary pandemics and the consequences of the ongoing combustion of the planet continue to give them weight and significance. In the West, but also in other parts of the world, we are witnessing the rise of new forms of racism that we could define as paroxysmal. The nature of paroxysmal racism is that, in a metabolic way, it can infiltrate the functioning of power, technology, culture, language and even the air we breathe. The double turn of racism towards a techno-algorithmic and eco-atmospheric variety is making it an increasingly lethal weapon, a virus. This form of racism is called viral because it goes hand in hand with the exacerbation of fears, including and above all the fear of extinction, which seems to have become one of the driving forces behind white supremacy in the world.

Mbembe speaks of late-Eurocentrism. I prefer the expression ‘nazi-liberal suprematism,’ because colonial privilege is the junction point between social darwinism and the politics of extermination: natural selection.

### AT: Liberalism Good—Peace

#### Liberal peace is inseparable from the violent façade of liberal pacification which obscures the escalating cycle of phenomenological violence at the heart of the world order that kills value to life and ensures nuclear war

Baron, et al, 19—Associate Professor in the School of Government and International Affairs at Durham University (Ilan Zvi, with Jonathan Havercroft, Associate Professor in International Political Theory at the University of Southampton, Isaac Kamola, assistant professor of political science at Trinity College, Jonneke Koomen, Associate Professor of Politics, Sociology and Women’s and Gender Studies at Willamette University, Alex Prichard, senior lecturer in International Relations at the University of Exeter, and Justin Murphy, anticlimactically just an independent scholar, “Liberal Pacification and the Phenomenology of Violence,” International Studies Quarterly (2019) 63, 199–212, dml) [ableist language modifications denoted by brackets]

Phenomenology, as we are using it, is not about lived experience. It is the philosophical tradition of revealing different types of beings and things that contain meaning in our world, the structures and/or contexts in which they exist, and how these structures and contexts are meaningful. Understood in this way, violence is one of these structures and/or contexts. A phenomenological perspective does not approach violence from a particular normative position, although it does not preclude normative critique. A phenomenological approach does not treat violence as a discrete thing that one agent does to another, although it does not preclude such acts being described as violent. Instead, a phenomenological perspective adds to our intellectual and methodological toolbox by identifying violence as a condition or context in which people function. Phenomenology allows us to identify violence occurring in ways and in places that we otherwise would not be able to recognize. It does not change the meaning of violence (as harm, for example). Instead, it treats violence ontologically, enabling us to reveal more accurately the extent to which violence exists in the world.

From a phenomenological perspective, violence is often inconspicuous. Violence can function as a naturalized or internalized regime of compulsion or domination. Pacification reveals both the pervasiveness of violence and forms of violence that may otherwise remain inconspicuous. The erasing of tradition and the enforcement of particular legal codes at the expense of indigenous cultural norms is one example of an inconspicuous form of violence that involves conspicuous and inconspicous consequences (Cocks 2014). In understanding violence phenomenologically, as a structure of revealing across multiple worlds, we are better able to reveal the extent to which violence shapes our world and how we are then shaped by violence.

Pacavere

The Romans understood violence as a necessary condition for pax. The liberal imagination blinds itself to [obfuscates] the ways that pacification functions as violence in our world order. International relations scholarship’s strict distinction between peace and violence reinforces this obfuscation. Yet, the violence of (and in) pacification is central to the contemporary world. A phenomenological approach shows that moments of violent rupture are not aberrations of the world order. Violent outbreaks are breakdowns of pacification. It follows that multiple structures of the world order function as the violence of pacification, of pacavere.12 These structures include liberal capitalism, colonialism and the postcolonial aftermath, and war. Each functions as a key site of pacification. Anarchist thought reveals the pacification in liberal capitalism. Postcolonial thought reveals the pacification of colonial projects. Both anarchist and postcolonial thought demonstrate how war is a breakdown of pacification, revealing the hidden violent structures of our worldhood.

Anarchist critiques of capitalism, unlike Marxist and liberal interpretations, take seriously the decisive role of state violence in structuring society and markets. Anarchists view the state as an institution that sustains elite appropriations of political and economic power (Proudhon [1861] 1998; Sorel 1999; Prichard 2015). Those at the bottom of the social hierarchy bear the costs of this enforced order. The state diffuses violence (pacification) throughout the entire society—often in ways that go unrecognized by its subjects (Sorel 1999, 65). The naturalization of violence consolidates arbitrary regimes of domination in society. While specific, countable incidents of violence may decline, the social order is largely premised on the threat of violence for contravening social norms making specific, countable incidents of violence relatively rare (Kinna and Prichard, forthcoming).

Anarchist thinkers view rising inequality in the context of declining riots, insurgencies, and assassinations (see Figure 1) as evidence of pacification. Incidents of proletarian violence, anticolonial violence, riots, and protests are all examples of resistance to the “regimes of domination” that shape contemporary society, regimes easily identifiable by those subject to them (Gordon 2007, 33). Drawing on these accounts, we interpret declining rates of riots as a sign of increased pacification, rather than evidence that the system is becoming less violent. Conversely, eruptions of antistate and anticapitalist direct violence are signs of a breakdown in pacification. Much like Heidegger’s example of broken equipment (1962, 102–3, 412–13), which draws our attention to the background structures of our world, brief instances of direct violence reveal violently structured social relations.

Although the liberal imagination obscures the centrality of violence, violence has always been central to the liberal world order—to the liberal worldhood—particularly during the colonial and imperial projects of the nineteenth and twentieth centuries (Bell 2007a, 2007b). Colonial violence was diffused throughout the entire society, often in ways that went unrecognized by the colonized themselves. The violence of pacification structured the very existence of the colonized subject. This violence transformed the colonized subjects into a different “species” (Fanon 1963, 35– 40, 43). Colonial pacification was more than direct and indirect violence; it was sufficiently diffuse to remake the psyche of the colonized, affecting their mental health and emotions (Fanon 1963, 35–106). Fanon (1963, 31) described it as “atmospheric violence,” a “violence rippling under the skin.” Unable to lash out against the colonizer, the colonized lived everyday within a world ordered by violence. In this world, the colonized could not respond to the colonizers for fear of directly violent reprisals and would turn to symbolic activities such as a dance circle to expose the violence experienced on a daily basis (Fanon 1963, 57). For the colonized, rituals such as the dance were a means of expressing existential frustrations with and resistance to the violence of colonial pacification through reenactments of direct violence. Ultimately, anticolonial struggles exposed the violence of colonialism by directing that violence back on its authors.

Practices of colonial rule were central to developing liberal norms of sovereignty, as well as to the domination and control of recalcitrant populations whether within Europe, such as the English domination of the Welsh, Irish, and Scots, or outside of Europe by settler colonialists against indigenous populations (Deloria Jr 1974; Anghie 2005; Miller 2006; Havercroft 2008; Shaw 2008; Barkawi and Stanski 2012; Coulthard 2014; Simpson 2014; Lightfoot 2016; Rueda-Saiz 2017). This civilizing imagination functioned phenomenologically. It produced insiders as civilized and peaceful and outsiders as violent, external threats to civilization. In doing so, this imagination successfully obscured how the structures of liberalism produced colonial violence.13

FOOTNOTE 13 Arguments about the foundational role of colonialism, primitive accumulation, and white supremacy in structuring the modern international system are particularly useful in thinking about phenomenological violence (Jones 2006; Anievas, Manchanda, and Shilliam 2015; Du Bois 1915; Shaw 2008; Coulthard 2014; Deloria 1974; Lowe 2015; Hartman 1997). The legacy of these practices pervades contemporary liberal peace-building (Richmond 2014; Sabaratnam 2015; Bouka 2013; Autesserre 2009) and liberal global governance (Koomen 2014a, 2014b, 2013), while trade liberalization can facilitate mass violence (Kamola 2007; Smith 2016). Césaire argues that colonialism produced a “boomerang effect” within European societies; Nazism was the return of violence previously “applied only to non-European peoples” (Césaire 2000, 36). At independence, international law became a mechanism for reinforcing this international order upon the previously colonized world (Grovogui 1996).

The idea of war as an external practice of states, not tied to their internal workings and located according to specific normative projections of Western identity, followed from this colonial mentality. This mentality legitimized the exporting of violence to create a Western imperial pax and was so widespread that it shaped the development of modern warfare (Ellis 1986; Proudhon [1861] 1998). The colonial wars reproduced and reinforced ideologies of Western superiority, evidenced in part by the West’s superior military technology. A consequence of this racist hubris was the inability to foresee the destructive tendencies of Western warfare when unleashed against themselves (Ellis 1986).

The discipline of international relations, founded in response to the unexpectedly destructive character of the First World War, reproduced this understanding of war.14 This understanding disguises the possibility of increasing violence within the liberal world by presuming a historical narrative of progress and being shocked by its aberration. War, however, is not the absence of peace or an aberration of liberal progress, but is instead a phenomenological breaking of the liberal worldhood.15

Once a liberal order of democracy, free markets, and international institutions are spread throughout the world, liberal ideology imagines peace as the end state. Yet, states often deploy war under liberal guises.16 Wars under the aegis of humanitarian values and regime change are examples of the multifaceted character of liberal pacification. Liberal regimes emphasize the violence of those that they are invading, while minimizing the violence involved in these military undertakings and the violence necessary to sustain the liberal societies themselves. What Pierre-Joseph Proudhon called “the moral phenomenology of war” (Prichard 2015, 112–34; Proudhon [1861] 1998) becomes an integral part of the everyday workings of society that shape innumerable aspects of our daily language. The upshot is that, within liberal ideology, the violence committed by liberal states is justified, whereas the violence committed by illiberal states is not.

Postcolonial and anarchist scholarship focuses on the incorporation of violence in the production of liberal spaces (Barkawi and Laffey 1999). These same concerns can be directed onto the liberal order itself. Seen from the perspective of marginalized and oppressed populations, the structures of liberal pacification take on a distinctly violent aspect. The liberal world is not less violent. Rather, the liberal world involves a sophisticated phenomenological process of legitimating certain types of violence in order to render other types of violence invisible.

Liberal Pacification

What does it mean to apply this third type of violence to our understanding of international relations? Pacification reveals liberalism as a violent process as opposed to a system that is emblematic of the absence of direct violence. There are parallels between the Pax Britannia, Pax Americana, and the ancient peace of the Pax Romana (Neocleous 2010, 13). However, our account emphasizes the crucial role of pacification as a distinct kind of violence in maintaining these pacific orders. Our theory offers the novel insight that incorporating pacification into the analysis of the liberal peace reveals crucial aspects of this peace that conventional and critical accounts neglect.

A focus on pacification provides three critical insights. First, it recovers the crucial role of pacification in the historical founding of the liberal order. Second, by distinguishing between three kinds of violence (Figure 2), we account for the empirical observations of the liberal peace as leading to a decline in direct violence and an increase in violence overall as part of the pacification of the Pax Americana. Conversely, the liberal version of the Pax Americana cannot account for key anomalies. Third, our approach draws attention to the violent ordering of social relations. This dimension of violence is neglected even in Marxist, postcolonial, neo-Gramscian, and post-structuralist critiques of the liberal peace, which primarily focus on the role of direct and indirect violence in maintaining the Pax Americana.

Contemporary liberal international relations theory emphasizes the nonviolent role of the liberal triad (democracy, free markets, and institutions) in causing the liberal peace. Yet, a quick review of the history of liberalism in the nineteenth and twentieth centuries shows that key figures in liberalism, from John Stuart Mill, to Joseph Galliéni, to American foreign policy elites, understood pacification as a necessary step in establishing and maintaining the liberal order

Mill, one of the philosophical founders of liberalism, conceptualized and deployed liberalism as a domination strategy. Mill argued that it is appropriate to impose despotism or slavery on “savages” who incline to “fighting and rapine,” but the government should use force as little as possible:

What they require is not a government of force, but one of guidance. Being, however, in too low a state to yield to the guidance of any but those to whom they look up as the possessors of force, the sort of government fittest for them is one [that] possesses force, but seldom uses it. (Mill 1998, 232–33)

In terms of our conceptual distinction, Mill argued that liberalism as pacification was a more effective instrument of violence than the direct modes of violence that governments usually deploy.

The history of European colonialism is replete with this line of reasoning. “[L]iberal improvement” was a regular plank of colonial strategy by France and Britain in the nineteenth century (Owens 2015, 154). Consider one example from the French colonial tradition. Galliéni, a military commander and administrator, consciously deployed liberalism as a domination strategy in the pacification of Tonkin during the 1890s. Galliéni’s strategy involved slowly spreading military outposts and deploying civil administrators to create markets, schools, and amenities. The rationale was that locals would gain a personal interest in the continuation of French control and would help to quell Chinese brigandage. “Piracy,” said Galliéni, “is the result of an economic condition. It can be fought by prosperity” (quoted in Owens 2015, 157). Galliéni devised a “theory of pacification” in which “the correct combination of force and politics can socialize, pacify, and domesticate a population into regulating itself” (quoted in Owens 2015, 157). What Mill proposed in theory, Galliéni enacted in practice; pacification—the violent reordering of social relations in a colony—was a more effective means of maintaining liberal rule than the deployment of direct violence.

While less explicit, the relationship between liberalism and imperialism remained present in the twentieth-century development of the Pax Americana. During this era, US policy makers sought to construct a zone of peace distinct from the zones of war associated with authoritarian regimes. The US State Department first recognized the concept of “hegemonic pacification” in the Euro-Atlantic conference diplomacy of the 1920s (Cohrs 2008, 619). The United States’ “strategic restraint” in the aftermath of World War Two was motivated by this concept of liberal, hegemonic pacification (Ikenberry 2009; Ikenberry 2011, 173). US defense officials Stimson, Patterson, McCloy, and Assistant Secretary Howard C. Peterson agreed that it was a matter of the security interests of the United States to maintain “open markets, unhindered access to raw materials, and the rehabilitation of much—if not all—of Eurasia along liberal capitalist lines” (Leffler 1984, 349–56; Barkawi and Laffey 1999). Liberalism as a domination and pacifying strategy continued throughout (and long after) the Cold War (Laffey 2003; Stokes 2003), as evident in one of the founding documents of the post–World War Two liberal order, NSC-68 (Ikenberry 2011, 168). While the enforcement of a Pax Americana eventually yielded a decline in direct violence, it produced an increase in other types of violence. The first insight of our theory is that pacification has always been part of the liberal project and that the violence in the liberal project never went away.

The second insight is that by reinterpreting the liberal peace as liberal pacification we are able to grant the empirical findings of liberal peace theorists while maintaining that the Pax Americana represents an intensification of violence overall. In the language of positivist social science, our theory is observationally equivalent to that of liberal peace theory. We expect that the quantity of direct violence inversely associates with the degree of pacification in a society. Therefore, our interpretation challenges research that identifies liberal institutions as the cause of declining violence. Liberal institutions, as apparatuses of liberal pacification, ensure that direct violence is increasingly rare while leaving the structures of violence and domination in place. The observational equivalence on particular dependent variables (in our case, all forms of direct violence) produces a theoretical change requiring the generation of novel observable implications (King, Keohane, and Verba 1994, 30).

Furthermore, increased suffering in liberal societies provides evidence contradicting the main claims of liberal peace theories, while remaining consistent with liberal pacification. At its core, liberalism is a project that tries to maximize the utility of its subjects (in other words, minimize suffering while maximizing happiness). As such, a state of liberal peace should lead to a decrease in markers of suffering. However, there is more slavery in the world today than ever before, with conservative estimates of between 12.3 and 27 million people in debt bondage, chattel, or contract slavery (Gordon 2012).17 Moreover, there is ample evidence of rising psychological disorders in liberal societies. A preponderance of evidence from the United States suggests that depression, anxiety, alienation, opioid dependency, stress, other related psychological disorders, increased social isolation, and the decline of community have increased throughout the twentieth century (Twenge, Zhang, and Im 2004, 320; Adler, Boyce, Chesney, et al. 1994; Twenge 2000; Twenge, Konrath, Foster, et al. 2008; Twenge, Gentile, DeWall, et al. 2010; Cohen and Janicki-Deverts 2012; American Society of Addiction Medicine 2016). Changes to human life associated with modernity have caused psychological stress to increase (Jackson 2014). Mortality rates have increased for some white, non-Hispanics aged 45–54 in the United States between 1999 and 2013 (Case and Deaton 2015). Modern technological advances from television to the Internet may contribute to increasing separation and alienation of the social human animal into individualized bodies connected by increasingly weak and empty bonds (Putnam 2000; Gray 2011; Turkle 2011). At minimum, new information communication technology such as Facebook can increase the stress and anxiety of its users (Lee-Won, Herzog, and Park 2015). The violent structuring of liberalism enables increases in social alienation, anxiety, stress, and human bondage through repression, economic control, and social isolation.

These are not isolated instances of suffering. They are fundamental structural features of our liberal world. If liberalism is a process of pacification rather than simply peace, then this rise in individual suffering in liberal spaces may be evidence of a similar process that Fanon equated with the psychic life of the colonist. Just as Fanon’s colonial subjects, unable to lash out at the settler through direct violence, internalized their suffering, modern liberal subjects, unable to resist liberal pacification, internalize their suffering (1982, chap. 6; cf. Sorel 1999, 118). Liberal peace should bring about a rise in happiness; that it has instead led to rising suffering is evidence of liberal pacification.

Third, in addition to offering an alternative interpretation of the liberal peace, our theory of liberal pacification supplements key insights from critical approaches to peace. Tarak Barkawi and Mark Laffey’s work on imperial processes and liberal spaces makes a similar point to ours, that the celebrated zone of liberal peace rests on practices of violence (Barkawi and Laffey 1999, 2002; cf. Neocleous et al. 2013). Their account, however, focuses on practices of direct violence, such as humanitarian interventions against authoritarian regimes or corporations hiring local militias to make work sites in the global south safe for economic extraction (Barkawi and Laffey 1999, 422). Our point is that these moments of direct violence lead to pacification wherein social relations have been so violently reordered as to make direct violence no longer necessary. Once direct violence has established liberal space, pacification functions as a structure of violence that sustains the space. Direct violence only manifests itself when pacification weakens.

Pacification, however, does not merely operate through manipulating the conscience of its subjects. While Marxist and Gramscian concepts of ideology and hegemony are consistent with our theory of pacification (Peceny 1997, 418), they do not address how the constructed political order sustains itself through a violent reordering of social relations. A Gramscian-inspired critique of the democratic peace can yield a bird’s-eye view of the ways in which liberal peace theory is itself deployed as an ideological tool (Ish-Shalom 2006, 569–75). However, Gramscianinspired approaches do not account for the ways that everyday practices of violence (for example, surveillance technologies, implied threats from weapons, security barriers, etc.) sustain liberal pacification. While ideational factors are important in pacification, these factors rest upon practices and structures that are of an ontological-existential character. To review, our reinterpretation of the liberal peace as liberal pacification offers three novel insights. First, liberal scholars and others associate the development of the liberal order with peace and a decline in violence by ignoring how pacification is part of the liberal project. Second, the empirically observed decline in violence equated with the liberal peace is not necessarily a sign of human progress but could be a sign of intensified repression or increases in other forms of suffering across the liberal world order. Third, our concept of pacification reveals violence that is neither direct nor indirect but is phenomenologically structured into the world order. Understanding liberalism as pacification produces a paradigm shift. Liberal pacification is violent in the sense that it coerces a specific type of liberal docility, while also preventing types of resistance that might be understood as violent, including riots, insurrections, civil wars, and interstate wars. Pacification reveals the ongoing violence at the heart of a political project that imagines itself to be against violence.

Conclusion

Our account of pacification recovers a crucial aspect of pax, one originally etched into Roman monuments. The heading of the Res Gestae (the funeral monument to Emperor Augustus) reads, “[t]his is how he [Augustus] made the world subject to the power of the people of Rome” (Beard 2016, 364). This monument does not celebrate peace as the absence of violence; it celebrates pacification. Pax takes the form of a process that violently reorders the world so that imperial subjects are rendered incapable of using violence to resist Roman rule. The absence of overt acts of violence depends upon the maximization of pacification.

The practice of pacification includes threats, coercion, intimidation, and surveillance to restructure and sustain social and political relations. When this type of violence operates effectively, it appears as the absence of violence; pacification’s violence resides in the structuring of the prevailing order. While such an outcome may appear peaceful, it entails, at best, a negative peace that operates through a violent and coercive reordering of society.

Liberal peace advocates measure direct violence and equate the decline in that kind of violence with peace. However, our claim is that the spread of liberal institutions does not necessarily decrease violence but transforms it. Our phenomenological analysis captures empirical trends in human domination and suffering that liberal peace theories fail to account for, including increased inequality, slavery, anxiety, addiction, and anomie. Our analysis also highlights how a decline in direct violence may actually coincide with the transformation of violence in ways that are concealed, monopolized, and structured into the fabric of modern liberal society. If our theory is correct, we will find increases in markers of suffering as society liberalizes. While we cannot say whether these indicators are unique to pacified liberal societies, it is significant that they are rarely, if ever, discussed in terms of violence and the liberal peace.

Liberal pacification is observationally equivalent to liberal peace. This is not a semantic argument. Liberal peace advocates claim that processes that promote individual freedom and autonomy (that is, democracy, free markets, and global institutions) cause peace. While the restructuring of the global order—pacification—reduces direct violence, it also restructures social relations in ways that are violent. Declines in directly observable violence render other forms of violence invisible as violence; in fact, insidious, coercive, and violent systems of military deterrence and compellence, nuclear terror, surveillance, and intimidation constitute the worldhood of the liberal order.

### AT: Markham

#### Goes neg. Only a reorientation of everyday discursive practices can break down the control state.

**Markham 20** - Annette Markham is Professor at RMIT School of Media and Communication and Professor MSO of Information Studies at Aarhus University, Co-Director of RMIT's Digital Ethnography Research Centre, executive committee of the Association of Internet Researchers. “The limits of the imaginary: Challenges to intervening in future speculations of memory, data, and algorithms.” Sage Journals. July 2020. <https://journals.sagepub.com/doi/abs/10.1177/1461444820929322>, AG

Discursive closure, hegemony, and deep structure power

The four themes above do not distinguish deliberate from accidental acts of closure. When power is direct or strategic, we might witness deliberate construction of coercive systems and production of messages that are intended to be highly persuasive or manipulative. We can also see more “soft conditioning,” whereby the coercion is subtler. On the other hand, when ideologies become part of the taken-for-granted infrastructures or institutionalized through organizational and cultural norms, power is more distributed. At this point, ideologies embedded in everyday discourses, materialities, and infrastructures function to self-regenerate. Power becomes hegemonic because both the control mechanisms and the ideologies are invisible, naturalized, and then neutralized. Henceforth, the origin of power is not nearly as relevant as its function. As Gross (2010) writes, “[i]t is the pervasiveness of hegemonic regimes, so deeply embedded and variously expressed in social, political, economic, and cultural institutions” that makes change so difficult (p. 341).

The theme of inevitability is an embedded and invisible ideology of technological determinism. It takes a different shape than when Marshall McLuhan was telling us the medium is the message. This continuously repeated mantra of powerlessness to avoid what is inevitable is not just something we invent; it is learned (or taught) in micro doses through our news feeds. The power of this discourse operates not only on the surface of everyday talk about such matters but at what those of us in critical organizational communication call deep structure levels of discourse (e.g. Mumby, 1988). It can also be a hidden curriculum, as Duffy and Chan (2019) aptly note, buried in the material functioning of the interfaces themselves as well as the imagined affordances we are building into their features.

This theme of inevitability teaches us that our present and possible futures are being determined by technology. The future world is likely to be dystopian, but we do not really have a choice, since it is an either/or proposition: We are either connected to social media or we do not exist. At least as expressed for the past 3 years by dozens of participants in MoRM, technology development is on a trajectory that cannot stop. Within this overarching imaginary, people should expect more and more encapsulation into black boxed algorithmic systems that may not work perfectly or represent us well. The momentum is carried and controlled by the technology itself, since individuals are disqualified from critically analyzing them (after all, even the programmers of algorithms cannot comprehend exactly how they work).

Inevitability and powerlessness are deeply connected to the concept or perception of control. Participants had different ways of embracing or dismissing the presence of technologies that control how we operate or communicate on a daily basis. But throughout the MoRM workshops, the overall trend was to connect the concept of control with two other concepts: neutralization and naturalization. Naturalization occurs when we accept current elements of sociotechnical contexts as simply “just the way it is.” Even a 3-meter scroll of the MoRM Terms of Services (TOS) (copied from a prominent social networking company in 2-point font) did not shock many people, since they were quite familiar with the need to simply agree to terms they had no intention of reading, even if it were easy enough to comprehend. Not one of the hundreds of participants we interacted with failed to sign our TOS.

Over time, the naturalization of objects, processes, or systems also neutralizes them. While Star and Bowker would detail this as “infrastructuring,” critical communication theorists would focus on the control or hegemonic power that can emerge from a habitual practice of perceiving or responding such elements of the lifeworld as if they are valuefree. Through MoRM, we can see how the naturalization process removes agency from all parties, human or not, effectively making it impossible to assign responsibility, blame, or accountability. This neutralization extends broadly to all aspects of the technical interface, the companies behind these, and the people using these capabilities. Rather than assessing how this understanding of control as external to the self is developed ideologically, we can use it as a lens through which to trace whose interests are maintained. We can ask: Who benefits the most from widespread narrative that the digital revolution is upon us, digital futures are inevitable, and there is no way to stop, reconsider, or rethink the current configurations?

Self-regulation and the limits of the imagination

Everyday discursive practices and materialities are powerful not just because they have remarkable potential to persuade others to think and act differently, but also because they operate in such unremarkable ways. Most of us do not recognize that we are shaping social structures when we go about the business of everyday life.

### AT: Nation-States Matter

#### The nationstate is a myth of nostalgic rage.

Bifo 20 (Franco “Bifo” Berardi, founder of the famous Radio Alice in Bologna and an important figure in the Italian Autonomia movement, is a writer, media theorist, and social activist, “Desire, Pleasure, Senility, and Evolution”) // ‘ansel’

Let’s think about the worldwide resurgence of “fascism.” Donald Trump, Matteo Salvini, Boris Johnson, Nigel Farage, Vladimir Putin, and Recep Erdoğan. Are they fascists? No, they are not. And the process that is expanding in large parts of the world, is this fascism? No, it is not.

Fascism was a historic phenomenon comprised of young people. It was a movement based on the will-to-power of a strong, energetic, futuristic movement. It involved people who expected a bright future, and promoted expansion, the colonization of territories and markets. Nobody expects a bright future nowadays. And expansion is no longer possible because the entire planet is subjugated, while markets are saturated. The colonization of territorial spaces is over—**only time can be colonized nowadays**. **The only direction for expansion today is the intensification of time and the acceleration of mental rhythms**. **Only the virtual expansion of cognitive space and the accelerated circulation of signs is possible**. But **this** kind of **intensification is blowing up the nervous systems of humankind**.

Forty years ago, I remember shouting, “No future! No future!” with some young British musicians. I thought it was the provocation of a unlikely avant-garde. Now, everybody thinks that the future is over; now, the sentiment aligns with a conformist position held by most of humankind. “No future” has become common sense, and this is why cynicism is expanding in contemporary culture, in contemporary political behavior. Futurism was the expression of a society that expected something from the future, and of a society that truly felt the warmth of community, whether encapsulated in the nation, the family, or social ties to working communities. All the above was the reality of lived experience a hundred years ago. No more! Today, the nation is a nonexistent thing. The dissolution of the nation is an effect of the pervasive digitalization of information and of power based on information. **Do you think that Google belongs to the United States? Not at all. The United States belongs to the territory of Google**. So does Italy, and France, and so on.

**National sovereignty has been dissolved by the virtual ubiquity of power**; **the nation has come back as a myth, as an aggressive form of identification, as nostalgic rage**.

Belonging has been transformed into a hopeless nostalgia that is at the root of contemporary supremacism. Supremacism is an expression of older people’s fears. For example, it is because they fear migration that they view it as an invasion.

And, largely, it is an invasion. One or two hundred years ago, racism was an integral part of the invasion by white people of the Southern territories of the world. Nowadays, racism is the fearful reaction by white people to the perceived invasion of their own territories. And the racist paranoia of the great racial “substitution” is not merely a phantom, because it corresponds to a real process (one that is happening without the aid of a conspiracy involving George Soros). The white race is—thank god—disappearing. This is the root of contemporary supremacism, which is simultaneously impotent and hyper-powerful; it is unable to change a future of certain decline, but at the same time it is perfectly able to destroy the world in desperate acts that aim to reassert a potency that has vanished.

“Impotence” is the word that explains what is happening, particularly in the Northern parts of the planet. Impotence and the desire for revenge. The neoliberal left has destroyed any possible expectation of a political transformation for the future. The neoliberal left: the Clintons, the Blaires, the D’Alemas, François Hollande, and so on. These traitors have destroyed any possibility of expecting something meaningful from politics and from reason. **Reason**, for its part, **has become the servant of financial algorithms**. When reason is the financial algorithm, the only thing that we can expect from the future is revenge—indeed, a revenge against reason. Horkheimer and Adorno speak of this revenge against reason in the preface to The Dialectic of Enlightenment. They write that **if reason is unable to grasp its dark side**, the unconscious dark side of reason itself**, then reason ensures its damnation**. It is dead. **Revenge against reason is the driving force of the neoreactionary movement** that is spreading: it is revenge against humanity itself.

#### Our arg obviously isn’t that nation-states don’t exist, but that focusing primarily on them is unproductive.

Joque, 18—PhD from the European Grad School, researches philosophy, technology and media and is the visualization librarian at the University of Michigan, go blue (Justin, “Buffer Overflow: The Space and Time of Cyberwar,” *Deconstruction Machines: Writing in the Age of Cyberwar*, Chapter 1, 31-32, dml)

Throughout the short history of cyberwar, the vast majority of attacks have taken place outside of declared conflicts and kinetic wars. It is striking, then, that if we follow both the media and military establishments in calling these events war, war appears no longer to exist in a specific time or place. If cyberwar is taken in its broadest sense to mean a new mode of war targeted against systems, it then marks a new relationship to the space and time of war and attests to the reconfiguration of global spaces by economic, legal, social, and military forces. While many are quick to see in cyberwar an inevitable apocalyptic catastrophe, and while others dismiss these warnings as pure hype, it is most productive to set aside that particular debate and instead explore the specific logic of cyberwar. Under the logic of computer and network-based attacks, certain tendencies of military and economic thinking about the global space of the twenty-first century come to the fore regardless of the ultimate success or failure of these computerized attacks.

Cyberwar exploits security gaps in digital systems and networks and at the same time leverages the global reach of these networks. The attacks that have been organized under the name of cyberwar create nearly immediate effects at a distance, sending information and malicious code around the globe at the speed of light. Cyberwar exists intimately within what Castells calls “the rise of the network society.”1 These attacks on networked digital systems both speak to and engage with these increasingly connected global spaces. Moreover, even while these attacks exploit the vulnerabilities of programs, they are exploited by and in order to leverage spatial and temporal networks. To understand what is at stake in cyberwar, especially as it moves outside the time and space of declared war, requires us to account for these shifts in geography and for the impact of cyberwar on the continual reconfiguration of geography and networks.

This transformation of global space through networks does not mark the end of geography. Rather, geographic space is supplemented by networks of computers, trade, international law, migrations, and so on, some of which privilege flows, speed, and networked contiguity, while others privilege place, slowness, and disconnection. Cyberwar takes place across and between this entire set of geographic and networked spaces. Twenty-first-century military and political strategy does not give up on geopolitics; rather, it engages a multiplicity of spaces and domains. Within these spaces, certain nodes are selected as sites of intervention for their importance to the multitude of networks of which they are part. In a sense, though territory does not disappear, it becomes another type of node in a global set of interwoven networks. Hence warfare, and especially cyberwar, ceases to be exclusively territorial (if it ever was) and becomes primarily concerned with networks. If territory is merely another node in a variety of networks, then war and politics have always been nodal, but what arises with cyberwarfare is a purposeful attempt to explicate and strategize a nodal politics. Thus we must attempt to interrogate the logic of cyberwar as it fixes upon this networked time and space of global politics.

#### Cyberwar distorts the idea of the nation.

**Dyer-Witheford and Matviyenko 19**(Nick and Svitlana, Associate professor at the University of Western Ontario, Professor of Communications at Simon Fraser University “Cyberwar and Revolution”, Chapter Two, CS) [redacted a slur said in a quote, denoted by brackets]

A state’s interpellation of its subjects, or of the subjects of another state, is in part a question of its cyberwar apparatuses’ access to or interdiction from specific platforms. Though platforms may be more or less global or local in scope, they are also national, in terms of ownership and legal governance and relations to a homeland state security apparatus. This is a dynamic around which the profit interests of specific blocs of digital capital and political interests of security state apparatuses mutually revolve (Google/Facebook/Twitter for the United States; VKontakte/ Yandex for Russia; Weibo/Baidu/Tencent for China). “National” interpellation of state subjects is manifestly in play in the banning by the Ukraine government of Russian social media and search engines in the midst of an ongoing war. It may also, however, manifest when military conflict is merely anticipated, as we saw in chapter 1 in regard to the “Sino-Google war” (Bratton 2016, 112) and its imbrication in intensifying China–United States hostilities. However, cyberwar subjectification is not simply a question of demarcating “national” platforms and “national” identities. The profit dynamics of Web 2.0 capital demand both an ever-enlarging user base and the self-activity (and hence self-revelation) of users. Because of this, it is possible to construct within social media interpellative micromachines, that is to say, specific user communities, as a sort of “partisan” presence inside ostensibly foreign digital territory. Within Facebook, one can form a nation, or a caliphate, or perhaps even an assembly or commune. Platforms owned by capital of another state, even an adversary state, can be seeded with subversive practices or used as digital territories across which wars are fought between other competing states, as the Gaza conflict was digitally fought out across Twitter. The truly global social media platforms, owned by U.S. capital, are particularly liable to this process, precisely to the degree that their huge profitability depends on amassing global users. This cyberwar seeding of subjectification involves agents. These are of various kinds: state military public relations agencies, such as the IDF’s Spokesperson’s Unit (now being widely copied by other militaries); clandestine troll armies, such as those of Russia’s Internet Research Agency; U.S. military “sock puppets”; or ISIS militant recruiters. The efforts of such agents may also be articulated with autonomous interpellative processes, such as those of dissenting movements within foreign states or citizen journalists with a spontaneous patriotism for the homeland. Agents may work positively, as “friends”; negatively, harassing enemies; or in contradictory, chaotic directions, generating a paralyzing anomic blur. Each of these comes with its own interpellative processes. For example, one can contrast the careful cultivation of the subject of an ISIS recruitment process with trolling practices associated with Russian hybrid warfare. In the former process, recruiters “monitor online communities where they believe they can find receptive individuals,” sifting through visitors to militant sites. They then create a warm virtual microcommunity around potential recruits, saturating them with messages that, depending on the orientation of the target, may emphasize religious devotion, the appeal of violent action, grievances against racism, religious discrimination, poor economic prospects, or positive depictions of life in militant-held territories. At the same time, they encourage the potential recruit to isolate himself from other contacts. At a certain point, communication shifts from public forums into private and encrypted channels. It is in this phase that options such as emigration to ISIS territory, as a civilian or fighter, or attacks at home are discussed. The cycle is a sustained, modulated “hailing” of an identified data subject as a supporter of the caliphate, a data relation that then translates into corporeal action (Berger 2015a, 2015b).9 Cyberwar trolling is an interpellation that reverses the logic of recruiting. An enemy, rather than a friend, is identified, vilified, enraged, exhausted, and metaphorically (and sometimes literally, through “doxing” and the like) destroyed, silenced, intimidated, or forced offline—with the correct subject position established negatively, in contrast to that of the unfortunate and despicable victim. While the term is loosely applied to many forms of online harassment, it is often more specifically used to characterize a strategy of escalating rancorous dissensus, for example, making a provocation that can be bootstrapped into intensifying abuse and insult. In this form, trolling is sometimes analyzed as having a distinct sequence; the lure, the catch, reeling in, and so on. It may be practiced solo or in teams (with one troll reinforcing another or making an apparently innocent conversational setup that can later be exploited) and can involve a number of gambits (such as professing support for a position but then undercutting it with damning “concerns”). Thus, for example, on a nationalist Ukraine internet forum, pro-Russian trolling can ramp up from an apparently measured remark about U.S. support for Ukraine to intensifying attacks on Ukraine’s corrupt incapacity for self-governance, Western homosexual degeneracy, ubiquitous fascism, cowardice, and inevitable defeat. The subjectifying address is “if you are like that, you are worthless; you don’t want to be like them, the [redacted]/fascists/CIA dupes, but like us, your brave Slavic brothers” (Szwed 2016).

### AT: Perm

#### The perm fails—sequencing is key. Refocusing our priorities is necessary.

**Félix Tréguer 19** – PhD in political studies from the School for Advanced Studies in the Social Sciences, associate researcher at CNRS and post-doctoral researcher at CERI Sciences Po in Paris. “Seeing like Big Tech: security assemblages, technology, and the future of state bureaucracy.” Taylorfrancis. Mar 2019. <https://research.gold.ac.uk/id/eprint/24517/1/9781315167305.pdf#page=156&zoom=100,0,0>, AG [language modifications denoted by brackets]

But post-Snowden controversies also show that these forms of resistance create a risk that we will overlook the pervasiveness of the institutions and technologies, of the rationalities and practices that created the problem in the first place. The risk is that all we are able to come up with are legal, technological or bureaucratic fixes to try to contain the most disturbing aspects of data-driven bureaucracies, without affecting the longer-term trend of a technological arms race that only seems to intensify the issues it was allegedly meant to solve.

Some kind of deeper resistance might be warranted. In his writings on power, Foucault once asked: “How can the growth of capabilities” – and he explicitly mentioned “techniques of communication – “be disconnected from the intensification of power relations?” (Foucault 1984, 48). Computing technologies have since become immensely powerful and yet, we are still struggling to find a satisfactory answer to this crucial question. Despite the hopes of early hackers and Internet pioneers, the decoupling of technology and power is not happening. The key question then becomes whether technology itself or law or ethics can actually be effective instruments to achieve such decoupling.

At this stage of technological development, if we feel like they cannot – at least not in the near foreseeable future – that means it is probably time to refocus on tackling the imaginaries and institutions that underlie the “growth of capabilities” itself: the blind [uncritical] faith in technological progress; the oft-repeated mantra that technology is neutral, that its negative potential will somehow be contained; places like the universities, R&D labs, ministries, start-ups, shops and factories where complex and powerful technologies are designed, produced and traded. As philosopher Jacques Ellul observed, “we set huge machines in motion in order to arrive nowhere” (Ellul 1989, 51). If it is not Thomas More’s eu-topia (“no place”) that we are fast approaching but rather a “dystopian void” (The Luddbrarian 2018), what we need is not just a technological fix, a bureaucratic patch, a principled law or even a good ethics; what we need first and foremost is to get off and stop the machine.

#### Fantasies DA: the perm reinvests in the cybernetic dream of perfectly self-organizing markets. Refusing their fantasy of cybernetic control is both necessary and sufficient.

Halpern, 22—associate professor in sociology and anthropology at Concordia University (Orit, “The Future Will Not Be Calculated: Neural Nets, Neoliberalism, and Reactionary Politics,” Critical Inquiry, Volume 48, Number 2, Winter 2022, dml)

It is perhaps an irony of history that the answer to this problem of overinundation and data surplus appeared to be a turn to cybernetics, new models of networked cognition, and ultimately perhaps even a new model of machine learning that might indeed learn from the distributed intelligence of millions, and now billions, of people. At the same time, such technologies make it impossible to encounter the very legitimate sources of pain in contemporary societies whether induced by structural racism, poverty, disease, or environmental degradation.

This returns us to our present. If Hayek and Hebb still worried about liberal subjects and objectivity, we might ask what concerns animate our contemporary networks? Markets, and now reactionary politics, seek instability and discrimination but without diversity. Shock has been normalized to be managed through our electronic networks. Networks appear to have the power to exacerbate fantasies of individual control and paranoid imaginaries of agential patterns. If “shock” for Klein was a mechanism to destabilize systems and nations to allow the entry of neoliberal governance, we might extend her observation to recognize that now it has become a tool to maintain existing neoliberal systems and to encourage the growth and proliferation of machine learning networks and algorithmic finance.58

I opened this article by arguing that cybernetics and its affiliated communication and human sciences aspired to the elimination of political and psychological trauma through a dream of self-organizing systems and autopoietic intelligences produced from the minute actions of small, stupid, logic gates, a dream of a world of networks without limit, focused eternally on an indefinite and extendable but never-defined future that might be consumed in the present. This dream may now be partially realized, and we have to generate a new set of fantasies.

To do so does not, however, mean wishing, like reactionary politicians, to return to a mythic past. It does not denote fantasizing a Cartesian ethics with transparent algorithms and no black boxes. To do so would only be to replicate the reactionary logic of the database, where processes of distinction and inevitably discrimination are stored only to be retrieved without consciousness or history.

Nor does it mean evading the power we have bequeathed from our machines. The apparatus of the epistemology of the neural net has opened to both positive potentials—neurodiversity, plasticity, and new forms of collectivity—even as it has enhanced the financialization of life and the necropolitics of neoliberal economics. As Randy Martin has argued, rather than separating itself from social processes of production and reproduction, algorithmic finance demonstrates the increased interrelatedness, globalization, and socialization of debt and precarity. By tying together disparate actions and objects into a single assembled bundle of reallocated risks to trade, the new market machines make us more indebted both to each other. The political and ethical question thus becomes how we might activate this increased indebtedness in new ways, ones that are less amenable to the strict market logics of neoliberal economics.59

Hayek, himself, gestured to this possibility within his own thought. Markets he argued, demand difference: “From the fact that people are very different it follows that, if we treat them equally, the result must be inequality in their actual position, and that the only way to place them in an equal position would be to treat them differently. Equality before the law and material equality are therefore not only different but are in conflict with each other; and we can achieve either the one or the other, but not both at the same time.”60 With these words he stated the fundamental dilemma of neoliberalism: to be free we must be put in relation to each other. But he also wavers: Does liberty denote equal treatment, and therefore a generic law, or differential and situated treatment, which might denote planning or coercion? The response of neoliberal discourse has been to automate this relation, thus obscuring its social character, and extract value from the differences between humans while maintaining that such relations emerge evolutionarily and thus are nonintentional but natural and necessary.

Might this discourse be disrupted? Recalling the argument that difference is the foundation for freedom or liberty, can we push this neoliberal imaginary until it folds? This tension might be the source of a possible freedom through relations, if they are historically situated. The fantasy of an archive of processes of differentiation might be mobilized to new ends— mainly to recognizing the permeable, political, and situated nature of social orders. The future, I argue, lies in recognizing what our machines have finally made visible, what has perhaps always been there, mainly the sociopolitical nature of our seemingly natural thoughts and perceptions. In that all computer systems are programmed, and therefore planned, we are also forced to contend with the intentional and therefore changeable nature of how we both think and perceive our world.

### AT: State Good

#### State rhetoric under the illusory guise of technological solutionism covertly perpetrates structural violence.

**Félix Tréguer 19** – PhD in political studies from the School for Advanced Studies in the Social Sciences, associate researcher at CNRS and post-doctoral researcher at CERI Sciences Po in Paris. “Seeing like Big Tech: security assemblages, technology, and the future of state bureaucracy.” Taylorfrancis. Mar 2019. <https://research.gold.ac.uk/id/eprint/24517/1/9781315167305.pdf#page=156&zoom=100,0,0>, AG

Stopping the machine? That begs the question of how best to challenge these new security assemblages.

For one thing, it is worth stressing that Big Data bureaucracies might not be that good at doing what they are supposed to. We can therefore oppose the arguments of those legitimising these new governance models on the grounds of accuracy and reliability. There are reasons – and growing evidence – to doubt that the new “regimes of truth” championed by “Big Data security assemblages” will in any meaningful way provide solutions to security issues (Aradau and Blanke 2015). Technological solutionism in the age of data governance, bolstered by marketing discourses, might only be recreating a veil of illusion of technocratic control, while putting evermore distance between bureaucracies and the social world they wish to make more orderly. After all, history tells us, bureaucracies tend to fail. By disregarding “all the subtleties of real social existence,” “reducing everything to preconceived mechanical or statistical formulae,” bureaucratic dispositifs like “forms, rules, statistics, or questionnaire” – even when fuelled by complex algorithms and troves of data –, remain abstract simplifications that might only reinforce the forms of structural violence they are said to alleviate or even solve (Graeber 2015, p. 75; see also Eubanks 2018, O’Neil 2016).

Bureaucracies often fail to meet their alleged goals but still, they strengthen the power of those who invest in them. They transform the social world and can go awfully wrong (Scott 1998). If, following Tim Mitchell and critical security scholars, we refuse to “see the state and private organizations as a single, totalized structure of power,” another complementary way of resisting these assemblages is to build on the conflicts that inevitably occur “between different government agencies, between corporate organizations, and within each of them” (Mitchell 1991, 90). We can amplify the words of those who denounce the oppressive and manipulative use of modern computer technologies, applaud tech workers opposing the direct involvement of their company in the military-industrial complex, or support security professionals seeking to automate intelligence oversight so as to catch up with large-scale surveillance systems and mitigate abuse. We can, and we should.

### AT: Tech Good—Education

#### Technology is the vessel of authoritarian algorithmic control that reinforce patriarchal notions of power and inequality.

**Hall 21** – Professor of Education and Technology, Research Associate in the Centre for Computing and Social Responsibility at De Montfort University. “Venturing Beyond the Imposition of a Postdigital, Anti-human Higher Education.” Springer link. Apr 2021. <https://link.springer.com/chapter/10.1007/978-3-030-65592-1_4>, AG

The Authoritarian Reproduction of Higher Education

Increasingly, HE labourers are co-opted into the implementation of disciplinary technologies, or technologies designed to control the classroom for value. The integration of learning environment, pedagogy, identity, and technology strips-back autonomy as fows of performance data provide ongoing, formative feedback to systems of algorithmic governance. Independence is reduced beyond the ability to provide feedback on behaviour and activity, in order to fulfl the desires of particular ideological conceptions of HE. Where behaviour and activity are wilful, they are constantly fnessed or managed out of the system (Ahmed 2019). Thus, the digital ecosystems of HE embed competitive techniques and manage risk through behavioural reengineering.

Ideologically, structures and processes are used to make claims focused upon accountability with performance-based incentives, and a commitment to the idea of a meritocracy, through which resources can fow to structures and service units focused upon particular kinds of teaching and research performance. However, it is important to remember that technologies are used against labour by structuring and accelerating work, and the emotional, social, and embodied costs of extended or intensifed work ‘ultimately falls on the workers who make the machine hum’ (Phillips and Rozworski 2019: 89). Algorithmic control cares little for social negotiation or discussions of the fows of power or inequality (McQuillan 2016; Pasquale 2018).

Both curriculum and research practices are overlain with institutionalised technologies that monitor and allow judgements to be made. This includes those for facial recognition and app-enabled attendance monitoring via Wi-Fi tethering (Andrejevic and Selwyn 2020; Meneses et al. 2019), which are marketed in terms of campus security, progression, and retention, but which damage or restrict free expression, privacy, and autonomy (Fight for the Future 2020). The utilisation of such technologies is framed around tracking the individual in response to their actions and location, with judgements imposed about legitimacy, behaviour, and identity. Where behaviours and identities do not match dominant norms, there is an additional layer of injustice in the deployment of the digital ecosystem, in particular given the lack of algorithmic accuracy in addressing people of colour and women, alongside non-binary and trans people (Grother et al. 2019). This is amplifed because the collection of sensitive biometric data is intrusive and tends to lack consent, even whilst information about individuals, contacts, behaviour, feelings, and practices is sequestered and re-purposed (Pasquale 2016).

Such technologies are authoritarian not simply in terms of their governance and the ways in which they maintain systemic order in the face of uncertainty directed for the production of economic value. They are also disciplinary in that they quantify human lives and experiences, construct particular identities based on dominant norms, and then enforce the internalisation of that quantifcation/construction (Stark 2019). They form a terrain of necropolitics that makes invisible certain bodies, or makes their existence a form of living death (Mbembe 2019). The process of making invisible is shaped by institutional formations that serve to benchmark individuals, subjects, and institutions, pivoting around human capital formation (World Bank Group Education 2020). This demands structures that can measure, monitor, and report learning outcomes and implement action plans predicated upon generating commodity and leverage graduate skills and contributing to innovation, across a comparable, international terrain.

The institution, whether postdigital or not, makes it diffcult for individuals and groups to move beyond these fows of power, or to challenge them collectively. There has been an emptying out of the politics of the University in the face of the disciplinary imperatives of commodity production and exchange. This means that any meaningful analysis of the humanist potential of a postdigital HE has to recognise its increasingly authoritarian policy and practice-based context, including:

• struggles in 2020 against cuts to humanities and social sciences courses that are deemed low-value, for instance at the universities of Sunderland and Portsmouth in the UK;

• struggles by graduate students at the University of California, Santa Cruz, taking part in wildcat strikes since 2019 to demand living wages;

• struggles in 2019 at the University of Juba in South Sudan against tuition fee hikes that threatened the right to education;

• the history of protest at Jawaharlal Nehru University in Delhi, including the 2016 sedition row, and 2019 struggles over accommodation fees and India’s Citizenship Amendment Act;

• the hostile environment created by institutional engagement with national immigration practices like the Prevent Duty in the UK;

• the use of court injunctions to halt demonstrations on campuses;

• media panics over issues like grade infation, which are presented as threats to the value of a degree or of higher education composition; and,

• discourses around free speech predicated upon disciplining specifc bodies and communities.

These struggles are responses to policy narratives that deform and re-purpose the epistemic role of HE in society. They enable us to analyse any postdigital conceptualisation of HE in relation to the authoritarian characteristics of the forms or structures of HE, its cultures or pathologies, and its activities or methodologies.

• First, the form or structure of the University or College develops in order to maintain the ideological repositioning of social reproduction around ordered liberties rather than democratic rights. Thus, HE gives individuals the liberty to develop their own human capital and that of their families, and any rights they have are rooted in the deployment of that human capital for entrepreneurial, value-driven ends (Bruff and Tansel 2018).

• Second, the cultures that emerge from these structures pathologically reinforce inequality in access to collective, public goods, based upon dominant, patriarchal notions of productivity (Bruff 2014). In order to consume social goods, individuals are expected to deliver value-for-money and to be economically productive, in ways that are defned hegemonically in relation to white, male, ableist, heterosexual norms.

• Third, these pathologies recalibrate social relationships in the name of markets through labour market reforms and regulation that supports corporate forms, such that the regulation and governance of institutions, data and justice is focused upon the production and circulation of value, rather than shared values (Connell 2013).

• Fourth, the terrain of HE is re-engineered methodologically, through commodifcation to enable the corporate parasitisation of notionally public organisations, through ideologies, policies, and practices of privatisation, marketisation, and fnancialization (Davies 2017). As a result, the activities of HE, like the production of textbooks, articles, and ways of knowing the world, become commodities that can be exchanged.

These characteristics interact through fows of data and digital lives, in order to discipline specifc kinds of useful knowledge and a specifc kind of useful knowledge producer, in relation to the authoritarian reproduction of value. It is in this context that postdigital HE takes shape.

### AT: Tech Good—Info Tech

#### Despite potential positive uses of technology, information tech has fueled radicalization and violence.

Bunse ’21 Dr Simone Bunse is a Content Manager for the Stockholm Forum on Peace and Development and Researcher at SIPRI. Her previous positions have included Director of Academic Affairs at Lead University, Costa Rica; Associate Teaching Professor at Georgetown University’s McCourt School of Public Policy, Washington DC, USA; Assistant Professor at INCAE Business School, Costa Rica; and Visiting Researcher at the Free University of Brussels, Belgium. (Simone Bunse, "Social media: A tool for peace or conflict?", Stockholm International Peace Research Institute, 8-1-2021, https://www.sipri.org/commentary/topical-backgrounder/2021/social-media-tool-peace-or-conflict. Accessed 7-4-2022, RS).

Human rights activists have used social media technology to organize peaceful protests and defend democracy for more than a decade. More recently, peacebuilders have discovered it can be a tool to understand conflict dynamics and counter extremism better. Yet the potential of social media as a megaphone for promoting human rights, democracy and peace is overshadowed by its dismal record of being used to drive radicalization and violence through disinformation campaigns. This ‘online frontline’ will continue to be the case, unless regulators, social media firms and citizens revisit current policies and practices.

At the 2021 Stockholm Forum on Peace and Development researchers, policymakers, tech companies and civil society organizations had an opportunity to explore how social media can be harnessed for peacebuilding purposes and to assess policy responses to harmful online disinformation campaigns. This Topical Backgrounder is inspired by these discussions, particularly on the Janus-faced nature of social media. It makes four recommendations—one each for peacebuilding practitioners, policymakers, social media companies and citizens—to protect peace, democratic institutions and people’s welfare:

Peacebuilding practitioners should systematize the use of social media technology for conflict stakeholder analysis, early warning, counter-messaging and the defence of democracy and human rights;

Policymakers should stem harmful social media disinformation campaigns by creating effective oversight and strict data management guidelines;

Tech companies should redesign their social media tools to prevent them from being employed for harmful political ends and from favouring conflict over consensus; and

Citizens should improve their resilience to disinformation, but also demand insight into the information collected about them by social media firms, how it is used and by whom.

