# Regulators and criminals crowd cyberspace in 2018

By Nicolas Reys

**In the traditional Chinese game of Go, two players capture territory by placing stones at intersections on a grid, and seizing ground faster and more shrewdly than their opponent. In 2018, the cyber landscape will be all Go, but the opponents won't be two friends engaging in a bit of harmless rivalry. Governments will be playing against business on the field of cyberspace.**

Governments have been steadily carving up cyberspace for years, encircling new territories and drawing ever higher virtual boundaries. 2018 will continue in the same way. New, non-tariff barriers will hamper businesses everywhere, while compliance requirements run the risk of distracting from cyber adversaries.

But now there is an accelerant in the mix: increasingly rapid digitalisation – and the mushrooming of social media in commerce – will prove too powerful a trend for governments and regulators to resist.

Official responses will vary. Some governments will see social media and cyberspace as the enemy, and try to entrap them. Others will try to turn the power of social media and digitalisation into a tool of influence, or balance it with individual and democratic freedoms. All these efforts will encroach on business. In 2018, this will start to pinch.

We will see the first large fines or regulatory sanctions targeting companies that don't comply with the fragmented rules of the new cyberspace. At the same time, global, fast-spreading cyber-attacks – affecting hundreds of organisations worldwide – will increase in frequency. This will complicate organisations' efforts to navigate the digital domain. Worse, it will distract defences and provide attackers with more opportunities.

Regulation and social media manipulators will place significant pressure on their intended targets. As businesses absorb attempts by governments to control their patch of cyberspace, they risk leaving themselves exposed to malicious actors that will take advantage of their distraction to attempt ever more destructive and targeted attacks. The large-scale disruptive attacks of 2017 (WannaCry, NotPetya) were unfocused and messy. Those of 2018 won't be.

## How social media is transforming governance

Digital risks have grown on a global scale in the past two years. 2016 saw the digital manipulation of the US electorate. 2017 saw WannaCry and NotPetya. Nation-states see these attacks as threats to both their sovereignty and control of a digital space crucial to their ability to govern. Furthermore, these attacks confirmed the scepticism and concerns that they have felt all along towards the new digital world. This pushed governments to implement one of three governance strategies in 2017:

1. **Let it go.** In the West, regulatory strategies have sought to balance freedom of speech and expression against the fear that social media and digitalisation are agents of chaos and division. Even the toughest legislation (the General Data Protection Regulation (GDPR) in Europe or New York State's cyber security regulations for banking) is based on protecting citizens' rights and safety.
2. **Go forth and conquer.** Russia, the Philippines and several states in the Middle East have tried to maintain as much control as possible over domestic public discourse. They have also weaponised social media and digitalisation into tools of propaganda. This approach often includes disseminating pro-government views across social media platforms – sometimes at great effort and expense – while monitoring for dissent to track and punish anti-government views.
3. **Stop and Go.** A few key exceptions aside, Asian and Central Asian countries have looked to control social media and the domestic digital space. This approach does not rely on the active use of social media to impose a government agenda. The chosen path here is to monitor, censor and legislate to create containment, national boundaries and protectionist policies. This, the thinking goes, mitigates the potential impact of social media and digitalisation on the domestic environment.

Asia leads the planet in the dynamism and pace of its embrace of technology. The continent is home to the largest number of internet-connected devices – also known as the Internet of Things (IoT). Its connected population has overtaken its peers in Europe and America. But Asia's embrace of the new is not just a fad. It is an economic engine, and a flywheel that must keep spinning freely to drive Asia's growth and development.

The Asian flywheel, though, is not frictionless. A significant number of governments in the region see a connected and digitised world as a threat to the very existence of their societies. They point to the mixed experiences of countries that have taken a more relaxed approach to governance, and adopt the Stop and Go strategy in response.

Between 2014 and 2017, significant legislative reforms affecting the digital space took hold in China, Japan, Vietnam, the Philippines, Hong Kong and South Korea, to name a few. Recent examples of new ways Asian countries are tackling digitisation include the declaration on 30 October 2017 by the Cyberspace Administration of China that [internet] service providers and private sector companies must work with the government to punish employees publishing illegal content online.

This follows the push for the broad data protection and cyber security law in China known as the Chinese Cyber Security Law. This law creates strict operational controls and compliance requirements for many organisations operating in China or holding a large amount of data pertaining to Chinese citizens.

In Europe, the new GDPR was created to protect the privacy of European citizens. But despite the best of intentions, the GDPR has had an unintended effect. Companies scrambling to comply with the new regulation have taken their eye off cyber security, at precisely the time cyber threat actors are sharpening their focus on European businesses.

In the US, businesses are navigating a new environment at home and abroad. Congress doesn't look eager to impose strong cyber security regulations, but some states do. At the same time, US businesses continue to be the main target of data breaches. Uber and Equifax are two recent examples that paradoxically signalled the problems of not having a cohesive data protection stance at the national level.

Meanwhile, Russia is flexing its online muscles. 2017 saw an unprecedented number of cyber attacks attributed to the Kremlin or Kremlin-linked agents. Three pieces of legislation passed last year will force businesses and citizens to adapt to a tightly controlled cyberspace and social media environment. The year ahead is key for Russia's online strategy. Ongoing cyber conflict with Ukraine provides a laboratory for cyber adversaries to test new weapons for deployment elsewhere, in a more targeted and effective manner.

## Pay to play – how a fragmented global approach hurts businesses

To create or capture new territories in the game Go, players need to balance internal and external tensions while remaining vigilant for their opponent's next move. Players must decide whether to create small and secure spaces, or to take on a less secure but more global position to cover a larger area of the board. A similar dilemma on cyberspace and social media governance across the world was visible in 2017. Its consequences will begin to show for businesses in 2018.

For multinational organisations with infrastructure and funding large enough to operate on a global scale, complying with competing regulatory frameworks will have a direct financial cost. For smaller businesses operating across only a few geographies, or focusing on a specific region, the main cost will be a loss of opportunity.

At their worst, cyber governance strategies being implemented across the digital space will hurt innovation and slow technological progress. As they stand, none of these strategies are likely to benefit the security of organisations and citizens. Threat actors have already demonstrated their ability to adapt to changing environments and exploit a distracted business community to launch attacks.

Despite these challenges, technology and digitalisation continue to grow. As that growth accelerates, it may derail efforts by governments to fragment the digital landscape. Until they do so, businesses must keep cool heads. Compliance is important, but so too is the resilience and security of their organisations. One should not distract from the others.

**Nicolas Reys**
Associate Director
✉ nicolas.reys@controlrisks.com

### About Control Risks CORE

CORE provides incisive analysis and forecasting on geopolitical and security issues, comprehensive country risk ratings, an extensive database of incidents, plus visualisation and analytics tools.