
THOMAS FLICHY DE LA NEUVILLE. DIGITALISING THE WORLD: THE ERA OF INVISIBLE POWER* // *English version of the article was submitted by the author for the bulletin "Russia and the Moslem World."*

Keywords: digitalising the world, cybernetic era, hackers, digital technology, technoliberalism, hybridizing, personalised marketing, captology, 5G, hybrid civilizations.

Thomas Flichy de La Neuville,
PhD(History & Geopolitics),
Rennes School of Business

Citation: Flichy de La Neuville T. Digitalising the World: The Era of Invisible Power // Russia and the Moslem World, 2020, No. 3 (309), P. 23–36. DOI: 10.31249/rmw/2020.03.02

It is clear that digitalising the world, which interconnects people and equipment, represents a major transition within our civilisation. It is changing the ways in which power is exercised, partly concealing it from public view. Hackers operate anonymously,¹ attacking websites that collect unwitting users' information. The cybernetic era is therefore making power less perceptible² and this, in turn, makes research into this current technological shift crucially important. However, this endeavour is not without risk. There is a danger that we mistake advances in digital technology for the true vitality of a civilisation built on the

* Translation of the title is presented in author's version

¹ The idea behind all anonymising systems is to blend various network users' communications together so that they become individually indistinguishable. As a result, it becomes impossible to draw a correspondence between data and identity.

² Cyberattacks have now become so sophisticated that it is impossible to determine where the perpetrators are located. This makes it difficult to implement aggressive tactics as recommended by the latest cyber strategy white paper.

ability to breathe new life into every part of society.³ Currently, real and virtual worlds are hybridising, generating fears around human life being stripped away in favour of technology. This concern is balanced out by hopes that a form of digital humanism will arise. Invisible power⁴ is not easy to spot. One of the dilemmas faced by research into cybersecurity is that most data is not accessible to the wider public. This complex field of study can only be deciphered using the technical capabilities of the army or intelligence services. It is possible to overcome this barrier by exploring the sources of information at either end of the chain. Upstream, a small number of philosophers are reflecting critically on the digital world. One example is Bernard Stiegler, who considers that the internet is a disruptive technology⁵ in that digital automation leads to tax avoidance and unemployment. Eric Sadin, meanwhile, defines artificial intelligence (AI) as a kind of rationality that interprets various situations in real time in order to continually propose services and products. This technoliberalism aims to mould behaviour. Lastly, Kave Salamatian sees the internet as a many-tentacled beast with a hyper-connected heart, whose underwater infrastructure provides an indication of the state of digital geopolitics.⁶ Downstream, various blogs and websites testify to the current vitality of technology. It is useful to cross-reference technology website Wired.com, which is written for a non-specialist

³ Arnold Toynbee wrote that “if we were to look at the history of war techniques in isolation in Greek history, we would observe continuous progress from beginning to end, before, during and even after the growth period. We would also observe that each step on the road to progress is stimulated by events that are otherwise disastrous for Hellenic civilisation,” Arnold Toynbee, *L’histoire* (Paris: Gallimard, 1951), p. 219. Translation from the French text.

⁴ The wider public is entirely unaware of how Google’s search engine works.

⁵ Magistrate and cyber specialist Myriam Quémener examines how French law is changing in reaction to disruptive digital technology.

⁶ The Suez Canal and Strait of Malacca are strategic points for underwater cables. China, meanwhile, is only connected to the world via four points.

audience, with French websites InternetActu.net and Reflets.info, which offer a more critical reading of the subject. Various online tools also enable us to assess the evolution of digital technology, from maps of the underwater cable network that carries 99% of internet data⁷ to maps of the users of TensorFlow or Shodan.io, which provides an overview of connected devices. It is also possible to approach the gamer-hacker community⁸, which is not opposed to talking about its underground activities⁹ (although IT specialists can be reluctant to come into contact with a world quite different from their own).¹⁰ However, neither upstream nor downstream information sources are location-specific. As a result, monitoring software such as Tadaweb.com and relational mappers such as Gephi.org give us an idea of digital geopolitics in specific places. Counter-intuitively, the enhanced imperceptibility of digital power does not tend to smooth out the idiosyncrasies in connected individuals' data. Digitalisation thrives by collecting personal data on a massive scale and this, in turn, means breaking societies down into pre-identified micro-groups. Enclosing groups of individuals into online silos is a prerequisite for effective personalised marketing, of which electoral marketing is an offshoot.¹¹ Paradoxically, when human societies

⁷ The Marea network is made up of cables no bigger than a hosepipe and was completed in 2017. It links Virginia to Bilbao and currently transmits 75% of the world's current online traffic.

