

SEEING STONES AND
SPACES BEYOND THE
VALLEY

03.06. BNN
17.07. WWA

Infrastructure, Algorithms, and the Future

BARTOSZ FRĄCKOWIAK

Translated from Polish by Dominika Gajewska

One should never tell anyone anything or give information or pass on stories or make people remember beings who have never existed or trodden the earth or traversed the world, or who, having done so, are now almost safe in uncertain, one-eyed oblivion. Telling is almost always done as a gift, even when the story contains and injects some poison, it is also a bond, a granting of trust, and rare is the trust or confidence that is not sooner or later betrayed, rare is the close bond that does not grow twisted or knotted and, in the end, become so tangled that a razor or knife is needed to cut it.

¹Javier Marias, *Your Face Tomorrow*

The war in Ukraine has put the relationship between technology, infrastructure and geopolitics into stark relief. Russia's attempts to cut its citizens off from the World Wide Web demonstrate that in its present form the Internet is not independent from local conditions, whether political or geographic. Counterintuitive experiments with creating a national internet make digital boundaries dependent on state boundaries, tethering digital territories to physical ones. The web is not as homogeneous and seamless as we tend to think, but has "walls," concavities, nodes, and a geometry² strictly bound up with physical geography, politics, and global power structures. This nexus of technology and geopolitics is most clearly seen in the material infrastructure of the Internet which we often forget about or are ignorant of, and whose existence is obscured *inter alia* by the special language we use to talk about various technologies.

The language we employ to describe new technologies tends to emphasize their lightness, swiftness, and ephemeral and non-material nature. We talk about the cloud and imagine scattered molecules of data, without weight or physical mass, ungraspable, floating nimbly in the air. Meanwhile the Internet, the cloud, or what allows us to experience technologies as "light," "swift," and mobile is in reality supported by a tangible backbone of material infrastructure. Starting with small

1 J. Marias, *Your Face Tomorrow*, Vol. 1 Fever and Spear, transl. Margaret Jull Costa, New Directions, New York 2014.

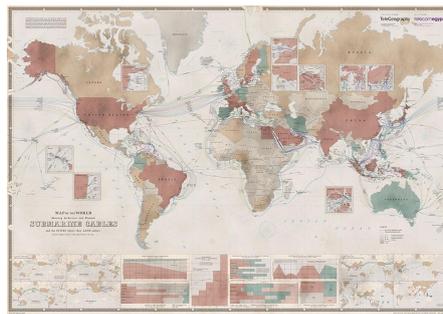
2 See: L. Drulhe, *Critical Atlas of Internet. Spatial analysis as a tool for socio-political purposes*, <https://louisdrulhe.fr/internet-atlas/> [accessed: 20.04.2022].

home routers, through the cables that connect them to the larger web structures managed by Internet service providers (ISPs) such as server farms and data processing centers, to Internet exchange points (IXPs), where the signals from different providers come together, all the way down to the backbone of the entire network – the large cable and optical fiber structures running along the ocean floor and traversing entire continents, transmitting binary sequences that code all the information from our world.

1. The data are not in a cloud but at the bottom of the ocean³

Around 95% of the global Internet currently travels along the bottom of seas and oceans. Some 400 submarine optical fiber cables connect different locations around the world, enabling faster information transfer between some of them, while disconnecting others (like Cuba) from the global exchange of knowledge and digital services and products. Some of the cables are several dozen kilometers long, others – like those running across the Pacific – span thousands of kilometers. They have to withstand powerful sea currents, submarine landslides, and the activity of large fishing trawlers. Their installation requires hard physical labor on the part of workers in factories and on ships.

An analysis of the nodes and connections created as part of this web sheds light on the planetary structures of power and exclusion and gives us insight into the relations between centers and peripheries as well as geopolitical conflicts and co-dependencies. A dense network of cables connects the United States with Europe, allowing for rapid and intensive information exchange, particularly between financial centers. Africa, meanwhile, has very few connections to South America. What sort of consequences can we expect from this limited exchange between the countries of the global South, just as the North and West engage in intensive cooperation? To what extent do cable networks give rise to new centers of power, to what degree do they recreate old colonial dependencies and block possible forms of alternative alliances? The answers to these questions will be of fundamental importance for the future of planetary power relations.



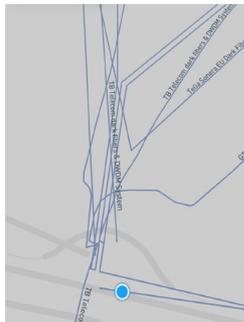
Worldwide submarine cable map from: J. Miller, "The 2020 Cable Map Has Landed," TeleGeography Blog, 16.06.2020, <https://blog.telegeography.com/2020-submarine-cable-map> [accessed: 27.03.2022].

