3

NETWORK EXPOSED

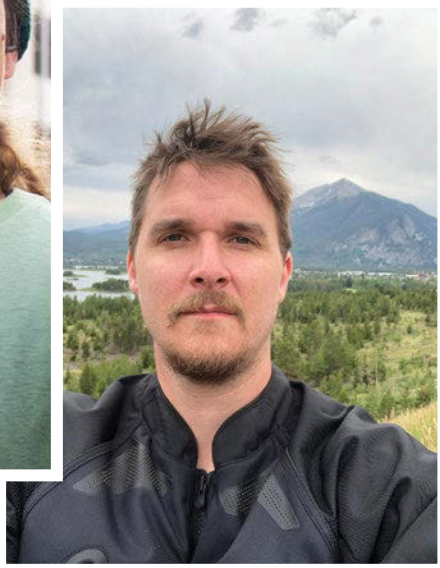
TRACKING SYSTEMS OF CONTROL

LISA LING &
CIAN WESTMORELAND
LAURI LOVE · JOANA MOLL
DENIS "JAROMIL" ROIO

GLOBAL MILITARY dominance, tactics of control, data tracking and surveillance practices call for a public debate on ethics and awareness around these interconnected systems. Former military service members Lisa Ling and Cian Westmoreland introduce and explain what they call the "Kill Cloud" behind the US military drone programme as a pervasive technological weapon system pursued to achieve dominance across space, cyberspace, and the electromagnetic spectrum. Their piece highlights what is happening behind the visible drone platform and aims to provide a better understanding on the real consequences of network centric aerial warfare. The subject of pervasive invisible surveillance infrastructures informs the reflections of security engineer and activist Lauri Love, who discusses the notion of "Sousveillance'', to denote vigilance

upwards from below. He provides an analysis on the current ethical issues concerning technological and intimate surveillance, reflecting on the urge of self-empowering ourselves from centralised power and authority.

Artist and investigative researcher Joana Moll describes the making of her three projects "The Hidden Life of an Amazon User", "The Dating Brokers" and "Algorithms Allowed". She exposes severe malpractice in the hands of corporate and governmental stakeholders and highlights the role of creative practice in uncovering and denouncing such actions. Finally, Denis "Jaromil" Roio, digital innovation expert, software artisan and ethical hacker, discusses the meaning of hacker ethics in 2021, stressing the importance of social movements to provide agency through collectivising big data controlled by financial and institutional powers.



LISA LING

Lisa Ling began her military career in the early 1990s as a medic and nurse. She became recognised for her information systems skills, and was encouraged to enter the combat communications field, where she participated in the operations, maintenance, and security of networked communications technology. The Intelligence Surveillance Reconnaissance (ISR) enterprise required more people to build and operate it, so her Combat Communications Squadron was assimilated into the Drone Program and moved to Beale Air Force Base. During her Military Career she was deployed to various locations, including the DCGS headquarters at Joint Base Langley-Eustis in Virginia, an Air National Guard site in Kansas, as well as several overseas deployments. Lisa served her last active-duty assignment with the site at Beale Air Force Base in California. After her military service, she travelled to Afghanistan to see firsthand the effects of what she participated in. She has a BS in History from UC Berkeley where she hopes to further her education.

Photo by Siri Margerin

CIAN WESTMORELAND

Cian Westmoreland served as a technician specialised in radio and satellite communications in the United States Air Force from 2006 till 2010. He was deployed in 2009 to Kandahar Airfield in Afghanistan to intercept command and control data over a 240,000 mile radius in Afghanistan and relay it through a high bandwidth satellite datalink containing voice communications, targeting data, imagery, and geographical data for both manned and unmanned aircraft tasked by the Combined Air Operations Centre at Al Udeid Air Base in Qatar and processed by the DCGS weapon system. His performance report stated that he assisted in "200+ enemy kills" and his unit received a Meritorious Unit Award. In 2010 he separated from Spangdahlem Air Base, Germany and spent a year hitchhiking across Eastern Europe, Central Asia, South East Asia and China. Several encounters with the spectre of organised violence drove him to seek understanding of his participation in war by receiving a bachelor's degree in international Affairs from Vesalius College in Brussels, Belgium.

Photo courtesy of the author

LISA LING & CIAN WESTMORELAND

THE KILL CLOUD
REAL WORLD IMPLICATIONS OF NETWORK CENTRIC WARFARE

AS FORMER MILITARY service members, we have a lifelong responsibility to submit for prepublication review any information intended for public disclosure that is, or may be, based on protected information gained while associated with the Department of Defense (DoD). We think this requirement is problematic as a constitutional matter and acts as a prior restraint on protected First Amendment speech. Nevertheless, this essay contains no such protected information. Instead, we use official government discourse to expose and interrogate what is not classified and currently exists in the public domain. Accordingly, and after consultation with our attorney, we did not seek pre-publication review.[1]

This chapter is about the United States' Global War on Terror, its ideological underpinnings, its ambitions, consequences, and more specifically, the technological approach pursued to achieve global military dominance across every spectrum of warfare, including space, cyberspace, and the electromagnetic spectrum itself. To fully appreciate this paper, it is important to be open to a civilizational critique of the United States and to recognize it on its own historical merit without relying on the mythical narrative of "American Exceptionalism." In the context of a rapidly warming world, issues of colonialism, water scarcity, forced migration, and war are all interconnected under the aspirations of technological progress.

We seek to introduce and explain what we have come to call the "Kill Cloud" behind the US military drone program. The modern militaries of the Global West wage war through remote surveillance and kinetic strikes with interconnected platforms, some of which ingest enormous quantities of data.[2] The use of this massive technological weapon system under the auspices of the "Global War on Terror" is invisible to the Western public. This chapter intends to illuminate greater aspects of modern drone warfare for the public eye to stimulate participation in the conversation around the ethics and scope of this developing weapon system. We have arrived at a time when enough information has been declassified for the public to engage in a robust dialogue about what is happening behind the visible drone platform.[3] Along with thousands of other soldiers and airmen, we were part of this interconnected system we are calling the Kill Cloud. We call it that because

there is no other word that fully describes the size and scope of this still evolving weapon system. Our professional military experiences were vastly different in many ways, yet both of us contributed to what we now see as terror. We share an abhorrence for the human toll shamelessly quantified in writing on our performance evaluations and awards.

After our service was over, we felt it was important to travel as civilians to reconnect with our humanity. Working with technology tends to disconnect those working with it, so we traveled as civilians to conflict zones to see for ourselves the human consequences of our actions. Through our process of disillusionment, a commitment arose to continue to question and reflect on this modern form of distributed networked warfare for the rest of our lives, along with a heartfelt desire to work toward positive social and cultural change. We have each turned to intellectual reflection as students in academia after our military service to critically analyze the power dynamics that have influenced this type of war. Lisa turned to history, and Cian to international relations. This collaborative chapter draws on our different experiences and is informed by research across interdisciplinary perspectives. We want to acknowledge the terror, the pain, and heartache that use of this technology has caused people living in the communities persistently surveilled, targeted, and blown to bits by connected peripheral devices (such as drones). It is our most sincere hope that once this writing is in the hands of the public that you, too, will understand the enormity, complexity, and barbarity of this vast distributed enterprise despite the promise of greater situational awareness, or the ability to see through the fog of war by adding Geospatial tools, Artificial Intelligence (AI), or other robotic platforms.[4]

There is an urgent need to widen the public's understanding of drone warfare. We must move from viewing the unmanned platform as a separate weapon, to including the entirety of the evolving systems behind it because of the insidious threats they pose to all of us. A drone can carry and launch lethal weapons and loiter at relatively low altitudes, terrorizing those living under them, so the tendency to focus on the drone platform itself is valid. However, such narrow framing obscures the distributed systems, bureaucratic institutions, and cultural biases behind the intensive intelligence, surveillance, and reconnaissance (ISR) production that directs these platforms toward their targets. There is no single term that could describe what this massive evolving weapon system is in a way that can be universally understood; the concept is unprecedented. Modern drone warfare is vastly more complex, insidious, ubiquitous, inaccurate, than the public is aware, and its colonial scope continues to bring endless war to communities of color across the globe.

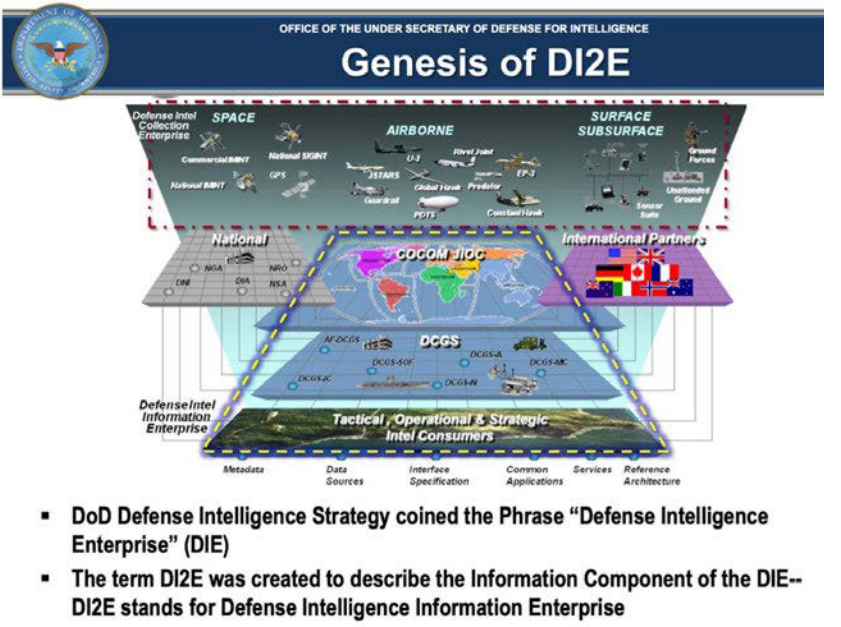


Diagram of the information component for the evolving weapon system we are calling the Kill Cloud. Image courtesy of Michael G. Vickers.[5]

The Drone Myth

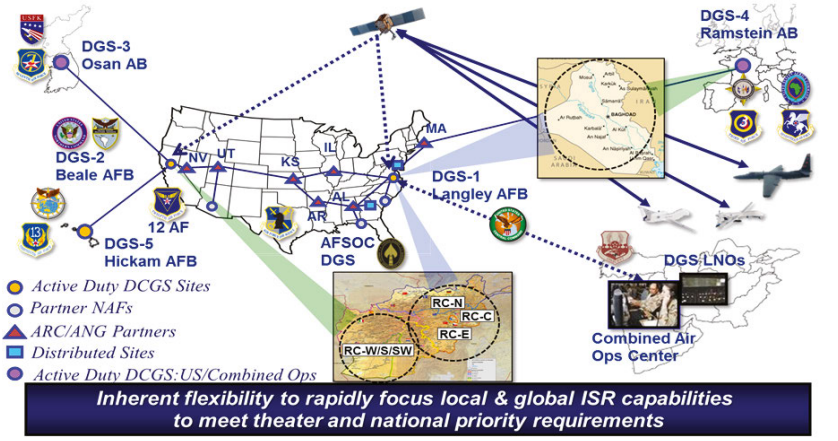
Retired Lieutenant General David Deptula, who was the primary planner of the air campaign in the First Gulf War and the former first Deputy Chief of Staff for ISR, was heavily involved in shaping and managing the US military use of drones; he uses the business-like description of an "Enterprise" to reference the networked socio-technical assemblage that functions silently and in secret behind the drone. This enterprise, this Kill Cloud as we call it, connects sensor and weapons platforms (drones) to a globally distributed network of devices, software, and a multitude of other nodes via satellites, cables, radio, and digital communication links that are accessed, operated, and maintained daily across all military branches, support agencies, and coalition partners, by thousands of people spanning the world (see Figure 1). This is what we refer to when we talk about network centric warfare (NCW), a means of navigating armed conflict that relies on distributed networks to kill with impunity.[6]

The public understanding of the intricacies of drone warfare remains extremely superficial and has been heavily influenced by the symbol of the drone itself. The popularized focus on drones promoted and dramatized in films such as *Good Kill* (2014), *Eye in the Sky* (2015), *Drone* (2017) and, to a lesser extent, *Pine Gap* (2018) inhibits conversation about and diverts public attention from the broader entanglements of network-centric warfare. While each of these films have a narrower focus on different aspects of an immense system, the much deeper ethical questions regarding a distributed (semi) autonomous, hyper-staffed, weapon of global connectivity and reach are not comprehensively interrogated. America's obsession with military planes and pilots harkens back to such films as *Those Magnificent Men in Their Flying Machines* (1965) or *Top Gun* (1986), so it is not difficult to understand how focusing on the deeper structural problems of this immense system have been averted. It is the myth of the drone, its simplicity and promise to make war shorter and safer, that dominates the discourse of the greater public today. Wars will not be made shorter or safer by adding remote connectivity, AI, or full autonomy to new or existing weapons.

General Deptula describes the phenomena of the clean and simple design of a drone drawing the public's focus away from the vast complex networks responsible for its operation in this way: "Everyone focuses on this little piece of fiberglass flying around called an unmanned aerial vehicle, but it's just a host for sensors that provide data to this vast analytic enterprise we call the Distributed Common Ground System [DCGS], which turns the data into information and hopefully knowledge" (Deptula, as quoted in *Airforce Magazine*).[7]

The press has not been immune to the lure of the drone myth, either. We both are regularly interviewed by journalists who only too quickly display disappointment upon learning that we were neither drone pilots nor sensor operators. They are even more disappointed to learn that the pilots are the least informed of all about the globally interconnected systems and equipment necessary to keep the drones flying and their sensors sensing. The term "drone" itself, which we adopt in this essay due to its wide public acceptance, is a misnomer because of the significant amount of labor required to keep them in flight. The drone myth obfuscates the Kill Cloud with its sleek design and straightforward conception: the drone aims to be war, simplified.

Yet, it is everyone's duty to see beyond this symbol of modern warfare and question the convoluted and complex mechanisms behind its operation as well as the idea that the proliferation of these systems will make us all safer. Similarly, the word "cloud" in relation to what we know as the internet is a marketing term and bears no relation to reality. It is not ionized water vapor condensing around particulates through surface tension freely floating in the air, nor is it some magical place.[8] The cloud is a distributed network of servers, databases, devices, software, data storage and computing power. Interface with the cloud provides users the



Air Force Distributed Common Ground System (US Air Force 2015, 32).[56]

means to view the same information and collaborate from various locations. The services we use every day to plan a trip (Google Maps), order a ride (Uber), avoid traffic (Waze), watch movies while they buffer (Netflix, YouTube, and others), link up with "People you may know" (Facebook Friend Recommendations) or identify that song you keep hearing (Shazam) are all rendered to your device using data sent from the cloud—and, disturbingly, all have applications that "can" be assimilated into what military planners envision for Cloud Supported Network Centric Warfare (NCW).[9] Technology companies have already been tapped by military planners for their collaboration with this massive weapons system.[10]

Obstacles to Public Understanding

A key obstacle limiting public understanding of the Kill Cloud is the very nature of distributed systems themselves, as Maarten van Steen and Andrew S. Tanenbaum state in *A Brief Introduction to Distributed Systems* in 2016: "Distributed systems are by now commonplace yet remain an often-difficult area of research. This is partly explained by the many facets of such systems and the inherent difficulty to isolate these facets from each other."[11]

A Distributed Common Ground System is described on the United States Air Force (USAF) official website as the "primary intelligence, surveillance and reconnaissance (ISR) planning and direction, collection, processing and exploitation, analysis and dissemination (PCPAD) weapon system that consists of at least 27 regionally aligned and globally networked sites."[12] The letters in the acronym PCPAD refer to the process that can direct sensors to collect data in near-real-time. That data collection and interpretation necessitates a more symbiotic relationship be-

tween military technology, communications personnel, and the intelligence community. The often-repeated Air Force phrase "no comms, no bombs" accurately describes the partnership needed between these two formally semi-segregated military sectors. Both are integrated into the Distributed Common Ground System, making the Kill Cloud a murky affair. In other words, when the communications sector and the intelligence sector work together, it is rarely transparent, include weapons and sensors, and the public can be assured that critical research information will neither be forthcoming nor forthright.[13]

Further complicating substantial public discourse is the prolific use of military acronyms and nebulous descriptors such as DCGS (Distributed Common Ground System), EPIE (European Partnership Integration Enterprise), "Military Aged Male" or "Target".[14] These acronyms and descriptors control public access to information and often serve to impede researchers' access to knowledge over time. They are part of a massive infrastructure built to increase the speed at which complex ideas and concepts are communicated within limited human networks while simultaneously obfuscating them to the uninitiated. The use of acronyms also strips away any emotional context that will communicate the effects of what the letters represent in the real world. For example, phrases like "Military Age Male" (MAM), "imminent threat" or "target" have become normative representations of human beings, many of whom never were, nor intended to be combatants; they were innocents. Dr. Sara Shocker, through her research was able to rigorously work around obstacles to empirically demonstrate that data analysts use stereotypes about gender and religion to inform who is selected as a drone target.[15] In her book, *Military Aged Males in Counterinsurgency and Drone Warfare*, Shocker argues that the normative use of the category "Military Aged Male" has contributed to the deterioration of civilian protections.[16] We both agree with her argument and her conclusions.

Compounding the many obstacles that acronyms and nebulous descriptors pose to public access to information, there is a lack of clarity and oversight surrounding the multiple classification processes that hold "state secrets." Items of critical public interest have been consistently locked behind phrases like "need to know" or "national security" and kept from public disclosure even when unnecessarily classified. The government selectively decides what, when, where, why, and how information is exposed. Much has been said on the topic, but little has changed. There is no clear definition for over-classification even in the public law signed by President Barack Obama designed to reduce it.[17] Furthermore, in the executive summary of a Department of Justice (DOJ) audit from 2013, both Congress and the White House recognized that over-classification of information interferes with accurate and actionable information sharing, increases the cost of information security, and needlessly denies public access to information. The audit found that the DOJ is susceptible to what was called misclassification, and that the DOJ

was not effectively administering its own classification policies.[18] This is one of the very few publicly accessible investigations demonstrating misclassification and over-classification, which is not exclusive to the DOJ. Within the Kill Cloud there are multiple classification systems in place managed by multiple agencies, branches of service, mission partners, and others. Over-classification is common because the incentive to classify materials, even unnecessarily, far outweigh any reasons or risks not to. Despite these failures, public interest whistleblowing is still prosecuted vigorously under the 1917 Espionage Act and the accused are denied a fair trial because any evidence can be hidden from the public under the auspices of National Security. Furthermore, any defense that allows the defendant to state motive is disallowed and has been from the case of Daniel Ellsberg forward. This precedent was upheld in the recent case of Daniel Everette Hale whose documents prompted The Council on American-Islamic Relations ("CAIR" or "CAIR Foundation") to submit an amicus curiae brief to support Hale during sentencing. CAIR represented hundreds of Muslim Americans who were placed on the US Government's Selectee and No-Fly Lists.[19] It is important to cite a part of the request here:

> The 2013 Watchlisting Guidance, a US Government publication, spelled out the criteria and procedures through which US persons are placed on the federal government's many secret lists. This document is unclassified, but the US Government had never agreed to make it available so that persons caught up in the lists and their representatives could come to understand the process. Daniel Hale disclosed this document, […] The availability of this information enabled CAIR to present focused claims on behalf of its clients, whose lives had been disrupted by being placed on the lists.[20]

From 2002 through 2008, J. William Leonard served as the Director of the Information Security Oversight Office. Leonard worked for the Department of Defense from 1973 until 2002 where his responsibilities included ensuring that classified national security information in the possession of defense contractors was properly protected. Other responsibilities included counterintelligence, critical infrastructure protection, and offensive and defensive information operations programs. He is one of few individuals we would look to for clarity on what should and should not be considered classified or, more to the point, what pieces of hidden information is in the publics' best interest to know.

One of the more recent debates on this topic surrounds Reality Winner's leak releasing information regarding the security of the 2016 US election. Leonard stated quite clearly that the document released by Winner, an accoladed cryptographic linguist who translated incoming data from drone platform sensors, should not have been classified and was in the public's best interest in an opinion piece for

The Washington Post dated December 21, 2020, and in the documentary film directed by Sonia Kennebeck, *United States vs. Reality Winner.*[21] While Winner's leak was not about network centric warfare, this is a clear instance where the government's' power to strategically over-classify information resulted in the persecution and five-year sentencing of another whistleblower associated with the drone program.[22]

Common Operating Picture

Command, Control, Communications, Computing, Intelligence, Surveillance, and Reconnaissance (C4ISR) is another one of many military acronyms used to describe a conceptual framework for the United States current approach to warfare. Command and Control throughout military history consisted of a commander observing from the highest point he could to get an accurate overview of the battle space. The commander would then use that information to direct his troops and formulate a battle plan for them to carry out. Maps allowed Generals or commanders to sit in a tent and conceptually visualize the battlefield. Wars have been won and lost based on who had the most accurate vision of realities on the ground or, put simply, the most accurate maps. Maps are coveted assets that win wars and communicating plans through a common picture with other forces was essential to accurately execute battlefield maneuvers. Until data was able to be transmitted wirelessly or beyond line of sight (BLOS), command and control had not really changed since Napoleon tried to conquer Russia in the middle of the winter of 1812.

Today, a Common Operating Picture (COP) of the air war is rendered from location data that is overlayed onto a topographical map and displayed on screens so that Air Battle Managers (ABMs) and other decision-makers can view the air war in real time. The ABMs send current information to the Air Operations Center (AOC) to provide Command and Control of the air war. ABMs have knowledge about aircraft, weapons, and surveillance. They use this information to control each aircraft by telling pilots, and sometimes ground troops, where to go and what to do with their weapons when they get there. The core functions of an ABM include orienting shooters, pairing shooters, solving problems, and making decisions. Sitting with the Air Battle Manager is an enlisted position called the Command-and-Control Battle Management Operator (C2BMO) who determines things like who has the most fuel, who is closest, who can get there fastest and who can stay on station longest in order to support the tactical decisions of the Air Battle Manager.[23] They create the air tasking order and task the aircraft within that order.

The COP, or what is described as a common picture of the air war, includes the aircraft platforms, locations, and available weapons. Air Traffic Controllers

(ATCs) operate radio equipment to relay flight and landing instructions, weather reports and safety information to pilots. ATCs are also responsible for plotting aircraft positions on radar equipment, as well as computing aircraft speed, direction, and altitude.[24]

Expanding the Kill Cloud

The US Military will be rolling out the Advanced Air Battle Management System (AABMS) in 2021. Air Force Chief of Staff Gen. CQ Brown, Jr. explains the improvements this way: "Nearly two years of rigorous development and experimentation have shown beyond doubt the promise of ABMS… We've demonstrated that our ABMS efforts can collect vast amounts of data from air, land, sea, space and cyber domains, process that information and share it in a way that allows for faster and better decisions".[25]

What this means in laymen's terms is that increased data is going to be ingested into what we are calling the Kill Cloud, attempting to eliminate the fog of war. More data does not necessarily mean less confusion unless it is managed well. As we will explain later, the OODA Loop (Observe, Orient, Decide, Act) concept takes more data and strives for faster and faster reaction times. What could go wrong? Many would argue that the answer is even more data; the appetite for increasingly more data is insatiable.[26]

Advanced Air Battle Management is becoming a multi-domain data collection and distribution system that uses a mesh network of various platforms in which nodes automatically assign which asset to respond. The possible end state is supposed to resemble how someone might call for an Uber or a Lyft with a cloud-based system choosing which driver is closest to you in time and distance to pick you up. The truth is that not even the Air Force knows what the whole system will be composed of when it is finished.[27] The goal is for soldiers on the ground to be able to identify threats, much like accidents and traffic choke points can be spotted and avoided on Waze with user input. Soldiers on the ground will be able to send what they see and experience so their information can be distributed to any number of proximal collection points where the data will be analyzed and used by mission planners or others in the future.[28]

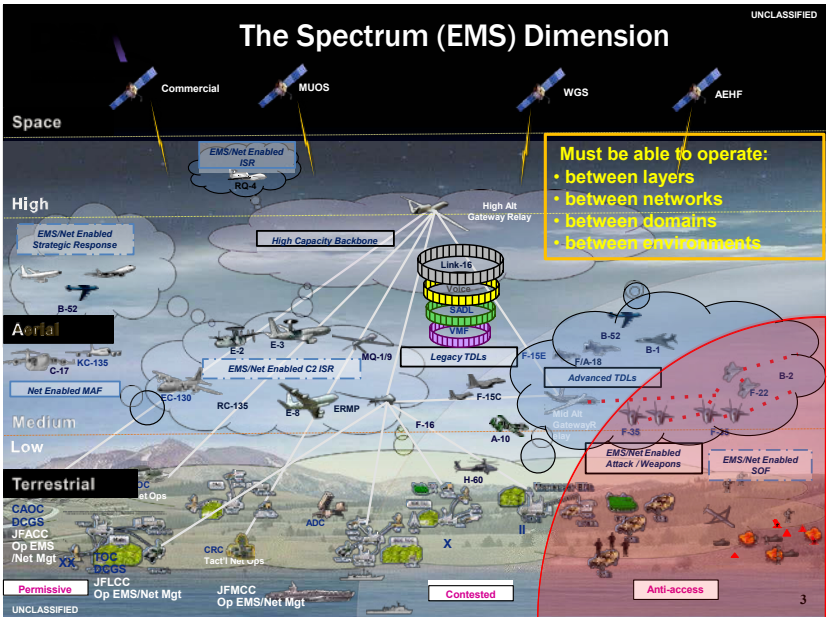
Until recently, battlefield communications between different entities were a complex, cumbersome, and time intensive task to plan and execute; often errors occurred that required more planning and execution from the field and on the fly. Today, it is possible for dissimilar networks to effectively communicate BLOS from great distances using what is known as a Battlefield Airborne Communications Node (BACN) pronounced "bacon" for short. This capability makes the aspirational goal of a Common Operating Picture plausible from a pure technology

perspective. The assemblage of Internet Protocol (IP) and software defined radios, a gateway manager, and Advanced Information Architecture (AIA) allows the exchange of data from disparate sources to be collated and transmitted or stored as necessary for mission planners and others to use. Because the link can be configured to be device agnostic, it is now possible to send text messages from a cell phone to a pilot flying overhead.[29]

These systems, originally flown by NASA (North American Space Agency) in high altitude airframes for testing, were soon in high military demand. BACN evolved "[…] from a joint operational need to an enduring capability."[30] Because this equipment can be deployed on mobile platforms, the use of this technology reduces the logistical and security footprint, as well as the requirements needed for static ground-based systems. In the future, these systems will be further facilitated by low earth orbit satellites deployed by civilian contractors. According to *Air Force Magazine*, "the military is waiting for the commercial industry to build its satellite communications constellations on orbit, such as SpaceX's Starlink array and an Airbus LEO constellation, so it can tap into the capability on a large scale."[31] Like much of the Kill Cloud, this piece will evolve to facilitate the ingestion of mass amounts of data using software and algorithms for AI and machine learning to compute and connect the massive amounts of source and sensor data, using an Edge Computing strategy, with the goal of speed and accuracy beyond what is currently available.[32]

After a significant testing exercise at Eglin Air Force Base, Florida on September 3, 2020, that included thousands of personnel, hundreds of contractors, expeditionary 5G towers, robot security dogs made by Ghost Robotics, and a plethora of connected legacy weapons, Chris Brose of Anduril Industries stated: "You're taking cognitive burden off of the operator when it comes to understanding the environment, ruling out false positives and finding objects that the user has said that they care about."[33] It is important to note that according to the Anduril Industries website, the company is run by what they call a team of experts from Oculus (owned by Facebook), Palantir, SpaceX, Tesla, and Google.[34] There are 28 separate companies each with billion-dollar government contracts working on ABMS. This is the system the Air Force describes as: "[…] the Air Force and Space Force's priority program to develop the military's first Internet of [deadly] Things and is the services' primary contribution to Joint All-Domain Command and Control, a Defense Department-led effort to securely connect all elements of the US military—every sensor and shooter—across land, air, sea, space and cyberspace."[35]

Notably, one of the Anduril experts implementing systems that are supposed to create greater situational awareness of the battlefield came from Facebook, a company with a well-known sordid history of difficulties rendering fact based unbiased data. Google, where another expert worked previously, has also manipulated users' reality with curated search results favoring those who pay good advertis-



Initial capabilities of the JALN or Joint Aerial Network that include Space, Aerial, and Terrestrial layers. A graphic simulation of Kill Cloud topology.[57]

ing money to be rendered first. The machinations used to translate battlefield data into actionable intelligence or "knowledge" used for life-or-death battlefield decisions is ripe for further interrogation. This is one area where ethicists, researchers, and legal scholars are better positioned to clear murky waters than technologists alone. As previously noted, the expansion of this technology continues to evolve within a troubling colonial context.

Colonial Underpinnings of the "American Peace"

The United States, despite its merits, is a nation that was born out of colonization and the destruction of indigenous societies. Indigenous people were labeled savages under the ideological frameworks of The Discovery Doctrine and Manifest Destiny. These cultural beliefs provided the "moral" impetus for settler expansion westward in North America and beyond. This expansion disregarded the territorial rights of indigenous peoples and was upheld as recently as 2005 in the case of *City of Sherrill v. Oneida Indian Nation of New York*, 544 US 197.[36] Leaders of the free world often deny the colonial frameworks they are party to in favor of memorializing the legacy of European descendants. Unlike other anti-colonial struggles in world history, popularized heroes of the American Revolution were

not indigenous peoples who often played crucial roles, but British colonizers and their direct descendants. We often criticize authoritarian nations that submit their people to involuntary servitude to achieve civilizational objectives, and yet most of our initial infrastructure was built by African slaves, Chinese immigrants, and indentured servants. It took a civil war to outlaw chattel slavery, and almost immediately thereafter, arbitrary laws were created that forced former slaves into prison labor where conditions were sometimes worse. It is not the last time that the legal system of the United States will be weaponized against a whole race of people inside or outside US territory; the Chinese Exclusion Act is another example, Japanese internment another, and the list continues into present day Islamophobia shrouding what is witnessed or ingested in a fog of historical prejudice and White supremacy.

We brand our country as a nation of laws, but this has hardly ever stopped laws from being selectively enforced. Racism is not always presented by those intending to do harm; it is built into cultural assumptions, exclusionary ideological frameworks, and ignorance. The United States military is viewed by many in the US as a forward-thinking multicultural institution. In basic training, a common trope uttered by instructors is that there is only green or blue, nothing more. This means that the cultures of those individuals who signed up are put aside in favor of an identity based exclusively on one's branch of military service, Blue for the Air Force, and Green for the Army. As of 2018, White people in the US military still numerically outnumber those of other ethnicities. Whether intended or not, military recruiters primarily target the poor and underserved with offers of college tuition, debt forgiveness, and healthcare.[37]

The military is inherently dehumanizing, with the purpose of enforcing political will through violence. Military members are broken down, reassimilated, and calculated as units of monetary value. The process of training humans willing to work together under a rigidly enforced hierarchy to kill an enemy does not require empathy or understanding for other cultures. Members are instructed to fall in line, which often means accepting the current "other" into their reconstructed world view. Military members are also drilled to view civilians as lesser human beings as a method of retaining trained personnel. Furthermore, meaningful discussion about racist assumptions affecting US foreign policy decisions to invade and terrorize with Shock and Awe tactics remain to be had. We cannot overstate the importance of grasping the futility of intelligence requirements used to characterize a "threat" within cultures that very few analysts, if any, have the cultural competency to fully comprehend. This lack of cultural familiarity has made the death toll of network centric warfare more of a reflection of Eurocentric bias than global safety. The racial implications of nations with a colonial legacy surveilling and bombing Indigenous communities across the Middle East, Southwest Asia, and Africa must be reckoned with.

Cell Phone that Belonged to the Former President of Afghanistan, Hamid Karzai, on display at the National Museum in Kabul. Photography by Lisa Ling.

As one can imagine, people living under a constant threat of connected weaponized surveillance capable devices change their behaviors to reduce their traceability; they do not engage in normal daily activities and are terrified of making new associations with people and communities. The smart phone—once a technological wonder that defines our modern existence—has become monopolized by war and converted into a surveillance tool. These devices are now integrated into a global weapons system that has the potential to mark individuals for death, and they know it. The behaviors of these populations change in response to the imminent possibility of being targeted with seemingly no rhyme or reason. Behavioral changes often become an intelligence identifier, creating suspicion in the eyes of those airmen and their colleagues, analyzing local populations' movements and actions. It creates a perpetual cycle of fear and distrust for the innocent civilians that these platforms are supposed to protect. Smart phone data can be compared and compiled with other data sources through the collaborative cloud we loosely identify as the Kill Cloud. That data gets packaged, tagged, and stored until someone somewhere decides it is useful again. Data can be retrieved from months or years in the past to support an imminent decision to pursue and strike a suspected "threat."[38] Despite the military's preference to talk about warfare as if it is a business and to use business-like terminology surrounding this globalized weapon system, it is not a business—it is brutal violence; it is terror.

While we do not specifically address non-military CIA drone operations of which we claim no first-hand experience nor direct knowledge, we argue that the distinction commonly made between targeted killings in areas outside or inside recognized armed conflict zones are problematic, and that distinction makes no

difference to those living under them. Remote warfare is justified by using "lawfare" to legitimize it. In other words, legal interpretations of international humanitarian law (IHL) allow the US government to execute any drone operation with impunity.[39]

Some Things Never Change

The ability to pick up a smartphone and video chat in real time with a friend on the other side of the globe is something that most people today take for granted. We grow impatient when a call lags and curse our service providers. Very few people acknowledge the effort that goes into making this possible; fewer understand the complex technology or machinations weaved into the multiplicity of technologically moderated human connections. Fewer still can tell you exactly what went wrong at what part of what process or how to fix it. To step back and fully appreciate the scale, complexity, and capacities available today, and how the vast weapons system discussed in this paper connects, a brief history may be helpful.

