Walter Amedzro St-Hilaire

Digital Risk Governance

Security Strategies for the Public and Private Sectors

Springer

Digital Risk Governance

Walter Amedzro St-Hilaire

Digital Risk Governance

Security Strategies for the Public and Private Sectors

Springer

Walter Amedzro St-Hilaire
Chair of Institutional Governance & Strategic Leadership Research, Canada
Northwestern University, USA
University of Ottawa, Canada
PRISM-Pole SEE, Paris 1 Pantheon-Sorbonne University, France
ExpertActions ExiGlobal Capital Group Co, UK

ISBN 978-3-030-61385-3 ISBN 978-3-030-61386-0 (eBook)
https://doi.org/10.1007/978-3-030-61386-0

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

This book is affectionately dedicated to
Maedge, Swincy, Shéa and Élodie,
Thank you for existing!

Preface

The fifth generation of mobile phone standards is heralded as a breakthrough innovation. Faced with a certain amount of excitement, it is important to identify the real stakes behind the concept – quite marketing – of "5G revolution".

The IMT-2020 standard aims to answer the question of the limits of 4G, while being in its extension: it does not correspond to a major technological leap. It is therefore a question of evolving in continuity in order to meet the challenges of the limits of the current standard, which are those of congested networks in areas with high point traffic, such as during large gatherings, the ability to provide network access to a large number of connected objects, and the existence of excessively long latency periods.

It should be noted that mobile technologies have evolved at the same pace as technological innovations and social demands: the deployment of 5G should thus accompany the ultra-connectivity of society, as the fifth generation of mobile phone standards will go further than just increasing speeds. The impact should be significant not only in technical terms, but also for the economy and society.

The book did not wish to address all the questions raised by the technological dynamics: mobile networks are increasingly at the heart of citizens' daily lives, which raises many political, economic, societal and territorial cohesion issues, particularly around their uses.

However, it can already be noted that the ultra-high-speed connection will make it possible to do more than just improve the quality of ultra-high-definition video broadcasting: it will in fact guarantee coverage of specific needs in various sectors as well as uses linked to the Internet of Things. Communications between a large number of connected objects should be facilitated, and this in the context of more reliable networks with very low latency. For the innovation introduced by this technology lies first and foremost at this level: enabling massive communications, almost in real time, thanks to the optimization of frequency bands by more complex digital modulations and better beam pointing. These advances should lead to the coverage of specific needs in sometimes critical sectors.

However, in addition to the concerns associated with the exposure of individuals to radio frequency electromagnetic waves, there is another major issue: that of digital security and the security of the accompanying Internet networks.

Indeed, initially developed on libertarian theoretical bases, and built on a decentralized technical architecture (allowed by technological progress), the digital and the Internet have undergone significant changes since the mid-2000s: recentralization of the web, around closed systems and proprietary technologies, development of applications, "platforming", and, above all, the emergence of large private players (benefiting from powerful network effects that support their offers of new services and digital tools). These digital giants – the (American) Gafam and the (Chinese) BATX – are now outperforming enterprises in traditional sectors in terms of financial valuation. They are reaching an unprecedented number of users (Facebook claims 2. 5 billion active users each month).

Far from the egalitarian and individualistic utopia of the beginnings, cyberspace and the digital world are nowadays the place where conflicts of interest, struggles of influence and antagonistic (economic and social) logics take place. In short, the return in new forms of the very classic competition for power. States, with the more or less ambiguous support of these digital giants, are thus developing strategies of domination, independence or autonomy in cyberspace.

At the population level, the now widespread deployment of digital tools poses (among other things) a real democratic challenge (for the expression of the general will). These tools can disrupt the political game by facilitating new modes of action for specific and targeted attempts at interference or manipulation: the theft of data and their public dissemination during presidential elections in some countries bears witness to this. Also, the so-called Cambridge Analytica case shows the danger of unscrupulous methods of mass data collection, analysis and cross-checking for the purpose of influencing political choices.

More generally, the absorption of attention by techniques that target each second of "available brain time" with dreadful precision can lead to fears that, in the long term, the time spent on the Internet will be reduced (in 2019, on average, a Singaporean spent 38 hours a week on the Internet). We must often acknowledge the disarray of political power in a society where digital technology is profoundly changing the behaviour and modes of democratic participation, particularly among the younger generations.

How, in this context, and in the face of formidable competitors, can we maintain an autonomous capacity for assessment, decision and action for institutions and enterprises in cyberspace? How can we guarantee sufficient "informational autonomy" for citizens and businesses that are increasingly dependent on technical intermediaries whose operations are often opaque?

This book has endeavoured to identify, on the one hand, the fundamental fields of digital security for institutions and enterprises (whether individual or collective), and to outline, on the other hand, the means of regaining it (whether they are covered by regulation or the implementation of public policies). It must be said that despite the intangible nature of the web and "cyberspace", the Internet, which allows its deployment, is still territorially anchored, giving power to the public

authorities: the network depends on essential strategic physical assets (data centres, cables, etc.) which require considerable investment and are at least partly governed by national legal systems; the active equipment and protocols used (for data communication or encryption) comply with technical standards negotiated within international bodies.

The dominant digital enterprises are themselves nationalities (Gafam in the United States and BATX in China) and are also subject to the constraints of local legislation, often extraterritorial in scope, or even competing (Cloud Act vs RGPD). Technologies (artificial intelligence) and human resources (engineers, programmers, etc.) are developing thanks to research and innovation ecosystem in which the national public authorities have their full share (public funding, links with defence industries or innovation agencies, training programmes and universities).