3 *'People think that data is in the cloud, but it's not. It's in the ocean.'* *The New York Times*, <https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html> [accessed: 20.04.2022].

At the same time it is extremely difficult to analyze something that evades our gaze, something that is doubly concealed. First of all by language which makes us think of the World Wide Web as a cloud, but also by the inconspicuous nature of the symptoms and manifestations of its infrastructure. On the one hand, its concentration and density emerges in ordinary, everyday places: in a beautiful field traversed by a stream in the vicinity of Plock or on the beach in Mielno, a popular tourist resort. Someone unfamiliar with the “secret” code of the Internet’s underground infrastructure won’t even notice that somewhere just around the corner the Internet is flowing and that the cloud is to be found on the sea floor and in the earth, and not in the expanse of air. On the other hand, the WWW infrastructure is squarely off-limits, protected by CCTV cameras, the double gates of datacenters, mantraps, military-level security and bunkers dating back to the Cold War.



The internet flows along the Denmark–Poland 2 cable somewhere in this speculative area. Author’s photo.



Places where the biggest number of fiber-optic cables come together in Poland. They are the backbone of the internet. Most of the data transferred in this region flow through them. Part of the map from: <https://www.infrapedia.com/app> [accessed: 26.04.2022]. Author’s photo.

This game of visibility and invisibility is strictly bound up with power: who it is that owns and creates the connections, why do they want them to be visible or invisible; how do they mask, mark and tag them; and under what rules do they create them? But for data to enter into circulation, there must be a place where they begin their journey. These places are the datacenters, immense server facilities where the entire internet resides.

The desolation of data processing centers

Like cables and cable hubs, data centers are located in specific geographical locations. It is this local context that, in a non-straightforward way, informs their functionality and the nature of the resources they hold in the environmental, political, landscape, climate, economic, social, and geological sense. Some datacenters, like Kolos⁴ in Ballangen, Norway, above the Arctic Circle, use renewable energy – specifically hydropower. The climate conditions and the possibility of using cold air at the site to cool servers are also important factors. Others, like Swiss Fort Knox,⁵ considered the most secure datacenter in Europe, have been built inside mountains. The center has many levels of infrastructure, along with landing areas, airstrips on mountain ledges, as well as server facilities, generators, a hotel, and a water supply inside one of the massifs in the Swiss Alps. Other facilities can be found in old anti-nuclear bunkers or 100 feet under the streets of Stockholm, like Bahnhof's Pionen datacenter.⁶

The Internet has a material nature, temperature, and chemical composition. The server cases, bundles of cables, fire-fighting systems, electricity generators, batteries, cooling systems – all of these elements of the Internet infrastructure have their textures, smells, flexibility, temperature, and physical and sensual properties. But the Internet also has weight. During a visit to one of the datacenters in Gdańsk, the company co-owner giving us a tour of the facility pointed out that the floors have to be capable of bearing substantial loads – one of the factors taken into account when designing a datacenter or selecting a site. In that specific location the floor had to support a weight of 35 tons. Quite a lot for a cloud.

Through their security systems, materiality, appearance, locations, architecture and special narratives, datacenters confer value on what is stored in them, i.e. surplus data.

Datacenters tend to be depicted as deserted and abandoned places out in the wilderness.⁷ On the outside, we imagine them as embedded in a virgin landscape, surrounded by hills, fields and forests. Their interiors, meanwhile, are sterile, empty and dehumanized spaces straight out of futuristic fantasy novels or movies. A.R.E. Taylor claims that such images support a narrative that casts man as a threat to the security, automation and objectivity of data.⁸ Because of such visual representations datacenters have become fantastic, imaginary spaces, ideological and unreal objects.

4 “Kolos. Powering the Future,” <https://kolos.com/> [accessed: 20.04.2022].

5 “Swiss Fort Knox. Europe's most secure datacenter,” *Mount10*, <https://www.mount10.ch/en/mount10/swiss-fort-knox> [accessed: 20.04.2022].

6 H. Menear, “Pionen: Inside the world's most secure data centre,” *DataCentre*, 8.07.2020, <https://datacentremagazine.com/data-centres/pionen-inside-worlds-most-secure-data-centre> [accessed: 20.04.2022].

7 A.R.E. Taylor, “The Data Center as Technological Wilderness,” *Culture Machine* 2019, Vol. 18, <https://culturemachine.net/vol-18-the-nature-of-data-centers/data-center-as-techno-wilderness/> [accessed: 7.04.2022].

8 Ibid.

Inside the data center, man is seen as a source of error and is therefore a threat to the smooth running of the system. Moreover, on the phantasmatic level, his presence is an obstacle to bringing about a fully automated utopian future. The untouched and unpolluted (by human presence) space of the datacenter is also closely bound up with the ideology of knowledge created by data analytics companies. Data are supposed to be objective and free of the influence of human nature (by definition imperfect), without error and prejudice. They are to be the outcome of ideal mathematical procedures, of flawless calculation, and speak for themselves. The aesthetics of vanishing and absence fuels representations of knowledge as something unmarred by human prejudice and error, by man's archaic clumsiness and unpredictability.