⁸ The website Pastebin, for instance, lists the most recent hacking operations.

⁹ Tim Jordan and Paul Taylor, "A Sociology of Hackers", *The Sociological Review* (vol. 46, no.4, November 1998), pp. 757-780.

¹⁰ People with Asperger's syndrome (a form of autism characterised by communication difficulties) are particularly likely to thrive in IT professions. Steve Silberman, "The Geek Syndrome", *Science*, 12 January 2001.

¹¹ One of Quantcube Technology's flagship products is Global Macro Smart Data, a real-time predictive platform licensed annually to users. Since May 2013, Quantcube Technology has predicted 21 election results with 92% accuracy, several weeks before the polls even opened. The start-up notably predicted that the UK would vote to leave the EU in 2016 and that Donald Trump would win the 2016 US presidential election (a fortnight ahead of time in the latter case), as well as the results of France's first round of presidential elections in 2017 and the 2018 American mid-terms.

are digitalised, their identities become more distinct, to the extent that micro-groups of connected but single-minded individuals find themselves in opposition to one another.¹² Pay close attention to it and the permanent connectivity generated by all-governing algorithms appears more belligerent than unifying.¹³ To understand this, we have to examine the digital revolution's workings so that we can sketch out the potential geopolitical consequences.

The Commercial Dynamics of the Digital Revolution

Driven by an ambition to replace human unpredictability with artificial intelligence, the digital revolution uses captology to monopolise consumers' attention and has remained largely untouched by cyber-dysfunctionalities.

Artificial Intelligence: A Trojan Horse Designed to Rob Humans of their Independence

In the years to come, the development of artificial intelligence will be flanked by the development of 5G and quantum computing. 5G is one hundred times faster than 4G and interconnects people with digital devices. It provides the conditions for everything from smart cities to automated environments. 5G is designed for the Internet of Things, such as smart cars and drones, for example. Switzerland has taken an early lead in this area, launching 338 5G masts on 17 April 2019. This technology is not without its risks, however, as it has to be

¹² Major digital platforms' most significant means of reducing friction between these different identities is to moderate users' posts. This invisible task was analysed by Tarleton Gillespie in *The Custodians of the Internet* (Yale University Press, 2018), p. 296. It consumes a huge amount of resources. Global platforms use automated detection tools to moderate content. The task of moderation itself involves flagging up offensive or inappropriate content.

¹³ Unless, of course, these virtual confrontations threaten the cybersecurity upon which foreign investments depend.

relayed every 800 metres. The waves are very high in frequency and non-continuous. China has a number of 5G-related patents. In May 2019, US President Donald Trump banned American telecoms networks from buying Huawei equipment. The US has expressed fears about wide-scale espionage and has pressured its allies to freeze out the Chinese company. However, should Huawei and other Chinese businesses be prevented from rolling out 5G capabilities in Europe, the cost to European telecoms operators would be €55 billion and 18 months of lost time. Secondly, new quantum computers (and IBM Q in particular) are rendering current cryptographic protocols obsolete. But the ten or so quantum computers currently in existence are still in the experimental stage. In the next few years, the development of AI will primarily allow it to guide consumers' choices, but also to reform state bureaucracy.¹⁴ A new science – captology – has been developed to this end.

