Black swan in the Cloud

‘To regulate and to protect’, **Michael Haba** discusses the challenges of regulating cloud-based critical infrastructures

Late modernity is said to be fascinated with risk. By permeating our society, risk has found its way into our daily lives – affecting our thinking and/or decision-making. In this ‘risk society’, regulators are tasked with the anticipation and control of risks, and risk-based regulation has become the bread and butter of any regulator. However, such regulation will not and cannot result in the anticipation and management of all risks, because of a number of issues – one of them is the frequent focus on the known and available while a blind eye is being turned to the unknown and unpredictable. So what if a ‘black swan’, a highly unpredictable and rare event, but one with a high impact, appears?

State and non-state actors have paid increasing lip service to the importance of protecting critical infrastructures, that is systems and networks that make up the infrastructure of today’s society, such as banking and finance, energy, water or telecommunications. One typical justification for more intrusive regulation is rooted in the understanding that both security and reliability of critical infrastructures are regarded as public goods that would be under-supplied in the absence of any kind of state intervention. However, this raises the issue as to what should be considered a critical infrastructure. The increasing significance and widespread use of new technologies including (but not limited to) The Internet of Things (the internet working of a variety of connected devices) and Cloud Computing (on demand access to shared computing resources and data) have renewed regulatory interest in information infrastructure and its protection from cyber risks.

Over the past few years, cyber-related incidents have enjoyed considerable attention, ranging from security breaches to email systems (such as Yahoo), the hacking and releasing of politically salient information (such as the release of the Clinton campaign emails) to attacks on banking systems (such as Central Bank of Bangladesh, and more recently Tesco Bank and Lloyds Bank in the United Kingdom). According to professionals in the field such as computer scientist W. Daniel Hillis or former US cyber security advisor Richard Clare, modern society has already become over-dependent on information technology. Consequently, legislators and regulators worldwide have started to treat information infrastructures in the same way as more traditional ones, such as water and energy. The contemporary challenge is to develop laws and regulations to prescribe what ought to be considered as critical and how operational risks that emerge from these critical systems should be adequately addressed and managed.

Risky Cloud business?

While regulators try to anticipate and manage risks, business people are located at the other end of the spectrum: Many of them are natural risk-takers, because taking high risks usually involves the prospect of high profits. Yet, introducing a new product in a market is a risky venture. For example, to build, operate, and maintain information infrastructure that is fit for the purpose of Cloud Computing, namely a relatively global infrastructure that enables a convenient and on-demand provisioning of shared computing resources to multiple customers, is currently both a knowledge-intensive and costly (usually) private enterprise involving both substantial investment in technology and human capital. It follows that the market for providing global information infrastructures has very high entry barriers. It is therefore not surprising that only a few large multinational corporations operate in this market.

Having made these investments, it is imperative for these corporations to fill this infrastructure to capacity as quickly as possible. In order to do so, they will seek to attract large industrial or institutional customers from the public or private sector, including ministries of defence, other ministerial departments, regulatory agencies, local governments, universities, health services, and large industries such as the automotive industry, utility companies or banks.

However, such a business approach leads to a situation where a small number of providers are responsible for the operation of a ubiquitous service on which societies critically depend. But the regulatory concern does not stop there.

Cloud Computing may give rise to systemic, if not existential crisis due to its inherent complexity. This complexity increases the risk of system-wide failures which in turn can trigger cascading failures across critical infrastructures: Firstly, Cloud Computing is based on virtualization technology, that is the process of transforming physical hardware resources into a pool of virtual resources that can be shared by many clients. As a technology, virtualization is brought to life on the basis of complex interactions between a plethora of technical components that have been rigidly designed and involve issues concerning resource, performance, and security management such as scaling of system and network resources, task scheduling, fault and security isolation, as well as data confidentiality and integrity management. Being a tightly coupled and interactive large-scale system, Cloud Computing is thus intrinsically vulnerable to disruption.

Secondly, cumulative dangers exist because of inter-sector dependencies, particularly in cases where the large institutional customers of Cloud Computing service providers are themselves providers of critical infrastructures and to a significant extent relying on Cloud Computing to operate their critical infrastructure services.

It follows that a disruption of the upstream Cloud Computing infrastructure is likely to cause a disruption of the downstream critical infrastructure, in the worst case bringing about a multi-sector infrastructure collapse. At its worst, this could constitute a catastrophic event.

Is the Cloud a black swan?

Are we therefore dealing with a risk of a black swan event that is worth watching out for? Should we worry about a highly concentrated global market for large-scale Cloud Computing services for providers of international, national and local critical infrastructures? Some will argue that the probability of the occurrence of such a catastrophic event is too remote. Others will point to the ‘failure of collective imagination’ that is said to have been at play during the financial crisis of 2007–8. They would therefore advocate some form of intervention in view of potentially unpredictable consequences of conditions in which complexity meets interdependence. The financial sector has explicitly addressed issues associated with the built-up of systemic risks. Yet, other regulatory spaces are still to follow suit.

Given the uncertainties involved, regulators and regulated critical infrastructure service providers would be highly imprudent to turn a blind eye to Cloud Computing as an emerging new technology that needs to be far better understood in terms of its risks and potentially systemic effects. Resorting to methods of trial and error seems to be the least feasible option. Instead, approaches of risk mitigation might take the route of highly prescriptive standards applying to critical infrastructure providers when it comes to questions of availability, disaster recovery, and business continuity. The important question here has to be whether or not the high expectations created in elaborate plans and reported ‘readiness’ will be dashed when a black swan appears in the Cloud.

Michael Haba is an MSc Regulation alumnus. He is writing in a personal capacity.