This tension – between the fantasy of an ideal computational logic that converts every aspect of life and reality into data (a mathematical model) and the vision of man as an indefinite being, not reducible to information, eluding the grasp of machine logic – defines the key challenge that we face as humans and one that will determine our future. Can man be reduced to a series of zeros and ones, turned into a calculable statistical model? Or, just as we have discovered the laws of nature, can laws be found to predict man's actions, behavior, thoughts, moods, and desires?

This aspect of data being “natural” is underscored by the language we use to talk about them. Data are obtained, collected and mined like natural resources, and not seen as something produced by socio-technological systems. Often a bucolic vocabulary is invoked to describe them: streaming, cloud computing, data lakes, etc. This nature-inspired linguistic imagery gives rise to a media ecology in which data become part of the laws governing the universe – independent of humans and existing objectively.

Meanwhile, it is human prejudice that informs these only seemingly dehumanized and automatic algorithms.⁹

3. Algorithms and infrastructure as a new model of hidden power

As part of the industrial complex, datacenters justify and stimulate the production of increasing amounts of data (surplus data), while also giving them value. This is how a significant portion of the new system of surveillance capitalism comes into existence. The narrative of data saturation, of large quantities of data being necessary for the emergence of new knowledge and the development of a more intelligent way of managing different parts of reality, is cited as the main rationale for the construction of new datacenters. At the same time, the creation of these new centers sets up a situation in which “it would be a pity” not to create more (surplus) data and not to store them in places awaiting and attracting (seducing) them.

Mél Hogan notes that the American industrial prison complex worked in much the same way.¹⁰ The prison infrastructure built and managed by REIT (real estate investment trusts) provided a framework for and inspired subsequent legal changes, including the criminalization of immigration. The scheme made money as long

9 Ibid.

10 M. Hogan, “The Data Center Industrial Complex,” https://www.academia.edu/39043972/The_Data_Center_Industrial_Complex_forthcoming_2021_ [accessed: 7.04.2022].

as prisons were in demand. And a demand arose when a sufficiently large number of bodies – most of them black and Latino – were recognized as criminals to be incarcerated under laws enacted specifically for this purpose. In this manner, public funds allotted to the judiciary were pocketed by the private owners of investment fund assets. Once constructed, the infrastructure fueled a legal system that rationalized its existence and created conditions for a more intense accumulation of capital.

Similarly, the complex of over 8000 datacenters all over the world connected via a network of fiber-optic cables provides the material justification for producing increasing amounts of data. The latter are in turn processed by AI algorithms to more efficiently automatize different areas of life and the economy. Via interconnected networks of sensors embedded in different material objects and collecting all kinds of data, Internet of Things systems send and receive “dense” streams of data from data centers.

It is algorithms – alongside infrastructure – that constitute the second layer of the power backbone in surveillance capitalism. They require enormous datasets and surpluses in order to learn to recognize new patterns, improve their ability to “predict” the future, and evolve into increasingly capable systems of rules and functions. At the same time the assumptions they are based on, the criteria according to which they classify input and the rules that govern their operations tend to be confidential and hidden. This isn’t solely due to the fact that users do not know the language of programming and therefore lack the competence to understand AI, but also due to patent law and commercial secrecy. Those who create algorithms and deploy them often want their *modus operandi* to remain secret. This gives them greater influence over user choices, behaviors, and needs.

Just like the infrastructure, algorithms are part of the visibility/invisibility game. Those responsible for machine learning are increasingly better at identifying our proclivities, behaviors, needs, desires, and habits. They can identify various patterns in different datasets – from the natural sciences and medicine through economics and socio-political processes, to management, control and surveillance techniques. They not only “notice” regularities and correlations, but also formulate hypotheses regarding future developments by extrapolation. Many of our individual and collective choices – who we talk to, what sort of content we are exposed to, where we travel, how we love and with whom we associate, what we listen to, how we arrange our interiors and construct our visual messages, how we get to work, forecast the weather and natural disasters, predict election results and gauge terrorist threats – is often the outcome of algorithmic activity.

4. Algorithmic bias and normalization

Unfortunately, the awareness that this is happening does not automatically give us insight into the criteria, rules, and premises on which algorithms operate, their architecture, the sequences of commands and instructions that inform them, or the procedures and actions they set in motion. Nor do we know what sorts of datasets were used to train them. Algorithms learn to recognize patterns based on specially prepared datasets so they can subsequently classify and make generalizations outside those sets.