Captology: The Art of Invisible Manipulation

AI is first and foremost about emotions.¹⁵ Algorithms turn our mental space into code in an effort to capture our attention. The origins of captology reside in the work of BJ Fogg from Stanford University, who published *Persuasive Technology: Using Computers to Change What We Think and Do* in 2003. Persuasive technologies have been designed by choice architects to nudge people's choices in a certain direction. Rooted in behavioural economics and neuro-marketing, they lend algorithms a governing power. This new economy considers our attention

¹⁴ State start-ups could find themselves at the cutting edge of government reforms.

¹⁵ For Pierre Bellanger, "software and algorithms are human thought in code. Only a third of our brains is dedicated to rational cognition. If the majority of our thoughts emerge from our unconscious, as soon as networks develop they become unmoored from reason, control and any understanding of our own thoughts. The internet is coding and connecting up our dreams." Translation from the French text.

spans as a rare and precious resource that can be used to a business' advantage when it is focused on information which, in turn, provokes a particular action. Bernard Stiegler has criticised psychotechnology that short-circuits our attention spans, as had Noam Chomsky and Edward S. Herman before him when they denounced the media's role in manufacturing consent. Captology can also build on artificially generated anxieties, such as the 'fear of missing out'. This particular fear is largely fuelled by certain aspects of modern technology, such as mobile phones and social networking sites, such as Facebook or Twitter, which enable users to constantly compare their profiles. As the world's internet usage grows, a proportion of individuals will become psychologically dependent on being online and suffer from anxiety whenever they are not logged in.

Cybercrime's Minimal Impact on Global Digitalisation

Although cybercrime is becoming increasingly prevalent,¹⁶ especially in developing countries,¹⁷ groups of hackers rarely manage to paralyse organisations or states for long periods of time. In reality, cyberattacks (which are often supported by states¹⁸) are a sophisticated version of three ancient practices, namely *sabotage*, *espionage* and *subversion*. Although the costs involved in these operations have plummeted, cyber-sabotage is

¹⁶ The most effective hackers operate from Israel and India.

¹⁷ Cybercrime is mostly fuelled by developing economies, which have recently become a significant force as far as fraud is concerned. Attacks originating in Brazil continue to rise, making it one of the world's five most prolific cybercrime hotspots.

¹⁸ The Tor network, which is spreading through the darknet, uses the onion routing technology that was developed by the US Navy in the 1990s. This military technology was mostly financed by the US government to promote democracy around the world. Until 2017, the US government funnelled nearly all its funding via the US Navy, the State Department and the Broadcasting Board of Governors that emerged from the CIA. As a result, major intelligence agencies can reverse data anonymising processes to uncover Tor users' true identities.

still limited in scope. It has done damage in various ways: it is now possible to blow up a pipeline, break a dam, scramble a radar, delay a nuclear programme, shut down a bank, take control of a car¹⁹ or assassinate someone by booby-trapping their mobile phone. Cyber-espionage is the real growth area: today, spies are overwhelmed by the amount of stolen data on offer, rendering them incapable of interpreting all this information shorn from its cultural context. In the world of espionage, attacks are becoming increasingly sophisticated. Certain viruses erase themselves as they go, for instance, making them impossible to trace.²⁰ They can also mutate, just like biological viruses.²¹ As for subversion, while it is easy to start a protest movement online, it is very difficult to maintain in the long run. As a result, sabotage makes it temporarily trickier for the world to go digital, whereas espionage harvests the results of our constant connectivity. Ultimately, only non-commercial subversion is capable of endangering the current digital transition, but it is too infrequently executed to pose any serious kind of threat.

Global digitalisation is rooted in market dynamics and enables power to be exerted invisibly upon connected individuals. It is aiding financial capitalism to manoeuvre towards a new international geopolitical stance.

Digital Empires vs Digital Vassal States

Geopolitics in the digitalised world are characterised by three major trends: an erosion of American power, an increase in

¹⁹ Hackers can control the automatic windows and the indicators on a dashboard, or even cause the engine to malfunction.

²⁰ According to Kaspersky Lab's predictions for targeted threats in 2019. The next viral infections will be imperceptible.

²¹ Viruses use an unstable enzyme to multiply. Because there is no corrective system to call upon, this error remains in the genome. It occurs in about one out of every 10,000 cases. Much variation therefore exists within a viral population.

