

Huawei, Big Brother and Technological Self-Destruction

5G is just the latest innovation giving powerful forces more ability to monitor and control our lives.

Andrew Nikiforuk | The Tyee | February 2019

Some of Canada's strategic allies, including Australia, the United States and New Zealand, [have banned](#) China's high-tech firm Huawei Technologies from supplying [5G technology](#) for reasons of national security.

The threat is real. But that's only part of a crazy *Black Mirror*-like story of the introduction of a technology that threatens to make the world a more fragile and authoritarian place than it has already become.

The U.S. made its decision to shun Huawei in part based on a 2012 report by the U.S. House Intelligence Committee that [found](#) neither Huawei nor ZTE, another Chinese tech giant, were "willing to provide sufficient evidence to ameliorate the Committee's concerns" about their ties to the Communist Party of China (CCP). [Australia](#) and [New Zealand](#) followed suit last year after political scandals over Chinese interference in their national affairs.

Typically, Canada has yet to make a decision and is reviewing the matter. The issue is complicated by a U.S. request [to extradite](#) Huawei's chief financial officer, Meng Wanzhou, to face bank and wire fraud charges. She was released on bail in Vancouver and is under 24/7 surveillance while awaiting a hearing.

Two major Canadian telecom carriers, Telus and BCE, have [invested heavily](#) in Huawei technology, while [13 Canadian universities](#), (including UBC, University of Victoria, Simon Fraser and University of Toronto) are using computing services or receiving research funding from the company.

Huawei [maintains](#) Canada can't say no to its technology for delivering 5G next generation wireless service and rejecting it "would set Canada's wireless competitive advantage back years."

Officially, the Chinese complain that the Americans are playing geopolitical games with vital technology and that Canada, "a frightened bird," has got caught in the middle.

"Having conjured the accusation that the Chinese company represents a national security threat out of thin air, it has roped in its allies as accomplices in its fear mongering," thunders the China Daily. "The attacks against Huawei are now unabating and unceasing."

Technologies the key to building empires

Technologies help to forge empires while dominant empires, in turn, help to spread technologies that speed and extend the process of colonization.

In the 1950s, the French historian and Christian radical [Jacque Ellul](#) warned that technology threatened the very existence of civilization as it became a self-directing, autonomous and totalitarian force in human affairs.

The weight of "technique" had grown so great, wrote Ellul, that it would tolerate no obstacles and broach no criticism. Ellul's definition of "technique" was broader than just machines and devices. He included any efficient method for organizing humans — from electoral polling to genetic engineering.

Because all social and political life would eventually get caught in the web of interconnecting technologies, it was "impossible to foresee all the consequences" of any new technique, he wrote. He noted that the movement to replace the natural with the artificial and the different with the same was relentless.

As new forms of technology "absorb an enormous number of phenomena and brings into play the maximum data," they create economic monopolies warned Ellul. These monopolies, in turn, impose more disruptive change on humans because everything must be subordinated to technology.

Ellul considered networks of technologies to be the world's most powerful colonizer and the greatest threat to human freedom.

The principle tenet of technique, said Ellul, was boldly amoral: “Since it was possible, it was necessary.”

And 5G technology will play a key role

The [fifth generation wireless technology](#) — thus 5G — offers far greater speed and the ability to connect to massive numbers of devices of all kinds. It’s considered essential for self-driving vehicles, the Internet of Things and uses not yet imagined.

Last week the China Daily, a propaganda arm of the Communist Party of China, [announced](#) the arrival of another technical marvel in the country’s modernization campaign: a self-driving bus in Chongqing in southwestern China. The paper even provided a video of a 12-passenger vehicle moving down the street, guided by laser radar. But 5G technology, with its high-speed connectivity, is needed to move autonomously. Huawei helped develop the bus.

Last August, the Australian government [released](#) a disconcerting statement about 5G technology. The curious announcement effectively banned Huawei from installing 5G technology in the country without citing the firm by name. The Aussies just noted that companies “who are likely to be subject to extrajudicial directions from a foreign government” wouldn’t be permitted to install 5G technology in their telecommunication carriers.

But the government press release first praised 5G’s benefits, portraying the technology as an elixir that “will improve the daily lives of Australians, strengthen our connectivity and accelerate our networks.”

Moreover, the new technology would “underpin the development of smart cities and the [Internet of Things](#),” the government enthused, and also connect “industrial control and safety of life systems, like remote surgery and autonomous vehicles.”

Who, after all, would want to live in a dumb city or feel left out by not having their rectal thermometer connected to the vast Internet of Things?

