The Anarchist Library
Anti-Copyright



Anonymous
From One Vulnerability, Another
Summer 2021

Translated for The Local Kids, Issue 7
Previously published as *D'une vulnérabilité l'autre* in *Avis de tempêtes (Bulletin anarchiste pour la guerre sociale)*, Issue 39, March 2021

theanarchistlibrary.org

From One Vulnerability, Another

Anonymous

Summer 2021

On the microscopic scale, the destruction of autonomy (the reduction of spaces to determine your life) through the introduction of evermore technological prostheses can only give way to a biting despair. A sensation that correlates with the degree of depreciation and abrasion that you're subjected to. The wheel of progress turns ever faster. Before, broad transformations in society could span several generations. Today, inside the space of one generation it sometimes seems that you're not born in the same world. This explosion of speed requires an extraordinary capacity of human beings to adapt. In response there's a whole range of functional "defects" towards the world's conduct. For example this can be manifested in neurotic or bodily illnesses. Human beings don't live isolated in outer space but indeed inhabit this planet. Every adjustment to their "habitat" influences their possibilities and capacities to reflect, but also to feel and act. This is of course not a privilege of the hyper-technological society that we know today. We could say that every civilization works in this way. Thus the question acquires more depth; from which point on does a sharp

adjustment in the habitat leads to a loss of autonomy, a suppression of freedom? If every adjustment is not in itself contrary to freedom? But these are questions that by far surpass the modest reflection of this article.

Let's take a bit of distance from daily life and let's try to think on a macroscopic level. The expansion of the techno-industrial Moloch – which we could call the "megamachine", following Lewis Mumford – seems also to go together with an increase in its vulnerability. If the systems are more complex and the techniques become complicated, they are also more vulnerable to a simple breakdown, an incident, an unforeseen event. Because it doesn't effect only an isolated component but the whole system. Or as Günther Anders summarized it; "The bigger the machine, the more seriously endangered are its parts, which had operated individually before their merger into the larger machine." And he logically concluded that "the larger the machine complex, the greater is the catastrophe if the complex breaks down." Of course this is a theory – or rather, an observation – that has been taken to heart by the system engineers since a long time. The fragility of data networks, the dependence on a centralized electrical grid, the just-in-time production which aims to limit stocks, the interconnection of systems (even the most "vital" ones as the drinking water distribution which depends on the proper functioning of electric pumps); all this keeps on inspiring thousands of studies, projects and strategies to raise the "resilience" of systems. But not without bitterly noting that faced with technological progress, it's like fixing a leak by opening the tap.

This fragility of the megamachine is now part of a discourse surrounding "collapse". The hypothesis is that the technological system is going towards a total failure because of several reasons ranging from a shortage of energy resources to climate changes. We don't want to support a "catastrophic" version which, barring some exceptions, shows itself to be a useful defence of the actual system. Because it only promotes preparations for survival while waiting for the floods to come, instead of focusing on attacks or

insurrection (including in its most anti-authoritarian forms). Nevertheless, all the elements have to be taken into account. It is by considering the world in its entirety that our perspectives can become relevant and not by only building castles in the air or by being content with our daydreams of eternal rebels. To say the least it would seem ridiculous to consider insurrection without taking into account the question of the metropolis, of climate change, of cultural flattening, of sectarian hate or of social cannibalism that is brewing, etc. The reflection of anarchist critiques of power – whatever they might be – can take an unexpected depth on the question of autonomy or liberty when faced with the acceleration of devastating climatic events and the frenetic race of a ravaging industrialism. On the condition that it gets rid of the skeletons that still clutter anarchy; programmatism, fear of the unknown, victimism borrowed from the left, determinism borrowed from Marxist materialism, etc. There's still a long way in front of us.