Social media as a peacebuilding instrument

Participants in the Stockholm Forum sessions highlighted four uses of social media technology in peacebuilding research and practice: conflict stakeholder analysis; early warning; counter-messaging; and social mobilization for peaceful protest and democracy. However, none of the four uses has yet fulfilled its potential.

Conflict stakeholder analysis

Peace and conflict researchers increasingly examine social media content to map conflict actors, trace the links between them and identify their local support networks. This has greatly improved the understanding of Nigeria’s Boko Haram, for example, which has relied on social media for its messaging since 2009.

Early warning

Researchers also monitor social media content to gain better insights into local grievances—a key driver of violence. In sub-Saharan Africa, for example, local grievances have provided a fertile ground for the expansion of extremist groups. Tracking such grievances online in real time can feed into early warning systems for conflict.

Counter-messaging

Young peacebuilders use social media platforms to develop viable counter-messages to extremists. These are more likely to be successful if grounded in local (sometimes high-risk) in-person activities or activism.

Social mobilization for peaceful protest and democracy

Social media technology has also created opportunities for people to mobilize politically in defence of democracy and human rights. In 2009 in Moldova, for example, young people relied on Twitter to oppose the country’s communist leadership. In Iran, citizens used Twitter to organize protests against the results of the 2009 presidential election, leading to calls for Twitter to be considered for the Nobel Peace Prize. During the Arab Spring in 2011, protestors in Egypt and Tunisia took to social media platforms to organize, spread their message internationally and ultimately overthrow dictatorial regimes. Particularly in repressive regimes, social media has been a communication channel for people to stand up for human rights or share evidence of human rights abuses thereby preventing government monopolization of information. It is hence no coincidence that social media giants, such as Facebook, Twitter and YouTube, are blocked in China, Iran and North Korea.

All four uses of social media could be employed a lot more strategically to reap benefits for peacebuilders or human rights activists. To date, much of the hope connected to social media as a tool for human rights, democracy and peace after the 2009 ‘Twitter revolutions’ has subsided or been replaced with concern about its potential to contribute to conflict.

Social media as a driver of conflict

In the worst cases, social media platforms have been used to suppress internal dissent, meddle in democratic elections, incite armed violence, recruit members of terrorist organizations or contribute to crimes against humanity, as in the case of persecution of the Rohingya in Myanmar. In 2020 there was evidence of social media manipulation in 81 countries and of firms offering ‘computational propaganda’ campaigns to political actors in 48 countries. While propaganda is not new, the 2021 Stockholm Forum highlighted some of the reasons why propaganda on social media presents distinct challenges compared to traditional media, unintentionally drives conflict or affects peacebuilding efforts.

From news editors to tech companies

The rise of news distribution and consumption via social media platforms has shifted the gatekeeping power for information dissemination from editors and journalists—bound by professional codes of ethics, principles of limiting harm and editorial lines—to tech companies owing allegiance primarily to their shareholders. Professional news outlets across the globe now ‘compete with content producers—domestic and international—who produce junk news that is sensational, conspiratorial, extremist, and inflammatory commentary packaged as news’. Social media providers are currently protected against liability for user content and have shied away from becoming ‘arbiters of truth’.

Creation of echo chambers

To maximize profit by growing user engagement and participation, social media companies have created sophisticated tools which filter information and place people in virtual echo chambers. These confirm or even radicalize the users’ world views. Currently, the algorithms underlying social media platforms’ business model amplify the angry and divisive voices which drive engagement, pushing users towards ever more extreme content.

Voter manipulation and offline violence

The pigeonholing of information not only shapes people’s world views, but also their behaviour. The violent storming of the United States Capitol Building in January 2021 was, in part, motivated by the false widespread claim that the 2020 election was rigged. Stockholm Forum speaker Aws Al-Saadi, the founder and CEO of Tech4Peace—a large fact-checking network in the Middle East and North Africa—explained how online rumours can kill and fake online news about specific people in Iraq has sometimes prompted others to take justice into their own hands. Maria Ressa, CEO of online news outlet Rappler in the Philippines, argued: ‘Social media has become a behaviour modification system. And we’ve become Pavlov’s dogs that are experimented on in real time. And the consequences are disastrous.’

Interference in conflict dynamics

It is also increasingly clear that even well-meaning global social media campaigns can interfere in conflict dynamics. A recent article explained how, after an information leak, the international #BringBackOurGirls social media campaign to free the high-school girls kidnapped by Boko Haram in Chibok in 2014 hindered rescue attempts and may have encouraged the group’s growing reliance on gender violence and kidnapping for international attention and ransom.

Risks to peacebuilders and humanitarian efforts

Another prominent theme in several Stockholm Forum discussions was the risk that adverse social media reactions pose to peacebuilders or humanitarian efforts. For example, individuals working in projects with colleagues from countries considered to be adversaries (Armenia/Turkey; Armenia/Azerbaijan) cancelled their participation in these collaborations after suffering personal attacks on social media. Systematic online campaigns to defame humanitarian organizations are another example. Between 2013 and 2017, hundreds of humanitarian White Helmet volunteers were killed in Syria after manufactured social media claims that they were terrorists with links to al-Qaeda and the Islamic State.

### AT: Tech Good—Peace

#### Technology doesn’t reduce violence, but obscures it as a failure to take advantage of liberal freedom. The impact is permanent everywhere war.

Johnson, 18—Professor, Environmental History, Loyola University Chicago (Benjamin, “Coded Conflict: Algorithmic and Drone Warfare in US Security Strategy,” Journal of Military and Strategic Studies, Volume 18, Issue 4, dml)

Understanding technology as more than a neutral tool that is exogenous to political and social life has been an important site of intervention for critical theory, especially in understanding how technology interacts with social and political existence to obscure and perpetrate violence. The conceptual, theoretical and discursive underpinnings of the liberal peace have been advanced and critiqued on a number of fronts. For example, these works have focused on the adherence of research to quantitative ‘large-N’ statistical testing where the liberal peace is treated as a scientific phenomenon; 35 the role of liberal peace as a ‘tripartite international discursive environment’ in which superficial technical solutions to resolve conflict are produced; 36 the ‘punitive ethos’ inherent to liberalism’s normative influence on counter-terrorism policy;37 the limits to liberalism’s understanding of actors in terms of states and their institutions;38 the inherent violence of Western modernization and its links to liberal peacebuilding; 39 and lastly the liberal character of empire building through imperial expansion.40

This body of literature has teased out the implicit and explicit forms of violence that underpin liberal internationalism. Violence undertaken in the name of spreading liberal democracy has increasingly been exposed and difficult to ignore, especially as war has expanded through visual representations and made available to people outside of conflict zones.41 James Der Derian has gone so far to argue that with respect to a global liberal project of civilizing the world, “in spite of, and perhaps soon because of, efforts to spread a democratic peace through globalization and humanitarian intervention, war is ascending to an even higher plan, from the virtual to the virtuous.”42 Commenting on the discursive narrative that technology enabled distance has allowed for a peaceful or ‘clean’ type of war, Der Derian goes on to argue that “at the heart of virtuous war is the technical capability and ethical imperative to threaten and, if necessary actualize violence from a distance – with no or minimal casualties” and that “on the surface, virtuous war cleans up the political discourse as well as the battlefield [...] virtuous wars promote a vision of bloodless, humanitarian, hygienic wars.”43

The notion that liberal war has somehow become surgical and bloodless is linked to what a number of authors have identified as a shift from government to governance. Rather than ‘boots on the ground’ and active attempts at state building, liberal interventionism has shifted to emphasize the management of and engagement with populations at a distance. Again, this should not be understood as an altogether new phenomenon. Heathershaw argues that liberal peacebuilding, while theoretically linked to Kant’s notion of a perpetual peace, is more recently linked to discourse that proliferated at the end of the Cold War.44 Democratic peacebuilding was developed by the United Nations (UN) along with its major donors and analysists in the immediate post-Cold War period, which was understood as a “watershed moment akin to 1919 or 1945”, thus spawning the ‘new interventionism’ that dominated policy rhetoric during the 1990s and early-2000s.45

However, along with this discourse there has been a pronounced shift in practice towards increasing forms of bio-political governance in the Foucaultian sense of the term. For Dillon and Reid, “global liberal governance is substantially comprised of techniques that examine the detailed properties and dynamics of populations so that they can be better managed with respect to their many needs and life chances” and where “biopolitics is the pursuit of war by other means.”46 Foucault has made a lasting contribution to the critique of liberal security and war, which becomes especially useful in theorizing current conflict environments. For Evans, life itself becomes the object of political strategies, which holds implications in terms of security. 47 Echoing Dillon and Reid, Evans states that “in the process of making life live, [those general strategies for effecting power] entail the regulation of populations for society’s overall betterment.”48

The notion of ‘bettering’ society is implicated in the idea that freedom must be produced in a very particular manner linked to distant governance.49 The idea that freedom is an actively created condition for life can be related to the work of Mark Duffield, who has offered one of the most comprehensive critiques on liberal interventionism over a number of years. Duffield has demonstrated and analyzed the merging of security, development and humanitarian discourses, all of which are increasingly underpinned by the same logic of ‘governance at a distance’ enabled by network technologies. In particular, security and humanitarianism has taken an explicitly neoliberal turn as disaster affected populations are now expected to self-manage. Duffield explains that the merging of security and humanitarianism within a neoliberal framework has led to the notion of ‘resilience,’ which “focuses on narcissistic and subjective forms of care-of-the-self.”50 Duffield argues that remote technologies for surveillance and bio-political management are part of the neoliberal shift in political economy more widely.51 Within this paradigm shift, affected populations are to be “made free” and to “embrace risk and thereby develop foresight and enterprise.”52 Again, the idea of being ‘made free’ emphasizes the liberal interventionist role of producing freedom, but not in terms of emancipatory conditions circumscribed by a positive commitment to liberty in the philosophical sense, but rather through a contradictory and explicitly negative form of liberty within an absence of formal constraints. A positive form of liberty would imply the need for various forms of material and resource commitment (money, time, people, expertise, etc.), whereas negative liberty simply assumes an ideological and structural commitment to removing obvious obstacles or barriers to expressing one’s freedom. People are made free via the removal of institutional, cultural and other social restrictions (including social protections), thus enabling their own volition.53 For Duffield, “resilience embodies a new biopolitics that differs from the actuarial and protective biopolitics [...] that underpins the great modernist project of Welfare Fordism.”54

This distancing of humanitarianism, development and security should not obscure the violence perpetuated in their name. Just as security begins to appear as an ‘everywhere’ and ‘permanent’ war, populations are abandoned to a state of “permanent emergency.”55 These populations are the same groups that are made the objects of securing against, where “liberalism proceeds on the basis that ‘Others’ are the problem to be solved.”56 The remote management of populations through techniques of biopolitical governance is accomplished with the underlying rationality of risk aversion, which is argued to be intensified by the repeated difficulties encountered by allied Western forces in recent campaigns. There is an explicit relationship between the failures of these campaigns and the growth of remoteness as an ordering logic for state intervention, leading Duffield to argue that ground or “terrestrial” forms of “liberal interventionism now [lie] burie[d] in the ruins of Iraq, Libya and Syria.”57

### AT: World Getting Better

#### Their data cherrypicks limited stats to represent a whole, thus using a concept of progress to create a metastable closed-off world that they have under control. This project is violently extractive.

**Bardin and Ferrari 22** – Dr Andrea Bardin is Senior Lecturer in Politics at Oxford Brookes University, UK; PhD Political Philosophy and History of Political Thought (University of Padua); PhD Political Theory (Brunel University London); Laurea summa cum laude in Philosophy (University of Padua). Marco Ferrari is Ph.D in Philosophy and Postdoctoral Research Fellow in Political Philosophy at the Università di Padova. “Governing progress: From cybernetic homeostasis to Simondon’s politics of metastability.” Sagepub. The Sociological Review Monographs 2022, Vol. 70(2) 248–263. Mar 2022. <https://journals.sagepub.com/doi/pdf/10.1177/00380261221084426>, AG

The point of government in a neoliberal perspective is neither to limit the freedom of initiative, nor to assume that social stability depends on an invisible hand, but rather to carry on a detailed regulation of liberties for the sake of the ‘spontaneous’ equilibrium of the markets. An incessant work of data extraction through ever perfected algorithms sets the conditions of possibility of the subjects’ behaviour – economic actors, ideally selfemployees – and orients it towards the preservation of the system’s dynamic stability. Social change is thus governed and reduced to the hyper-modern idea of progress, conceived as a variation within the parameters deemed necessary for the reproduction and survival of the system. All the ‘irrational’ noise that is not immediately reducible to progress thus conceived is either silenced or – once neutralised – included in the pattern as a risky and unforeseen opportunity to perfect the system’s survival (Castel, 1991; Dean, 1998; Ewald, 1991). More radically, these elements are normatively integrated in the system’s core dynamics in the form of an ethics of flexibility (Fraser, 2003) establishing the ‘good’ functioning of governmentality.

The government of progress is thus resolved in the incessant operation of protection, management and promotion of homeostatic mechanisms deemed capable of self-regulation, but in fact selected and – if necessary – substituted with others, offering a more inclusive and complex capacity of adaptation to the macro-mechanism of the market. This macromechanism is the undisputed horizon that imposes to political power the task of providing a homeostatic equilibrium functional to its progressive implementation. With its ‘soft’ determinism and immanent teleology the market thus appears to be a hypermodern version of the clockwork universe theorised in early-modern mechanical science, and the vector of a similar onto-epistemological reduction of social reality to a mathematical form. And this reduction still relies on a ‘mythical’ concept of progress alimenting an ‘illusion of simultaneity’ that hides a plurality of paths by projecting the ‘eternal present’ of the market on all possible futures.

Simondon: Progress and metastability

The connection we have established between cybernetics and neoliberalism will allow us to use Simondon’s concept of ‘metastability’ against both of them. Although acknowledging Wiener’s invention of the term (Simondon, 2014, p. 236), Simondon elaborated the concept of metastability drawing on Canguilhem’s work and in explicit contrast to the cybernetic concept of homeostasis. Metastability describes systems macroscopically stable but internally characterised by an uneven distribution of potentials and hosting processes that make that stability only apparent. Metastable systems enjoy a ‘stability far from equilibrium’ in which the aleatory ‘encounter’ with a minimal quantity of energy or information can trigger a brusque alteration of equilibrium, and lead to the invention of new structures and hence to a new ‘metastable state’. The notion of metastable equilibrium marks the project of an ‘axiomatic of human sciences’ Simondon presents in explicit opposition to the cybernetic theory of society, questioning at the same time the notion of homeostasis and the deterministic ontology the latter relies upon (Simondon, 1958/2020, pp. 697ff.). Briefly sketching Simondon’s project will allow us to outline the theory of government he elaborates in contrast to Wiener’s, and explain how this may be used as an antidote to the neoliberal conception of government and the hyper-modern condition it shares with cybernetics. Simondon’s concept of ‘metastability’, we will argue, can support an alternative understanding of progress based on the idea of government as the facilitation of normative invention.

In his social theory, Simondon expands on Canguilhem’s study of social normativity. Canguilhem’s starting point is a critical reading of the biological modelling of society adopted within the French sociological tradition. In that paradigm the sociologist is asked to define the ‘normal type’ and provide the politician, the social physician, with the task of re-establishing the ‘normal state’, independently of the way society ‘appears to itself’ (Durkheim, 1924, p. 54). Canguilhem provides a decisive critique to the organic model and a radical turn to its political implications. What he considers socially ‘pathological’ is not the deviation from normality, but, on the contrary, the very normalisation of a ‘stable’ form of equilibrium. Relying on the work of the German neurologist and thinker Kurt Goldstein, he assumes that, both organically and socially, ‘the healthy state, much more than the normal state . . . is the state which allows transition to new norms’, while ‘pathological constants’ are ‘repulsive and strictly conservative’ (Canguilhem, 1991, p. 228) and in fact typical of a form of life stuck in its own ‘narrowed milieu’ and incapable of further normative invention (Goldstein, 1995, p. 188). Simondon welcomes Canguilhem’s advice to consider society in its own terms, as ‘neither machine nor life’ (Canguilhem, 2002), and takes it a step further, also attacking the technological modelling of society theorised by cybernetics.

Simondon detects in Wiener’s cybernetic theory of society an attempt to reduce the complexity of social systems to the technological model of the ‘automaton’. For Simondon automata are emblematic of the hyper-modern condition – they represent a rigidly deterministic understanding of change that de facto cancels it: ‘the automaton is entirely given in its initial state, it functions but does not become’ (Simondon, 2016, p. 401). ‘Direct adaptation’ and ‘structural stability’ are the hallmarks of ‘the perfect automaton’, and ultimately rely on the same normative assumptions implicit in the concept of ‘homeostasis’ that Wiener’s technological model implicitly sets as the ultimate goal of social organisation. Simondon reverses this value judgement while questioning the epistemic value of the model itself. The very study of technical objects shows that ‘automatism’ describes ‘a rather low degree of technical perfection’ and its idea is in fact a myth rooted in ‘economic or social’ thinking rather than in technical knowledge (Simondon, 1958/2017, p. 17). In social theory, the ideas of automatism and homeostasis, although describing a crucial aspect of social dynamics – that is the closure within ‘a stereotypical, hypertelic and inevolutive adaptation’ – fail to grasp the ‘constructive and creative adaptation’ of societies. While for Wiener homeostatic stabilisation defines both the core functioning and the goal of social systems, for Simondon a degree of social homeostasis is both a prerequisite of society – the ‘rate of automatism’ that grants ‘stability and cohesion’ – and a problem (Simondon, 1958/2020, pp. 422–423).

Wiener’s hyper-modern renewal of the Hobbesian myth of a political ‘automaton’ is, from Simondon’s perspective, an epistemological mistake and a political danger. Statistical mechanics hinders a proper understanding of processes harbouring a ‘margin of indeterminacy’ (Simondon, 1958/2017, pp. 147–159) that can only be understood through a ‘non-probabilistic method’ (Simondon, 1958/2020, p. 697), and the myth of the automaton surreptitiously becomes a goal whose actual realisation would destroy the very system it was supposed to save. A perfect ‘automatic’ homeostasis, far from solving the problem of social regulation would substitute the social system’s ‘tense’ metastability with the kind of dynamic stability that ultimately leads the system to exhaustion. The self-destructive goal of automatism is in fact the cancellation of any ‘margin of indeterminacy’ with the result that ‘there is no longer any possible variation; the functioning repeats indefinitely’ (Simondon, 1958/2017, p. 152) until entropy consumes all the residual potentials, leading to the ‘resolution of all tensions’, that is ‘death’. For Simondon, on the contrary, a system only keeps working and developing as long as it ‘conserves the tensions in the equilibrium of metastability instead of nullifying them in the equilibrium of stability’ (Simondon, 1958/2020, p. 226).

It is on this basis that Simondon sketches his theory of government as an alternative to Wiener’s. Playing a biological model against Wiener’s normative assumption that ‘a good homeostatic regulation is the ultimate purpose of societies, the ideal that must animate every act of government’ (Simondon, 1958/2017, p. 162) Simondon theorises government as an act of normative invention relying on existing social automatisms but exceeding them. An ‘act of government’ for Simondon should be ‘grounded in homeostases so as to develop itself and to continue its coming-into-being, rather than remaining perpetually in the same state’ (p. 162). Governing is ‘inventing’ solutions aimed at making the system ‘metastable’, that is open to further invention, rather than contributing to reproduce the ideal order imagined by social theory and imposed by politics as a goal.

Many critics of neoliberal governmentality, and in particular of its ‘algorithmic’ version, have been inspired by Simondon. This is evident in their stressing the importance of creating spaces of political conflict in which social invention – the ‘transindividual . . . coupling between the inventive and organisational capacities of several subjects’ (Simondon, 1958/2017, p. 258) – can take place against the dominant neoliberal neutralisation of subjectivity and conflict (Rouvroy & Berns, 2013; Stiegler, 2016). The idea of ‘progress’ may appear to be embedded in precisely the stance these theorists are criticising, but we believe that Simondon’s concept of metastability allows for a different idea of progress. In neoliberalism, the market’s ‘spontaneous’ continuation is paradoxically assumed as the goal of politics, which entails the reduction of progress to a sequence of preventive social adaptations to ever-emerging ‘local’ risks within the naturalised framework of the market. Thus, the neoliberal promotion of risk-management ethics – a lifestyle informed by constant planning, resource management, etc. – is one of the most powerful ideological tools for the preservation of social homeostasis within the market economy. This government of behaviour is capable of de-activating the potential reinvention of social forms. ‘Governmentality’ thus conceived is not simply a matter of preventing the risk of a radically disruptive event, it is about governing its possibility as such. The ‘progressive’ mechanisms of social reproduction governed by the market’s open dynamics thus entirely absorbs what is a completely different kind of ‘risk’ represented by human inventiveness and imagination, which Simondon theorises under the label of metastability.

The ‘risky’ politics of metastability theorised by Simondon is based on the assumption that progress conceived as the ‘invention of new goals’ makes radical novelty possible. This concept of progress is based on an understanding of social systems as inherently metastable because of the ‘fairly dangerous’ automatism characterising the human being, who ‘always risks inventing and equipping new structures’ (Simondon, 1958/2020, p. 423). This is not to say that Simondon resorts to a vitalist view on the exceptionality of life over matter or some sort of social evolutionism. Rather, he theorises ‘invention’ as an emergent property of the bio-technical nature of human beings and societies. This tendency towards invention is for Simondon embedded in the partial indeterminacy or ‘historicity’ that, in his ontology, defines all systems and processes (Bardin, 2021, pp. 36–37). At the level of human natural and social (i.e. ‘transindividual’) ‘historicity’, technical activity is not a mere vector of technological progress, it is an actual challenge to existing social norms. Human ‘progress’ takes place at the scale of the ‘metastable’ system formed by ‘human beings and the world’ and mediated by technical objects whose functioning exceeds all efforts of symbolisation (Simondon, 1958/2017, p. 168). Progress thus conceived is not a triumphal march, it is the result of a disharmonious relationship between biological patterns that vary in the very long term of natural history, the quick accumulation of technoscientific innovations, and the social rhythm of culture that attempts to render these processes compatible with its institutional present (Simondon, 2010). This is neither ‘progress conceived as a march in a direction fixed in advance’, nor a process of ‘humanisation of nature’, but rather an aleatory process of ‘naturalisation of humans’ mediated by the ‘techno-geographical milieu’ they keep inventing (Simondon, 1958/2017, p. 58).

This notion of progress entails a political risk because it leaves political practice without a safety net. In this open dynamic, the emergence of finality and hence of social invention is grounded on the structural lack of control of technical reality that nurtures the very possibility of human freedom: ‘Man [sic] frees himself from his situation of being enslaved by the finality of the whole, by learning how to create finality . . . as not to have to be passively subjected to a de facto integration’ (Simondon, 1958/2017, p. 119). This is what, according to Simondon, cybernetics itself teaches us, but crucially missing the point that risk cannot be recaptured within the existing social norms and mode of production. On the contrary, risk conceived as a structural margin of indeterminacy (‘historicity’) is embedded in technical activity, and a constant challenge to the whole ‘system of values’ (Simondon, 1958/2020, pp. 414–415). We believe Simondon’s concept of metastability opens in this sense to the possibility of moving beyond the paradoxical conflation of determinism and teleology theorised within the hyper-modern idea of progress, ultimately shared by cybernetics and neoliberalism, and allows to ‘think together nature and excess, technology and revolution’ (Toscano, 2012, pp. 107–108). It thus calls for an alternative theory of government.

Governing progress, in Simondon’s sense, is part of the collective effort of inventing mediations and solutions in which science and politics can play a crucial role if they do not reduce the reality of non-symbolic processes to their – also scientific – imagination. This kind of government will have more to do with the ‘invention’ of new technical and cultural possibilities than with the dreamed regulation of the existent by a philosopherking (Simondon, 1958/2017, pp. 161–163). Such inventions run, of course, the risk of failure, but this is precisely where their political value lies. Simondon’s concept of progress does not allow acts of government a safety net offered by social theory predictions. On the contrary, Simondon’s social theory certifies that not running the risk of normative invention is equal to suffering a different kind of defeat, the defeat of accepting an allegedly ‘progressive’ politics that, as a matter of fact, reaffirms the norms codified by the theory and resists radical change. This is precisely how Wiener sees progress grounded on the idea of the dynamic stability (homeostasis) of ‘local and temporary islands of decreasing entropy’, which ‘enables some of us to assert the existence of progress’ (Wiener, 1954/1988, p. 36). Instead, Simondon’s vision is condensed in an ethical formula that critically mirrors Wiener’s statement by reversing it, and postulates that ‘there are no lost islands in becoming, no domains eternally closed in themselves’ and ‘each gesture’ is an act of invention within a (metastable) network that connects past and future (Simondon, 1958/2020, p. 377). This ethical gesture is inherently political, it requires the active consideration of entropy and death as part of a system’s functioning, and the assumption of social invention as the core of an idea of progress to be formulated beyond the hyper-modern condition.

Conclusion: Governing progress

If one assumes the exhaustion of the (hyper-)modern idea of progress, one is also deprived of the theoretical background that has long informed the mechanical understanding of social dynamics, an understanding that still informs neoliberal governmentality. A critique of the concept of homeostasis that grounds this idea of progress, we have claimed, allows for a different approach. In this sense, our article firstly offers a historical contribution by exposing the onto-epistemological stance that underpins much theorisation of early modern science and cybernetics, liberalism and neoliberalism. Secondly, it aims to show that Simondon’s concept of metastability opens the path for a reformulation of the idea of progress within a framework that sees partial indeterminacy (or ‘historicity’) at the core of social dynamics and their government. From this perspective, knowing the social and acting politically means favouring the ‘metastable’ tension that enables scientific and political invention, defying the automatic defence of a mythically established social order. Governing progress therefore requires the radical endorsement of change, which includes the contemplation of death and failure as a necessary part of it, and therefore the opening of social systems to a future beyond the mere preservation of their own existence.

## Answers

### Alt Fails—AI

#### Governance is necessary, rejecting engagement with AI regulation fails.

**Gulson et. al. 22** - Doctor of Philosophy, Professor at University of Sydney, current research investigates whether new knowledge, methods and technologies from life and computing sciences, with a specific focus on Artificial Intelligence, will substantively alter education policy and governance. “Algorithms of Education: How Datafication and Artificial Intelligence Shape Policy.” 3lib. May 2022. <https://3lib.net/book/21413757/7421ff>, AG

Toward Problematization

The three options above may each offer viable responses to the new challenges created by synthetic governance depending on the context. Moreover, each would be comfortably familiar to those in the field of critical policy studies. Certainly, there is need for a more robust discussion about regulation, data privacy, and the monetization of data generated in education. However, each of the above positions depends on an assumed distinction between human and machine that we have sought to trouble, locating political agency in a human subject who promotes, enhances, tames, regulates, hides from, or even destroys machines. Yet synthetic governance as we have characterized it is built upon a network infrastructure that is “medium of contemporary power, and yet no single subject or group absolutely controls a network.”31

Between the abstraction of data, the materiality of information systems, the emergence of new forms of thinking, and changes in the visceral terrain of political life, we can identify new governing relations where humans are in the loop, but not as independent arbiters of algorithmic decision-making. Even more strikingly, machine cognition is a product of human thinking that feeds back into human culture, and we must consider the view that governance has never been anything other than a cybernetic feedback loop. Resisting the deleterious impacts of automation will not be a matter of simply regulating or resisting the use of AI. Rejecting AI is untenable; this is not going to stop its development and use, nor does such a position reckon with the genealogy of the present moment and the long history of statistical reasoning in education governance that has brought us to our current position.

While this may seem somewhat fatalistic, we believe that we can develop a politics that is not premised on a dichotomous view of human and machine and that works with the uncertainty that is the departure point and destination of new data-driven technologies. While the instrumental, market rationalities underpinning education today will likely be reinforced by machines, it may also be possible that new rationalities and techniques might create other ways of thinking about the problems of education governance, disrupting long-standing problems and solutions in education.

We need a politics that is critical but not antitechnology, a politics that does not formulate the problem poorly by opposing human values, agency, and interest on the one hand, and technology on the other. We argue that a politics adequate to synthetic governance would not juxtapose human agency and technological determinism; rather, we would need to consider how to more consciously navigate this reconstitution. It will not always be possible to break open the black box of AI and digital platforms, because this assumes a particular form of separation between human and machine that is no longer tenable. Rather, we might ask: What kinds of worlds are being created by algorithms, and how will we respond to the types of new truths that are being created? What are the limits of rectification, of appeal and regulation? This perspective challenges some of the primary approaches to automation, and the technical and political solutions to issues of bias and black-boxing, that reflect a desire for a human in the loop as a corrective or safeguard.

We thus need to rethink political agency in synthetic governance. The epigraph from Edwards that opens this chapter suggests it is entirely likely that we have willingly been assimilated into new relations with technologies and that this process cannot be reversed. We could go further by suggesting that the assimilation Edwards describes would not have been particularly susceptible to our willing otherwise. This does not mean that politics is impossible, but perhaps not a politics of the deliberative variety. We think it vitally important that we develop a critical synthetic politics that responds not to fears that technology will get away from us (the singularity) so much as the politics of networks that become so diffuse as to resist meaningful intervention.

A synthetic politics begins from the premise that there is no outside of algorithmic decision-making and automated thinking. We must think with and through our imbrications with other modes of cognition as a kind of “co-learning” with automated systems.32 A particular rationality is needed— to be open to the co-adaptation of humans and machines by recognizing that machine learning is the latest iteration in a longer history of thought that has never been limited to the human. Education is a site where we can embrace synthetic thought with a carefully articulated view of the risks, rather than reacting against it or embracing it uncritically. Education is a site in which we can remain open to the uncertainties, risks, and possibilities of synthetic governance.

### Alt Fails—Crackdown

#### Extreme post-pandemic politics incites resistance that coopts the alt.

**Bratton 21** – Benjamin Bratton’s work spans Philosophy, Architecture, Computer Science and Geopolitics, He is Professor of Visual Arts at University of California, San Diego, Program Director of The Terraforming program at the Strelka Institute, and author of several books including “The Stack: On Software and Sovereignty.” “The Revenge of the Real - Politics for a Post-Pandemic World.” June 2021. AG

The rapid but awkward appearance of face masks in the West entails an even more radical confrontation with the limits of the subjective per se . It makes clear that regardless of one’s subjective ethical intention, good or bad, one remains a contagion vector just the same. As said, it doesn’t matter if one wishes to do good or harm, one’s biological proximity to others will cause good or harm regardless. Subjective intent is irrelevant.

A source of confusion for many is a shift in ethics from a position that calibrates subjective moral will to one that recognizes one’s self and body as an object in a cause-and-effect relationship with the world. It is often presumed that agency and subjectivity (if not also identity) are interchangeable, but the consequentialist ethics of being an object (less a subject) works differently. Outcomes are not a mirror of an internal mental state. They are not directly dependent on public demonstration, performance, and ritual to effect physical change. The implications for other biopolitical and ecopolitical conditions, such as combating climate change, are decisive.

The main misapprehension so common in the mask war—that risk can be privatized—is not unexpected if considered in the context of how social ethics is already predicated on moral subjectivity. As opposed to the epidemiological conception of society, this practice sees ethics as the individual calculus of risk, reward, and consequences. The naked-faced do not mean harm, one assumes, and may even imagine themselves as bearing the burden of risk for everyone. This confusion between subjective and objective ethics cuts both ways, in that someone with a positive moral subjective disposition may imagine that the absence of harm they bring by wearing a mask is somehow due to their personal intention of goodness. It is not. To be contagious is not to be a bad person, but it does mean that, irrespective of one’s wishes, one may cause objective harm to others. The harm that one person may bring to another person has nothing to do with the affective bond or antagonism they feel.

The revenge of the real arises in the ethical challenges posed by the realization that the virus is indifferent to the moral projections we might make upon it. A viable post-pandemic politics cannot be predicated solely on the calibration of subjective intention because subjective intention is not the only cause of the effects we wish to realize or prevent. This is a challenge to political philosophy as well, in that it demands the conceptualization of an ethics of being an object , not of being a subject, which is, obviously, difficult for everyone and insulting for many. That is in no small part because of how many people have been long subordinated into positions by which their social identity is erased or diluted by being made into a human object.

And yet, the private vocality of subjective determinism cannot hold. The extreme subjectivism that asks you to “be the change you wish to see in the world,” as if internal mental states cause the external world to come into being, is not the solution to neoliberalism; it is its pinnacle.

This shift to the objective has everything to do with the biopolitics of medical care and the relation between immediacy and abstraction. The body as a medical object is a real thing, flesh and blood and tears. Each of us, at different times, lives in a body as a medical object. When needed we assume this objectivity and receive care accordingly. When someone’s temperature is taken or they are intubated, or their internal organs are monitored by the puncturing of the skin and the externalization of their blood, which is then analyzed for telltale traces, the care is not based entirely on the testimony of symptoms of this one body, but rather on this particular body as exemplary of a larger abstraction of medical knowledge about all the bodies that exhibit a similar pattern of symptoms, and all the bodies through which the virus has passed. That abstraction, the transference between the particular patient and the generic human, is the stuff of both high-tech and high-touch expertise.

This also underscores the role of modeling abstraction in positive biopolitics more generally. The capacity to provide care to the singular body in front of you requires the moment in which it becomes any body , to which a model medical abstraction, based on years of pattern recognition, must be applied as care. This is an epistemological relation, not just an affective one. Through the medical professional, it is a model sensing and acting back upon the world recursively through careful expertise that would be impossible by sheer reckoning. The doctor may care deeply for their patient on an interpersonal level, but more likely they are able to care for them because they are able to see them as an object.

Taken seriously, the implications are profound. One’s sense of bioethics would extend then not only to the protection of personal privacy and the prevention of the violence of being treated like a mere object, but also to the deliberate and ethical self-objectification as a responsible participant in the model abstractions through which the care of others is realized. An overemphasis in bioethics on the sanctity of the sovereign individual, and the protection against over-intervention, over-sensing, and over-objectification, may obscure the ethical problems of under-intervention, under-sensing, and lack of access to medical care based on exclusive models of the whole and, consequently, limited access to intervention. Those in socio-economic positions that prevent them from receiving the medical care they need may be less concerned about the psychological insult of being treated like an object by medical abstraction than they are about the real personal danger of not being treated at all. For this reason, among many others, the broken sensor layer and the inability to cohere inclusive and equitable biopolitics is itself a form of collective violence.

When model abstractions built over years of expert care and collaborative honing become a matter of life and death, a more nuanced approach comes into focus, regarding both what is and isn’t invasive “surveillance,” and how a society should undertake sensing and modeling so that it can compose itself deliberately. The same can be said for climate models, which will demand a similar reckoning with a social “ethics” that is not based on coaxing enough subjective moral gestures to change planetary geochemistry but on more direct interventions in a composite condition.

To be sure, the ways that this post-pandemic politics complicates deep cultures of individualism, subjectivism, and experientialism now at the center of conception of the common good, will invite vociferous reaction and resistance. These habits and impulses reside at the core of Western social thought, so why would they be anything but stubborn? One assumes as well that this resistance will come not only from the obvious political right-wing cultures that have hitched themselves to sovereign power over biopower until the literal end of the world, but also, I am sorry to say, from philosophers to whom people have looked for guidance as to what the interrelations between biology, politics, and the body have been and should be.

Behold the fear in this voice, already introduced above: “At stake here is nothing other than the new and ‘normal’ biopolitical relation between citizens and the State. This relation no longer has to do with free and active participation in the public sphere, but instead concerns the routine inscription and registration of the most private and most incommunicable element of subjectivity, the biopolitical life of the body ” (emphasis mine). So wrote Italian philosopher Giorgio Agamben. Once more, the “biopolitical life of the body” is not incommunicable, nor the basis of a private subjectivity, as should be obvious to anyone with a rudimentary interest in modern biological knowledge, let alone epidemiology.

Perhaps we should have seen it coming, but what happened next was one of the most cataclysmic and grotesque self-owns in the history of philosophy.

### Impact Defense

#### Framing issue---we are physchologically predisposed against emerging tech.

**Thierer 14** - senior research fellow at the Mercatus Center at George Mason University. “Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom.” Semantic Scholar. Mar 14. <https://www.semanticscholar.org/paper/Permissionless-Innovation%3A-The-Continuing-Case-for-Thierer/1744da518f1fbde038c22e04b42840019fc23bb8>, AG

C: WHY DOES DOOMSAYING DOMINATE DISCUSSIONS ABOUT NEW TECHNOLOGIES?

One of the reasons that precautionary thinking often creeps into technology policy discussions is that, as already noted, our collective first reaction to new technologies often is one of dystopian dread. We assume the worst for a variety of reasons.25 In the extreme, the initial resistance to new technologies sometimes takes the form of a full-blown technopanic, which refers to “intense public, political, and academic responses to the emergence or use of media or technologies, especially by the young.”26 Some new technologies were initially resisted and even regulated because they disrupted long-standing social norms, traditions, and institutions.

What drives this fear and the resulting panics?

There are many explanations for why we see and hear so much fear and loathing in information technology policy debates today, and even some occasional technopanics.27There exist many general psychological explanations for why human beings are predisposed toward pessimism and are risk-averse to new technologies and technological developments.28 For a variety of reasons, humans are poor judges of risks to themselves or those close to them. Harvard University psychology professor Steven Pinker, author of The Blank Slate: The Modern Denial of Human Nature, notes:

The mind is more comfortable in reckoning probabilities in terms of the relative frequency of remembered or imagined events. That can make recent and memorable events—a plane crash, a shark attack, an anthrax infection—loom larger in one’s worry list than more frequent and boring events, such as the car crashes and ladder falls that get printed beneath the fold on page B14. And it can lead risk experts to speak one language and ordinary people to hear another.

29 Clive Thompson, a contributor to Wired and the New York Times Magazine, also notes that “dystopian predictions are easy to generate” and “doomsaying is emotionally self-protective: if you complain that today’s technology is wrecking the culture, you can tell yourself you’re a gimlet-eyed critic who isn’t hoodwinked by high-tech trends and silly, popular activities like social networking. You seem like someone who has a richer deeper appreciation for the past and who stands above the triviality of today’s life.”

30 Beyond these root-cause explanations, there are many other specific factors that contribute to the rise of technopanics and lead us to fear new technological developments. Importantly, however, each of these particular explanations builds on previous insight: Survival instincts combined with poor comparative risk-analysis skills lead many people to engage in, or buy into, technopanics.

• Generational differences: Generational differences often motivate pessimistic attitudes about the impact of technology on culture and society. Parents and policymakers who dread the changes to cultural or privacy-related norms ushered in by new technologies often forget they, too, were children once and heard similar complaints from their elders about the gadgets and content of their generation. Yet these cycles of “juvenoia”—or “exaggerated anxiety about the influence of social change on children and youth”—repeat endlessly and drive panics from one generation to the next.31

• Hypernostalgia: As already noted, many stasis-minded critics just can’t seem to let go of the past. They are too invested in it or wedded to something about it. They engage in forms of hypernostalgia and ask us to imagine there existed some earlier time that was more exceptional and valuable than the unfolding present or unpredictable future.32 Such critics are guilty of both “rosy retrospection bias,” or “the tendency to remember past events as being more positive than they actually were,”33 and a general “pessimistic bias,” or “a tendency to overestimate the severity of economic problems and underestimate the (recent) past, present, and future performance of the economy.”34 These critics fear how technological change challenges the old order, traditional values, settled norms, traditional business models, and existing institutions—even as the standard of living generally improves with each passing generation. We see this at work, for example, in debates about privacy when critics yearn for the supposed solitude of the past, or in copyright debates when critics bemoan the loss of record stores and traditional methods of experiencing music.

• Bad news sells: Many media outlets and sensationalist authors sometimes use fear-based tactics to gain influence or sell books. Fearmongering and prophecies of doom are always effective media tactics; alarmism helps media outlets break through all the noise and get heard. This is particularly true as it relates to kids and online safety, where hypothetical threats to children have often dominated media coverage.

• The role of special interests: Many groups and institutions exaggerate fears and agitate for action because they benefit from it either directly by getting more resources from government, the public, or other benefactors, or indirectly from the glow of publicity that their alarmism generates. Many companies also overhype various online concerns and then also overplay the benefits of their particular tool as a silver-bullet solution to online pornography, privacy, or cybersecurity concerns. Again, bad news sells—and, in this case, it sells products and services to fearful citizens.

• Elitist attitudes: Academic skeptics and cultural critics often possess elitist attitudes about the technologies, platforms, or new types of media content that the masses or youth adopt before they do. These elitist views are often premised on the juvenoia and hypernostalgic thinking described above. Some researchers also have an incentive to perpetuate fear because alarmist research grabs attention and attracts more funding.

• “Third-person-effect hypothesis”: When some people encounter perspectives or preferences at odds with their own, they are more likely to be concerned about the impact of those things on others throughout society and to call on government to “do something” to correct or counter those perspectives or preferences. Psychologists refer to this as the “third-person effect hypothesis,” and it explains many technopanics and resulting calls for government intervention, especially as they relate to media policy and free speech issues.35

Most technopanics blow over in time, but they can do real harm in the short term. Technopanics can encourage policymakers to adopt far-reaching controls on information flows and innovation opportunities more generally.

Worse yet, continuously elevated states of fear or panic can lead to dangerous tensions throughout society. For example, the past decade witnessed a “stranger danger” panic about hypothetical online bogeymen, leading to overblown suspicions about sexual predators online and even the general presence of males near children.46 Similarly, excessive panic over cybersecurity matters can lead to paranoia about the potential danger of visiting certain websites or using certain digital tools that are, generally speaking, safe and beneficial to the masses.47

The final reason that these fear tactics are dangerous is that they lead to a “risk mismatch.” That is, fear-based tactics and inflated threat scenarios can lead to situations where individuals and society ignore quite serious risks because they are overshadowed by unnecessary panics over nonproblems.

### Tech Good—AI

#### AI key to save millions each year – medical tech.

Bornet ’21 Bornet is Chief Data Officer at Aera Technology and a board member at the Intelligent Automation Council. He is a contributor and senior advisor at The Institute for Robotic Process Automation & Artificial Intelligence (IRPA AI). (Pascal Bornet, "Council Post: Saving Millions Of Lives Per Year With Intelligent Automation", Forbes, 5-13-2021, https://www.forbes.com/sites/forbestechcouncil/2021/05/13/saving-millions-of-lives-per-year-with-intelligent-automation/?sh=352cbe4d1349. Accessed 7-4-2022, RS).

Intelligent Automation (IA) is more than a way to revolutionize business and save money — it also has the potential to save lives by the millions and increase healthy life expectancy. Intelligent automation can be applied to medical diagnosis and research to prevent unnecessary deaths. In addition, it provides more equitable access to healthcare worldwide. It also can be used in transport to augment the abilities of human drivers, preventing deaths and injuries from traffic accidents.

Preventing Deaths Through Diagnosis And Research

So many deaths worldwide are caused by chronic non-communicable diseases such as cardiovascular disease, cancer, diabetes and respiratory illnesses.

An important characteristic of these diseases is that recovery rates are higher the earlier the disease is detected. Leveraging machine learning (ML), IA can save lives by analyzing scans and other medical data such as blood pressure to produce quick and reliable diagnoses. Unsurprisingly, ML can process lung or breast scans in minutes or seconds where a human would take hours, but what’s more remarkable is that it has advantages over doctors when it comes to identifying cancer.

Another common factor among these diseases is the potential to find cures through research. Not only does ML help innovation in medical research (e.g., by simulating the combination of molecules), but it also plays a vital role by automating the documentation and checking of clinical trials, freeing up human researchers for higher-level cognitive tasks and making the research process quicker and more efficient.

Preventing Deaths Caused By Medical Errors

Medical errors are a sad and often overlooked element of modern healthcare. In the U.S., they cause over 250,000 deaths per year, which is higher than any other single factor except heart disease and cancer.

In 2006, Emily Jerry, a two-year-old recovering from cancer, tragically died after a pharmacy technician gave her 20 times the recommended concentration of intravenous saline solution. Emily’s father wrote, “Medical-care workers are dedicated, caring people, but they are human. And human beings make mistakes.”

IA, in conjunction with human professionals, can double-check prescriptions and identify discrepancies from doctors’ instructions or medical best practices. It is never tired nor distracted, so it is not vulnerable to lapses in concentration, which happen to everyone but can have disastrous consequences in healthcare.

IA can also monitor patients’ health in real-time. It can alert a nurse or doctor about an emergency based on a patient’s blood pressure, heart rate or other vital signs. It can even detect patterns that predict heart attacks, strokes or sepsis in advance, saving lives and freeing up doctors’ and nurses’ time from data collection.

Reducing Deaths From Preventable Causes In Developing Countries

The global disparity in wealth and resources means that many people in the developing world die of diseases that would be easily preventable in wealthier countries. This is largely due to inadequate access to healthcare. According to the WHO, there is a global shortage of 4.3 million healthcare professionals.

IA technology brings healthcare to anyone with access to a smartphone — which is an increasing proportion of people, even in regions that lack other infrastructure and technology. Applications can link patients with doctors remotely, while diagnostic tools can partially take the place of the doctor by diagnosing skin conditions, burns and chronic wounds based on a digital photo.

Medical care often requires physical supplies such as vaccines or donated blood, which cannot be delivered digitally. To provide these life-saving supplies to remote locations without adequate road infrastructure, Zipline International uses innovative, intelligent drones that can deliver supplies.

Reducing Deaths From Traffic Accidents

Road incidents can be deadly and can cause permanent disabilities. Human error is a factor in most road accidents, and there is potential for self-driving cars or IA-assisted driving technology to save lives by reducing or eliminating this factor. Research from the U.S. Department of Transport estimates 94% of traffic accidents are caused by human error.

Even before fully autonomous self-driving cars become the norm, IA can assist human drivers and help them to drive more safely. Cars can already be augmented with kits that allow them to monitor the driver using an internal camera, detecting when they become drowsy and alerting them. Automatic sensors can also be used to augment the human driver’s vision, warning them of unexpected obstacles. Cruise control and assisted parking are further examples of IA technology working together with human drivers to help them drive more safely.

Conclusion

Health organizations that want to start embracing the benefits of IA should start with the most common use cases in their industry: new patient onboarding and appointment scheduling with the support of automated workflows and cognitive agents, patient health monitoring leveraging cameras and sensors in hospital rooms, medical diagnosis and drug discovery supported by machine learning, staffing level prediction and real-time adjustment processes, automation of invoicing and claims management and patient experience improvement through real-time and 24/7 communication. If you start with these smaller, everyday processes then build forward from there, you will be able to embrace IA in ways that make your routines and processes easier from the beginning.

Overall, based on my research and expertise, I believe IA technologies could reduce early deaths by 10–30%. Back in 2017, a 20% reduction in the 56 million total annual deaths worldwide would have meant saving 14 million lives every year — the equivalent of the populations of Switzerland and Singapore.

### Tech Good—Peace

#### Tech creates peace along multiple vectors.

Fatima ’18 Quratulain Fatima is the Project Lead of the Agency for Barani Areas Development, with a focus on gender inclusive development and conflict prevention, and she was the first woman to join the Pakistan Air Force. She is a 2018 Aspen New Voices Fellow, a BuildPeace Fellow 2017-18 and Oxford Global Leadership Initiative Fellow 2016. (Quratulain Fatima, "Peace technology: A promising tool against wars at reduced price", news.trust.org, 3-23-2018, https://news.trust.org/item/20180323160358-p5wkq/. Accessed 7-4-2022, RS).

From apps to help citizens avoid missiles and land mines to rumor tracking mobile-based services using SMS, peace technology is one promising tool to prevent conflict

It has been seven years since I left Pakistan's Air Force, where I was part of the war against terrorism. I left hoping our conflicts would end soon, but nothing has changed. A World Bank-UN study "Pathways for Peace" has found that in 2016 alone, more countries experienced conflict than at any time in past 30 years. According to the same study, the economic cost of responding to conflict for 2012 was US $9.46 trillion which is 2.4 times the total GDP of Africa. Whereas, targeting resources toward countries at high risk of conflict each year could result in average net savings of $33 billion per year from avoided conflicts for the international community. But instead of saving more, we are spending more - and more people are dying.

With conflict resolution and rebuilding costs increasing at an alarming rate in prolonged conflicts like Afghanistan, Syria and Iraq, many experts say that the focus of the international community needs to shift from conflict resolution to conflict prevention. It is high time that, in addition to existing peace-building tools, we explore new, effective and cheap tools of conflict prevention.

Today in a second career where I am building water infrastructures for poor farmers, I find I am able to try to prevent conflicts that I was responding to in the Air Force. I have experienced that investment in conflict prevention tools reduce military spending and free tax money for education, health and other priorities. One such tool is the use of information and communication technology for conflict prevention. This technology is most commonly known by the collective name of peace technology or "PeaceTech." PeaceTech includes, but is not limited to, the use of mobile phones, digital applications, geographical information systems, social media and even digital games for achieving peace.

Even in relatively poor countries, technology is already an integral part of life that does everything from bringing news and entertainment to saving lives. Everyone tweeting can now become a voice, and thus a stakeholder, in a conflict. So why not use the technology as an effective and low-cost peace tool?

In Pakistan, I work on a project where we map geographical features on the earth surface, called a Geographical Information System (GIS). This was initially developed to design water dams and ponds in arid areas, but has been successfully put to use to prevent and resolve communal water disputes among farming communities at zero cost. Using this tool, the locations and conflict intensity can be geographically pinpointed on maps. These maps are then analyzed to assess what interventions are needed to stop conflict from breaking out. The GIS system also acts as an early warning network for conflict and a database of resolutions.

While still in its early stages, we hope this project will help stop violence before it starts, helping government officials and non-governmental organizations to use geo-spatial data to support existing conflict prevention mechanisms like village elders and community organizations in the area.

GIS is only one of the many PeaceTech tools that are making prevention work around the world. The Una Hakika (which means "are you sure?" in Swahili) project in Kenya is a rumor tracking mobile-based service using SMS and a web and mobile-based platform (wikirumours) moderating misinformation and disinformation to track and counter violence-inciting rumours in Kenya's Tana Delta. An impact evaluation for Una Hakika shows that a number of 300 rumour investigations led to results benefiting an estimated 45,000 people over a period of a year.

Likewise, tech fans in Syria are creating apps to help citizens avoid missiles and land mines. These early warning systems received reports of ballistic missile launches, made calculations and sent early warnings through SMS and email to the publics to avoid attacks. Until now peace builders have been predominantly using traditional tools of prevention - diplomacy, mediation and consensus-building. These approaches have their limits, however, and what is often missing is outreach to the individuals in communities at risk of a violent conflict. Peace technology is one promising tool for making these connections. It can also be effectively used as a data collection tool to build a strong responsive database for organizations working on conflict prevention.

### Tech Inevitable

#### Tech’s inevitable, cat’s out of the bag, regulation stops the worst abuses

**Mcintosh 10** – PhD in international studies from the University of Denver, Professor Emeritus of International Relations, Associate Professor of Political Science at Slippery Rock University. “The Transhuman Security Dilemma.” Journal of Evolution and Technology, Vol. 21 Issue 2. Dec 2010. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.187.1886&rep=rep1&type=pdf>, AG

Personal and political security are at risk from the potential for abuse of NBIC technologies by States and other organizations. Left in the control of elites, these technologies could be used to create dystopian societies to rival anything in science fiction. In fact, the entire notion of personhood could be at risk. If these technologies can be distributed and regulated for the good of the community, however, they hold the promise of making a far better world. The diversity of humanity could be recognized as a value to be protected, even as people learn to see beyond external forms to the humanity within. Yet even under the best regulatory regime, the pressures of competition and the desire of each individual to improve set up the potential for a dilemma that affects not merely the interaction and security of states, but the lives and liberty of each person. This is not a danger that can be edited out of the human genome, for it is inherent in the nature of competitive interaction, coupled with the expected comparative advantage of those who choose to take advantage of the new technologies. Here, then, is the conundrum: in our attempt to remake ourselves, we will not entirely leave our old selves behind, any more than we have escaped our animal past, and nor will we escape the pressures inherent in social and political systems. The balance of factors argues that change is coming. Evolution never ends, even when it is to some extent self-directed. Yet like so many other technologies, the tools of evolution-by-design will not solve the most basic problems of human or global security. There are things we cannot or will not leave behind. Trapped by the dilemmas inherent in security and economic competition, political and security issues will continue to challenge our descendants, no matter what forms or enhancements they possess.

### Transhumanism Good

#### We have passed the Rubicon of technology. Only transhumanism mitigates existential risk. Any alternative cedes inevitable self-annihilation.

**Verdoux 9** – Philippe Verdoux is a BA in philosophy from the University of Maryland, graduate student in the Department of Philosophy at Harvard University, has published papers in numerous academic journals, including the Journal of Future Studies, the Journal of Evolution and Technology, Techne: Research in Philosophy and Technology, and Erkenntnis, soon to be an Affiliate Scholar at the Institute for Ethics and Emerging Technologies. “Transhumanism, Progress and the Future”. Journal of Evolution and Technology. Vol. 20 Issue 2. Dec 2009. <https://jetpress.org/v20/verdoux.pdf>, AG

3. Rational capitulationism

An argument for the anti-progressionist version of transhumanism here advocated goes as follows:

Premise 1. The futurological program of transhumanism would by all accounts increase the likelihood of self-annihilation.