Meanwhile datasets may reflect the biases, stereotypes and assumptions held by different social groups, thereby reproducing various historical ideologies. They may also be selected so as to further the interests of those who own the means of production involved in creating AI systems. Both algorithms and databases function within a network of power relations and are neither neutral nor objective.

The first stage influenced by the human agent is the choice of a database to train a given algorithm. This selection is already based on certain assumptions about what is important and what to pay attention to, which section of reality the algorithm is going to scan for certain features and patterns, and what data can be ignored. People then “tag” the objects in a given database and introduce a preliminary categorization. They decide whether a given item meets a defined criterion and mark it accordingly, assigning it to a particular category. These two initial stages are where stereotypes relating to norms and anomalies are most often reproduced along with racial, gender, or ethnic bias. Old and conservative taxonomies are introduced into the world of artificial intelligence by the way input (the datasets on which the machine learning algorithms are going to be trained) is organized.¹¹

The datasets thus prepared with their human-created taxonomy become a training ground of algorithms. At this stage the stereotypes and biases encoded in the database and its taxonomy are usually amplified. The machine learning algorithms transform the data into a multi-dimensional statistical model whose nature is that of a vector space. Items are placed within a multi-dimensional coordinate system in which they are assigned specific numerical values that define their location. For example, the words or expressions in natural language begin to function as entities suspended at varying distances from one another and appearing in different configurations depending on the frequency of the correlations or relationships obtaining between them. The word “doctor” may appear more often next to the word “man” than the word “woman,” hence in the vector space “doctor” and “man” will be found closer together. If this statistical model is one day used by an artificial intelligence device recruiting doctors to work in a hospital, it will likely select male candidates more often than females, since it will have identified a correlation between these two categories.

The algorithmic creation of a statistical model via training also means removing all anomalies and flattening reality into an average. Should results appear that diverge from a specific trend or model, they will be ignored and absorbed into the average. This reinforces and normalizes stereotypes. Atypical patterns, truly innovative ideas, or non-standard concepts will be ignored by the machine learning algorithm. If the database contains elements that deviate from the statistical norm, they will be rejected. In this manner the multifariousness of reality is diminished, and all that is atypical, different, vibrant, non-obvious, non-standard, differing from the norm, is neutralized. As we can see, although they seem a very cutting-edge technology, AI algorithms actually tend to be very conservative. Not only do they replicate the existing order and preserve the status quo, but actually reinforce it.

Another way in which reality gets oversimplified is by having the machine learning

11 V. Joler, M. Pasquinelli, “The Noosphere Manifested: AI as Instrument of Knowledge Extractivism,” 2020, <https://noosphere.ai/> [accessed: 9.04.2022]. Polish version: “Nooskop ujawniony – manifest. Sztuczna inteligencja jako narzędzie ekstraktywizmu wiedzy,” 2020, transl. K. Kulesza, C. Stępkowski, A. Zgud, <https://nooskop.mvu.pl/> [accessed: 9.04.2022].

algorithm focus exclusively on a given set of traits. This means limiting the “resolution” of the world to that particular set. This is how AI misperceives objects that the human eye perceives as clearly different, e.g., a turtle and a gun, if the arrangement of selected traits is reminiscent of the pattern that the algorithm learned to recognize. For instance, Google’s AI algorithms mistook a turtle for a gun.¹² At the same time, the algorithm may differentiate between objects perceived as identical by humans if we introduce different features into its model.

This knowledge regarding the operation of algorithms is usually unavailable to us. It is locked inside a black box. Often we are unfamiliar with the source code, the datasets on which the algorithms were trained, or other input data. Algorithms are the invisible backbone of our world, a kind of invisible labyrinth or invisible strings that move our bodies, our affects, and our cognitive processes. The aim of Biennale Warszawa 2022 “Seeing Stones and Spaces Beyond the Valley” is to get inside the black boxes, to take algorithms out of the space of invisibility, and to show how they shape us, the materiality of our world, and the social processes that we participate in.

Vladan Joler and Matteo Pasquinelli note that narratives about mysterious AI algorithms, impossible-to-understand operations taking place inside neural networks, and the rhetoric of impenetrable black boxes all fuel a kind of mythology around artificial intelligence which presents it as unknowable and not subject to political control.¹³ We want to overcome this stalemate, shed light on the political underpinnings of technology, and highlight that the direction in which technology develops is not determined by obscure and mysterious forces, but depends on our agency as people and on the political decisions we make. This makes the debate on what kinds of technologies we want, and what kinds we don’t want so very important. What sort of future do we envision and by what means can we attain it? One of the fundamental goals of the program is to unblock our socio-political imagination with regard to the future of technology – showing that it is possible to shift from a critical analysis of surveillance capitalism to thinking about democratic or communal technologies.