***

"We need not be surprised, then, that in more than one area the Power Complex has been undergoing severe strain. Though immune to any frontal assault except by another power system of equal size, these giants are particularly vulnerable to localized guerrilla assaults and raids, against which their mass formations are as helpless as was heavily armored Goliath against a nimble David who did not choose to use the same weapons or attack the same part of the anatomy." - Lewis Mumford, *The Pentagon of Power* (2nd volume of "*The Myth of the Machine*"), 1970

So what about this vulnerability of the megamachine? Is it real or is it one of the many ghosts that have been the travel companions of revolutionaries? There have been the tales of the historical mission of the proletariat, the inherent contradictions of capitalism, the coming awakening of the still dormant masses, the revolution conceived as a *Grand Soir*, the progressive disappearance of massacres and hatred in humanity, the catharsis caused by wars and catastrophes. Enough reasons to be cautious. A far-flung revolt as

the one in Chile in 2019 didn't lead up to an open insurrection. The uprisings in the Arab world have been drowned in blood and gave way to other horrible monsters. The multiplication of the sabotage of cell towers or fibre optics didn't cause an institutional or economical breakdown. This is not to deny that blows have been dealt. Certainly, they weren't deadly but they demonstrated their potential at the same time as their shortcomings. So let's evaluate that fragility, which is here not synonymous with "social revolution" but rather with possibilities of liberty or an extension of chaos from where the unknown can emerge, "good" or "bad". And to that end, let's look closer at one of the backbones of the megamachine: the electrical grid.

On 8 January 2021 at 14:04 CET, the alarm systems turn red when the European electrical grid sees a sharp drop in frequency of the alternating current supply (50 Hertz) [in the North-West Area, the opposite occurred in the South-East]. The cause of this frequency deviation is still not certain but probably it was due to the tripping of a circuit breaker (incident, failure, sabotage… no clarifications on that matter) in a substation in Croatia. The European electrical grid is connected from Warsaw to Paris and from Istanbul to Copenhagen. And for this network to function it needs a stable frequency. The equilibrium between supply and demand of electrical energy has to be guaranteed at all times. The grid deals with fluctuations by [either temporarily reducing the production of electricity or] temporarily supplying additional electricity and reducing the consumption of electricity, specifically of major customers. To stabilise the grid in January 2021, several big industrial sites are disconnected as a matter of urgency (specifically in Italy, France, Austria, Romania, etc.). But also several high voltage lines are cut off (14 in total) because when they cannot maintain the right electric pressure, the electric current will fast find another way (to other lines) which then can result in overcurrent. Thus the totality of lines of the electrical grid is at risk of a snowball effect.

Recent months have shown us many more examples of the vulnerability of the digital networks. We can think of the cell towers and the transmitters that cut off the communications of millions (as in the case of the fire at the Marseille transmitter in December 2020 or the Limoges one in January 2021), of the sabotage of fibre optic connections (as in the attack in Crest in February), of the manual cuts or burning of fibre optic cables (as in Pierrellat during the same month). Let's bet that the same vulnerability can be found in all networks, including the electrical that feeds everything that exploits, destroys and controls. For understanding to become incisive action, we certainly have to get rid of the ghosts that haunt our spirits and understand, with all it entails, that we're in hostile territory and we have to act accordingly. With joy in our bodies and liberty in our hearts.

On the Austrian side, the spokesperson of the electricity network operator EVN speaks of an "almost blackout". The incident achieves the third of four warning levels in the European ENTSO-E classification ("*Emergency – Deteriorated situation, including a network split at a large scale. Higher risk for neighbouring systems. Security principles are not fulfilled. Global security is endangered*"). From their side, the French network operator RTE boasts about their "defence barriers" consisting of disconnecting major industrial zones and supplying more electricity through gas power plants or hydroelectric dams. What is certain, is that the European grid – a giant that merits the "megamachine" qualification – is vulnerable, especially because of its size and centralisation.

Let's mention also that new electricity sources (wind and solar), by definition intermittent, cannot manage all these fluctuations in frequency and cannot respond to sudden demands. They cannot function without the support of a more "conventional" electricity production (like coal or gas power plants). Their multiplication on the territory constitutes another element of instability and fragility to the electrical grid. To amend this, mega-batteries are being built a bit everywhere. They would be capable of storing electricity to be supplied to the grid in case of need. But their efficiency is still questionable. In France, RTE started building these mega-batteries on sites in Vingeanne (Côte d'Or), Bellac (Haute-Vienne) and Ventavon (Hautes-Alpes) in the summer of 2020, in addition to their project for a hydroelectric power station for producing and storing energy in Fos-sur-Mer (Bouches du Rhône).