By now, the truth of this proposition should be obvious: the philosophy of transhumanism asserts both that (i) the advanced technologies of the GNR revolution will enable us to world-engineer and personengineer in radically new ways – possibly even enabling us to construct a novel species of technologized posthumans to take our place on the phylogenetic tree – and (ii) the “enhancement” technologies that promise to make the creation of posthumans possible ought to be pursued, albeit in a circumspect if “proactionary” manner (More 2005). As expounded in the futurological argument of Section 2, of all the technology kinds that humans have devised since the Oldowan industry (circa 2.6 mya), those of the GNR revolution are by far the riskiest: not only has the number of existential risks and probability of their actualization increased significantly in the past 50 years, but this trend may actually be exponential. In the worst case scenario, this exponential growth of existential risks would persist into the next couple centuries, thus precipitating an ERS. It is therefore by virtue of transhumanism’s imperative that we should foment and catalyze the further development of GNR technologies that its futurological program will increase the likelihood of self-annihilation. Nonetheless, it is crucial to note that…

Premise 2. The alternative futurological programs proposed would almost certainly increase the likelihood of self-annihilation more than transhumanism would.

There are myriad reasons for accepting this claim. One line of argumentation suggests that humanity has (so to speak) crossed the Rubicon of technological development: there is no turning back now, at least not without further exacerbating our existential plight or significantly increasing human suffering.31 Consider the option of broadly relinquishing (say) genetic engineering, due to the profound risks associated with its dual use properties. How might this be accomplished? As Walker writes in a 2009 article:

Relinquishment requires us to not only stop future developments but also to turn back the hands of time, technologically speaking. If we want to keep ourselves completely immune from the potential negative effects of genetic engineering we would have to destroy all the tools and knowledge of genetic engineering. It is hard to imagine how this might be done. […] Think of the alcohol prohibition experiment in the early part of the century in the U.S. Part of the reason that prohibition was unsuccessful was because the knowledge and rudimentary equipment necessary for brewing was ubiquitous. It is these two features, availability of knowledge and equipment, that has made biohacking possible. And where would a relinquishment policy be implemented? If it is truly a viable and long-term strategy then relinquishment will have to be adopted globally. Naturally very few countries with advanced genetic technologies are going to be enthusiastic about genetically disarming unless they have some pretty good assurances that all other countries will also genetically disarm. This leads us to the usual disarmament impasse. (Walker 2009.)

Indeed, just as a community of computer hackers emerged in the second half of the twentieth century, so too has a group of biohackers – or “hobbyists who experiment with DNA and other aspects of genetics” – recently emerged (see Ayres 2008). Thus, a central concern with broad relinquishment is that imposing moratoria on an entire domain of emerging technology would only drive experimentation “underground,” given that the two necessary conditions of knowledge and equipment are satisfied (which they are).32 This goes not just for genetic engineering but nanotechnology as well: relinquishing this field of research would likely result in the creation of a community of nanohackers – or hobbyists who experiment with the technological manipulation of matter on the nano-scale. And who would argue that a biohacker, or nanohacker, or any other amateur tinkering with unprecedentedly powerful GNR technologies would pose less of a risk than professional scientists working in the controlled environment of the laboratory?

In contrast, the steady-as-she-goes option relinquishes not any particular field of technological research but rather the use of GNR technologies to modify the human organism. This position is exemplified by the bioconservative Francis Fukuyama (2002), who argues that political liberalism is predicated on the existence of a common metaphysical essence shared by all humans, since it is in virtue of this essence that we humans are moral beings with an “inherent value” (and therefore deserving of equal rights). Thus, by modifying this essence with person-engineering technologies, the transhumanist project would extract a necessary ingredient from political liberalism’s moral recipe. It follows that only world-engineering technologies ought to be pursued. But again, we are left with the crucial question: How might one enforce such a restriction? Wouldn’t any attempt to prevent person-engineering just drive experimentation underground? And might these underground person-engineers actually emerge as superior to us “normals” in some important respect? Kurzweil, in fact, gestures at the plausibility of the latter scenario in a mock dialogue with Ned Ludd, who expresses (like Fukuyama) a strong aversion to any technological modification of the human organism. Kurzweil rejoins to Ludd’s anti-technology protestations: “If you’re speaking for yourself, that’s fine with me. But if you stay biological and don’t reprogram your genes, you won’t be around for very long to influence the debate” (Kurzweil 2005, 226; emphasis in original).

Furthermore, Walker points out that Fukuyama “says nothing about how we are to address the dual-use problem: the development of 21st century technologies for peaceful purposes necessarily bring with them the prospect that the same technology can be used for civilization ending purposes” (Walker 2009). It is indeed a nontrivial lacuna in Fukuyama’s vision for the future that he fails to provide any implementable strategies for controlling and mitigating the existential risks associated with world-engineering technologies – the very same artifactual products of the GNR revolution that would be used for personengineering purposes. In sum, then, the broad relinquishment and steady-as-she-goes options both pose serious logistical problems, the most worrisome of which (in my mind) pertains to the possibility of engendering a community of clandestine experimentalists driven “underground” as a result of moratoria imposed on one or more kinds of technological research.

Before concluding this subsection, though, it is worth taking a brief look at why the anarcho-primitivist option of comprehensive relinquishment also fails.33 To begin, recall the problems with Kurzweil’s arguments against primitivism: all those given involve fallacious mischaracterizations of the position or inaccurate portrayals of our “primitive” ancestors according the specious “Hobbesian ideology” (see Zerzan 1998, 258). Nonetheless, there are a number of cogent and compelling reasons for rejecting the proposition that an anarcho-primitivist revolution ought to be pursued: for one, recreating the mode of life had by our Pleistocene forebears would entail a massive, albeit transitory, increase in human suffering. As Ellul (a major intellectual source for Kaczynski) notes, “arrest and retreat only occur when an entire society collapses” (Ellul 1964, 89). Indeed, given the world population today, which far exceeds what could be supported by hunting, gathering, and fishing (especially after the many deleterious alterations of the environment brought about by human activity – see the “Holocene extinction event”), a primitivist revolution would entail realizing at once all the Malthusian catastrophes that technology has obviated over the centuries, such as that avoided by the Green Revolution (which of course introduced a myriad of new and more serious anthropogenic problems). While one could, and Kaczynski in fact does, argue along utilitarian lines that the suffering caused by transitioning to a long lost modus vivendi – the “primitivist singularity” – would ultimately be less than that resulting from the GNR revolution, the thought of effectuating such suffering via an overthrow of industrial capitalism and its heteronomous megatechnics is for most thinkers (present company included) too morally repugnant. We may thus eliminate the anarcho-primitivist position as a viable alternative plan for the future.

And with these negative appraisals we come to our…

Conclusion. The futurological program of transhumanism ought to be implemented rather than the alternative options available, that is, if one wishes to maximally minimize the inevitable increase in the probability of self-annihilation.

There are, I have attempted to show, dire eschatological consequences to all the possible routes into the future thus far proposed: no matter which is ultimately implemented, our chances of survival have fallen nontrivially. And, as I have also attempted to establish, technology constitutes a crucial enabling factor in the network of causes responsible for our existential plight. But what are the practical implications of this thesis with respect to transhumanism? If absolute progress driven by technology is illusory and our future dismal, then why not jettison – so to speak – technology from the ship of humanity’s future?

My line of reasoning to the conclusion above follows a simple process of elimination: transhumanism offers (what one might call) the safest unsafe passage into the future, that is, compared to the alternatives specified. But not only does the transhumanist program appear to constitute the best option for the future by avoiding the problems associated with certain forms of relinquishment, but it might actually contribute positively – in ways the alternatives could not – to the amelioration of our predicament. I refer here specifically to the creation and use of cognitive enhancement technologies, including neural implants, tissue grafts and nootropic drugs (Walker 2008b; Bostrom and Sandberg 2006; Bostrom and Sandberg 2009). After all, who better to grasp, manipulate and control the problems unique to the GNR revolution than an advanced “species” of cognitively enhanced posthumans?34 Indeed, as many authors have noted, the rapid expansion of human knowledge in the past several centuries has entailed a corresponding increase in individual ignorance (Winner 1977, 283; see also Kelly 2008). No doubt, a major obstacle to effectively guarding against the worse possible scenarios considered by Bostrom (2002) is epistemic or cognitive in nature. It thus follows that enhancing our ability to think carefully, comprehensively and deeply about the (impending) problems confronting intelligent life on Earth will greatly augment our collective ability to survive. Person-engineering must not be wholly restricted.

The general view defended here is, I believe, already implicit in certain corners of the transhumanist literature: one finds in several authors a recognition of the technogenicity of our worsening situation as well as a sense that the best way to fix this situation – now that we have crossed the Rubicon of technology – is more technology, designed and implemented in a strategically prudent manner.35 Walker, for example, argues that “even though creating posthumans may be a very dangerous social experiment, it is even more dangerous not to attempt it: technological advances mean that there is a high probability that a human-only future will end in extinction” (Walker 2009). And as I have already discussed, Bostrom has not only recently suggested that transhumanists eschew the term “progress”, but he continues to be a major intellectual figure in the exploding field of techno-eschatology.

In closing, a primary impetus behind this paper was to make the position that I have termed rational capitulationism explicit. This involved refining and elaborating Walker’s incipient arguments put forth in his 2009 article. In pursuing this end, I have attempted to emphasize that one can be a pessimist about the future, one can identify technology as the primary cause of our existential plight, and one can hold an anti-progressionist conception of history while at the same time advocating the descriptive and normative claims of transhumanism – in particular, the moral assertion that we ought to pursue both worldengineering and person-engineering technologies by fomenting the GNR revolution. This is, it appears, our best hope of surviving the future.

#### Transhumanism is the inevitable essence of human evolutionary progress.

**Lilley 12** - Professor of Sociology at Sacred Heart University, Fairfield Connecticut, PhD and MA, University of Massachusetts, Amherst; BA, College of the Holy Cross) teaches and conducts research on society and technology. “Transhumanism and Society: The Social Debate over Human Enhancement.” Springer. July 2012. <https://link.springer.com/content/pdf/10.1007/978-94-007-4981-8.pdf>, AG

Strong Claims of Inevitability

Whereas the conservationists often take the offensive in the rhetoric of risk, the transhumanists clearly are the aggressors in this contest. First, the transhumanists convey a sense of inevitability through their sweeping account of technological innovation. This is most effective when describing human history in terms of successive waves of beneficial technologies used to alter, control, or bypass nature, for example, fire-building, agriculture, vitamins, and vaccines. According to proponents, transtechnologies represent the next step in progress.

Second, outright inevitability claims are made. I’ll categorize such claims as ‘‘strong’’ when transhumanists declare an immutable process and ‘‘moderate’’ when they assert that social conditions are, and will continue to be, favorable but not necessarily causal for the development of transhumanity. I’ll start with the strong claims by identifying the immutable process and where is it located: (1) Evolution—it operates either in the broad expanse of the universe or, more specifically, life on earth. (2) Homo cyberneticus and the drive to self transform— it is deeply ingrained in human nature. (3) Technological momentum—exponential growth thought to be an internal dynamic of technologies. Transhumanists often depict these processes overlapping, however for the sake of clarity I will describe each in turn.

Evolution

In the most general sense, evolve means to develop over time. When used to describe change in organisms over generations the connotation of improvement often becomes pronounced (especially when our species is the subject). Charles Darwin preferred the phrase descent with modification rather than evolve because the former was neutral regarding adaptations. A modification might provide functional advantage to an organism but always in response to the demands of the environment at a particular point in time. Environments change too, and a subsequent modification is ‘‘judged’’ in relation to its time and place. As Stephen Jay Gould asserts, it is all about ‘‘local adaptation, not of general advance or progress.’’ (2007, p. 209)

It is often suggested that the concept of evolution dealt a blow to the conceit that, of all living beings, humans are unique and privileged. However, this depends on what version we accept. If we follow Gould’s approach it is hard not to be humbled. He argues that evolution is a messy affair: punctuated and not gradual, affected by cataclysms (e.g., asteroid strike), and very complex–competition or symbiosis playing out at many levels (genes, individual organisms, and collectives of organisms). Human evolution and human consciousness were not preordained: ‘‘Humans arose, rather, as a fortuitous and contingent outcome of thousands of linked events, any one of which could have occurred differently and sent history on an alternative pathway that would not have led to consciousness.’’ (211) By asserting that bacteria are the champions in terms of adaptability and long term success, he challenges the assumption that humans’ most highly regarded faculties make our species the best fit.

Gould’s take on human evolution is not shared by the general public. The common understanding is that humans are the most evolved species with regard to thinking, language, and sociality. For many it is a source of pride to think that nature selects for these capacities and our species has come out on top. Transhumanists tend to utilize this flattering interpretation but add the caveat that the selection process continues and that humans will not be the pinnacle of evolution. Kurzweil (2005) argues that intelligence provides a competitive advantage because ‘‘[i]ntelligence, if sufficiently advanced, is, well, smart enough to anticipate and overcome any obstacles that stand in its path.’’ (206) Modifications that increase computation power tend to be retained, and in the long run the trajectory is ever upward. Humans are on the high end of the continuum of smart species but we will evolve in synergy with our most advanced technology to become higher-order computation beings.

In his book, Mind Children, Moravec (1998a) predicts that robots with computation power superior to that of the human brain will eventually supersede humans. The transhumanists, in contrast, do not anticipate that humanity will remain idle. Young’s (2006) model of ‘‘harmonious complexification’’ (366) portrays life as moving toward increasing order, complexity, and self-organization and he sees humans as both producer and product of this process. Our species will initiate and ride the transhuman and posthuman wave. Kurzweil emphasizes the inevitability of this progression:

[W]e are a product of evolution, indeed its cutting edge. But extending our intelligence by reverse engineering it, modeling it, simulating it, reinstantiating it on more capable substrates, and modifying and extending it is the next step in evolution. It was the fate of bacteria to evolve into a technology-creating species. And it’s our destiny now to evolve into the vast intelligence of the Singularity (298).

Transhumanists also describe evolution as if it were a steamroller. Evolution is the driving force of life and it crushes species that fail to keep pace with change. Given evolutionary pressure, the human species must move forward as a matter of survival. Furthermore, humans must continually adapt to sociotechnological change or else risk being left behind. To avoid enslavement or extinction, humans must become transhuman to stay ahead of robots or AI entities in computation power.

Homo Cyberneticus

A superior motivational system is not based solely on avoidance of harm; inspiration and commitment to a creative project are important as well. The transhumanists understand this and make sure to balance the concern for being displaced by machines with the promise of self-transformation. Evolution may be harsh and unforgiving but, according to the transhumanists, evolution has produced one species, homo sapiens, that is equipped and prepared to direct it. We are ‘‘steersmen,’’ Homo cyberneticus, proclaims Simon Young. This is a bold declaration meant to inspire confidence and forward-thinking.

Clark (2003) explains that we are the creative project. In other words, because we are essentially dynamic and self-constructing and have the ability to expand with our technologies, we will continue to be the most innovative species.

Our self-image as a species should not be that of ancient biological minds in colorful young technological clothes. Instead, ours are chameleon minds, factory-primed to merge with what they find and with what they themselves create (141). Our cognitive machinery is now intrinsically geared to self-transformation, artifactbased expansion, and a snowballing/bootstrapping process of computational and representational growth… Plasticity and multiplicity are our true constants (8).

The transition to transhumanity is not only manageable but is expected of ‘‘natural-born cyborgs.’’

Technological Momentum

In a paper published in 1965, Gordon Moore, co-founder of Intel, described how the number of transistors per square inch on integrated circuits had doubled every year between 1959 and 1965. He suggested that the trend might continue indefinitely. Moore’s Law can be cautiously interpreted as a useful observation of past accomplishments or it can be understood as a predictor of future developments. Winner (1997) identifies a number of well-known writers including Nicolas Negroponte, George Gilder, Alvin Toffler, and Esther Dyson as expressing the latter view. Moravec (1998b) extends the trend line for MIPS (millions of instructions per second) into the future to make the case that increase in computation power will allow for the rise of super-intelligent robots: ‘‘At the present rate, computers suitable for humanlike robots will appear in the 2020s. Can the pace be sustained for another three decades? The graph shows no sign of abatement.’’ (6)

According to Kurzweil’s (2001) ‘‘law of accelerating returns,’’ the rate of technological change is greater than commonly understood because

technological change is exponential. In exponential growth, we find that a key measurement such as computational power is multiplied by a constant factor for each unit of time (e.g., doubling every year) rather than just being added to incrementally. Exponential growth is a feature of any evolutionary process, of which technology is a primary example. One can examine the data in different ways, on different time scales, and for a wide variety of technologies ranging from electronic to biological, and the acceleration of progress and growth applies. Indeed, we find not just simple exponential growth, but ‘‘double’’ exponential growth, meaning that the rate of exponential growth is itself growing exponentially. These observations do not rely merely on an assumption of the continuation of Moore’s law (i.e., the exponential shrinking of transistor sizes on an integrated circuit), but is based on a rich model of diverse technological processes.

In his most expansive projections he takes for granted that exponential growth will continue unabated and that ‘‘it will only take a quarter of a millennium (in our own case) to go from sending messages on horseback to saturating the matter and energy in our solar system with sublimely intelligent processes.’’ (Kurzweil 2007) Even the major social disturbances of the twentienth century have not delayed this progression: ‘‘But the evolution of intelligence here on Earth is actually going very well. All of the vagaries (and tragedies) of human history, such as two world wars, the cold war, the great depression, and other notable events, did not make even the slightest dent in the ongoing exponential progressions I previously mentioned.’’

It should be noted that Gordon Moore resists technological determinism, i.e., the view that technology is an autonomous force and proceeds according to internal dynamics. He believes that social forces are pivotal to microchip advances, specifically, a collective-fulfilling prophecy is at work in which projected trends become benchmarks for industry competition. Maybe it is a byproduct of his macro level of analysis, but Kurzweil’s law of accelerating returns does comes across as being deterministic. He insists that exponential growth will be sustained until it finally comes up against fundamental constraints of physics. Social constraints or, for that matter, social factors behind the construction and diffusion of technologies receive little attention.

Being more cautious, other transhumanists make use of the ceteris paribus clause, for instance, ‘‘if funding for research continues,’’ ‘‘as long as we dispel irrational fears,’’ etc. Even so, they cite the same exponential trends and make the same extrapolations as Kurzweil. Hughes (2004), for example, employs Moore’s Law as a template for growth rates in many fields and he predicts that

NBIC technologies [nanotechnology, biotechnology, information technology and cognitive science] will definitely also change how we work, how we travel, how we communicate, how we worship and how we cook. But the most fundamental changes in our lived experience will come from their impacts on our bodies and brains (7–8).

For Hughes it is not a question of whether technological advances will continue (they will), but how advances can be managed to best realize social values such as liberty and equality.

Technological acceleration, evolution, and Homo cyberneticus resound with the march of progress. This is a powerful theme in Western civilization that is now common to global culture. It is very difficult to deny or discredit. Critics may find it easier to dismiss the transhumanists’ assertion that it will turn out good in the end than to dispel the common belief that there is no stopping change.

#### Transhumanism is good

Walker 9 - is an assistant professor at New Mexico State University and holds the Richard L. Hedden Chair of Advanced Philosophical Studies. His current primary research interest is in ethical issues arising out of emerging technologies, e.g., genetic engineering, advanced pharmacology, artificial intelligence research and nanotechnology. “H+: Ship of Fools: Why Transhumanism is the Best Bet to Prevent the Extinction of Civilization”. Metanexus. Feb 5, 2009. <https://metanexus.net/h-ship-fools-why-transhumanism-best-bet-prevent-extinction-civilization/>, AG

Option: transhumanism future.

The transhumanist future is one where both world-engineering and person-engineering are permitted. Specifically, as noted, the transhumanist view is that we should create persons who are smarter and more virtuous than we are. The application to our problem is obvious: our fears about the misuse of 21st century technology reduce down to fears about stupidity or viciousness. Like the Australian research scientists, the worry is that we may be the authors of an accident, but this time one of apocalyptic proportions: the end of civilization. Likewise, our moral natures may also cause our demise. Or, to put a more positive spin on it, the best candidates amongst us to lead civilization through such perilous times are the brightest and most virtuous: posthumans.17

It is worth pointing out that there is no need to deny what Fukuyama claims: there are real dangers in creating posthumans. The problem with the transhumanist project, says Fukuyama, comes when we think seriously about what characteristics to change:

Our good characteristics are intimately connected to our bad ones: If we weren’t violent and aggressive, we wouldn’t be able to defend ourselves; if we didn’t have feelings of exclusivity, we wouldn’t be loyal to those close to us; if we never felt jealousy, we would never feel love. Even morality plays a critical function in allowing our species as a whole to survive and adapt…. Modifying any one of our key characteristics inevitably entails modifying a complex, interlinked package of traits, and we will never be able to anticipate the ultimate outcome.18

So, although Fukuyama sees the pull of transhumanism, how it might look “downright reasonable”, the fact that traits we might hope to modify are interconnected means that “we will never be able to anticipate the ultimate outcome.”

What Fukuyama fails to address in any systematic way is the fact that there are even greater dangers associated with not creating posthumans. So, a prudential and moral reason for creating posthumans is not that this is without risk, rather, it is less risky than the alternative here: steady-as-she-goes. If forced to put some hard numbers to these scenarios, I would venture to suggest there is a 90% chance of civilization surviving the next two centuries if we follow the transhumanist path, while I would put the chances of civilization surviving a steady-as-she-goes policy at less than 20%. But then, I am an optimist.

It might be objected that it is foolhardy or worse to try to put such numbers to futures where so much is uncertain. I have some sympathy with this objection. Thinking about the future where so much is uncertain is hardly analogous to putting odds on a horse race. On the other hand, a lot more is at stake in thinking about our future and so we have no choice but to try to estimate as best we can various risks. If it were protested that it is simply impossible to make any meaningful estimate then this would prove too much. For then there would be no reason to think that the transhumanist future is any more risky than any other future. In other words, the complaint that the transhumanist future is risky has traction only if we have some comparative evaluation in mind. Surgery that has only a 1 in 10 chance of survival is not risky, comparatively speaking, if the chances of survival without the surgery are zero. Anyone who criticizes transhumanism for putting civilization at risk, as does Fukuyama, must explicitly or implicitly hold that the chances of survival in a non-transhumanist future are greater. This is what transhumanists deny.

This line of thinking is further reinforced when we consider that there is a limit to the downside of creating posthumans, at least relatively speaking. That is, one of the traditional concerns about increasing knowledge is that it seems to always imply an associated risk for greater destructive capacity. One way this point is made is in terms of ‘killing capacity’: muskets are a more powerful technology than a bow and arrow, and tanks more powerful than muskets, and atomic bombs even more destructive than tanks. The knowledge that made possible these technical advancements brought a concomitant increase in capacity for evil. Interestingly, we have almost hit the wall in our capacity for evil: once you have civilization destroying weapons there is not much worse you can do. There is a point in which the one-upmanship for evil comes to an end—when everyone is dead. If you will forgive the somewhat graphic analogy, it hardly matters to Kennedy if his head is blown off with a rifle or a cannon. Likewise, if A has a weapon that can kill every last person there is little difference between that and B’s weapon which is twice as powerful.

Posthumans probably won’t have much more capacity for evil than we have, or are likely to have shortly. So, at least in terms of how many persons can be killed, posthumans will not outstrip us in this capacity. This is not to say that there are no new worries with the creation of posthumans, but the greatest evil, the destruction of civilization, is something which we now, or will soon, have. In other words, the most significant aspect that we should focus on with contemplating the creation of posthumans is their upside. They are not likely to distinguish themselves in their capacity for evil, since we have already pretty much hit the wall on that, but for their capacity for good.

### Thesis=Wrong

#### Tech doesn’t overdetermine the social. The potential for uncontrollable tech doesn’t mean tech controls us.

**Gulson et. al. 22** - Doctor of Philosophy, Professor at University of Sydney, current research investigates whether new knowledge, methods and technologies from life and computing sciences, with a specific focus on Artificial Intelligence, will substantively alter education policy and governance. “Algorithms of Education: How Datafication and Artificial Intelligence Shape Policy.” May 2022. AG

Automation, Technology, and Governance

Many critical perspectives of technology continue to center a human actor as either a participant, user, or object of technological decisionmaking.9 We would, perhaps a little unfairly to some, locate much of this work in the instrumentalist view, where technology is seen to be a tool serving human ends. Even approaches that treat AI and algorithms as sociotechnical assemblages can continue to treat these technologies as tools to be utilized, resisted, or ameliorated. This section provides an overview of theories of technology that move beyond the dichotomous view of humans and machines that, as noted above, tends to dominate current discussions of AI and algorithms in education governance. We turn to concepts that suggest “we can think, signify, make sense and represent who we are in part only because of technology.”10 We examine what this conceptualization means for understanding the links between technology, automation, and governance.

The view of human-technology relations that we take up is the “substantivist” position, according to which technology is a dynamic system that “is a decisive mediator of social actions and cultural values.”11 Stiegler, in a detailed theorization of “technics,” which he defines broadly to include the first Stone Age artifacts and the latest digital platforms, argues that technology and culture are irreducible.12 Roberts outlines that, for Stiegler, culture can be understood as

the product of technics as the prosthetic relationship between the human and its “exteriorisation” in matter. Technics therefore does not have the instrumental sense of technology as a tool that the human makes use of but rather defines the human as no longer simply a biological being.13

There is constant movement between two nonautonomous agents in the imbrication of humans and machines. As Mackenzie notes, “The technical runs ahead of culture, but it is not alone. It enlists humans to power its instantiation. . . . It is not autonomous or intrinsically dynamic.” Technology has collective implications; it shapes the social, cultural, andpolitical conditions of human life, but this does not imply technological determinism.14 As Roden argues, “While technology exerts a powerful influence on individuals, society and culture, this cannot be an ‘autonomous’ influence because there are not ends or purposes proper to it.”15

Stiegler’s emphasis on exteriorization provides a helpful way to theorize machines and governance, including exploring the emerging political rationalities of anticipation, prediction, and automation. For Stiegler, exteriorization describes the condensation of culture into “prosthetic” artifacts that augment human action (e.g., a hammer). An example of exteriorization is the significant shift from statistical governance to algorithmic governmentality, which results in “a certain type of (a)normative or (a)political rationality founded on the automated collection, aggregation and analysis of big data so as to model, anticipate and pre-emptively affect possible behaviours.”16

The combination of automation and behaviorist approaches allows us to begin to examine how governance is increasingly exteriorized as aspects of the cognitive processes involved in governance become condensed into machines.17 Increasingly, governance is operating through machines that are changing the organization of life, and thus “the critique of the evolution of artificial networks must concentrate on their emergent powers of cognitive, somatic and economic synchronization.”18 In other words, the so-called black boxes of AI, schools, classrooms, and even educational systems themselves inscribe autonomous interiorities to these objects. Thus, initiatives designed to produce “explainable AI,” for example, are attempts to expose the interiorities of AI, which for our purposes are the exact same logics, discourses, and rationalities that have governed classrooms, schools, and educational systems for the past forty years and that have been exteriorized into new platforms.19 In contrast, we will emphasize the synthetic relationship between the exteriorization of human culture and its folding back into human cognition through our engagement with machines.

Central to our theorization of synthetic thought is what Roden calls “new substantivism,” and self-augmenting technical systems. This perspective does not collapse automation into autonomy or suggest that self-augmenting technical systems are self-aware. Self-augmenting techniques, and specifically the forms of AI and automation upon which we focus, are those that are technically abstract, but the “techniques do not determine how they are used.”20 Examples include the wide applications of machine learning, from medicine to streaming services and online shopping platforms. Recommender systems that anticipate userpreferences are another example. While mostly used in business applications, these shape everything from what song is recommended next in a streaming service like Spotify to what problem should be undertaken in an adaptive math tutoring program. As Roden argues, “Techniques are more abstract the more they are available for reapplication or reconfiguration in disparate contexts.”21 We might suggest, therefore, that in education governance different applications will employ different algorithms, and there is an abstract isomorphic relationship between algorithmic approaches adopted across myriad contexts, from funding, resourcing and predictions of results.

With the increasingly widespread use of algorithms and AI, we suggest self-augmenting technical systems are beginning to reshape not only what is knowable but also what is doable. A system of this kind “does not remove human agency but mediates it through networks where no single agent or collective is able to exercise decisive control over the technical system.”22 These technical systems act as catalysts for further action rather than determining this action. Machines are thus creating semiautonomous conditions of existence, and in doing so they are creating new conditions of possibility for what we can understand as action and control in education governance. As Savat posits,

any technology, or machine, opens up a specific form of action, recognising that thought too is a form of action. At the same time, any technology or machine may close off certain forms of action (and thought).23

Much of the work on technology and governance indicates that control is difficult if not impossible to ascertain, because “the order of a network is total and open, horizontal and distributive, inclusive and universal.”24 Therefore, it may be that we need to come to grips with an idea of technology and governance that is neither controllable nor in control. As Roden suggests,

we need not attribute agency or purposiveness to technology to explain why the evolution of technical systems eludes our control. If technology is “out of control” it does not follow that it is “in control” of us or under its own control.25

If technology is neither in nor under control, then we need to grapple with the possibility that new types of governance systems exteriorize thought by automating certain cognitive processes. However, automation, if we follow Roden, does not mean rendering governance fully autonomous. Yet automation does reinforce digital data that become the basis of algorithmic governmentality and that can change the possibilities for political agency and governance. As noted by Crogan, Stiegler posits that “algorithmic governmentality disrupts established material and institutional arrangements for producing and verifying truth.”26 Through forms of automated decision-making, governance takes the individual and fragments it, instantiating a central insight of Deleuze’s theorization of societies of control, which involve the transformation of populations— which were the object of governance in disciplinary societies— into “samples, data, markets, banks” and individuals into “dividuals,” or “numbered bodies of coded ‘dividual’ matter to be controlled.”27

### AT: AI Impacts

#### No tech accidents, no algorithmic arms race.

Michael Shermer 17. Publisher of Skeptic magazine, a monthly columnist for Scientific American, and a Presidential Fellow at Chapman University. 04/2017. “Why Artificial Intelligence Is Not an Existential Threat.” Skeptic, vol. 22, no. 2, pp. 29–35.

Why AI is not an Existential Threat First, most AI doomsday prophecies are grounded in the false analogy between human nature and computer nature, or natural intelligence and artificial intelligence. We are thinking machines, but natural selection also designed into us emotions to shortcut the thinking process because natural intelligences are limited in speed and capacity by the number of neurons that can be crammed into a skull that has to pass through a pelvic opening at birth, whereas artificial intelligence need not be so restricted. We don't need to compute the caloric value of foods, for example, we just feel hungry. We don't need to calculate the waist-to-hip ratio of women or the shoulder-to-waist ratio of men in our quest for genetically healthy potential mates; we just feel attracted to someone and mate with them. We don't need to work out the genetic cost of raising someone else's offspring if our mate is unfaithful; we just feel jealous. We don't need to figure the damage of an unfair or non-reciprocal exchange with someone else; we just feel injustice and desire revenge. Emotions are proxies for getting us to act in ways that lead to an increase in reproductive success, particularly in response to threats faced by our Paleolithic ancestors. Anger leads us to strike out, fight back, and defend ourselves against danger. Fear causes us to pull back, retreat, and escape from risks. Disgust directs us to push out, eject, and expel that which is bad for us. Computing the odds of danger in any given situation takes too long. We need to react instantly. Emotions shortcut the information processing power needed by brains that would otherwise become bogged down with all the computations necessary for survival. Their purpose, in an ultimate causal sense, is to drive behaviors toward goals selected by evolution to enhance survival and reproduction. AIs -- even AGIs and ASIs -- will have no need of such emotions and so there would be no reason to program them in unless, say, terrorists chose to do so for their own evil purposes. But that's a human nature problem, not a computer nature issue. To believe that an ASI would be "evil" in any emotional sense is to assume a computer cognition that includes such psychological traits as acquisitiveness, competitiveness, vengeance, and bellicosity, which seem to be projections coming from the mostly male writers who concoct such dystopias, not features any programmer would bother including, assuming that it could even be done. What would it mean to program an emotion into a computer? When IBM's Deep Blue defeated chess master Garry Kasparov in 1997, did it feel triumphant, vengeful, or bellicose? Of course not. It wasn't even "aware" -- in the human sense of self-conscious knowledge -- that it was playing chess, much less feeling nervous about possibly losing to the reigning world champion (which it did in the first tournament played in 1996). In fact, toward the end of the first game of the second tournament, on the 44th move, Deep Blue made a legal but incomprehensible move of pushing its rook all the way to the last row of the opposition side. It accomplished nothing offensively or defensively, leading Kasparov to puzzle over it out of concern that he was missing something in the computer's strategy. It turned out to be an error in Deep Blue's programming that led to this fail-safe default move. It was a bug that Kasparov mistook as a feature, and as a result some chess experts contend it led him to be less confident in his strategizing and to second-guess his responses in the subsequent games. It even led him to suspect foul play and human intervention behind Deep Blue, and this paranoia ultimately cost him the tournamentt.[ 13] Computers don't get paranoid, the HAL 9000 computer in 2001 notwithstanding. Or consider Watson, the IBM computer built by David Ferrucci and his team of IBM research scientists tasked with designing an AI that could rival human champions at the game of Jeopardy! This was a far more formidable challenge than Deep Blue faced because of the prerequisite to understand language and the often multiple meanings of words, not to mention needing an encyclopedic knowledge of trivia (Watson had access to Wikipedia for this). After beating the all-time greatest Jeopardy! champions Ken Jennings and Brad Rutter in 2011, did Watson feel flushed with pride after its victory? Did Watson even know that it won Jeopardy!? I put the question to none other than Ferrucci himself at a dinner party in New York in conjunction with the 2011 Singularity Summit. His answer surprised me: "Yes, Watson knows it won Jeopardy!" I was skeptical. How could that be, since such self-awareness is not yet possible in computers? "Because I told it that it won," he replied with a wry smile. Sure, and you could even program Watson or Deep Blue to vocalize a Howard Dean-like victory scream when it wins, but that is still a far cry from a computer feeling triumphant. This brings to mind the "hard problem" of consciousness -- if we don't understand how this happens in humans, how could we program it into computers? As Steven Pinker elucidated in his answer to the 2015 Edge Question on what to think about machines that think, "AI dystopias project a parochial alpha-male psychology onto the concept of intelligence. They assume that superhumanly intelligent robots would develop goals like deposing their masters or taking over the world." It is equally possible, Pinker suggests, that "artificial intelligence will naturally develop along female lines: fully capable of solving problems, but with no desire to annihilate innocents or dominate the civilization."[ 14] So the fear that computers will become emotionally evil are unfounded, because without the suite of these evolved emotions it will never occur to AIs to take such actions against us. What about an ASI inadvertently causing our extinction by turning us into paperclips, or tiling the entire Earth's surface with solar panels? Such scenarios imply yet another emotion -- the feeling of valuing or wanting something. As the science writer Michael Chorost adroitly notes, when humans resist an AI from undertaking any form of global tiling, it "will have to be able to imagine counteractions and want to carry them out." Yet, "until an AI has feelings, it's going to be unable to want to do anything at all, let alone act counter to humanity's interests and fight off human resistance." Further, Chorost notes, "the minute an A.I. wants anything, it will live in a universe with rewards and punishments -- including punishments from us for behaving badly. In order to survive in a world dominated by humans, a nascent A.I. will have to develop a humanlike moral sense that certain things are right and others are wrong. By the time it's in a position to imagine tiling the Earth with solar panels, it'll know that it would be morally wrong to do so."[ 15] From here Chorost builds on an argument made by Peter Singer in The Expanding Circle (and Steven Pinker in The Better Angels of Our Nature[ 16] that I also developed in The Moral Arc[ 17] and Robert Wright explored in Nonzero[ 18]), and that is the propensity for natural intelligence to evolve moral emotions that include reciprocity, cooperativeness, and even altruism. Natural intelligences such as ours also includes the capacity to reason, and once you are on Singer's metaphor of the "escalator of reason" it can carry you upward to genuine morality and concerns about harming others. "Reasoning is inherently expansionist. It seeks universal application," Singer notes.[ 19] Chorost draws the implication: "AIs will have to step on the escalator of reason just like humans have, because they will need to bargain for goods in a human-dominated economy and they will face human resistance to bad behavior."[ 20] Finally, for an AI to get around this problem it would need to evolve emotions on its own, but the only way for this to happen in a world dominated by the natural intelligence called humans would be for us to allow it to happen, which we wouldn't because there's time enough to see it coming. Bostrom's "treacherous turn" will come with road signs ahead warning us that there's a sharp bend in the highway with enough time for us to grab the wheel. Incremental progress is what we see in most technologies, including and especially AI, which will continue to serve us in the manner we desire and need. Instead of Great Leap Forward or Giant Fall Backward, think Small Steps Upward. As I proposed in The Moral Arc, instead of Utopia or dystopia, think protopia, a term coined by the futurist Kevin Kelly, who described it in an Edge conversation this way: "I call myself a protopian, not a Utopian. I believe in progress in an incremental way where every year it's better than the year before but not by very much -- just a micro amount."[ 21] Almost all progress in science and technology, including computers and AI, is of a protopian nature. Rarely, if ever, do technologies lead to either Utopian or dystopian societies. Pinker agrees that there is plenty of time to plan for all conceivable contingencies and build safeguards into our AI systems. "They would not need any ponderous 'rules of robotics' or some newfangled moral philosophy to do this, just the same common sense that went into the design of food processors, table saws, space heaters, and automobiles." Sure, an ASI would be many orders of magnitude smarter than these machines, but Pinker reminds us of the AI hyperbole we've been fed for decades: "The worry that an AI system would be so clever at attaining one of the goals programmed into it (like commandeering energy) that it would run roughshod over the others (like human safety) assumes that AI will descend upon us faster than we can design fail-safe precautions. The reality is that progress in AI is hype-defyingly slow, and there will be plenty of time for feedback from incremental implementations, with humans wielding the screwdriver at every stage."[ 22] Former Google CEO Eric Schmidt agrees, responding to the fears expressed by Hawking and Musk this way: "Don't you think the humans would notice this, and start turning off the computers?" He also noted the irony in the fact that Musk has invested $1 billion into a company called OpenAI that is "promoting precisely AI of the kind we are describing."[ 23] Google's own DeepMind has developed the concept of an AI off-switch, playfully described as a "big red button" to be pushed in the event of an attempted AI takeover. "We have proposed a framework to allow a human operator to repeatedly safely interrupt a reinforcement learning agent while making sure the agent will not learn to prevent or induce these interruptions," write the authors Laurent Orseau from DeepMind and Stuart Armstrong from the Future of Humanity Institute, in a paper titled "Safely Interruptible Agents." They even suggest a precautionary scheduled shutdown every night at 2 AM for an hour so that both humans and AI are accustomed to the idea. "Safe interruptibility can be useful to take control of a robot that is misbehaving and may lead to irreversible consequences, or to take it out of a delicate situation, or even to temporarily use it to achieve a task it did not learn to perform or would not normally receive rewards for this."[ 24] As well, it is good to keep in mind that artificial intelligence is not the same as artificial consciousness. Thinking machines may not be sentient machines. Finally, Andrew Ng of Baidu responded to Elon Musk's ASI concerns by noting (in a jab at the entrepreneur's ambitions for colonizing the red planet) it would be "like worrying about overpopulation on Mars when we have not even set foot on the planet yet."[ 25] Both Utopian and dystopian visions of AI are based on a projection of the future quite unlike anything history has given us. Yet, even Ray Kurzweil's "law of accelerating returns," as remarkable as it has been has nevertheless advanced at a pace that has allowed for considerable ethical deliberation with appropriate checks and balances applied to various technologies along the way. With time, even if an unforeseen motive somehow began to emerge in an AI we would have the time to reprogram it before it got out of control. That is also the judgment of Alan Winfield, an engineering professor and co-author of the Principles of Robotics, a list of rules for regulating robots in the real world that goes far beyond Isaac Asimov's famous three laws of robotics (which were, in any case, designed to fail as plot devices for science fictional narratives).26 Winfield points out that all of these doomsday scenarios depend on a long sequence of big ifs to unroll sequentially: "If we succeed in building human equivalent AI and if that AI acquires a full understanding of how it works, and if it then succeeds in improving itself to produce super-intelligent AI, and if that super-AI, accidentally or maliciously, starts to consume resources, and if we fail to pull the plug, then, yes, we may well have a problem. The risk, while not impossible, is improbable."[ 27]

### AT: Degrowth-y Alts

#### The alt is naïve primitivism that is worse than what we have now.

**Bratton 21** – Benjamin Bratton’s work spans Philosophy, Architecture, Computer Science and Geopolitics, He is Professor of Visual Arts at University of California, San Diego, Program Director of The Terraforming program at the Strelka Institute, and author of several books including “The Stack: On Software and Sovereignty.” “The Revenge of the Real - Politics for a Post-Pandemic World.” June 2021. AG

There are certainly aesthetic and stylistic reasons to prefer homogenous village-scale communities to the “alienating” anonymity of the big city. Indeed, there is a direct if implicit anti-urbanism in anti-automation politics and aesthetics. Some may have forgotten that, despite their bucolic pleasures, small towns are also facial recognition–based social control systems from which many people have given their lives to escape.

For example, the petit bourgeois Primitivism of the all-organic neighborhood farmers market stands as a kind of wishful idealization of what infrastructure might be and “where things come from.” Although it provides an anodyne experience, its symbolism reeks of a Restorationist cultural politics that symptomatically prioritizes ambiance at hand over equity at scale. It is an aesthetic indulgence claiming to be an ethical politics that is claiming to be a more resilient economics. And yet, the world cannot actually “be like this always”; it is not possible for every piece of fruit to be handed to you in person.

One reason the positive biopolitics for which I advocate does not already exist is because of the persistent illusion that immediate participatory emergence is the righteous means and ends. For some who advise that mutual care efforts are not just tactical responses at the edge of the network but should be the whole of the network, the implied logical preference is for a less-systematic, decentralized, volunteerist rewilding of health care and of biopolitics more generally. To be sure, that would be a recipe for even worse disaster. Just ask Brazil.

### AT: Stack

#### Stacks are just layers of systems—they’re meaningless without the hard political work to ensure those systems function.

Scannell, 18—teaches sociology and women’s, gender, and sexuality studies at Hunter College (R. Joshua, “Architectures of Managerial Triumphalism (Review of Benjamin Bratton, The Stack: On Software and Sovereignty),” <https://www.boundary2.org/2018/11/r-joshua-scannell-architectures-of-managerial-triumphalism-review-of-benjamin-bratton-the-stack-on-software-and-sovereignty/>, dml)

Design, then, and not theory, because Bratton’s Stack is a speculative document. Given the bewildering and potentially apocalyptic conditions of the present, he wants to extrapolate outwards. What are the heterotopias-to-come? What are the constraints? What are the possibilities? Sounding a familiar frustration with the strictures of academic labor, he argues that this moment requires something more than diagnosis and critique. Rather,

the process by which sovereignty is made more plural becomes a matter of producing more than discoursing: more about pushing, pulling, clicking, eating, modeling, stacking, prototyping, subtracting, regulating, restoring, optimizing, leaving alone, splicing, gardening and evacuating than about reading, examining, insisting, rethinking, reminding, knowing full-well, enacting, finding problematic, and urging. (303)

No doubt. And, not that I don’t share the frustration, but I wonder what a highly technical, 500-page diagnosis of the contemporary state of software and sovereignty published and distributed by an academic press and written for an academic audience is if not discoursing? It seems unlikely that it can serve as a blueprint for any actually-existing power brokers, even though its insights are tremendous. At the risk of sounding cynical, calling The Stack a “design brief” seems like a preemptive move to liberate Bratton from having to seriously engage with the different critical traditions that work to make sense of the world as it is in order to demand something better. This allows for a certain amount of intellectual play that can sometimes feel exhilarating but can just as often read as a dodge—as a way of escaping the ethical and political stakes that inhere in critique.

That is an important elision for a text that is explicitly trying to imagine the geopolitics of the future. Bratton seems to pose The Stack from a nebulous “Left” position that is equally disdainful of the sort of “Folk Politics” that Srnicek and Williams (2015) so loathe and the accelerationist tinge of the Speculative Realists with whom he seems spiritually aligned. This sense of rootlessness sometimes works in Bratton’s favor. There are long stretches in which his cherry picking and remixing ideas from across a bewildering array of schools of thought yields real insights. But just as often, the “design brief” characterization seems to be a way out of thinking the implications of the conjuncture through to their conclusion. There is a breeziness about how Bratton poses futures-as-thought-experiments that is troubling.

For instance, in thinking through the potential impacts of the capacity to measure planetary processes in real time, Bratton suggests that producing a sensible world is not only a process of generalizing measurement and representation. He argues that

the sensibility of the world might be distributed or organized, made infrastructural, and activated to become part of how the landscape understands itself and narrates itself. It is not only a diagnostic image then; it is a tool for geo-politics in formation, emerging from the parametric multiplication and algorithmic conjugation of our surplus projections of worlds to come, perhaps in mimetic accordance with one explicit utopian conception or another, and perhaps not. Nevertheless, the decision between what is and is not governable may arise as much from what the model computational image cannot do as much as what it can. (301, emphasis added)

Reading this, I wanted to know: What explicit utopian project is he thinking about? What are the implications of it going one way and not another? Why mimetic? What does the last bit about what is and is not governable mean? Or, more to the point: who and what is going to get killed if it goes one way and not another? There are a great many instances like this over the course of the book. At the precise moment where analysis might inform an understanding of where The Stack is taking us, Bratton bows out. He’s set down the stakes, and given a couple of ideas about what might happen. I guess that’s what a design brief is meant to do.

# Bronze Night Aff

### Notes

Evidence from the starter packet file and from the neg section in this file can both be useful for case extensions/answers to other off-case positions; I just didn’t want to be any more duplicative than necessary. I tried to largely keep stuff specific to the aff here.

I think this is a strategic K aff against framework and against K strats. In the latter context, you might want to defend more of the “governable” part of “governable stacks”—take a look at the “Governance Turn” card for more of an idea for that. Part of the “governable stacks” proposal certainly involves governance, but I think that it can be possible to walk a line of saying that the aff can say the state is not always irredeemably awful without having to defend USFG action in the plan—see more in the framework notes section.

I would recommend researching the (many, many) examples in the 1AC Schneider evidence!

### 1AC

#### “At the start of the twenty-first century, we are faced with the increasing dependence of our life support systems on global networks and the possibility of system-wide catastrophe. From energy supplies to agriculture to the global climate, these systems are now directly exposed to… the possibility that a local breakdown could spread globally. We seem to be learning repeatedly that the unavoidable dark side of our networks of… information is the ever-present threat of contagion and cascading system failure.”

#### It’s funny, then, that debaters hail plan-focused debates as the best way to “learn repeatedly” on this topic when they have repeatedly failed to learn this fact. US-NATO cybersecurity cooperation is embedded within a vast network of information architectures that the alliance has become fully dependent on. We cannot hope to debate about that network through the unfathomably limited model of policy scenario comparison, for cyberwar’s essence is that it is a war against knowledge itself.

#### Thus, when exploring how we can debate it, “we must resist deciding in favor of catastrophe or boredom, for in doing so, the entirety of cyberwar will certainly escape us. Instead, we must attempt to interrogate the history and discourses of cyberwar… as it hides in the theoretical space between war and nonwar.”

--green highlighting was already read in the tag and doesn’t need to be read twice!

Joque, 18—PhD from the European Grad School, researches philosophy, technology and media and is the visualization librarian at the University of Michigan, go blue (Justin, “Root Kit,” *Deconstruction Machines: Writing in the Age of Cyberwar*, Introduction, 1-8, dml)

At the start of the twenty-first century, we are faced with the increasing dependence of our life support systems on global networks and the possibility of system-wide catastrophe. From energy supplies to agriculture to the global climate, these systems are now directly exposed to global fluctuations and, with them, the possibility that a local breakdown could spread globally. We seem to be learning repeatedly that the unavoidable dark side of our networks of communication, production, finance, and information is the ever-present threat of contagion and cascading system failure.

Nowhere is the logic of this threat of global system breakdown clearer than in the expanding discourse around cyberwar. Over the past decades, a growing chorus of politicians, military strategists, computer security experts, and journalists has cited the dangers and opportunities that the subversion of digital systems provides for future conflicts. Governments are investing increasing amounts of energy and money in guaranteeing that they can attack, subvert, and monitor opponents’ digital networks, from command-and-control systems to banking to electric grids. The early outbreaks of cyberwar, such as a series of Russian attacks on Estonia in 2007, have resulted mainly in temporary inconveniences, but as militaries invest in being able to destroy physical infrastructure through networked attacks and governments attempt to subvert other states, future cyberwars threaten the possibility of massive destruction and destabilization.

Cyberwar seizes directly on the networked nature of twenty-firstcentury economic, military, and communicative power by exploiting vulnerabilities, bugs, and insecurities in the code and systems that run these networks; the more well connected and technologically advanced one is, the more one has to fear the contagious threat of both networked accidents and attacks. The military investment in cyberwar and the political, media, and economic responses to acts of cyberwar speak directly to the complicated nature of our networks and information technologies. It is here, where these technical, programmatic, and social systems begin to break down and are transformed into sites of military intervention, that we can most fully begin to elucidate what is at stake in these global networks.

DEFINING CYBERWAR

There is no easily agreed-upon definition of cyberwar. Even within closely related literatures, there exists an ongoing debate over what constitutes cyberwar. Some, such as Rid, who has written at length declaring there is no such thing as cyberwar, question whether such a concept is a helpful lens for thinking the present situation at all.1 The term cyberwar, in most invocations, refers to the notion of cyberspace and the possibility of a war carried out in this global networked space, wherein computer systems are taken over to disrupt and surveil an enemy’s communication and networked infrastructure either as part of a “kinetic” war or as a form of low-level conflict aimed at gaining geopolitical advantages. Though it is important to follow authors, strategists, legal scholars, and others wherever they happen to see “cyberwar” occurring, one particular etymological meaning will guide this inquiry. The prefix cyber- refers to the term cybernetics. Cybernetics, originating from the Greek kubernētēs (“steersman” or “governor”), is the science and study of systems, their structures, regulation, emergent properties, and possibilities, spanning disciplines from technology to biology to society. By explicitly thinking the cyber- in cyberwar as referring to systems, it will be fruitful to understand cyberwar as a war against systems: computer systems, state systems, systems of organization, and even systems of meaning.

This etymological understanding of cyberwar closely mirrors some of the earliest deployments of this term. One of the first unclassified uses of the term cyberwar comes from a 1992 publication by Arnett.2 For him, the term means the replacement of human operators with machines that decide on targets, trajectories, movement, and so on—essentially the culmination of a long history of the insertion of “intelligent machines” into the arsenal of war fighting. That same year, Der Derian used the term “in the sense of a technologically generated, televisually linked, and strategically gamed form of violence.”3 Arquilla and Ronfeldt subsequently published a paper defining cyberwar as a tactical and strategic movement whereby communication, information, and the visibility of the battlespace become the central concern. They assert that while information technology brings cyberwar to the fore, it is not necessarily a technological phenomenon. In fact, the exemplary case of cyberwar they recount is a thirteenth-century Mongol offensive against Khwarizm, where the Mongols succeeded in defeating a significantly larger army by cutting off communications and disrupting the control of forces.

These definitions complement each other. Der Derian and Arnett’s definitions focus on carrying out a kinetic war through the cybernetic organization of humans and technology, while Arquilla and Ronfeldt’s definition stresses disrupting all of the enemy’s cybernetic systems regardless of whether they are human, technological, or a combination. We are faced, then, with something much more expansive than war in cyberspace; rather, what these authors begin to explore in the early 1990s is an understanding of war in which one tries to construct and defend systems of communicating, knowing, controlling, and, ultimately, existing. Simultaneously, one attempts to disrupt, infiltrate, corrupt, and destroy these same systems belonging to the enemy. Arquilla and Ronfeldt state that such a strategy “may aim to confound people’s fundamental beliefs about the nature of their culture, society, and government, partly to foment fear but perhaps mainly to disorient people and unhinge their perceptions.”4

Clearly this is not completely new. Belligerents have always attempted to deceive their opponents and disrupt economies and governments. Furthermore, war has often had as a central objective the destruction of one critical system and the infiltration of another: the body and the territory of the opponent. Despite this, we can outline three critical factors that mark cyberwar as a historical shift. First, proponents of cyberwar, such as Arquilla and Ronfeldt, stress that in cyberwar, information and structures of knowing become central rather than peripheral to conflict. They say that cyberwar “means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself.”5 Second, cyberwar attempts to disrupt not only the enemy’s knowledge but also the entire structure of knowledge. In short, cyberwar invests epistemology itself as a battlespace. Third, cyberwar seeps outside of “war” proper. In calling into question modes of knowing, cyberwar breaks down the limits of the time and space of war.

