RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 086 – 23 May 2018

The Fourth Industrial Revolution: Its Security Implications

By Cung Vu

Synopsis

The term "Fourth Industrial Revolution", alternatively known as "Industry 4.0", is a buzzword nowadays but what does it actually mean? What are its security implications?

Commentary

THE TERM "Fourth Industrial Revolution" (FIR) is a buzzword introduced by Klaus Schwab during the World Economic Forum in 2016. It is defined as the convergence of technologies to blur the lines between the physical, digital, and biological worlds. It is also used interchangeably with the more popular term "Industry 4.0" coined by the German government in 2011.

In fact, it is the convergence of underlying technology domains of nanotechnology, biotechnology, information and communication technology and cognitive science where the whole is greater than the sum of its parts.

Security Implications of Industry 4.0

The security implications of the FIR are too complex to fully grasp. These technological waves are coming fast and leaders, whether in private sector or in public service, need to be prepared. The major concern is what happens to the economy and job distribution. However, there are other security implications leaders need to be aware of to develop informed policies and strategies.

Let's peel off each layer of the FIR "onion" one by one. As the security implications are both deep and wide, the following are only highlights of the security aspects of the underlying technology domains.

Nanotechnology: A technology conducted at the nanoscale (one nanometer is equal to one billionth of a meter), materials at this dimensions behave differently from bulk properties. Nanotechnology is used to produce nanomaterials, smart materials, nanoelectronics, nanosensors, nanodevices, nanomedicine and so on.

Nanotechnology has numerous homeland security and defence applications. It is used for detecting potentially harmful materials, finding pathogens in water supply systems, or for early warning and detoxification of harmful airborne agents. Nanomaterials are used to build lighter and stronger armour and parts for vehicles, equipment, and aircraft. Nanomaterials also allow building of smaller, more powerful rockets, bombs, and other explosive devices.

Biotechnology: Biotechnology is a broad discipline in which biological processes, organisms, cells are exploited to develop new technologies and products that help improve our lives.

Biotechnology has advanced such that personalised drugs could be developed based on individual DNA. We are now not only able to sequence and synthesise DNA, but also edit it. We can not only modify existing life but also create new life from scratch. This has very grave implications as potential new viruses could be created from the laboratory.

Information and Computing Technology (ICT): It seems that almost all aspects of our life now depend on the ICT. The Internet-of-Things allows endless connectivity to improve how we work and live. As a result, our dependency on the digital world has made us more vulnerable. Cyber attackers could exploit such vulnerability to serve their purposes, which could include cyber theft, cyber crimes, cyber attacks, influencing public perceptions, or terrorism.

Cognitive Science: The interdisciplinary, scientific study of the mind and its processes. Advances in the development of human-machine interfaces, algorithms, and power sources as well as other components are making robots readily available for personal and industrial use.

Brain stimulation drugs have been used as cognitive enhancement to keep soldiers alert for days without sleep. Amphetamine and Fenethylline, nicknamed "the jihadists' drug," are known to be taken by terrorists in suicide bombing missions or to allow them to go to battle not caring if they live or die.

Technology Convergence: The security impacts of technology convergence are virtually limitless and the following example is only for illustration purposes:

Enter the Humanoid: New Arms Race?

Artificial Intelligence (AI): One of the technology intersections which receives a lot of attention is artificial intelligence where "intelligence machine" could be created to

operate and react like a human being. That means a machine could see, hear, talk, learn and reason.

This leads to the fear that human jobs, both blue and white-collar, would be lost to robots or even the human race could eventually be taken over by robots. Only time will tell. In the near term, as machines get smarter and smarter, the potential threats are also gradually increased.

Comparing to cyber security, artificial intelligence security risks are much more critical. The new arms race has begun. As president Putin put it “Whomever becomes a leader in this sphere will be the master of the world", Russia has exploited AI in cruise missiles and drones. AI could help in analysing both satellite and radar data to find, detect and counter targets hundreds of miles away.

China is incorporating AI in autonomous unmanned aerial systems. Their drone swarms could utilise neural networks to deny the US the freedom of navigation in the South China Sea. The US also leverages AI in its Third Offset Strategy to develop cutting-edge technology for military and intelligence purposes.

Homeland Security Front

In the homeland security front, attackers are using AI to study and learn about the target, identify vulnerabilities to generate hacks. Let’s take a look at a few areas of AI:

In *speech recognition,* a startup company named Lyrebird has developed an algorithm that can mimic anybody’s voice after analysing a few pre-recorded audio clips. It can read text with intonation and punctuation.

In *visual recognition*, computer scientists were able to exploit AI to modify or synthesise images to impersonate people online. When both audio and video technologies combined, they could be used to generate fake news to persuade public opinions or to fabricate terrorist propaganda.

In *machine learning,* scientists have demonstrated that AI-generated malicious links outperform human competitors in terms of composing phishing tweets, distributing them over the cyber space and victimizing more users.

In another area of machine learning, researchers have pointed out many *pattern recognition* algorithms are very easy to be manipulated to trick computers, and the implications are scary.

For example, the visual sensor/machine may interpret a “STOP” sign as a “YIELD” sign or “100 km/hr” as “20 km/hr” speed limit sign when a slightchange such as noise is introduced to a pattern learning algorithm. Think of the scenario if you are in an autonomous vehicle approaching an intersection or on a highway and in front of a-18 wheeler truck travelling at a very high speed.

At the moment, the machine could achieve super-human performance in narrow domains. Machine learning will continue to make progress to perform in complex

situations but the negative side is we do not know how it will behave when encountering situations outside its programming parameters.

Way Forward

There is a need for public and private sectors, policy and technical experts to communicate to address the security risks from the current industrial revolution.

Leaders could provide continuous workforce education in multiple disciplines such as data analytics, biotechnologies, automation, computer science, artificial intelligence to enhance societal resilience, to mitigate job risks and to prepare for unknown challenges. Public awareness is also critical in order to maintain social order in adverse situations.

As we are still struggling with establishing sound protocol and governance of cyber security especially in the international governance realm, the situation is exacerbated in artificial intelligence. It remains a huge challenge as states continue to maintain or develop rules and regulations to their own advantage.

Cung Vu PhD is a Visiting Senior Fellow at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. He is also a consultant for the Hawaii Natural Energy Institute, University of Hawaii and has served as Associate Director at the Office of Naval Research Global in Singapore.