The Kill Cloud owes much of its existence to Benjamin Franklin's discovery of electricity, Michael Faraday's discovery of electrical current production, Alessandro Volta's discovery of how to store electricity, and Werner Von Siemens development of the dynamo electric generator. These discoveries effectively established the foundational requirements for electronic devices in use today. The invention of the electric telegraph was a means for militaries to communicate at the speed of a trained person's ability to punch an on/off switch on either end of a copper wire. Unknown to Michael Faraday at the time, his discovery into how to produce electric current also enabled the first loop antenna, which took signals from a copper wire to electromagnetic waves. From these discoveries, not only was communication speed increased, but the foundation of modern maneuver warfare was born in a hybrid of accidental intentionality. Major investments were made in laying underwater cables so that commerce could be more regulated and controlled. Combined with the steam engine, these innovations increased the speed at which wars were fought significantly. Technological advances gave way to colonial conquest, and the ability for armies to communicate instantly over thousands of miles, setting the stage for the colonial consequences still being felt today. Gayatri Spivak calls this *epistemic violence* —the harm that dominant groups like colonial powers wreak by privileging their ways of knowing over local and Indigenous ways. It is still true today, and the Kill Cloud has become the colonial way of knowing.

Much more recently, we moved from hardware to software switching making it possible to remotely access and control hardware while moving to faster data transmission. There are 7 types of electromagnetic wavelengths that are known

and exploited by the military and others for different purposes. Every second of every day, radio waves pervade every millimeter of this earth likely carrying more information than every civilization possessed in total for most of human history. The control of the electromagnetic spectrum is of great political, economic, and military consequence. The ability to use the spectrum for friendly forces while denying it to an adversary is to control the operational tempo in which battles are fought as the use and exploitation of the electromagnetic spectrum increases in every domain of conflict. As the name implies, Network Centric Warfare is centered on communications networks, and the ability to exploit connectivity and coordinate actions at an increasingly faster pace with exponentially more data. These are the building blocks of the Kill Cloud and, while they are vast and complex, it is not important to fully understand these technologies to grasp the implications we are presenting.

Bias of Data Collection

In the January 2013 issue of *Air Force Magazine*, Lieutenant General Larry James, the Airforce ISR Chief at the time, described the DCGS as follows: it processes more than 1.3 petabytes of data a month—equivalent to 1,000 hours (about 1 and a half months) a day of full-motion video. [40] In a September 2016 edition of *Air and Space Magazine*, Roger Mola describes the DGS-1 (now called DCGS-1) processing facility as a windowless warehouse that can hold about 1,500 people.[41] While he toured DGS-1, there were about 70 analysts working in teams of six and he described them as "enlisted personnel that looked to be between 18 and 25-years old."[42] He mentions "that within seconds, raw bits of data from Afghanistan are transmitted by satellite and fiber-optic cable to a network of 27 centers around the world for processing, analysis, and dissemination, to military units and a number of government agencies."[43] He also notes that "nearly 6,000 active and reserve air personnel, assisted by hundreds of civilian contractors, work with the data in the system."[44] All this system ingested data will not necessarily become actual knowledge or situational awareness. Much like spellcheck has dulled our ability to spell words from memory, or the use of smart phones has all but removed our ability to memorize a friend's phone number, access to modern technology does not necessarily improve knowledge just as politically charged social media posts have been known to alter our perception of reality. Our dependance on multiple streams of data will not necessarily work to decrease the fog of war.

It is good to mention that raw data does not necessarily mean without bias, just as witnessing events play out on a video screen on the other side of the globe does not necessarily offer reliable knowledge. In the film *National Bird* by Sonia Kennebeck, General Stanley McChrystal observes that, while discussing viewing

drone feeds from 10,000 feet, "you don't know what's going on, you know what you see in two dimensions." Watching two-dimensional video on a screen is also different from the situational awareness one gets by being there. It is important to understand that being on any operations floor for any remotely connected process is vastly different from being physically there. This should be obvious but, clearly, it still needs to be stated; awareness will *always* be limited by distance, sometimes in critical ways. Raw data, when used in a scientific sense, refers to information gathered for a research study before the information has been analyzed or transformed.

In the context of a research study, there are limits and ethical considerations that determine the validity of the study and, by extension, the validity of the data returned. Much of the ingested ISR data is without context. Data without contextual information is inaccurate missing a full picture at best, or bad information that contributes to the death of an innocent at worst. In ISR, "Knowledge Production" violates long standing research norms. These norms were utilized to prevent bias in scientific and scholarly research, and to certain extent, they have. Donna Haraway wrote, "The situation or context that data is collected in has an inalienable relationship to the nature of the knowledge it can generate."[45] This is true even in the fog of war, perhaps especially then.

As we have discussed, the appetite for more data and a faster operations tempo is insatiable; one reason is the Observe, Orient, Decide, Act (OODA) Loop, an acronym used to frame the maneuver warfare derived approach to conflict.[46] It was created by John C. Boyd, a Korean War Fighter Pilot, to describe the process that he used to survive aerial dogfighting. The military's primary objective is to defeat its "enemy" by incapacitating their ability to make decisions through shock and disruption. The ordinance dropped on Iraq on March 23, 2003, was an example of this strategy. Thus began the "Shock and Awe" campaign designed to disrupt the Iraqi Forces OODA Loop. Boyd believed that going through the OODA loop faster than your enemy would end with you living, and your opponent dying. Many military strategists are convinced that big data analytics synthesizing massive quantities of input used to uncover information about enemy operations will enable this strategy to scale from fighter pilot to battle. This enormous collection of data is intended to assist with combat operations to help define targets, but does it? Does using big data reveal patterns and "orient data in a way to be visible to someone who may not otherwise be able to recognize it due to their own personal biases or background"?[47] This sounds good in theory, but the emphasis on speed and simplicity can lead to rash judgements. When the OODA Loop is applied from a technology-mediated distance, things can fall apart quickly. Through secrecy, distance, and compartmentalization, no participant sees the full picture, and their perception is limited by their narrow scope. Equipment failures, the weather, and a multitude of other factors can interfere in practice. In addition, high operational

tempo, inaccurate data, absence of context or metadata, cultural bias, and racism can also mis-orient commanders, analysts, and those who pull the trigger providing circumstances ripe for error that can result in the death of innocent civilians.

On any given day, intelligence analysts at a base in the United States will support a drone operation over a conflict happening on the other side of the world and can launch a missile at a "target" deemed a "potential threat." At the end of a shift, the same analysts will re-enter the reality the rest of us see and experience, unable to say anything to their family or friends who remain completely unaware that remote wars are being fought remarkably close to their homes by people they see every day. For the family and friends of those working in a SCIF (Sensitive Compartmented Information Facility) prosecuting these wars, missing a favorite television show is bothersome, but to others, who depart from remote war zones into their communities daily, the trivialities of life just become even more trivial. People prosecuting these remote wars from home, understand how isolating it can be to have real time information, updated daily, that cannot be shared. Conversely, the weapon system also supports what is called dynamic re-tasking so that if a natural disaster were to hit a base, it is possible that the data could be transmitted and processed elsewhere and ordinance could still be fired by another crew with little notice and even less familiarity with what is happening on the ground.[48] What is still true is that people here in the United States will not know it happened, but those a world away living under drones will, and it may be the only part of the Western world they ever see.

Many of the people living under Western surveillance depend on the land they cultivate to survive and are acutely aware of the impact their actions have on future generations. They have survived for centuries within their cultural operating systems that have evolved over thousands of years and, while many have little use for the written word, their knowledge of life and the world around them is in many ways better than our own observations. Their natural unmediated situational awareness is something the Western world has lost over time; we do not believe technology will ever be able to fully reconstruct it.

These people are inextricably connected to the land they inhabit, yet euro-centric cultural misunderstandings dismiss them as backward or primitive. Instead of using a critical lens to observe, Western voyeurs operating a multitude of different sensors do not question the notions of backward or primitive, these ideas are accepted, ingested, categorized, and stored within the system. This information will be kept until someone in the chain of command decides it is needed for "accurate situational awareness" of current or future operations. This information may be utilized later within a frame of more erroneous assumptions taking the viewer further from what can be considered objective truth or awareness. The truth is that these are exactly the people and cultures the Global West desperately

needs to engage. We have a lot to learn from good stewards of the environment, especially as the natural world continues to warm around us.

Every year since 9/11, the West laments the devastation that occurred when the World Trade Center fell. It was a tragic event for those directly affected, and it was also tragic for every single innocent person whose life was destroyed by the Islamophobic Global War on Terror (GWOT). The devastation and destabilization brought about after the towers fell has ravaged the lives of millions of people, many now part of the human flow of refugees around the world.

Now that we can pass more data over longer distances, while flipping on/off selector switches in remotely accessible locations via software switched devices, it becomes a matter of ease to weaponize industrial advancements under the guise of protection. It is the ever-present and redundant pretext for more war. What is happening today is both accidental and intentional, and can be seen as an inevitable branch of the evolution of technology within the context of colonialism. The ways in which technologies are used follow a long history of colonial wars of aggression. Innovative technology will carry us to new frontiers faster, continuing the same destructive patterns if no substantive changes are made.

Despite repeated insistence to the contrary, these technological advantages have not prevented armed conflict and their continued evolution has not shortened or ended wars. Militaries arm drones by promising the public that they will only be used defensively to protect soldiers, but this promise disappears the moment higher-ups decide to label something or someone as a threat, which militaries the world over can do (and have done) in an instant. As soon as something or someone is labeled a threat, the drones will start buzzing and communities living below them will hear them day in and day out. Arming drones will not keep soldiers on the ground safer; it will lead to more situations that endanger them. These weapons inevitably change the perception of militaries in locations where drones are deployed. The resentment created by replacing actual soldiers on the ground with machines serves to radicalize populations, making engagement more dangerous for everyone while continuing to perpetuate endless wars. This resentment then becomes intergenerational as children grow up with an ever-present threat to their everyday reality, making any future attempt at de-escalating violence far less achievable. These are logical conclusions about the relationship of autonomous armed aerial platforms to people living below them. The more wars are automated, the less accountable militaries will be. Like the telegraph facilitated colonial exploits of the past, so too does the use of the Kill Cloud in countries whose resources continue to be plundered.

It is the tendency of Western academics to parse systems and explain processes as if they are somehow separate in purpose or function, but we believe it is critically important to understand the interdependent connected nature of these emerging technologies and how their use has perpetuated ceaseless conflict in far

flung places around the globe, as well as the military's devastating impact on our climate. In a joint Brown and Boston University study, the only one of its scope, researchers found that at least 37 million people were forcibly displaced from their homes. This number exceeds those displaced in every war since 1900 except WWII. The researchers state that this number is an extremely conservative estimate and believe the true number to be closer to 48 to 59 million people from every country the US has involved itself in under the auspices of the GWOT.[49]

To put this into perspective, this number conservatively translates to the entire population of Canada or Poland. Numbers can never adequately communicate what it must be like to lose one's home, community, or country, nor the incalculable emotional, physical, social, and financial damage displacement causes. For those able to return to their country, there is no guarantee of safety or security because water sources, food supplies, hospitals and other necessities have been decimated. These are the human costs often overlooked or completely ignored when looking at the functions of distributed *weapon systems*, but we cannot forget that the technology militaries wield have devastating human and environmental consequences. This Global War on Terror was the impetus the Kill Cloud needed to take center stage with military planners and the intelligence community; no stone goes unturned, no dollar spared, no rights supersede the threats that can be imagined with this expansive and destructive weapon we call the Kill Cloud.

Conclusion

> *"Faith preserve us all, and fertilize this ground with truth, crack these foundations with pressure of humble roots. Let ancestors rise and inhabit life once more to guide us back home from the hard night's journey behind the door."*
>
> Cian Westmoreland

As regretful participants within the Kill Cloud, we urge others to engage with the unseen aspects of drone warfare. We can all view images of drones with missiles and have heard of how they terrorize people living below them; but crucially, there has been little attention given to the less transparent programs, devices, processes, or policies that govern their objectives. The expanding machinations that send drones and other platforms out to ingest data and hunt people remain absent in most media discourse. This weapons system is hyper-staffed, and the appetite for its growth is insatiable. We must collectively pull back the veil of the Kill Cloud and see it for what it is: a massive effort of coordinated killing and global power projection under a colonial pretext that has created more problems than solved. A compounding factor that faces any society impacted by violent conflict is envi-

ronmental devastation. This devastation exacerbates issues of scarcity brought on by increasingly unpredictable weather due to the rapidly changing climate. Instead of addressing problems underlying conflicts that have continued to create more conflict, the United States has prioritized national spending toward militarizing emerging technologies. This has only served to exacerbate instability with perilously misguided actions aimed at fighting terrorism with more terrorism.

More bandwidth, like the irradiated medicines touted by snake oil salesmen of the past, is not the remedy for what ails us. Massive federally subsidized projects, such as the deployment of Starlink satellites, are being implemented under the auspices of bridging a digital divide and providing internet connectivity to the underserved.[50] This project intends to blanket the earth with high bandwidth access to allow the US military to project its vision of global security with increasingly more surveillance and automation.[51] As wars come home, smart city technology ingratiates itself in our everyday lives and its preemptive threat modeling will empower police to apply military tactics in the civilian world, further marking the underserved as threats.[52]

As described by Naomi Klein, the book *Conflict Shorelines* by Eyal Weizman observed that almost every drone strike by the US was within areas bordering on 200mm of rainfall per year. 200mm is the minimum amount of rainfall necessary to grow cereal crops without irrigation; he called this the "Aridity Line."[53]

Weizman also discovered what he calls an 'astounding coincidence'. When you map the targets of Western drone strikes onto the region, you see that "many of these attacks—from South Waziristan through northern Yemen, Somalia, Mali, Iraq, Gaza and Libya—are directly on or close to the 200 mm aridity line'… To me this is the most striking attempt yet to visualize the brutal landscape of the climate crisis".[54]

We believe that climate change and war are connected, and should be addressed accordingly. We cannot continue to perpetuate war while claiming to address climate change. The inflow of refugees directly affected by wars, instigated or perpetuated by the Global West, has led to a resurgence in xenophobic political rhetoric. Misguided efforts to stem the flow of refugees have only served to exacerbate existing inequality as we see increased militarization of the border lands. Even though we are all contributing to the problems that led to this human flow, refugees are still being treated like invading forces. The treatment of refugees along the US border and by the European Union's (EU) Frontex program reveals a deep-seated "otherization" at work. Militaristic responses only serve to embolden inhumane treatment and racism, yet do little to address the driving forces that perpetuate the problems leading people to flee their homes. It is a vicious feedback loop that results in more dehumanizing treatment bolstered by a *perceived* threat centric model. Politically expedient emission targets of less than 2 degrees celsius temperature rise, as discussed in the Paris Climate

Accords, are insufficient and ineffective at best. It will only take a 1.5 degree rise to threaten regions without sufficient resources to mitigate it.[55] War perpetuates the destruction of food and water resources on all sides of any conflict. There is no *effective* process currently in place for the public to request redress from our national role in conflicts or climate change, voting is not going to fix this. aWhile the promise of this technology is touted to lesson human suffering by sanitizing the harmful effects of war, the reality of its implementation tells a different story. In the chain of events that causes the death of another, the two of us and many others cannot escape the integral part we played. Our nations are works in progress; what we have learned is that it is time to decolonize, and it will require all of us to do it. It is our hope that others will join the discourse surrounding the ethical use of emerging technologies and continue to take steps within their communities to push the pendulum toward a more just and regenerative future. We believe that by this extension, the possibility of a more lasting peace between states, starting with its global citizens, will be achievable.

