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 anticipa-
tion and control of risks, and risk-based regulation has become the broad 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, ap-
ppears?

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 understand-
ing that both security and reliability of
critical infrastructures are regarded as
public goods that would be under-sup-
plied 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 devic-
es) and Cloud Computing (on demand,
access to shared computing resources
and data) have renewed regulatory in-
teres in information infrastructure and its
protection from cyber
risks.

Over the past few years, cyber-related
incidents have enjoyed considerable at-
tention, 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 Hills or
former US cyber security advisor Rich-
ard 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 contem-
porary challenge is to develop laws and
regulations to prescribe what ought to
be considered as critical and how op-
erational 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 lo-
cated at the other end of the spectrum:
Many of them are natural risk-takers,
because taking high risks usually in-
volves 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
local infrastructure that enables a
convenient and on-demand provision-
ing of shared computing resources to
multiple customers, is currently both a
knowledge-intensive and costly (usu-
ally) private enterprise involving both
substantial investment in technology
and human capital. It follows that the
market for providing global informa-
tion infrastructures has very high entry
barriers. It is therefore not surprising
that only a few large multinational com-
panies operate in this market.

Having made these investments, it
is imperative for these corporations to fill
this infrastructure to capacity as quick-
ly as possible. In order to do so, they
will seek to attract large industrial or in-
stitutional 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 in-
dustry, utility companies or banks.

However, such a business approach
leads to a situation where a small num-
ber 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 sys-
temic, if not existential crisis due to
its inherent complexity. This complex-
ity increases the risk of system-wide
failures which in turn can trigger
cascading failures across critical infra-
structures. Firstly, Cloud Computing is
based on virtualization technology, that
is the process of transforming physical
hardware resources into a pool of virtu-
al resources that can be shared by many
clients. As a technology, virtualization
is brought to life on the basis of com-
plex 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 isola-
tion, as well as data confidentiality and
integrity management. Being a tightly
coupled and interactive large-scale sys-
tem, Cloud Computing is thus intrinsi-
cally vulnerable to disruption.

Secondly, cumulative dangers exist
because of inter-sector dependencies,
particularly in cases where the large
institutional customers of Cloud Com-
puting 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 up-
stream Cloud Computing infrastructure
is likely to cause a disruption of the
downstream critical infrastructure,
in the worst case bringing about a mul-
tiple system failure collapse. At its
worst, this could constitute a cata-

crophic event.

Is the Cloud a black swan?
Are we therefore dealing with a risk of
a black swan event that is worth watch-
ing 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 inter-
vention in view of potentially unpre-
dictable consequences of conditions in
which complexity meets interdepend-
ence. 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, reg-
ulators and regulators critical infra-
structure 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, ap-
proaches of risk mitigation might take
the route of highly prescriptive stand-
ards 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 elabo-
rate plans and reported ‘readiness’ will
be dashed when a black swan appears
in the Cloud.

Michael Haba is an MSc Regulation al-
umus. He is writing in a personal capacity.