RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 029 – 22 February 2018

The Fourth Industrial Revolution: An Orwellian Nightmare?

By Tan Ming Hui and Walid Lemrini

Synopsis

Recent development in technology may turn our reality into a dystopian Orwellian nightmare - should we worry about it?

Commentary

IN GEORGE Orwell's *1984*, the protagonist Winston carefully keeps his back to the telescreen in his living room, to stay out of detection in the fear of certain punishment, as he begins writing in his diary. Fear of the "Big Brother" watching is not anything new, but for this generation living in the age of the Fourth Industrial Revolution (4IR), the dystopian masterpiece may make one feel an eerie sense of familiarity and foreboding.

The rapid development of new technologies could enable, or already is enabling, totalitarian-style surveillance and control to silently creep into our everyday life.

Use or Misuse of Technology?

Recent developments in disruptive technologies such as Artificial Intelligence (AI), big data analytics, and quantum computing have symbolised the advent of what many have referred to as the 4IR. Presage of an ongoing global societal reorganisation, the 4IR and its actors are paving an uncertain path regarding the impact technology will have on our lives in the years to come.

On the one hand, the 4IR will make our lives easier. New technological breakthroughs could be synonymous of better-designed strategies to tackle climate change or medical treatments to diseases like cancer.

On the other hand, the 4IR sparks an ethical debate on the risk the use of modern technologies by states, companies, and individuals represents to people's privacy and freedom. Increasing use of surveillance technology, progress in big data analytics, machine-learning and deep-learning (in term of image and voice recognition), have enhanced the capacities of states and corporations to profile individuals.

Through the Internet of Things (IoT) and the way people use online platforms such as cloud services and social networks, data are collected and turned into antecedents by states and companies. States through collecting data on their citizens can better localise and predict risks to social stability, such as terrorist threat, tax frauds, and more.

Companies, by analysing massive sets of data on their current and potential clients, can also implement well-informed business strategies. Yet, the potential for misuse of these data is very real.

How Real the Orwellian Nightmare?

In June 2014, the Chinese Communist Party (CCP) announced that it wanted to implement an experimental 'Social Credit System' (SCS) ranking Chinese citizens based on their level of trustworthiness. To do so, the government, with the support of eight private companies (among which Alibaba's affiliate Ant Financial Services Group that operates Alipay), has aimed at collecting data on its citizens' daily activities.

As such, Chinese citizens are to receive a score between 350 (worst score) and 950 (best score) depending on their expenditures, the people they associate with, their political stance, or even whether they jaywalk in the streets. Based on these scores, people are rewarded or punished, as the scores will determine their chances to get into universities, to get a job, or even apply for a loan.

The SCS, which Beijing wants to make mandatory from 2020, rests on the fast growth of China's technological sector, making the most of programmes such as *'Xue Liang'* (meaning Sharp Eyes) to develop an almost omnipotent 'Police Cloud'. This not only serves the government's agenda to cultivate obedience, but also enables better monitoring of political dissidents.

Even Democracies…

Democratic countries like the United States and the United Kingdom have also made the most of surveillance technology, but have been less transparent about it, as suggested by the Snowden affair. In May 2013, the affair shed light on the secret Prism operation involving American and British intelligence.

Tapping into the database of Internet giants such as Microsoft, Facebook or Google, the US and the UK gathered the personal information of millions across the globe. This sounded an alarm which prompted people to think about the risk involved when states and companies collect data on the most private parts of their lives.

Meanwhile in Japan, in preparation of the 2020 Tokyo Olympic Games, the Abe

administration has approved in March 2017 a controversial legislation which makes it easier to arrest individuals on the basis of plotting and committing one of 277 crimes. Prime Minister Shinzo Abe has defended the revised bill in the light of increasing terrorist threats.

However, those crimes include "conducting sit-ins to protest against the construction of apartment buildings" and "mushroom picking in conservation forests", activities not exactly terrorist-related. In response, the Tokyo Bar Association has expressed its stark opposition to the new legislation, pointing to potential government misuse.

Security versus Privacy Debate

The security versus privacy debate seems to continue endlessly. Some people may be more prepared than others to give up some degree of privacy in exchange for security. For example, countries that have had traumatic experiences with terrorism and public violence could be less concerned about their governments collecting intelligence for the promise of greater national security.

This is especially if, in their mind, they are not the targeted group marginalised by criminal profiling. In the wake of 9/11 terrorist attacks, the American public was generally supportive of the Patriot Act, which unprecedentedly expanded the US government's surveillance powers to prevent another similar attack.

However, public support of the act dropped overwhelmingly after Edward Snowden exposed that the surveillance system's collection of metadata was so intrusive that it encroached the privacy rights of all US citizens, even the millions of "innocent" ordinary people.

Hence, the key here seems to be promoting greater public education and awareness, and maintaining a minimum standard of government transparency.

Taking Matters into One's Hands?

To ensure impartiality and transparency, as well as to navigate the moral risks of surveillance and data collection, one tends to fall back on the rule of law and the justice system to enhance the accountability of policymakers.

More importantly, people could also make use of new technologies to empower themselves and regain control of their personal data. For instance, blockchain technology, in combination with cryptography, is a possible mean of deterrence to safeguard privacy. It allows us to store data in an encrypted, transparent, and verifiable way, making sure that records of transactions between two parties are permanent and unmodifiable.

However, as trust in government wanes across the world, there needs to be an independent authority that can be trusted to keep the provers neutral. The provider of such validation technologies can be NGOs or the civil society.

Estonia provides a potential model for countries grappling with new technological advancements and the many ethical implications. The small Baltic country runs a

highly efficient and secured e-government system, by setting clear legal parameters to protect personal information and promote data transparency.

It looks like the technological revolution is here to stay, and instead of being trapped in an Orwellian nightmare, perhaps it is time for people to confront the reality as it is and make the 4IR theirs.

Tan Ming Hui is an Associate Research Fellow in the Office of the Executive Deputy Chairman and Walid Lemrini is a student research assistant at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg