# 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.