This "incident" in a simple local transformation substation but with serious consequences, reminds us of another rather resounding fact on the other side of the Atlantic Ocean. On 17 April 2013 around 1 o'clock in the morning, someone opens a technical vault next to the electrical substation of Coyote (California) and cuts fibre optic cables. It takes a moment before the operator notices. Ten minutes later, another set of cables is cut in a manhole close-by. Thirty minutes pass before the surveillance cameras of the substa-

tion register a faraway trail of lights. The investigators believe this to be a signal coming from a flash light. Shortly after, at 1:31 a.m., the cameras register flashes from a rifle and sparks coming off the fence when bullets touch it. At 1:41 a.m. the Sheriff's department receives a call from an operator at the energy centre who heard the shots. The police arrive 10 minutes later, but everything is already back to normal. They arrived one minute after another signal with a flash light marks the end of the attack.

On what were these mysterious attackers firing? On the big transformers of this substation. These are simple things, being nothing more than spirals of copper wire inside metal cages. They also have reservoirs with cooling liquid because of the heat they produce. It was exactly these reservoirs that the shots were aimed at. After being riddled with hundreds of holes, the precious liquid began leaking away. The cops didn't notice that 200 000 litres of oil were slowly being drained. After a short while, the transformers overheated and exploded. 17 out of 21 transformers at the substation were knocked out. One or two more would have immediately put California in the dark. At this occasion, the electricity company could quickly reroute power around the substation. Silicon Valley continued to receive electricity but was asked to limit its power consumption for that day. The damage took 27 days to be repaired. As the FBI itself admitted; "It doesn't take a very high degree of training or access to technology to carry out this attack." If several substations would be targeted during the same period, thus preventing a rerouting, it would have been a different story.

On the subject of a "black-out", engineers and officers warned against the fragility of the grid in a recent special report in the *Revue Militaire Suisse* (Issue 5, 2018). They developed several hypothetical scenarios; their conclusions? Setting aside the cause of the breakdown of the electrical grid, in broad strokes it goes like this: if the black-out doesn't last more than a day, restoration goes quickly. If it lasts more than 48 hours, restoring the grid becomes

less likely or even impossible. All the instruments that control the networks are powered themselves by electricity and only have an autonomy of 2 to 5 days. Once they run out of battery, someone has to be dispatched to restart them at the same time as the rest of the network. Thus external support is necessary if the network is not restored after 5 days. In case the black-out is only regional, emergency and repair teams can be dispatched on site. If it is national or continental, the situation can last or even be fatal for the whole grid.

Another example, this time from the digital world. On 10 March 2021, a fire erupts in the data centre of OVH in Strasbourg. The private company OVH has the biggest web hosting service of France. The fire allegedly starts at the base of the building where the electrical supply facilities are. That's what the company points to as being the cause; an inverter (changing the electrical frequency) would have caught fire. This explanation sounds reasonable, except that according to reports of employees and firefighters the fire spread extremely rapid. This could indicate several points of origin. Everyone can speculate on the origins of this fire, the authorities can communicate what suits them (it's after all the most important host of France, spearheading the data centres) but a rather less "accidental" cause stays plausible. Moreover because there are worldwide very few examples of data centres that perish in flames due to a technical fault. That said, failure or something else, the result is very "tangible" (our apologies for using this obsolete term in this virtual world). Hundreds of thousands of websites went offline, huge sets of data were lost for companies and institutions. Like a mini-apocalypse in the cloud. It isn't even necessary to go into detail to be able to grasp the vulnerability of the digital megamachine. A significant part depends on a single, physical structure. This depends itself on an uninterrupted connection by fibre optic cables and a constant supply of electricity (because the emergency circuits cannot completely replace the grid).