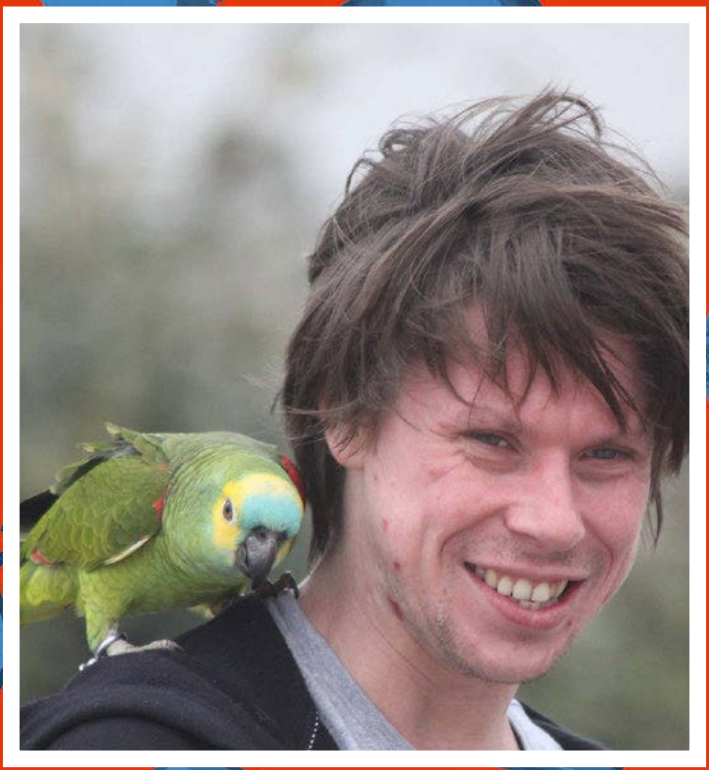
Notes

1. "The Unreasonableness of 'Reasonable' Prepublication Review, Part 1", *Yale Law School*, accessed July 18, 2021, https://law.yale.edu/mfia/case-disclosed/unreasonableness-reasonable-prepublication-review-part-1.
2. Vickers, Hon Michael. G, "The Warfighter Expects and Deserves Secure & Reliable Access to Information & Services from Any Device, Anywhere, at Anytime in a Form That Is Useable Regardless of Classification Domain", http://c4i.gmu.edu/eventsInfo/reviews/2013/pdfs/AFCEA2013-West.pdf.
3. "DOD Aims for New Enterprise-Wide Cloud by 2022", *U.S. Department of Defense*, accessed July 18, 2021, https://www.defense.gov/Explore/News/Article/Article/2684754/dod-aims-for-new-enterprise-wide-cloud-by-2022.
4. "How the Military Is Revolutionizing Situational Awareness" *FCW*, accessed July 18, 2021, https://fcw.com/articles/2012/03/15/feature-inside-dod-situational-awareness.aspx; "Intelligence Center Develops Distributed Common Ground System-Army Tactical-Engagement Teams to Support Mission Command", *eArmor*, accessed July 18, 2021, https://www.benning.army.mil/armor/earmor/content/issues/2015/JAN_MAR/Edwards.html.
5. Vickers, "The Warfighter Expects and Deserves Secure & Reliable Access to Information & Services from Any Device, Anywhere, at Anytime in a Form That Is Useable Regardless of Classification Domain", http://c4i.gmu.edu/eventsInfo/reviews/2013/pdfs/AFCEA2013-West.pdf.
6. Andresen, Joshua P. "Due Process of War in the Age of Drones", *SSRN Electronic Journal*, (2015): https://doi.org/10.2139/ssrn.2574914; and Presidents' Unchecked License to Kill", accessed July 18, 2021: https://www.justsecurity.org/75980/trumps-secret-rules-for-drone-strikes-and-presidents-unchecked-license-to-kill.
7. "Airpower Comes of Age", *Air Force Magazine*, accessed July 18, 2021, https://web.archive.org/web/20210617225946/https:/www.airforcemag.com/article/Airpower-Comes-of-Age.
8. "DOD Aims for New Enterprise-Wide Cloud by 2022", *U.S. Department of Defense*, https://www.defense.gov/Explore/News/Article/Article/2684754/dod-aims-for-new-enterprise-wide-cloud-by-2022.
9. "Technology Innovation and the Future of Air Force Intelligence Analysis: Volume 2, Technical Analysis and Supporting Material", *RAND Corporation*, (2021), https://doi.org/10.7249/RRA341-2; "Want to Understand MDC2? Think About Uber, USAF Official Says", *Air Force Magazine*, accessed July 18, 2021, https://www.airforcemag.com/Want-to-Understand-MDC2-Think-About-Uber-USAF-Official-Says.

10. "Technology for Innovative Entrepreneurs & Businesses", *TechLink*, accessed July 18, 2021, https://techlinkcenter.org/news/new-us-army-software-rapidly-converts-live-drone-video-into-2d-and-3d-maps.
11. "A Brief Introduction to Distributed Systems", *SpringerLink*, (2016): accessed July 18, 2021, https://link.springer.com/article/10.1007/s00607-016-0508-7.
12. "Air Force Distributed Common Ground System", *U.S. Air Force*, accessed July 18, 2021, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104525/air-force-distributed-common-ground-system.
13. "Air Force Moves Ahead with Headquarters-Level Merger of Intel, IT Functions", *Federal News Network*, accessed July 18, 2021, https://federalnewsnetwork.com/air-force/2019/01/air-force-moves-ahead-with-headquarters-level-merger-of-intel-it-functions.
14. "Air Force Distributed Common Ground System", *U.S. Air Force*, accessed July 18, 2021, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104525/air-force-distributed-common-ground-system; "European Partnership Integration Enterprise Opens New Facility", *DVIDS*, accessed July 18, 2021, https://www.dvidshub.net/news/297660/european-partnership-integration-enterprise-opens-new-facility.
15. Sarah Shoker, *Military-Age Males in U.S Counterinsurgency and Drone Warfare* (Palgrave MacMillan, 2021).
16. Ibid.
17. "Reducing Over-Classification Act", *Govinfo.gov*, accessed July 18, 2021, https://www.govinfo.gov/content/pkg/PLAW-111publ258/pdf/PLAW-111publ258.pdf.
18. "Audit of the Department of Justice's Implementation of and Compliance with Certain Classification Requirements", *U.S. Department of Justice Office of the Inspector General*, accessed July 18, 2021, https://oig.justice.gov/reports/2013/a1340.pdf.
19. "Government's Motion In Limine to Exclude Certain Evidence, Argument, or Comment at Trial" *Project on Government Secrecy*, accessed July 18, 2021, https://fas.org/sgp/jud/hale/usa-exclude.pdf.
20. "United States District Court for the Eastern District of Virginia, Alexandria Division – Motion for Leave to File Amicus Curiae Brief on Behalf of CAIR Foundation", accessed July 18, 2021, https://storage.courtlistener.com/recap/gov.uscourts.vaed.405902/gov.uscourts.vaed.405902.219.0.pdf.
21. "Why Joe Biden Should Pardon Reality Winner", *The Washington Post*, accessed July 18, 2021, https://www.washingtonpost.com/opinions/why-joe-biden-should-pardon-reality-winner/2020/12/21/9e6f4094-4162-11eb-8db8-395dedaaa036_story.html; Kennebeck, Sonia "CodeBreaker Films", Enemies of the State, 2020, https://www.codebreakerfilms.com/films.
22. "National Security and America's Unnecessary Secrets", *The New York Times*, accessed July 18, 2021, https://www.nytimes.com/2011/11/07/opinion/national-security-and-americas-unnecessary-secrets.html.
23. "Command & Control Battle Management Operations: Controlling the Chaos", *Air Education and Training Command*, accessed July 21, 2021, https://www.aetc.af.mil/News/Article/1578287/command-control-battle-management-operations-controlling-the-chaos.
24. "Air Traffic Control - 1C1X1", *U.S. Air Force*, accessed July 19, 2021, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104595/air-traffic-control-1c1x1; "Air Battle Managers: Offensive Coordinators of the U.S. Air Force", *Air Combat Command*, accessed July 19, 2021, https://www.acc.af.mil/News/Article-Display/Article/2111041/air-battle-managers-offensive-coordinators-of-the-us-air-force; "U.S. Air Force - Career Detail - Air Battle Manager", accessed July 19, 2021, https://www.airforce.com/careers/detail/air-battle-manager.
25. "Network Centric Warfare: Creating a Decisive Warfighting Advantage", accessed July 18, 2021, https://www.hsdl.org/?view&did=446193.
26. "Eliminating the Fog of War", *SIGNAL Magazine*, accessed July 18, 2021, https://www.afcea.org/content/eliminating-fog-war.
27. "The Air Force Tested Its Advanced Battle Management System. Here's What Worked, and What Didn't", accessed July 20, 2021, *C4ISRNET*, https://www.c4isrnet.com/air/2020/01/22/the-us-air-force-tested-its-advanced-battle-management-system-heres-what-worked-and-what-didnt.
28. "With Its Promise and Performance Confirmed, ABMS Moves to a New Phase", *U.S. Air Force*, accessed July 19, 2021, https://www.af.mil/News/Article-Display/Article/2627008/with-its-promise-and-performance-confirmed-abms-moves-to-a-new-phase.
29. "Network-Centric Warfare Airborne Military Communications Links Approved for Deployment", *Military Aerospace*, accessed August 1, 2021, https://www.militaryaerospace.com/home/article/16709544/networkcentric-warfare-airborne-military-communications-links-approved-for-deployment.
30. "Battlefield Airborne Communications Node (BACN)", *Air Combat Command*, accessed August 1, 2021, https://www.acc.af.mil/About-Us/Fact-Sheets/Display/Article/2241383/battlefield-airborne-communications-node-bacn.
31. "LEO Constellations" *Airbus U.S. Space & Defense, Inc.*, accessed August 4, 2021, https://airbusus.com/leo-constellations; "Musk's Satellite Project Testing Encrypted Internet

with Military Planes", *Reuters*, accessed August 4, 2021, https://www.reuters.com/article/us-spacex-starlink-airforce/musks-satellite-project-testing-encrypted-internet-with-military-planes-idUSKBN1X12KM; "Global Lightning' SATCOM Project Expanding to AC-130, KC-135", *Air Force Magazine*, accessed July 20, 2021, https://www.airforcemag.com/Global-Lightning-SATCOM-Project-Expanding-to-AC-130-KC-135.

32. "The Air Force Just Conducted the First Test of Its Advanced Battle Management System", *C4ISRNET*, accessed August 1, 2021, https://www.c4isrnet.com/air/2019/12/21/the-air-force-just-conducted-the-first-test-of-its-advanced-battle-management-system.
33. "The Air Force Just Conducted the First Test of Its Advanced Battle Management System", *U.S. Air Force*, https://www.af.mil/News/Article-Display/Article/2446122/gatewayone-and-attritableone-test-moves-joint-force-one-step-closer-to-iotmil-d.
34. *Anduril*, accessed August 1, 2021, https://www.anduril.com/company.
35. "GatewayONE and AttritableONE Test Moves Joint Force One Step Closer to 'IoT. mil,' Demonstrates F-22, F-35 First Secure Bi-Directional Data Sharing", *U.S. Air Force*, https://www.af.mil/News/Article-Display/Article/2446122/gatewayone-and-attritableone-test-moves-joint-force-one-step-closer-to-iotmil-d.
36. "City of Sherrill v. Oneida Indian Nation of N.Y, 544 U.S. 197" (2005) ", *Justia US Supreme Court Center*, accessed July 19, 2021: https://supreme.justia.com/cases/federal/us/544/197.
37. "Distribution of Race and Ethnicity among the U.S. Military", *Statista*, accessed July 20, 2021, https://www.statista.com/statistics/214869/share-of-active-duty-enlisted-women-and-men-in-the-us-military.
38. "Technology Innovation and the Future of Air Force Intelligence Analysis: Volume 2, Technical Analysis and Supporting Material", *RAND*, accessed July 20, 2021: https://www.rand.org/pubs/research_reports/RRA341-2.html.
39. Dunlap Jr., Charles J., "Lawfare: A Decisive Element of 21st-Century Conflicts?", 54 *Joint Force Quarterly* 34-39 (2009), accessed July 20, 2021, https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=6034&context=faculty_scholarship.
40. "ISR After Afghanistan", *Air Force Magazine*, accessed August 18, 2021, https://www.airforcemag.com/article/0113isr.
41. "The Intel Net", *Air & Space Magazine*, accessed July 20, 2021, https://www.airspacemag.com/military-aviation/the-intel-net-180960363.
42. Ibid.
43. Ibid.
44. Ibid.
45. "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective ", *JSTOR*, accessed July 20, 2021, https://www.jstor.org/stable/3178066.
46. "The Fastest Ooda Loop: The Implications of Big Data for Air Power", accessed July 20, 2021, https://apps.dtic.mil/dtic/tr/fulltext/u2/1040684.pdf.
47. "A Critique of the Boyd Theory—Is It Relevant to The Army?", accessed July 20, 2021, https://apps.dtic.mil/dtic/tr/fulltext/u2/a374770.pdf.
48. "The Intel Net", *Air & Space Magazine*, https://www.airspacemag.com/military-aviation/the-intel-net-180960363.
49. "New Costs of War Study: 37 Million Displaced by U.S. Post-9/11 Wars", *Watson Institute*, accessed July 20, 2021, https://watson.brown.edu/research/2020/Post-9/11DisplacementStudy.
50. "Cherokee Nation Begins Installation of Starlink in Rural Areas", *5news*, accessed July 21, 2021, https://www.5newsonline.com/article/news/local/cherokee-nation-installs-starlink-in-rural-areas-tribe-hopes-to-close-the-digital-divide-chief-hoskin/527-97d8396d-2ab1-4c95-a508-80c86821f619; "Google Cloud Wins SpaceX Deal for Starlink Internet Connectivity", *CNBC*, accessed July 21, 2021, https://www.cnbc.com/2021/05/13/google-cloud-wins-spacex-deal-for-starlink-internet-connectivity.html.
51. "U.S. Army Signs Deal with SpaceX to Assess Starlink Broadband", *SpaceNews*, accessed July 21, 2021, https://spacenews.com/u-s-army-signs-deal-with-spacex-to-assess-starlink-broadband.
52. "242. Military Implications of Smart Cities", *Mad Scientist Laboratory*, accessed July 21, 2021, https://madsciblog.tradoc.army.mil/242-military-implications-of-smart-cities.
53. Klein, Naomi, "Let Them Drown", *London Review of Books*, June 2, 2016. https://www.lrb.co.uk/the-paper/v38/n11/naomi-klein/let-them-drown.
54. Ibid.
55. "The Paris Agreement", *UNFCCC*, accessed July 21, 2021, https://unfccc.int/process-and-meetings/the-paris-agreement/the-paris-agreement.
56. "Reachback and Distributed Operations ISR", *Curtis E. Lemay Center*, January 29, 2015, https://www.doctrine.af.mil/Portals/61/documents/AFDP_2-0/2-0-D11-ISR-Distributed-OPS.pdf.
57. "Joint Spectrum Center (JSC) Overview Brief", *Defense Information Systems Agency*, accessed August 18, 2021, https://storefront.disa.mil/kinetic/app/resources/disa/DSO%20JSC%20Overview%20brief.pdf.



LAURI LOVE

Photo by Sylvia Mann

Lauri Love is a Security Engineer and activist based in the UK. In 2018, he successfully fended off the prospect of 100 years in the US prison system for his alleged involvement in online activism. That landmark appeal ruling has proven a critical precedent in subsequent high profile extradition cases. He played a prominent role in the student and Occupy movements in Glasgow during 2011-12. Love is being recognised as an expert on hacking, surveillance and privacy issues in the UK and has made a principled stand against the country's forced decryption laws.

LAURI LOVE

SOUSVEILLANCE

REVOLUTIONARY REAPPROPRIATION OF VIGILANCE BY THE NETWORKED POLITY

I WAS BORN in 1984 of a neurodiverse phenotype—autistic, eccentric and prone to flights of fancy—if relatively debilitated in executive function and other properties required by normative society, I came of age as the Internet blossomed and saw in its potential a wonderful new kind of world, in which my taxing misfittedness might instead give way to a relative adaptedness that could be most beneficial and valued. I struggled to follow the prescribed trajectory of an intellectual, not quite managing to complete academic degrees as mental health difficulties and/or the more pressing need to right inexcusable wrongs in society interfered with the expected monomania of ticking boxes. Though having a great desire to better the world, I had no taste for fame or prominence. Regardless, fame, or perhaps infamy, was nevertheless thrust upon me when in 2013 it suited the agenda of certain components of the US hegemonic power structure to criminally persecute me through legal instruments and the complicity of the United Kingdom's courts, for supposed involvement in an Anonymous-heralded hacktivist campaign to seek redress and reform after overzealous prosecutorial abuses drove the Internet wunderkind Aaron Swarz most tragically to suicide.

I was dealt then by fate a harrowing but potentially quite useful opportunity to raise a bulwark against the extra-territorial arrogation of global policing perversity by the United States, and set a precedent raising the bar against plucking poor souls from overseas and subjecting them to the assorted torments and inhumanities of the carceral system that still today in that cursed state carries the wretched torch of slavery and the worst manifestations of evil that it accrued. On the gambit that my very life might be forfeit, a great and noble alliance of good-doing that arose in a campaign to which I will forever be grateful was able thankfully to convince the highest court of the United Kingdom that it would be not only wrongful, but "*unjust and oppressive*" to render me to the US.

I hope only that the still-scarring limelight of that most difficult of episodes in my life may yet save many others, most notably and pressingly Julian Assange, from the similarly horrific fate of falling into the appalling and unmitigatedly hei-

nous estate of incarceration in the United States that all of good conscience and character are increasingly coming to the consensus can only rightly be redressed by one outcome: total abolition.

Content now to reassume the privilege of non-notability and non-celebrity, I now ply some modest trade as a security engineer, and am occasionally induced to venture a few words that might have some beneficial, if also modest, effect on the hearts and minds of others. My remaining aspirations, neither modest nor humble by necessity, are to facilitate the realisation of universal quantum post-Turing hyper-computation while avoiding the menaces of uber-mechanised moral hazard, and thereby to achieve, perhaps even in this most precious lifetime of human incarnation, perfect and complete enlightenment for the benefit of all sentient beings. By vying so for the nigh-on impossible, I hope at the very least not to join the unfortunate ocean of settling that besets us now. Too long we have settled for what is; we must rejoice today and tomorrow that we are ever capable of realising what yet might be.

Sous-, You, Sur-? Prepositional Modalities of Vigilance in the Context of Hierarchies of Power

We are used to the concept of surveillance: the vigilance of those with power and (more or less legitimate) authority 'down' onto the citizenry, the congregation, the class, the userbase—or in these digital Ed-Snowdenian pantopticraptic days, the whole damned digital world. Then again, we are used to thinking of power and authority in general as operating in the prepositional modality of a classical hierarchy—from the top to the bottom, the centre to the periphery, governors to governed. So we are schooled, and not without cause or reason, as the well-conditioned internalise the suggestion that their role is to accept power and authority and thus by extension surveillance. The expectation, more implicit than explicit, being that the *quid pro quo* and equity awaits necessarily their ascendence from hoi-polloi to the hallowed spheres of the elite.