Creative, active and political efforts to design the future are important insofar as AI algorithms – created for the purpose of extracting and classifying our most intimate data – generate statistical models of the future solely by extrapolating past patterns. As a result, they can discover nothing truly new or stumble upon an idea not thought or documented before. Machine learning cannot progress beyond recreating the past. In the best case scenario, it produces variations on past patterns, reconfiguring, mixing, and processing them. Machine learning algorithms forge a future that is a mythological image, repeated and reproduced, which makes them mythical machines. Because of this, they frequently reproduce existing classifications, dichotomies, prejudices and gender, class, racial and sexual stereotypes. If algorithms learn to classify based on datasets informed by Western beliefs and values, then they will reproduce them, making automatic decisions that only seem objective and neutral. In 2016, Microsoft created a bot which was supposed to learn from user posts on Twitter. Over the course of 24 hours it

12 J. Vincent, “Google’s AI thinks this turtle looks like a gun, which is a problem,” *The Verge*, 2.11.2017, <https://www.theverge.com/2017/11/2/16597276/google-ai-image-attacks-adversarial-turtle-rifle-3d-printed> [accessed: 9.04.2022].

13 V. Joler, M. Pasquinelli, op. cit.

became an automated racist and sexist hate discourse spewer merely by replicating the patterns it recognized in the communications between “human” agents.¹⁴ Meanwhile, Tinder’s secret Elo Score algorithm which measures users’ desirability perpetuates the sexist practice of viewing people as sexual objects and rating them on a number scale. AI experiments designed to identify a person’s sexual orientation based on their facial features are equally problematic. These are only some examples¹⁵ of algorithms that perpetuate binary distinctions and replicate existing ideologies. The regressive and conservative character of seemingly progressive technologies manifests itself clearly when we realize that the social categories replicated by these algorithms have been undermined and deconstructed for many years not just by male and female critical thinkers, but also within the framework of various public policies aimed at achieving equality. If introduced without appropriate caution, automation may obliterate previous critical efforts. For the moment, it seems that generalizations and the duplication of old social divisions and power structures are the norm.

Machine learning algorithms are closely connected with the industrial datacenter complex which rationalizes producing surplus data, as Mól Hogan writes.¹⁶ Surplus data are needed to improve algorithms. They give them the material to work on so they can find new patterns in the world and, potentially, take over successive tasks from people. Algorithms read our emotions based on our facial expressions and listen in on our conversations, not only processing the meaning of the words we speak, but also analyzing the tone and sound of our voice, the subtle changes of volume and intensity, and trying to “understand” the rich context of our utterances. By collecting thousands of data points from different moments in time we can obtain a stunningly detailed psychological profile of an individual, comprising many nuances that even the most astute psychotherapist would fail to detect, as well as a detailed reconstruction of a life.¹⁷ Self-driving cars on the other hand are taught to make ethical decisions based on programmable “value” hierarchies that can be activated in hypothetical situations on the road. Internet of Things (within whose framework material objects packed with sensors “talk” to one another) systems transmit information to one another, integrate data, create new correlations, eavesdrop on us and gather information about how our mood relates to our behavior and bodily reactions via various fitness, sports or health apps and wearables . Algorithms can also diagnose cancer from ultrasound images, often better than a human, seeing subtle changes that may herald the beginning of a developing cancer image.

AI can also be used for racial profiling and can directly serve authoritarian regimes in instituting systemic oppression and violence. The first disclosed example of algorithm-based racial profiling involved a system developed by the Chinese company CloudWalk.¹⁸ Supplied with data on the faces on Uyghurs and Tibetans,

14 J. Vincent, “Twitter taught Microsoft’s AI chatbot to be a racist asshole in less than a day,” *The Verge*, 24.03.2016, <https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist> [accessed: 10.04.2022].

15 Inspired by M. Hogan, op. cit.

16 Ibid.

17 “Made to Measure”, <https://madetomeasure.online/de/> [accessed: 20.04.2022].

18 P. Mozur, “One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority,” *The New York Times*, 14.04.2019, <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> [accessed: 9.04.2022].

the algorithm learned to recognize people belonging to those ethnic groups. It was then hooked up to CCTV monitoring systems. This made it possible to create a database of Uyghur entrances and exits from a given neighborhood, to track Uyghur movements around the city and record how frequently they went past certain locations. Based on this knowledge, maps of the typical movements of a given minority were developed. What is more, if a group numbering more than the standard number of “sensitive” individuals appeared in a neighborhood, the system would automatically send a warning to the appropriate services.

