PATRICK NICOLET

Group Chief Technology Officer and Group Executive Board Member of Capgemini

Thomas GOMART

Donc Patrick si tu le veux bien, je te donne la parole pour commencer.

Patrick NICOLET

In this short exposé, I would like to present an enterprise point of view on cyber power. Let us start with a definition that you can find in the latest Ifri report on digital power which was supported by Capgemini: Cyber power, also known as digital power, is defined as one's ability to exploit digital data to contribute to modify the behavior of others on the international scene and to achieve one's goal. Despite its immaterial nature, it has very concrete implications on the real world.

States strive to keep cyber power as one of their prerogatives due to the competitive advantage they get from controlling the networks. Historically, states who have managed to shape and control networks have proven to be more successful in the long run as exemplified by the British naval power which emerged in the XVI century and was at the foundation of the British empire dominance over the world for centuries. All governments today see cyber power as sovereign and strategic on par with nuclear forces.

States focus primarily on infrastructure: e.g. *data centers* as exemplified in a report published last year on the geopolitics of data where we showed how, in the aftermath of the Snowden scandal, governments all around the world have launched data centers building plans to relocate their most sensible data within their national borders. *Submarine communication cables*: The US and the UK can access at least one quarter of the transatlantic communications thanks to their early and massive investment in submarine communications cables. *Network*: States also control the strategic communication signals and decide to whom and under which conditions they can be used (e.g. US-China trade war and the limitations to the usage of Huawei 5G technology)

Eventually though, governments are including data and AI as an element of their cyber power portfolio, for better and worse, e.g. China's social control system relies heavily on its ability to capture, analyze and store data about its citizens. Technologies such as video surveillance and facial recognition can be used to expose and shame wrongdoers on a big screen at a crossroad. China's cyber power goes beyond its frontier as it exports its "smart city" (which in China is called "safe city") to other countries, especially in Africa.

Today, companies live in a permanent state of aggression with advanced persistent threats coming from governments or organized crime, or even combined as for North Korea. This is aggravated by new regulations such as the Network and Information Security directive adding around 10% costs to the enterprise IT budget (before fines!) and notwithstanding potential reputation damages.

Despite the governments' efforts to retain it, a large part of cyber power is now owned by a very limited number of companies. While states focused primarily on infrastructures, tech giants were built on software with the like of Microsoft, Amazon Google and Facebook. The source of their wealth resides in revenue from software licenses, retail and monetization of insights on consumer data through advertising. They have however expanded to the infrastructure world, directly competing with governments, e.g. Amazon went from selling books to becoming a selling platform for all vendors and eventually built its own cloud service, promoting the so-called "as a Service" model.

As a result, these companies have acquired an overwhelming share of cyber power which impacts the way they are being perceived in the physical world: *The size*: Facebook claims 1.59 billion people daily active users in June 2019, allowing Mark Zuckerberg to joke with Indian Prime Minister Modi about the respective size of their "populations". *The wealth*: Altogether, the GAFAM's revenue is higher than the GDP of France, the UK or Germany. Individually they're

close to countries like Indonesia (~1000B USD). Google and Amazon have invested over 40B USD in the last 12 months for R&D and capital expenditure. Apple and Facebook over 25B USD. *The power struggle*: States want to regain control through tax and regulations, e.g. U.S. Democratic presidential candidate Elizabeth Warren called for dismantling the GAFA, in the wake of recent data-misuse scandals.

The same is valid for the Chinese tech giants: The only country that can today compete with the USA with companies such as Tencent, Alibaba, Xiaomi or Baidu. It is worth noting that in the case of China, there is alignment between the State and these Tech giants

Moving to digital infrastructure, i.e. clouds, become the norm and is a complex undertaking. Once the transition is done, the different security and data protection requirements such as GDPR increase again significantly your costs of operations, notably because you have very little bargaining power against the tech giants (lock-in effect).

All industries have the potential to become cyber powers. Despite all the risks and the downsides, enterprises are embarking on extensive digital transformation to avoid the disruption by new entrants and to stay in tune with their clients who are accustomed to the consumerization of IT. It helped them generate new revenues and be more agile to operate in a Volatile, Uncertain, Complex and Ambiguous (VUCA) world as mentioned yesterday by J-P. Agon. Traditional companies can become the cyber powers of tomorrow: In a connected world, limits between economic sectors will morph into new ecosystems, e.g. automotive industry is currently structured around three assets, engineering, supply chain and distribution. Tomorrow, it will be electric, autonomous, connected and will need to be associated to a large range of services. Data management, ownership and valuation will determine who will be the winners.

To conclude, I will say that he emergence of new cyber powers in these future ecosystems is one of the biggest risks in our business as the value is shifting online. The USA and China have clear strategies and the means to execute. The battle for data, the only asset in your information system, is the next one and must be won. Not in a defensive way with regulations but by enabling our industry incumbents to become the next generation of cyber powers. The decision of the European Commission to block the plan for a Siemens-Alstom rail merger is highly questionable in this context.

Thomas GOMART

Thank you, Patrick. I think your very last point on Alstom and Siemens could be a very interesting point for our debate.