Thus the term cyberwar describes two distinct but related phenomena. On one hand, it is a strategy for fighting war, and we will include whatever is named cyberwar by strategists, legal theorists, authors, and warriors. On the other hand, we will mean a historical shift—in a sense, a global cyberwar that marks a tendency whereby the critical element in war becomes the flow of information and the fortification and disruption of systems. In making this shift, cyberwar has opened an epistemological and cybernetic battlespace wherein notions of war, enmity, and knowing become directly contestable. While these concepts have always been unstable and problematic, cyberwar seizes them as systems of direct military intervention, turning what was once a question for philosophers into a domain of the global battlespace. In its most abstract sense, cyberwar has become an event that calls everything including itself into question at the moment it arrives. It is the historical possibility that all systems may break down—or, in their military occupation, be caused to break down—but it is also possible that cyberwar may undermine itself before anything actually “happens.” Cyberwar as historical event marks a moment of radical militarized unknowability.

A COMPROMISED HISTORY

Many discussions of cyberwar, be they historical, strategic, or legal, begin not with the earliest examples or contemporary attacks but rather with a future catastrophe that demonstrates the danger of our overreliance on vast, connected, yet vulnerable systems. These catastrophes normally start with a nonstate actor or a “rogue” state hacking into key networks, destroying critical infrastructure in the United States or multiple European countries. Airplanes crash into each other, trains derail, communication channels shut down, and electrical systems are disabled. Not only are these systems forced to shut down but they are hijacked and made to spin out of control, sometimes destroying themselves so completely that they would take months to return to normal usage. These imagined scenarios often place the reader at the time immediately following the catastrophe. At this point in time, one can survey the wreckage of our technological hubris before the aftermath begins in earnest. It is the moment when the full scale of a possible collapse is revealed but not yet realized.6

Where a historical account begins in the past, it often starts with a CIA attempt to secretly destroy a Soviet gas pipeline.7 According to Thomas Reed, a National Security Council staffer, in 1982, the CIA was able to insert an intentionally faulty piece of code into a pump that the Soviet Union obtained from a Canadian company. According to Reed’s account, the pump was installed in the Trans-Siberian gas pipeline; varying pump speeds and valve settings produced extreme pressures that caused an explosion large enough to be detected by U.S. satellites. The secret introduction of a so-called logic bomb—a somewhat antiquated term for a malicious piece of code inserted into software—has been touted by a number of commentators as one of the earliest examples of cyberwar.

Although Reed, who made this story public for the first time in a 2004 book, never referred to this attack as cyberwar, this story has become something of an origin myth for those who write about cyberwar more generally.8 The event prefigures a number of issues that arise again and again in the myriad discourses surrounding cyberwar. Most important, it becomes clear how vulnerable complex systems of computation have become. These systems aggregate code written across the globe and parts manufactured outside the purview of their owners into complex networks that belie attempts to control them. Computation is exposed to the exterior places in which it is produced.

Furthermore, even if unintentionally, the use of this event as the first in a series of international cyberattacks offers an answer to a question that is often asked of theorists of cyberwar: how can such an event lay claim to being “war”? Is this merely sabotage? Placing the origin in the Cold War responds to those critics of cyberwar hype who believe it is nothing more than a collection of high-tech tools in service of the ancient techniques of spying, deception, and sabotage. For the Cold War proved that wars need not be explosive and could consist of decades of low-level conflict. As Virilio says of the threat posed by nuclear weapons, “the weapon’s serious danger is not that it could explode tomorrow. . . but that for thirty years it has been destroying society.”9 The bomb’s destructive power has been felt directly through its threat. Likewise, as can be seen in the futuristic scenarios described earlier, cyberwar seems always to threaten catastrophe. Placing cyberwar’s origins in the Cold War suggests the possibility of a nonwar that is as destructive as a kinetic war. The second half of the twentieth century has demonstrated that even in the absence of a hot war, conflict can destroy governments and societies.

Furthermore, at least for those theorists and strategists of cyberwar in the United States, this origin story contextualizes contemporary cyberwar discourses in another way. Several military and political commentators writing about cyberwar as a strategic area of study were the same theorists who worked on nuclear deterrence strategy in the latter part of the Cold War. A number of authors—many of whom work for the RAND Corporation, a think tank that was created in 1948 to provide research and analysis to the U.S. military—even attempt to employ strategies learned from nuclear deterrence research to mitigate military hacking and offensive use of global networks.10 Tying the origin of cyberwar to Cold War global strategic thinking offers an opportunity for those making the transition from strategizing in a bipolar world defined by nuclear weapons to a multipolar, interconnected global economy.

While the Siberian pipeline attack’s similarity to contemporary issues surrounding cyberwar is noteworthy, the most striking aspect of the whole affair is that it possibly never happened. Following the release of Reed’s book, an ex-KGB officer with direct knowledge of the region at the time disputes Reed’s account. He acknowledged there was an explosion but claims it was at a different, smaller pipeline and was caused by specific construction mistakes, not by faulty equipment.11 Moreover, no known media reports from the time confirm an explosion, which Reed claims was the size of a small nuclear blast. Other than Reed’s account, no other documentation has been found, and the CIA has never confirmed the event.12

The origins of cyberwar in this event are seemingly impossible to verify. Pipeline explosions were common at the time, and there would have been no way for the CIA to know for certain if it was caused by their purposefully faulty equipment or accidently faulty Soviet equipment. Given our current evidence, the event is completely unknowable. Moreover, even if there was an explosion, it is impossible to verify if it was the logic bomb or a mechanical failure. Depending on one’s perspective, either the fake event or fake refutations seep into the historical record like a computer virus corrupting the system’s memory.

Thus, in a largely unrecognized way, this event is archetypal for cyberwar. Cyberwar and cybersecurity weave a complicated relationship between the knowable and the unknowable. Our networked world has become so complex in sheer technical terms that the system as a whole cannot be known from the outside. Mapping even just the public Web has become a scholarly pursuit in its own right. Computers and networks represent information as tiny bits on a magnetic disk or pulses of light across a cable that, owing to their size, speed, and complexity, are on their own essentially meaningless and impenetrable to human observers. One always interacts with abstractions and complex representations of the material reality of computing. Cyberwar, in attacking these systems, is always on the verge of being meaningless itself. Moreover, in attacking systems of knowing that guarantee information, a successful attack impairs even our ability to know if something has happened. Cyberwar is fought precisely in this space between the possible catastrophe and the possibility of nothing happening at all.

The event itself is ambiguous and our public historical record is already compromised. It could of course be argued that all history is ambiguous, constructed, and selective. What is unique in the case of cyberwar is that the whole structure of knowing and observing is opened as a site of direct military intervention. It is not only a question of interpretation and selective archives. The entire archive and our ability to comprehend the archive may be attacked at any moment. In a sense, we are dealing with a limit case of historical unknowability—not just ambiguity but a military attack on the data of history itself. Now, even if the victors write history, it may no longer be written from data they control.

Thus an effective understanding of cyberwar will only be possible by not prematurely deciding in favor of an event happening or not happening. Cyberwar operates both as a strategy and as a mediatized cultural phenomenon directly in the space between happening and not happening. It succeeds as a military strategy by never succeeding too much. It always seems to be leading us to the verge of catastrophe and at the same time to an interminable boredom where nothing will ever actually happen. Cyberwar could easily be dismissed as not really being war or violent, but what is so virulent and dangerous about cyberwar is its ability to atomize and distribute warfare into everyday life. Cyberwar succeeds so much more effectively for being either overhyped or dismissed. Ultimately, we must resist deciding in favor of catastrophe or boredom, for in doing so, the entirety of cyberwar will certainly escape us. Instead, we must attempt to interrogate the history and discourses of cyberwar by following its vacillations between these two poles as it hides in the theoretical space between war and nonwar.

#### Our historical interrogation begins relatively recently, on April 26, 2007. Not a very important date by American standards, but one remembered by many Estonians as the “Bronze Night.” Estonia decided to move the Bronze Soldier, a Soviet memorial statue, out of Tallinn, its capital, provoking violent pro-Russian protests. Soon after, the extremely Internet-reliant Estonia was devastated by a DDoS cyberattack of Russian origins, isolating the country and shutting its economy down for two weeks.

#### The Bronze Night is now widely considered the world’s first cyberwar. Though the Russian government has denied official responsibility, NATO saw the attack on its vulnerable member as not just a threat, but the harbinger of a new era of war which it was woefully unprepared for. In response, Estonia led the alliance in establishing its Cooperative Cyber Defence Center of Excellence, as well as a comprehensive overview of the laws of cyberwarfare—the Tallinn Manual—and, gradually, the small country became the epicenter of NATO’s cybersecurity efforts.

#### NATO missed the real significance of the Bronze Night, which was not simply that it was vulnerable to a new form of warfare, but that it was fundamentally outdated in the face of the cybernetic transformation of the planet, as it was founded on the relevance of geopolitical factors like nation-states and physical boundaries like the “North Atlantic” which hold no sway in the digital era. NATO did get one thing right, though: there’s no going back.

Joque, 18—PhD from the European Grad School, researches philosophy, technology and media and is the visualization librarian at the University of Michigan, go blue (Justin, “Buffer Overflow: The Space and Time of Cyberwar,” *Deconstruction Machines: Writing in the Age of Cyberwar*, Chapter 1, 38-43, dml)

While Moonlight Maze was declared a cyberwar by a few individuals, a row between Russia and Estonia in 2007 is often mentioned as one of the earliest all-out cyberwars.17 On April 26 of that year, Estonia moved the Bronze Soldier, a memorial to Soviet soldiers killed during World War II, from the center of the Estonian capital Tallinn to a cemetery on the outskirts of town. Russians within both Estonia and Russia protested. Riots broke out in Tallinn, killing one and injuring more than a hundred people.18 In response, the Russian parliament called for the resignation of the Estonian government and stopped rail service from St. Petersburg, train shipments of oil through Estonia, and even heavy vehicles from crossing a major bridge from Russia into Estonia.19

At the same time, a host of computer-based services in Estonia were hit with a distributed denial-of-service (DDoS) attack. A DDoS attack involves overwhelming a server with traffic such that it is no longer able to respond to legitimate requests. It is relatively easy to automatically block computers that are sending inordinate numbers of requests to a server, so most DDoS attacks must be distributed across a large number of machines to succeed. This is achieved either by maliciously taking over machines to create what is called a botnet, some of which have involved tens of millions of computers, or by convincing people to voluntarily lend their machines for the purpose of an attack. These voluntary or commandeered machines are then turned against servers to overrun them with requests and disable them. DDoS attacks thus do not require breaking into a machine and do not compromise private data that may reside on the server; rather, they disable the server for as long as the botnet can continue sending requests.

In Estonia, these attacks targeted government websites and critical businesses such as banks and newspapers, shutting down ATMs and some means of communication within the country. These attacks were especially symbolic because, at the time, Estonia was one of the most well-connected countries in Europe, with more than 90 percent of bank transactions completed online. The country even allowed Internet voting by this point. Seven years prior, in 2000, the Estonian parliament declared Internet access a human right.20 Estonia was ultimately unable to counter the attacks and responded by shutting off Internet connections to other countries. This allowed services to resume within the country but prevented access to those outside the country. The attacks finally slowed down two weeks later. The Russian government denied any responsibility, and a number of security specialists have speculated that the attacks would have likely been more destructive if there had been direct government or military involvement, but there were extensive calls on Russian Internet for participation and instructions for how to join the attacks against Estonian institutions.21

The attacks on Estonia were carried out with a clear intent to disrupt the country in response to moving the Bronze Soldier, but beyond that and some technical details of the attack, little is discernable. The underlying purpose and the actors involved remain largely unknown, as Russia has refused any cooperation with Estonian law enforcement in finding and apprehending those responsible, despite a treaty guaranteeing mutual legal assistance. While it seems unlikely that the Russian government or military directly organized the specifics of the attacks, they have offered it their tacit approval by refusing to assist in any investigations. Thus the attacks against Estonia appear most likely to have been a “war” carried out by patriotic hackers not officially affiliated with the military, but perhaps with military support, and clearly outside the bounds and means of traditional kinetic warfare.22 As much as it is possible to discuss the purpose of these attacks that were carried out by a variety of unidentified individuals, the attacks were aimed directly at disconnecting Estonia from the global Internet and economy. In addition to the DDoS attacks, the other provocations all served to disconnect Estonia. Cutting rail and heavy truck connections to Estonia act in this light as physical denial-of-service attacks. To return to Castells’s point mentioned earlier, exclusion from global networks is perhaps now one of the gravest threats that could be wrought upon a nation. A denial-ofservice attack, in both its digital and physical forms, relegates the target to the space of place, severing its connections to global networks. While cyberwar functions through a variety of modes, it seems one goal that is often invoked is to disconnect one’s enemies from global spaces of flow.

All these attacks function at the same time to allow a level of plausible deniability. The physical infrastructure disruptions were claimed to be due to lack of passengers, repairs, and safety concerns rather than retribution. The cyberattacks were attributable to unknown patriotic hackers rather than a government or military group that could be held accountable. While in some cases it may be that governments and militaries truly were not involved, in the cases in which they were and attempt to deny their involvement, it is likely in many cases that this is due to fear of being cut off from global networks themselves. Ene Ergma, the speaker of the Estonian parliament at the time, claimed in an interview that “attacking us is one way of checking NATO’s defenses. They could examine the alliance’s readiness under the cover of the statue protest.”23 While Estonia did not invoke Article 5 of the NATO treaty, which outlines countries’ responsibility of mutual defense, NATO responded by creating the NATO Cooperative Cyber Defence Centre of Excellence in Estonia’s capital.24 The creation of the Centre of Excellence served to reassert Estonia’s position in a network of mutual defense, from which it was believed that Russia was attempting to sever Estonia. Thus this conflict can be read as a series of actions aimed at severing and reasserting Estonia’s connection to global flows of information, capital, people, military assistance, and goods.

It is also clear from these attacks that we are witnessing a significant blurring of the distinction between civilian, military, and political spheres. Just over a year after the Estonian crisis, when Russia entered a kinetic war with Georgia over South Ossetia, a wave of cyberattacks against Georgian targets followed Russian physical attacks. Like the Estonian attacks, the degree of Russian involvement was largely indeterminable. These attacks followed a similar logic of attempting to disconnect Georgia from global networks and also to assert the legitimacy of the Russian cause, perhaps with the hope of winning the global media’s blessing and thus support for maintaining global connections.25 In both these conflicts, it is evident that cyberwar does not merely seize upon an increasingly connected world but rather intervenes directly in global space itself to attempt to define, create, and undermine spaces of connection and disconnection. The increasing military and state interest in cyberwar is, then, not simply a result of the rise of global networks but rather an active force that both promotes and attacks such connections. Although the attacks in Estonia and Georgia were in response to geopolitical (and networked) change, they sought actively to reshape a set of interconnected networks and spaces.

OPERATION ORCHARD AS MICROSCOPIC WAR

A few months after the attacks against Estonia, on September 6, 2007, Israeli fighter jets attacked a supposed nuclear installation in Syria. The jets entered Syrian air space, destroyed the site, and returned without being fired upon. Despite the two countries technically being at war since 1948, both downplayed the event, which is now known as Operation Orchard.26 One of the most noteworthy elements of the attack was that a state-of-the-art radar system completely failed to detect the Israeli airplanes. Although it is unclear why the radar system failed, a number of commentators have suggested that the most likely cause was an advanced electronic attack on the system. Some sources even suggested it was possible that the computer chips that ran the radar system were fabricated with a “back door” so that they could be forced to malfunction.27

Even if this was not the case in the Israeli attack on Syria, chips being compromised during their production is becoming a growing military concern. The U.S. military has been working to create verified production facilities within the United States, but the growing number of commercial chips used in military equipment has complicated these efforts. There have been attempts to create systems to verify chips after production, but with current technology, it is nearly impossible to guard against a back door that is only triggered under specific conditions.28

There arises in cybersecurity a numbers game that generally favors attackers over defenders. For instance, microchips have become so complicated that a few transistors arranged in such a way that they can be activated for some malicious purpose are almost impossible to detect in chips now made of billions of transistors.29 Furthermore, even if it were possible to check chips for insecurities, it would be possible to limit the number of compromised chips to a small number in a production run, requiring that nearly every chip be checked to guarantee security (and one would, of course, have to guarantee that the system that checked the chips had not been compromised itself).

Two important phenomena emerge from the insecurity of supply chains in a digital and globalized world. First, the space and time of war spread outside war itself in an even more insidious way than we saw previously. Cyberwar, especially as it includes physical points of intrusion into chips, requires, in a sense, that the war start before the war. The trap must be laid long before a conflict breaks out. The war then extends along the entire supply chain. Any place that weapons, infrastructure, or any systems containing chips are designed, assembled, and stored becomes a potential battle space in a future conflict. Though sabotage has always been a threat for warring parties, the globalization and commercialization of the computer chip market mean that a country may end up fighting the very country that designed and manufactured the majority of its computing power. Prior to the growth of computerbased weapons, it may have been possible to sell low-quality armaments or steel to a potential future enemy, but hiding such built-in failures was difficult. Now the situation is inverted, and the work required to find faults and back doors in chips is substantially greater than the work involved in creating and hiding them. It is, then, not only that a nation or group can be disconnected from global flows but also that these global flows can be turned against an adversary, quickly turning supply chains and capital flows into potential threats.

Second, new, more complicated gaps open between knowing and seeing. The military reliance on more and more complicated technology has, over the course of the past century or so, pushed military operations beyond the field of sight. With the introduction of computer chips, and especially chips that could be attacked or sabotaged, the battle space now includes the microscopic. Moreover, technologies like radar and other advanced warning systems now rely exclusively on these technologies, and thus attacks that are imperceptible and microscopic can disrupt one’s ability to see on a macroscopic level. This is precisely what is believed to have happened in Syria. As Richard Clarke said of the attacks, “the view seen by the Syrians bore no relation to the reality that their eastern skies had become an Israeli Air Force bombing range. Syrian air defense missiles could not have been fired because there had been no targets in the system for them to seek out.”30 While war can now happen at every level from the microscopic to the global, defeat on one level easily spills over to all the others. Not only does war expand into cyberspace as a new domain of battle but other domains with their own geographies—including the macroscopic geographies of supply chains and the internal microscopic geographies of chips themselves—become realms of war and localized battle spaces.

War becomes rhizomatic and spreads out in all directions, including downward to the microscopic and imperceptible. Supply chains have always been important to war efforts, but what has changed is both the depth and breadth of global supply chains. Following World War II, the European Coal and Steel Community was created with the express purpose of tying French and German markets together to prevent another war, but this relied on the products of coal and steel being perceptible and war being a macroscopic phenomenon.31 Now supply chains are intertwined on an imperceptible, molecular level, making their interdependency a potential source of instability rather than stability.

While nuclear weapons harness the microscopic power of atoms to create unprecedented levels of destruction, they are anathema to any type of precision, rendering them useless in any conflict short of all-out warfare. Cyberweapons act to counter this lack of precision. Instead of releasing the maximum power from atoms, bits are manipulated, corrupted, and destroyed with exacting precision. Not only are precise sites and types of machines selected for destruction but levels of destruction are dialed in to precisely determine the possible responses. This is not to say that these political calculations are always, or even often, done well or to the benefit of anyone. Nor is it to say that what is precisely chosen and destroyed will not create results that will spiral out of control. Still, interventions are weighed and aimed at specific nodal sites in global networks, moving these calculations away from geopolitics toward a nodal politics.32 This networked political calculus does not replace the geographic but rather embeds geopolitics in what Virilio calls “metageophysics.”33 Ultimately, war in this new nodal space spreads out in every perceptible and imperceptible direction, intertwining with the civilian and the everyday. It follows the supply chains of advanced industrial nations all over the world, increasing the possibility that an imperceptible war could be fought unbeknownst to all observers. War then atomizes and moves along these multiple geographies, both spatial and aspatial, exploiting global flows and seeking infinitesimal advantages.

#### This transformation is occurring at a level beyond material infrastructures or international governance: digital technology has transformed life, communication, and the mind itself. The cybernetic episteme—the global system of understanding based on quantification and data analysis—is upon us. It weighs thirty trillion tons, it’s alienating friends and families, and it will destroy the planet.

Emmelhainz, 21—independent researcher and writer who has lectured and taught at an array of international institutions (Irmgard, “Authoritarianism and the Cybernetic Episteme, or the Progressive Disappearance of Everything on Earth,” e-flux #122, November 2021, dml) [section 4 was not omitted, the article just skips from 3 to 5]

Life and society worldwide have been transformed by digital technology, including the fabrics of emotional relationships. Many believed the internet would be the largest ungoverned space in the world with unlimited emancipatory potential, and trusted Big Tech to make the world a better place. Yet power and capitalism filled that space with surveillance systems, the production of private capital, the monetization of data, and the control of human lives. Social media now shape daily life and many have lost faith in the possibility of a shared consensus reality. We are living in a scenario similar to one imagined by Black Mirror: our belief in digital communication and social media creates narcissistic personalities, selves dissociated and dislocated from their reflections online. Digital communication offers an opaque mirror that delivers egos without bodies, eliding alterity.

The collapse of reality, however, is not an unintended consequence of advancements in, for instance, artificial intelligence: it was the long-term objective of many technologists, who sought to create machines capable of transforming human consciousness (like drugs do). Communication has become a site for the extraction of surplus value, and images operate as both commodities and dispositives for this extraction. Moreover, data mediates our cognition, that is to say, the way in which we exist and perceive the world and others. The image—and the unlimited communication promised by constant imagery—have ceased to have emancipatory potential. Images place a veil over a world in which the isolated living dead, thirsty for stimulation and dopamine, give and collect likes on social media. Platform users exist according to the Silicon Valley utopian ideal of life’s complete virtualization.

The internet, moreover, has radically changed the political communications game and must be considered a complex propaganda apparatus. Although a single Tweet can destroy someone’s career, and fake news can start a real news cycle, meaning is subordinate to the circulation of vacuous content. The capitalist capture of data for profit does not rely on policing content; the production of capital only relies on the constant exchange and circulation of information. We don’t yet know the full extent of the manipulation of companies such as Facebook, Google, and Amazon in the last two elections in the US or in other elections around the world. But it is undeniable that digital platforms are actively censoring content in the interests of particular political actors. For instance: in October 2020, Zoom canceled a meeting hosting Palestinian human rights activist Leila Khaled; a month before, Facebook and Twitter censored information detrimental to Joseph Biden’s presidential campaign. The same two companies intervened and shut down pro-Trump accounts in 2020, even Donald Trump’s own Facebook and Twitter accounts.

After the attempted coup at the US capitol on January 6, 2020, Facebook’s recently instituted oversight board ruled that Trump had created “an environment where a serious risk of violence was possible.” In this light, it seems likely that he will continue to be banned from the platform. According to journalist Shoshana Zuboff, however, this is insufficient, given that the oversight board’s decision (whose work is supported by a $130 million endowment from Facebook) follows years of inaction by CEO Mark Zuckerberg, who indulged and appeased Trump while entrenching what Zuboff calls “surveillance capitalism.” A liberal might think that shutting up Trump and helping Biden is not bad, as they are actions that seemingly advance the interests of the Democratic Party. What is at stake here, however, is not whether the platforms take a “good” or “bad” stance on a particular issue; the problem is that they have immense unchecked power and can act as they please. Platforms are allowed to secretly extract behavioral data from users, whether or not users are aware, transforming the information into targeted ads, destroying privacy, changing human experience into data, altering elections, and reshaping human civilization. This structure can be termed the “cybernetic episteme,” and the new form of control, which goes beyond the previous regime of biopower, can be termed “neuropower.”

According to its Greek etymology, an “episteme” is a system of understanding. In The Order of Things, Michel Foucault uses the term “épistemè” to mean the nontemporal or a priori knowledge that grounds what is taken as truth in a given moment. Several epistemes coexist at a given time, as they constitute parts of various systems of power and knowledge. The cybernetic episteme, as defined by the collective Tiqqun some twenty years ago, describes our relationship to technology and machines (which are inseparable from the workings of capitalism). The cybernetic episteme is based on the modern tenet of progress and human-led transcendence achieved through science and technology.

Under neuropower, the sensible gives way to cognitive pathologies. These pathologies depend on the consumption of content rather than the sharing of meaning. As Thomas Metzinger explains, the internet has become an integral part of how we model ourselves, as we use it for external memory storage, as a cognitive prosthesis, and for emotional self-regulation. This has radically changed the structure of conscious experience, creating a new form of waking consciousness that resembles “a mixture of dreaming, dementia, intoxication, and infantilization.” Other effects of neuropower are humans’ growing invisibility to each other and a paroxysmal racism that infiltrates power, technology, culture, language, and work. For Franco “Bifo” Berardi, racism has become a “virus” that exacerbates fear—above all, the fear of extinction, which seems to have become one of the motors behind white supremacy in the world. Dissociated from our environment, alienated from each other, we are oblivious to the challenges that are being posed to humanity by the Capitalocene.

A complex form of authoritarianism is emerging, linked to digital platforms owned by the powerful CEOs who make up the notorious “Silicon Six.” Under the new authoritarianism, populations are no longer commanded: they are asked to participate, and in this simulation of involvement, the “ideology of connection” replaces the idea of social relations, neutralizing democratic demands from users to have control over their own lives, rights, and data. In this way, people are made passive. Cédric Durand explains the difference between the original conception of the World Wide Web and the subsequent development of closed platforms. The WWW began as a decentralized architecture in which a generic transaction protocol (http) and a uniform identification format (URI/URL) generated a space of flat content. In this space, human and nonhuman agents could have access to information without any third-party mediation. In contrast, closed platforms use application programming interfaces, or APIs, to mediate interaction, giving way to data loops in which interactions are more dense. The technical object that sustains this hierarchical architecture is the API, each of which is owned by a platform. On the one hand, big platforms, by way of APIs, offer apps that incorporate basic and indispensable data for users. On the other, platforms have access to the additional information generated by the API, such as user activity and buying habits. As the ecosystem grows in complexity, the platform is able to accumulate more and more data. We become more densely connected with each other and with the platforms every day, as our lives get more and more tied to the cloud. Our dependency on platforms provides the ground for technofeudalism. Historically, feudalism was characterized by a fundamental inequality that enabled the direct exploitation of peasants by lords. The lord was both the manager and master not only of the process of production, but of the entire process of social life. In today’s technofeudalism, platform owners are the digital lords and users are the serfs. Rather than commodity production, these platforms are geared towards accumulation through rent, debt, and the privatization of the basic infrastructure that sustains our lives. What is at stake is no longer “true” or “fake” information but the cybernetic episteme upon which our lives and subjectivities have been built.

The cybernetic episteme is premised upon modernity’s enclosure of experience. In modern epistemology, which is the precondition of the cybernetic episteme, the self is externalized and experienced at a remove from the body. Perception is centered on the brain and eyes instead of the whole body, separating sensation from reason. The self’s relationship with the world is mediated through mirrors, camera lenses, the canvas, the microscope, and mathematical models. The cybernetic episteme, moreover, is inextricable from colonialism, which entails dispossession, dislocation, dissociation, and appropriation. Ariella Azoulay has called the logic underpinning these processes “the shutter”; this logic is materialized in photographic technology that separates humans from objects, self from the world, and people from their lands. The shutter is the principle of imperialism by which campaigns of plunder have left people both worldless and objectless. For Azoulay, the logic of the shutter was invented centuries before photography gave it a technological apparatus, and it enabled the dispossession of non-Western peoples in tandem with the accumulation of visual and material wealth in archives and museums in the West.

The cybernetic episteme is likewise conceptually constituted by this shutter, since it relies on capturing, naming, moving, and archiving subjects—as does imperialism. In this regard, the cybernetic episteme naturalizes the mediation of the self; it creates not only the condition of detachment from the world, but allows the appropriation of the cultures of others, as well as the dissolution of collective being. The shutter is akin to Heidegger’s Gestell or “representation,” which goes hand in hand with Eurocentrism and Anthropocentrism. The Gestell and the shutter both imply that the world and experience have become representation, through an aesthetic order in which what is produced as artifice becomes the reality of experience.

In a 2017 Facebook promo video for a new virtual reality technology, Mark Zuckerberg and his colleague Rachel Frank tele-transported themselves to Puerto Rico after a devastating flood. They intended to showcase the potential of the new technology, but instead revealed its inherent violence. The ability to transport oneself to faraway places “as if” one’s body were present gives the illusion that one we can make a difference in the world through technology. Another example, in a different register of colonial modernity is that way Western museums allow visitors to "transport" themselves by observing objects looted from elsewhere, like the Pergamon Museum in Berlin where museumgoers can roam around the Ishtar Gate, which has been on display in the museum since 1930. In a section of Ariella Azoulay’s video Undocumented: Unlearning Imperial Plunder (2020), she films actual visitors to the Pergamon while noting that dislocation is the essence of (imperial) modernity. The VR museum visitor is at the center of a world, but they are not really there (an effect similar to the dispositive of perspective in painting). For globalized Western culture, the ground for vision, enlightenment, culture, and even social change is the dislocation and disappearance of bodies.

Disembodiment and dislocation are also fundamental epistemological premises of transhumanist Silicon Valley ideology. In this ideology, the teleology of secular modern individualism culminates in the uploading of a person’s mind to a new biological, artificial, or biological-artificial body. The utopian goal of expanding and preserving human consciousness is physically and spiritually achieved. Transhumanism is the dream of enhancing the human body through technology, and ultimately escaping human suffering by transcending the “errors” of death and aging.

Posthumanism takes things a step further: its goal is to immortalize consciousness by uploading it to a robotic or synthetic body. Posthumanism does away with the biological dimension of the self, fundamentally altering what it means to be “human.” In both trans- and posthumanism, technology promises to give us the divine attributes of omnipresence, omnipotence, and omniscience, making humans into “pure consciousness,” achieving a kind of individual and secular transcendence. In the first episode of the British TV series Years and Years (2019), Bethany, an adolescent whose face is hidden behind a 3D emoji mask, announces to her parents that she is “transhuman.” She declares: “I don’t want to be flesh. I want to escape this thing and become digital, I want to live forever as information.” Eventually Bethany becomes a hero with transhuman superpowers: her mechanized eyes and brain, which are connected to all the data in the world, allow her to make visible the horrors that the British government have perpetrated in a refugee camp. This techno-utopian narrative implies a democratic ideology, insofar as one political goal of democracy is to make visible the ordeals of oppressed minorities—in this case through virtual disembodiment.

In contrast to this techno-utopian narrative, science fiction—especially cyberpunk literature— generally portrays transhumanism as a nightmarish apocalyptic scenario of social control and individual subjection. Several episodes of Black Mirror do this, for example. But what Black Mirror and Years and Years have in common is that technological advances and the increasing symbiosis between humans and machines are associated with political, economic, and social instability. In reality, “mind uploading” has attracted millions of dollars of investment from the billionaires of Silicon Valley and beyond. In a mixture of engineering and enlightenment, consciousness is now being hacked through biofeedback techniques, meditation practices, and microdosing drugs. Many critics have observed that the utopian ideology of transhumanism underpins the Valley’s culture of “move fast, break things, and make as much money as possible.” Technologies aiming to expand human consciousness are rooted in purely extractivist, capitalist values. In this sense, cybernetics is a political project on a planetary scale. As described by Tiqqun, cybernetics is a gigantic “abstract machine” made up of binary machines deployed by empire, and a form of political sovereignty that has merged with the capitalist extractivist project.

2.

In the pre-cybernetic era—that is to say, before the 1940s—machines were intended to emulate humans; their actions resembled human behavior, but ostensibly without intent or emotions. This is why Donna Haraway describes pre-cybernetic machines as “haunted.” They seemed animated by ghosts, reminiscent of Walter Benjamin’s automaton that was inhabited by a hunchbacked dwarf. Machines were not self-moving, self-designing, or autonomous. They could not achieve human dreams, only mock them. In turn, humans related to machines by using or acting upon them: switching them on or off, using them as tools to achieve an end. Today, the relationship between human and machine is based on internal, mutual communication in a feedback loop. Early machines were led; today, machines lead us. This does not mean that machines have simply become humanized through the proliferation of androids. Rather, humans have surrendered consciousness to AI, becoming obedient and predictable. In the twenty-first century, machines have blurred the distinction between the artificial and human mind, not only because machines can imitate human functions, but because humans have become increasingly passive, since we are now subject to neuropower.

Within the cybernetic episteme, it is no longer enough to talk about a “control society”; we must talk instead about a composite of interlinked forms of oppression (exploitation, alienation, and domination), in tandem with extreme securitarianism. Another way to see the cybernetic episteme is as the reconceptualization of social worlds into information-processing systems. Practices of computation are used to produce new organizational and infrastructural apparatuses, which in turn create value and profit by exploiting and disposing of human life. Social worlds are subsumed into technologies through techniques such as statistical forecasting and data modeling.

The cybernetic episteme stems from a world brought into being by Europeans; this world began with the discovery of the “new world” and the creation of empires and colonies (which coincided with the scientific revolution). In this sense, the cybernetic episteme is inseparable from the Western civilizing project for the whole world, which connected disparate places through technologies like the telegraph and steam shipping, often powered by the extraction of fossil fuels like coal. This project has culminated in globalization as the deregulation and financialization of world economies.

The Western civilization project, based on Enlightenment values including equality, peaceful public life, access to modern science, the rule of law, democracy, and technological progress, involved the creation of infrastructure to unify nations and the world. We can call this infrastructure the “technosphere.” The technosphere comprises not only digital technology but all machines, factories, computers, cars, buildings, railways, and mobility infrastructure, as well as systems of food production, resource extraction, and energy distribution. Today, the infrastructure of the world—the technosphere—is shaped by information, which means that the world we inhabit is designed by data.

The technosphere is a supplement humans have created to help overcome the limits of “human nature” insofar as humans cannot live independently from structures geared towards sustaining life. The technosphere has promised to enable us to increase production and reproduction with less human effort. Moreover, the technosphere is also regarded as the main tool humans have to fight decay, entropy, and death, since it comprises all the structures humans have built to keep themselves alive on the planet. The total mass of the technosphere amounts to fifty kilos for every square meter of earth’s surface—a total of thirty trillion tons, which coexists with the diminishing hydrosphere (water, the frozen polar regions) and the biosphere (all of earth’s living organisms). The ultimate price of the technosphere is global warming and environmental devastation. Like humans, the technosphere needs external energy input, which is not sustainable as long as it comes from fossil fuels that will eventually be depleted.

From this standpoint, the cybernetic episteme represents the gradual merging of human activity into the activity of what we have built and surrounded ourselves with. Much of this built environment is invisible. Infrastructure and data are partially occult because we are alienated from them, even as we are produced and managed by them. The invisible infrastructure that sustains our lives is what matters politically right now. And insofar as the technosphere is cybernetic, it is inextricable from capitalism and politics.

3.

Human communication is at the center of the cybernetic global order. The neural system of globalized networked society is digital communication. In a 1975 film called Comment ça va?, Anne-Marie Miéville and Jean-Luc Godard discuss the “illness” of information. They begin with an image of the Carnation Revolution in Portugal, published in the leftist newspaper Libération. At the time, photojournalistic images had begun to proliferate as a form of information, and Godard and Miéville critique Libération (the most left-wing newspaper in Europe in those days) for failing to include the reader in the creation and dissemination of information. They ask: “How is it that things enter and exit the machine?” (Comment ça va de l’entrée à la sortie de la machine?). This question is about how ideas, words, discourses, human interaction, and images become information and then reach readers and viewers.

In Comment ça va?, mass media represents an illness that has killed communication and language. Last year, Godard updated his critique of the media in an interview posted to Instagram. He stated: “Plato’s cave has been fixed on paper/screen.” For Godard, the consequence of the becoming-information of communication and language is the loss of ambiguity in communication. Digital technology has infiltrated every aspect of existence, and the margin of error between the transmission and the reception of a message has been eliminated by mediatization and digitization. For Godard, digital communication denies the force of the image or the word because it eliminates redundancy, misunderstanding, the possibility of reading between the lines, and the possibility of alterity.

In a more recent film of his—Adieu au language from 2014—Godard suggests that digital media have destroyed face-to-face communication. He asks: What kind of self could emerge in a time when objects and bodies are disfigurable and refigurable through virtual manipulation? Godard posits that the origins of today’s totalitarianism can be traced to the interruption of interior experience by the spectacle. In the film, Godard features a lengthy quote from Philippe Sollers explaining that the spectacle “cuts off” the subject from its interior life—a process that is, paradoxically, highly seductive. Furthermore, for Godard digital communication creates a new form of isolated solitude where people lack ties to others. In this light, technology has not become an extension of man, as Marshall McLuhan predicted, but has instead attained autonomy from man, since digital media can communicate amongst themselves without human mediation. For Godard, this means that the “face-to-face” encounter—a basic form of human relation that is the foundation of ethics—is no longer possible.

Sherry Turkle, a clinical psychologist and sociologist, comes to similar conclusions: daily conversations no longer involve eye contact, and face-to-face discussion has been replaced by words on a screen. According to Turkle, texts, tweets, Facebook posts, Instagram messages, and Snapchats split our attention and diminish our capacity for empathy. They have created new codes of etiquette; no longer do we feel restrained from reaching for our phones in the presence of other people. This new etiquette entrenches a culture of individualism and isolation from each other. This isolation cultivates the perfect ground for fascism.

The digitization of communication not only has political and communal consequences. It also affects the neuroplastic potential of the living brain. The cybernetic episteme reshapes our working memory by rearranging its contents. As Warren Neidich writes, the new focus of power is not only the false reproduction of the past (the manipulation of the archive), but the manipulation of our working memory—the type of memory that influences our decision-making. Authoritarian neuropower wants nothing less than to shape our future memory, argues Neidich.

If the nervous system of cybernetics is digital communication, at the center of digital communication is desire. Mark Fisher devoted his last lectures at Goldsmiths in 2017 to this subject. During one lecture, he played for his students a famous Apple TV commercial from 1984, directed by Ridley Scott and originally broadcast during the Superbowl. In an overt reference to George Orwell’s novel 1984, the commercial depicts a dreary, repressive control society. This society is seemingly liberated when a buxom blonde woman tosses a sledgehammer at a large screen broadcasting the image of an authoritarian figure, causing the screen to explode. The commercial ends with these lines crawling across the screen: “On January 24, Apple Computer will introduce Macintosh. And you’ll see why 1984 won’t be like 1984.” Fisher observes that the video counterposes top-down bureaucratic control to upstart entrepreneurialism. The dreary control society depicted in the commercial is an allusion to not only the Soviet Union, but also IBM, the dominant computer maker at the time. Apple posits itself as the dynamic, colorful new company that will liberate society from dreary IBM, ushering in a new, more vibrant world order. This new world order will fulfill our (capitalist) desires in a way that the communist world cannot. As Fisher suggests, we now live in that world of libidinal capitalism.

Elsewhere Fisher writes that what drives the circulation of information is the user’s desire to make one more connection, to leave one more reply, to keep on clicking. Capitalism persists because cyberspace is already under our skin, writes Fisher; to retreat from it would be like trying to retreat into some nonexistent precapitalist imaginary. In his view, we believe we have as much a chance of escaping capitalism as we do of crawling back inside our mother’s womb.

5.

By means of the cybernetic episteme, Silicon Valley has shaped the world we all live in. As we are poisoned equally by microplastics and fake news, losing our grasp of a shared reality, the “Silicon Six”—as Sacha Baron Cohen called the titans of Silicon Valley in a 2019 speech—propagate algorithm-fueled fear, propaganda, lies, and hate in the name of profit. As Baron Cohen pointed out, the major online platforms largely avoid the kind of regulation and accountability that other media companies are subject to. “This is ideological imperialism,” he said. “Six unelected individuals in Silicon Valley impos[e] their vision on the rest of the world, unaccountable to any government, and acting as if they are above the law.” He called digital platforms the greatest propaganda machine in history.

Democratic institutions have failed to reign in the information chaos and the destruction of the public sphere. As Shoshana Zuboff argues, we inhabit a communications sphere that is no longer a public sphere. She describes this situation as an “epistemic coup” that has taken place in four stages: First, by way of companies gathering personal data about us and then claiming it as their own private property. Second, through data inequality, which means that companies know more than we do. Third, through the epistemic chaos created by algorithms. And fourth, through the institutionalization of this new episteme and the erosion of democratic governance.

Baron Cohen observes that people can take a stand against platforms by recognizing our power to boycott them. (One example is the mass defection from WhatsApp to Telegram when the former announced that would share its user data with Facebook.) But we also need to defend the existence of facts and a shared reality, understanding the world not as something we see but as something we inhabit—treating life not as something we have, but as something we live. Anti-platform strategies might be accused of Luddism, but they are not necessarily opposed to technology—only to certain uses of technology.

It is also crucial that we regard the cybernetic episteme as inextricable from a broader malaise: humanity’s relationship to life and the planet is a toxic one. The very technologies that supposedly enable us to read, think, flourish, and desire are destroying the world we inhabit.

#### Vote affirmative to pursue insurgent governable stacks that increase security cooperation with the North Atlantic Treaty Organization in the area of cybersecurity. The aff reassembles the technical layers of the cybernetic episteme into new stacks—layered architectures of hardware, software, networks, and infrastructure which divide the world into sovereign spaces—that can fractally spill up to align with radical struggles across the globe.

Schneider, 22—assistant professor of media studies at the University of Colorado Boulder (Nathan, “Governable Stacks against Digital Colonialism,” tripleC 20 (1): 19-36, 2022, dml)

The spinning wheel remains a cipher and a site of conflict, an everyday technology summoned to a contest over the meaning of democracy. Despite having political ties with Gandhi’s assassin, the Hindu nationalist prime minister Narendra Modi promotes homespun cloth and has done photo-ops operating a spinning wheel. Modi has meanwhile shuttered boards that gave artisans a voice in policy under the slogan “Minimum Government and Maximum Governance” (Vincent 2020). The technology itself does not guarantee self-governance, but it can be the symbolic base from which ever-enlarging acts of self-governance defeat an empire.

In the spirit of the technological cipher I propose the pursuit of “governable stacks”: an orientation toward ungovernable organising under digital colonialism.

The geek-colloquial meaning of stack, in the most relevant sense, is a set of interoperating hardware and software. Benjamin H. Bratton (2016, xvii) goes further, describing the stack as “a new architecture for how we divide the world into sovereign spaces”. Its layers come with intersecting relations of dependency, along with emergent freedoms. A stack might include all that enables one to use a social media service, for instance: the server farms, the corporation that owns them, its investors, the software the servers run on, the secret algorithms that analyse one’s data, the mobile device, its accelerometer sending biometric data to the server farm, the network provider, the backdoor access for law enforcement, and so on. The layers of a stack might further include the sun or coal powering it, the wars fuelled by rare-earth mining, and the mythologies and rituals that dictate what people in it will tolerate. Each layer is in fact multiple layers, and layers build on each other.

Before governable stacks were the topic of this article, they were an experience for me, particularly through an organisation in which I have been an anecdotal participantobserver for a decade. May First Movement Technology (mayfirst.coop) is a cooperative that provides web hosting, cloud services, and public education for a 850-strong membership composed largely of activist organisations in the United States and Mexico (Lopez et al. 2007). Through the tools May First offers, I have been able to move much of my daily computing away from companies that surveil and extract into servers I co-own and govern, running commons-based software. I have formed relationships with the people who maintain these services and participated in decision-making over bilingual conference calls and online ballots. I learn about new tools from fellow members, and we sponsor events that teach people outside our membership how to challenge the power of big tech in their lives and their communities. Akin to the slow food movement, this is slow computing (Schneider 2015), its pace measured not by bandwidth or processing speed but by the attention to the social dimensions of everyday practice.

While Silicon Valley elites escape to phone-free retreats (Marantz 2019) and agonise about their children’s exposure to screens (Bowles 2018), May First offers no such “abhorrence of machinery” (Chaplin 1966, 373). It does not accept the false choice between addictive, surveillance-addled apps and a fantasy of returning to some blissful innocence. Instead, members share technologies that do what they need and that they can reasonably control. These technologies, and the self-governance we surround them with, are our stack. May First does not demand that you ‘learn to code’, or otherwise trade traditional knowledge for digital expertise. For me, being part of a governable stack like May First has unlocked political possibilities. The experience motivated years of working to build governable stacks elsewhere, because I know that it can be done. I poured myself into developing alternative ownership models like “platform cooperatives” (Schneider 2018) and “exit to community” (Mannan and Schneider 2021) that are better suited to making tech governable. With time, ungovernable stacks have come to feel like foreign lands. I may use them, but they never feel like home.

Governable stacks are cyborg assemblages of inter-operating technology, in symbiosis with human relationships (Haraway 1991; Puar 2012). Those relationships organise power, in partnership with the technology more than through domination over it. We learn with each other, and we learn with the machines, which take on life of their own – through their own intelligence, or that which we affectionately project onto them. In the sense of Grace Lee and Jimmy Boggs’s dialectical humanism, governable stacks invite the people who use them to change their relationship with technologies, to imagine different sorts of technologies, and to be changed themselves.

Perhaps governability can be achieved by reconfiguring tools that already exist; perhaps it is necessary to make new ones. Tiziana Terranova (2014), who has proposed the complementary idea of a “red stack”, writes that insurgent stacks become “new platforms through a crafty bricolage of existing technologies, the enactment of new subjectivities through a detournement of widespread social media literacy”. Older technologies may be better suited to this than newer ones (Maxigas and Latzko-Toth 2020). Even the colonial platforms can be repurposed – as the Algerian writer Kateb Yacine said of the French language – as spoils of war. The lifeblood of the governable stack is not any claim to innovation but the self-governance that flows through it. What emerges from there is the point.

The Guifi.net community Internet network in Catalonia (guifi.net) became the condition of possibility for a suite of “community cloud” services deployed through it (Selimi et al. 2015). FairTEC (fairtec.io) combines into one product a stack of preexisting services across three European countries: a sustainably manufactured smartphone, a non-commercial operating system, a cooperative telecom, and a cooperative phone rental company. The developers of the CommonsCloud (commonscloud.coop) see their shared technology as only one layer of a larger community stack, which also includes “social” and “discursive” layers – the context and substance of their self-governance. Layers form over time, too. Governable stacks of the past lurk in the archaeology of colonial systems through legacies like Indymedia, an activist social network whose participatory servers and software prefigured the corporate “Web 2.0” (Pickard 2006). Indymedia itself drew from decades of organising among activist communityradio stations, particularly in Latin America (Ruiz Martinez 2021). There can be no one governable stack – only many, whose archipelagos of commoning enable each other and give rise to more.

Technologists seeking alternative visions have often gravitated to the Free Software and Open Source movements, which employ creative licensing to enable the sharing of accessible and modifiable code. These movements have been successful in terms of the sheer volume of widely used software in their commons. But their emphasis on the freedoms of individual users, as well as of corporations, has privileged those with the technical know-how to take advantage. The software commons has spawned operating systems that fly in military jets and databases that aid in the imprisonment of asylum seekers (Ehmke 2020). In the name of freedom, too, developers have harboured sexism and other forms of exclusionary culture (SSL Nagbot 2016). Governable stacks should prioritise community accountability alongside individual freedom.

Another emerging strategy for challenging digital colonialism has come from within. Employees at Silicon Valley giants have achieved reforms by organising against certain ethical outrages at their workplaces (Tarnoff 2020). Yet there are limits to what these campaigns are likely to achieve, since these workers are invested – often literally, through stock options – in the basic business models of their employers. Employees’ actions can present the impression that their protest cleanses the colonial tools they produce. Governable stacks do not seek merely to improve the occupier. “Decolonization is not an ‘and’”, as Tuck and Yang (2012) put it. “It is an elsewhere” (36).

Experiences with governable stacks introduce us to possible elsewheres. The spinning wheel was an elsewhere, the invention of a democratic India. May First Movement Technology is an elsewhere for its members, who in turn become part of its learning and evolving. Collectives, families, and movements can assemble and adjust their stacks over time, wherever possible seeking to make their technological lives ever more governable. I next turn to strategies to guide the process of doing so.

5. Governable Strategy

May First is infinitesimally small by the standards of the tech economy. “Goldman Sachs doesn’t care if you’re raising chickens”, as the political theorist Jodi Dean (2011) has said. It’s a reminder for anyone tempted to see too much potential in personal practices, technological or otherwise. But spinning wheels are small, too, and they helped drive away the British Empire.

adrienne maree brown (2017) credits Grace Lee Boggs for helping her see that (her emphasis) “what we practice at the small scale sets the patterns for the whole system”. She explains this in a chapter called “Fractals”, which recalls how she shifted her activism to better reflect her political values in daily practice. Fractals are mathematical phenomena, frequent in nature, whose patterns at smaller scales repeat at larger scales. They are appealing and widely used as a metaphor, being both mathematically precise in theory and conveniently vague when applied to human affairs. Those like brown and Boggs who apply fractal-talk to politics exercise a kind of faith. To make good on that faith, there must some linkage, some strategy, that connects self-governance from the scale of small communities to the larger societies those community seek to transform. There was a fractal in the free maroons of Saint-Domingue who stormed down from their mountains into combat with French troops so the whole island could be free.

There was a fractal in the spinning wheel on the Indian National Congress flag, extending from a traditional practice to an eventual industrial policy. These chickens came to roost because they were part of a strategy that involved organised confrontation with colonial power. Self-governing became a challenge, a threat. In even small experiments, governable stacks can begin to normalise the otherwise elusive fact that better ways of organising technology are possible. Carefully chosen practices sever habits of dependency on the systems we seek to resist.

It is an uncomfortable matter of fact that nowhere has been so successful a counterweight to the power of Silicon Valley as China. The country has not only barred certain data-colonising companies with its ‘Great Firewall’ but has cultivated comparably ubiquitous Internet firms, using comparably invasive colonial practices to produce platforms that are at once hyper-capitalist and dominated by state interests (Chu 2017; Hong 2017). And yet China’s policy of sovereignty shows that dependence on hostile stacks is not inevitable.

Rather than trading one colonial power for another, Western Europe has sought a high road in demanding privacy regulations and investments in commons-based technology (Lemley 2020). Projects such as the Sovereign Cloud Stack (scs.community) seek to supplant reliance on corporate walled gardens with globally replicable, locally deployed tools. Several European governments have adopted and funded free/open-source software like the Matrix (matrix.org) messaging protocol and NextCloud (nextcloud.com), a file-sharing platform. Countries far from the power centres, like Uganda and Lebanon, have experimented with imposing taxes on the use of foreign social media (Boxell and Steinert-Threlkeld 2019). Although such efforts have been widely perceived as acts of repression more than solidarity, similar policies could be used for different goals. Echoing the Cold War-era Non-Aligned Movement among countries caught between the United States and the Soviet Union, some have been calling for a “digital non-aligned movement” that asserts many diverse sovereignties against the duelling forces of Silicon Valley and Shenzhen (Freuler 2020; Mejias 2020).

Sovereignty need not be solely the purview of nation states. The discourse of digital sovereignty has been particularly important among indigenous communities whose members are used to seeing their pre-digital sovereignty effaced; they have developed governable stack-layers such as tribal broadband lines (Blackwater 2020), cryptocurrencies (Tekobbe and McKnight 2016), data governance (Carroll et al. 2020), and linguistic autonomy (Pinto 2018). Amelia Winger-Bearskin (2020) draws on the Haudenosaunee practice of wampum agreements to propose “ethical dependencies” in software; these would encode and enforce certain commitments up and down the stack. Laying claim to collective sovereignty is central to such practices. Glen Sean Coulthard (2014) challenges the “colonial politics of recognition” – when people accept their colonisers’ definition of their sovereignty, rather than their own – to insist on more autonomous forms of self-determination. He describes how tribal nations can produce sovereignty through “community-scale activities” such as cooperatives and assemblies in everyday life (68). The indigenous organiser Berta Cáceres, before her murder by Honduran paramilitaries, denounced the pseudo-democracy of political representatives but affirmed the “decisive” democracy possible through poor people’s movements (Castellanos and Pine 2020).

Sovereignty can occur at levels ranging from the network backbone to last-mile connections, up through the hardware and software of devices, to the collaboration tools in the cloud. Sovereignty looks like a user-owned cooperative or a city providing connectivity, or like Douglass (douglass.io), an operating system whose apps take their names from icons of Black liberation. The tech publication The Markup has paid a “privacy tax” by developing its own software that protects user data rather than adopting the standard surveillance-based offerings (Angwin 2020). For Archive of Our Own (archiveofourown.org), a fan-run fandom repository, sovereignty puts creators in control of how they publish and protects their work against copyright overreach. What makes technology sovereign is when its stewards are the people who depend on it, protected from outside control by any legal or extra-legal means available. The data, the algorithms, and the interfaces are for their users, rather than acting surreptitiously against them.

5.2. Democracy

The other side of sovereignty is participatory democracy – its guarantor and its everyday practice. Here we resist the temptation of autocratic vanguardism by designing governable stacks to be accountable and alive. The style of democracy may be that of the Debian operating system, a constitutional republic of coders (debian.org/devel/constitution), or like the Ethical Source Movement’s vision of many collectives deciding on the ethical limits of how their software can be used (ethicalsource.dev). Digital democracy is beginning to have dedicated tools – from smaller-group decisions on Loomio (loomio.org) to the scale of cities or countries through Barcelona’s Decidim (decidim.org) or Polis (pol.is), which is employed by the government of Taiwan (Stempeck 2020). Platform cooperatives practice democracy at the level of the company, such as at Stocksy United (stocksy.com), co-owned by artists in dozens of countries (Schneider 2018). On a network scale, the federated social network Mastodon was able to counteract an incursion by the alt-right platform Gab, as it did earlier with Islamic State accounts – through self-organised activity by server administrators and app developers (Caelin 2020). Countering hate speech doesn’t need to depend on the might of a global monopoly; it can be tangible and empowering.

