Crédit Agricole Group economic and sector analysis

Prospects

Aperiodic – no. 20/050 – 18 March 2020

The point of view

Smart connectivity and data: the major challenge of digital security

Digital technology and innovation – including cloud computing, artificial intelligence (AI), the Internet of Things (IoT) and, soon, 5G – are speeding up the digital transformation of businesses and, more broadly, the economy and societies around the world. This is reflected in large-scale changes in every area and emerging new behaviours, all of which is happening very fast, disrupting social and economic stability.

All this requires appropriate communications infrastructure built on upgradeable and more agile network architecture that harnesses new digital technologies[1].

Paradoxically, while these remarkable digital developments and transformations are making such infrastructure more open and agile, they are also making it more vulnerable to cyberattacks. More intensive generation, collection, processing and consumption of data is creating loopholes at various points in networks, including end users' mobile devices. This entails risks and heightens the critical need to secure infrastructure and control the use of data.

Data and artificial intelligence: Europe on the offensive

At this point in time, the United States and China are dominating the data war, with their platforms handling huge volumes of subscribers' personal data. Even though the battle for control over personal data seems, in my opinion, to have been lost, Europe has nevertheless responded by putting in place the General Data Protection Regulation (GDPR), successfully implemented on 23 May 2018 with the aim of controlling the processing of personal data and protecting private individuals.

On 19 February 2020, the European Commission unveiled its strategies in support of a European digital transformation reflecting its fundamental values of openness, fairness, diversity, democracy and trust. This strategy notably encompasses critical infrastructure and cybersecurity. The goal now is thus to make Europe a major player in AI and the data economy.

The massive expansion of the industrial IoT will trigger an exponential rise in the production of industrial data. With the rapid growth of 5G networks, the advent of edge computing and huge progress in algorithmic data processing, Europe is keen to – and, indeed, must – seize its chance to become a major player in the management of industrial data: its supremacy in this global war for control over data depends on it.

Edge computing, or intelligence at the edge of networks

Data generated by sensors connected to the IoT is sent to processing centres for storage, analysis and use. These centres consist of servers and computers, generally installed in a data centre.

[1] SDN (software-defined networking), NFV (network function virtualisation), APIs (application programming interfaces) and edge computing (where computation and information processing happen at the edge of the network, as close as possible to the end user).

Thanks to technological developments, hardware located at the edge of networks now also has built-in computing power and analytical capability as well as being able to passively store data. In other words, data can now be processed directly as close as possible to its source – for example, a voice assistant or a driverless vehicle.

Edge computing notably reduces latency and the energy cost of using infrastructure, both key factors in the development of future services, the most advanced of which include driverless vehicles and smart transport.

Smarter, more flexible connectivity is undermining network security

The evolution of network architecture, with many functions now virtualised and reconfigurable via software, the cloud and the IoT (particularly the industrial IoT), has significantly increased the number of points at which hackers and other cybercriminals can access networks. Making intelligence and data accessible at the edge of networks further heightens this risk. Furthermore, our own mobile devices and laptops, if not properly protected, are potential gateways.

Connected objects, the cloud and all supply chains – particularly for on-demand services (such as SaaS, or Software as a Service) – all constitute vulnerabilities and are therefore cybercriminals' favourite targets. According to a recent survey, the number of cyberattacks on supply chains surged 78% in 2018 alone.

This means all critical (IT and telecoms) infrastructure at banks, telecoms operators, energy suppliers and government bodies is a prime target. Note that in 2018, 34% of cyberattacks worldwide targeted the finance and technology sectors. It is also estimated that 35% of cyberattacks around the world in 2018 were launched from IP (Internet Protocol) addresses in the United States and China.

Industrial espionage has always existed, and this is not about to change. In a highly competitive environment where business and geopolitics intermingle, achieving global technological supremacy means mastering AI and 5G.

Consequently, and to protect assets where their customer and business data is stored, all businesses and governments must meet the challenges posed by cybersecurity and infrastructure security. Otherwise, they run the risk of losing their customers' fundamental trust. ■

Rabindra Rengaradjalou
rabindra.rengaradjalou@credit-agricole-sa.fr

Consult our last publications

Date	Title	Theme
11/03/2020	China is slowing down in the short, medium and long term	China
04/03/2020	The power of "animal spirits"	Economics
03/03/2020	France – Residential real estate: recent developments and outlook for 2020	France, real estate
26/02/2020	Can flexible packaging do without plastic?	Sectoral
19/02/2020	Portugal – The country's momentum continues	Portugal
12/02/2020	US election pages – February 2020: how do you outmanoeuvre an elephant…	USA
11/02/2020	Italy – 2019-2020 Scenario: Consumption to the rescue of growth	Italy
06/02/2020	Italy: how many votes are the "Sardines" worth – 6,000, 250,000 or 25%?	Italy
06/02/2020	France – Pension reform: What impacts will the reform have? What issues are still unresolved?	France
05/02/2020	Italy – Monthly News Digest	Italy

Crédit Agricole S.A. — Group Economic Research
12 place des Etats-Unis – 92127 Montrouge Cedex
Publication Manager and chief Editor: Isabelle Job-Bazille
Information center: Dominique Petit - **Statistics:** Robin Mourier
Contact: *publication.eco@credit-agricole-sa.fr*

Access and subscribe to our free online publications:
Internal Website: https://portaileco.ca-sa.adsi.credit-agricole.fr/en
Website: http://etudes-economiques.credit-agricole.com
iPad: Etudes ECO application available in App store platform
Android: Etudes ECO application available in Google Play

This publication reflects the opinion of Crédit Agricole S.A. on the date of publication, unless otherwise specified (in the case of outside contributors). Such opinion is subject to change without notice. This publication is provided for informational purposes only. The information and analyses contained herein are not to be construed as an offer to sell or as a solicitation whatsoever. Crédit Agricole S.A. and its affiliates shall not be responsible in any manner for direct, indirect, special or consequential damages, however caused, arising therefrom. Crédit Agricole does not warrant the accuracy or completeness of such opinions, nor of the sources of information upon which they are based, although such sources of information are considered reliable. Crédit Agricole S.A. or its affiliates therefore shall not be responsible in any manner for direct, indirect, special or consequential damages, however caused, arising from the disclosure or use of the information contained in this publication.