The observational converse has also always obtained: ministers or barons observing the monarch, and on occasion holding them to account on the basis of such observations and the dialectic they enable. Even unto the base of the hierarchy has it been ever possible to gaze upwards, to view, to the extent of acumen to analyse, and more recently even to document the workings of power. However, there was not for most of history, in most recorded societies from which we inherit tradition and structure, much, if any formalised, countenanced, nor effective mechanism for vigilance and accountability to flow counter to the gradient of hierarchical power.

Thus we had to await the nigh contemporary coinage—courtesy of cybernetician, engineer, professor and inventor Steve Mann—of the term "*Sousveillance*", a straightforward reversal of the preposition in the French compound to denote vigilance upwards from below. Like most ideas, birthed of their time when context and contingency conspire, the emergence of the concept of sousveillance is reflective of the environment in which it became manifest—like a panoramic polaroid bringing into focus and relief the concomitants of its occasion.

In particular, sousveillance obtains and empowers in an age of near ubiquitous facility for the masses to record with fidelity—something it is easy to forget was once more or less the exclusive province of bodies vested from centralised power and authority, to whom were afforded the opportunity and responsibility of entering into the record, the rolls, the chronicles. We are blessed however with both—opportunity and responsibility—of making, storing and disseminating records to an extent that our antecedents could scarce have imagined possible.

One could perhaps at a squint cast as one of the functions of folklore and fairytale to capture, if not the particularities, then the generalities and gist of the exercise of power, and thus exert some influence, albeit vaguely and culturally, over its future exercise. The *Panchatantra* (Five Treatises), for instance, a collection of interrelated animal fables dating in written form between 200-300 BCE and of an oral lineage much older, can be taken as an allegorical vehicle to impress indirectly the essence and elaboration of good governance through the anthropomorphisation of animals embodying archetypes and tendencies still easily recognisable by readers of today, and influencing more familiar western corpora, most notably the fables of Aesop, but also Boccaccio, La Fontaine and the brothers Grimm.

Culture however, though exercising momentous influence, does so with the loosest of grips and with quite fallible efficacy against the sociopath and tyrant. The direct and viscerally causal exercise of moderating force and requisition of inverse representation—the accountability of the powerful unto its subjects—consequent to observational and recording faculties, had to await in extending franchise broadly for the invention and proliferation of the printing press. At that crux in the dance between technology and realpolitik did the second great symbol of power emerge to truly equal the first: the pen became as mighty in potentiality as the sword.

The pamphleteers thus, empowering themselves not with martial armaments but with verbal ornaments, with wit and satire—something before suffered by the crown only to the jester and a few in court, and even then at the risk of losing ones head—were now able to twist inflection on the fortunes of the powerful with more efficacy by the raising of contempt, derision and ire, than the prince, duke or baron could achieve by raising armies. Joining then the ranks of the clergy, the nobility, and commoners, arose *the fourth estate* of the realm: the press and news media that self-organised from the scattershot agendas of individual empressors

into a regulatory capacity inextricable from the state, though at differing times as varyingly independent as the preceding three estates.

Nevertheless, though greatly enlarging both the means of moderation and accountability, as well as the breadth of those enfranchised to exercise either, the press did not yet afford universal nor unmediated ability for individuals in the body politic to proceed from observation to intercession in the face of the vagueries and abuses of the powerful. The essential flow from recognition to remediation remained, despite the democratising influence of the press, constrained by the necessity of traversing conduits of institutions, and the great water that cleanses the mires of power was oft enough sullied along these capillaries by editorial prejudice, the constraint of the mores and mendacities of a privileged class, and too often stemmed entirely in the editor's cutting room, or by the censor's hand.

Providence however had yet in store more twists to exert upon the social fabric. The letter gave rise to the postal service, the first democratic verbal interconnection of people at geographic remove. The post in turn inspired with the advent of electricity the telegraph, greatly decreasing the latency of this new phenomenon—*The Network*—and increasing its throughput and extent. The necessity of encoding the written word, which the telegraph greatly increased (though visual signalling and the demands of secrecy had already given it a head-start), spurred on the encapsulation into discrete forms of verbal thought that tentatively progressed, from the untamed analogue through alphabetisation and the standardising influence of the widely disseminated written word, into digitisation. No longer were writings but conventionally informative, they were now a new veritable essence; *Information*: something not just quantifiable, but about which an entire science, theory and praxis would evolve and begin to exert its own influence back upon the genius in humanity.

The theory of information, though collegiate, international and fraternal as a theoretical discipline of mathematics, became—in the ineffable poetry of destiny—most fecund when, for better or worse, its practice between decisively uncollegiate foes became determinative to the fate of nations. In war it was then—as a continuation of the age-old necessity of keeping secret from potential interceptors the true content of messages—funnelled through the technology of digital transmission, now traversing the very aether itself, that the fraternal mathematical theories of information and logic now wrought from digital intrigues—the coded messages of generals and admirals—the utility, sharpened to existential necessity, of a new participant in information and its networking: *the calculating, computing machine*. Now observations intended to have limited disseminative ambit were—through the mechanisation of arithmetic process—liberated against the will of their senders, and in the process could change the course of global history.

At this epoch, man—made in God's image—realised as never before God's creative function. From humanity issued a new entity, in a certain manner rendered

in man's image: the logic gate, and the grimoire of beneficent daemonic forms constituted therefrom. And the logic gate went forth, multiplied and prospered. Indeed, it is not too much of a conceit to say that the logic gate, latterly realised as the transistor, is now the most successful species of being on planet Earth today, for it has consistently doubled in number, density and interconnection since its inception, enjoying thus a geometric growth denied to biological species except in extreme brevities.

All Bets Are Off—The Topological Singularity That Renders All Extant Social Contracts Defunct

We are all familiar, if not with the theory, then with the phenomenology of phase transitions. We see water freeze to ice, ice melt to water, water evaporate or boil into stream and steam condense back into water. Less widely appreciated is the information theory—the entropics—of phase transitions. Briefly surmised, the input or extraction of heat energy which is usually correlated with increase or decrease of temperature, takes on a more mysterious role at the phase transition. Heat is the random velocities of molecular constituents of matter, but on condensation and in freezing, an environment extracting heat from a gas or liquid ceases to change the temperature and instead affects the orderliness of this heretofore inchoate cacophony of jitters. The molecules become arranged in more-organised, highly-structured and typically more-compact formations.

A similar phase transition occurs in the interconnection and mutual entrainment of an informational network when conditions begin similarly to favour long-range correlations between the dispositions of constituent elements. In the informational network constituted by our neurons, their electromagnetic interrelation to one another and via the skeletal-musculature field to the environment, this phase transition gives rise to consciousness, an integration of atomic awarenesses into an experiential stream that comprises our typical daily experience.

If we take as Gregory Bateson suggests, that information is "difference that makes a difference", then consciousness is perhaps the superlative exemplar—a topology of dense, informationally rich, integral yet almost infinitely open-ended interconnection, that weaves from mere sentience the double sapience we cherish as our defining characteristic.

So then the network of information whose history we have briefly reprised can be seen to have met with a topological-connectivity-enacted epochal phase transition. Those of us privileged to remember a world largely not yet visibly affected by this transition and survive to see a world in which scarce little escapes its effect are spared the misleading seeming mundaneness of its commonplace nature to our younger compatriots. We speak of course of *The Internet*, the Network

of Networks, the Great Chain of Being made manifest by the digital and all it can represent, whizzing hither and thither at speeds approaching that of light—of causality itself—and in densities that boggle even the minds of the adept.

Those online, increasingly a supermajority of humanity, are now connected, may interface one to another, one to many or many to one, with restrictions diminishing logarithmically towards zero. Can we say at this point that the default discretisation of political power—geographical proximity on the basis predominantly of accidents of birth—retains legitimacy as the basis of social compacts? When association, common endeavour and the intertwining of destiny may now self-organise on the basis of myriad other concerns than how far an army might march before encountering another, surely we must consider that all extant contracts imagined between polities and the powers over them are rendered null and void.

This truth upon inspection and mediation stands undeniable and inescapable, though it has yet to be faced, except in some dreams, some words [cf. *A Declaration of Independence of Cyberspace* by John Perry Barlow], and the valiance of thus far evocative if sometimes abortive attempts of emergent collective consciousness to assert a will to sentience, sentiment, values and the exercise of power in their service, though it be necessarily at times in lesser or greater defiance of the *ancien remines* [cf. The Open-Source Community, Cyberarmy, Hacktivismo, Freenode/Libera, Freenet, Blockchain, Anonymous, etc.].

The fact remains—and is of such gravity that it will attract unto itself further facts, ever increasing its transformative potence—that we now face one another as humankind. And in mutual observation—shall we call it '*interveillance*'?—we await perhaps the greatest political shift of all, visible on the horizon of history, where the dialectic between this emergent networked polity and the systems of entrenched power that have managed thus far, if occasionally tenuously, to suborn and shackle it, must play out as inevitably as the rain must fall and the sleeping must wake.

The last great globally transformative dialectic of power is widely considered to be that of *the labour movement*—when the notion, first elaborated in the form of words, became realised in practice, that the workers, in unison, might through collective bargaining reclaim the productive value of their toils from the usurpation of the capitalist classes, and engage (sometimes even successfully) in the reimagining of society made possible by the resultant redistribution of potency.

A vision arises then, as the network awakens unto itself and finds through fumble and falter its footing at last, that we must face another grand dialectic of power, and through collective bargaining we the networked must elicit a new settlement with the remnant analogue powers, represented now predominantly by state, church and corporation, whose compacts remain on the basis respectively

of geography, creed and greed—restrictions that the network finds increasingly irrelevant and must face with increasing irreverence.

The Third Symbolic Archon of Power—No Longer but Pen and Sword—Ecce Potentialis Monoculis

Though ironic perhaps to the point of distaste in its invocation at the Langley headquarters of the Central Intelligence Agency of the United States of America, two epitomes respectively of information and networking fouled by subordinance to secrecy and exclusivity, and professed and extroverted noble ideals masking unacknowledged and introverted toxicity and violence—the verse of John's Gospel, 8.32 remains of divine provenance and universal application: "*And you shall know the truth, and the truth shall set you free.*"

LulzSec logo, 2011

Sousveillance as a form of praxis wherein truth is instrumentalised through oversight and accountability into eventual guarantorship of freedom, came into its own in the context of the network when what had heretofore been a great fear of the machinations of power and on occasion a great moderator too—the leak—became itself as democratised as literacy made the pen, and nothing shall ever make the sword. Before the network, leaking had been predominantly a tool of those inside the tent of circumscribed power to engage in intrigues one amongst another: a department or a minister or an aide, disgruntled or avaricious, or from time to time even afflicted by conscience, channelling information through the still distorting lens of the established press to the masses. In the network it has evolved into a more perfected form.

Firstly, the disintermediation of the (ever corruptible, thus ever corrupted) established press, possible because the network enables the viral proliferation of content and routes around the censorship it rightly perceives as damage, is seen not just in the transcendence of curation, editorialization, distorting presentation, and selective publication of the leak, but also in supplanting of the (ever corruptible, thus ever corrupted) professional class of journalist as mediator between the press and the source, another cause of myopia and prejudice, and a pinch-point for power.

Experiments in the transcendence of both these modes of mediation have been transformative, if yet far from perfected. Most notable of course remains WikiLeaks, an organisation accepting contributions by anyone, and if they meet the sole bar of being verifiably authentic, granting to the public the revolutionary boon of direct access to original source materials, facilitating perusal, but declining or at least minimising editorial discretion and selectivity of publication, save for the mitigation of potential harm.

The transformative effect of this paragon is testified not only in the great utility the network has derived from its endeavours, but even more poignantly perhaps in the ruthlessness and sheer villainy of the reactionary efforts by the powerful (most publicly enacted through the offices of the *United States Department of [In]Justice*) to destroy its most visible personage, Julian Assange, who at the time of publication remains, after over a decade of unmitigated fuckery, in a battle against being rendered to the state whose war-crimes he helped the world to know, to be undoubtedly held in conditions of torture perhaps unto his death.

Not even the marginalisation of WikiLeaks, however, can stop the continued manifestation of the monocle as a new contender and equal to the pen and the sword. The subversive merry pranksters and hackers *Lulzsec*, operating alongside and synergistically with WikiLeaks, gave the monocle the power to strike fear into the hearts of assorted emperors lacking both clothing and security, and the even more potent power through humour and mirth to inspire the already fermenting collective manifestation known as Anonymous to briefly rise to the dubious honour of becoming "public enemy number one", supplanting even the most useful spectres of rogue states and terrorists.

These prime movers may be gone or past their prime, but the potential they demonstrated cannot be suppressed by the criminalisation of a few good denizens of the network. Evolution heeds not the beck of power to halt, to cease or to desist. The monocle renders only more powerful—through innovations in the decentralisation of fault-tolerance by transcending single points of failure—the network's capability to obtain leaks and to make them available at large.

Protocolisation of Conduct—Emergent from Consensus—Enforced by Cryptographic Mathemagics

Thus we touch upon the latest, greatest discipline of information theory, most proximate to magic, to the divine: *cryptography,* in its maturity not just the study of encoding and decoding, ad-hoc schemes whose security could only be assumed until demonstrated lacking. Now nestled between mathematics and computer science and becoming the equal and indispensable partner of both, cryptography offers to the network new and staggering potentialities through increasingly

powerful *primitives*—basic constituents from which systems of open-ended agility can be spun.

Bitcoin, and the sprawling ecosystem of blockchain-contingent, even blockchain-transcending systems of distributed, decentralised, fault-tolerant and censorship-resistant rich information interplay are revolutionary towards power and authority in a way so novel it was almost universally agreed to be unviable: they have allowed the network to come to a most powerful state of being—*consensus*. By coupling an economic externality as incentive yoking self-interest to mutual benefit, the anonymous genius we know by the pseudonym Satoshi Nakamoto overcame the trifling hindrance of a mathematically proven impossibility and solved the problem of *Byzantine consensus* in a distributed and decentralised system. Agreement was now, and shall forevermore remain possible to achieve between potentially mutually-untrusting participants in a network as *a shared state*, a set of truths, a reality construct contributed to by all, but owned and controlled by no single entity or subset—truly something more than the sum of its parts.

The Bitcoin network consensuates two powerful primitive notions: the ticking of a network clock, and the integrity of a ledger giving the authority—without the need of any central arbiter—of all participants to possess and transact.

While this prototypical consensus is quantitative and fiduciary, we ought remind ourselves that the digit and tally-mark also emerged in service to the reckoning of private property and enabling of commerce. Yet the digital now encompasses not only the quantitative and coveted, but also the qualitative, universal, ineffable and sublime: *Wikipedia*, *Project Gutenberg*, photography video and missives of our beloveds.

So one imagines that networked cryptographic consensus might very well and imminently extend to the emergence and contingent concretion of collective value, and that protocolisation might carry yet further the democratisation of power through the facilitation of oversight and accountability that the leak has given us yet but piecemeal and haphazardly. Where before it took acts of personal courage, integrity and the [mis]fortune of standing to blow the whistle, and it took yet more complex and fragile instruments of untarnishing proliferation to make of the blown whistle a clarion call to justice, we can conceive already of cryptosystems in which the vesting of any and all powers and authorities to individuals, offices and entities from the networked polity (that must ultimately and always be the ceding source), is automatically and inexorably yoked to a responsibility of adherence to consensuated values no longer just assumed until found otherwise, but guaranteed cryptographically.

For there exists a synthesis of the transparent and the opaque made possible by the cryptographic primitives of "*commitment to state*" and "*proof in zero knowledge*". A few examples should suffice to prime the imagination of the reader. Consider the sadly residual problem of discrimination in the workplace, say in the

context of hiring. A company may institutionally, or a manager sporadically and autonomously, be inclined contra the normative values of society to prefer to hire applicants not only on merit of skills and experience, but because they have the right kind of name, complexion of skin, or creed. We may however define a game—rules for hiring if one is to have the suffrage of participation in the networked economy—when an entity makes a decision, to which we afford the default privilege of opacity, that is to be one's own business, it is required that a cryptographic commitment be made to all inputs to that decision, and the decision made. Once committed to, this information exists in an opaque yet immutable form on the network. Upon suspicion of discrimination here, or malfeasance of any kind more generally, the system can oblige the opening—transparency—of some statistical sample of these commitments, and a mathematical function can be computed thereon. The system's participants may then determine that, for instance, other factors considered equal, the company or manager hired preferentially applicants in a racist, sectarian or otherwise discriminatory manner. This may be known without compromising the privacy of particular applicants—though if it be deemed useful, for instance to identify victims for compensation, then they might be identified, but the contents of their resumes or the jobs to which they applied be kept private.

Similarly, for example, insider trading might be disincentivised by the facilitation of its detection by committing the input (reasons it was deemed sensible) to make a trade and the trade made, and again through computation in zero knowledge of statistical functions discrepancies be ascertained between trades and the available '*kosher*' public knowledge which might inform them.

Polity as Argus Panoptes—Moral Photonic Pressure of Myriad Eyes

Generalising from these examples, we can envision that the cryptographic capacity for the operation of entities in the networked polity, be they of governance, business, or anything else upon which consensuated values would take a view, to be afforded opacity, thus privacy and competitive freedom by default, and yet render unto the system in a manner minimising the compromise of these desiderata the facility of exercising the functions of oversight and accountability, while dispensing with the requirement for some privileged ombudsman or regulator, limited, imperfect and corruptible as they tend to be.

