By Geert Lovink and Ned Rossiter

Original illustrated version here:
http://obieg.u-jazdowski.pl/en/numery/estetyka-kontyngencji/uwagi-o-nbsp-sieciach-i-nbsp-kontyngencji

Polish translation:
http://obieg.u-jazdowski.pl/numery/estetyka-kontyngencji/uwagi-o-nbsp-sieciach-i-nbsp-kontyngencji

"There's no such thing as singular devices. Totality is the truth."
Günther Anders

The internet is an administrated world. This translation of the German *verwaltete Welt*, introduced by Max Horkheimer, opens up a spooky universe that stands in stark contrast to the bright transparency that we experience online. How do we sense today's darkness that is "hiding in the light"? For the traumatized critical theory generation, administration was considered an abstract bureaucratic killing machine. These days it is becoming harder and harder to be objective and localize administration *an sich* and externalize it as a rude imposition that resides outside of daily life. In this neoliberal age, we first and foremost administrate ourselves. All the rest has become outsourced procedures that we click away after we have filled out a form or profile, submitted our user name and password, and quickly agreed to the terms of service.

Why have processing and filing out forms become so invisible? We certainly do not spend less time on filling out online registration forms, creating profiles and scanning our eyes, fingers, and passports. Despite all the daily identification work, we do not have a clue about the network politics that govern the present. No matter how much we get used to the increased complexity, speed, and storage capacity of our intimate machines, there is nothing "natural" about connected computers. Without constant monitoring by humans the network immediately becomes defunct and falls apart. One missed patch and the machine is hijacked.

The term contingency is the perfect postmodern empty signifier. Whether it is the coupling of irony and solidarity with contingency (Richard Rorty) or the historical and radical contingency of power (Žižek in dialogue with Butler and Laclau), contingency stretches the spectrum from unforeseen possibility to imminent annihilation. What is Schumpeter's logic of "creative

destruction" if not the ultimate entrepreneurial fantasy that the ferocity of the markets can be controlled? We're drawn to the seductive danger of risk. The delirium of the titans of industry supposes that contingency can be tamed and made productive in the form of security procedures and insurance contracts. The current state of planetary collapse, societal anxiety, and extreme capitalism signals a total submission to the incapacity of decision. The spiritual quest to orchestrate contingency has produced a society of despair and a living hell for species–beings.

As our planet races toward species depletion and social dislocation, we are presented with the enormous challenge of deciding how to orient the economy and society, labor and life in ways beyond the logic of permanent destruction. There is, nonetheless, another nihilistic option. Contingency also occupies the space of almost imperceptible vibration and inspires an aesthetics of dizziness. What are the possibilities and consequences of embracing contingency in an age of amplified disorientation? The computational manipulation of affect presents a new front in strategies of engineering outcomes that consolidate sovereign power. Google glasses, Fitbits, DNA analytics, smart homes, biometrics. The calculation of sensation operates as a key technique of algorithmic governance. But can the low–fi buzz of something awry, out of kilter, a general unsteadiness serve as tactical interventions against breakdowns designed to destroy our collective will? Beyond protocological inoperability, can we design confusion as a technique of counter–power?

Network normality is a permanent state of exception. Much like other machines, computers need constant maintenance and monitoring. If one forgets to run a critical update the connection can fall apart overnight. As this type of daily tinkering remains mostly unnoticed for ordinary users, similar to comparable work in the reproduction sector such as cleaning and childcare, there's a tendency to focus on sexy topics such as algorithms, robots, and artificial intelligence and forget the fundamental role of the system administrator.

Contingency is boring precisely because it requires an exhausting form of alertness to details. Its procedures demand our full and ongoing attention. One distraction is enough for a catastrophe. To be on the lookout is not enough. We need to read up, assess, and then act. The first step is to make a backup. The copy is our fallback option, a largely invisible foundational ritual of techno–culture. Machines are not yet programmed to take care of

themselves and thus do not run automatic backups as a default, let alone automatically upgrade themselves.

Nothing's as difficult as machinic self–reproduction. This state of the art is the radical anomaly of the computer's first century. Instead of raising the computer as a robot that is destined to mind its own business, early generations of hardware, software, and networks are maintained through human supervision – as if they have to be breastfed, raised in close proximity to the human species. This is all the more strange as humans, in their status as wetware, tend to expect otherwise. Computers are supposed to be tools, servants, slaves, not babies. Why do laptops and smart phones simply no longer work when we put them aside for a couple of weeks? Who came up with this horror of "constant care"? The fact is we have not made copies at the right moment, and time and again are punished for this. We cry and cry over the personal failure and blame the organized stupidity of humankind after each data loss.

The copy will not prevent outages and is, at best, intended to reduce the off time. However, we can easily be fooled by installing a copy of the old network if the deeper problem is not properly addressed. Who knows, the backup might come in handy once the Event unfolds, which is "likely but not certain to happen." These days we are fundamentally unsure about the status of the Event. Should we label hacks, bugs, and ransomware as accidents? They may be "unforeseen" for some but we all know, all too well, that we should have known better and have taken countermeasures a long time ago and close the exploit. Insiders would rather not speak of "risks."