Chinese power, and competition between the two to digitally colonise the rest of the world.

Eroding America's Digital Power

American power entered the virtual world via an oligopoly: GAFAM. Made up of five major businesses (Google, Apple, Facebook, Amazon and Microsoft) and founded by former hackers,²² GAFAM physically stores information.²³ As such, this big data is accessible to the US and its British relay station.²⁴ 80% of data goes through the United States. Listening stations are positioned close to where underwater cables reach land.²⁵ Cable geopolitics also reflect Chinese-American tensions,²⁶ as well as Portuguese-Brazilian wrangling for control over the former Portuguese colonies' economic market.²⁷ These cables can foster dependency among overseas territories far from major

²² Examples include Steve Jobs (Apple), Mark Zuckerberg (Facebook), Bill Gates (Microsoft) and Linus Torvalds (Linux).

²³ The internet's infrastructure is mainly made up of high-capacity underwater fibre optic cables linked up to terrestrial cables and routers. For Europe, the most important cables are those that link the continent to the UK and, from there, to the US via the Atlantic Ocean.

²⁴ To evade American surveillance, Brazil has built its own cable link to Spain. China has also built the Sea-me-we 5 cable to connect with the Middle East and, ultimately, Europe. The Huawei Marine group is laying more and more underwater cables, for instance between Brazil and Cameroon.

²⁵ Historically, underwater cabling helped the British Empire to increase its financial power. The first functional cable was laid in 1851 between the coasts of France and England with the primary aim of telegraphing stock market information. Today, the Seaborn Networks consortium has now started building an underwater fibre optic connection between Fortaleza in Brazil and Wall Street. Known as Seabras-1, the project will eventually link up to African financial markets via South Africa.

²⁶ The United States has responded vigorously to increasingly powerful Chinese investments. In 2013, the American administration thwarted plans to lay a new transatlantic cable between New York and London, to which Chinese firm Huawei was meant to contribute.

²⁷ The SACS cable has linked Angola to Brazil since February 2019, while ELLALINK connects Portugal to Brazil via Cape Verde.

population centres.²⁸ Because GAFAM behaves like a state, Denmark dispatched an ambassador to it in 2017. In reality, it is more like a kleptocracy living off stolen data.²⁹ Its hybridised belief system borrows from both left-wing libertarianism and right-wing technological determinism. The resulting techno-libertarianism is espoused by visionary, charismatic founders who generate innovative commercial offerings that are always technologically avant-garde. With support from investment funds, GAFAM spent \$58 billion on research and development in 2016. They partly owe their monopoly to the brilliant Chinese and Indian minds that staff Silicon Valley. They are still in competition with China, however, which is trying to prevent them from developing any further.³⁰ To maintain its dominant position, the US has to speed up its industrial integration with Europe.³¹ If it hopes to re-establish its digital sovereignty, Europe needs to redouble its efforts and investments. If it does not, it will have to accept strategic alliances which reduce it to nothing more than a digital vassal state.

China's Rise to Cybernetic Power as an Indicator of Rare Resources

China's demographic collapse has forced the emerging power to concentrate on technology. China is now hugely connected, and over half of its population has been online since 2017.

²⁸ New Caledonia has been linked to Australia via the Gondwana-1 cable since 2009, guaranteeing it the fastest possible communications. Orange is also planning to link French Guiana to the Caribbean.

²⁹ GAFAM's system bears historical comparison to the extremely mobile Venetian gondolier company, which was able to pass information shared by travellers to the doge.

³⁰ There are similarities between China's efforts and the way the US attempted to block the USSR's forays into the nuclear and aerospace industries in the 1950s.

³¹ It should be noted that despite its legal stability and appeal, France has not been able to create any ground-breaking innovations for the past 20 years due to its rigid labour laws.