This openly racist state surveillance system could be combined with an analysis of the genetic data of “sensitive” groups collected by the Chinese authorities. DNA seems to be another area now being penetrated by the drill of data extraction and algorithmic data analysis. Feelings, diseases, mental health issues, addictions, intimate relationships, sexual activity, neuroses and orientations are no longer the only data sources that can be used to create our profiles. They can be combined with a thorough AI analysis of individual DNA sequences and the creation of incredible correlations between our genes and behavior. It isn’t difficult to image the consequences of such far-reaching surveillance and commodification of our unique life code. Companies and political parties would be able to purchase data packages in categories linking specific behavioral profiles with specific genetic code sequences on the data market.

The testing of new AI systems in the field of migration, refugee procedures and directly at state borders also poses similar problems. Refugees, stateless persons, people on the move, people without documents – often fleeing war and persecution or places whose ecosystems have been rendered unlivable by climate change – are especially at risk of exploitation. We are not just talking about human trafficking or various forms of labor exploitation, but also about situations in which these people are stripped of the rights protecting citizens against privacy violations involving the extraction, collection and processing of personal data.

Moreover, due to the liminal status of refugees and the fact that it is easy to define them as “outside the law,” state services working arm in arm with private tech companies have been taking advantage of the situation to test controversial surveillance technologies and automatic decision-making and data extraction systems. They not only track the digital footprint of refugees using data from their phones, but also, like Palantir (a company specializing in advanced data analytics) profile them by pooling data from different sources. US Immigration and Customs Enforcement used these methods when Donald Trump was in office to organize deportations and split up migrant families.¹⁹

Automatic lie detectors that try to measure deception and identify potentially suspect persons based on facial and voice parameters as the individual responds to more and more challenging questions are also tested at borders. But will the algorithm, trained on datasets rooted in a specific context, take cultural differences in expression into account? Will it be able to tease apart inconsistencies in someone’s story caused by trauma-related cognitive impairment and those resulting from deception? Who would be held responsible should a refugee want to appeal

19 S. Woodman, “Palantir Provides the Engine for Donald Trump’s Deportation Machine,” *The Intercept*, 2.03.2017, <https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/> [accessed: 10.04.2022].

a decision made by the algorithm? The designer of the system, the programmer, the immigration official, or perhaps the algorithm itself?²⁰

5. Surveillance capitalism and cyberwar

As Svitlana Matviyenko writes, platform users become the cannon fodder of cyberwar. They often function as perfect, automatic information transmitters. Reified, treated as a resource and a product all at the same time, a source of data and a mathematically profiled behavioral weapon, it is their very *humanness* that makes them exploitable: their fears, anxieties, desires, weaknesses, sensitivities, vulnerabilities, addictions, knowledge, habits, behaviors, and beliefs. All of these quintessentially human, emotional, affective and cognitive states are converted into data.²¹ In this process, a person becomes a certain kind of statistical configuration of traits and properties, a mathematical model or pattern whose specificity and parameters can then be processed by AI. It is the algorithms that predict behaviors and arrange them into correlations. They let us know what to do to make a given person – as a statistical data pattern – behave in a certain way. In this manner, by way of behavioral manipulation, it is possible to control the behaviors, views or addictions of individuals or entire populations.

This is how digital big data monopolies and all kinds of state agencies linked together by capital ties and relations of power function. Shoshana Zuboff dubs this new paradigm surveillance capitalism. Its many definitions include the following: “[a] new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales” or “a parasitic economic logic in which the production of good and services is subordinated to a new global architecture of behavioral modification.”²² The same human experience in its complexity and indefiniteness is captured by various data-collecting sensors and then flattened into a statistical average. In the end, a model is created that can be managed and manipulated, and whose states and behaviors can be predicted via the extrapolation of future patterns and tendencies from past ones, and which can then be sold as a product, a data package in a specific category (e.g., those contemplating death; those experiencing problems with body image; pregnant women; those at risk of addiction; those prone to take risks; those fearing for their families; depressed people, etc.).

If the algorithm knows more about you than you know about yourself, it can steer you towards beliefs or habits that benefit the group or company that created it and thus generate financial, propaganda or military gains. The same mode of operation, consisting in converting human behaviors and qualities as well as

20 P. Molnar, “Technological Testing Grounds. Migration Management Experiments and Reflections from the Ground Up,” EDRI, Refugee Law Lab, 2020, <https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf> [accessed: 10.04.2022].

21 “Reconsidering Cyberwar: an interview with Svitlana Matviyenko,” <https://machinic.info/Matviyenko> [accessed: 5.04.2022].