Contingency critics see the term as fundamentally anti–revolutionary. In a society driven by contingency plans nothing ever happens – until it happens. Protest meetings can only be held if they're pre–registered with authorities. Mass public gatherings have become an insurance liability. In the society of circuits "fun guerilla" stunts are forbidden. Sudden interruptions to vanilla life are seen as terrorist acts. Every unexpected move is immediately classified as a terrorist attack. On the bright side, contingency can also be seen as a disruptive force when we define contingency as the enemy of algorithmic architectures and computational governance. Are we on the side of disruption or the disrupted? Increasingly, the Event is suppressed by technologies of pre–emption and prediction. Invention is one the wane as a result of this. So is experimentation. It's hard to say if something like the flash crash is an instance of contingency or part

of the surge logic of high frequency trading.

“Thank you for sharing your bitcoin wallet with us. We enjoyed your digital ignorance.”

Pattern recognition is defined by the logic of preemption and prediction. Sensation submits to the politics of parameters. Nonetheless the society of control is never totalizing but can rather be disrupted and subject to hacks, leaks, infrastructural sabotage, and the like. We’re sinking further and further into the online nightmare, driven by privacy and security myths. Will we ever get rid of information? At what point do we simply become indifferent to data, any data and just exist, without being monitored, sending out data, receiving updates of our newsfeeds? Computational rules orchestrate power in society. Systems of measurement determine our sensory world. Regimes of calculation can and will be hacked. Disruption underscores the logic of control and it is hard for us to think the two together.

As Paul Virilio asserted, the car is producing the accident. In the same fashion, the network produces the hack. Is there a way to escape this logic? If we cannot overcome the inevitable, would it be possible to politely remove ourselves from the scene and enter a different ball game altogether? How can we disrupt the disrupters and skip over the security hole? If money is already digital and the nation’s fiat currency is yet another cryptocurrency, how will it be possible to ever escape “surveillance capitalism”? Can we introduce “collective forgetting” as a design category? Deleting data is one option, but how to prevent data storage in the first place? Data are remarkably similar to the other big World War II invention, the nuclear bomb: after its proliferation there can be containment, and even disarmament, but the knowledge is out there. The anchorage inside the human condition is a fact and becomes non–reciprocal.

Anticipatory technologies populate the society of sensing. Governance is outsourced to the machine, bringing into question the function, relevance and perhaps even existence of governments. In Ridley Scott’s *Blade Runner* (1982) the orchestration of society and the generation of replicants are placed in the hands of the Tyrell Corporation. There’s no need for government–as–state in the dystopian worlds of Phillip K. Dick. Nowadays it’s the algorithmic modulation of populations via Facebook that wins elections, not some stooge politician out on the hustings.

Both populists and autocrats establish national intranets aimed at cultural suffocation – a sealed network in which closure is everywhere and imagination a forgotten relic of another world. We could set aside this archaic response as an historical atavism, and return our attention to planetary computation and focus on the merits of corporate globalization. However, the current world system is collapsing and national algorithmic sovereignty is on the rise. "Internet independence" speaks to diverse audiences. These national social media, along with other platforms that might pertain to the regional, are being built with the sole purpose of population control and financial surveillance. This is not about the protection of national software industries. Starting with the Great Fire Wall in China, there are now similar policies in place from Iran, Russia, Turkey, and Saudi–Arabia to the UK.

Collective isolation of entire populations remains an effective way to rule, albeit the oversight might no longer be 100% effective. Even the most explicit forms of censorship are filed under the rubric of "governance." The aim is not to exercise power but to ban online contingency through self–censorship. In this age of digital hegemony, there is no such thing as safety and absolute control. Systems are dynamic and never perfect. As long as the national–alternative solution offers impeccable service and instant comfort, the illusion of missing out does fade away and the new normal sets in. As long as the promise of prosperity remains intact, mind control and perception management are not perceived as such and can even generate a sense of safety. Most important is the actual experience of information density and social relevance inside the closed world. Information (and value) exchange can indeed reach unprecedented levels, up to the point of exhaustion.

We don't have to be part of the elite to understand the merits of the slow food movement and the cultural trend to log–off from the machine. Humans need a break and have an incalculable possibility to abandon their platform obligations and banal online habits overnight. The organizational intelligence of the umbrella movements in Hong Kong (2014) signals well how to accomplish political life off–the–grid. Using something as straightforward as Bluetooth communication protocols makes it possible to reclaim an element of infrastructural autonomy that refuses to be captured by the centralizing architectures of data centers and engines of inspection. Such actions demonstrate how contingency haunts regimes of infrastructural power. They are indeed interventions hiding in the light. The desire and

compulsion to find ways of working around apparatuses of control can, at times, foreground how flaws and sites of rupture are internal to the workings of the machine. In this regard we don't need to invest hope in the utopian imaginary that another world is possible. That world is *right here, right now.*