Without roles, offices and agencies vested by centralised powers deriving legitimacy ultimately—as all yet do today—from some manner of coercive authority, underpinned by the potentiality of force through the monopolisation of violence, we perceive within our imminent reach the dream of cryptographic anarchy:

order, justice, equality and freedom, without the archon singular and central, but through the distributed and holistic archonate of the monocles of all participants.

Argus Panoptes we might collectively constitute, not a Leviathan that rises beastly from the masses to swing a sword, nor merely by the pen that inscribes indelible, powerful in the province of a few, but by the gaze of a collective and a transparency that need not come at the unnecessary injury of privacy to individual or group. The many eyes of Argus might well mostly be sleeping, but a few remaining vigilant and the ability to select that few after-the-fact, yields a potential where in the limit, ideally, the mere pressure of possible observation is enough to keep the conscience functional.

Solitary Whistles Blown May Yet Cohere Into an Orchestra of Right

We participate today in an economy which we know to facilitate the most horrific of crimes and abuses, and hope the appendages of coercive authority will mitigate these, while perceiving that as often as not they are complicit therein. Yet we, the participants of the networked polity, are the very ones who turn the cogs and gears, press the buttons, sign the authorisations, give transit to the information that enables these enormities. Too often however, those forming the chains of causation that enable e.g., war-crimes, exploitation of labour, ecological destruction, etc. see so small a part of the picture that neither their culpability nor agency rise to the level of Eichmanns. But imagine an app with the tagline "*Let us collectively oblige one another to be just*". Imagine the bank teller who receives the suggestion that today it might be good to highlight transactions between this and that company for vigilance, or someone peripheral to this or that factory to contribute a piece of a jigsaw puzzle. In a cryptographically-empowered networked world where all the eyeballs of both humans and machines can be harnessed through transparency toward justice, in what shadows will evil find a place to lurk, as the sunshine floods to every crevice and corner?

JOANA MOLL

Photo by Francesc Melcion

Joana Moll is a Barcelona/Berlin based artist and researcher. Her work critically explores the way technocapitalist narratives affect the alphabetisation of machines, humans and ecosystems. Her main research topics include internet materiality, surveillance, online tracking, social profiling, and interfaces. She has presented her work in renowned institutions, museums, universities, and festivals around the world. Furthermore, she is the co-founder of the Critical Interface Politics Research Group at HANGAR (Barcelona) and co-founder of The Institute for the Advancement of Popular Automatisms. She is currently a visiting lecturer at Universität Potsdam (DE), Escola Elisava (ES) and Escola Superior d'Art de Vic (ES).

JOANA MOLL

BEHIND AND BEYOND
TRACKING NARRATIVES & USERS' AWARENESS

IN FEBRUARY 1999 I visited an exhibition by William Kentridge, a graphic artist, filmmaker, and theatre arts activist, at the Museum of Contemporary Art of Barcelona (MACBA). Back then I was a pre-graduate art student and I felt that drawing and sculpting were interesting and necessary in many ways, but meaningless in many others, in the sense that, back then, the creative process did not answer to anything but my inner world, and the results were just measured by varying degrees of self-satisfaction. In other words, I believed that art practice was isolating and dramatically detached from its concurrent realities.

Kentridge was born in South Africa to a Jewish family in 1955. His parents were lawyers well-known for representing victims of the apartheid. In essence, Kentridge's work examines the profound social injustice caused by such a discriminatory system through drawings, animations, films, and theatre performances. It was the first time in my life that an artist exposed the political dimension and the activist possibility of art and art practice to me. Moreover, even though back then I ignored the particularities of the apartheid, through Kentridge's drawings, I could experience, intensely, the deep social, political, and emotional toll left behind by this policy of racial separation.

Regardless of Kentridge, it took several years to articulate and integrate a conscious critical artistic practice capable of informing and being informed by its coexisting realities. Moreover, defining what "critical practice" means has become central (and a never-ending process) in my work, as I believe that the term must be constantly revisited to coherently engage with the realities that I am trying to affect. My work lies at the intersection of art, research, and investigative journalism, with a strong focus on techno-capitalist narratives and their effects on the alphabetization of machines, humans, and ecosystems. In particular, over the last ten years, I've consistently targeted the hidden layers of the so-called data economy apparatus: from its physical infrastructures to the geopolitics of data, corporate surveillance practices, the commodification of user data, and materiality of data. One of the major drives, and outcomes, of my work, is to expose critical techno-social arrangements that govern our lives but are mostly opaque to the

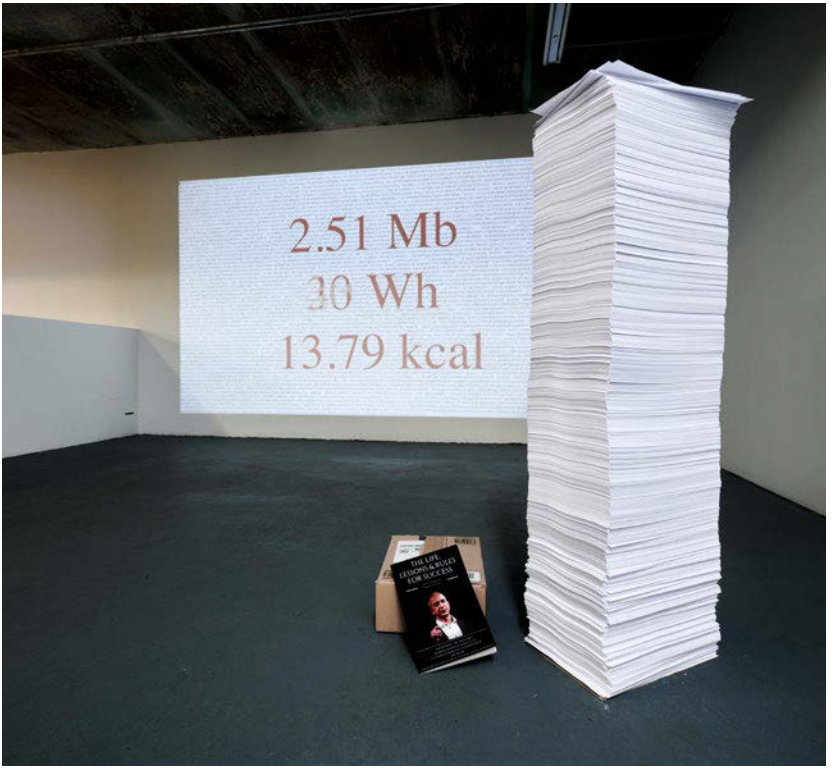
average citizen, and in turn, generate dramatic power asymmetries between the ones running the technical infrastructures and the ones using them. I believe that producing evidence is a crucial act to empower users to identify and promote sustainable, transparent, and accountable forms of governance, which are essential to forging a fair and just society.

In this text, I will focus on describing the making of three of my recent projects that expose severe malpractice at the hands of corporate and governmental stakeholders and, at the same time, highlight the role of creative practice in uncovering and denouncing such actions.

The Hidden Life of an Amazon User (2019)[1]

On June 17, 2019, in Utrecht, I purchased *The Life, Lessons & Rules for Success: The Journey, The Teachable Moments & 10 Rules for Success Cultivated from the Life & Wisdom of Jeff Bezos* from the Amazon website. In order to purchase the book, the Amazon website forced me to go through 12 different interfaces composed of large amounts of code—normally invisible to the average user. This code carries out all sorts of operations, such as organizing and styling the site's content, supporting interactivity, and recording the user's activity—such as their clicks and scrolls. Overall, I was able to track 1,307 different requests to all sorts of scripts and documents, totalling almost 10,000 A4 pages worth of printed code, adding up to 87.33MB of information. The amount of energy needed to load each of the 12 web interfaces, along with each one's endless fragments of code, was approximately 30 watt-hours. According to their promotional materials, Amazon's business model is based on "obsessive customer focus", entailing "constantly listening to customers to enhance and improve the customer experience."[2] In other words, their business relies on continuously tracking and recording their customers' behaviour and activity to improve the monetisation of each user, and ultimately to increase Amazon's revenue. These processes are carried out by cookies and other supporting technologies embedded on websites, apps, videos, and other digital media formats. When a user visits a website, tracking software will automatically trigger the collection of all sorts of user data, which is now owned by the company that executes the tracking (e.g. Amazon, Google, Facebook, etc.)—and which has a legal right to exploit it.

The act of purchasing (for example a book on Amazon) has thus been turned into a tracking and monetization device, with the aim of adding layers to the already-complex setting of power relations online: including user profiling, social-sorting, task assignment, energy use and waste, and 'smoothening of liberal logi(sti)cs'.[3] Thus, the 8,724 pages of code that track and personalize a user's behaviour and experience—and that I involuntarily loaded through the browser—



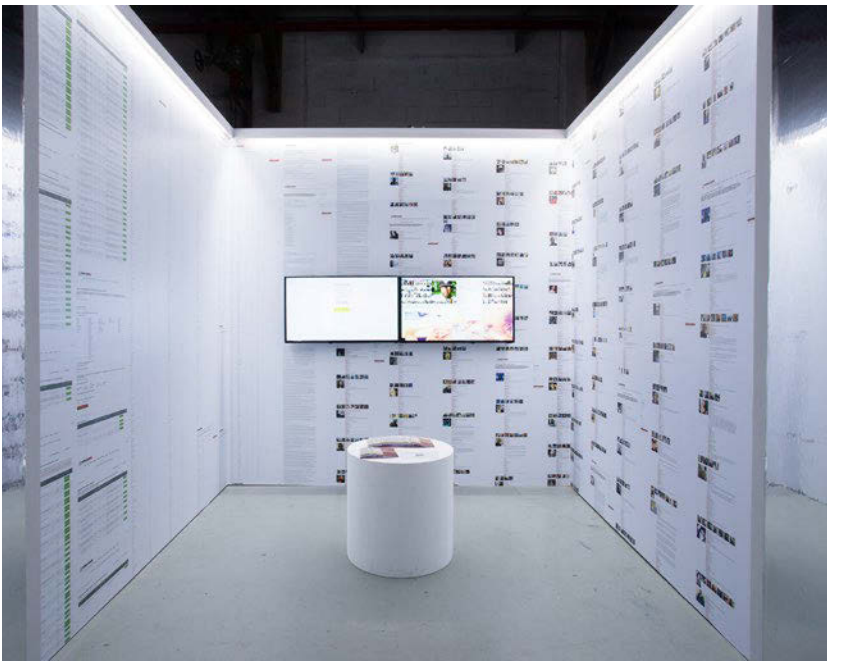
The Hidden Life of an Amazon User, Exhibition: BIG D@T@! BIG MON€Y! at HALLE 14—Zentrum für zeitgenössische Kunst / Centre for Contemporary Art, from 26.9. to 5.12.2020. Photography by Walther Le Kon.

are evidence of Amazon's core money-making machinery at work. "A machinery that sustains the patriarchal-colonial regime that determines how power is distributed along hands, territories and whole modes of existence at large"[4]. Moreover, this distributive operation implies that all the energy needed to load this relatively large amount of information was effectively demanded from the user, who ultimately assumed not just part of the economic cost of Amazon's hidden monetization processes, but also a portion of its environmental footprint.

All these aspects are drawn on in *The Hidden Life of an Amazon User,* an interactive artwork that details the intricate labyrinth of interfaces, code, and energy that make possible the purchase of Jeff Bezos's book—with the aim of casting light on Amazon's often unacknowledged but aggressive exploitation of their users, which is embedded at the core of the company's business strategies. Such strategies rely on apparently neutral, personalized user experiences afforded by attractive interfaces. These interfaces obfuscate the sophisticated business models embedded in endless pages of indecipherable code, all of which are activated

by the user's labour—again, clicking and scrolling—and hence based on a hidden mode of delegation. In turn, these strategies incur a significant energy cost, part of which is involuntarily assumed by the user. To put it bluntly, the user is not just exploited by means of their free labour, which allows these companies to collect and trade in massive amounts of user data, but the user is also forced to assume part of the energy costs of such exploitation.

The Dating Brokers (2018)[5]



The Dating Brokers, 2020 Digital Arts Festival-Taipei, 01.–15.10.2020. Photo courtesy of the author.

In May 2017, Tactical Tech and I bought 1 million user profiles from online dating pages for € 136. These profiles were acquired at USDate.org[6], a US-registered company that trades in online dating user profiles from around the world. The data package selected included photographs of each user (almost 5 million in total), username, email addresses, nationality, gender, age, and highly detailed personal information about sexual orientation, interests, profession, physical and personality traits of each user. The purchase of these profiles exposed an extensive network of interconnected companies which capitalized on all this information without the conscious consent of the users, who are ultimately the ones being exploited. This project was commissioned by Tactical Tech, a Berlin-based NGO with

a very specific focus on digital rights and data transparency. Tactical Tech and I collaborated on several projects before developing The Dating Brokers. In this specific case, the collaboration began in 2017. I had begun developing research for The Dating Brokers during 2016. During this time, Tactical Tech was developing research on the global industry of online dating and I was hired as an external consultant to advise them on data collection and processing issues. Later, Tactical Tech proposed commissioning The Dating Brokers. This commission was crucial to the project, not only on the financial side, but most importantly, on the legal side, as the project revealed sensitive user data and disclosed information that could harm a group of particularly powerful companies which could potentially take legal action against me. In that sense, Tactical Tech had the legal infrastructure to respond to potential legal claims.

The research before the formalization of the project lasted more than a year. The first step was to buy the profiles on USDate.org, a company that was advertised on Google and was very easy to access. We acquired 1 million worldwide user profiles. The data packet contained 630,426 male and 310,235 female profiles aged between 18 and 80 from 38 different countries. The buying process was exceptionally quick and easy. After making the payment through a PayPal account, I received several links to download the profiles. It was precisely this fluidity throughout the process that made me wonder why it was so easy to buy online dating profiles. I then began researching the business dynamics of the global online dating industry and I discovered that constantly exchanging profiles between different platforms was a very well-established practice in this industry. These practices fulfil the need to have a continuous flow of new faces to raise the chances of match-making between users and increase the number of paid subscriptions.

The next step in the research focused on finding the source of the profiles we had purchased. USDate.org declined to provide this information. I then applied different reverse engineering techniques, such as extracting metadata from the pictures in our dataset, looking at the data structure, and comparing it with that of profiles found in different dating sites. The result of this investigation generated irrefutable evidence that pointed to Plenty of Fish (POF). In 2017, POF was the second most used online dating service in the United States, just after Tinder, and according to the companies' public records, it had more than 150 million users and an average of 65,000 new subscriptions every day. But if POF and USDate.org were actively exploiting those profiles, who else could potentially do that? I found out that POF was part of an extensive conglomerate led by Match Group, the largest online dating services company in the world. In 2007, among many other companies, Match Group owned apps like Tinder and OkCupid. The user data policy of Match Group clearly stated that any user information belonging to any service affiliated with Match Group could be freely shared among each other. In other words, any profile created on any Match Group service, for example, in POF,

could potentially end up in Tinder and OkCupid. To expose this business practice, I drew a map that included all the companies affiliated with Match Group, and found more than 130 online services and apps that belonged to that company, which in turn, were potentially capitalizing on the profiles we had bought.

Sadly, that was just the tip of the iceberg. Match Group was itself a sister company of IAC, an American holding company that owns brands across 100 countries, mostly in digital media. Its very extensive portfolio of digital services includes Vimeo, Investopedia, The Daily Beast, or Daily Burn, among many others. In total, we could identify around 170 IAC-related companies and services. The company's privacy policy, just as in Match Group, stated that any user data created in any company affiliated with IAC could be shared with any of its services, including Match Group.

The network for utilizing data from dating profiles doesn't end with IAC and its brands—it extends much further, into countless third-party companies. Tracking users' online activity has become a major business model in the last decade. Put simply, online tracking is the act of collecting data from a user while they are interacting with a digital service, like reading the news or purchasing something online. Even though online tracking is an established practice within the digital economy, users are often not aware of the number of third-party companies that are keeping information on their online behaviour via trackers. Back then, we couldn't find any official document that listed the third-party companies with whom Match Group and IAC were sharing their users' information. However, during the investigation, we used some tools that allowed us to identify more than 300 third-party cookies linked to IAC and Match Group businesses that were potentially collecting all sorts of data on user behaviour. And this only accounted for desktop browser activity—it didn't even include trackers on mobile apps, which could potentially make the list of third parties twice as long.

Overall, we were able to map a network of more than 700 interconnected companies and online services that potentially utilised the 1 million profiles we bought from USDate. Nevertheless, we believed that there are many more undisclosed services that generate value from the dating profiles owned by Match Group. We also believed that the $0.57 average revenue per user that Match Group reported in their Q2 2018 Investor Presentation was just a fraction of the user profile's real value. This value was obfuscated by a complex web of other companies and services. This business ecosystem did not just affect the 1 million profiles we bought—this group of individuals was representative of everyone who has ever had a dating profile on one of the online dating services that are owned by companies such as Match Group. As seen in this analysis, the data collected, shared, traded, and sold on dating app's users travels far and wide and could potentially be instrumentalised by third-parties for advertising and individualised pricing, but also to restrict access to health insurance, credit, education and much more.

Tatiana Bazzichelli and Joana Moll at *Activation: Collective Strategies to Expose Injustice*, Disruption Network Lab, November 30, 2019, Kunstquartier Bethanien Berlin. Photo by Maria Silvano.