Practices of local democracy from the Global South have been migrating into governable online tools. Participatory budgeting practices originating from Porto Alegre, Brazil (Cabannes 2004), have appeared in apps like Cobudget (cobudget.co) and Decidim. A founder of an experimental political party in Argentina, Partido Red, has applied the same logic of “liquid democracy” to a blockchain-based governance platform, Democracy Earth (democracy.earth). Mexico City’s 2016 exercise in crowdsourcing its constitution has been studied as a model around the world.

Digital democracy has the potential to evolve rapidly and creatively. People can participate in far more rapid and fine-grained ways than was possible when the prevailing regimes of corporate and state governance first appeared. Organisational designs that work well could become part of a governance commons, enabling other groups to adopt, adapt, and share them back into the common pool (Schneider et al. 2021). In this way, small-scale accountability can spread, and it can creep into larger and larger kinds of communities, demonstrating that colonial control was never necessary. The more we demand and practice the arts of self-governing, the harder we are for someone else to govern.

5.3. Insurgency

The spinning wheel stood for household autonomy, but it was also defiance against British rule. Governable stacks must be similarly insurgent. Some of the earliest online social media emerged through Indymedia’s coverage of anti-capitalist protests. Twitter has its roots in technology for coordinating street protests (Costanza-Chock 2020, Chapter 3). While investors and accelerators receive frequent credit for innovation, insurgency is just as much a source of it.

Insurgency might mean challenging government subpoenas of member data, as May First has done, or facilitating leaks about abuses of power. Resistance might take the form of what the Catalan Integral Cooperative calls “economic disobedience” (cooperativa.cat/economic-disobedience), which includes refusing to pay unjust taxes or interest. Insurgents might choose not to submit the data of a friendship to the social graphs of colonial platforms, or to actively deceive those platforms, just as the Tor network (torproject.org) disguises its users’ locations. Like Copwatch groups or the Driver’s Seat Cooperative (driversseat.sco), insurgents can do data collection on the colonisers, sousveillance from below (Browne 2015).

To the extent that establishing the expansionist, slaveholding republic of the United States was also an anticolonial conflict, it relied on self-governance as resistance. The colonists organised through a Continental Congress, which extracted lessons from the Haudenosaunee nations – yes to confederation, no to matriarchal authority – to prefigure a future government. After independence, Alexis de Tocqueville (1840/2006) observed how the flourishing of civic associations energised the politics of the fledgling republic. Successful poor people’s struggles against the country’s wealthy elites, from the 19th-century Populists (Goodwyn 1978) to the 20th-century movements for Black power (Nembhard 2014), grew out of tangible collective organising in labour unions and cooperatives.

Insurgents might use colonial platforms for education and organising. They might spread viral messages and enjoy themselves. But if they have governable stacks to go back to, they are more than just subjects. They are maroons, with swamps and forests of their own.

#### Governable stacks are the only solvent mechanism for cybersecurity cooperation. Legal mechanisms for constraining cyberwar are a pipe dream; the proliferation of debates on those terms creates a smokescreen for cybernetic infrastructure to spread across the planet, which makes militarism and nuclear annihilation inevitable. We must reorient the resolutional model of thought towards corporeal care.

Dyer-Witheford and Matviyenko, 19—associate professor of information and media studies at the University of Western Ontario; assistant professor of communication at Simon Fraser University (Nick and Svitlana, “What Is to Be Done?,” *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*, Chapter 3, 151-161, dml)

As we have argued, from 1945 on, the hegemonic status of the United States, as the world’s chief capitalist power, was intrinsically related to the development of computers and networks. The role of digital systems in its military–industrial complex, initially tightly coupled with nuclear weapons, spread through other aspects of its war-making system as well as through the general economy. In both aspects, it contributed to the United States’s eventual Cold War victory. In the aftermath of that victory, the United States continued to develop its digital military capacities into the ever more direct weaponization of network, creating the technological human assemblages of what is today referred to as cyberwar. The scope of NSA global surveillance and sabotage programs and the sophistication of the Stuxnet nuclear centrifuge-destroying malware are only the most manifest instances of this process, which is today an integral part of a wider upgrade of U.S. military capacities that ties together a nuclear primacy with the militarization of space and drone warfare. Accompanying and spurring on this process is the additional dynamic of cyberwar adoption by the forces antagonistic to the global dominance of the United States and its allies. These antagonists include the defeated socialist powers, Russia and China, now paradoxically resurrected as capitalist competitors in the world market, or, in the case of North Korea, surviving in a macabre afterlife of state socialism. They also include the forces of militant Islamic jihadism, beckoned into existence by the West as an anticommunist ally, only to become its opponent in the long war on terror. All these actors converge on the militarization of digital networks. Many observers today see a moment that recapitulates the decline of previous imperial hegemons within the global capitalist system—Spain, Holland, Britain—and parallels the moments of extreme instability as old powers and new contenders confront each other.7 The rise of cyberwar is part of this tumult and quite possibly a precursor and preparation for widening and intensifying conflict. Schematically, we can envisage three potentially intertwining trajectories such a process might take:

1. Network degradation. Alexander Klimburg (2017) outlines the possibility of a “darkening web” characterized by persistent and gradually intensifying cyberwar between states and between states and terrorist movements conducted in a variety of registers. Security breaches, aggressive malware, and botnet attacks proliferate. Digital industrial sabotage and critical infrastructure attacks begin to multiply, as do the accidental runaway effects of cyberweapons. Networks are deeply and chronically infected with computational propaganda, fake news, and viral mis- and disinformation. In response to adversarial incursions, states intensify algorithmic surveillance, censorship, and preemptive virtual policing. Cybersecurity provisions become increasingly mandatory and elaborate. Attribution problems, falsification of evidence, and the overlap between military and intelligence forces and criminal networks create a chaotic digital twilight of hacking and trolling, botnets and viruses, malware, surveillance, and bugs, shutdowns, blocking, and filtering, in which uncertainties exacerbate suspicions and hostilities, altogether making the internet increasingly impossible to use. In short, the “darkening web” is what already exists now, only more so. One of the cofounders of Twitter, Evan Williams, offered his diagnosis, suggesting that “the Internet is broken” (Streitfeld 2017). But maybe it’s not. Maybe the internet is finally what it was always meant to be. Maybe it is perfect, but not for us, the excommunicated user-subjects. For cyberwar.

2. Hybrid escalations. Similarly rooted in the present is the likelihood that the simultaneous virtual and kinetic conflicts, such as the Syrian civil war, the fighting in Donbas, and the many branches of the war on terror, continue and break out in new regions, bringing ever higher levels and varieties of cyberweapons, deployed for purposes ranging from intelligence gathering, battlefield surveillance, and munitions delivery to sabotage of enemies’ domestic and military resources. The use of drones and other semi- or fully automated weapons systems expands and takes new directions, such as the development of swarms of small autonomous vehicles—“slaughterbots” (Economist 2017a)—for house-to-house fighting in ruined cities. The biometric and networked tracking of refugees created by such conflicts, and the control and interdiction of their entry to affluent fortressed homelands, becomes a major activity of the nation-state security apparatus. Because present hybrid wars are also in large part proxy wars, where local battlefield actors are directly or indirectly supported by major powers, they are charged with the possibility of abrupt collisions between the most powerful militaries on the planet.

3. “Thermonuclear cyberwar.” We borrow this phrase from Erik Gartzke and Jon Lindsay (2017), who are among several authors currently pointing to a renewed and dangerous rendezvous between cyber- and nuclear weaponry. The last decade of debates between defense intellectuals about cyberwar has split those who see digital attacks a new equivalent of nuclear weapons, capable of disabling whole societies through critical infrastructure attacks, and skeptics who deride such anxieties as hyperbolic and implausible. But “cyber” and “nuke” are not separate. As we have seen, they were twinned at the moment of conception, with the development of each dependent on the other. And the connection is not just historical; it is current. Now cyberwar weaponry is part of a new approach to nuclear war fighting, the left-of-launch approach. Early ventures in antiballistic missile defense, such as Reagan’s “Star Wars” strategic defense initiative, depended on shooting down swarms of missiles as they plunged through the atmosphere toward their target. Left of launch, in contrast, aims to “strike an enemy missile before liftoff or during the first seconds of flight,” using “cyber strikes, electronic warfare and other exotic forms of sabotage” (Broad and Sanger 2017). This doctrine was incubated during the Obama administration and inherited by the Trump presidency. Advocates of the left-of-launch nuclear strategy present it as a defensive measure. However, the doctrine destabilizes basic premises of deterrence that have, since 1945, restrained nuclear weapon use (Cimbala 2017). Deterrence depends on a dread faith by all parties that both their own and their enemies’ nuclear weapons will work. The possibility that nuclear weapons systems might be secretly disabled raises prospects both of overconfidence (trusting one can sabotage an opponent’s system) or panicked preemption (fearing left-of-launch attacks on one’s own nukes and falling into a “use ’em or lose ’em” mind-set). More generally, control and command of nuclear weapons depend on communication systems whose collapse in a crisis situation could have catastrophic results.8 The origin of the internet lay in the U.S. attempt to ensure continuance of such systems in the event of nuclear war; now the weaponization of the internet itself constitutes a possible cause of nuclear war.

Facing such prospects, liberal commentators propose diplomatic measures to control and mitigate cyberhostilities. Klimburg (2017), for example, suggests a series of initiatives to be undertaken primarily by the United Nations and the Internet Corporation for Assigned Names and Numbers (ICANN), the long-standing (and controversy-ridden) forum for internet governance. In these venues, he suggests, it should be possible to work out a series of agreements—“digital arms” limitation treaties, comparable to those on nuclear weapons; an “attribution and adjudication” council to assess and arbitrate responsibility for cyberattacks; international cooperation against cybercrime; the promotion within ICANN of “civil society” perspectives to counter those of states and corporations. He suggests that “standing bodies” regulating cyberwar would be comparable to the Intergovernmental Panel on Climate Change and emphasizes the importance of “scientific and authoritative advice from experts to political decision makers on how to avoid disaster” (344).

Such proposals, seemingly eminently sensible, ignore the reality that the tensions driving the rise of cyberwar are also incapacitating the fragile apparatuses and institutions of international cooperation that have existed since 1945. As Jon Lindsay (2012) observes, while proposals for cyberwarfare treaties are “well meaning,” they would, within the current state of international great power relations, be “hacked to bits,” because “cyberoperations, like other types of intelligence and covert operations, take place in the shadows. An international treaty on cyberweapons would be . . . totally unenforceable, since such activity is designed to evade detection and attribution.” The conjuncture in which cyberwar rises, and part of the reason for its ascent, is the breakdown of nuclear arms limitation and nonproliferation treaties. Klimburg’s comparison of the regulation of cyberwar and climate change is unfortunately all too telling, given the failure of global capitalism to generate any binding interstate agreements on carbon emissions and the recent withdrawal of the United States from even the nonbinding Paris accord on global warming. And like slowing climate change, reducing the risk of cyberwar requires deep, systemic social change.

The argument of this book is that cyberwar is a manifestation of the competitive nature of capitalism, which, beneath the surface of globalization, fosters a war of all against all, conducted in the accelerated, automated, and abstracted forms on which this entire mode of production now depends. It follows from this that the prospects for reducing the dangers of cyberwar, and of the other types of war of which it is now part, depend strongly on movements and struggles to constrain and, ultimately, abolish this internally antagonistic order. A recognition of the extreme difficulty of this project is inherent in the point on which we opened this chapter, namely, Noys’s observation that the military high-technology “endocolonization” of society has been a factor in decomposing the traditional industrial working-class movements that were historically the main agencies of socialist and communist projects. However, there is also a possible reversal of this logic, if averting war, including cyberwar, becomes entwined with other issues, such as struggles for social equality and ecological sustainability, a focal point for recomposition of movements looking beyond capital, drawing on new and diverse constituencies. We have indicated some of the issues that we think might be drawn together around resistance to the rise of cyberwar: antisurveillance sentiment, rejection of the secrecy of the security state and its new digital complexes, concern over the corruption of the general intellect by mis- and disinformation, objection to corporate and military criminality, and, of course, revulsion at the exterminatory horrors of war, from the terror of dirty wars to global thermonuclear catastrophe.

In his reflections on Marxist theories of war and revolution, Balibar (2002) remarks on the coexistence within this body of thought of two contradictory elements, one stressing the idea of “revolutionary war,” the other of “revolutionary peace.” The first stresses “armed struggle against capital,” the second “the refusal of capitalist wars”—“in many respects this class war is therefore also a non-war, or an anti-war” (11). If, in the title to this chapter, we invoked Lenin’s What Is to Be Done?, it is partly to remember that, though Lenin is today primarily thought of as a theorist of revolutionary war, perhaps the major decision of Leninism was one for peace (even if his later adoption of Trotsky’s formula of “no war, no peace” resonates with today’s state of cyberwar). The outbreak of World War I precipitated a schism in the international socialist movement. Leading European socialist democratic parties all too rapidly discarded their longheld view that war exemplified the irrationality of competitive capitalism, forgot their commitments to peace and worldwide worker solidarity, rallied behind their governments, and joined the march to mass slaughter. Only the faction of what is sometimes known as the Zimmerwald Left (Nation 1989), led by Lenin, continued to speak out for internationalism. It was thus not just revolt against exploitation but rejection of the holocaust of World War I, a program of “bread and peace,” that gave communism a moral claim to universality. Terrifying contemporary parallels to the pre1914 years today demand an updated strategy for “bread and peace,” with “bread” understood as a securing of ecological conditions for species life and “peace” as elimination of systemic social violence.

One of the slogans of the Zimmerwald Left was “Krieg dem Krieg,” “war on war,” and it is tempting to take this up, in a very literal sense, and propose a “cyberwar on cyberwar.” As we have seen, there is a hacking front to both the struggles against digital militarism and contemporary anticapitalist movements. They have exposed the workings of the cyberwar complex and brought it to light. Their main figures are defectors from that complex. More broadly, over recent decades, many critical theorists have argued for forms of “cyborg” dissent and for deployment of the arms available to “immaterial labor,” whether in the networked mobilization of protest or in more direct digital disruptions of war making. Cyberwar on cyberwar is both a metaphorical and practical possibility, and we have seen situations when “Krieg dem Krieg,” in the most concrete sense, is the only effective response to murderous attack.

However, we would suggest that to conduct “cyberwar on cyberwar,” though it may sometimes be necessary, is to fight on unfavorable terrain. We have seen that hacktivism suffers problems of accountability, transparency, provocation; can itself be compromised and ensnared within the exploits of the military–internet complex; and is ultimately highly vulnerable to the police and intelligence apparatus. And, as Noys (2013) observes, even reliance on the speed with which networks can circulate struggles tends to discount how much more advantage such velocity today gives capital’s military–security complexes (in this respect, we note that the huge, worldwide, and digitally mobilized protests against the Iraq War in 2003 must be reckoned a tragic failure of networked activism). Cyberwar on cyberwar is a method of fast politics, and speed is where the user-subjects ultimately lose, encountering the inhuman acceleration of machinic processing power. To succeed, such resistance requires a break from the mainstream paradigm of today’s “platform capitalism” with all its repetitious “Twitter revolutions,” “Facebook revolutions,” or “Snapchat revolutions,” slogans that should remind us that, as Lacan once notoriously noted, an ultimate misconception of revolution is as a desire for a new master or a master in a new form that leads away from the systemic change rather than not toward it. Here we disagree with the conclusion of Brian Massumi’s (2015, 243) otherwise excellent study of the new “ontopowers” of military networking, where, discussing the logic of speed and preemption, he suggests that countermovements have no choice but to “go forward, with the flow.”

While tactical resistance can involve any and all of the “memes of production” (Deterritorial Support Group 2012), a reconstitution of the left today must ask, what is the opposite of cyberwar? To this, we would answer that the antithesis of cyberwar is corporeal care of the subject achieved through the “balanced conceptions of space and time within culture” and “awareness of spatial and temporal dynamics [that] keep state and market power in check” (Sharma 2013, 314). It is from this perspective that we need to recognize cyberwar’s production of time and space and envision different times and spaces—those of the care of bodies. This orientation against the social destruction, physical, psychological, and infrastructural, of cyberwar does not mean totally abandoning the digital—which, because it so much composes the very texture of everyday life, would be not only difficult but often politically fatal. But it does mean its rearticulation to a set of purposes radically different from those of digital capital. In particular, this strategy requires theoretical reconsideration and practical subversion of the addicted, complicit digital user, the figure envisioned by neoliberal Silicon Valley, by way of desynchronization and emancipation.

This can be described as recognizing a position in and against the military environment of cyberwar in which all of us are now imbricated and finding ways to develop subjectivities that are simultaneously of the network and off the network. It requires the “slow” time necessary for the in-person (rather than online) organization of antiwar collectives, movements, and alliances; defection from compulsive social media use; trammeling corporate capacities to intensify and maintain such addictive behavior; the patient defense and reconstruction of the basic public institutions of corporeal care—free health services; the cultivation of mental health; the recovery and deepening of the legacy of a semidestroyed (or, in many places, never created) welfare state in a new “commonfare”; universal education provisions; worker–community control of workplaces and the means of production; ecological protections—and the assertion of such priorities against the expense and logic of networked militarization. In this work of solidarity, the subject exploited and excommunicated by digital capitalism can transition from alienation toward reciprocity. And to those who say that the accelerated logic of cyberwar means we don’t have time to do all this before catastrophe arrives, we just say, you may be right, but still we have to do it anyway! We can build a “counterwar machine” constructed on the diagonal line that runs between waging cyberwar on cyberwar and fostering the caring corporeality that is opposite of cyberwar.

At the end of her study of world labor activism, Beverly Silver (2003, 176) notes a major reason for the shortage of militant working-class movements in the early twenty-first century. Neoliberalism’s restructuring, globalization, and financialization, with its “growing structural unemployment, escalating inequalities and major disruptions,” has repeated the crisis patterns of previous eras of capitalism, with one crucial exception. The missing condition is large-scale armed conflict. This “global political–military context contrasts sharply with . . . that [which] produced radicalized and explosive labour unrest in the first half of the twentieth century.” As Silver notes, war then involved the mass mobilization of populations that characterized total war. States depended on their working classes to provide not just millions of soldiers but labor in munition plants, shipyards and aircraft factories, hospitals, and farms. When mass mobilization met the horror of mass deaths and mutilation, revolutionary social turmoil could result.

As Silver (2003, 175) observes, advanced capitalism’s turn to high technological weaponry apparently breaks this link between war and worker revolt. Cyberwar can be seen as an extension of this “automation of war.” Nonetheless, as we have suggested, the tendency of digital militarization to liquidate the labor of war is not yet completely fulfilled. Humans remain as the indispensable conscious links and relays within the networks and nodes of digital conflict. Indeed, what we have seen in this book is the surprisingly wide diffusion of participation in cyberwarfare, from the highly specialized military and intelligence units at the cutting edge of advanced cyberoperations to strata of mercenary and criminal proxies, online vigilantes, patriotic hackers, corporate and criminal marketers of cyberweaponry, cybersecurity personnel, and on to the corporate content moderators and state censors and surveillance agents now indispensable to the prosecution of war waged in cyberspace and across scores of hybrid battlefields. To these more or less intentional contributions to the mechanisms of cyberwar must be added the unknowing (or partially unknowing) participation of network users, whose online activities and addictions provide the vital vectors for the memes, exploits, and hijackings of subterranean cyberconflicts and whose reconstitution as data-subjects habituated to ceaseless state and commercial surveillance constitutes the inevitable accompaniment to such operations.

Surveying this field, we can say that military mobilization has not so much been abolished from cyberwar as reconfigured in subterranean, etiolated, and unfamiliar forms. This decomposition of the labor of war, equivalent to Virilio’s state of “endocolonization” by the apparatus of high-technology militarism, may, as we have proposed in this chapter, contain potentials for reversal. If, to date, cyberwar is not, at least in the centers of capitalism, producing the massive havoc of earlier forms of war, the migrant refugees of hybrid conflicts around the world, fleeing algorithmically directed drones, social media–activated death squads, and cybernetic strikes at social utilities, bear witness to its potential to do so. Already, even in ostensibly secure zones of the planet, the costs of militarized and criminalized networks, in terms of escalating social paranoias, crumbling confidence in everyday communication and polarizing social relations, becomes daily more apparent. If this course persists, unforeseen forms of unrest by the new workforces of cyberwar may interrupt its inhuman trajectory.

#### Plan-focused debates replicate the folly of the Tallinn Manual by attempting to apply liberal technological literacy to a problem that has outpaced liberalism itself. The formation of governable stacks begins not with the question of how security cooperation over cybersecurity “should” occur, but what “is” cybersecurity and how it came to be that way in the first place.

Gray and Eloff, 22—School of Philosophy at North-West University (Chantelle and Aragorn, “Fabulation in a Time of Algorithmic Ecology: Making the Future Possible Again,” *Technology, Urban Space and the Networked Community*, Chapter 5, 105-133, SpringerLink, dml)

In his 2008 article, “The End of Theory: The Data Deluge Makes the Scientific Method Obsolete”, Wired editor Chris Anderson notoriously argues that the era of the scientific method built around testable hypotheses is fast-becoming obsolete due to the advent of “petabyte-scale” data accumulation and analytics. Observing that tech companies like Google treat this “massive corpus as a laboratory of the human condition” (Anderson 2008), Anderson polemically implores us to forget every theory of human behaviour, from linguistics and sociology to ontology and psychology. “With enough data”, he avers, “the numbers speak for themselves” (ibid.), and statistical correlation renders superfluous any theorisation of causality. The Californian Ideology (Barbrook and Cameron 1996)1 implicit in this overstatement of the benefits of data-driven research has been challenged by several commentators (see, e.g., Pigliucci 2009 and Mazzocchi 2015) and is patently specious. The appeal made by Silicon Valley zealots to ‘pay no attention to the man behind the curtain’ relies on a mythical, and sometimes even eschatologically feverish, conception of science as a purely objective pursuit, as well as a facile conception of human thought and behaviour—indeed, subjectivity—wherein we can be comprehensively understood via the purely quantitative approaches of Big Data analyses and the statistical aggregation of deep learning systems. As Louise Amoore underscores in Cloud Ethics, this ideology confronts our “fallible, intractable, fraught political world with a curious kind of infallibility. In the cloud, the promise is that everything can be rendered tractable, all political difficulty and uncertainty nonetheless actionable” (Amoore 2020, 55). This dream of complete mathematical and technological control over reality—of “a kind of atlas of clouds for the ineffable, a condensed trace of the trajectories of our future lives with one another” (ibid.)—is hardly new. What legal theorist Antoinette Rouvroy refers to as “algorithmic governmentality”2 (Rouvroy and Stiegler 2016, 6), by which she means “the increasingly statistical governance of the ‘real’ ensuing from a convergence of contemporary technological and socio-political evolutions” (Rouvroy 2011, 119), can be traced at least as far back as first-order cybernetics (Wiener 1965, 12) and, before that, to Leibniz’s calculus ratiocinator (cf. Couturat 1901). What makes the contemporary problem novel, however, is that the latest technologies, for example cloud computing, practically unlimited data storage, high-speed global communications networks and, most importantly, machine learning—and here we mean specifically new forms of connectionist ‘artificial intelligence’ that, unlike older symbolic AI models, rely on multi-layer artificial neural networks that are assumed to represent the biology of human cognitive structure—have powerfully exacerbated the quest for (and assumptions of) ‘Algorithmic Supremacy’. As digital technology theorist Dan McQuillan argues, data-driven modelling via statistical induction is assumed to bear inherent significance, but this approach, which McQuillan describes as a form of “machinic Neoplatonism” (McQuillan 2018), tends to entirely elide the broader subjective and inter-subjective contexts within which analyses and modelling unfold and is thus, via this unwarranted delimitation, able to present itself as operating with a level of mathematical objectivity it simply does not possess.

This creates several insidious problems. For one, as Bernard Steigler observes in The Age of Disruption, this deferral to the ‘superiority’ of algorithmic reason legitimises “the systematic exploitation and physical reticulation of interindividual and transindividual relations” in the service of the data economy (Stiegler 2019, 7). In other words, the kinds of transgenerational, intergenerational, interpersonal, personal and even pre-personal3 circuits that used to “emerge through affective relations of various kinds” over time within and across societies to forge “dreams, goals, objectives and common horizons” have been disrupted in unprecedented ways (ibid., 16). Rouvroy argues, in fact, that subjectivity is bypassed by contemporary digital automisation so that subjects are rendered little more than a “collection of infraindividual data” that are “recomposed at a supra-individual level under the form of profile” (Rouvroy and Stiegler 2016, 12). Second, the speed at which what we have elsewhere termed the Algocene4 has emerged, as well as the level of technological literacy a coherent understanding of this shift entails, has far exceeded our capacity to theorise its effects, with the result that many analyses of our contemporary condition remain trapped in anachronism, projecting the image of an old world and its struggles onto a new and largely alien terrain. It is perhaps not too hyperbolic to claim, as many have, that the staggering technological shifts of the last 20-odd years necessitate theoretical engagement on the scale of a new geological era or epoch. This is no longer the world of industrial capitalism, nor even of Foucault’s disciplinary societies (Foucault 1977), Deleuze’s control societies (Deleuze 1992) or Guattari’s Integrated World Capitalism (Guattari 2000), although these are all vestigially inflected in the new situation, which has variously, although far from exhaustively, been termed societies of hyper-control and computational capitalism (Stiegler 2019), cognitive capitalism (Yann Moulier-Boutang 2012), platform capitalism (Srnicek 2016), the age of planetary computerisation (Guattari 2013), The Stack (Bratton 2015), infopolitics (Koopman 2018), instrumentarianism (Zuboff 2019) and algorithmic governmentality (Rouvroy and Berns 2013). Third, because of the speed at which digital innovation operates, whatever effects this new “hyper-synchronization of consciousness” (Vignola 2017, 188) is having on subjectivity can only be perceived in the most miniscule of ways, yet we have to rely on this minimum of information for a symptomatology because, if we follow Deleuze via Nietzsche, it is only through a symptomatology that we can trace etiological factors in order to find the most inventive corrective therapy. A difficult task indeed considering the constraints we are outlining here! The point is, we urgently require new tools to grapple with the implications of the encroachment of algorithmic reason and governmentality into more and more aspects of our lives and minds. Far from eschewing theory in favour of the transcendent mathesis universalis of our new digital overlords, situated thinking about our times has never been more crucial. If, however, this kind of thinking has not been forthcoming to the extent we would hope for, then this too perhaps forms part of the symptomatology of the Algocene. In describing something that is unprecedented, we need to take care, as McKenzie Wark argues, to find “a renewed language for describing the present situation and identifying what in the received language of capitalism [or, for those further behind the times, Marxism] impedes forward movement in thought and action” (Wark 2019, 6). Having said this, we also hold that it is important not to reduce the entire social field to algorithmic control, despite its near-ubiquity. What is rather vital is to understand what this new way of experiencing subjectivity produces and what, in turn, produces it. As Guattari explains of the Freudian Unconscious, it produced new desires, which included “hysteria, infantile neurosis, psychosis, family conflict, the reading of myths, etc.” (Guattari 1995, 10). So too what Stiegler refers to as “negative collective protention”, or the nihilistic expectation of nothing, except perhaps The End (Stiegler 2019, 19, 50), has produced new desires, and here we have to seriously consider that The End might in fact—probably is—desired, even collectively so (especially given that we also face Anthropogenic doom).5

How, then, do we change this desire? How do we use the diagnostic tools at our disposal in the schizoanalytic mode—that is, a therapeutic mode—to produce something new, something healthier? How do we change our practices and ways of being in the world so that life—rather than a misguided idea of Algorithmic Supremacy—matters again? In this chapter, we attempt to give a broad symptomatology of algorithmic subjectivity, drawing on a range of scholars who have gone before us. Our aim, diverging from most theorists, however, is not to propose legal or other reforms. We understand the algorithm to already present itself as an ethicopolitical arrangement of values, assumptions and propositions about the world. Our question—yes, our desire—is not: How ought the algorithm be arranged for a good society? but rather: What is a good society? For it is from the latter question, we hold, that healthier algorithmic arrangements will flow, not the other way around.

## Case

### AT: Communication=Possible

#### Cybernetics has robbed meaning of its stability.

**Dyer-Witheford and Matviyenko 19**(Nick and Svitlana, Associate professor at the University of Western Ontario, Professor of Communications at Simon Fraser University “Cyberwar and Revolution”, Chapter Two, CS)

There is no longer a Master-Signifier that stabilizes meaning, that knits together the chain of signifiers and hinders their tendencies to float off into indeterminacy. While the absence of such a master might seem to produce a situation of complete openness and freedom—no authority is telling the subject what to do, what to desire, how to structure its choices—Žižek argues that in fact the result is unbearable, suffocating closure. A “setting of electronically mediated subjectivity [that] is one of infinite doubt and ultimate reflexifisation” intensifies “the fundamental uncertainty accompanying the impossibility of totalization” in a symbolic environment where “there is always another option, link, opinion, nuance or contingency that we haven’t taken into account” (Dean 2014, 212). Computational propaganda that aims to mystify invasions and occupations, or promote cynical disaffection from an adversary’s political system, actively weaponizes the “decline in symbolic efficiency,” but it is endemic to the whole field of cyberwar. The extreme uncertainty and opacity of cyberwar do not, however, inhibit the interpellative effects of contending cyberwar apparatuses as they summon up cybersoldiers, patriotic hackers, vigilante militias, and security-conscious digital citizens. On the contrary, the problems of verifying or disproving multiple alarms and accusations accelerates these processes and puts them into overdrive. To put this point in psychoanalytic terms, as we noted previously, commentators on Althusser have criticized the appropriation of Lacan’s theories of the subject in his account of ISAs. These critics point out that what Althusser misses in Lacan’s account is that the subject is always incomplete; it is precisely what can never be fixed by a specific subject position or identity. However, the implication of this incompletion is not that the subject remains some untouched and primordial haven of authenticity but rather that this lack drives to ever more compulsive (because unfulfillable) attempts to attain a definitive identity. Translating this into political terms, we would say that it is the inescapably incomplete, provisional, and easily falsified nature of all accounts of cyberwar that energizes the adoption of increasingly militarized, extreme, paranoid, and unshakable subject positions vis-à-vis its alleged events.

### AT: Global Cybernetics Inevitable

#### The US is key to global cybernetic expansion:

#### Epistemologically.

Avila, 20—former Non-Resident Fellow at the Digital Civil Society Lab in Partnership with the Center for Comparative Studies in Race and Ethnicity at Stanford University (Renata, “Against Digital Colonialism,” <https://autonomy.work/wp-content/uploads/2020/09/Avila.pdf>, dml)

Increasingly, there is also a merger of political power and tech power in the US, which is then extrapolated to the rest of the world. A handful of huge corporations, like Amazon Web Services and Palantir, have built a ‘revolving door’ to develop and entrench Silicon Valley’s capacity to expand their services abroad.19 The neocolonial role of international aid takes a new shape, this time as technology, as the revolving door between the most powerful governments in the world and technology companies manifests in global diplomacy. The CEOs of tech companies navigate the world as ‘new envoys’ of digital colonialism – diplomats showcasing the power of their enormous technical empires to heads of state. Often, their revenues are larger than the entire GDP of their countries they are visiting, and their arrival sends a distorted message of prosperity and progress to overcome systemic inequalities and leapfrog into a better future. For many precarious and debt-fuelled governments, it is difficult to reject offers of ‘free’ digital infrastructure and services. In addition, current global trade rules run the risk of consolidating a regime favourable to digital empires, blocking the possibility of smaller actors to innovate and take ownership of their digital futures.

#### Infrastructurally.

Avila, 20—former Non-Resident Fellow at the Digital Civil Society Lab in Partnership with the Center for Comparative Studies in Race and Ethnicity at Stanford University (Renata, “Against Digital Colonialism,” <https://autonomy.work/wp-content/uploads/2020/09/Avila.pdf>, dml)

Early manifestations of this process can be seen in the ‘free’ provision of critical infrastructure – from cables to connectivity – to large populations. This process led to the silent privatisation of the digital infrastructure of entire nations.7 Big Tech CEOs were meeting heads of state, shaking hands and promising alliances for a connected future.8 The most audacious even used Washington as a backdoor to reach places like North Korea, Cuba and China.9 Some nations even opened tech embassies in Silicon Valley, signalling their availability to tech companies, which increasingly behaved like states who provided “aid” and well-intentioned efforts to digitise countries through free infrastructure and services.10 This included proposals to build broadband cables and spread connectivity in remote areas using balloons.11 What started as an aggressive public relations campaign around 2013 has continued discreetly by the five leading tech companies in developing countries across the world, particularly in Africa.

The accelerated penetration of tech companies in emerging markets has taken place not only via generous offers of connectivity and infrastructure to populations. Tech giants have also been providing digital infrastructure to dozens of governments, ranging from cloud services to entire mail and office suites. Amazon and Microsoft have led this process, followed closely by Facebook and Google. The fact that an entire nation delegates its digital services to a company based in Silicon Valley is alarming. The company is then in a position to handle not only highly sensitive government documents, but also is in possession of critical information relating to the entire country.

But national security advisors, parliaments and watchdogs remain largely silent about this new form of dependency aside from a few notable cases where sanctions and political pressure have been deployed. This has included the case of Microsoft providing services to Russian firms;12 Iranian users unable to get security updates from US-based products and services;13 and even deleted accounts on services as vital as GitHub, a platform which hosts code for developers. This is an important reflection on the fragility of a tech industry highly dependent on a US-based ecosystem of products and services, which becomes vulnerable to political vendettas, national security letters and collaboration with security services.14

### AT: IR Good

#### Prefer our theory of power. Modern IR analysis is distorted and the affs ideological diagram of The Stack effectively maps the digital complexities that make up the modern age of geopolitics.

Dyer-Witheford and Matviyenko 2019—associate professor of information and media studies at the University of Western Ontario; assistant professor of communication at Simon Fraser University (Nick and Svitlana, *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*) //ansel

CRITICISM OF ARMS, ARMS OF CRITICISM Our project requires an analysis in terms very different from those of official discussions of cyberwar, and its echoes in the media, discussions often cast in a language that assumes and imposes the inescapable necessity of a technocratic realpolitik and prepares and armors its audiences for trajectories of mounting crisis. Just as, in previous decades, we were habituated to apocalyptic prospects by an anodyne “nukespeak,” so today we are being trained to a more creeping catastrophe by a militarized “cyberspeak” that promises us resilience against hostile intrusion through social media service upgrades, improved smartphones, and the steady surrender of individual and social freedoms to enhanced powers of the security forces. This numbing discourse must be broken open and defamiliarized. The topic of cyberwar has, however, largely been ignored by critical social theorists, sometimes where one would least expect. The most ambitious and sophisticated of all recent scholarly attempts to conceptualize the scope and depth of the internet as a technosocial institution is in our opinion Benjamin Bratton’s (2016) The Stack: On Software and Sovereignty. For Bratton, **the concept of a “stack**” (in computer science, a collection of data elements that must be accessed in a specific order) **provides a metaphor for the architecture of the internet, envisaged as a layered series of terrestrial, platform,** urban, communication, **interface**, and user operations. The combined interactions of **these different digital levels**, Bratton argues, **now compose an “accidental megastructure” of global governance either destabilizing or reinforcing the spatial and temporal boundaries of the nation-state**. Yet what is striking is **the limited attention** **this** otherwise comprehensive, virtuoso **examination of digital networks gives to** that most **sovereign of activities, war, and the possibility** **of** what Bratton (2016, 298) glancingly refers to as “**Stack versus Stack**” conflicts, a topic that he defers as a matter for later study. This is all the more surprising because, as Bratton acknowledges in a footnote, the modeling of the internet as a “stack” of technosocial activities was pioneered within U.S. cyberwar agencies with very nonaccidental strategic agendas (441n8). One of the NSA documents released by Snowden, “Bad Guys Are Everywhere, Good Guys Are Somewhere” (Risen and Poitras 2013; Müller-Maguhn 2014), contains a diagram of the architecture of the internet in terms of an interdependent “stack” of geographical, physical network, logical, cyberpersona, and persona levels, derived from the work of national security intellectual Paul Rosenzweig (2012). The diagram is defined as a tool that enables the NSA to conceive how to scan and disrupt the operations of antagonists at multiple levels: “the stack” is a concept for cyberwar fighting. No account of networked sovereigns and subjects can now postpone reckoning with this reality, so we hope that our book can supplement Bratton’s, even though it is written in a different political register

### AT: Stack=Bad Metaphor

#### Hate to say it, but not our Stack—we reclaim the metaphor via stacktivism.

Lovink, 20—founder of the Institute of Network Cultures at the Amsterdam University of Applied Sciences (Geert, “Principles of Stacktivism,” tripleC 18 (2): 716-724, 2020, dml)

Lately, the concept of “the stack”, once a technical insider term used amongst engineers and geeks[10], has jumped context and transformed into a general container concept, in danger of becoming an empty signifier. As a meta-concept The Stack has been detached from its author and his Californian-nihilist program for the aspirational cool-crowd and turned into a symbol for the need to bring together interrelated crises, from climate change, inequality, AI and automation to covid-19. In Bratton’s world, you sign up from the program and carry the card, otherwise the entry sign points to exit. No affect, behavioural noise or regional ambiguities please – we’re performing Important Theory here. Perhaps this is a form of group therapy for the insecure? That’s fine if you like the taste of testosterone in your milk shake.

This is the time to design one, two, three, indeed many stacks and not to dismiss the ambitious efforts of others because, after all, where are the European antidotes to Bratton or Zuboff? Europe tragically fails in the production of contemporary reference texts, both at the speculative and the critical level. While the late Bernard Stiegler comes in mind, a lot of translation work is still to be done in order to transform his philosophy of technology into workable programs decoupled from his often-obscure neologisms. For instance, where are the counterproposals of the crypto-blockchain system? The Bratton bible, written in the quasi-authoritarian voice of a Master Designer, can also be read from a grass-roots perspective and should be praised for its multi-disciplinary analysis of techno-social (power) practices. Why not be ambitious? There’s a lot at stake. As a proposal, Bratton’s reading of The Stack should be compared to Dante’s hell, Sloterdijk’s notion of the spheres, Deleuze and Guattari’s Mille plateaux, Hui’s cosmotechnics and Stiegler’s The Age of Disruption. But instead of conducting hermeneutic exercises, the proposal here is to transplant the term into the hacktivist context and define the principles of “stacktivism”: dancing stacks[11].

#### Stack design is a useful metaphor.

**Crombie et al. 21**(David, Canadian politician, professor and consultant, “Rethinking the Stack: New Narratives for an Era of Collective Intelligences”, 12.1, CS)

We are neither coders nor engineers but driven by a shared sense that the scope and speed of technological change has literally implicated us – folded us – in the workings of distributed intelligent systems that affect how we relate, speak, work. It is this transformation of our own agency we wish to comprehend, and the emergence of collective intelligences that bring human and non-human agency together in new constellations. While we realize that “stack design” is an abstract design proposition, we want to build on the technical metaphor of the stack as a layered system to facilitate a more holistic systems design conversation – and find out more about the role each of us might play in that process. Stacks are generally defined as “the set of technologies an organization uses to build a web or mobile application ... a combination of programming languages, frameworks, libraries, patterns, servers, UI/UX solutions, software, and tools used by its developers”.2 A quick look at the stacks used by key players in and across the platform economy suggests that these modularized systems have more in common than their fierce competition for users might suggest. Rather than repeating the usual invocations of global brands (and their market power), we want to shift the focus of our conversation to the stacks that sustain the power of these actors – a first step toward a more comprehensive understanding of the relational infrastructures behind data-driven societies, what we have termed the condition of distribution, and a different way of thinking about the design of (fairer) markets for a more cooperative economy.3 Adopting the principle that technology stacks are in principle subject to codesign, we showcase a series of complementary co-design processes to explore how we might best facilitate such a conversation. In these examples, we focus on the role of data – from the data monetization controversy (data-as-right vs data as-commodity) to “platform” cooperatives adding a digital technology and data governance layer to the much older organizational practices of the cooperative. We do not, however, assume a comprehensive understanding of data governance approaches. Our invitation to join the “stack design” conversation begins with a much simpler idea – the search for a narrative (with a wide range of characters and multiple conflicting plots) that might be able to frame a cross-sectoral systems design conversation in which many actors see a role for themselves. So before we turn to technology, we define our non-technological point of departure, leaving the question of where exactly to draw the line between the technological and the non-technological to the side for now. While we are not yet sure what the scope and structure of such a conversation will be, we do know that we want such a narrative to allow us to comprehend the condition of distribution that serves as infrastructural context for the ways in which we live and work.

### AT: State Key To Solve Cyberwar

#### Stacktivism overcomes divisions, pools information, and develops interconnectivity in order to create a digital commons to combat the new era of technological war

**Lovink 20**(Geert, founding director of the Institute of Network Cultures, PhD from the University of Melbourne, “Principles of Stacktivism”, CS)

We need to define new forms of collective action that some call the commons that is defined by the ability to act together. The design question here is what comes next after the model of social networks, which has been so compromised and overshadowed by the social media monopolies. This is a digital commons in which collective forms of money is included, a redistribution of wealth that has been produced together and should never again be allowed to be expropriated. We need to collectivise our knowledge and learn from the mistakes that were made in projects such as Wikipedia and Creative Commons, but also of the self-centric notion of free software as promoted by Richard Stallman, who could only think in terms of individual freedom of the singleuser- as-programmer – until his 2019 downfall. What Bratton’s static metaphysical view in particular lacks is the role of actors (and their interests, ideologies). Instead of trashing the stack, the proposition here is to make the model more dynamic (or dialectical) by introducing stackivism. Let’s define stacktivism as a form of Internet activism that no longer bothers with the distractive noise on social media channels and dares to dig deeper in order to make a real difference. Instead of talking only about upload filters, fake news or the deployment of cheap online moderation armies, we are working on a next Internet. The charm of protocol driven direct action or stacktivism is that it goes both up (from network to platform to stack) and down (protocols, data centres, cables), at the same time. The Internet is more than social media, more than you and your app. This may sound like a simple, self-evident slogan but the integral practice-based vision of stacktivism is a promising one, beyond techno-solutionism and it critics, the liberal-tech engineering status quo procedures, the discontent offline romanticism, liberal privacy concerns, legalistic NGO approaches and the after-the-fact Academic Truth that confines itself to the closed monads of peer-review journals. Stacktivism embodies Adorno’s critique of totality as a lie while climbing up the abstraction ladder in order to enjoy the view. Digitisation Takes Command. The stacktivist dilemma is a classic one: How can the multitudes gain power while pulverizing power at the same time? The digital is now an encompassing global sphere. Is this dark enlightenment in action? In this light, how should we judge the Will to Stack? Dare to think in term of political strategies when talking about cosmotechnics (or cosmic networks, for that matter). We’ve left the era of technology-as-tool far behind us. The nasty feedback machines strike back and try to corner us, suppressing our desires and needs, even without us noticing the closing down of communication and expression. Can The Stack (formerly known as the Internet) only be understood in its totality once it has fallen from its unity and been reduced to fragments (read: geo-political blocks and national webs)? Can we be global in scope on the protocol level, yet act locally in networks of strong-ties? Is it worth to think of cosmotechnics-for-good? Stealing code from the rich and inserting into networks of the poor, in the spirit of Aaron Schwartz and Anonymous’ SkyNet? Do you still believe that another WikiLeaks is possible, beyond the focus on celebrity? **Let’s upgrade and broaden the vision how the** **fight against moral injustices could look like in the age of geo-political cyberwarfare** **and attacks on our critical infrastructure, not just the Internet but water, gas, electricity,** **bridges and hospitals. These are The Stacks of the People, and we’ll better not be naïve about their vulnerability. We depend on The Stack. Making visible and defending critical public infrastructure could be one of the many tasks of stacktivism**.This leaves us with the question how to organise strategic forecasting in times ofcollapse. How can we bring together new forms of collective intelligence that are trulyplanetary in nature, which is to say conflictual and variegated, and not merely designedto replicate Western policy production? Call them organised networks or think tanks,we’re gathering in a closed forum, on Telegram, Mastodon or Signal in order to get **t**hings done, overcoming the divisions that aren’t ours. In theory we have all the communication skills, tools and ideas, yet we often do not know how to organise ourselvesoutside of surveillance capitalism and state control. Ni Zuckerberg, ni Xi Jinping19. Howcan we redistribute critical resources and talents? The need to bring together differentand messy idioms of knowledge (technical, spiritual, cultural, political) is widely felt.What we will do next is act, together. What we need are simple, appealing images,models that bring people together to act.

### AT: Tallinn Manual Good

#### The Tallinn Manual is an ethical and juridical failure.

**Barrett 17**(Edward, Ethics professor in the Department of Leadership, Ethics and Law, “On the Relationship Between the Ethics and the Law of War: Cyber Operations and Sublethal Harm”, CS)

To begin, the manual’s purely legalistic assumptions—derived from applicable treaties and customary international law—can generate ethically problematic definitions of just cause. Functionally, Article’s concept of armed attack and the ethical concept of just cause are the same: they define a casus belli to which one may justifiably respond with lethal defensive force. But the related legal definitions of “uses of force” and “armed attacks” can—from an ethical perspective—lead to both overly permissive and overly restrictive conclusions. Following international law, the manual defines uses of force as acts “that injure or kill persons or damage or destroy objects.” Those of sufficient “scale and effects” are deemed armed attacks. On the one hand, this framework can be too permissive vis-à-vis property. Ethically speaking, large-scale property destruction and damage do not in themselves justify lethal defensive harm; the property in question must be lifesustaining, and this prerequisite is not intrinsic to the definition of armed attack. On the other hand, this framework can be too restrictive vis-à-vis persons. From an ethical perspective, one may respond to unjustified and culpable threats to life with lethal force if necessary; the scale of death is irrelevant. While legally limiting forceful responses to cases of armed attack–level fatalities might promote utility, it also might contravene the moral right of self-defense. This problem accounts for the “contrary view” of the United States following the International Court of Justice’s Nicaragua judgment, which asserted that “any illegal use of force can qualify as an armed attack triggering the right of self-defense; there is no gravity threshold distinguishing illegal uses of force from armed attacks.” In addition to being simultaneously overly permissive and restrictive, legal definitions of just cause can also be arbitrary because of the way in which judgments are made. What counts as harm sufficient to rise to the level of an armed attack is determined through practice, which in reality can mean that the definitions of stronger parties will prevail. Reliance on international law therefore does little to discourage wars initiated by the powerful in defense of “national interests” that merely support a desired standard of living. A dialogue between ethics and international law thus serves to provide necessary critiques of self-serving legal interpretations of both kinetic and cyber operations. A second ad bellum-related flaw in the manual involves the relationship between culpability and just cause. In assessments of whether an armed attack has occurred, the experts were “divided over the issue of whether the effects in question must have been intended.” The minority of experts asserted that espionage “unexpectedly result[ing] in significant damage” should not be considered an armed attack. On the other hand, the majority concluded that “intention is irrelevant in qualifying an operation as an armed attack and that only scale and effects matter.” According to their analysis, victims of unintentional grave harm would possess a right to respond in kind, if necessary. But from an ethical perspective, on the relationship between the ethics and the law of war majority’s position is erroneous. Culpable acts are those done intentionally, freely, and with knowledge or vincible ignorance of the relevant normative and empirical facts; and only culpable murderous acts compromise one’s capacity for justice and dignity to the degree required to forfeit one’s right to life and incur liability to lethal defensive harm. Although the response advocated by the manual’s majority would be excused if the victim were unable to know that the act was unintended, the response would still not be justified. Third, the discussion of ad bellum proportionality is problematic primarily because it misunderstands the criterion, which requires that the total expected good caused by a war outweighs the total expected harm. Instead, the manual asserts that the issue at hand is “how much force . . . is permissible once force is deemed necessary” (that is, once last resort has been satisfied), and concludes that the proportionality criterion limits this amount to “that required to end the situation that has given rise to the right to act in self-defense.” In other words, the manual stipulates that the ad bellum criterion of proportionality, instead of ensuring that the goods at stake are commensurate with anticipated harms, requires one to use only a necessary amount of force to put an end to the situation. One can easily imagine a case in which this leads to massive defensive retaliation to stop a much less harmful attack. Additionally, the entire analysis is misplaced, as the imperative to use only necessary amounts of force is an in bello issue. Fourth, the manual’s treatment of when temporary functionality losses would qualify as a just cause is self-contradictory. Like kinetic weapons, cyber weapons can physically destroy or damage computers. But because of their potential to be transitory or reversible, cyberattacks can also merely compromise functionality. While permanent losses of functionality can create the same effect as physical destruction, temporary functionality losses are unique to cyber operations and require additional analysis. Part of the manual’s discussion on functionality occurs in the in bello section that defines a cyberattack. Associating attacks on objects with damage or destruction, the majority asserted that interference with functionality would qualify as damage and thus constitute a use of force only if “restoration of functionality requires replacement of physical components.” Accordingly, a transitory or reversible loss of function not requiring the replacement of physical components would constitute neither an attack nor, by extension, a just cause. But elsewhere in the manual some experts argue that actions not resulting in physical damage would qualify as an armed attack if the ensuing negative effects were—although others still maintain that direct “harm to persons or physical damage to property” is a precondition for an armed attack. Ethically speaking, justified responses would be a function of both an attack’s culpability and overall effects. Assuming culpability, a temporary loss of the functionality of a system that was not physically damaged would be a casus belli if the event resulted in death, for example, in the event of the temporary disabling of an air traffic control system that caused mass casualties. Fifth, from an ethical perspective, although the manual’s treatment of in bello proportionality is excellent, it could be improved in one way: Since civilians on both sides retain all of their rights, one should not dismiss consequences such as loss of email or banking services from collateral damage calculations. Of course, such costs could be awarded relatively low values. Sixth and finally, the manual unfortunately adopts a purely legal approach to targeting nonparticipating civilians, arguing that cyber operations that do not qualify as “uses of force”—ones that merely inconvenience—may be intentionally directed against civilian objects such as computers. Interference with functionality is permitted if physical repair or operating system reinstallation is not required. Data, related or unrelated to functionality, is also targetable. Large-scale email blockage also does not qualify as an attack. Additionally, and as mentioned earlier, none of these harms need to be minimized or considered in collateral damage proportionality assessments. That these conclusions follow logically from their premises demonstrates the danger of purely legal approaches. From an ethical perspective, intentionally harming civilians, in addition to usually being strategically ineffective, is unjust. In peacetime or wartime, persons who have not culpably transgressed the rights of others have forfeited none of their own, and are not liable to any degree of harm—not even the inconveniences described above. Accordingly, domestic and international statutes should define these injustices as punishable crimes, and appropriate executive and legislative oversight should be implemented. And if nonparticipating civilians are to be affected by cyber operations before or during war, these effects must be minimized and weighed in the ways currently associated with, respectively, economic sanctions and dual-use objects.

## Alternative Methods/Theses

### Mediation

#### We begin our analysis at the medium, the aesthetic space that separates the human from the nonhuman world. Cybernetics has changed the altered the field of our medialogical relationship with the world around us. Our desires, fears, affects, are embedded within the network of the technosphere – In the face of this we look to *radical mediation*. We look to the middle. To the infinite, chaotic, flux of the world as a lens imbued with radical potential. This radical aesthetic dwells in the gap between subject and object, individual and milieu. Only through this interjection can we move to openness and dismantle the cybernetic drive towards complete interconnectivity.