400 million Chinese people play online games, for example. China is attempting to disentangle itself from ICANN, a legal authority based in California that regulates the internet, by boycotting multilateral meetings. Its objective is to draw a strict dividing line between the 'Chinese internet' and the 'global internet'. In an attempt to 'cleanse' the internet, the Chinese Communist Party has long sought to strengthen its grip on what it describes as information pollution and 'electronic opium'.³² Chinese internet users are online for about three hours a day, and over half of that time is spent on a mobile device. They browse and watch online videos, abandoning TV screens in favour of more nomadic options. The Chinese have outclassed the Americans when it comes to AI. AI thrives when data is collected in massive quantities, and China has huge amounts of homogenised data that enables it to outstrip the US. The country's 'social credit' system, which awards every citizen a certain number of points, will enable it to extract vast amounts of data when it comes into force in 2020.³³ Two modes of plundering data are thus going head-to-head: GAFAM pilfers our data on the one hand, while the Chinese government pilfers its own citizens' data on the other. The Chinese have the data but the Americans have the algorithms, which is why it is so crucial to the Chinese that they manage to plunder the latter or attract the very best engineers. Competition here is fierce and has left behind India, which is only responsible for developing existing programs. In order to maintain its digital independence, China restricts how its rare metals are exported and used, as these will go on to be used in the mobile phone manufacturing process. For Guillaume Pitron, the battle for rare metals is the hidden side of the digital revolution. Tensions will become particularly high in territories targeted by cyber-colonists.

³² Internet addicts are viewed as both 'deviants' who need their behaviour correcting and 'sick patients' who require medical help.

³³ This system is based on the questionnaires used by certain American insurance companies.

Major Powers Competing to Digitally Colonise Africa

If the digital colonisation process were modelled on an algorithm, it would include the following steps. First, it would facilitate a cyberattack on the target state's communications and present itself as its saviour. Next, it would connect the country to the internet, secure its strategic networks and capture local cyber elites by rolling out a master's degree programme in digitalisation. It would then pillage its data, take over the consumer market and, finally, engage in online electoral marketing to maintain its grip on its conquered market. Connectivity is growing rapidly in Africa. In 2018 alone, 35.2% of Africans were using the internet, compared with 16% in 2012. China has taken a very original stance towards Africa. First of all, Chinese businesses have provided the continent with technological tools at very competitive prices. For instance, Shenzhen-based electronics manufacturer Huawei has been operating in Africa since 1999. In 2013, it partnered up with Microsoft to conquer the African smartphone market and is now outperforming the Californian giant in this sector in Africa. Huawei's ambition is now to sell premium telephones to an African middle class looking for enhanced services. There are, however, significant differences between countries, from North Africa³⁴ to the Sahel region.³⁵

³⁴ Algeria – considered the least secure country – had to call in specialist cyber police officers to monitor its baccalaureate exams in 2017. The British are also taking an interest in this promising market and organised a cyber-forum in 2018. In 2019, Orange set up a specialist cyber defence subsidiary in Morocco: Orange Cyberdefense Morocco officially opened for business in Casablanca on 16 April 2019. A master's degree in cyber defence has been set up in partnership with the Université Polytechnique Hauts-de-France in Valenciennes to attract local talent and launch their careers. France also has a long-established presence in Libya as, in 2007, Amesys – a French subsidiary of Bull – sold its Eagle program to the Gaddafi regime to track its opponents. After changing its name to Advanced Middle East Systems, the company then sold a similar system to Egypt known as Cerebro.

³⁵ In the Sahel region, practices are changing as internet cafés offer faster internet speeds rather than access to computers. The French army ran several cybersecurity courses, including in Nouakchott, Mauritania, from 10 to 13 September 2018 and in Niamey, Nigeria, from 29 January to 3 February 2018.