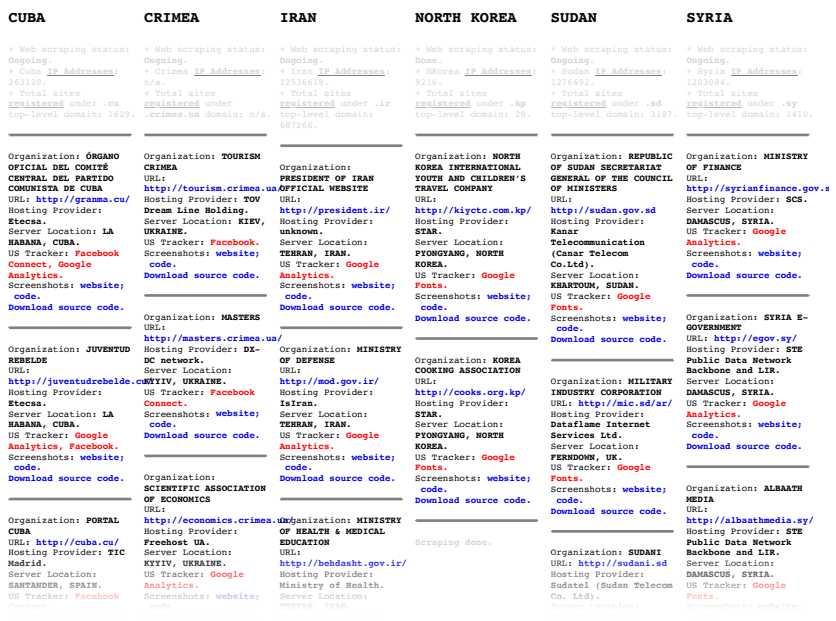
The investigation produced extensive evidence and the task of coherently and ethically reflecting it in a single artwork was quite complicated. For this reason, I decided to divide the project into two formats: an artwork that sought to provoke an emotional reaction towards the wild transaction of intimacies within the global online dating ecosystem, and an interactive report that would disclose the evidence produced and explain the investigation process.

Managing the amount of data that had been generated during the project was also a complicated task. To me, it was of utmost importance to anonymize any information that could lead to the identification of any of the profiles that we purchased. Due to the technical complexity of this operation, I collaborated with Ramin Soleymani, a computer engineer who developed software to anonymize photographs and texts. This collaboration was crucial to the project, for if this anonymization had not been possible, I wouldn't have made the project public.

The project enjoyed international attention. Since its publication in November 2018, the project has been exhibited in centres such as Ars Electronica, Fotomuseum Winterthur, and Photograpers' Gallery. Media such as *The Financial Times*, *O'Globo* and *la Repubblica*, among others, also mentioned the piece. The Dating Brokers was the first published project to disclose extensive research on the commercialization of data dynamics within the global online dating industry.

A few days after publishing the project, Match Group contacted Tactical Tech and asked us to remove certain pieces of evidence. We declined the petition as Match Group refused to comment on any of it.

Algorithms Allowed (2017) [7]



CUBA

+ Web scraping status: Ongoing.
+ Cuba IP Addresses: 263120.
+ Total sites registered under .cu top-level domain: 1629.

Organization: **ÓRGANO OFICIAL DEL COMITÉ CENTRAL DEL PARTIDO COMUNISTA DE CUBA**
URL: **http://granma.cu/**
Hosting Provider: **Etecsa.**
Server Location: **LA HABANA, CUBA.**
US Tracker: **Facebook Connect, Google Analytics.**
Screenshots: **website; code.**
Download source code.

Organization: **JUVENTUD REBELDE**
URL: **http://juventudrebelde.cu**
Hosting Provider: **Etecsa.**
Server Location: **LA HABANA, CUBA.**
US Tracker: **Google Analytics, Facebook.**
Screenshots: **website; code.**
Download source code.

Organization: **PORTAL CUBA**
URL: **http://cuba.cu/**
Hosting Provider: **TIC Madrid.**
Server Location: **SANTANDER, SPAIN.**
US Tracker: **Facebook Connect**

CRIMEA

+ Web scraping status: Ongoing.
+ Crimea IP Addresses: n/a.
+ Total sites registered under .crimea.ua domain: n/a.

Organization: **TOURISM CRIMEA**
URL: **http://tourism.crimea.ua/**
Hosting Provider: **TOV Dream Line Holding.**
Server Location: **KIEV, UKRAINE.**
US Tracker: **Facebook.**
Screenshots: **website; code.**
Download source code.

Organization: **MASTERS**
URL: **http://masters.crimea.ua/**
Hosting Provider: **DX-DC network.**
Server Location: **KYYIV, UKRAINE.**
US Tracker: **Facebook Connect.**
Screenshots: **website; code.**
Download source code.

Organization: **SCIENTIFIC ASSOCIATION OF ECONOMICS**
URL: **http://economics.crimea.ua/**
Hosting Provider: **Freehost UA.**
Server Location: **KYYIV, UKRAINE.**
US Tracker: **Google Analytics.**
Screenshots: **website; code.**

IRAN

+ Web scraping status: Ongoing.
+ Iran IP Addresses: 12536618.
+ Total sites registered under .ir top-level domain: 687266.

Organization: **PRESIDENT OF IRAN OFFICIAL WEBSITE**
URL: **http://president.ir/**
Hosting Provider: **unknown.**
Server Location: **TEHRAN, IRAN.**
US Tracker: **Google Analytics.**
Screenshots: **website; code.**
Download source code.

Organization: **MINISTRY OF DEFENSE**
URL: **http://mod.gov.ir/**
Hosting Provider: **Iran.**
Server Location: **TEHRAN, IRAN.**
US Tracker: **Google Analytics.**
Screenshots: **website; code.**
Download source code.

Organization: **MINISTRY OF HEALTH & MEDICAL EDUCATION**
URL: **http://behdasht.gov.ir/**
Hosting Provider: Ministry of Health.
Server Location:

NORTH KOREA

+ Web scraping status: Done.
+ NKorea IP Addresses: 9216.
+ Total sites registered under .kp top-level domain: 28.

Organization: **NORTH KOREA INTERNATIONAL YOUTH AND CHILDREN'S TRAVEL COMPANY**
URL: **http://kiyctc.com.kp/**
Hosting Provider: **STAR.**
Server Location: **PYONGYANG, NORTH KOREA.**
US Tracker: **Google Fonts.**
Screenshots: **website; code.**
Download source code.

Organization: **KOREA COOKING ASSOCIATION**
URL: **http://cooks.org.kp/**
Hosting Provider: **STAR.**
Server Location: **PYONGYANG, NORTH KOREA.**
US Tracker: **Google Fonts.**
Screenshots: **website; code.**
Download source code.

Scraping done.

SUDAN

+ Web scraping status: Ongoing.
+ Sudan IP Addresses: 1276692.
+ Total sites registered under .sd top-level domain: 3187.

Organization: **REPUBLIC OF SUDAN SECRETARIAT GENERAL OF THE COUNCIL OF MINISTERS**
URL: **http://sudan.gov.sd**
Hosting Provider: **Kanar Telecommunication (Canar Telecom Co.Ltd).**
Server Location: **KHARTOUM, SUDAN.**
US Tracker: **Google Fonts.**
Screenshots: **website; code.**
Download source code.

Organization: **MILITARY INDUSTRY CORPORATION**
URL: **http://mic.sd/ar/**
Hosting Provider: **Dataflame Internet Services Ltd.**
Server Location: **FERNDOWN, UK.**
US Tracker: **Google Fonts.**
Screenshots: **website; code.**
Download source code.

Organization: **SUDANI**
URL: **http://sudani.sd**
Hosting Provider: **Sudatel (Sudan Telecom Co. Ltd).**

SYRIA

+ Web scraping status: Ongoing.
+ Syria IP Addresses: 1203084.
+ Total sites registered under .sy top-level domain: 1410.

Organization: **MINISTRY OF FINANCE**
URL: **http://syrianfinance.gov.s**
Hosting Provider: **SCS.**
Server Location: **DAMASCUS, SYRIA.**
US Tracker: **Google Analytics.**
Screenshots: **website; code.**
Download source code.

Organization: **SYRIA E-GOVERNMENT**
URL: **http://egov.sy/**
Hosting Provider: **STE Public Data Network Backbone and LIR.**
Server Location: **DAMASCUS, SYRIA.**
US Tracker: **Google Analytics.**
Screenshots: **website; code.**
Download source code.

Organization: **ALBAATH MEDIA**
URL: **http://albaathmedia.sy/**
Hosting Provider: **STE Public Data Network Backbone and LIR.**
Server Location: **DAMASCUS, SYRIA.**
US Tracker: **Google Fonts.**

Algorithms Allowed. Photo courtesy of the author.

Algorithms Allowed was developed as part of the web residency program—"Blowing the Whistle, Questioning Evidence"—curated by Tatiana Bazzichelli for the Akademie Schloss Solitude and ZKM Center for Art and Media in 2017[8].

Earlier that year, I was invited to participate in an online exhibition where artists were asked to come up with unconventional objects to be sold on eBay. My first idea was to sell Google Analytics (GA) cookies found within a North Korean website. I was quite sure that I wouldn't find any, but to my surprise, I could identify GA within the first website I visited: The official webpage of the DPR of Korea[9].

Cookies and other tracking technologies are generally embedded in the source code of a website. Thus, by "simply" looking at the code that builds any site, cookies, and the companies that own them, are "easily" identifiable. For the eBay exhibition, I accessed the source code of "The official webpage of the DPR of Korea", looked for the GA code, and copied and paste it into a .txt file. Afterward I created an auction page to sell the .txt file named "Google Trackers in North Korea Official Page".

Interestingly, once I submitted the auction, I automatically received a warning message (embedded within an orange frame) from eBay preventing me from publishing the auction, as eBay's policy forbade the selling of items that originated from North Korea due to the sanctions enforced by the US Department of the

Treasury's Office of Foreign Assets Control (OFAC). The company also threatened to remove the item and prohibit me from using their services any longer if I violated this policy. Nevertheless, I decided to insist, and this time the message was framed in a strong red and directly forbid me to sell the item.

In 2017, the US was currently enforcing embargoes and sanctions against Cuba, Iran, North Korea, Sudan, Syria, and the Ukrainian region of Crimea. Thus, all transactions carried out with these countries, including software and data, were prohibited and heavily sanctioned by the US government. Nevertheless, I found Google trackers and other online services such as Google Fonts, Facebook connect and other tracking technologies mostly owned by American IT giants, within several websites owned by countries under US embargo. The list of websites included the official website of the President of Iran, the Syrian e-government, and the official website of the Cuban Communist Party, among hundreds of others. It is important to remember that these websites are stored inside hard disks placed in physical territories. Thus, these companies were violating the same policy that eBay accused me of. Ultimately, *Algorithms Allowed* sought to produce evidence to reveal an incredibly absurd but highly problematic legal grey area, and thereby expose the ambiguous relationship between code, public policy, geopolitics, economics, and power in the age of algorithmic governance.

Conclusion

I believe that one of the main differences between "traditional" acts of whistleblowing and whistleblowing by means of artistic practice resides in the fact that the evidence is portrayed by an artwork, not by a citizen or a group of citizens (with whom we can easily empathise and deeply engage with the cause they are publicly denouncing). Thus, the aesthetic representation of evidence within an artwork, which ultimately will expose and interrogate wrongdoing along with its multilayered consequences, is a particularly critical phase as it implies a great deal of responsibility. I believe that art practice has the ability to do just that: to transcend the story and activate experience by allowing for the arrangement of different pieces of evidence across multidimensional layers. I believe that *The Hidden Life of an Amazon User* represents this idea best: the project discloses the multiple material costs of a simple purchase at Amazon.com by exposing the several interfaces, code, and energy involved in this process, resulting in 15 minutes of a continuous scroll. Such an arrangement seeks to force the user to spend a substantial amount of time, energy, and attention (in comparison to what would usually be spent when buying at Amazon, which in this case was roughly 3 minutes) throughout the different vectors that make a regular shopping trip to Amazon possible, and thus experience Amazon's online purchase process energy-intensive machin-

ery in the flesh: the fingers get tired, the attention deflates, forcing the body to be aware and present, or in other words, turning the usually passive role of the body (when it interacts with a screen) into an active entity capable of experiencing the physical dimension of digital interaction.

Honestly, I haven't thought about or followed Kentridge's work for many years, nor have I considered him a crucial reference in my work, so it came as a surprise when his name promptly popped up in my mind when I was asked to write about my work and the relationship relationship between art practice and whistleblowing. However, I believe that as much as our practices are extremely unrelated, they greatly converge in the act of going beyond storytelling and intentionally affecting the body. From my perspective, Kentridge's success in exposing the deep political and social anxieties caused by the Apartheid relies on the strength of his hand drawing, the presence of his body. Similarly, I believe that the most successful projects I've developed are the ones that expose misconduct and actively include the body as a mechanism to understand the consequences of wrongdoing in a "disembodied" ecosystem such as the digital. In that sense, far from being meaningless, drawing and sculpting as an art student played a fundamental part in shaping the role of the body throughout my practice. Funnily, when I was writing one of the early versions of this text, I discovered that Kentridge and I were born on the same day.

Notes

1. Moll, Joana, *The Hidden Life of an Amazon User*, November 11, 2019, accessed April 28, 2021, https://janavirgin.com/AMZ.
2. Premack, Rachel, "Jeff Bezos Said the 'secret Sauce' to Amazon's Success Is an 'Obsessive Compulsive Focus' on Customer over Competitor", *Insider*, accessed June 5, 2019, *https://www.insider.com/amazon-jeff-bezos-success-customer-obsession-2018-9*.
3. Moll, Joana, and Jara Rocha, "Tilt the Scroll to Repair: Efficient Inhuman Workforce at Global Chains of Care." *Digital Work in the Planetary Market*, (Cambridge: MIT Press, September 1, 2021).
4. Ibid.
5. Moll, Joana, *The Dating Brokers*, November 1, 2018, accessed April 28, 2021, https://datadating.tacticaltech.org.
6. "Start Online Home Business. Buy Dating Profiles, Dating Profiles for Sale | General Dating Industry Support Services LLC", *USDate*, accessed May 25, 2021, https://www.usdate.org.
7. Moll, Joana, *Algorithms Allowed*, May 1, 2017, accessed April 28, 2021, http://www.janavirgin.com/ALGORITHMS_ALLOWED.
8. "Web Residencies by Akademie Schloss Solitude & ZKM 2017–2020", *Web Residencies by Akademie Schloss Solitude & ZKM 2017–2020*, accessed May 25, 2021, webresidencies-solitude-zkm.com.
9. "Democratic People's Republic of Korea", *Korea-Dpr.com*, accessed May 25, 2021, korea-dpr.com.

DENIS "JAROMIL" ROIO

Photo by Riccardo Bernardi

Denis Roio, better known by his nickname Jaromil, is the founder of Dyne.org and the Chief Technology Officer (CTO) of the DECODE EU flagship project on technological sovereignty and data ownership, involving pilots in co-operation with the municipalities of Barcelona and Amsterdam. Jaromil published his PhD on Algorithmic Sovereignty (AlgoSov.org) and received the Vilém Flusser Award at transmediale (Berlin, 2009) while leading the R&D department of the Netherlands Media Art Institute (Montevideo/TBA) for six years. He has been a fellow of the "40 under 40" European Young Leaders programme since 2012, and was listed in the "Purpose Economy" list of the top 100 social entrepreneurs in the EU in 2014.

DENIS "JAROMIL" ROIO

HACKER ETHICS IN 2021

INTERVIEW BY TATIANA BAZZICHELLI

This interview was conducted on May 19, 2021.

Tatiana Bazzichelli: This anthology reflects on how whistleblowing contributes to shaping change, new courses of action and digital tools among communities of activists, hackers, artists, and researchers engaging with participatory technologies and networks. To what extent is whistleblowing a source of inspiration to you and the free and open-source software networks you belong to?

Denis "Jaromil" Roio: When I think of whistleblowing and free software, an image comes to my mind. It's a photo of Julian Assange with Richard Stallman, holding a picture of Edward Snowden. It was taken at the Ecuadorian Embassy during Assange's period in there, when Stallman visited him.

Photo courtesy of Richard Stallman.

It's a photo of one of the most prominent whistleblowers, co-founder of WikiLeaks, together with a prominent free software activist holding the picture of another whistleblower. The photo depicts three people, including the one in the picture, who will be remembered in history: Assange, Stallman and Snowden.

This point of connection between whistleblowing efforts denouncing corruption within the system and free software is difficult to spot if we don't look at the context in which it is grafted. I believe this to be "corporate culture." Whether it is in public or private, corporate culture has built systems that are collective and that grow in complexity, to the point that corruption can be hidden, or even functional, to the scope of its mission. We live in a world that is dominated, regulated, or governed by only few corporations, national states, and their institutions, together with even bigger oligopolies; such organisations are guided by forms of collective agency coordinated through advanced methods of working together and organising work. Whistleblowers are individuals within these organisations that raise a flag and "blow the whistle" because of a particular ethical sense that something isn't right and should be observed and respected, and that it has essentially been suppressed by collective agency.