Grusin 2015 (Richard Grusin, English, University of Wisconsin-Milwaukee, “Radical Mediation”) //ansel

**I develop the concept of radical mediation in order to make related but independent arguments about the dualistic character of mediation in Western thought**. I argue that although media and **media technologies have operated and continue to operate epistemologically as modes of knowledge production**, th**ey also function technically, bodily, and materially to generate and modulate individual and collective affective moods or structures of feeling among assemblages of humans and nonhumans**.6 This affective mediation of collective human and nonhuman assemblages operates independently of (and often more efficaciously than) the production of knowledge.7 Like the way media operate affectively, mediation must also be understood ontologically as a process or event prior to and ultimately not reducible to particular media technologies. Mediation operates physically and materially as an object, event, or process in the world, impacting humans and nonhumans alike. Radical mediation participates in recent critiques of the dualism of the Western philosophical tradition, which make up what I have elsewhere called the nonhuman turn in twenty-first-century studies.8 Indeed, as I suggest in the essay’s final sections, radical mediation might in some sense be understood as nonhuman mediation. I derive the term radical mediation from the concept of radical empiricism set forth by William James in Essays in Radical Empiricism, published in 1912, two years after his death.9 James’s radical empiricism has been redeployed in recent books by Adrian Mackenzie and Anna Munster in order to make sense of the technical and embodied experience of our current media environment, what Mackenzie calls “wirelessness” and Munster characterizes as the “anaesthesia of networks.”10 Both books start from James’s paradigmatic definition of radical empiricism in “A World of Pure Experience”: To be radical, an empiricism must neither admit into its constructions any element that is not directly experienced, nor exclude from them any element that is directly experienced. For such a philosophy, the relations that connect experiences must themselves be experienced relations, and any kind of relation experienced must be accounted as ‘real’ as anything else in the system. 1

**In developing** the concept of **radical empiricism James means to reject both the empiricism or realism that starts with objects or the real in itself and the rationalism or idealism that sees the real as an imperfect manifestation of a universal logos or spirit**. **In so doing he also means to insist on the affectivity of relations and the reality of affect**, in a way that I take as consonant with the famous claim in The Principles of Psychology that we do not cry because we are sad but we are sad because we cry.12 For James “ordinary empiricism,” despite “the fact that conjunctive and disjunctive relations present themselves as being fully co-ordinate parts of experience, has always shown a tendency to do away with the connections of things, and to insist most on the disjunctions.” On the other hand, rationalism, to counter empiricism’s dismissal of relations, has sought “to correct its incoherencies by the addition of trans-experiential agents of unification, substances, intellectual categories and powers, or Selves.”13 James’s alternative to the debate between empiricists and rationalists suggests a promising way to move past current debates about objects and relations, or ontology and politics. Object-oriented ontologists like Graham Harman insist on the disjunction between objects, their “withdrawal” from contact with other objects, and thus the separation of ontology from politics.14 Contemporary and historical Marxists, not unlike rationalists, introduce “trans-experiential agents of unification” like capital or capitalism to hold together disparate and unrelated objects or practices.15 By starting with experienced relations, and insisting that “any kind of relation experienced must be accounted as ‘real’ as anything else in the system,” **James would start in the middle, in** what he famously called in the 1890 Principles of Psychology “**the blooming, buzzing confusion” of the world**.16

With radical mediation I too would start in the middle. By taking James’s radical empiricism as a source for the concept of radical mediation, we just need to substitute mediation for “relation” and immediate for “real” to retain a sense of James’s meaning in the new term: “the [mediations] that connect experiences must themselves be experienced [mediations], and any kind of [mediation] experienced must be accounted as [‘immediate’] as anything else in the system.” Where James is concerned with the empirical reality of relations, my concerns start with the immediacy of mediation. James describes relations primarily as connecting experiences. I see mediations as generating, refashioning, and transforming experiences as well as connecting them, similar to what Bruno Latour calls “translations” or Karen Barad describes as “intra-actions.”17 Mediations are always remediations, which change or translate experiences as well as relating or connecting them. I substitute mediation for James’s relation to emphasize that while radical empiricism insists on the reality of experienced relations, radical mediation also insists upon an immediacy that transforms, modulates, or disrupts experienced relations. Radical mediation challenges what Barad calls representationalism: “the belief in the ontological distinction between representations and that which they purport to represent” (MU, p. 46). In these traditional representationalist accounts, mediation is understood to come between, or in the middle of, already preformed, preexistent subjects or objects, actants or entities. The role of mediation in such accounts is precisely to connect, or negotiate between, actants, categories, and events (or subjects and objects), which would otherwise have no way of understanding or interacting with one another. Especially in post-Hegelian, Marxian thought, mediation has been opposed to immediacy, functioning as what might be called an agent of correlation, which filters, limits, constrains, or distorts an immediate perception or knowledge of the world or the real.18 **Mediation** **has** in these accounts **been understood both as enabling our knowledge of reality** **and as preventing or making impossible the direct** and immediate **relation with the world** that Brian Massumi (and others) insist upon as a fundamental component of human and nonhuman experience. In many traditional philosophical accounts **we cannot experience the world** directly or immediately **because we cannot know the world without some form of mediation**.

Although Massumi has at times taken issue with the concept of mediation, I want to follow his claim that “philosophical thinking must begin... immediately in the middle” by suggesting that we understand mediation itself as a place to begin.19 As articulated in different ways in the nineteenth- and twentieth-century American tradition by Ralph Waldo Emerson, Henry David Thoreau, Charles Sanders Peirce, or James, or in the twentieth and twenty-first centuries by Alfred North Whitehead, Gilbert Simondon, Gilles Deleuze, Massumi, or Barad, where we begin is immediately in the middle.20 Mediation should be understood not as standing between preformed subjects, objects, actants, or entities but as the process, action, or event that generates or provides the conditions for the emergence of subjects and objects, for the individuation of entities within the world. Mediation is not opposed to immediacy but rather is itself immediate. It names the immediacy of middleness in which we are already living and moving: “Where do we find ourselves?” Emerson asks in the opening of his famous essay “Experience” and then answers: “In a series of which we do not know the extremes, and believe that it has none. We wake and find ourselves on a stair; there are stairs below us, which we seem to have ascended; there are stairs above us, many a one, which go upward and out of sight.”21 In asking where we find ourselves, Emerson is asking where the world and its nonhuman entities find themselves as well. In developing the concept of radical mediation I operate from a sense that where we find ourselves (both at the beginning of the twenty-first century and in human and nonhuman history more generally) is immediately in the middle, in mediation itself.

Remediation I have been thinking and writing about the history and theory of mediation for twenty years—most notably in my work on the logics of mediation in the late twentieth and early twenty-first centuries. I have also been concerned throughout this work with thinking through in various and partial ways the ontological status of mediation.22 In the nearly twenty years since “Remediation,” I have included the ontological and affective reality of mediation among the methodological premises of my work.23 Building upon Latour’s distinction between intermediaries and mediators, in which mediators are not neutral means of transmission but actively involved in transforming whatever they mediate, I insist that **mediation** **operates** not by neutrally reproducing meaning or information but **by actively transforming human and nonhuman actants, as well as their conceptual and affective states**. Thus, the concept of radical mediation helps make sense of how in the twenty-first century media and mediation operate within the world as objects or events no different from any other and how their contemporary operation lets us see some things about mediation that have often been obscured. This concept of radical mediation departs from the way mediation has been used in Western thought at least since Immanuel Kant and G. W. F. Hegel, but more likely going back to Aristotle—although as a literary critic turned media theorist, I hesitate in making definitive assertions about the history of the Western philosophical tradition. The history of philosophy notwithstanding, I am concerned with interrogating the way in which mediation has been conventionally defined and deployed as a secondary concept or category, as something that enters the scene belatedly, after humans and nonhumans, representation and reality, or culture and nature have already been divided up and parceled out.

Although remediation has not always been recognized as doing so, from very early on I have understood it to be making a case for the experiential immediacy of mediation. Perhaps this concern has not been evident because remediation’s double logic divides immediacy from hypermediacy in a formal sense, having to do with the visual aesthetics of the screen, its composition and design. As half of the double logic of remediation, the logic of transparent immediacy imagines a form of visual mediation in which the medium erases itself so that there is an immediate subjective encounter with, or apprehension of, the object of mediation, or the real. **This visual logic of transparent immediacy can now be seen as** a version of what, following the terminology of speculative realism, **we might call media correlationism, in which mediation functions as the necessary intermediary between human agents and the nonhuman world**. As half of the double logic of remediation, transparent immediacy holds that **the subject’s contact with the real depends upon the erasure of the medium**, which correlates **and thereby obscures the relationship between subject and world**. Hypermediacy, on the other hand, refers to the proliferation of media forms and practices. From a media correlationist standpoint, therefore, hypermediacy would seem to block or prevent the erasure of the medium that defines transparent immediacy. From the perspective of radical mediation, however, hypermediacy does not prevent immediacy but rather constitutes it—not through the erasure of an intervening visual medium but through the immediacy of mediation itself. By using remediation I emphasize the point that both logics are at play in mediation, that the double logic of remediation entails both the transparency of media correlationism and the obscurity of radical mediation, and that these two different concepts of mediation are just as contradictory as immediacy and hypermediacy are. But remediation deploys the concept of immediacy in another way as well, which moves toward what I am defining here as radical mediation. In addition to referring to a formal style or logic of visual mediation in which all signs of mediation are erased or concealed**, immediacy is also used in remediation to refer to the embodied, affective experience that comes both from the direct encounter with the real provided by transparent mediation and from the immediate encounter with mediation** provided by hypermediated modes of mediation. Remediation tried to underscore the phenomenal or experiential aspects of mediation by mobilizing Derrida’s argument in “Economimesis” that mimesis is not about the resemblance between a representation (or mediation) and its object, but a relation between “two producing subjects.”24 With premediation, I developed the affective immediacy of mediation further in terms of Maurice MerleauPonty’s contention that the optic is an extension of the haptic, claiming that because all bodily senses are haptic, mediation is as well (readers of Marshall McLuhan will undoubtedly hear echoes of his claim that print is visual, while electric media are haptic). As Silvan Tomkins and Daniel Stern help us to understand, our interactions with media are always affective, and media themselves can be said to possess affective lives.25 And as I have argued elsewhere in relation to the 2011 Sendai earthquake and its consequent tsunami and technical catastrophes, **the affectivity of media aftershocks caused by the quake must be understood to have the same ontological immediacy as its geotechnical aftershocks**.26 To understand radical mediation as affective and experiential rather than strictly visual is to think about our immediate affective experience of mediation as that which is felt, embodied, near—not distant from us, and thus not illuminated or pictured, but experienced by us as living, embodied human and nonhuman creatures. Where remediation focused largely on the visual aspects of mediation, **radical mediation would take into account the entire human sensorium. For radical mediation, all bodies (whether human or nonhuman) are fundamentally media and life itself is a form of mediation**.27 As Benjamin had similarly noted about mechanical reproduction, the remediation of new digital media has worked to bring our media devices nearer our bodily medium, engaging us directly in what I have elsewhere characterized as the affective life of media.28 **The core of radical mediation is** its immanence, immediacy itself—not the transparent immediacy that makes up half of remediation’s double logic but **the embodied immediacy of the event of mediation**. In our affective, bodily interactions with media devices, indeed with the world of humans and nonhumans, there is no distance or perspective from which to see immediacy, from which immediacy could be made into something one could paint or draw or re-present, or something that needed mediation. “**Bodies**,” writes Barad apropos the invertebrate brittlestar, “**are not situated in the world**; **they are part of the world**” (MU, p. 376). Interestingly Emerson makes a similar point in “Nature” when he includes “all other men and my own body” under the category of “NATURE” or the “NOT ME.”29 The same claim, I would aver, can be made for media and mediation as well. In theorizing the affective embodiment of radical mediation, **we should attend to the immediate affective experience of mediation itself**. But to suggest that mediation is immediate is to swim against a strong popular current running through the history ofWestern thought, one which would categorically distinguish mediation from immediacy, a distinction that both remediation and premediation set out to challenge and that is further problematized by the concept of radical mediation.

### Borderless Cosmopolitanism

#### Tag 1 – RAID THE ARCHIVE

#### Tag 2 – The spectre of the non-western Other haunts the resolution, inducing an ethos of total control for the western subject through top-down risk management. NATO, at its core, a question of borders, as the west artificially cordons off those deemed worthy of being and those to be deprived. Vote aff to affirm borderless cosmopolitanism, a rupture in the crystallized western archive that embraces instability to render oneself ungovernable by the LIO’s sovereign authority. <This conceptual power hinges on the order and stability of its security state. The so-called neutrality of the closed system of debate through fairness, predictability, and stasis is not benign but rather a violent fidelity to the ordered security paradigm of territorialization.>

Mbembe 18 (Achille, research professor in history and politics at the Wits Institute for Social and Economy Research at the University of the Witwatersrand. “The idea of a borderless world”) //ansel

\*modified for gendered language

As the 21st century unfolds, a global renewed desire from both citizens and their respective states for a tighter control of mobility is evident. Wherever we look, the drive is towards enclosure, or in any case an intensification of the **dialects of territorialisation** **and deterritorialisation**, a dialectics of opening and closure. **The belief that the world would be safer, if only risks**, ambiguity **and uncertainty could be controlled** and if only identities could be fixed once and for all, **is gaining momentum. Risk management techniques are increasingly becoming a means to govern mobilities**. **In particular the extent to which the biometric border is extending into multiple realms, not only of social life, but also of the body, the body that is not mine.**

I **would like to pursue this line of argument concerning the redistribution of the earth**. Not only through the control of bodies but the control of movement itself and its corollary, speed, which is indeed what migration control policies are all about: controlling bodies, but also movement. More specifically I would like to see whether and under what conditions we could re-engineer the utopia of a borderless world, and by extension, a borderless Africa, since, as far as I know, Africa is part of the world. And the world is part +of Africa.

It is important to attend once again to what is obviously a utopian intent, the question of a borderless world. From its inception “movement” or more precisely “borderlessness” has been central to various utopian traditions. The very concept of utopia, refers to that which has no borders, beginning with the imagination itself. **The power of utopianism** lies in its ability to instantiate the tension between borderlessness, movement and place, a tension—if we look carefully—**that has marked social transformations in the modern era**. This tension continues in contemporary discussions of movement-based social processes, particularly international migration, open borders, transnationalism and even cosmopolitanism. In this context, **the idea of a borderless world can be a powerful** albeit problematic **resource for social, political and even aesthetic imagination**. Because of the current atrophy of an utopian imagination, apocalyptic imaginaries and narratives of cataclysmic disasters and unknown futures have colonised the spirit of our time. But what politics do visions of apocalypse and catastrophe engender, if not a politics of separation, rather than a politics of the humanity, as species coming into being? Because we inherit a history in which the consistent sacrifice of some lives for the betterment of others is the norm, and because these are times of deep- seated anxieties, including anxieties of racialised others taking over the planet; because of all of that**, racial violence is increasingly encoded in the language of the** **border and** **of** **security**. As a result, contemporary borders are in danger of becoming sites of reinforcement, reproduction and intensification of vulnerability for stigmatised and dishonoured groups, for the most racially marked, the ever more disposable, those that in the era of neoliberal abandonment have been paying the heaviest price for the most expansive period of prison construction in human history. I refer to the prison here, the carceral landscapes of our world, precisely as the antithesis of movement, of freedom of movement. There is not a more dramatic opposition to the idea of movement than the prison. And the prison is a key feature of the landscape of our times.

In proposing to re-examine the question of a borderless Africa and a borderless world, I would like to stay away from dominant ways with which this issue has been dealt. That is under the sign of Kant and his promise of unbounded cosmopolitanism, and under the sign of liberal individualism understood as an antidote or to the deeply ingrained fascist impulses of European governance and bureaucracies. Although they seem to be worlds apart, both of these approaches are articulated around the concept of the fourth freedom.

In classical liberal thought there are three core freedoms: First of all, freedom of movement. Within freedom of movement, there is freedom of movement of capital, priority number one. But, since there is no capital without goods, there is freedom of movement of goods. Number three is services, and especially in these times of ours, the freedom of movement of those who can provide services. Those are the three core freedoms. So the concept of the fourth freedom has to do with freedom of movement of persons. Traditional engagements with the idea of a borderless world aimed at precipitating the advent of that fourth freedom. Within that configuration a borderless world would be a world of free movement of: capital, goods, services and persons. Such movement, such freedom of movement would not be restricted to the core economically rich countries or states, which is the case as we speak. The Schengen system, for instance, is limited to the core European countries. In fact, **if you have an American passport you can basically go wherever you want. The world belongs to you**. But this is not the case for every inhabitant of our planet. So in the configuration I have just referred to, the fourth freedom, the ability to move around the planet would no longer be limited to Europeans and Americans. It would be a radical right that would belong to everybody by virtue of each and every individual being a human being. It is a right that would be extended to poor members of the earth. So we keep going back to the question of the earth. There would be no visas, in some instantiations of the fourth freedom of movement there would be no quotas, and no bizarre category to fill in, because you would not even have to apply for a visa. One could just get on a plane, a train, a boat, on the road, or on a bike. Rights of non-discrimination would be extended to all. I will give you one little example. In Cameroon, until the beginning of the 1980s, it was possible to travel to France with one’s national identity card. Most people went to France and came back. They did not go because they wanted to settle there. Most people want to live where they “belong”. But they want to be able to come and go. And they are more likely to come and go when the borders are not hermetically closed. So,  a borderless world imagined by the fourth freedom of movement is premised, therefore on this right of non-discrimination and on this circulatory and pendular set of migrations.

To elucidate or pose differently the question of a borderless world, is to contrast two paradigms. On the one hand, examine the liberal idea of a borderless world through the free movement concept and contrast it with African precolonial understandings of movement in space. Contrasting these two paradigms will hopefully give us conceptual resources to expand on this utopian project of a borderless world.

When I say liberal classical thought, of course it is extremely complicated, we understand that. I am giving you an archetype, which itself needs to be properly deconstructed. And here I will rely in particular on a recently published work called Movement and the Ordering of Freedom published by Hagar Kotef, an Israeli scholar who teaches at School of Oriental and African Studies  in London. You might let your imagination work and understand why it is an Israeli who is interested in this. What Kotef shows in that work is the extent to which liberal political thought has in fact always been saddled with a contradiction when it comes to imagining the possibility of a borderless world. Her argument is that this contradiction stems from its conception of movement. She shows that, in fact, two dominant configurations of movement constantly come into conflict with one another, cancelling each other at times within classical liberal thought. **Movement** here **is seen** both as a manifestation of freedom and as an interruption, **as a threat to order**. **One of the functions of the state is, therefore, to craft a concept of order, stability and security** that is reconcilable with its concept of freedom and its concept of movement. **That is the contradiction**. Kotef argues, **the liberal classical state is the enemy of people who restlessly move around**.  **Such people are configured as an unassimilable other**. You cannot assimilate them. **They are constantly on the move**. There are colonial repercussions to all of this. The biggest problem of **the colonial state in** the continent of **Africa** from the 19th century onwards was to make sure people stayed in the same place. It **had a hard time achieving this**. They were constantly on the move. **They were “uncaptured**”.

So, the business of the state is how to capture them. Without capturing them, sovereignty does not mean anything. **Sovereignty means you capture a people, you capture a territory**, you delimit borders and this allows you, in turn, to exercise the monopoly of territory, of course, monopoly over the people and in terms of the use of legitimate force and, very importantly—because everything else depends on that—monopoly over taxation. **You cannot tax people who have no address**. The state sees such people as enemies, both of freedom, because they do not exercise it with restraint, and of security and order**. You cannot build an order on the basis of that which is unstable**.

The same state is a friend of self-regulated movement. Why? Because freedom here is understood as being about moderation, about self-regulation. It’s not about excess—excessive movement immediately conjures problems of security. So, as Kotef argues, movement not only has to be restrained via an array of disciplinary mechanisms, it has to be reconciled with freedom and to some extent self-restraint, but the ability to restrain or regulate oneself is not assumed to be the share of all subjects. Not everybody is able to restrain ~~him- or herself~~ themself. **Some movements were therefore configured as freedom, and others were** deemed improper and were **conceived as a threat**. That is the bifurcation we have in classical liberal thought**. It is the spectre that haunts classical liberal states**, from those years up to now. We have not gotten rid of that spectre.

The way in which classical liberal states have tried to resolve this contradiction has been by managed mobility, which is back on the agenda right now as I speak, in Europe and even in South Africa where I have been doing some work with the Department of Home Affairs on recalibrating inter-African migrations. The key concept is “managed mobility”. So, within the framework of managed mobility, certain categories of the population are constantly seen as posing a threat, not only to themselves and to their own security, but also to others’ security. Such a threat, it is thought, can be diminished if their movements are confined and if they are domesticated and subject to some type of reform.

In the classical liberal model security and freedom came to be defined as a right of exclusion. Order within that model is about securing the unequal ordering of property relations. Asserting the boundaries of the nation goes hand in hand in that model with the assertion of the boundaries of race. Now, defining the boundaries of race within that model requires a proper definition of the boundaries of the body; the centrality of the body in the calculus of both freedom and security.

First of all, let me say that **pre-colonial Africa** might not have been a borderless world, at least in the sense in which we **have** been defining borders, but where the existing **borders** were **always porous and permeable**. The **business of a border is, in fact, to be crossed**. That is what borders are for. There is no conceivable border outside of that principle, the law of permeability. As evidenced by traditions of long-distance trade, circulation was fundamental. It was fundamental in the production of cultural forms, of political forms, of economic and social and religious forms. The most important vehicle for transformation and change was mobility. It was not class struggles in the sense that we understand it. Mobility was the motor of any kind of social or economic or political transformation. In fact, it was the driving principle behind the delimitation and organisation of space and territories. So the primordial principle of spatial organisation was continuous movement. And this is also still part of present day culture. **To stop is to run risks. You have to be on the move constantly. More and more, especially in conditions of crisis, being on the move is the very condition of your survival. If you are not on the move, the chances of survival are diminished**. So **dominance over sovereignty was not exclusively expressed through the control of a territory, physically marked with borders**. It was not.  How was it then? **If** **you do not control a territory, how** **can you exercise sovereignty**? How can you extract anything, since as far as we know, power expresses itself also, if not primarily, through one or the other form of extraction.

All of that was expressed through networks. Networks and crossroads. The importance of roads and crossroads in African literature is astounding. Read Soyinka, read Achebe, read Tutuola. Roads and crossroads are everywhere in their literature. So crossroads, flows of people and flows of nature, both in dialectical relationships because in those cosmogonies people are unthinkable without what we call nature. So while the Anthropocene’s turn seems to be a novelty in parts of our world today, we have always lived in that. It is not new. Because you cannot think of people, without thinking of nonhumans. Read Tutuola, it is a world of humans and non-humans, interacting, acting with others. I do not want to exaggerate this. Fixed geographical spaces, such as towns and villages did exist. People and things could be concentrated in a particular location. Such places could even become the origin of movement and there were links between places, such as roads and flight paths, but places were not described by points or lines. What mattered the most was the distribution of movement between places. Movement was the driving force of the production of space and movement itself, if we are to belief some of those cosmogonies. Here I have in mind the Dogon cosmogonies that were particularly studied by Marcel Griaule, or other cosmogonies in Equatorial Africa dealt with by anthropologists and historians like Jan Vansina, John M. Janzen and others. Movement itself was not necessarily akin to displacement. What mattered the most was **the extent to which flows and their intensities intersected** and interacted **with other flows**, the new forms they could take when they intensified. Movement, especially among the Dogon, could lead to diversions, conversions and intersections. These were more important than points, lines and surfaces, which are, as we know cardinal references in western geometrics. So, what we have here is a different kind of geometry out of which concepts of borders, power, relations and separation derive.

If we want to harness alternative resources, the conceptual vocabulary type, **to imagine a borderless world**, **here is an archive**. It is not the only one. **But what we harness are the archives of the world at large, and not only the western archive**. In fact, the western archive does not help us to develop an idea of borderlessness**. The western archive is premised on the crystallisation of the idea of a border**.

## Framework

### Notes

This strategy against framework is centered around reasonability. This might seem odd with a K aff—most people don’t read K affs to be topical in the first place, so reasonability doesn’t come up nearly as much. However, I think it’s a pretty underutilized strategy that, with a lot of practice and explicit judge instruction, can appeal to a lot of more policy-leaning judges, because it lets you translate it into terms that make sense to them.

The most important thing to make clear is that this isn’t the same reasonability argument that you’d make with a policy aff against a T argument, because you can’t really pass off your interpretation as “reasonable”—at least, not in the same sense as a policy interpretation. Instead, you should **explicitly instruct** the judge to **choose** to decide that your interpretations are reasonable readings of the resolution, **even if they don’t think that our interpretations are the “true” definition of the word at hand**. Your offensive argument for why this is a good way for the judge to evaluate T debates (or, at least, the T debate that you are having) is that choosing to race to the “truest” interpretation enables the operations of cyberwar even if individual debates seem like they might be able to resist those operations, because the essence of cyberwar is redefining truth itself (editing the value of bits of information in computers to send false or faulty messages). Every attempt to establish a particular definition as “true” over the course of time has some militarized dimension; it’s just a question of how much. Thus, choosing to read seemingly unreasonable interpretations of the resolution as “reasonable” feeds faulty data into the algorithm and interrupts this process, if only a little bit.

You should only read the counter-interpretations that make sense based on the 1NC! Obviously these cards are pretty long! If you only had time to read one card (besides Joque, the reasonability card), I would read Collier, because it also references the US and NATO and says “cooperate.” **Don’t prioritize reading cards** (that’s why there aren’t many)—the 1AC has a lot of framework tricks and arguments built in. Use those!

### C/I—Cybersecurity—2AC

#### Cybersecurity is “the security of the environment formed by physical and non-physical components and characterised by the use of computers and other networked devices.” Debates about US-NATO security cooperation are more accurate when they theorize states as assemblages rather than unitary actors.

Collier, 18—Cyber Security DPhil Candidate based at the Department of Politics and International Relations, and the Centre for Doctoral Training in Cyber Security, University of Oxford, formerly worked at the NATO Cooperative Cyber Defence Centre of Excellence (Jamie, “Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision,” Politics and Governance, Volume 6, Issue 2, July 2018, dml)

Refreshed thinking is required to better understand the provision of cyber security and the configuration of cyber security actors. Here, the term cyber security is defined as the security of the environment formed by physical and non-physical components and characterised by the use of computers and other networked devices. Cyber security actors, by definition, provide security in some capacity. Yet this does not mean that all actors strive to achieve a single, unitary concept of security. The prevalence of private actors means that cyber security is often provided by actors who prioritise other commercial objectives over security. Encryption disputes between the US government and technology firms show that different actors have altogether different motivations.

This makes the study of the different cyber security providers, and how they interact with one another essential. The concept of global cyber security assemblages provides a conceptual anchor that provides a means for further understanding these issues. The term provides a more appropriate concept for understanding contemporary cyber security contexts when compared to more traditional frameworks. The security assemblage term refers to new hybrid structures that are often simultaneously public and private, global and local. The use of the term is part of an emerging body of scholarship within IR literature that seeks to empirically assess complex structures where a range of different global and local, public and private security agents, interact, cooperate and compete to produce new institutions, practices and forms of security governance that cannot be captured neatly though the boundaries of nation states (Abrahamsen & Williams, 2011; Williams, 2016).

The assemblage concept therefore moves away from the traditional centre of the nation-state to multi-layered, networked configurations that are able to accommodate a range of entities including (inter)governmental, para-governmental, nongovernmental, and private organisations (Voelkner, 2013). The boundaries of an assemblage can be drawn in alternative ways to the traditional contours of national borders. They can be drawn to examine the provision of security within a territory but can also be used to examine security or governance contexts that are inherently international. The issue of internet governance, for example, comprises a global assemblage of actors, albeit one dominated by US actors (Carr, 2014). Perhaps the most defining characteristic of the assemblage concept is therefore an accommodation of the forces of globalisation and a scepticism of rigid borders and distinctions. Of course, much of the above relates closely to other terms including actor network theory; indeed, the difference between the terms is one of emphasis, rather than kind (Acuto & Curtis, 2014) with the similarities and differences between the two concepts discussed in greater detail elsewhere (Acuto & Curtis, 2014; Müller & Schurr, 2016).

For the purposes of understanding cyber security provision, it is the notion of assembly and disassembly— where actors relinquish, transfer and develop capacities and functions—that is central to the added value of the assemblage concept. As security functions emerge and are captured by either public or private actors, actors assemble greater capabilities and responsibilities. As private actors increasingly take on strategic, ethical, and foreign-policy alignment issues that were previously outside their purview, they are assembling into more political actors. Conversely, as aspects of cyber security are increasingly regulated and managed by states, other aspects of private actors’ capabilities and responsibilities are disassembling. Contemporary cyber security practices are replete with these instances of assembly and disassembly. Assemblage thinking therefore pays attention to the instability of security networks. While cyber security is provided by a vast array of actors, assemblage thinking also highlights the contestation related to the roles and responsibilities of security actors. In light of emerging and shifting actors, the point is not to demonstrate that states are stronger or weaker. Rather, the intention is to examine the complex configuration of actors that maintain contingent and multifaceted relationships with each other (relationships that cannot be captured by static and often state-centric theories). Cyber security is replete with global and local, public and private agents whose relationships are deeply competitive as well as cooperative, conflictual, and at times coordinated. While the concept of a security assemblage has been applied to cyber security in previous literature (Stevens, 2012, 2016, pp. 181–186), the argument for why and how the concept should be used and applied to cyber security remains underdeveloped—an imbalance this article hopes to correct.

These hybrid structures are clearly observed through contemporary examples with the cyber security of critical national infrastructure (CNI) in the UK a case in point. The vast majority of CNI is owned and managed by corporations—itself a broad church that includes a variety of actor types including not-for-profit community owned private limited firms, regional and UK-based firms, multinational firms (National Grid operates in both the US and UK for example, probing traditional global-local distinctions) and state-owned or quasi-state owned firms (the now approved Hinkley Point nuclear plant will be owned and managed by a combination of French-state majority owned EDF energy and Chinese state-owned China General Nuclear Power Corporation) (Ward, Pickard, & Stothard, 2016). As a collective, these corporations cannot neatly be categorised as ‘private’ given the variety of entities including the presence of both partially and fully state-owned entities. Corporations provide cyber security alongside a range of government departments, including GCHQ and its subsidiary, the National Cyber Security Centre (NCSC); the Cabinet Office, the various government departments that are largely responsible for infrastructure related to their department and related institutions such as the Centre for the Protection of National Infrastructure (Collier, 2016). All of these government entities have their own identities, agendas and motivations—a reality that means that ‘the government’ is not necessarily a coherent entity at all. Adding to the plethora of actors are various international organisations and multilateral bodies. Various actors work together within this cyber security assemblage, often in unusual ways. With Chinese-based firm Huawei providing communication equipment for CNI organisations, GCHQ employees will routinely monitor, take apart and inspect the equipment supplied (due to security concerns) at a centre that is itself funded by Huawei (Rifkind, 2013; Rosenzweig, 2013).

An assemblage approach also considers the normative agendas behind the traditional categories and distinctions used in IR literature. Pursuing assemblage thinking means paying attention to the relationships between a variety of actors and the forces that impel them to act in the way they do (Lisle, 2013). The process of assemblage formation is not neutral but deeply political. Different actors have clashing views on what aspects of cyber security should be ‘public’ or ‘private’ as well as where the boundaries of these distinctions lie. Returning to the UK example, the UK 2016 Cyber Security Strategy declared that market based solutions to cyber security have ‘not produced the required pace and scale of change’, meaning that ‘Government has to lead the way and intervene more directly by bringing its influence and resources to bear’ in a move that overtly seeks to increase the government’s cyber security purview (HM Government, 2016). On the other hand, governments have also sought to relinquish both their authority and responsibility of cyber security issues within other contexts in order to avoid the backlash of security failings (Carr, 2016). This is also observed in recent US encryption disputes that reflect broader political disagreements about the agency afforded to different actors. Law enforcement organisations’ interests in accessing intelligence on devices clash with technology firms who instead seek to protect their customers’ data from government access, (albeit while simultaneously selling user data to other businesses and using it themselves for the purposes of targeted advertisements). Various government entities compete with each other for ownership of cyber security and the tax revenue that accompanies the issue. Alternative visions of cyber security are proposed within such intra-governmental competition—the issue may be framed through a military, business or criminal prism depending on the government entity that seeks to capture the issue. These tensions are mirrored at the international level where various multilateral organisations compete for relevance on the issue including the North Atlantic Treaty Organization (NATO); the United Nations (UN) through the Group of Governmental Experts on Information Security; The European Union Agency for Network and Information Security (ENISA); the International Telecommunication Union (ITU); etc. It is this notion of contestation that further distinguishes an assemblage approach from other theoretical lenses that merely acknowledge the importance of units other than states or the increasingly blurry lines that exist between different types of actors.

### C/I—NATO—2AC

#### NATO is an assemblage, “a number of disparate and heterogeneous elements convoked together into a single discernible formation.” That’s limited and predictable.

Handeland, 19—Master of Science candidate in International Relations, Department of International Environment and Development Studies, Norwegian University of Life Sciences (Lars, “Exploring the knowledge-politics nexus in global governance: A case study of the anti-chemical weapons assemblage in Syria (2013-2017),” <https://nmbu.brage.unit.no/nmbu-xmlui/bitstream/handle/11250/2642646/Handeland2019.pdf>, dml)

Originally developed as a concept by the philosopher Gilles Deleuze and his writing partner, the psychoanalyst Felix Guattari, defined assemblage in the following way: “An assemblage is a number of disparate and heterogeneous elements convoked together into a single discernible formation” (Deleuze & Guattari as cited Bueger, 2014c, p. 60). Importantly, the French word they use is agencement. Derived from the verb agencer, the noun agencement can roughly be translated into the ‘act of assembling’, and highlights the ongoing and neverending processes of shifts and transformations (Phillips, 2006). 8

The term ‘convoked’ implies that they are brought together towards a function or purpose. Indeed, “every assemblage is characterized by the process of constituting a "territory" that holds together distinct or heterogenous elements…”(Hayden, 1998, p. 96). The territory, then, comes to signify the identity of a given assemblage, which is derived from its purpose or function. Indeed, the assemblage is not “a random collection of things, since there is a sense that an assemblage is a whole of some sort that expresses some identity and claims a territory” (Wise, 2005, p. 77).

Next, understanding how assemblages ‘claims a territory’ requires a look at some of the associated ideas found in the work of Deleuze and Guattari. As such, the terms territorialization-deterritorialization, the material-expressive axis, and practices of assembling must be outlined first.

To start with, I think it is worth quoting Deleuze and Guattari at length here, giving their original formulation of an assemblage’s features:

On a first, horizontal axis, an assemblage comprises two segments, on of content, the other of expression. On the one hand it is a machinic assemblage of bodies, of actions and passions, an intermingling of bodies reacting to one another; on the other hand it is a collective assemblage of enunciation, of acts and statements, of incorporeal transformations attributed to bodies. Then on a vertical axis, the assemblage has both territorial sides, or reterritorialized sides, which stabilize it, and cutting edges of deterritorialization, which carry it away. (Deleuze & Guattari, 2013, pp. 102–103)

In other words, there are two axes in in the assemblage; a vertical axis of territorialization and deterritorialization, and a horizontal axis of components (DeLanda, 2006, p. 12). The vertical axis captures the stability of the assemblage, i.e. whether its internal stability increases or decreases , whereas the horizontal consists of elements ranging from the purely material to the purely expressive (Patton, 2006, p. 27). These four features gives the assemblage a tetravalent systematization, which signifies the means of combination (Dewsbury, 2011). Next, I unpack these two axes to discuss and assess their applicability as thinking tools for studies of international relations.

On the vertical material-expressive axis, there is the material or machinic end, which consist of matter and bodies (Patton, 2006, p. 27). On the other end there is what Deleuze and Guattari calls the collective assemblage of enunciation, a rather broad category of different expressive elements including discourses, knowledges, semiotics and gestures. Taken together, the heterogeneous elements in an assemblage include socially situated subjects, materials, objectives and different “knowledges, discourses, institutions, laws and regulatory regimes” (Murray Li, 2007, p. 266).

At the same time, assemblage thinking accentuates becoming and emergence, meaning that its ‘territory’ is never fully stabilized. In fact, a core perspective in assemblage thinking is that “structural stability is seen as exception rather than the norm” (Bueger, 2018, p. 619). As such, the territory claimed by the assemblage constantly undergoes processes that stabilize, weakens and reshapes it. In assemblage thinking these are termed: territorialization, deterritorialization and reterritorialization, respectively. This leads us to the second and processual horizontal axis of the assemblage.

As for processes that increase hegemony among the content or elements of the assemblage, called territoritalization, this is “first to be understood as a process that defines or sharpens the spatial boundaries of actual territory” (Bueger, 2018, p. 620). For the study of global governance, territorialization refers to the process of carving out a territory of political space that can be governed. The physical boundaries of such a space can be rather fluid, spread across great distances and be located at many sites. For instance, in Bueger’s (2018) study of the counter-piracy assemblage, territorialization referred not only to the creation of a special zone in the Indian Ocean, but also to the various sites and fora all over the world where stakeholders met and developed plans for action.

Importantly, “territorialization also refers to non-spatial processes. Practices such as classifying or sorting in and out, defining which actors, objects and practices belong to the territory, and what particular role they have are also processes of creating homogeneity” (Bueger, 2018, p. 620). Indeed, in Bueger’s paradigmatic case study, territorialization also included creating consensus on which practices of governance were to be considered legitimate regarding counter-piracy efforts, which ended up being inscribed in document called Best Practices Management. Hence, the making of consensual knowledge was a crucial aspect in the process of territorialization by creating homogeneity among the vast array of relevant stakeholders.

As a result, processes of territorialization in global governance settings are infused with power when, for instance, boundaries are drawn up to delineate specific knowledges as authoritative at the expense of other ways of knowing. This is why the act of sorting out what belongs and does not belong in the assemblage directs attention to the power dynamics at play in the assemblage as territorialization can work “through shutting out contingency and entrenching one particular assemblage…over others” (Müller, 2015, p. 36). Consequently, territorialization is a crucial dimension for analysis as it highlights what might be termed the practice of inclusion and exclusion, which defines what belongs and what does not.

However, even though an assemblage could be deeply entrenched, it is never final and always vulnerable to processes of deterritorialization, which destabilize the it (DeLanda, 2006, p. 12). More concretely, the idea of deterritorialization as a process that can undo the stability of an assemblage allows this mode of inquiry to capture transformations and changes on the ‘territory’. Thus, the erosion of boundaries understood in a broad sense, such as undermining identities, are processes of deterritorialization (Alvesson & Sköldberg, 2017, p. 58).

The important point here is that for studies of expertise, the concept provides the means to account for how, for instance, knowledge claims put forwards by experts can be contested, challenged and critiqued. This can result in a destabilization of the assemblage and make it shift and transform. As such, by opening up for new relations to be established means that relations of authority can shift, thus creating ‘windows of opportunity’ where new connections can be made. Therefore, “in the process of assembling one always sees a territorialising force and a deterritorialising potential: here is where power comes to play (Lancione, 2013, p. 359).

The territory, then, can be unmade by the forces of deterritorialization and finally there is a potential for reterritorialization of the relations between components in the assemblage (Hayden, 1998, p. 96). As far as this author is aware, the notion of re-territorialization has not been widely used in the literature on assemblages in IR. The idea here is that while assemblages are inherently unstable, they also tend to reestablish themselves because they express a purpose or function. The longevity of certain institutions could be taken as an example of this. For instance, one could say that NATO expressed a purpose or function so that while the end of the Cold War initiated a deterritorialization of the NATO-assemblage, it nonetheless reterritorialized, albeit in a different form. Importantly, the idea of reterritorialization is not a synthesis of a territorialization thesis and a deterritorialization antithesis (Legg, 2011, p. 129), but aims to capture yet another transformation that the territory might undergo.

Taken together, these processes are then “the qualitative transformations of complex assemblages on the basis of proliferating relations between heterogeneous terms (Hayden, 1998, pp. 95–96). Because this is an ongoing and constant process, the assemblage is always becoming or emergent rather than a static or stable being (Wise, 2005, pp. 78–79). Hence, an analysis centered on assemblage thinking should look for the changes and transformations on a given ‘territory’, and question how the assemblage articulates relations between its constituting elements, for instance, the relationship between knowledge and politics.

### C/I—USFG—2AC

#### The USFG is an assemblage. Did you not see Hamilton?

Aroney, 2—Professor of Constitutional Law at The University of Queensland (Nicholas, “Imagining a Federal Commonwealth: Australian Conceptions of Federalism, 1890-1901,” Federal Law Review, 30(2), 265, dml)

Putting these points together, Just apparently sought to show that it was necessary to have a strong federal government in which the will of the majority prevailed, but that such a government must first be formed with the consent of each of the several colonies as independent bodies politic. As the Herald had maintained, a federation comes into being by unanimous agreement of the constituent bodies politic, and they agree to confer limited functions on a central government that makes its decisions by majority rule, but the remainder of their constituent and governmental powers are retained.

Just also felt it important to draw the attention of his Australian readers to Hamilton's famous discussion of Montesquieu's classic definition of the 'Confederate Republic'. As reproduced by Just, Montesquieu had said:

It is very probable that mankind would have been obliged, at length, to live constantly under the Government of a single person, had they not contrived a kind of constitution that has all the internal advantages of a Republican, together with the external force of a Monarchical, Government—I mean a Confederate Republic.

This form of Government is a convention by which several smaller States agree to become members of a larger one, which they intend to form. It is a kind of assemblage of societies, that constitutes a new one, capable of increasing by means of new associations till they arrive at such a degree of power as to be able to provide for the security of the united body. ... As this Government is composed of small Republics, it enjoys the internal happiness of each, and with respect to its external situation, it is possessed, by means of the association, of all the advantages of large Monarchies.

A Republic of this kind, able to withstand an external force, may support itself without any internal corruption. ... As this Government is composed of small Republics, it enjoys the internal happiness of each, and with respect to its external situation, it is possessed, by means of the association, of all the advantages of large Monarchies.[47]

In Montesquieu's day, political reflection suggested that large, territorial monarchies had the advantage of external security, but they also suffered the internal disadvantage of a tendency to despotism, whereas the small republic had the advantage of a virtuous citizenry actively participating in the government, but suffered the external disadvantage of susceptibility to assimilation by larger powers. Montesquieu suggested that the advantages of each might be secured in what he called the confederate republic.

Hamilton commented on this idea in Federalist No 9. As reproduced by Just, Hamilton proposed that the 'definition' of a 'Confederate Republic' or 'Federal Government' was 'an assemblage of societies' or 'an association of two or more States into one State'. So long, Hamilton maintained, that the 'separate organisation of the members be not abolished', but rather exists 'by a constitutional necessity for local purposes', then despite their 'subordination' to an additional 'general authority' or national government created for specific purposes, the scheme remains 'an Association of States or a Confederacy'. Indeed, Hamilton pointed out, the proposed United States Constitution treated the states as 'constituent parts' of the Union, allowing them 'direct representation in the Senate' and leaving them with 'certain exclusive and very important portions of the sovereign power'.[48]

### Reasonability—2AC

#### Reasonability: You should choose to understand our interpretations as reasonable readings of the resolution. Cyberwar operates at the level of epistemology itself, which means competing interpretations is a regime of veridiction that furthers the militarization of the cybernetic episteme.

Joque, 18—PhD from the European Grad School, researches philosophy, technology and media and is the visualization librarian at the University of Michigan, go blue (Justin, “Spear Phishing: Nodal Subjects,” *Deconstruction Machines: Writing in the Age of Cyberwar*, Chapter 4, 157-165, dml)

Leaking information, anonymity, and privacy are not only issues of secrecy or its lack but are intimately tied to the subject’s relation to truth. Faced with the contingent and vulnerable nature of these networks and information, any political subject always exists in a complex relation to truth or, at the very least, the veracity of her information. Any political efficacy from leaking information and destroying institutional secrecy requires the production of truth or some sort of truth-effect in the network that would engender a political response. Given the risks that false information could be leaked for the purposes of deception, or produced for other ends, as we saw in the case of Sabu, it becomes difficult to determine the veracity of any individual bit of information. More fundamentally, cyberwar in its very functioning is an attack on truth and its material and epistemic underpinnings. Under the threat of cyberwar, and the possibility that any information may have already been compromised, epistemology and truth become not only philosophical concerns but military-strategic problems as well.

In this light, it becomes difficult to separate any truth from its political and military investment. Derrida in “Plato’s Pharmacy” suggests that “the opposition between the true and the untrue is entirely comprehended, inscribed, within this structure or this generalized writing. The true and the untrue are both species of repetition. And there is no repetition possible without the graphics of supplementarity.”18 Here, for Derrida, the true does not transcend the structure of writing in general. There is no unity but only a relation among units of inscription. The true and the untrue are movements of repetition within and between systems, a movement defined by text and network. Truth and its opposite become emergent effects of networks and texts rather than transcendental or global attributes of systems. Like certificate authorities for verifying identity on open networks, the guarantee of any information is merely deferred to a different level. Truth emerges as a result of the structure and folds of a given system.

This is not to suggest that truth is relative; it is intimately tied to the real and material movement of texts, programs, bits, capital, and so on, through the various global networks and systems at stake.19 Still, what makes information true is precisely its inscription within a given network and its repetition throughout rather than through some preexisting global phenomenon. Lacan’s insights in this regard are especially helpful. He suggests that truth is a function of language.20 Truth is produced by the entire network of signifiers and subjects and always points to the truth of the structure rather than the veracity of an individual statement.21 Thus truth for Lacan is always a question of the symbolic and is never synonymous with the real. The real can never be falsified, for it is always exactly where it is; it is “always in its place.”22 A bit is never on its own true or false; the signifier in the real is, as Kittler suggests, merely a voltage difference.23 It is only through language, interpretation, and software that the bit comes to produce an effect; through the networks of signification, the networks of voltage difference become capable of producing a truth-effect. It is on these grounds that cyberwar becomes so insidious, by threatening to flip bits at the level of the real; underneath language, it demonstrates both the symbolic threat possessed by this real and the inability for the symbolic ever to achieve a full unity or mastery.

Truth becomes an effect of its movements through space and the programs that operate upon it. Any politics that commits itself to truth alone as the grounds for a politics risks merely partaking of the autoimmune violence of undecidability. The end of secrecy cannot in itself be a panacea for political injustice. In August 2010, Reporters without Borders sent an open letter to Assange suggesting precisely that his politics (insomuch as they were a politics of truth rather than of mere destruction) were shortsighted and paid little attention to the chain of effects that followed the dissemination of the “Afghanistan War Logs”:

You have unintentionally provided supposedly democratic governments with good grounds for putting the Internet under closer surveillance. . . .Indiscriminately publishing 92,000 classified reports reflects a real problem of methodology and, therefore, of credibility. Journalistic work involves the selection of information.

Reporters without Borders insists that journalistic work is not simply about providing information but rather about filtering, selecting, and assessing information, in short, about the program that is brought to bear upon information. Even though they may take issue with Assange’s choices of selecting information, his attempts at sharing leaks were also founded on a commitment to selecting information. Still, his selection was significantly more programmatic and consisted largely of sharing all information, except for information about sources (or even knowing, as the technological infrastructure behind WikiLeaks was designed to completely protect leakers); this still constitutes a decision to share only certain information.

Either way, this decision amounts to a political and strategic commitment. Terranova explains the stakes well when she describes the circulation of images as a type of warfare:

The hyperreal does not really involve a metaphysics of being and appearance so much as a kind of information ecology which also includes a dimension of warfare—a warfare to determine the differential power and dominance of some types of images over others.24

Alongside images, all texts and information are subjected to this dimension of warfare that differentiates their efficacy and ability to reformulate flows and networks. It is not merely the bits of information that determine their efficacy but their selection and differential relation.

The specific politics and strategy of pure transparency ultimately turn against themselves on two levels. On the level of truth, such a commitment can never guarantee the secrecy of the leaker while producing technologies that coax information from organizations. The same secrecy tax that burdens corporations and governments also causes individuals to reveal their secrets. On the level of effect, then, any technological and social system for supporting leaks is forced to engage in these complex networks and texts, in short, to decide what individuals’ secrecy matters and what secrecy does not matter. The problem then becomes an undecidable political question. This is not to say that it is a priori negative but that such an act constitutes an opening rather than a necessarily efficacious politics.

With the belief in an abstract machine that moves unwaveringly toward the end of secrecy or the belief that this decision can be avoided through technology, we risk that information becomes its own truth. Leaks become, as raw data, an objectification of the sociopolitical relations that produce, use, and manipulate information and thus mark and measure truth itself. Information thus becomes what Foucault describes as a regime of veridiction, which “in fact, is not a law of truth, but the set of rules enabling one to establish which statements in a given discourse can be described as true or false.”25 Information and the technologies of antisecrecy establish both the truth and the very rules enabling one to ascertain the truth. The regime of transparency in an informational economy becomes not about the quality or effect of information but about its mere possession, existence, and exposure. This is not to downplay the importance of these leaks or to minimize the great risks and costs individuals have taken on to bring this information to the public but rather to insist that this information alone does not guarantee an effective politics.

RESISTANCE AFTER THEORY

In this light, we can understand the media as “tactical” insomuch as all sides of these conflicts seize upon media, their reuse, and their reconfiguration for the purposes of war and conflict. Raley, commenting on the Critical Art Ensemble and Lovink’s, among others’, conception of tactical media, states, “Tactical media comes so close to its core informational and technological apparatuses that protest in a sense becomes the mirror image of its object, its aesthetic replicatory and reiterative rather than strictly oppositional.”26 While the focus of tactical media is largely on art and protest practices, with cyberwar, media become tactical to all involved, including states and armies. Despite these different forces who are now involved in using media tactically, all of them appear caught in this system that Raley outlines, where the use of these media requires that one mirror the object of intervention. When media become objects of war and tactics, it becomes impossible to step outside these processes of mediatization and its disfiguration in the face of this violence.27

To understand the media as tactical under the constant siege of cyberwar requires taking the McLuhanesque insight that “the media is the message” in the most deconstructed sense possible. There is no longer any meaningful way to separate the two. Perhaps before the rise of computers, when command functioned on the level of a physical machine and data could not touch it (e.g., no message could be sent over the radio that would turn it off—or worse yet, turn a car off while one is driving), a separation could be made between media and message. The rise of reprogrammable media that combine data and command requires abandoning any distinction between media and message. Subjects and truth are produced through the topologies and texts that send various messages through a multiplicity of media. Tactics in relation to media can then truly no longer be oppositional, for there can be no transcendental space from which a stable space of opposition could be constructed. Rather, the only tactical movement that remains is to discover the outsides that are folded inside texts, networks, and the unstable interface between them. But, the translation of local information to global networks always risks perversions, corruptions, and interventions.

Despite, or perhaps even because of, the difficulty of acting or deciding within these complex global networks, there is a great appeal to the possibility of controlling situations through instantaneously knowable surfaces. Data appear as a vast field of computable truth. But the coherence of these surfaces is always belied by the vulnerability and contingency they contain within and the instability of the subjects whose traces exist in these vast fields of data. Still, many discourses, including those of information transparency, continually claim the efficacy of managing surface effects. Rather than recognizing those forces, which resist control, a host of actors increasingly seek out finer-grained modes of analysis, holding on to the fallacy that everything today is flowing and visible.

Chris Andersen, a prominent technology journalist, has stated the belief in these analytic modes of knowing in its most radical and succinct form. In an argument analogous to Greenberg’s claims of a coming transparency, Andersen states that the age of huge data sets means that we no longer need models or theories of the world and instead can “run the data” in real time:

Out with every theory of human behavior, from linguistics to sociology. Forget taxonomy, ontology, and psychology. Who knows why people do what they do? The point is they do it, and we can track and measure it with unprecedented fidelity. With enough data, the numbers speak for themselves. The big target here isn’t advertising, though. It’s science. The scientific method is built around testable hypotheses. These models, for the most part, are systems visualized in the minds of scientists. . . . But faced with massive data, this approach to science—hypothesize, model, test— is becoming obsolete.28

For Andersen, we do not need to know why things happen but merely be able to predict them in real time: no theories, no models, no interpretation, just a pure flow of data. In many ways, it is the scientific version of Bill Gates’s fantasy of frictionless capitalism, but for Andersen, the signifier of capital is gone too. His is a fantasy of an infinite flow of information processed in real time, and the world constantly re-created anew out of predicting algorithms. It is a utopia, a nonplace, with no slowness and no topography that could hold information into a theoretical system. Beyond theory, we no longer need categories, only momentary statistical conglomerations. In this world, one need not know or theorize gender, class, or even individual subjects; everything becomes an individual record in a large-scale database.

It is, in short, the fantasy of a world without cyberwar, a world beyond cyberwar. This utopian vision would only be possible if computation and data were perfectly secure and always represented the world exactly. These descriptions of a pure world of data-driven discovery rest on the fantasy that all being and becoming can be perfectly encoded as data. This utopia requires that all data be perfectly secure and no accident, gap, or military force affect this correspondence. At the same time, it is a fantasy of the utter success of cyberwar, insomuch as it requires that technicians, politicians, scientists, and bankers are able to extract data from every system. In sum, Andersen hopes for a cyberwar that would end all cyberwars, an impossible cyberwar that would defeat all resistances.

Andersen is not alone in this vision of the future. A whole field of “hypothesis-free science” has gained traction in several disciplines.29 Advertisers, high-frequency stock traders, and security agencies all mine massive stores of data to find customers, profits, and criminals with no interest in theorizing what is being sought. Even Latour’s actor network theory appears committed to the tracing and recording of surface-level phenomena that provide no theory aside from the method of following an individual actor’s own theory.30 Here, again, information becomes its own veridiction. As long as the variables correlate, it does not matter why or how, and if the correlation is off, the algorithm updates automatically to improve accuracy for the next round.

### AT: Iteration

#### Machine Learning DA: Mechanistically weighing the consequences of fiated plans over and over makes debate algorithmically violent at the level of form, which has material significance. They’ve created uniqueness for our offense because iteration is a process, so disrupting one instance jams the gears.

Amoore, 22—Professor of Human Geography in the Department of Geography, Durham University (Louise, “Machine learning political orders,” Review of International Studies, February 15, 2022, dml) [language modifications denoted by brackets]

Yet, what I propose here is that machine learning political orders reverse Deleuze’s dictum so that the political problem is constituted by the posited solution; or, the solution gets the problem it deserves. The retroactive logic of deep learning commonly begins with the identification of the target output from the model, actively using the output signals that diverge or converge on the target as an experimental space of modulation and adjustment. Though there are multiple possible functions or ‘solutions that will match the data’, a machine learning algorithm will use ‘two sources of information to select the best function: one is the dataset, and the other (the inductive bias) is the assumptions that bias the algorithm to prefer some functions over others’. 40 In order to change the output signal, the weights within the hidden layers of the neural network adjust and modify the signal that feeds forward to the next layer. Why does this computational process matter for how the political problem and the solution interact? The retroactive move from target solution to the weights in the model means that the parameters and dimensions of an intractably difficult political question – democracy, pandemic response, border security, stability in the economy – become configured as infinitely adjustable in relation to the solution. Where the concept of problematisation suggests a multiplicity of actions that could take place under the broad unifying conditions of the formulation of the problem – and, indeed a space for normative deliberation of possible actions – this retroactive paradigm forecloses the multiplicity of plural solutions to a single target, and reduces the framing of the political problem to the weighting of inputs. Every adjustment or modification of the parameters in the deep learning model is simultaneously an arrangement of the political problem.