The Middle East: Digital Islands and Rich Pickings

The Middle East has two digital ‘islands’, Iran and Israel, which represent opposing yet mirroring forces. Israel provides 7% of the world’s cybersecurity. Its industry benefits from high levels of investment³⁶ that aim to protect a territory stripped of its strategic importance, while also improving its ability to export innovations. On 6 May 2019, Israel sent out a warning to hackers operating outside its borders. After one cyberattack, the Israel Defense Forces bombed a building in the Gaza Strip that was sheltering Hamas hackers. This has not prevented Israel from recruiting hackers keen to offer it their services for a hefty fee. Hackers are highly coveted. In fact, Dubai even organised a hacking fair! Three former Israeli intelligence officers founded XM Cyber in 2016 to operate in this particular field. The digital island that is Israel stands in opposition to Iran, a country with equal levels of creativity³⁷ but lacking in Western investment. Iran appears to have been behind cyberattacks on certain British banks in December 2018. The viruses used – Shamoon 1, 2 and 3 – also targeted petroleum infrastructures in the Gulf’s oil monarchies.³⁸ In Turkey, the nationalist Cyber-Warrior Akincilar group has hacked anyone or any organisation deemed opposed to the interests of Turkey and Islam.³⁹ Saudi Arabia, meanwhile, has enjoyed technical support from certain Israeli cybersecurity firms, who have made use of their position to gather data on the behaviour of the country’s elites⁴⁰ or

³⁶ \$800 million in 2017.

³⁷ The word ‘algorithm’ was invented by Persian mathematician al-Khwarizmi in the 9th century.

³⁸ Cybercrime can sometimes be a proxy for military action. This was the case for these Iranian cyberattacks, which were designed to relieve pressure on the country during the embargo.

³⁹ They hacked into *Charlie Hebdo*’s website, for instance, in 2011.

⁴⁰ In 2017, representatives of Herzliya-based NSO Group Technologies held a series of meetings in Vienna and at least one Gulf nation, during which a \$55 million contract was signed to supply Saudi Arabia with its famous Pegasus spyware.

opponents.⁴¹ Despite the protection offered by these Israeli companies, Saudi Arabia is now the most frequently targeted Middle Eastern country when it comes to cyberattacks,⁴² which mostly aim to steal information from private and public institutions' information systems.

The growth in digital power offers a very imperfect reflection of each state's real clout: GAFAM's rise covers up for the United States' geopolitical decline, while China's technological power conceals its demographic fragility. Conversely, in both Africa and the Middle East, hacking operations designed to steal digital or financial resources reveal the weaknesses of supposedly powerful forces.

Social digitalisation rates are therefore a better reflection of the resources that are immediately available rather than their future potential. The internet has become a bitterly contested space among competing economic powers. The aim of this competition is to effectively privatise a space that is temporarily free for users to explore. Permanent connectivity, which devours instant data and interconnects objects and reified human beings, bypasses anyone who refuses to accede and labels them as suspicious. In future, states and individuals will generate a fog of incorrect data in an act of defiance designed to shield themselves from view.⁴³ Finally, digitalisation is throwing up unexpected

⁴¹ Jamal Khashoggi and Omar Abdulaziz wanted to set up a cyber-opposition movement.

⁴² The lack of local training and a general lack of awareness of the dangers of cyberattacks have left the kingdom exposed.

⁴³ Voice cloning is now a reality. Using a single minute of recorded audio, Lyrebird and Wave Net can digitally recreate an individual's voice to have him or her 'say' whatever they want. Similarly, Stanford University has demonstrated facial control in which a person's facial expressions are recorded live but edited by an actor, with a computer instantly reproducing the latter's movements yet with any target person's face. Such deepfakes can attack individuals, organisations and states. University College London has developed its *My Text in Your Handwriting* program to accurately reproduce a person's handwriting from a single sample. A talking robot named Luka mimics the characters from the TV series *Silicon Valley*, recycling dialogue from the first two seasons. The robot responds to questions by generating new phrases based on

geopolitical changes. Ultimately, it will sweep away repetitive jobs and temporarily concentrate power in innovative territories, while making it possible for states and businesses to identify opinion leaders using relational mapping. Lastly, it will enable military chiefs to order robots to kill targets using AI-powered facial recognition. We are entering into the era of hybrid civilisations.

the models provided to it. In 2022, it is believed that populations in developed nations will read more fake news than genuine information. Automatic text, image and audio generators could contaminate the entire human communication network. 8.5% of Twitter accounts are already run by bots.