22 S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York 2019.

the entire environmental, social, relational and material context into data, can be capitalized upon in the interest of corporations and states. It can also be weaponized as a resource and a tool in cyberwar. As Matviyenko writes, “[c]yberwar is a capitalist war,”²³ adding that it is data about human emotions, desires, behaviors and vulnerabilities analyzed by AI that serves the aims of cyberwar by increasing polarization among platform users and reproducing antagonisms and toxicity within “echo chambers” and various information and worldview bubbles.²⁴

Polarization and antagonization drive users to produce more and more new data. They mobilize the intimate affective-behavioral factories inside us to produce new data in response to provocations – in outbursts of indignation and the need to stand up for “one’s team,” in the deep desire to manifest one’s refusal to go along. The real purpose behind Facebook arguments, rows, battles and wars is to artificially foment antagonism via algorithmically provoked conflict. The reality overshadowed by such conflicts shows a different division into those who profit from the data produced in these “ideological agonies” and those “whose fears and desires are instrumentalized by war, *platform users*.”²⁵ Based on this diagnosis, Matviyenko concludes that capitalist platforms politicize and militarize communication.

Moreover, every new form of defiance, every new protest, strategy or resistance tactic is analyzed and recognized by AI algorithms which learn its pattern, dynamics and technique so they can quicker notice it in the future and respond accordingly, undermining its effectiveness and potential. As a matter of fact, this is precisely how authoritarian government works too. The cyberwar context, also now with the war in Ukraine, brings to light the nexus of two authoritarian techniques: on the one hand, silencing users, taking away their voice and communication tools totalitarian-style, and on the other, the neoliberal method of seducing people with freedom and inspiring them to speak “freely” so that their articulated thoughts and feelings can be caught in quantification nets and the “free expression” commodified into datasets. Both tactics – silencing people and encouraging them to speak (shout, agonize, argue, engage in angry exchanges) – are of key significance in the dialectics of the war in Ukraine.

6. The Non-Aligned Technologies Movement and the Data Garden

AI algorithms are designed to capture correlations between phenomena, but they are incapable of understanding causality. One of the main errors within this perspective is conflating correlation with causation. If, for example, those who travel regularly are more likely to enter into new relationships, it does not mean that there is a cause-and-effect connection between travel and the lifespan of an intimate relationship or the readiness to initiate a new one. By extracting various kinds of data, machine learning can set up any random type of correlation and then present it as a causal relationship.²⁶ Algorithms obsessively “adjust the curve,” producing

23 *Reconsidering...*, op. cit.

24 See: *ibid.*

25 *Ibid.*

26 V. Joler, M. Pasquinelli, op. cit.

different correlations without giving an explanation. This is why AI lacks deeper insight into certain phenomena and fails to understand or explain them. Mistaking correlation for causation turns dangerous when we attempt to predict the future via algorithms. Since AI algorithms are used in border procedures, forensics and wartime decision-making, it may be that preemptive actions taken in response to various predictions will be completely off the mark and falsely create suspects, criminalize innocents, or identify the wrong targets.

It is equally risky to entrust our future to AI which only reproduces past models and cannot detect novelty, leveling innovation and deriving its visions of the future from correlations of past phenomena. Under these circumstances human creativity and agency have a major role to play. It is man who can explain the causal relationships between phenomena and devise a plan, so that we can reach the future we want, step by step. It is human imagination that comes up with previously unimaginable visions, and human thought that generates previously unthinkable ideas. When we use the expression “outside the valley” in the title of our exhibition we want to go beyond the mental frameworks proposed by the companies, discourse and practices of Silicon Valley, but also continually work to push the limits of our imagination, to stretch it, to question the obvious not only in order to lay bare injustice and power relations, but also to open up a field for potentiality, creative praxis and ideas. To transcend the valley of our imagination, to try and test what appears unlikely, beyond reach, alternative, at odds with the prevailing paradigm, and what gets us thinking about a better world, without darkness and without the apocalyptic-catastrophic valley.

Such practices, prototypes, ideas, speculations and imaginings are part of our exhibition and public program. I would like to point out two alternatives that respond to the challenges of the datacenter industrial complex and what Nick Couldry and Ulises Ali Mejias have dubbed data colonialism.

Let's imagine that instead of datacenters where information is kept in binary code we start effectively encoding data (texts, films, photographs, sounds) in plant or other types of organic DNA.²⁷ The music of Miles Davis, Martin Luther King Jr.'s *I have a dream* speech, photographs, Shakespeare's sonnets, a computer virus