To begin at the ‘end’, with a target output of the model, is thus to transform radically what a political claim can be in the world. For example, machine learning algorithms are increasingly being deployed in immigration and borders decisions. The introduction of machine learning in the sorting and classification of visa applications does not merely automate some aspects of a previously human centred bureaucratic process. More than this, the building of a model of the flows of immigration claims actively constitutes what a border can be and how it is understood as a political question. Moreover, the space to challenge the political formulation, such as for example to question the racialised criteria that are applied to the judgement on a person, is also closed out by the machine learning process. In contrast to the rules-based models that I described as engineering racialised assumptions into association rules (for example, in Rakesh Agrawal’s data mining models), machine learning learns and generates new racial formations from the data examples. With machine learning forms of classification, there are no criteria as such; there are only inputs, outputs, features, and functions. The model will also adjust with the volatilities and geopolitical disruptions of migration, shifting its thresholds so that the derived outputs are decoupled from the input data of a visa application.

There are profound political consequences of this more generative and disruptive approach to data inputs. In 2020, for example, the Joint Council for the Welfare of Immigrants (JCWI) challenged the UK Home Office’s use of a ‘streaming algorithm’ to allocate visa applications to high, medium, and low levels of risk. The JCWI identified the nationality data that were among the inputs to the algorithm that scored some applicants as ‘high risk’, effectively automating the decision to refuse the visa. JCWI and Foxglove Legal successfully argued that the nationality data are proxies for race and, therefore, in breach of the provisions of the Equality Act 2010.41 If the algorithm had been a solely rules-based ‘if … and … then … else’ sequence, then the juridical removal of racist input data would arguably substantially change the outputs of the system. However, with machine learning it would be a mistake to conclude that the removal of a racist input will excise the racialised propositions of the model. The streaming of visa applications into risk-rated clusters, as exhibited in the JCWI case brought by Foxglove, is an example of a solution defining and configuring the political problem, so that immigration targets are the starting point. When the input data are not variables (in the functionalist sense) but features, the UK Home Office can agree to remove a racist input (as they have done) while continuing to weight other features in ways that revitalise racist inferences that were not strictly present in the input data. For example, the weighting and parameters applied to travel, to familial relationships, or to periods of time spent outside the UK can serve to constitute a suspicious population and to generate a red-flagged output. When the model is learning about salient features and clusters from the dataset, its racialised assumptions will exceed the categories of the input data and extend to the groupings and communities created by the machine learning process. It is not only the use of data from which race can be inferred, but more significantly that the immigration algorithm forecloses the potential of a person’s future on the basis of a racism that pervades the model all the way down.42 In short, the question of what kinds of political actions, which political claims, or which policy agendas can be designed and made, is condensed down to the foreclosure of a target output solution.

When the design of a machine learning model becomes a valued political object in itself, the derivative outputs of the model are exchangeable and tradeable beyond any specific defined political problem or ‘domain’. 43 In common with the models built by Cambridge Analytica, everything becomes a function of deep learning to the point that there are no bad outputs – even where this may be illness, racism, death, destitution, social hardship, child poverty – there are only target outputs and the adjustable parameters of a problem. Amid the loss of more than 170,000 lives to COVID-19, the UK launched its national data strategy in 2020, describing the ‘high watermark of data use set during the pandemic’ where businesses, government, and organisations had been ‘freed up’ to ‘innovate and experiment’. 44

A period marked by lack of effective emergency planning and horrifying loss of life is thus articulated as a ‘high watermark of data use’. In his testimony before the UK House of Commons Science and Technology Select Committee, former advisor to the prime minister, Dominic Cummings, explained that conventional civil contingencies ‘did not have the data architecture’, and that ‘companies [DeepMind] had stuff we could use off the shelf, hack it together for the NHS.’ 45 Behind the rhetoric of his testimony, Cummings’s account does express the deep faith placed in deep learning models to address the data gaps in bureaucratic structures. On the day that he appeared before MPs, Cummings released a photograph of a whiteboard used to map early pandemic planning. Among the scrawled notes, a question is posed: ‘who do we not save?’. Viewed from the perspective of the building of machine learning models for the pandemic – or the ‘hacking together’ by private tech companies – the question of who will not be saved is but a mere parameter in a model, to be adjusted in relation to NHS capacity. In the event, this parameter was also a deeply racialised metric – with people of black and South Asian ethnic background four times more likely to die from COVID-19 in the UK.46 In common with the racialised logics of the immigration algorithm, the pandemic models did not need to begin with race as a category or input to nonetheless generate a deeply racialised model of algorithmic violence. The machine learning model itself has extraordinary resilience in the face of complete moral and political failures because a weight can always be adjusted, a threshold modified, a parameter tweaked. The question of ‘who do we not save?’ is translated into the parameter of a model whose target outputs are the starting point. In a situation where there is a total and abject failure of policy and good governance, the innovation in data science and AI is nonetheless fostered by the racialised violence and social turbulence that is generated. Whether this is incorrect or unjust decisions made in an algorithmic benefits system, poor judgements on policing deployment, or the catastrophic pursuit of a modelled ‘herd immunity’, machine learning political orders learn something from the data generated by the volatility.

A similar sense of the productivity of fractured governance is present in the UNHCR’s statements that ‘even in highly volatile and chaotic environments’, digital systems will ‘radically expand the responses that can be crafted for challenges in health care, education, migration, and security’. 47 The organisation envisages machine learning technologies within a process of ‘competitive disruption’ to what it calls ‘obsolete’ institutional structures ‘with legacies dating back to World War II’. The flexibility and agility of a deep learning model – deployed, for example, in UNHCR’s ‘Project Jetson’ predictive models of refugee movements – becomes a condition of possibility for the imagination of adaptive digital humanitarian and pandemic response, so that social and political relations are reconfigured as the parameters of a model.48

In each of the examples I describe above, functionally arranged structures of postwar social and international orders are reimagined along the dimensions of a machine learning universal function. That is to say, a function that is immanently mappable from a target output to the weightings of the layers of the problem. To propose that a policy or an institution must deliver on a function thus also shifts its ground – for something to ‘function’ it no longer needs to work as such.49 As Debbie Lisle has argued, the cultures of science and engineering mobilise a politics within which ‘failure’ itself is rendered an ‘instructive experience’. 50 Within a machine learning logic, the instructive experience of failure permits the model to learn those unknown things that are beyond the distribution of data in a training dataset. Though machine learning orders cannot be said to fail as such – or at least the output of the model is never a failure but only a signal – the retroactive generation of political problem from output solution means that the very idea that a neural net can approximate any function becomes a powerful political idea. In short, though these ideas of failure are ontologically distinct, they become epistemically aligned; there is slippage between failure as learning, and the idea that there can be no ethical failure, nor catastrophic policy failure.

At stake in retroactive design, then, is not merely that deep learning algorithms are deployed to govern society, but rather that society comes to understand itself and its problems through the lens of the deep learning model. The relations among people, objects, and space become rendered as features from which something useful can always be extracted, from which a function can always be found. However, the plurality and multiplicity of those relations, and the potentiality for new or alternative political projects to emerge, is radically foreclosed around the retroactive mapping from target output to the weighting of parameters in a model. It is to the usefulness of exposure to contingency that I now turn, with a discussion of how technological trials became perennial and indefinite.

Trial by design: How the test became an indefinite trial

The concept of alpha and beta testing has its origins in IBM’s 1950s software development, when the ‘A’ test signalled the in-house testing to improve the engineering and the ‘B’ test referred to the verification through user engagement and development. In his account of Cold War America and the culture and politics of computers, Paul Edwards describes the emergence of cybernetic culture and its penetration of state and military thinking. In the context of Edwards’s ‘closed world’ integration of a ‘seamless web’ of human and machine systems, the engineer deploys the testing regime in a form that mirrors the hierarchical logics of computers.51 As an engineering practice of the twentieth century, the test formed an intrinsic part of the rules-based and cybernetic approaches to government and computer science. As Edwards depicts the Cold War collaborations of IBM, RAND, and the aircraft corporations, the process of political planning itself became an ‘if … then’ proposition, ‘constructing a list of tests to perform’, identifying failings as information problems, and creating feedback loops from test to engineer.52 In this sense, the Cold War alliances between computer science, mathematics, and the military state embodied a specific understanding of testing as practice, and of errors as problems of fallible human perception that could be corrected with machine systems.53

This conception of testing and the sequential procedures of the ‘list of tests to perform’ is aligned with the rules-based computation and rules-based social and international political orders I have described. It is a conception of the test that is deeply probabilistic and conceives as testing as a process concerned with the calculation of probabilities. As Orit Halpern describes the cyberneticians’ practices, ‘they focused on the ability to calculate the probability that one set of interactions (the missile hitting the plane) will occur, over other sets less likely but possible’. ‘This is a worldview composed of functionally similar entities – black boxes’, she writes, composed only of ‘their algorithmic actions in constant conversation with each other producing a range of probabilistic scenarios’. 54

Against this historical backdrop of probabilistic alpha and beta testing within functionally similar entities, the rise of deep learning algorithms is most profoundly possibilistic in its orientation to the future.55 As a mode of political ordering, machine learning circumvents modern notions of testing in science and engineering by turning to the trial and trialling as experimental technology. The trial is a more possibilistic approach precisely because it refutes the functionally similar entities and probabilities Halpern denotes in cybernetics, and it embraces instead the generation of multiple possible functions in order to defer a decision on what is politically useful. Understood in this way, the rise of trialling in contemporary machine learning has more in common with the conduct of stress testing to anticipate uncertainty in finance than it does with alpha and beta testing in software engineering.56 The machine learning model dwells indefinitely in its trial phase because it is designed and redesigned through its exposure to people, objects, places, and scenes, perennially modifying itself in response to what it has learned through its encounters. In this way, the ‘demo’ as technological demonstration, has a close relationship with the ‘demos’ as the people, the population and democracy.57 ‘Our forms of technological testing and demoing’, writes Halpern, ‘envision a world where artificial intelligences and computers can replace the democracy that is now imagined to be obsolescent’. 58 As deep learning models penetrate public space, for instance in live facial recognition biometric systems in urban spaces, at borders, and in military spaces, every trial of a deep learning model is also an active reconfiguration of that space as the model adapts in response to the contingencies it yields.59

For example, in the world’s first legal challenge to police use of automated facial recognition algorithms (AFR), the appellant, Bridges, argued that South Wales Police unlawfully extracted his biometric data during two trials of the technology.60 Bridges had been subject to AFR during a protest outside an arms fair in Cardiff in 2018, and during a Christmas shopping trip in 2017, with each trial of the system storing his biometric data, cross-matching with a watchlist, generating match scores, and modifying the sensitivity of the model. The court of appeal found in Bridges favour in 2020, following testimony from an expert computer scientist whose account vividly illustrates how the trial indelibly marks and recalibrates a gendered and racialised system. ‘AFR systems will have a higher error rate for women and people from black and ethnic minority groups’, he testified, and ‘where an end user is adjusting threshold values it may make the AFR system particularly sensitive for some individuals. People from that ethnic group will be wrongly matched more often.’ Thus, the trial of AFR – ongoing for a seemingly indefinite period from 2017 – will continue to generate racialised outputs and clusters of suspicion, even where individual biometric datasets are deleted. As Rocco Bellanova and Marieke de Goede describe architectures of data analysis, ‘the infrastructure aims at defining the “right population” to be algorithmically governed.’ 61 The very communities who are already disproportionately targeted by the state will experience an intensification of scrutiny and control. In this way, the capacity of a person to be present, or to gather with others, in public space is iteratively and intimately related to the exposures of a machine learning model that is indefinitely trialled across multiple spaces. Unlike the feedback loops of Edwards’s Cold War military-computer science collaborations, the error rate of the biometrics are contingent on the shifting infrastructural thresholds and parameters of the algorithm. Whereas the cybernetic mode of testing was concerned with the engineering of human and machinic component parts, the machine learning mode of indefinite trials makes the limit and the threshold the object of the trial, so that setting sensitivities, moving borders and boundaries reconfigures both algorithm and action.

In this way, the orientation of the indefinite trial is closer to an experimental and open-ended process of design than it is to engineering. The very etymology of design is from the Latin designare, to designate, to mark out, and related to disegnare, to contrive or intend. It is precisely this process of designating and marking out that I see at work in the indefinite trials of deep learning technologies in cities, at borders, in public space. Bruno Latour outlines a philosophy of design in which ‘design has been extended from the details of daily objects to cities, landscapes, nations, cultures, bodies, genes.’ 62 For Latour, the practice of design is counterposed to historical notions of building or engineering, so that ‘things are no longer “made” or “fabricated”, but rather designed.’ ‘This was the old way’, he writes, ‘to build, to construct, to destroy, to radically overhaul’ through engineering.63 By contrast, to design something, for Latour, is never to found something radically new but always to seek perennial iterative modification, so that ‘it is never a process that begins from scratch: to design is always to redesign.’ It is for this reason – the practices of design as open-ended iterative modification, even as ‘anti-revolutionary’ – that I align contemporary machine learning models with design and not strictly with engineering.64

Indeed, many contemporary deep learning practices such as ‘transfer learning’ definitively reject ‘handcrafting representations’, in favour of ‘greedy exploration’. 65 Every action is a modification of the residue that is already lodged within the layers of the model, it is never a complete overhaul or disruption. As Latour suggests, ‘to say everything has to be designed and redesigned, it will never be revolutionary’. 66 This foreclosure of something different, something revolutionary, is a crucial problem in machine learning political epistemes. As I have described, even where the practice of trialling a model is found to be in breach of law, or where racist data inputs are removed, still nothing revolutionary can emerge. For design can always modify and adjust and move the threshold, each adjustment another indelible mark, a marking out and a demarcation line. When Latour concludes that ‘designing is the antidote to founding, colonizing establishing’, I must disagree with him, for it is precisely colonising in ways that incorporate ever-increasing layers, extend to ever more domains of life, and dwell quietly in the violences of the modified weight. What new or alternative politics can possibly emerge when every potential pathway has already been narrowed to a mere parameter? It is to the implications and potentials for alternative political futures that I now turn in conclusion.

Design interruptions: Resisting machine learning worlds

In setting the themes that animate this Special Issue on disruption, Nicole Grove posed the question ‘what kind of worlds are in store for us as algorithms disrupt forms of organisation and advocacy for more equitable futures?’. 67 I have sought to map out how machine learning actively incorporates the data from disrupted and fractured forms of organisation, and why it is that advocacy for alternative political futures becomes foreclosed in the logics of retroactivity and perennial trialling. I have suggested that a machine learning political episteme – one that eschews rulesbased computational and political orders – is profiting from the undoing of postwar international and social institutions, from the deep neural networks powering the Vote Leave campaign to the so-called ‘digital transformation’ of the pandemic NHS. While, of course, I am not nostalgic for cybernetic worlds of rules-based computation and the liberal international order, nevertheless it is the case that notions of democratic life, human rights, and social ethics also grew amid such rules oriented orders. Where machine learning political orders are precisely profiting from the undoing of rights and collective public institutions, there are new challenges for the politics of resistance.

What happens to the space for resistance amid the power of the machine learning algorithm? What are the possibilities for reopening the futures that are condensed and foreclosed in the output of a deep neural network? Where machine learning algorithms are increasingly learning from the features of social scenes and the gathering of people in public space, is collective politics reduced to a being together that is merely the clustering of attributes? As Judith Butler has put the question, ‘what does it mean to act together when the conditions for acting together are devastated or falling away?’. 68 Such questions are more urgent and acute because the threats to the rights to protest and freedoms to assemble are intensified by a machine learning order that absorbs the attributes of collective action. In her treatise on political assembly, Butler imagines that the ‘gathering signifies in excess of what is said’ and that ‘popular assemblies form unexpectedly and dissolve’, exercising a ‘plural and performative right to appear’. 69 Yet, this plural and performative excess of the gathering of vulnerable bodies in public space is precisely under threat from the retroactive and trialling logics of the machine learning polity.

When the machine learning algorithm becomes the mise-en-scène of the public square, the means of arranging the scene and extracting the features, what political claim can be heard that is not already extracted and scored, and who can make it? The task for resistance, I suggest, is to interrupt the ordering of the political scene in order to ask how it might be otherwise. My emphasis on interruption consciously rejects the vocabularies of disruption that animate the force of disruptive technologies and ‘push on the fracture until it breaks’ tech industry cultures. To interrupt the scene is to resist its very condition of appearance, to locate the breaches in algorithmic arrangements and to show how they could be otherwise. As Walter Benjamin notes of Bertolt Brecht’s device of ‘interruption’ in epic theatre, ‘the truly important thing is to discover the conditions of life’, where this discovery ‘takes place through the interruption of happenings’. 70 To interrupt the scene of a machine learning political order would be to confront the plural branching pathways that could have yielded a different output and to amplify those branches as political decisions. In every arrangement of a machine learning model there are the traces of the rejected alternative. Brecht’s device of interruption presents the observer with the traces of what could have been present, with the actor performing ‘in such a way that the alternative emerges as clearly as possible’, allowing ‘other possibilities to be inferred’ even while she [they] ‘represents one out of the possible variants’. 71 In this way, the interruption of the scene works against the grain of the algorithm’s reduction to one visible output, showing the contingency and multiplicity of the one out of many possible variants. Here lies a significant form of resistance; to amplify the branching points as moments where things could have been otherwise, where other possibilities could be inferred; and to refuse the reduction of political difficulty to one that is the output.

To resist being governed by a machine learning political order will necessitate naming the harms – beyond the conventions of privacy, data protection, and existing bodies of rights – of the foreclosure of alternative political futures. Though the machine learning political orders I have described close off political contestation and unheard claims, under the figure of the machine learning model there remains a teeming politics. When the solution precedes the political problem, the adjustment of parameters is also a real and violent modification of people’s lives – as migrants, as benefit claimants, as people gathering in the city square. It is for this reason that the deep learning practice of modifying ‘weights’ in the model must be rendered heavier and more burdensome than the lightness of an adjustment implies. The weight in a machine learning model is not merely a technical weight on a connection in the neural net. It is the full burden and heaviness of a rejected visa application, a past facial biometric captured at a protest, a refused welfare claim, the extracted features of the refugee. In her compelling account of how colonial formations endure, Ann Laura Stoler foregrounds the ‘enduring fissure’ and the ‘durable mark’ of imperial duress.72 Stoler’s affecting thought about ‘duress’ foregrounds the ‘hardened, tenacious qualities of colonial effects’ and ‘endurance’ in the ‘capacity to “hold out” and “last”, to endure as a countermand to “duress” and its damaging qualities’. 73 The weight of the machine learning algorithm could be freighted with the heaviness and endurance of Stoler’s imperial duress. Each adjustment and modification of the model a squeezing and a tightening of the conditions of liveability of a political space, a community. Every indefinite trial a trial in the fullest sense of something that is borne by vulnerable bodies.

### AT: Reflexivity/Skills

#### Their info reflexivity claims are a smokescreen for algorithmic control.

Tazzioli, 21—Lecturer in Politics and Technology, Goldsmiths University of London (Martina, “Technologies of Control and Infrastructures of Redistribution,” e-flux #123, December 2021, dml)

A well-known slogan that emerged from the disability movement during the 1990s goes: “Nothing about us without us.” It stresses that no policy should be adopted without fully involving those who are affected by that policy. Nowadays, it is a catchphrase used across different fields and institutional settings, signaling that “participation” has become a placeholder for inclusion, democracy, and horizontal decision-making processes. Yet, what does “participation” in a given system mean when the epistemic-political codes, the ability to maneuver, and the stakes of the participation are set in advance by the party in control? So-called “participatory programs,” like surveys and other forms of data acquisition, have been used extensively by humanitarian agencies since the 1990s, and more recently have shifted into systems for practicing what I instead call “participatory confinement.” In such systems, individuals are nudged and encouraged to actively participate in their own confinement and governmentality, “for their own good.” Christopher Kelty, a scholar of science studies and anthropology, rightly claims that this sort of “participation is more often a formatted procedure by which autonomous individuals attempt to reach calculated consensus.” Not only are the goals and forms of participation often preestablished and surreptitiously imposed, but individuals are also de facto pushed to corroborate, contribute to, and improve mechanisms of confinement and coercion. Here, I focus on refugee humanitarianism as a case study for coming to grips with modes of participatory confinement as a systematic political technology of governmentality.

Modes of participatory confinement in refugee humanitarianism are inflected by clear-cut asymmetric relations between asylum seekers on one side, and humanitarian actors on the other. This initial condition and its trend towards reform by way of inviting participation is reminiscent of the diagnosis of prison reform by Michel Foucault in a lecture he gave in 1976. Furnishing an anticipatory example of participatory confinement, he writes: “There is an attempt to make prisoners themselves participate in devising the very programmes for their punishment, through the prisoners’ councils and so on. This is the idea that the individual, singly or collectively, is meant to accept the punitive procedure.” Nowadays, participatory approaches are center stage on the agendas of international agencies and NGOs in the context of the so-called “refugee crisis” in Europe. They continue to operate with the same neoliberal logics of prior reforms to systems of punishment and control that performatively invite the exploited to frame the forms of that exploitation, while actually ceding no power to the “participant.”

Furthermore, invoking a term from Tiziana Terranova, participatory confinement in refugee humanitarianism can also be considered a form of “soft control.” Asylum seekers are increasingly asked to answer questionnaires and provide detailed information to humanitarian actors about their coping strategies, migratory journeys, the logistics of border crossing, and their protection needs. These activities are presented to refugees as an opportunity to improve their individual situation and, at the same time, the asylum system at large; in actuality, they just increase the control that the system has over refugees. In The Undercommons, Fred Moten and Stephano Harney refer to a similar process as the “invitation to governmentality” which subjects are repeatedly exposed to. Elaborating on this notion, it can be argued that this “invitation” in the context of humanitarian participatory programs also involves pushing subjects to perform unpaid labor by providing feedback. They thus implicitly consent to being sites for the extraction of knowledge, which is used by NGOs to further enforce modes of control and governance. Speaking of an invitation to governmentality in these terms also sheds light on the multiple forms of interpellation that individuals are subject to, and how they are nudged to participate “for their own good.” That is, the invitation to governmentality that individuals are exposed to in different contexts often turns into a form of subtle coercion.

## Ks

### Governance Turn—2AC\*\*\*

#### \*\*\*Note while prepping: This card is particularly useful against Moten and Harney/logistics Ks. If you are quite sure that the other team will go for a K and won’t read framework, you could put this in the 1AC if you wanted (you can still read this card if the neg reads framework, but be careful, as it might enable them to make TVA arguments!).

#### The alt’s totalizing anti-governance orientation discounts methods of repurposing the stack-layers of governance towards ungovernability in favor of fleeting viral moments of spontaneity.

Schneider, 22—assistant professor of media studies at the University of Colorado Boulder (Nathan, “Governable Stacks against Digital Colonialism,” tripleC 20 (1): 19-36, 2022, dml)

Theorists and practitioners of anticolonial resistance have persistently stressed the centrality of self-governance in everyday life as both the means and the end of their movements, alongside acts of outright insurrection. By self-governance I mean to evoke other terms like autonomy, autogestión, autogestió, community control, self-determination, self-management, self-organising, self-rule, sovereignty, swaraj, and more – together encompassing how groups of people become impervious and intolerable to those who want to govern them by governing themselves. The aspiration to be “ungovernable” has appeared among thinkers ranging from the philosophers Michel Foucault and Giorgio Agamben (Thaning, Gudmand-Høyer and Raffnsøe 2016) to former Black Panther Lorenzo Kom’boa Ervin (Anderson 2020), each seeking to assert the vital personhood of people caught in dehumanising systems. Such systems utilise “governmentality” to extend their power into subjects’ lives (Li 2007). Scholars of governance tend to regard it as something done to – or at best, for – most people, rather than something they do themselves (Levi-Faur 2012). Self-governance against colonialism is something else, something people do to govern while becoming ungovernable.

To become ungovernable under digital colonialism, how should we be learning to self-govern?

I pose this question while observing that the platforms most available for online organising are not well-suited for self-governing; tools for basic group decision-making are not widespread, and nor are mechanisms to hold those in authority accountable (Schneider 2021). The design of social platforms inclines toward enabling the governmentality of platform owners, aided by their user-administrator proxies, rather than user governance that could turn against the owners’ interests. Campaigns of digital resistance often employ the same colonial firms they oppose. Those confronting digital colonialism today might therefore orient their struggles, as past anticolonial movements have, by rediscovering and reinventing the art of self-governance.

Settler colonialism and digital “user experience” both involve what legal scholar Sanjukta Paul (2020) calls the “allocation of coordination rights”. Regimes dictate who has the right to self-organise, or not, and under what conditions. Micro-targeted discrimination singles out individuals for exposure to exploitative advertising, stifling public outcry (Benjamin 2019). Algorithmic decisions about public-service provision make it harder for harmed communities to put collective pressure on individual decision makers (Eubanks 2018). Humanitarian organisations collect data about refugees, which the refugees themselves cannot access while the organisations use it for future fundraising (Madianou 2019). Individual users might have options on a platform to access or delete their own personal data, yet platform companies alone can develop products from the users’ data in the aggregate (Couldry and Mejias 2019a). Platforms impose the developers’ cultural norms, projecting a false universality that leaves little space for user communities to practice their own cultures (Kwet 2019; Milan and Treré 2019; Duarte et al. 2019). And at least as much as platforms might enable activist organising, they introduce new varieties of surveillance and repression (Tufekci 2017; Canella 2018).

“Governance is what we are fighting for”, writes Black Lives Matter co-founder Alica Garza (2020, 273). “We are fighting for the right to make decisions for our own lives and to ensure that right for others”. Her movement’s protests have made whole sections of cities ungovernable through daring, fraught, fleeting attempts to implement alternatives to policing. Progress goes slowly, with setbacks and blowback, until seemingly all at once even those in power no longer have any choice but to build on the fragile experiments from the streets.

What would community-governed technologies look like, and how can they resist exploitation? I introduce the concept of “governable stacks” as a means of ungovernable organising under digital colonialism. From here, this article reviews how anti-colonial leaders and thinkers have thought about self-governance. It then turns to the perils of recent failures among resistance movements to self-govern under digital colonialism. The following two sections present governable stacks in detail as a concept and as a practice.

2. The Trouble of Governance

“Governance is the extension of whiteness on a global scale”, write Stefano Harney and Fred Moten (2013, 56). NGOs are the “laboratories” of governance, which turns democracy into labour. It is a cheap sort of domination because the subjects do it to themselves: “Governance arrives to manage self-management, not from above, but from below” (55). Harney and Moten reply with a politics of refusal and “being without interests”, a call to imagine what it would mean “to struggle against governance” (57): “We are the general antagonism to politics looming outside every attempt to politicise, every imposition of self-governance” (20).

Harney and Moten’s polemic can claim many ancestors. They cite Frantz Fanon, who stressed the “spontaneity” of popular uprisings, the ungovernable reaction of the lumpen-proletariat, “the most spontaneous and the most radically revolutionary forces of a colonized people” (Fanon 1961/1963, 81). They celebrate the ungovernable villages of escaped slaves in the Americas, including the maroons of Saint-Domingue’s high hills, whose raids did not wait for Touissant Louverture’s command but made possible the eventual independence of Haiti (Lebrón Ortiz 2020).

“You know, I love C.L.R. James”, says Moten in passing (Harney and Moten 2013, 155). James, the Trinidadian chronicler of Louverture’s revolution and an instigator of others from Tanzania to Detroit, praised spontaneity as well. His book with Grace Lee Boggs and Pierre Chaulieu, Facing Reality, describes a “most conscious and finished opposition to the parliamentary procedure” found among dockworkers. By their account, “dockers do not like votes”; “they sense the general sentiment and act on that” (James, Lee and Chaulieu 1958/1974, 121-122). What holds sway is a worker’s je ne sais quoi ability to capture the attention of the others, regardless of role or position: decision without institution.

The age of networks has only deepened the allure of spontaneity among radical theorists, as with Michael Hardt and Antonio Negri’s admiration for the “multitude” and the “assembly” against fixed organisational forms (2017), or Manuel Castells’s (2015) “networks of outrage and hope”. Underground tracts from such pseudonymous figures as the Invisible Committee (2009) and the Vitalist International (2019) long for rebellions whose disorder is their vindication, while adrienne maree brown (2017) presents spontaneous self-organisation in nature as a theory of social change. Each seems to profess that organisational forms of revolutions past no longer compute – in part because we now have computers.

An antithesis: over a century ago, Vladimir Lenin (1902/1961) regarded those “who kneel in prayer to spontaneity” as a “fungus” among revolutionaries. Where there is spontaneity among the masses, it obtains power only through an organised and disciplined vanguard party, such as the one he would lead in Russia. Rosa Luxemburg (1904) recoiled at the rigidity of Lenin’s vanguard, one moulded by the discipline of the factory, the army, and the bureaucracy. She called for a movement that would be “supple as well as firm”, capacious enough to hold the full humanity of its participants. Yet a communist regime came to pass in Germany not through her homegrown movement but through Soviet tanks rolling into Berlin. Those tanks emanated from Stalin’s dictatorship; Luxemburg was right to worry about a vanguard modelled on industrial discipline. What she longed for remains so often elusive: a movement firm enough to gain power yet supple enough to wield it humanely.

Now, stop and go back, and reconsider those apparently kneeling before spontaneous resistance, against the strictures of governance. Synthesise the dialectic. Fanon also warned against the “cult” of spontaneity (1961/1963, 130) and stressed that the “enlightening of consciousness” necessary for liberation is “only possible within the framework of an organisation, and inside the structure of a people” (142). He held that spontaneous energies must find institutional cohesion. C.L.R. James affirmed, in his final interview, “I believe you must have an organisation” (Fitzpatrick 1989) in the Leninist sense. He celebrated the Paris Commune as a forerunner of the Russian soviets, regarding that uprising as “first and foremost a democracy” (Johnson 1946). And in “Every Cook Can Govern”, an essay that took its title from a phrase of Lenin’s, James recommends to workers the ancient Athenian method of ruling by sortition, selecting authorities from the citizenry by lot. The anticolonial organisation, in this light, must be creative and accountable, reaching into the lives of those who are self-governing and also outward as a model to others. As Adom Getachew (2019) documents, the independence movements James helped to inspire sought not just nation states but a new order of global governance.

Grace Lee Boggs was long a fellow traveller with James in the factions and divisions of sectarian Marxism, a student and friend of Third World revolutionaries (Boggs and Boggs 1974; Boggs 1998/2016). She and James Boggs thought their way into a “politics of personal development” (King 2017) that rejected partisan orthodoxies in favour of a more iterative “dialectical humanism”, in which political visions and the people who hold them evolve together through struggle. From the systems thinker Margaret J. Wheatley came Boggs’s frequent affirmation of “critical connections” over “critical mass” (Boggs and Kurashige 2012, 50) – a conviction that the germ of seismic change lies in the thick relationality of how people choose to self-organise day to day. She drifted from Leninism, but the imperative of self-governance only deepened.

Later in life, Boggs’s attention turned from achieving state communism to commoning, the work of people continually discovering what they are seeking to achieve by stewarding shared projects and resources. She became a mentor to veterans of the 2011 Occupy Wall Street and its “leaderless” travails. After her passing, Rodrigo Nunes (2021, Chapter 1) in Brazil envisions post-2011 movement organisation with naturalistic language like “nebula” and “ecology”. He confesses attempting to recuperate a kind of vanguardism, a “networked Leninism” – before concluding with an insistence that above all activists should “think and act ecologically” (Conclusion).

In Boggs we see the origins of passages about mycelia and butterflies and trees in the writing of her disciple adrienne maree brown (2017). brown’s “emergent strategy” for activists revels not in conflict with corporate opponents but in apparitions of friendship in online threads and tips for weaving consensus processes. Seeking to transcend “protest politics”, Boggs described her mentorship of younger organisers as

projecting and initiating struggles that involve people at the grassroots in assuming the responsibility for creating new values, truths, infrastructures, and institutions that are necessary to build and govern a new society (Boggs and Kurashige 2012, 68).

Fred Moten acknowledges the Boggses’ influence as an example of unpayable debts (Harney and Moten 2013, 153). What he and Harney offer in place of governance is “study”, a term of art that is also resolutely plain, in reference to the learning and planning that takes place among groups of people in spaces that are ungovernable by reigning institutions. Like the maroons of Saint-Domingue or the American South, study surely involves an order of its own, apart from the colonial university, a practice of insurgent self-rule. The maroons of study, for Harney and Moten, are never-settled communities of criminal exodus. But their maroons undertake “fugitive planning”. They study to plan, they plan so they can find the space and time to study. To do either, and therefore both, there must be something of the self-governance Harney and Moten seem to disavow.

These anticolonial thinkers see the trouble with governance in the sense of governmentality, a back-door aid to domination. And yet they also assert the otherwise troublesome kind of self-governing, the kind that is ungovernable and opaque and maroon from the vantage point of the imperial capitals – and, now, of the colonial platforms. The next section recalls how platforms have enabled their users to feel ungovernable and powerful for a time. But without the means of self-governing, those sensations have been fleeting.

3. Virality as a Colonising Strategy

I once entered the office of a labour organiser to find her there, head in her hands. She was running a campaign in the ever-shifting, just-in-time, atomised theatre of urban retail. Why so down? The workers were migrating to Instagram. At least on Facebook, you could corral them into groups, you could post updates. On Instagram, every message had to be hilarious or enraging or gorgeous if you wanted it to reach them. Sometimes the information an organiser needs to share is not any of those. But isn’t it still important?

Without persistent groups or organisations, Instagram’s eminent form of shared experience is the viral image, which circulates an affective impression of shared experience. To spread, the image must be the kind of image that would spread, according to the tastes of the poster’s followers and the secret churning of the platform’s engineering. An announcement for next week’s union meeting may not qualify. An organiser trying to strengthen workers’ bonds isn’t interested in infecting them like a virus.

The rise of ubiquitous social media rode on waves of protest, from the Battle of Seattle to the Arab Spring. Individual voices, linked with hashtags, seemed to herald collective liberation (Papacharissi 2015). And yet, despite the outpourings of promise and hope and near-term victories, those digitally mediated uprisings have fallen under the police of Mohamed Morsi and the bombs of Bashar al-Assad, the famines of the Yemeni civil war and the warlords of Libya. ‘Pirate’ political parties arising out of online protest have tended to collapse upon their first encounter with power, if they ever get there.

At the Occupy Wall Street encampment in 2011, reporters would arrive and be transfixed by the media centre – the nerve centre, the centre of power because it was media (Schneider 2013, 36). And media was powerful indeed, as it drew thousands upon thousands of people into what began as a small, precarious protest. Videos of police attacking activists, in particular, bred sympathy and participants, and a feeling that the movement might be on the brink of sparking some kind of revolution. At least at first. By the following year, the videos didn’t work the same way. As an activist monitoring the analytics data noticed at the time, “Riot porn is losing its luster for mass online consumption” (Schneider 2012). As the social-media attention waned, so did the movement’s confidence.

The likes of Vladimir Putin, Donald Trump, and Xi Jinping discovered how to outlast digital insurgencies, obscuring outbreaks of dissent under a deluge of obfuscation. Spontaneity is a commodity online, and empires can produce it for themselves.

Experience with multitudinous networks has led their early enthusiasts to call for more self-ordering. Hardt and Negri (2017) clarify their embrace of leaderless movements by stressing the need for “the institutionalization of free and democratic forms of life”, organised enough to be “able to take hold of the common” (xx). To Zeynep Tufekci (2017), the networked “signal” of movements can be self-defeating without organisational “capacity”.

The classic strategy of imperial domination – divide et impera, divide and conquer – proposes to dominate by training subjects to feel an illusion of power through their conflicts with one another. On colonial platforms, too, users direct their energy for and against each other, gaining influence and affirmation through their jousts and, in so doing, identifying themselves ever more deeply with the non-transferable reputation they obtain on the platforms. Virality is fleeting if it ever happens, but the possibility is there, so we pursue it. Before long we have recapitulated the final scene of the 1954 McCarthyist blockbuster On the Waterfront, in which the dockworkers flee from their union’s problems into the arms of the boss, newly able to experience their collective exploitation as individual liberation.

### Perm—Stacks—2AC

#### Perm: Stack the aff and the alt. Mutual exclusivity is counterproductive; in the cybernetic era, it’s more productive to assume partial interlinkages between movements and focus on layering them through stacktivist praxis. Not everyone has to be a stacktivist for the perm to solve!

Lovink, 20—founder of the Institute of Network Cultures at the Amsterdam University of Applied Sciences (Geert, “Principles of Stacktivism,” tripleC 18 (2): 716-724, 2020, dml) [emojis in original article…]

We can also read The Stack as a pedagogical framework within the Bauhaus tradition as a proposal for a general design principle, as John Thackara has recently done, updating the Bauhaus foundation course for the age of global warming[12]. As an abstract model describing the architecture of the Internet, the stack provides us with a useful spatial division of layers such as protocols, data, applications and user interfaces. Bratton’s notion of The Stack comes out of the US postmodern literary tradition of cognitive mapping (Jameson), which seeks to make intelligible (and containable) complex processes. Bratton combines this approach with decades long attempts to visualise the vertical integration of technologies drawn in 2D, with maps of networks that strive to capture relations between the different players. His aim is to produce a general network theory able to provide deeper insights in the dynamics of power: blowing up 2D tech engineering plans to a 3D dimension able to modulate planetary transformation.

Benjamin Bratton also invites us to think tech in relation to geo-politics and location. At the same time The Stack can be seen as method, a mechanism. However, the book is consciously vague about how material infrastructure and ideology relate. In the light of Trump, Putin and Xi Jinping, Bratton’s global engineer seems a tragic, retrograde figure. At best The Stack works well as a multi-disciplinary guideline of past globalist techno-social practices that, ironically, have become outdated since 2016, the year of its publication and the year of Brexit and Trump. For all its ambition to delineate the geo-political contours of techno-operations supposedly occurring on a planetary scale, the book settles with an oddly depoliticised aesthetic imaginary.

How can we free up The Stack from its current confinements and turn into an improvised dance? Let’s define a stacktivism, an active and reflective reading of stacks-on-the-move, that is not afraid of the subject (formerly known as user) and involves action, committed by confused, selfish, messy players. With this I mean grassroots interventions that do not take the current (Internet or IT infrastructure) stack as a given and turn the Will to Totality of the engineering class and their financial backers against itself. In comparison with the hacktivism and (tactical) media activism, stacktivism is indeed Hegelian in scope (Understanding Totality). It is confronting “das Ganze” and can be considered counter regressive as it takes into account the real-existing totality of today’s interrelated tech-architectures as opposed to the shrinking paranoid world of the online self that is in constant danger of collapse under the weight of its own self-image, surveillance, precarity and depression.

Niels ten Oever, Amsterdam-based Internet governance researcher and activist emphasises the importance of linking contexts and levels:

“The stack never was and never will be. The stack always was an abstraction, a story that was told to keep people working in an isolated manner, ensuring engineers stuck to their own layer. As long as you worked within your own parameters and delivered what the layer above and below you expected of you, you would not get into trouble. Stacktivism, on the other hand, works across the stack: it is a cross-stack collaboration, an attempt to realign and redesign the interfaces. Looking for interconnections and associations that cannot be drawn from above, that defy standardization. Interconnections that escape abstractions and stereotypes. They are established through dynamic and unpredictable handshakes: questions, answers, and re(-)cognition”[13].

Stacktivism is ambivalent and struggles with totality, the global scale and the planetary whatever. Think big, but act in small steps, that’s the motto. We Are Infrastructure. Stacktivism fights against the comfort of ignorance and tries hard to overcome the designed lure to drift off, hovering above it all in a subconscious fashion. While defining what stackitivism could become, it is good to keep mind that we’re free to use Bratton’s The Stack as a theory toolbox and not interpret it as a hermetic belief system. Designs can intermingle. In line with Bratton, stackivism claims to understand and oversee all levels, from the politics of code, algorithms and AI to the behavioural science manipulation of moods, interface design choices and is alert to 5G electronic smog, phishing emails, fake news and the other sleazy suggestions of your “friends”. How about your bot sensibility? This hyperawareness comes at a high price. Not everyone is a stacktivist ☹

Traditionally, direct action has been put in opposition to the talk fest. When we act, we stop talking and start doing. In the context of hacktivism this means that we no longer consume but start to code in order to be able to hack into computer systems in order to make real, tangible changes in society. Like Robin Hood, let’s define what stackivism-for-good could look like. How do we build rhizomatic links between global governance, protocol design, the ethics-without-consequences industry, code writing and investigative hacking? Who will be in charge of subversive foresight? Can we dream aloud together? How can delegate trust to our think tanks that work in the public interest?

Stacktivism is a sovereign attitude in that it is not begging for a correct form of representation and could be considered post-democratic and post-identity, yet remains always all-too-human. Inside Douglas Rushkoff’s Team Human stacktivists take up the task of creating missing links: they are the meme sharers, idea connectors, intercultural fellow travellers, poly-disciplinary networkers. The social creation of new protocols remains an act of common decision. We are fighting at the conceptual forefront of tech. Nobody needs to give us permission. Unlike the tactical media interventions of the 1990s, stacktivism is – by definition– abstract and conceptual in nature, knowing that code is power and power is code. How to dismantle invisible power? Do we fight abstractions with abstractions, design with counter-designs?

According to Internet and civil society researcher Corinne Cath we could see stacktivism as a “playful human evolution of Bratton’s concept of The Stack. It critiques its modular conception of world into discrete layers. To remedy this flattening, it calls for the inclusion of the inherent messiness of the Internet: the entangled basement wires, packets lost in translation, rugged governance cultures and the idiosyncratic usages of the humans who rely on it to function flawlessly”[14]. Francesca Musiani (CNRS, Paris) found the lessons of decentralisation telling:

“Decentralization often becomes a technical, political, economic and social aim in and of itself, reaching outside the ‘hacker’ circles of the early p2p systems. However, this has had side effects. Decentralization has become an objective in and of itself, with little understanding of intent or assessment of actual effects. I love Phil Agre's 2003 observation in this respect when he said: ‘Architecture is politics, but should not be understood as a substitute for politics’. Decentralized protocols are too readily assumed, because of their technical qualities, to bring about decentralized political, social and economic outcomes. A more fine-tuned appreciation of the social dimensions of the stack is likely to improve things in this regard”[15].

Media historicism (aka archaeology) has so far failed to develop critical concepts to understand the current situation, also known as platform capitalism. There is more to the Internet than the politics of the senses. Notation systems and perception are so 20th century. What matters now is who owns the Internet in terms of data centres, cables and PR; and this is first and foremost a question of material analysis. A comparison with the Roman road system, as described in Innis’s Empire and Communications is more relevant here[16]. Let’s, for instance, investigate the relation between the modernist stack and the fuzzy post-modern cloud buzzword.

How does Bratton’s design relate to recent proposals by stacktivists Francesca Bria and Evgeny Morozov for a European move towards “data sovereignty”? It’s too easy to unmask Bratton as a Californian techno-solutionist. How much is gained by planting this (now effectively empty) label on him? To determine, to think technologically remains an utmost urgency and it is precisely the “stacking” of issues, factors and contexts that will bring us further into the constitutive force of technical systems. The spectacle of clashing characters should not distract us (in fact, the silo phantom, the silence and separation is, oddly, our main problem, in this hyperconnected world).

### AT: Academy Bad

#### The aff’s cooperative re-imagination of communication and value can redefine the subjectivity of society. The academy is key—if we win a link, it proves that we’ve identified a crack in the system from which new relationalities can emerge.

Hall, 20—Professor of Education and Technology, De Montfort University (Richard, “Platform Discontent against the University,” *The digital age and its discontents: Critical reflections in education*, Chapter 7, 130-132, dml)

The proletarianization of the University is predicated upon atomized competition, which utilizes new forces of production to reshape relations between people, in order to extract value. A critical element of this is enforced separation between individuals, and the ability for individual agency to be repurposed by structural requirements. However, in order to extract maximum value, capital requires individuals to work in concert, or to collaborate as producers, distributors and consumers. This gives opportunities for cooperative re-imagination. For Marx (1866), the cooperative movement was a transformational force where it understood its relationship to labour as the point of social production. Thus, he argued that producer cooperatives, as opposed to consumer cooperatives, are a manifestation of class antagonism that can point towards ‘the republican and beneficent system of the association of free and equal producers’ (ibid., emphasis in the original). This analysis of cooperation rests on forms of self-mediation by human beings of their material activities in society. In an idealized cooperative state, activities are no longer piecemeal or solitary, or governed by capital; rather, they are governed by alternative networks of solidarity and purpose: ‘This is not possible without the community. Only within the community has each individual the means of cultivating his gifts in all directions; hence personal freedom becomes possible only within the community’ (Marx & Engels 1998: 86).

A focus on the communal and associational characteristics of cooperation is critical to Marx’s praxis, because in them he sees the individual developing the capabilities of their species (Marx 2004). As a result, a refocusing upon cooperative values and principles, grounded in the conceptual framework of the self-in-association, acts as a moment of refusal of alienated socialization, in which the producers of society are estranged from both the means and conditions of production of that society. However, discontent at the present state of things does not coalesce into a single, counter-hegemonic position, predicated upon a unified collection of alternative governing principles for life. It therefore becomes important to think about alternative forms of knowledge production and an integration with alternative conceptions of mutuality, solidarity and cooperation, such as those emerging from indigenous or marginalized communities.

Indigenous methodologies or modes of being help both to develop a fresh focus on knowledge and to reframe the idea of movement towards a more humane social production as a liminal process, engaging the body, emotions and cognition (Tuhiwai Smith, Tuck & Yang 2018). In this sensuous, epistemic opening, knowledge is rooted in people, place, philosophy, values, communities, axiologies and cosmologies, which generate ‘relational accountability’ (Wilson 2008: 77). Such accountability is mutual, respectful and dignified, and acts as a beginning for refusing the domination of knowledge from the global North imposed as progressive and rooted in an ideological, evidence-based epistemological standard. Here, cooperative techniques for social reproduction might enable forms of relational accountability between peoples and places. Moreover, in this process, they offer the possibility of liberating material forces, including technology, and connecting them to alternative conceptions of the world, in order to widen autonomy and freedom.

For Marx (1866; 1970) a cooperative revolution in the governance of technology forms a crucial strand in changing the general conditions of social production, because it redefines the subjectivity of society towards humanity and away from the commodity and the valorization of capital. If we are to do this, then a shared, associational expression of individual lives is required, in order to realize the essence of what it means to be human. Marx’s idea was that the expression of my life and those of my peers are immanent to each other, and should be mediated directly rather than through the market, private property, the division of labour and commodity exchange. This requires an alternative conception of how to integrate the forces of production into our communal being, and a liberatory conception of how those forces are subordinate to our essence and our social relations (Bookchin 2005). Beautifully, Marx (1844) argues that through such practices ‘our products would be like so many mirrors, out of which our essence shone’ as a ‘free expression’ of our lives.

At issue is how to find cracks in the system of capital, into which technologies for alternative, liberatory conceptions of society can be inserted. Dunayevskaya (1958) has argued that these need to be situated inside organizations that are beyond value-production, or they risk degenerating under competition. As a result, a re-imagination of the University has to engage with more than the cooperative possibilities of the collective ecosystems currently structured to reproduce value. A re-imagination of the potential for forces of production to enable social connection and knowledge sharing, and to liberate time for autonomous activity rather than the imposition of commodity production, comes up against structural contradictions. Thus, a re-imagination of technology as a means for liberating knowledge for a new society demands a new material literacy as a radical, pedagogical project at the level of society.

This is a transitional project that critiques the place of technology as it is currently instantiated inside the University. It critiques the relationship of the digital University, and its techniques of governance, to knowledge production and the generation of social wealth. It also critiques these relationships and techniques in terms of their ability to enable humanity to engage with global economic and environmental crises. It critiques the limitations in our collective ability to produce knowledge inside the University to engage with these crises, in part through the separation of polity and economy, such that the latter dominates the former. It critiques these limitations as they are reproduced inside organizations conditioned by the State to generate value through exploitation and expropriation. In this way, it moves beyond the fetishization of technologies and techniques, including the ways in which these are reproduced and enclosed inside institutions like universities (see Ampuja, Chapter 2, in this volume). The potential for relational accountability and the recomposition of peoples, places and technologies offer an alternative set of possibilities for intellectual work beyond the capitalized University.

#### Imaginaries change the world—the diffusion of cybernetics proves!

Atanasoski and Vora, 19 – Neda Atanasoski, Professor of Feminist Studies and Critical Race and Ethnic Studies at the University of California, Santa Cruz; Kalindi Vora, Associate Professor of Gender, Sexuality and Women's Studies at UC Davis; 2019( “Introduction: The Surrogate Human Effects of Technoliberalism,” *Surrogate Humanity: Race, Robots, and the Politics of Technological Futures*, Duke University Press, Accessed via Michigan Libraries, pg 23-24, bam)

Dissident Technologies and the Disruption of Technoliberal Enchantment: Our Itinerary

Dominant techno-utopic imaginaries direct funds and structure engineering research labs around the world, and therefore also impact the distribution of differential conditions of comfort versus misery in the present along vectors of race, gender, class, and other social hierarchies. The surrogate human effect explains how difference continues to inform what subjects become legible as human through technology design imaginaries that respond to market values by focusing on innovating and improving, rather than challenging, social and cultural structures and processes that are predicated by categories of gendered racial hierarchy. To this end, Denise da Silva offers the concept of “knowing (at) the limits of justice,” a practice that “unsettles what has become but offers no guidance for what has yet to become.”59 To insist on “knowing at the limits” of representational categories of difference, we must ask: If the predominant fantasies of systemic social change in mainstream Euro-American public discourse dwell upon the techno-utopics of a world in which all of those who are already human and already subjects ascend into the realm of those whose lives are supported by “human-free” or “unmanned” technological infrastructures of service (whether in factories, in the military, or in the nursing home), then how do we think about the relationship of new technologies to possible fields of political protest or action?

The dissident technological imaginaries we include in each chapter take up categories that challenge those of technoliberal capitalism and its projected futures. We read these design imaginaries as exploring the possibilities of technology to break from historically sedimented dynamics of freedom and unfreedom woven into the fabric of technological modernity. In addition to offering critique, each chapter thinks through how such design imaginaries can push at the limits of what is possible, disrupting the confining notions of (technoliberal capitalist) possibility housed in the engineering imaginaries we critique. We explore these questions through juxtaposing engineering imaginaries that embrace the surrogate effect, thereby advancing the infrastructure of technoliberal futures, with imagi- naries that do not.

### AT: Afropessimism

#### The digitization of the carceral state disproves the historical continuity of anti-Black oppression—it takes different forms.

Jefferson, 20—associate professor of geography and geographic information science and O’Connell Scholar in the College of Liberal Arts and Sciences at the University of Illinois Urbana-Champaign (Brian, “Introduction: NextGen Nightmare,” *Digitize and Punish: Racial Criminalization in the Digital Age*, Introduction, pg 13-16, dml)

A point of emphasis in the book is that carceral power is silently spreading through infrastructures of cellular towers, datacenters, fiber-optic cables, smart sensors, and video cameras. Carceral functionality is becoming a key attribute of the smart city. This is not meant to say that the prison-industrial complex is being wholly supplanted or that it is bound to disintegrate. Even though incarceration rates have reached their lowest points in decades, the history of carceral management is not one of a linear development. Nor is it a history of a changeless institution. Carceral space has manifested in the form of extraordinary rendition sites, immigrant detention centers, and internment camps. This book traces an emergent form of carceral space that is characterized by machines that traverse human anatomy, public housing facilities, public schools, transportation systems, telecommunications systems, and street networks in U.S. cities. The book also emphasizes that the deeper telecommunications and IT firms entrench themselves in crime control policy, the more likely it is for these infrastructures to continue to expand.

The extension of carceral management through the Internet of Things (IoT), or networks of devices that communicate with each other, is greatly influenced by the movement of capital.42 On one hand, the carceral state’s circumscription of black and latinx communities was partly catalyzed by the flight of industry from cities, which rendered entire groups deskilled and unemployable. Decades of revelatory research demonstrates how cities turned to mass criminalization to manage the enormous economic, political, social, and medical problems arising from deindustrialization.43 On the other hand, in addition to outbound industrial capital, the carceral state’s digital architecture owes its existence to inbound information capital. The infrastructure sector has emerged as one of the most important sectors in finance, knowledge, and technology industries.44 IT companies have insinuated themselves in seemingly all facets of urban life, including government agencies, private businesses, social networks, transportation systems, workplaces, and infrastructure. These companies have also nestled their way into criminal justice administration, which is reshaping geographies of carceral governance.