Whistleblowing is an individual act against a collective corruption—the corruption of a collective place—and it has many similarities with foundational events of the free software movement. If you look back at the history of many Unix free and open-source software— Unix variants like Linux, or BSD—they opposed the adoption of proprietary software built by corporations, because they contained bugs that were hidden from the users. They gave errors that were hiding away problems from users, like the blue screen of death that we saw on Windows, reporting numbers that can only be interpreted by the software creators; one had a hard time figuring out what was happening in his or her own computer. This led to a situation where responsible software developers and engineers "blew the whistle" declaring unethical to hide code running on people's computers. These acts of constructive rebellion have worked better than money in motivating developers to rewrite entire operating systems.

Ethical objection and constructive rebellion is a point of contact between these two phenomena, and we can see the positive impact of free software today. Free and open-source software has changed the very corporations that it fought, because many of the operating systems that we run today have in one way or another inherited characteristics of the ethos of free and open-source software. Nowadays, we have an increasing transparency in various degrees in the operating systems that we use. In most cases free software projects were born from isolated efforts that sought to oppose the status quo in a creative way, showing that something else was possible. But there is a common pitfall in this way of action which is common to movements motivated by ethical objection: organisational capacity to make project scale and be sustainable. Somehow, we all have to learn from the

systems we want to improve, as corporations have demonstrated much better capacity in organising collective, establish workflows and arguably in some cases establish a fair governance.

My source of inspiration as a software developer and a user of operating systems was the rebel, the genius, and the "messianic figure" of Richard Stallman, who denounced corruption within institutional apparatuses as much as Julian Assange. Over the years, I have had the opportunity to look within corporate processes, and I have realised that the collective effort—the effort to collectively find solutions from within systems—is also a source of inspiration. Because I don't think a messiah can save a society, no matter how good he or she can be, what matters is a collective vision that can be shared and understood by everyone involved.

TB: In the context of whistleblowing, one important challenge is how to make classified information, which is in the public interest, available—while also considering security and privacy when opening up potentially sensitive data. Do you think it is possible to preserve openness when dealing with leaks of large datasets?

DJR: We have seen incredible advancements in the field of cryptography over the past ten years, and technical solutions that can be used for a variety of things. Zero-knowledge proof technologies, and multi-party computation techniques that can be adopted in order to reach more transparency in processes while granting the privacy of the participants. This is important to say, because the hype around crypto projects has steered most discussions around the tokenisation of value, ending up creating financial markets—something that we do not need to grow more than what we have today. We still need to divulge most of the opportunities offered by cryptographic advancements today, outside of toxic financial hypes. There is much more to be done to make processes of transparency and accountability more agile while preserving privacy. We need methods to practice good, balanced governance and oversight that is not biased by knowledge of private details. Much of my work as a developer and scientist over the past ten years has been dedicated to making these opportunities known and usable to the public. Last, but not least, is the paper I recently published in pre-print: "Reflow: Zero Knowledge Multi Party Signatures with Application to Distributed Authentication" (May 2021).[1]

TB: To explain it technically, is it possible to apply the zero-proof technology to large data sets and guarantee openness, as well as security and privacy for classified information?

DJR: The point is to make the origin of certain data traceable when it is needed, and to make the data analysable without this information being disclosed all the time. The principle is well known in the intelligence community as "need to know." We don't need a reviewer to know all private details, but we do need a reviewer to analyse the larger picture and spot patterns of deviance. Often, data about the participants and subjects of this analysis is embedded or linked univocally to it,

but this is not always necessary. Zero-knowledge proof in general is a very flexible field of cryptography that can be adapted to many use-cases.
For instance, one can be sure of the possession of an ID of someone without knowing the ID. We can follow traces contextually, and within a certain context we can be sure that the trace is that of the same person, or of a subject that operates in a network. The boundary of privacy and disclosure is context. Here I recall the formulations that Professor of Information Science Helen Nissenbaum named "Contextual Integrity": principles that help us understand how confidentiality and integrity can affect context and should affect the subjects operating within a context.

TB: Hackers have long been challenging power dynamics and generating criticism of closed systems. If we reached a more just society, we would not need acts of whistleblowing. How do you think hacker communities could contribute to supporting whistleblowers technically and socially in order to make their work more effective?

DJR: I believe that hackers can help by assisting investigative journalists; people trained within a profession that has held this role in society for a long time. Of course, there is a similarity between investigative journalists, hackers, and investigators in general: they are all liminal subjects. If we see societies as "semiospheres", following the theories by Professor Yuri Lotman, then we have cells whose osmotic membrane are such liminal roles that allow the information to penetrate within the society, be understood, be "digested." Hackers, journalists, investigators, cultural mediators and maybe more future liminal roles have the responsibility to share information that can be useful to nurture society, as well to keep out what is not useful or dangerous. This is a delicate process. We can hardly think of societies that are made knowledgeable of every single event that happens in the world; even when declared, global knowledge is a myth; "freedom of information" is a delicate cultural process. Hackers have been often arrogant in thinking that they can steer this process alone. Many of us have already understood that interdisciplinarity is necessary. Therefore, I think that hackers can help by interfacing themselves with the expertise of other disciplines.

When interacting with diverse aspects of society we should value more diversity in disciplines, for instance it is detrimental to many societies that studies in humanities are losing ground to scientific education, a trend driven by market demand of technicians.

Hackers: better be humble! The many I know, after the "rock star moment" of the early 2000s, are aware of this, and so will be able to contribute to society even more. Not to belittle what has been done by the "stars" so far—some had an important role as change agents—but there must also be ways to communicate with society and not end up being alienated by it. We need to be hybrids, and to learn how to share our knowledge and talents with others.

TB: Could you describe some collective initiatives pushing for transparency and social justice, that could be a source of inspiration in the creation of distributed methods of knowledge awareness?

DJR: I have had the luck of an unconventional life, which also included being a squatter in Europe. I have been living off very few resources for long periods, also in more than a few difficult contexts, but what made always the difference was the collective around me: our agency and the power to shape our society and the city around us. As squatters, we were serving the purpose of most vulnerable people, the people left on the wrong side of capitalism. By squatting, I learned that in Italy, the Netherlands, Germany and other places in Europe there is a heritage of resisting through collective solidarity in direct response to rising levels of poverty. Entire families organised to occupy abandoned buildings, to build their lives in there, or activists taking the initiative of cleaning and repairing abandoned places and organising the best social initiatives for cultural and anti-mafia agendas. One large motivation was reclaiming our time by not working as an employee under a boss, always in need of money to buy back our time. Another motivation was collectively envisioning how the texture of the city could be improved by repopulating it with people, rather than letting it be shaped by the dynamics of financial speculation, which mostly serve the interests of those who accumulate more assets, money, and space. Because of these factors, it was especially important to investigate the reason behind the abandonment.

In Amsterdam, I learned how to investigate and use background information about abandoned buildings, collectively organised in a "parallel cadastre" called "Speculanten Onderzoek", a research centre on speculation in the city. Many buildings we knew of were bought and then left abandoned by financial speculators, undeveloped assets that, when left empty, rapidly turn into scars through the living texture of a city. Across Europe, there are entire buildings owned by people who have perhaps never stepped into them, just to park their financial capital. Those of us who investigated this sort of speculation did not only contribute to make our cities a better place: we stood up as a grassroots movement against speculation, corruption and even mafia organisations.

TB: In our conversation at the 2020 Logan Symposium you mentioned how social movements in Italy and in the Netherlands challenged city policy on financial speculation and hidden illicit cash flows. How can we create agency through collectivising data controlled by financial and institutional powers?

DJR: The way to make this possible is the de-penalisation of collective, researched and well-motivated conversion of private property in common and public space. Financial markets, and in general the financial world, have become a completely abstract and detached world of non-existing processes that simply underpin numbers and values: the very processes of production are no longer linked to the abstract representation operated by financial markets.

Researchers like David Hakken and Christian Marazzi have written at length about this. When the production dynamics no longer match their financial representations, there is a huge imbalance between the capacity to buy and sell physical objects, and their real use. In Marxian terms: the use value is not aligned with the exchange value, nor economists are taking care to better define the so called "externalities" that should serve as indicators for the evaluation of use value. At this point, it does not make sense for regulations to protect only—and even violently—a concept of property based exclusively on exchange value. When the Netherlands was still a social democracy such a depenalisation clause was in place to allow occupants to go through a civil case, so that we could explain our reasons, present our collective plan: this approach made many things possible at zero budget, arguably producing more opportunities of development than a subsidized institution can ever provide. Today, I regret seeing only a few squatted social centres left in Europe, and I regret seeing many well-meaning occupants repressed with disproportionate force and violence, forced to marginalisation and "forced to bleed", to quote our common friend and cultural agitator, writer and editor Marco Philopat.

TB: You have been working for many years in the framework of Dyne.org on AI and inclusion, to influence policy making through pilot projects in Amsterdam and Barcelona. What have you achieved in this sector so far and what more needs to be done?

DJR: I am critical about the adoption of artificial intelligence. There is an urgent need for our societies to reclaim knowledge and control of algorithms—especially AI ones used for mass surveillance and societal control. We have done our best to explain this by analysing the Dutch context in which AI is deployed by law enforcement.[2]

From a philosophical standing point, I think it is particularly important to consider that AI can fail in their decisions and doing so, when given too much power over people, can commit crimes. Then we should not ask ourselves if AI have standing, but primarily how to deal with victims in the living world. In the future, there will be a growing number of victims of AI crime. I did my best to document what happened after the assassination of Jean Charles De Menezes back in 2005, and tried to inspire solutions in the direction of restorative justice for AI crimes.[3] I'm very happy that just recently the European Commission has released guidelines for ethics in AI, and I think they should be read by anyone working in the field, including our friends on the other side of the Atlantic.[4]

TB: It is crucial to establish and develop new policies in the technological sector to create a real change. For that scope we need an intersectionality of expertise, where the technical meets the social and the political. Could you give us some examples from your experience working on blockchain technologies and data ownership at DECODE EU?

DJR: The research we conducted at DECODE became the understated consciousness that technocracy is a growing power that needs to be limited, complemented with the collective understanding of what technology does. We worked hard to make people understand what is being done with their data. We did not want participants to become technicians and learn to code, but we wanted code to be closer to human language and be easily understood by participants without technical training.

What I am proposing here is an inversion of vision. I propose we stop working to make machines understand and interpret human agency through very complex and often non-deterministic processes. I propose we work so that humans can better understand what machines do for them through the development of technologies that are verifiable and deterministic. Today, most technologists work so that machines can perceive humans, their sentiments and expressions; I argue that we need technologies that can be perceived better by us humans.

This vision lead us to develop the Zencode language and its secure execution environment the Zenroom VM, which turned out to be remarkable—overwhelming at times—technical achievement for the DECODE project.[5] This free and open-source software is easy to embed in any application to manipulate, authenticate and encrypt data in less than 2MB of memory: anyone can use a simple human-like language to describe actions to be done on data structures, including very advanced functions like zero-knowledge proof, multi-party computation and homomorphic math. Fairly complex actions to be executed by machines (even on small chips) can be described this way, to execute anything like business logic, data analysis, and end-to-end encryption communication. The important thing is that the code executed can be easily reviewed also by non-technical people.

We did this because of the advent of GDPR regulations. In Europe, we needed and wanted a greater defence of our privacy from the sort of data extraction operated by multinational corporations. The GDPR raised the liability on service providers (including online communities) to define responsibilities for private data manipulation and storage: liability embodied in the role of the "data protection officer" (DPO). But in most cases the DPO is a person with a background in law, lacking the engineering knowledge required to review the technical processes applied to data, creating a situation in which needs and liabilities propagate through an organisation as an entire engineering team becomes necessary to interpret code for the DPO to understand and review. With Zencode, a language that can be shown even to final users, anyone can have the ability to check what is being done with her or his data. In Amsterdam we used this system to design a way for young people to buy beer at the counter of a pub without showing their ID, but with a zero-knowledge proof credential.

This was done using cheap and inexpensive free and open-source hardware—a Raspberry Pi connected to a scanner and RFID scanned passports, a totally open-source framework—to produce a credential that could be used on a mobile phone or printed on paper as a QR code to show proof of age. We also used this in Barcelona to power petition signatures for the rights to the city in collaboration with the amazing democratic platform Decidim.

All this work allowed us to streamline development processes while keeping them transparent to ourselves and our colleagues despite the growing complexity. Today, still, very few people understand the difference between symmetric and asymmetric keypair cryptography. Only a few of us have managed to learn how to use PGP. While trying to make people navigate the complexity of cryptography, I think that we should also try harder to make this technology simpler, more usable, intelligible—and hackable! Especially as it is free and open-source.

TB: The main challenge of social change lies in the invention and production of new courses of action and intervention, both on and offline. You mentioned, on various occasions, the role played by WikiLeaks in inspiring the blockchain communities to develop new distributed and privacy-oriented transaction technologies. Could you tell us more about this early phase of blockchain development, and what is important to consider for preserving these initial goals?

DJR: This happened in 2011, at the time of the financial blockade of WikiLeaks. I'm talking about the time when WikiLeaks was becoming very popular on the trail of the 2007 Baghdad airstrike, when footage from *Reuters* journalists on a US Army Apache helicopter, known as the *Collateral Murder* video, was leaked by Chelsea Manning to WikiLeaks. Back then, following the bashing of WikiLeaks by conservative US politicians and without any court mandate, Visa and Mastercard closed the possibility of receiving donations to WikiLeaks. In the eyes of many of us, this was a breach of the normal course of law; an act of aggression against an organisation trying to eradicate corruption from the military-industrial complex. Many hackers who supported WikiLeaks thought that it was a good idea to step out of Visa and Mastercard networks, to not trust them as neutral anymore, and to adopt cryptography for the radical decentralization of networks, to make possible flows of values. The financial blockade of WikiLeaks was in February 2011, and right after we saw an increase in the mining and exchange of Bitcoins. This was a moment of rupture; a rupture that was generative, as much as it was destructive.

At that time, Bitcoins were less than $1. That was the moment in time, the rupture in history that brought Bitcoin to fame. It is hard to believe today, and difficult to remember for most people, because no one paid attention to Bitcoin until it surged to fame a few years later. I guess this part of history is relevant for understanding how ethics are transformed and value is created in society, what motivated me to write "Bitcoin, the end of the Taboo on Money" (April 2013).[6]

Today, we can tell that the Bitcoin experiment itself became an instrument of the financial sector, and a tool for deregulation: the crypto world became an acceleration of the financial sector itself, which is the industrial oligopoly it posed to destroy in the first place. What became of this hype was almost completely derailed from its initial ethos: it did not liberate WikiLeaks from its role, nor from its own biggest enemy; it only marginally allowed more organizations like WikiLeaks to thrive off peoples' donations.

TB: Whistleblowing is heavily persecuted in many countries and is often treated as an act of treason. How could we politically contribute to making the work of whistleblowers more accepted in society?

DJR: To make whistleblowers more accepted by society, we need society to be more accepted by whistleblowers. Let us look at the individual dimension of the actions of a whistleblower: it is an individual act of responsibility as much as a desperate act that cuts ties with the context it is denouncing. It is sometimes a romantic dream, that the system around one whistleblower may recognise the value of the effort, but I argue that, in most cases, antagonizing a system we are part of is not the best way to improve it.

We have seen what has been inflicted on the minds, souls and bodies of those who have had the courage to stand up to what are clearly huge injustices and huge discriminations and huge corruptions in human history. Throughout history, we have burned people in the middle of squares, tortured them and imprisoned them for years without trial.

When I say that whistleblowers need to accept society, I do not mean that corruption should be accepted. What I am trying to say, is that we need to stop accepting that sacrifice is the only way to do this. I would like to imagine a world in which, to quote Tina Turner, "we don't need another hero": we do not need sacrifice to denounce corruption. We do not need to mourn a loss, or to amend deep wounds, to say that something was wrong; that a collective system became unjust, deviant and corrupt. In some cases, we can assume that an organisation has degenerated into corruption despite the well-meaning intentions of its agents, who became unable to spot their own mistakes and their damaging effects. I believe that we all need to make an effort to be ethical participants of society, and to inspire others to do so. We need to understand society, to see if there are ways to improve it, and look for collectives (not a single hero, messiah or hacker) that can take up this challenge, understand the urgency and act.

Notes

1. Roio, Denis, Alberto Ibrisevic, Andrea D'Intino, "Reflow: Zero Knowledge Multi Party Signatures with Application to Distributed Authentication", May 2021, https://arxiv.org/abs/2105.14527.
2. Roio, Denis, "The Algorithmic Sovereign", *Amsterdam Alternative*, January 17, 2020, https://amsterdamalternative.nl/articles/8920.
3. Bianchi, Amos, and Denis Roio, "Frames from the life and death of Jean Charles de Menezes", 2010, *jaromil.dyne.org*, https://jaromil.dyne.org/journal/three_frames_de_menezes.pdf; Adnan Hadzi and Denis Roio, "Restorative Justice in Artificial Intelligence Crimes", *Spheres*, November 20, 2019, https://spheres-journal.org/contribution/restorative-justice-in-artificial-intelligence-crimes.
4. "Ethics guidelines for trustworthy AI", accessed July 5, 2021, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.
5. Zenroom, accessed July 5, 2021, https://dev.zenroom.org/ and https://zenroom.org/; *DECODE*, accessed July 5 2021, https://decodeproject.eu.
6. Roio, Denis, "Bitcoin, the end of the Taboo on Money", *jaromil.dyne.org*, April 6, 2013, https://files.dyne.org/readers/Bitcoin_end_of_taboo_on_money.pdf.