The government then described the price of these conveniences. It noted that 5G technology would so radically change mobile networks that the technology would

“increase the potential for threats to our telecommunications networks” and that the threats would multiply over time.

Previous generations of mobile networks generally consisted of a secure core, including data routing and access control, while the edge consisted of devices such as laptops and phones. But 5G technology erases those boundaries in order to connect smart homes and driverless vehicles to the Internet of Things.

Which, the Australian government concluded, “provides a way to circumvent traditional security controls by exploiting equipment in the edge of the network — exploitation which may affect overall network integrity and availability, as well as the confidentiality of customer data.”

Progress builds complexity, and complexity invites fragility.

China, technology and state control

No country in the world has employed technology to control its citizens as effectively and systematically as China. Since 2015, China’s Ministry of Public Security has begun to roll out a “[social credit system](#)”. The program, which will include facial recognition for 1.3 billion people, awards every citizen a digital grade based on data collected on their behaviour, purchases, social media habits, political views and even traffic fines. Good or “sincere” citizens, as defined by the Communist Party of China, can skip a medical wait line or rent a car without a deposit. Insincere citizens, who jaywalk, don’t pay their debts or criticize the state, will lose their right to fly or book a train ticket. (To date, as many as nine million blacklisted citizens have been denied train travel.)

“At its core, the system is a tool to control individuals’, companies’ and other entities’ behaviour to conform with the policies, directions and will of the Communist Party of China,” [notes](#) an astonishingly blunt 2018 report by the Australian Strategic Policy Institute. “It combines big-data analytic techniques with pervasive data collection to achieve that purpose.”

Samantha Hoffman, an Australian China scholar and author of the report, noted that China’s social credit system “is not only an issue of political influence and control internationally. It’s also a human rights issue, and new legislation should reflect that. Through contributions to smart cities development in China, for example, Western companies are providing support to build a system that has

multiple uses, including uses that are responsible for serious human rights violations.”

Hoffman’s report also argued that “steps must be taken to shield overseas Chinese communities from the kinds of CCP encroachment that will only proliferate with a functioning and tech-enabled social credit system.”

Companies like Huawei and WeChat make such “technology-enhanced authoritarian control” possible, just as Facebook and Apple do in North America.

“Chinese tech companies operate because the Chinese Communist Party allows them to,” Hoffman [told](#) an Abu Dhabi newspaper.

It does not matter if a company, or the individual leadership of a company, is indifferent toward the Party — they are still legally responsible to the Party.”

She added that the fact that Huawei operates in other countries carries not only national security risks but also threats to civil liberties.

The Chinese empire is now ascendant while the United States struggles with the weight of its own former greatness. In *Telecommunications and Empire*, author Jill Hills argues that after the Second World War and into the 1990s, the U.S., as the “world’s dominant economic and military power, attempted to restructure the international market of telecommunications to expand its direct and indirect control over the domestic markets of other governments.” It strived to “create a world in its own market image.”

Why would China behave any differently?

5G technology empowers Big Brother

Huawei is a global leader in developing 5G technology. Founded in 1987 by Ren Zhengfei, a former officer of the People’s Liberation Army and a military technology researcher, the company has become a global behemoth operating in 170 countries and selling more cellphones than Apple. It generates revenue of \$125 billion a year and employs 170,000 people.

The company is aware of the security concerns. In an unusual [New Year's greeting](#), its chairman Guo Ping declared that Huawei “has never and will never present a security threat.”

“We must not be discouraged by malicious incidents or temporary setbacks and must remain determined to achieve global leadership,” he said. “Setbacks will only make us more courageous, and incredibly unfair treatment will drive us to become the world’s number one.”

Guo warned that 5G markets “that choose to not work with Huawei — they will be like an NBA game without star players. The game will go on, but with less deftness, flair and expertise.”

“We will achieve what we’ve set out to do — to bring digital to every person, home and organization for a fully connected, intelligent world,” he said.

He did not acknowledge that a fully connected world allows state or corporate surveillance of every citizen’s activities around the clock and brings us closer to China’s social credit system.

In 2017, a group of Finnish technicians [laid out](#) the security risks posed by 5G technology, no matter which corporation is providing it. It echoes the concerns of the Australian government and UK authorities.

They noted that every generation of wireless technologies posed different security challenges.

But as 5G allows the connection of billions of devices to the so-called Internet of Things “the security threat vectors will be bigger than even before with greater concern for privacy,” they concluded.

As more and more devices are connected, they noted, “A security breach in the online power supply systems can be catastrophic for all the electrical and electronic systems that the society depends upon.”

