Why China's new cybersecurity law is a threat to international businesses & innovation

George Haour writes on China and cybersecurity and the potential ripples in the way China does business

China has the world's largest market for digital shopping, mobile payments, and internet-enabled financial services. Close to 400 million people in China do most of their payments using their smartphones. China's overall business in information technology is a market of well above USD $300 billion, and it is estimated that more than 700 million Chinese have access to internet. So any law impacting the online space—cybersecurity included—will make ripples in the way China does business.

That's why its new cybersecurity law—due to take effect in June of next year—is particularly alarming. It is part of an ongoing government program to reinforce China's cybersecurity, and arguably targets non-Chinese hackers. But it comes amidst continuous tensions between the US and China, not just in terms of cybersecurity (each country has accused the other of hacking), but with trade, the economy, and, of course, the US election, which will inevitably change how business is done between the two nations. The law appears to be counterproductive in several ways.

First, as the law sets forward, important network equipment and software will have to receive government certifications. This means that specific pieces of intellectual property or technical features will have to be divulged, which could easily be passed on to Chinese companies by the regulators behind cybersecurity. It shouldn't be forgotten that the state in China has tremendous power and plays a critical role in economic plans. Government interference is much more prevalent than in Western nations. And under the veil of cybersecurity, regulators will have access to proprietary information that could benefit Chinese firms at the expense of foreign business.

The type of businesses most at risk will be those with special hardware and systems for network management. But it could even include data from and for ATMs. New generation ATMs have a much higher level of connectivity with mobile integration and face recognition. This makes them more vulnerable to hacking and means confidential devices and information will have to be used for protection. And under this law, that creates a big entry place for government snooping.

This law is also counterproductive because companies gathering data in so-called 'critical areas' will have to store that data inside China. At this stage, the definition of 'critical' is worryingly broad. Complying with this requirement will force international firms to make expensive investments to build duplicate facilities within China. This is in total contradiction with the free flow of data, expected to swell in 2020 after the introduction of 5G.

International companies will have to weigh this risk against the opportunity to do business in China. China has had a long reputation for 'copying' without getting insider access, and this law could only open the ease to which China's business sector can review competition. For international companies there is no easy way forward as the choice is black or white. Either foreign companies will comply, knowing China has a way to peek into what previously was private, or they will choose to stand by principles of privacy at the risk of being excluded from the Chinese market. Despite the challenging dilemma, companies are likely to comply and give in to China's demands. The market is too huge and far too ripe for future growth, especially when compared to more stagnant outlooks in Europe and the US.

In addition to creating barriers for international business in China, this kind of legislative move goes completely against innovation

In addition to creating barriers for international business in China, this kind of legislative move goes completely against innovation. It could well be considered to be part of what is called 'indigenous innovation' in China. This consists in favouring Chinese firms by establishing non-tariff barriers, such as specific standards or regulations on products, in order to prevent non-Chinese firms the access to China's large and dynamic market. And the impact would be wide-ranging, from consumer electronics to products such as equipment to produce renewable energy, including windmills and solar panels.

Innovation involves a complex process, but it requires a society to be as open as possible and to allow vibrant exchanges between people. While cybersecurity is important, this law will wrap around the free market as it grips security. Within China, entrepreneurs are, by and large, not bothered by their government's management of the internet, called the 'great firewall'. However, this new law is a new step to tighten the government's grip on the internet. Furthermore, far from favouring China's champions in this very dynamic area, such as Huawei, Lenovo, or Tencent, this law will handicap them in the long term. Maybe the hope is that these companies themselves will fight to alter the law and mitigate the negative implications for China's internet landscape.

US companies have already began to strongly lobby against the law, as well as China's position that the internet must be managed by authorities. But despite the efforts of any company, Chinese or other, the cybersecurity law is just a piece in a larger ongoing political puzzle that companies will have to deal with. Trump's stance on trade is equally, if not more, alarming for business. In the end, agility will be key for companies to succeed in the tense political environment. ■

Georges Haour is a Professor of Technology and Innovation Management at IMD business school and co-author of the new book - Created in China: How China is Becoming a Global Innovator (Bloomsbury, London, 2016).