A central argument in this book is that the criminal justice system’s smart infrastructure is creating new geometries of carceral space. On one hand, carceral space is incredibly centralized. Extraordinary rendition sites, detention centers, jails, and prisons, which are designed to monitor, discipline, governmentalize, punish, and sometimes execute or torture those caught within their grasp, are a few examples. IT firms have penetrated these spaces. For instance, technology corporations sell geographic information systems to help custodial authorities organize cell arrangements according to demographic categories, predict inmate movements and behaviors, and identify potential escape routes (see chapter 2). Yet, on the other hand, carceral space is incredibly decentralized. Carceral geographers highlight the elaborate logistics required to shuttle humans, information, and resources across prison facilities and entire landscapes.45 Architects have characterized rural prison facilities as urban exostructures, as they provide relief to the city’s overburdened criminal justice apparatus.46 Technology firms have also infiltrated this decentralized dimension of carceral management. Wireless networks of smart cameras, phones, sensors, and tablets extend the reach of the carceral system. At the scale of the city, smart cameras and environmental sensors send alerts to patrol vehicles dispersed throughout street networks. On regional scales, real-time crime centers receive data and transmit them throughout states and, increasingly, between them. Owing to their portability, criminal justice technologies also circulate on international scales. Today there exists a global market for public security technology that traverses capitalist, communist, and socialist nations. On yet a grander scale, electronic forms of monitoring probationers depend on Global Positioning System satellites, which extend the reach of carceral technology all the way into low Earth orbit.

Taking the carceral state apart and making it less recognizable through the lens of smart infrastructure helps short-circuit illusions that it is neatly bounded in terms of geography and functionality. While the illusion of a monolithic carceral Leviathan echoes modern theories of the state that never seem to fade away, carceral statecraft is an open, dynamic, and variegated sociotechnical process of quarantining human beings. As such, our understanding of carceral state power, Katherine Beckett and Naomi Murakawa observe, “must be as capacious, complex, and adaptive as the policies and institutions involved in it.”47 The present study insists that analysis of this power’s sociotechnical substrate is also necessary to understand carceral conditions in the twenty-first century.

DESIGN OF THE BOOK

Digitize and Punish retells the history of mass criminalization by focusing on technology corporations and technology bureaus. The book’s objects of analysis are not criminalized communities but rather the computer programmers, corporate-bureaucratic intellectuals, state officials, and technologists who update the tools that criminalize them. It tells untold stories of the contingencies, failed projects, unintended consequences, and technical breakthroughs involved in constructing the digitized carceral state. It illustrates how these efforts have simultaneously augmented the carceral state and created new avenues of subverting it.

This project employs an intersectional approach to understand the nexus of carceral power, racism, and IT capital.48 The perspective was notably captured by the Combahee River Collective and Kimberlé Williams Crenshaw, who demonstrated the inadequacies of understanding social hierarchy through one measure, or axis of division.49 As such, structural analysis of the relations between racial difference, technological development, and political economic mutation is necessary to understand the relevant factors in racial criminalization in the digital age. The question is not if racial criminalization behaves in a structural manner but rather how it maintains, if not increases, its structural integrity from generation to generation. This book therefore seeks to explain how information capital exploited the surge of racial criminalization near the end of the last century and, at the same time, how racial criminalization was exploited by the rise of information technology.

#### The aff is an internal link turn and the perm solves. Embracing both black use of technology as well as blackness as technology creates moments of sociality within ontological structures of fungible commodification---that places blackness, in this sense, as paraontological with respect to Wilderson

Brock, 20 - André Brock Jr., PhD, Associate Professor in the School of Literature, Media & Communication at the Georgia Institute of Technology; 2020(“Making a Way out of No Way Black Cyberculture and the Black Technocultural Matrix,” in *Distributed Blackness African American Cybercultures*, NYU Press, 2020, Accessed Online via Michigan Libraries, bam)

Throughout this book, I have framed Black online identity and Black digital practice as Black cyberculture, an awkwardly named construct incorporating cyberspace (itself a dated term) and technoculture. As mentioned earlier, technoculture can be understood as the relations between, and politics of, culture and technology. Dinerstein (2006) argues that “technology is the American mythos” (p. 570). When defined this way, however, technoculture often tricks upon the racial identity of whiteness, and white racial ideology and technological beliefs become the norm. That obviously won’t do! Black technology users are not white (even if they are Western), so it becomes necessary to interrogate how Black people make sense of their existence as users and as subjects within advanced technological artifacts, services, and platforms. This final chapter is that catechism, firmly placing Black folk at the center of information and communication technology use. I offer this interrogation not as a summary of the previous chapters but as a provocation for those who are interested in centering Blackness as digital practice.

Reorienting technoculture to incorporate Blackness invites an inquiry into the possibilities of Blackness as technology—not Black bodies (been there, done that) but Blackness as technology—in the same way that Blackness often stands in for the best of American entertainment and culture. I am not arguing for minstrelsy and blackface here, to be clear, even though those representations of Blackness are as American as apple pie. Nor am I suggesting that Blackness is a nonserious use of technology; indeed, technology use for Blacks often occurs from the margins of society, where survival, joy, and resistance intertwine uncomfortably in the everyday. Chun (2013) contends that race-as-technology “posits a comparative equality or substitutability—but not identity—between the two” (p. 8). Chun goes on to probe how whiteness incorporates science and technology to build technologies and institutions of race—a helpful formulation for antiblackness and technology but not as necessary here. Instead, I would like to begin from the introduction’s discussion of “technology as text” to build out from the possibilities of Black thought into a concept of Black technoculture. From there, I will discuss Afrofuturism as an analytic for Black technology use and time and Black technoculture. Finally, I close with a foray into a libidinal framework of Black technoculture.

Technologies as Cultural Texts

My argument here centers on the digital’s networked and distributive capacity for banal, everyday Black information and computer technology (ICT) practices, but others have argued similarly for artistic and technical artifacts (Fouché, 2006; Ebo, 1998; McGahan, 2013; Weheliye, 2002). “Technology as text” has multiple postulations for distributed Blackness and for Black technoculture:

• code (interface and practices)

• the digitally distributed content generated by and mediated by that code

• signifyin’ and other cultural discourses of Black digital practitioners

The first two are instrumental and organizational; think of the possibilities for art and discourse that were introduced by Grandmaster Flash’s innovative technique of scratching records as part of a musical performance. The last marks the generative relationship between the first two, revivifying the noncommunicability of Blackness into a mediation for the production of Black life and thought. From this perspective, code, digital discourse, and language-as-culture can (and do) constitute racial identity. Adding technological mediations of discourse (Herring, 2001) allows one to examine computer-mediated communication and digital practice as racial identity as well.

It is vital, however, to not incorporate the digital’s technocultural alienation (drawing on whiteness’s Manichaean separation of mind and body; Dyer, 1997) into my formulation of online Blackness. I wrote the previous sentence long before I read Wilderson (2010), but his words advance my claim: “As an accumulated and fungible object, rather than an exploited and alienated subject, the Black is openly vulnerable to the whims of the world and so is his or her cultural ‘production’” (p. 56). Here Wilderson states that because Black folk have no legible stature in the West as political agents, they have no inalienable rights to Black cultural production. Thus Blackness (in online spaces and elsewhere) is immediately captured by Western culture, leaving little possibility for emancipation from that framework. I agree: while I recognize possibilities for emancipation through radical and decolonizing digital practices, my pressing concern for Black technoculture is to make manifest the vitality and joy of Black uses of ICTs. While these libidinal impulses may become commodified or surveilled, they are paraontological—that is, the embodied cognition they express preexists the platforms on which they are published, visible, and deemed appropriate for consumption. The digital mediates culture—in this case Blackness, but otherwise typically white Western—in ways that allow for sociality despite commodification. The next section reviews other researchers’ takes on Black technological practice, which I then extend to specifically examine digital practice.

### AT: Capitalism

#### Collective resubjectivization generates material liberation.

Hall, 20—Professor of Education and Technology, De Montfort University (Richard, “Platform Discontent against the University,” *The digital age and its discontents: Critical reflections in education*, Chapter 7, 130-132, dml)

The proletarianization of the University is predicated upon atomized competition, which utilizes new forces of production to reshape relations between people, in order to extract value. A critical element of this is enforced separation between individuals, and the ability for individual agency to be repurposed by structural requirements. However, in order to extract maximum value, capital requires individuals to work in concert, or to collaborate as producers, distributors and consumers. This gives opportunities for cooperative re-imagination. For Marx (1866), the cooperative movement was a transformational force where it understood its relationship to labour as the point of social production. Thus, he argued that producer cooperatives, as opposed to consumer cooperatives, are a manifestation of class antagonism that can point towards ‘the republican and beneficent system of the association of free and equal producers’ (ibid., emphasis in the original). This analysis of cooperation rests on forms of self-mediation by human beings of their material activities in society. In an idealized cooperative state, activities are no longer piecemeal or solitary, or governed by capital; rather, they are governed by alternative networks of solidarity and purpose: ‘This is not possible without the community. Only within the community has each individual the means of cultivating his gifts in all directions; hence personal freedom becomes possible only within the community’ (Marx & Engels 1998: 86).

A focus on the communal and associational characteristics of cooperation is critical to Marx’s praxis, because in them he sees the individual developing the capabilities of their species (Marx 2004). As a result, a refocusing upon cooperative values and principles, grounded in the conceptual framework of the self-in-association, acts as a moment of refusal of alienated socialization, in which the producers of society are estranged from both the means and conditions of production of that society. However, discontent at the present state of things does not coalesce into a single, counter-hegemonic position, predicated upon a unified collection of alternative governing principles for life. It therefore becomes important to think about alternative forms of knowledge production and an integration with alternative conceptions of mutuality, solidarity and cooperation, such as those emerging from indigenous or marginalized communities.

Indigenous methodologies or modes of being help both to develop a fresh focus on knowledge and to reframe the idea of movement towards a more humane social production as a liminal process, engaging the body, emotions and cognition (Tuhiwai Smith, Tuck & Yang 2018). In this sensuous, epistemic opening, knowledge is rooted in people, place, philosophy, values, communities, axiologies and cosmologies, which generate ‘relational accountability’ (Wilson 2008: 77). Such accountability is mutual, respectful and dignified, and acts as a beginning for refusing the domination of knowledge from the global North imposed as progressive and rooted in an ideological, evidence-based epistemological standard. Here, cooperative techniques for social reproduction might enable forms of relational accountability between peoples and places. Moreover, in this process, they offer the possibility of liberating material forces, including technology, and connecting them to alternative conceptions of the world, in order to widen autonomy and freedom.

For Marx (1866; 1970) a cooperative revolution in the governance of technology forms a crucial strand in changing the general conditions of social production, because it redefines the subjectivity of society towards humanity and away from the commodity and the valorization of capital. If we are to do this, then a shared, associational expression of individual lives is required, in order to realize the essence of what it means to be human. Marx’s idea was that the expression of my life and those of my peers are immanent to each other, and should be mediated directly rather than through the market, private property, the division of labour and commodity exchange. This requires an alternative conception of how to integrate the forces of production into our communal being, and a liberatory conception of how those forces are subordinate to our essence and our social relations (Bookchin 2005). Beautifully, Marx (1844) argues that through such practices ‘our products would be like so many mirrors, out of which our essence shone’ as a ‘free expression’ of our lives.

At issue is how to find cracks in the system of capital, into which technologies for alternative, liberatory conceptions of society can be inserted. Dunayevskaya (1958) has argued that these need to be situated inside organizations that are beyond value-production, or they risk degenerating under competition. As a result, a re-imagination of the University has to engage with more than the cooperative possibilities of the collective ecosystems currently structured to reproduce value. A re-imagination of the potential for forces of production to enable social connection and knowledge sharing, and to liberate time for autonomous activity rather than the imposition of commodity production, comes up against structural contradictions. Thus, a re-imagination of technology as a means for liberating knowledge for a new society demands a new material literacy as a radical, pedagogical project at the level of society.

This is a transitional project that critiques the place of technology as it is currently instantiated inside the University. It critiques the relationship of the digital University, and its techniques of governance, to knowledge production and the generation of social wealth. It also critiques these relationships and techniques in terms of their ability to enable humanity to engage with global economic and environmental crises. It critiques the limitations in our collective ability to produce knowledge inside the University to engage with these crises, in part through the separation of polity and economy, such that the latter dominates the former. It critiques these limitations as they are reproduced inside organizations conditioned by the State to generate value through exploitation and expropriation. In this way, it moves beyond the fetishization of technologies and techniques, including the ways in which these are reproduced and enclosed inside institutions like universities (see Ampuja, Chapter 2, in this volume). The potential for relational accountability and the recomposition of peoples, places and technologies offer an alternative set of possibilities for intellectual work beyond the capitalized University.

#### Mastery DA: The notion of a universal dialectic is a neurotic projection of the will to mastery---it transforms the alt into genocidal party politics---only the affirmative’s rejection of static linearity solves

Berardi 15 (Franco Berardi, like Lenin but not depressed, *AND: Phenomenology of the End*, p. 90-95)

Desire for the Absolute is visible in the historical sphere as a will of total palingenesis, purification of the social community from the traces of the past. The reference to purity is transparent in the Russian conception of Revolution, particularly in the Leninist persuasion that the revolutionary political party is the “incarnation” of the pure idea coming down from German Philosophy, and must be embodied by a small organization of professional bearers of the Revolutionary Truth. The Russian exacerbation of the role of pure subjectivity entered the scene of the world history in 1917. The Soviet Revolution—that Lenin managed to unleash against the will of many prominent leaders of the Russian socialist movement, provoked a catastrophic polarization in the worldwide social conflict, and forced the worker’s movement to identify with a totalitarian experiment, based on the authoritarian statalization of class struggle. The Russian revolution provoked an irreversible rupture and a permanent laceration in the body of society whose effects persisted worldwide all along the century. Lenin forced the workers of the world to defend the Socialist State of the Soviets, and to enter a process of permanent war. This war lasted until 1989, but since the beginning the worker class was doomed to unavoidable defeat. The messianic utopianism, widespread in the Russian society of the nineteenth century merged with the hyper-voluntaristic project of the Bolsheviks, so the history of Communist revolution began as a tragedy in the context of the immolation culture, and since the beginning was destined to end as a tragedy. The violence and the authoritarianism that the Leninist experiment unleashed in the country and exported worldwide brutally changing the prospects of the international movement for worker’s emancipation, were inscribed in the Russian history of the previous centuries, and still prevail in the Russian political life, after the end of the Soviet dictatorship. Leninist communism may have ruined Russia, but certainly Russia has (forever?) ruined Communism as a possible alternative to Capitalism, as the Russian subjectivism and cult of purity have dragged the international movement of the workers into a vision of permanent military mobilization that was not part of the Marxian imprinting. The spontaneous goal of the workers movement is to expand the space of autonomy from capitalist exploitation. The idea that the movement is taken in a dialectical contradiction is an effect of the Hegelian interpretation of the social process: this idea becomes historical reality when the Russian palingenetic cult of pureness melts with the Hegelian tradition. The fusion of Marxism and Leninism is the origin of the workers defeat, in my opinion. Lenin brings into the worker’s political discourse an element of subjectivism and of purity that did not belong to the experience of autonomous social movements. The workers movement was aimed to emancipate spaces of life and of the territory from the capitalist domination, but the Leninist breakthrough transformed the movement into a project of absolute separation from the existing world, of radical demolition and of palingenetic purification. In the first part of the book, Lenin confirms Lassalle’s argument: the purification (epuration, cleansing) is strengthening the party. This idea of ideological cleansing (epuration) is the main thread of the history of the Soviet Communist Party, particularly in the Stalin age. According to the words of Lenin: “the worker class is only able to elaborate an economic unionist consciousness, but is unable to understand the radical opposition to the system.” (Lenin, What has to be done?) This impurity of the worker class has to be overcome, so that society can adapt to the purity of the communist ideal. Only a party which is the bearer of the pure Logos can be the bearer of the revolutionary project—not the aggregation of impure social bodies. In her biographical essay on Lenin, the French historian of Georgian origins Hélène Carrère d’Encausse speaks of two major episodes of clinical depression in the life of Lenin that are generally ignored by the hagiografic Leninist tradition. The book (Lenine, la Revolution et le pouvoir, 1979) is interesting especially because it is focusing on the affective life of the communist leader: the importance of the relation with the mother, the sister, and particularly of the wife, Nadeezda Krupskaja, who took care of him in the periods of acute psychic crisis. The book also speaks of Ines Armand, the lover who disturbingly entered the life of Lenin, and was later removed, neutralized, as a potential danger for the political integrity of the leader. Depression is the peculiar feature of the psychological description of Lenin, and depressive crises are coinciding with the most important political decisions of his life. The first major crisis, according to Hélène Carrère d’Encausse, occurred in the year 1902, and coincided with the decision of founding the Communist party and the draft of What has to be done? The second occurred in 1914, when Lenin takes the decision of breaking with the Second International before Zimmerwald Congress, and the Communist Schism at the European scale. The third occurred in Spring 1917 and coincided with the decision of launching the Soviet insurrection which actually took place in October. These decisions, that marked the emergence of the Communist identity, and forced a voluntary acceleration on the history of class struggle all over Europe and worldwide, can be linked in my opinion with the depressive cycle of Lenin. When intelligence is depressive, only will is the therapy that makes possible ignoring the abyss. The abyss is not removed, not resolved, not avoided or overcome. It is ignored, but still it is there, and the decades following the Revolution have actually exposed its persistence, so that the century sunk down into the abyss. More than in the political meaning of the decisions of Lenin, here I’m interested in the relation between Bolshevik voluntarism and the male inability to deal with depression. By the political point of view, the Bolshevik breach provoked a general precipitation of the confrontation between workers and capital in the world: workers were pushed everywhere towards a totalizing form of opposition, and actually towards civil war. The social autonomy was obliged to choose between revolutionary terror and capitulation. And where the communist parties succeeded in seizing political power, this was turned into violent dictatorship and submission of social life. This way the Leninist strategy prepared the worldwide catastrophe that at the end of the century has provoked the worst possible defeat whose effects we’ll be experiencing for decades. The project of a rebirth of the world beginning with the palingenetic violence of the revolution is a mythology that has no historical foundation. History has never known abolition, palingenesis or rebirth. History is always about stratification, negotiation, coevolution, autonomy or dependence, identification or extraneousness. Not about abolition. Leninism can be considered as an attempt to deny depression, as an assertion of the purity of will, as a refusal to accept the finiteness of human potency: male hysteria that was already at work in the Dostoevsky’s writings.

#### Marxist theorizations of change fail to account for the ontological nature of modern capitalism – the aff’s approach is the only way to create individual value in the world of utility

Magrini 11 (James, Professor at the College of DuPage, “Working to Recover the Essence of Education for the Sake of Teaching and Teacher Education: Towards a Phenomenological Understanding of the Forgotten, Ontological Aspects of Learning” p. 4)NCF

It is evident that there is a serious problem with educational procedures emerging out of the “bureaucratic/rational choice model” that is two-fold in nature, a problem that is in fact antibiotic, as in a vicious sense of codependence. Instructors who are increasingly alienated from what might serve as legitimate, or authentic, curriculum for the preparation of teachers entering the field are slaves to institutions governed by pre-determined standards of achievement. These institutions are then filtering ill-prepared (alienated) teachers into a system that is governed in much the same way, namely, by standards and competencies established by bureaucratic agencies that are at a remove from authentic educational purposes and practices. Teachers are thus alienated in a duplicitous sense, both from the curriculum they are now forced to teach and the students who cannot relate to what is being taught. Bonnett (2001) echoes the sentiments expressed earlier when stating that the current “predisposition to regard outcomes of education as definable in advance of the process of education” engenders a deterministic system of education that obscures authentic subject-hood and we lose sight of the fact that humans are “individual centers of consciousness capable of relating to the world in ways that have personal meaning, for this is essential to human being against some sort of mechanized and depersonalized being” (p. 30). In short, there is a loss of ownership on the part of both educator and student, but beyond this, there is a loss of authentic subject-hood; ironically, by means of education, we are losing sight of what it means to be truly human. The alienation from the curriculum and authentic subject-hood of which I speak should not be conceived in terms of Marxist theory, which tends to focus on ideology and the critique of capitalism and its detrimental effects on schools. Rather, I conceive alienation and depersonalization in terms of what Heidegger (1979) calls the oblivion, or forgetting, of Being, which is grounded in the failure to ask about “the truth of being itself” and about “the way the essence of human being belongs to the truth of Being” (p. 246). This condition, which pervades the world of education, grows from the tradition in Western metaphysics and its subsequent influence on the rise of science and technology. In short, education is moving us farther away from essential issues of human dwelling as linked with our Being, and the ontological aspects of our existence. It is now to the potential recovery of this essential, forgotten ontological notion of authentic Beingin-the-world as related to education that I turn.

#### Stacktivism socializes technology and reshapes the foundation of capitalist notions of value.

**Dragona 15**(Daphne, PhD from the Faculty of Communication & Media Studies of the University of Athens, “From Community Networks to Off-the-cloud toolkits: Art and DIY networking”, CS)

Firstly, all networks discussed follow a usercentered approach. The human and non human elements that a network involves are balanced by always allowing the users to have control of the nodes of the network; setting them up, controlling them and sustaining them. In the era of algorithmic automation and control, its important to remember what Munster and Lovink wrote, that the rise of networks should be made understood as an all too human behaviour [77]. Whereas as Medosch says ‘in ubiquitous computing, it is usually the devices which get smarter and the people who remain stupid’, in the cases of such initiatives a ‘new Internet of People’, following here Nold and van Kranenburg, and can emerge against the Internet of things [78, 79]. Secondly, the topologies of DIY networking are exposed and understood by a merging of the social and the technological. As a user is always behind a node and in control of a node, it is easier to realize the edges and nodes, the architecture and potentiality of the network. This idea of “becoming the machine” that Pasquinelli mentioned can be understood as becoming the node and gaining control of the network. Thirdly, all infrastructures of different scale are based on open software and hardware leaving open to the users the possibility for modifying and even repurposing them for their own needs; this way not only the DIY but also the DIWO ethos is encouraged embracing the logic of thinking, sharing, working together. This in a manifestation of what Hardt and Negri have stated when they argued that “being with” is no longer enough”; a “doing with” is necessary [80]. Alternatives based on collaboration and sociality are introduced to spread and teach people how not only to modify and use infrastructures but also to make decisions, possibly based on criteria which are qualitative and humanistic [81]. Staying out of the market of centralized systems and platforms, a new system and theory of value is embraced. Encouraging forms of exchange economy and providing tools and knowledge freely and openly, a significant effort is made for social value to outbalance market value, for sharing networks to surpass zones of property. Fourthly, and in continuation of the above arguments the infrastructures proposed can be seen as part of the new ‘Network Commons’ as Armin Medosch puts it. Although Medosch refers primarily to the community networks, this can greatly stand for the wider family of offline sharing networks as they are systems in terms of infrastructure and content that are meant to be constructed, possessed and managed by all. Through such platforms, users are invited “to speak and think, to become informed and to participate”, as Stavrides has put it for the necessity of the contemporary commons [82]. The making of the common in the case of infrastructures is therefore a process based on potentialities, skills and affects of the users and this can be approached as meaningful acts of commoning.

### AT: Ivory Tower

#### Stacks are as material as you can get.

**Mohorčich 17**(Jospeh, Ph.D., Johns Hopkins University, “POWER PRAGMATISM”, CS)

A sensible plan for radical transformation, therefore, will start with a plan for taking care of basic human needs: an alternative technology stack for keeping human beings alive so that they don’t die when the standard systems of feeding and caring for them fail or are removed. Gupta argues that “you don’t [convert to a new life-support stack] by pulling the old one down. You [convert] by building a new one, prototyping it, bootstrapping it from the resources of the old, proving that it works, and then pulling the population across.”403 As Bratton points out, stacks are “intrinsically modular,” so each is “also a platform, and an interface even, for the redesign and replacement of the Stack-we-have with a Stack-we-want.”404 To think about radical transformation—up to and including revolution—without thinking about infrastructure is to neglect that engineering and politics are embedded in each other. Because any plan for political transformation must start with some kind of life-support plan, it makes sense to start working on these types of plans and to bring this work explicitly into the political-theory fold. Working to diagram and assemble alternative life-support stacks has the potential to convert cycles of radical action from self-defeating to self-reinforcing. As activists and thinkers are increasingly existing stacks, and to not get enmeshed in questions about who’s going to call in sick to work or argue with Comcast this week, they are able to think, agitate, and act in a more engaged manner, which opens space for further political-material-technical moves that strengthen alternative stacks, which engenders further agitation and thought, which restarts the cycle. For example, Bitcoin’s role as a functional component of an alternative financial stack (i) demonstrates the technical viability of blockchain-based experiments to create alternative stacks for education, personal identification, energy markets, housing, carbon emission tracking, and so on, and (ii) pulls developers, users, and billions of dollars in wealth from existing financial stacks into alternative ones, which creates the material, technical, and social grist for further developments. To be sure, purchasing baby formula or pizza with a blockchain currency is not itself a shatteringly radical move, especially if the supply chains for what you have bought can still be traced through to structures of degradation, exploitation, and accumulation. This is why building alternative stacks for the production and transport of energy, food, heat, and information that interleave with alternative financial structures like blockchain currencies remains a critical and self-reinforcing task.406 Developing alternative life-support stacks opens up ways of rethinking radical separatism.

### AT: Settler Colonialism

#### The development of imperial technology explains the mechanisms of dispossession better.

Harris, 4—Department of Geography, University of British Columbia (Cole, “How Did Colonialism Dispossess? Comments from an Edge of Empire,” Annals of the Association of American Geographers, 94:1, 165-182, dml)

The emphasis on culture in studies of colonialism tends to obscure other forms of colonial power while making it impossible to contextualize the cultural argument and assess its salience. Rather than focusing on texts, systems of signification, and procedures of knowledge generation, as the colonial discourse literature is wont to do, a fuller understanding of colonial powers is achieved by explaining colonialism’s basic geographical dispossessions of the colonized. In so doing, the issue of power is not prejudged and the particular roles of different modes and theories of colonial power come into focus. I explore these propositions by considering the powers underlying the reserve (reservation) system in British Columbia, a system that, by allocating a tiny fraction of the land to native people and opening the rest for development, facilitated the geographical reorganization of the province. My conclusions are these: the initial ability to dispossess rested primarily on physical power and the supporting infrastructure of the state; the momentum to dispossess derived from the interest of capital in profit and of settlers in forging new livelihoods; the legitimation of and moral justification for dispossession lay in a cultural discourse that located civilization and savagery and identified the land uses associated with each; and the management of dispossession rested with a set of disciplinary technologies of which maps, numbers, law, and the geography of resettlement itself were the most important. Although no one body of theory explains colonial power, several theoretical perspectives yield crucial insights. Key Words: colonialism, colonial discourse theory, deterritorialization, colonial land policies, governmentality, reservations, British Columbia.

Influenced by Michel Foucault’s analysis of the relationships of power and knowledge (1972), by Edward Said’s examination of Orientalism (1978), by textual theory harnessed to colonial discourse analysis, and by many studies of the values and ideologies enmeshed in particular colonial encounters, most postcolonial scholars now identify culture and associated procedures of knowledge generation as the dominant power relations associated with colonialism. Whereas Frantz Fanon (1963) emphasized violence—the power of the gun—and Marx, to the extent that he wrote on colonialism, the aggressive reach of capital, postcolonial research and writing situates the momentum of colonialism in the culture of imperialists and colonists. A central goal, therefore, of colonial discourse theory is to identify the assumptions and representations inherent in colonial culture—in the binary of civilization/savagery, in the erasures of Aboriginal knowledge of time and space, in assumptions about race and gender, in the concept of the land as empty (terra nullius), and so on—and then, insofar as possible, to expose their contemporary manifestations. This work has focused much scholarly energy and has yielded important theoretical and practical results, but it is less clear that it has revealed the principal momentum and power relations inherent in colonialism.

Originating in literary and cultural studies, colonial discourse theory, indeed postcolonial scholarship generally, privileges the investigation of imperial texts, enunciations, and systems of signification. In so doing, it exposes implicit modes of seeing and of understanding that are held to infuse and validate colonialism while imparting much of its momentum. If Said offered broadly inclusive descriptions of colonial culture, and if others, more recently, have emphasized the variety of colonial voices and the importance of a local, contextual appreciation of different colonial cultures (e.g., Thomas 1994), in either case, culture is treated as a primary locus of colonial power. Moreover, as elements of colonial culture are assumed to have outlived formal colonial regimes, their identification becomes an active political project—the decolonization of representation (Hall 2000, 5). In itself, this is commendable enough, but if studies of colonial culture are not contextualized among other forms of colonial power, then it is well nigh impossible to assess the particular work and the relative salience of colonial culture itself. A study of travel writing, for example, may yield an appreciation of the inflected seeing of travelers and of the complicity of such seeing with colonial projects, while not beginning to address the relative importance of travelers’ seeing and writing in the whole colonial enterprise. Given its focus, it cannot. At best, it can yield a nuanced understanding of traveler perceptions and values, and suggestive ideas about their relationships with colonialism. Colonialism’s complexity may be affirmed, so too, perhaps, the discursive construction of reality comments tied more closely to theory than to a situated knowledge of colonial practices and power relations.

In the hands of some of its most able practitioners, postcolonial scholarship is a potent means of exploring the reworking (‘‘provincializing’’) of European thought at and for the margins of empire (Chakrabarty 2000, 16). However, most postcolonial scholarship is written out of British or American universities and emanates from the heart of a recently superceded empire or of a recently ascendant one that hesitates to acknowledge its own imperial background. American postcolonial scholarship is not preoccupied with America (Hulme 1995; Thomas 1994 172–73). In the background of such scholarship are European theorists, particularly Foucault, Derrida, and Gramsci; in the foreground, European colonial thought and culture. In these circumstances, as many have pointed out, it tends to be Eurocentric—or as the Australian anthropologist Patrick Wolfe puts it, occidocentric (1999, 1). So positioned, it is well placed to comment on the imperial mind in its large diversity, and even—especially in the hands of scholars like Homi Bhabha and Dipesh Chakrabarty who grew up in former colonies—on the ways in which European thought has been inflected and hybridized by its colonial encounters, but not on the diverse, on-the-ground workings of colonialism in colonized spaces around the world. A central claim of the distinguished Indian subaltern historian, Ranajit Guha, is that if British historical writing on the subcontinent reveals something of Britain and the Raj, it reveals nothing of India (1997). Somewhat similar criticisms have been made of much of the postcolonial literature: that it (or parts of it) anticipates a radically restructured European historiography, that it allows for nothing outside the (European) discourse of colonialism, that it is yet another exercise in metatheory and in European universalism (e.g., Slemon 1994; McClintock 1994). As the literary theorist Benita Parry puts it, the postcolonial emphasis on language and texts tends to offer ‘‘the World according to the Word’’ (1997, 12)—and the word tends to be European. But unless it can be shown that colonialism is entirely constituted by European colonial culture (a proposition for which it is hard to imagine any convincing evidence unless the concept of culture is understood so broadly that it loses any analytical value), then studies of colonial discourse, written from the center, must be a very partial window on the workings of colonialism.

The discipline of geography has responded to postcolonial thought in a variety of ways (Clayton 2003). Among others, studies of colonialism itself have come into vogue, most of them written in Britain, a few from the edges of empire. I am struck by how much the character of these studies has been influenced by the locations of their authors. Consider, for example, two recent books by historical geographers: Felix Driver’s Geography Militant: Cultures of Exploration and Empire (2000), and Frank Tough’s ‘‘As Their Natural Resources Fail’’: Native Peoples and the Economic History of Northern Manitoba, 1870–1930 (1996). From opposite perspectives, they treat a fairly similar period of British colonialism. Driver analyzes the culture of exploration, particularly the sites and nature of its production and consumption—as at the Royal Geographical Society. His is a study of the ways in which the British imperial mind, both popular and academic, processed explorers’ information. Tough’s work is embedded in the materiality of a declining fur trade in the northern Manitoba bush. It deals with forts and trade routes; with economies and survival strategies as a twohundred-year-old system of commercial capital vacated the region; and with native livelihoods found in a precarious balance between what remained of a hunting, fishing, and gathering economy and intermittent employment in uncertain industrial resource economies. Each is an authentic study, yet they have little to say to each other, and this is basically, I think, because one is written from London, the heart of an empire, and the other from the Canadian Shield, one of its many colonial margins. At least, as Derek Gregory has put it, ‘‘what seemed plausible in the lecture hall of the Royal Geographical Society in London . . . might well become a half truth on the ground’’ (1998, 21). The distinction, perhaps, is between studies of imperialism and of colonialism: imperialism ideologically driven from the center and susceptible to conceptual analysis, colonialism a set of activities on the periphery that are revealed as practice (Young 2001, 16–17). Only a few geographers have tried to bring both the imperial mind and the particularities of local colonial circumstances into focus (e.g., Clayton 2000 and Lester 2001).

But if the aim is to understand colonialism rather than the workings of the imperial mind, then it would seem essential to investigate the sites where colonialism was actually practiced. Its effects were displayed there. The strategies and tactics on which it relied were actualized there. There, in the detail of colonial dispossessions and repossessions, the relative weight of different agents of colonial power may begin to be assessed. If colonialism is the object of investigation, then Tough’s sparse Canadian Shield is promising terrain. It was not detached from London, of course, and may have been profoundly influenced by elements of imperial thought and culture, but the extent of this influence cannot be ascertained in London. Rather, I think, one needs to study the colonial site itself, assess the displacements that took place there, and seek to account for them. To do so is to position studies of colonialism in the actuality and materiality of colonial experience. As that experience comes into focus, its principal causes are to be assessed, among which may well be something like the culture of imperialism. To proceed the other way around is to impose a form of intellectual imperialism on the study of colonialism, a tendency to which the postcolonial literature inclines.

The experienced materiality of colonialism is grounded, as many have noted, in dispossessions and repossessions of land. Even Edward Said (for all his emphasis on literary texts) described the essence of colonialism this way: ‘‘Underlying social space are territories, land, geographical domains, the actual geographical underpinnings of the imperial, and also the cultural contest. To think about distant places, to colonize them, to populate or depopulate them: all of this occurs on, about, or because of land. The actual geographical possession of land is what empire in the final analysis is all about’’ (1994, 78). Frantz Fanon held that colonialism created a world ‘‘divided into compartments,’’ a ‘‘narrow world strewn with prohibitions,’’ a ‘‘world without spaciousness.’’ He maintained that a close examination of ‘‘this system of compartments’’ would ‘‘reveal the lines of force it implies.’’ Moreover, ‘‘this approach to the colonial world, its ordering and its geographical layout will allow us to mark out the lines on which a decolonized society will be reorganized’’ (1963, 37–40).

Along the edge of empire that was early-modern British Columbia, colonialism’s‘‘geographical layout’’ was primarily expressed in a reserve (reservation) system that allocated a small portion of the land to native people and opened the rest for development. Native people were in the way, their land was coveted, and settlers took it. The line between the reserves and the rest—between the land set aside for the people who had lived there from time immemorial and land made available in various tenures to immigrants— became the primary line on the map of British Columbia. Eventually, there were approximately 1,500 small reserves, slightly more than a third of 1 percent of the land of the province. Native people had been placed in compartments by an aggressive settler society that, like others of its kind, was far more interested in native land than in the surplus value of native labor (Wolfe 1999, 1–3). Figures 1 and 2 illustrate the scale of dispossession.

At these sites of colonial dispossession, it seems particularly fruitful to ask by what means it came about. The common emphasis in the colonial discourse literature is reversed. By starting not with texts, language, and strategies of representation, but with the dispossession of colonized peoples of their land— with, as it were, Figures 1 and 2—the relative weight of different colonial powers is not prejudged, and the question becomes simply: how was colonial power deployed to achieve this geographical effect? Rather than writing from the imperial center, rather than investigating colonial subtexts within a particular category of texts, the analysis turns on the primary effect of a particular settler colonialism and on the gamut of colonial powers that facilitated it. So situated, the distinctive roles of different components of the colonial arsenal should begin to come into focus (including maps like Figures 1 and 2). The cultural discourse of colonialism should begin to be contextualized, and some basis should be established for the evaluation of salience. Moreover, different theoretical points of attachment should come into focus, and it should be possible to sketch the work that particular bodies of theory accomplish.

This article is a rather schematic attempt to undertake such an analysis and, on that basis, to offer some preliminary conclusions. In a recent book on the reserve system in British Columbia (Harris 2002), I provide more texture for those who wish it. Yet the very starkness of an article that surveys an array of colonial powers may serve to emphasize my argument and encourage the discussion of the relationships among different forms of colonial power— and of different ways of theorizing them—out of which, I think, a more balanced geographical contribution to the study of colonialism is likely to emerge. I deal with British Columbia while assuming that my arguments bear, to some fair extent, on other theaters of settler colonialism.

The Power to Dispassess

The problem of reserves in British Columbia arose with the establishment of colonies and settlers some 70 years after people of European background began to frequent its coastal waters. After commercial capital reached the coast in the 1780s and 1790s, and the interior in the first decade of the 19th century, trade became the basis of the relationship between natives and nonnatives. The relationship was frequently mediated by violence, sexual liaisons of various sorts, and cross-cultural borrowing, but land was not at issue. Except for the few acres within their palisaded forts and, in some cases, a little land beyond for a farm or two, traders did not need it. For their purposes, it was sufficient to insert a handful of outsiders in ships or forts into native space.

But a territory had become known to the outside world, and its outline had been mapped. In French sociologist Bruno Latour’s terms, such ‘‘inscriptions’’ were transported to distant ‘‘centers of calculation’’ (1987, ch. 6). Sketchy information about a distant corner of North America was processed, thousands of miles from its source, within complex calculuses of diplomatic ambition, ideology, cultural stereotypes, and raw geopolitical power (Clayton 2000). Spain relinquished any claim to sovereignty along the north Pacific coast in 1795. Britain and the United States contended much longer, an intricate diplomacy at times verging onwar thatwas settled only in 1846 when the border between British North America and the United States was extended along the 49th parallel to the Pacific. This agreement, the Oregon Treaty, was a legal understanding between distant governments ‘‘respecting the sovereignty and government of the territory on the northwest coast of America.’’ It did not mention native people. In the eyes of the governments involved, the issue of sovereignty was settled. Three years later, in response to the American settlement of Oregon and the news of gold in California, the British government established the proprietary colony of Vancouver Island. Then, in 1858, following a rush of underemployed miners from California to the Fraser River, it established the crown colony of British Columbia. As Daniel Clayton puts it, ‘‘native space was reproduced as an absolute space of British sovereignty,’’ (2000, 236) although initially, in the aftermath of the Treaty of Waitangi and judicial rulings in New Zealand, officials in the Colonial Office were uncertain about the extent to which British sovereignty in these colonies was burdened by native title (Harris 2002, 15–16).

With the creation of these two colonies, land was framed in a new problematic. Colonies entailed settlers, and settlers required land, which could be got only by dispossessing native people. A relationship based on trade was replaced by one based on land. As their land was taken away, native people had to be put somewhere. A solution with many precedents in other settler colonies was to put them on reserves. Dispossession began in the 1850s and continued through the rest of the century. Physical violence, the imperial state, colonial culture, and self-interest all underlay it.

Violence. The establishment of colonies on Vancouver Island and the mainland changed the nature of violence there. It had long accompanied the fur trades. Coastal trading ships bristled with arms, greed was rampant on both sides, cross-cultural misunderstandings were frequent, and killing was the common result (Clayton 2000, ch. 6; Gibson 1992, 163, 170). In the interior, an axiom of the land-based fur trade was that perceived assaults on the personnel or property of the traders would be met with quick, spectacular displays of violence—sovereign power in the Foucaultian sense, though without a validating regime of rights (Harris 1997, ch. 2). Nor was the gold rush peaceable. Miners arrived with the latest weaponry (including six-shooters and spiral-bored rifles) and tactics of Indian fighting worked out in the American southwest. At the first sign of trouble, they organized themselves into companies, elected officers, and advanced in paramilitary formation. But with the creation of settler colonies, a new level of organization and calculation—the British military—was built into the equation of violence (Gough 1984). British warships operated along the coast; a detachment of Royal Engineers was sent out to survey land and maintain order. Such power was more often displayed than used—a few quick and very public hangings of suspected murderers after summary trials on the quarterdeck of one of Her Majesty’s warships, or a few villages shelled and destroyed—spectacles intended to instill fear. Officials considered such power ‘‘a grand persuasive.’’ Some held that it saved lives by preventing settler–native wars. Frequently, they judged it sufficient to anchor a warship just off a native village and ostentatiously prepare the guns.

In the interior, the space beyond the reach of a ship’s guns, the military equation was more balanced. In the 1870s, as settlers were moving in and preempting land, many natives leaders talked of war. Settlers feared, perhaps with justification, that a native uprising could wipe all of them out in a single night. But, as the chiefs knew, a shortterm victory was one thing; keeping at bay settlers and the armies that, sooner or later, would back them up was quite another. The results of wars across the border in which native warriors (some from British Columbia) had fought federal U.S. troops, was evidence in hand. Those who counseled war did so out of desperation. One chief put it this way: ‘‘A war with the white man will end in our destruction, but death in war is not so bad as death by starvation’’ (cited in Harris 2002, 206). Overall, the balance of physical power lay overwhelmingly with the state.

The imperial state. From the vantage point of London, Vancouver Island and British Columbia were two remote and relatively inconsequential colonies. Imperial attention focused, rather, on India and Ireland. After the advent of free trade in 1846, the role of settler colonies in the imperial scheme of things had become increasingly murky. Earl Grey, secretary of state for the colonies when the colony of Vancouver Island was created, held that colonies returned important image value for a great power and also that the honor of the crown required it to protect British settlers overseas (who had chosen to settle within the British empire) and also to protect native people from settlers who, left to their own devices, would probably exterminate them (Grey 1853, vol. 1, letter 1). Yet the coffers of the Lords of the Treasury opened reluctantly for honor, and British settler colonies around the world were expected to support themselves. Moreover, the duty of the crown to protect native people from settlers conflicted with the Colonial Office’s growing willingness to accord responsible government. As liberal humanitarian sentiments about the essential oneness of human kind and the opportunity to create a world of civilized, Christian people faded, responsible government came to dominate protection in Colonial Office thought (Metcalf 1996; Porter 1999). In settler colonies, where access to land was the predominant issue, only a hollow form of responsible government would exclude land policy from colonial jurisdiction. In effect, by the late 1840s and 1850s, the Colonial Office had no clear, consistent native policy. As a result, when the colony of Vancouver Island was created, it was readily inclined to turn over the management of native people to the Hudson’s Bay Company (which, it thought, had handled them much better than the Americans) and to rely on the judgment of the fur trader-cum-governor (George Douglas), who managed both colonies until his retirement in 1864. Thereafter, land policies were formulated by local settler politicians. The Colonial Office hardly interfered, and in 1871 when BritishColumbia became a Canadian province, land policy, now constitutionally a provincial responsibility within the Canadian confederation, remained in the hands of these same politicians. The state created a framework for the ordered development of a settler society, but did not, itself, provide the momentum for the development of that society or for the dispossessions and repossessions of land that accompanied it. When power passed to local politicians, they reflected the values and interests of their constituents.

Culture. The assumptions about the colonized other analyzed in the colonial discourse literature were pervasive in early modern British Columbia. Hardly a white person questioned the distinction between civilization and savagery or the association of the former with Europeans and the latter with native people. Nor did they question the proposition that civilized people knew how to use land properly and that savages did not. From these assumptions it followed that until Europeans arrived, most of the land was waste, or, where native people were obviously using it, that their uses were inadequate. Nor was there room for alternative understandings of civilized modernity. Rather, thought about native people focused on a simple binary: civilization and savagery with little of consequence between. From this it followed that if native people did not become civilized, and if, in a changing world, it was no longer possible for them to be savage, then they would die out, a common prediction in British Columbia well into the 20th century.

These social constructions were assumed, not debated. They pervaded thought about native people in the Colonial Office, in political, administrative, legal, and missionary circles in British Columbia, and in the settler mind. An Indian reserve commissioner, charged with laying out reserves, said this to a native audience on Vancouver Island in 1876:

Many years ago you were in darkness killing each other and making slaves was your trade. The Land was of no value to you. The trees were of no value to you. The Coal was of no value to you. The white man came he improved the land you can follow his example—he cuts the trees and pays you to help him. He takes the coal out of the ground and he pays you to help him—you are improving fast. The Government protects you, you are rich—You live in peace and have everything you want. —(cited in Harris 2002, 108)

At the time, few if any white settlers would have disagreed. There were arguments about how quickly native people could be assimilated and, therefore, about how much land should be allocated to them. Some settlers, biological racists to the core, considered natives utterly lazy, degenerate, and unredeemable; but a few found much to appreciate or pity in native lives, were well disposed toward native people nearby, and now and then supported their pleas for more reserve land. But even kindness— tinged by an educated, romantic appreciation of nature and, therefore, of lives assumed to live close to nature— was situated within the assumptions of the civilization/ savage binary. So was salvage anthropology, which in the influential presence of Franz Boas reached the coast late in the 19th century, there intent upon recovering the uncontaminated primitive condition. Boas had little interest in the native societies around him(which, he thought, were becoming civilized), except insofar as they supplied informants about earlier, precontact times.

These values had not been invented in British Columbia. As a considerable literature has shown (e.g., Seed 1995; Hulme and Jordanova 1990; Buckle 1991; Arneil 1996), some of them were as old as the European connection with the New World and had surfaced in the first European theorizing about their rights there by the Spanish theologian Francisco de Vitoria in the 1530s, or by the Dutch legal theorist Hugo Grotius a century later. They were powerfully and influentially elaborated by John Locke ([1690] 1947, ch. 5) in his labor theory of property. Locke held that God’s gift of land to Adam and his posterity acquired value only as labor was expended on it, and that labor justified individual property rights. Those who did not labor on the land wandered over what Locke called unassisted nature, land that yielded little and lay in common. This, he thought, was the condition of America before European settlers arrived. The land was ‘‘a wild common of Nature,’’ the original condition of the world before labor was expended on land and benefits accrued therefrom. Hence his famous dictum: ‘‘In the beginning, all the world was America.’’ In all the early settler colonies, ordinary (frequently illiterate) settlers—people who had never heard of Vitoria, Grotius, or Locke—held unsophisticated versions of these views.

By the mid-19th century, these old and pervasive ideas were powerfully reinforced by an increasingly strident racism and the achievements of industrial production. These years were the high water mark of ‘‘scientific’’ racism. The ideas of phrenologists, craniometricians, and polygenesists were in the air, and after Darwin’s The Origin of Species (published in 1859), it could be argued that, even if humans shared a common origin, there had been ample time for evolution to take different courses and produce different peoples. The very achievements of industrial society were the measure, it seemed, of an evolutionary advantage. The lurid tales of the massacres of English women and children at Morant Bay in Jamaica, or, later, at Lucknow and Cawnpore during the Indian Mutiny, confirmed in many minds the absurdity of treating natives as the equal of whites. Such judgments reached British Columbia. Even more important, I think, as the historian Michael Adas has pointed out, was the growing technological gulf between Europe and the rest of the world and the tangible measure it provided of the disjunction between civilization and savagery (Adas 1989). European weaponry and military discipline had made conquest relatively easy (Headrick 1981). Contrasts between Europeans and others seemed obvious: machine power versus animal or human power, progress versus stagnation, science versus superstition. The whole material paraphernalia of European modernity was a tangible yardstick of superiority, and the idea of progress, conceived in these material terms, was in the air as never before. Moreover, as the historian Mark Francis has shown, if civilization and progress came to be equated with technology and material wealth, then a measurable standard had been invented that native people could not attain (Francis 1998). They could be mannered, but they could not match European technologies or material wealth. Nor did they have the Europeans’ growing ability to dominate nature, another measure of progress. People who marked the land lightly and lived within the rhythms of nature were obviously unprogressive and backward. If civilization were measured in these terms, then native societies must be savage. For British Columbians of European background, the conclusion was obvious, and the rhetoric surrounding civilization, savagery, and unused land awaiting development was pervasive and uncontested.

### AT: Tech=Violent

#### Tech collectives have radical potential.

Toupin 21 (sophie, doctoral student in the Department of Art History and Communication Studies at McGill University, “More widespread than we think”) //ansel

During the anti-globalization movement of the early 2000s, tech collectives such as [Riseup](https://riseup.net/) and [Autistici](https://www.autistici.org/) came into existence to provide autonomous, non-corporate communication tools and “How-Tos” for social movements to organize safely and securely with emerging new media. In South Africa, the [Right2Know](https://www.r2k.org.za/) campaign was initiated in 2010 in response to the Protection of State Information Bill, which aimed at weakening the rights of journalists and whistleblowers to access information. As part of their work, R2K has published [guides for activists](https://www.r2k.org.za/2020/09/01/digitalsecurity/) to protect themselves digitally.

To heighten my own digital defense practice, I recently took a virtual workshop offered by the New York-based [Tech Learning Collective](https://techlearningcollective.com/). This collective provides technology education for radical organizers and revolutionary communities with special attention to underserved groups. These groups, which design tools and training for activists, are not a new occurrence. They have an interesting history across varying political cultures dating back, at the very least, to the national liberation struggles of the 20th century. Let’s take two of these, both armed struggles.

The first was the work of the section technique (technical branch) within the Front de Libération Nationale, the movement at the head of the Algerian struggle against French colonialism. In his essay, “Ici la voix d’Algérie” (“[This Is the Voice of Algeria](http://www.campusincamps.ps/wp-content/uploads/2015/10/fanon-this-is-the-voice-of-algeria.pdf)”), Frantz Fanon describes the section technique’s secret, mobile shortwave radio, whose transmitter was mounted on a moving truck that broadcast revolutionary messages from inside Algeria. The broadcast included information on the fighting, the history of the Algerian people, political and military commentaries, patriotic songs, and religious sermons encouraging commitment to the country’s freedom and independence. To listen to the revolutionary broadcast, most Algerians had to get their hands on radio sets designed by Algerian radio technicians, who had started opening shops for the sale of secondhand radio sets. The technicians had innovated in producing battery-powered radio in a country that, for the most part, lacked electrification. **Fanon suggests that the purchase of these radio sets did not mean “the adoption of a modern technique for getting news, but the obtaining of access to the only means of entering into communication with the Revolution, of living with it**.” In other words, Algerians were not simply listening to the broadcast or adopting an information technology for narrow instrumental purposes; rather, something changed in their disposition as a result of their participation in the broadcasts as listeners.

When French authorities understood the power of the Voice of Algeria as a force coming from outside the disciplinary mechanism of the colonial state, they passed a series of laws to prohibit the sale of radio sets to Algerians in order to restrict their access to the broadcasts. Further, as French forces were unable to take hold of the transmitter—they tried to bomb the truck that carried it, with no success—the only way to silence this revolutionary voice was to try to jam the airwaves. But even with French jamming attempts, the existence of the revolutionary broadcast was sometimes more important symbolically than being able to grasp its every word and sentence. Every evening, “Algerians would imagine not only words, but concrete battles,” Fanon says, thereby strengthening the national consciousness. The Voice of Algeria became a tool for the revolution not only through its technical branch—that is, its broadcast content—but also performatively, as the mere technical possibility of the broadcasts, against all odds and attempts to suppress, confirmed that the revolution was alive.

The second example comes from the technical committee that supported the South African national liberation struggle. From the late 1950s until the early 1990s, a technical committee developed technical artifacts and trained freedom fighters and their foreign comrades on how to use these tools to support the struggle. The technical committee’s approach to science and technology was influenced by major Cold War events such as the launch of Sputnik 1 in 1957. It was not only state actors, such as the American government, that were influenced by Sputnik 1, sparking an ambitious scientific and technological research program that would lead to the creation of the Internet. The launch would also influence the scientific and technological orientation of a national liberation movement.

After it was forced into exile, the technical committee and its members continued to operate in the United Kingdom. They designed tools for the people such as “leaflet bombs,” harmless leaflet launchers which would explode in crowded areas and facilitate the mass distribution of handouts. The first scene from the 2020 film, [Escape from Pretoria,](https://youtu.be/g6sJ3FOhs8U) is a good representation of how leaflet bombs worked and how white South Africans and foreigners especially could use their white privilege for the struggle as they easily navigated white areas. The committee also created small boxes containing audio amplifiers connected to tape recorders which would be left in crowded areas, often in townships, by freedom fighters. Thanks to a timing device, these boxes would then play a short, five-minute message once the operative was away.

Probably the most sophisticated project of the technical committee was an [encrypted communication system](https://hackcur.io/operation-vula/) that allowed freedom fighters to communicate secretly and transnationally between South Africa, Zambia, the United Kingdom, the Netherlands, and Canada in the late 1980s. Over almost a decade, the technical committee experimented with newly available technologies of the time such as telematics (combining computers and telephones), computer programming, and encryption, while at the same time training freedom fighters and their comrades to operate such systems. These communication systems later came to be included in Operation Vula in the mid-1980s, an operation that aimed to launch a people’s war.

These two examples show how contemporary tech collectives are rooted in a wider history of technical skills, tools, and groups supporting past and current struggles. In fact, the practical investment of national liberation struggles with science, technology, and communication are practices that might be more widespread than we think. Only by digging further into these radical science and technology traditions across varying political cultures will we have access to a different set of materials and ideas to think about what revolutionary science, technology, and communications can do.