27 See: J. Davis, S. Khan, K. Cromer, G.M. Church, “Multiplex, cascading DNA-encoding for making angels,” in: *A New Digital Deal: How the Digital World Could Work*, ed. M. Jandl, G. Stocker, Ars Electronica 2021, Festival for Art, Technology & Society, Hatje Cantz, Berlin 2021, pp. 148–155.
But how can one store information in plant DNA? Computers read binary code, i.e. information coded by zeros and ones. In order to encode sequences of zeros and ones in DNA we have to start by assigning specific numerical values to its various components. The genetic code consists of four basic nucleotides – adenines, cytosines, guanines and thymines (ACGT) – which code one of twenty amino acids by forming triplets known as codons (e.g., TGT, TCG, AAG, GTA). Some amino acids can be encoded by different codons, for example lysine (Lys) is encoded by AAA or AAG sequences. The codon sequence determines what amino acid sequences will combine to form the proteins typical of a given organism. Four nucleotides can be combined into sixty four three-part codon combinations.
We can start encoding information in binary code by assigning numerical values to particular nucleotides in accordance with their molecular mass: C = 0, T = 01, A = 10, G = 11 (from lightest to heaviest). In this manner, the sequence 11011000 will stand for the nucleotide sequence GTACC. Similar numerical values can be assigned to each of the sixty four codons coding particular amino acids, as well as to each of the twenty amino acids. The value 1101 is assigned to cysteine (Cys), encoded by the codons TGT and TGC. Alanine (Ala) – encoded by GCT, GCC, GCA, GCG – gets 1011, glutamine (Gln) – coded by CAA, CAG – gets 100. Other sequences of zeros and ones are assigned to the other seventeen amino acids on a similar basis: 0000, 00, 1000, 1010, 10, 101... Thanks to this system it is possible to redundantly encode any information previously rendered in binary code.

and much more has already been stored in DNA.²⁸ Instead of over 8000 datacenters using up precious water supply and leaving a huge carbon footprint we could create archival gardens storing our private data or data palm houses, where knowledge of key importance to humanity could be kept. One gram of DNA can store around a million gigabytes of data. As Mél Hogan writes, this means that all the data we currently produce in the world could fit inside a box the size of a car trunk.²⁹ Moreover, frozen DNA is extremely durable and can be preserved in that state for two million years. The idea is explored in the exhibition in the work *Data Garden* by the collective Grow Your Own Cloud.

While storing data in plant organisms is an answer to the challenges posed by the material infrastructure of the Internet, Couldry and Mejias propose to counter data colonialism with strategies and tactics employed by decolonization movements. They see the extraction of value from human life (via data) as a practice deriving from the 500-year history of colonialism.³⁰ They situate it within the *longue durée* and show how accumulation by dispossession (a notion proposed by David Harvey) may apply both to the appropriation of natural resources, land, labor, and data. The appropriation of data (extracted from human life) is akin to the appropriation of land, since in both cases someone (Google, or the conquistadors) claims the right to supposedly ownerless resources – land (in communities where private property does not exist) or data (including the digital footprint left behind by our online activity). Like land, data is said to belong to no one, to “lie fallow,” available to collectors as soon as the user signs a declaration renouncing his ownership rights (if we produce or store them within the framework of the services provided by digital platforms).

For Couldry and Mejias data extractivism and colonialism predate capitalism and mark a new stage of colonialism that makes it possible for successive phases of capitalism to emerge. They invite their audience to critically approach the excuses and justifications offered during the colonial period to justify the mass extraction of natural resources and – analogously – are being cited today to justify data extraction. They include rationality, progress, order, science, modernity, and salvation.³¹ These are accompanied by views presented as obvious and not subject to discussion, for example that without data collection the world won’t be able to develop, won’t be understood, sensibly managed, and finally (if a climate catastrophe comes about, for instance), will not be salvaged.³²

These claims should be countered with imaginative work on a global scale. All decolonization strategies have always been acts of imagination, and that is what we must do now, i.e., come up with alternative ways of conceptualizing data and technology. Couldry and Mejias propose the Non-Aligned Technologies

28 See: M. Hogan, “DNA,” in: *Uncertain Archives. Critical Keywords for Big Data*, ed. N. Thylstrup, D. Agostinho, A. Ring, C. D’Ignazio, K. Veel, The MIT Press, Cambridge 2021, pp. 171–178.

29 Ibid.

30 N. Couldry, U.A. Mejias, “The decolonial turn in data and technology research: what is at stake and where is it heading?,” *Information, Communication & Society* 2021, <https://www.tandfonline.com/doi/pdf/10.1080/1369118X.2021.1986102> [accessed: 10.04.2022].

31 Ibid.

32 Ibid.

Movement (akin to the Non-Aligned Movement of countries) that would boycott extractivist technologies and employ alternative ones, leading to the non-purchase or non-acceptance of the “free” products of digital monopolies and the reclaiming data (as well as any products developed using them) on behalf of those who generated them. It would impose taxes and sanctions on Big Tech to repair the damage inflicted by their technologies. It would work to develop a new imagination and new forms of community without extractivist technologies and the high costs associated with them, and create solidarity that would bring together “non-aligned individuals and communities globally through collective imagination and action.”³³

These ideas can serve as an inspiring point of departure for personal experimentation with alternative technologies: for the creation of new ideas, prototypes, organizations and collectives capable of building a new, democratic, just, and more equal world. There is one thing we know for sure – technologies will shape most political, existential, social, ecological and economic phenomena in this world. It will be up to us to design it as we wish.