The implementation of 5G will make computer air traffic control, delivery drones, virtual reality, self-driving vehicles, smart factories, robots and health care more dependent on interconnected devices. But their connectivity also makes them more vulnerable to security threats, the report said.

And the changes all put personal privacy at risk, as a 2015 [white paper](#) by Huawei acknowledged. “As open network platforms, 5G networks raise serious concerns on privacy leakage. In many cases, privacy leakage can cause serious consequences.”

Making technique faster, smarter and more efficient can only increase the power of the modern state and the corporations it now serves.

Well-connected in Canada’s Liberal Party

The Liberal Party of Canada has close ties to Huawei, which strategically located its research centre in Ottawa nearly a decade ago. Before his [resignation](#) last month, Scott Bradley, a Liberal candidate in 2011 and one of the nation’s top lobbyists, served as the company’s Canadian senior vice-president of corporate affairs. The former telecom executive also sat on the board of the Canada-China Business Council, which promotes investment between the two countries. (It was created by the power-brokering Demarais family.)

Bradley’s sister-in-law, Susan Smith, [co-founded Canada 2020](#), a Liberal Party [forum](#) where politicians, industry representatives and lobbyists network for a “progressive” hi-tech world. It is partly funded by Huawei and other corporations.

Prior to his abrupt departure, Bradley did his best to defend Huawei, which aims to dominate the \$26 billion 5G technology market in Canada.

“By banning Huawei, are you worried about China’s emerging technology leadership?” he [said](#) in December. “That’s a legitimate issue — perhaps you are. So how do you deal with that? Are you worried about how China will use technology for other purposes or around the world? ...That’s again a legitimate issue regarding why you should be understanding what China is up to. But by banning Huawei do you address those issues?”

John Manley, a former Liberal foreign affairs minister, sits on the board of directors for Telus, which has invested heavily in Huawei technology. After the arrest of Meng Wanzhou, Manley [suggested](#) the government should have just let her slip by authorities despite the U.S. arrest warrant, the same way Justin Trudeau is accused of pressuring the Attorney General to look the other way on

SNC-Lavalin's criminal activity. "I think it was a good opportunity for a little bit of creative incompetence on the part of Canadian authorities and somehow just miss her," said Manley.

Globalists will always defend the legal or illegal forces of globalization.

Trading freedom for smart thermostats

Technological society proceeds at its own pace with outcomes that steadily erode human freedom and crush the human soul. Various techniques deliver comfort and conveniences the way a household of slaves once did. But their greater and unified purpose is to exert total power over our lives in a technical environment. We have become slaves to a growing network of spying screens that modify our behavior with every click.

Harvard business economist Shoshana Zuboff calls our new tech master "surveillance capitalism." She considers it a "rogue force driven by novel economic imperatives." But the evidence from China and Western democracies suggests there is nothing rogue about it: technique manifests a tyrannical character everywhere regardless of its owners.

Ellul understood the monster at work and warned 50 years ago that in a technological society every human being will become a crop to be farmed and harvested by imperial technique because all human acts and thoughts "must be the object of human techniques."

Ellul was not a pessimist, but a realist. Only when the sleepers awake, will there be hope, he wrote.

"If an increasing number of people become fully aware of the threat the technological world poses to man's personal and spiritual life, and if they determine to assert their freedom by upsetting the course of this evolution, my forecast will be invalidated."

But the rise of Huawei and the imposition of 5G technology suggests that the technical noose on human affairs has just grown tighter.

We should call 5G technology by what it will make possible: "technology-enhanced authoritarian control with global consequences." 🍌

Sidebar:

5G'S POTENTIAL HEALTH RISKS

5G technology only works over short distances, and so requires from four to 20 times as many antennas as the current standard. As a consequence, it will substantially increase the public's exposure to radiofrequency electromagnetic fields.

Telecommunication companies have typically downplayed the effects of exposure to electromagnetic fields, saying there is no risk. But many independent scientists [warn](#) that increasing exposure can lead to “increased cancer risk, cellular stress, increase in harmful free radicals, genetic damages, structural and functional changes of the reproductive system, learning and memory deficits, neurological disorders, and negative impacts on general well-being in humans.”

In a letter to the European Union, Martin Pall, professor emeritus of biochemistry and basic medical sciences at Washington State University, [raised concerns](#) about 5G's health effects. “Here we have strong suspicions of similar or more severe risk... but we have no biological safety testing of genuine 5G radiation. Therefore, we have no risk analysis or risk management because we have no risk assessment whatsoever on 5G.”

The European Union [refused](#) to do a study, partly on the grounds that “the primary responsibility for protecting the public from potential harmful effects of electromagnetic fields remains with the member states.”

— A.N.