No door is therefore closed to the cyber risks of institutions and enterprises: technology and software, including algorithms, do not marginalize them, even if some institutions and enterprises are (as is often the case in high technology and science) on the cutting edge. Infrastructures are accessible to them (it is even a paradox): public money (national, local, public and private) finances universal networks accessible to all, thus ensuring the development of the Gafam, the first users of the information highways! Finally, while the market for digital services is dominated by the large North American players, not all of them are, far from it, in a lasting dominant position (at least in theory).

However, the balance of power today places some countries in a very special position. For the United States, it is a question of asserting world sovereignty, strengthened by the creation of the originally libertarian net (but financed by the Defense Department, at the price of accepting monopolies, which are so contrary to the historical practice of the United States), and a permanent and worldwide hunt for talent and nuggets – since "the winner takes all". For China and Russia, the assertion of sovereignty is expressed in a different, more defensive and sometimes more subtle way.

This geopolitical situation leaves little room for a still ill-defined institutional strategy: between the China–US duopoly of digital giants, investment capacities remain marginal in the other countries of the world. The emphasis is therefore on the defence of values (a demanding conception of privacy), and the main lever remains (by default) negotiating access for businesses to coveted domestic markets. Similarly, the defence that countries promote against cyber threats and cybercrime is the recognition of the application of the principles of international law in the cyber field and multilateralism. They try to win their partners to these lines of action and promote, without naivety, cooperation between friendly countries, with the appropriate reserve for vital and strategic sectors.

In this context of competition in cyberspace, the book also discusses strategies to respond to threats (to institutions and enterprises). These risks are also reflected in the questioning of the economic order, the legal order, and the tax and monetary system. Finally, the book considers how digital security (the ability of the institution and enterprises to act in cyberspace) can be exercised in its two dimensions: 1. the ability to exercise sovereignty in digital space, which is based on an autonomous

capacity for appreciation, decision and action in cyberspace (and which corresponds de facto to cyber defence), and 2. the ability to manage digital tools in order to master data, networks and electronic communications.

Finally, the book proposes a principle and a method of action: a 3-year appointment, precise and urgent measures in the field of data protection, and a reform of the regulations aimed at reinforcing digital security. It also proposes action on the levers of innovation and multilateralism to optimize the digital security of institutions and enterprises.

Walter Amedzro St-Hilaire

Acknowledgement

The author thanks Northwestern University, World Bank Group and the Chair of Institutional Governance & Strategic Leadership Research for funding this research.

Introduction

In the wake of the Snowden case and its cascading effects, attacks against high-visibility websites have multiplied and public opinion has become aware of the emergence of a new type of risk (digital security breaches). Before that, incidents revealing increasingly spectacular digital security breaches have multiplied throughout the world: theft of personal data files and credit card numbers from major distributors (Target in the United States, etc.) and at major telephone operators (to the extent that ExpertActions ExiGlobal Group has stated that these were not fatal incidents but rather incidents involving the responsibility of the person holding personal data).

However, beyond what can be attributed to attacks, it appeared that large operators were cooperating with states to deliver personal data and, more seriously, were engaging in trade in personal data (either as a result of very incomplete information about the rights of their customers or without their knowledge). These repeated incidents, these deliberate strategies, are beginning to move the citizen, who gradually understands that he is not the fortunate user of sophisticated techniques designed to protect this personal information, but rather a target.

However, wouldn't these doubts have positive effects, since the need is only perceptible in the crisis? One might think so in view of the indifference of the population, enterprises and governments to digital insecurity before the revelations of Mr Edward Snowden (on the occasion of the "Prism" affair) partially awakened these various actors. It is now possible to mention some major flaws in digital governance, some attacks, without being suspected of unbridled imagination or technical perfectionism hampering efficiency. This makes it possible to be listened to with more attention. This should make it easier to impose new security requirements on company staff and to improve compliance with the instructions of the security services (issued by specialists placed with high-level political or economic leaders).

However, until then, the emphasis was rather on seduction in the service of extensions of digital uses through a mechanism that was always the same: possibilities to increase one's capacities, to cure incurable diseases, etc. According to the Chair of Institutional Governance and Strategic Leadership Research, the use of connected objects dedicated to health could save us 6 months of life expectancy in

the coming years. Several experts recognize the development of self-medication but refuse to see the consequences of the development of digital health care. Similarly, Google has undertaken a tour of the world's small and medium-sized enterprises, of which only 51% have an active website, arguing that the most active online businesses could grow and export "up to twice as much" as the average.

Without any specific proven knowledge of nanotechnology, Google X embarked on a research project on nanoparticles to diagnose diseases such as cancer. In passing, Google X did not fail to collect a maximum of personal data on the health status of potential users of its medical diagnosis. And this discovery is certain and monetizable. Indeed, sometimes, other aims emerge according to ExpertActions Group: what Google wants with the generation of autonomous cars is to capture the time that motorists spend in their car. And capture the personal data that goes with it.

However, this is still nothing compared to Google's goals, which focus on the development of knowledge on demand (information reaching people before they even look for it). According to the Chair of Institutional Governance and Strategic Leadership Research, the search engine of the future will be the perfect personal assistant that will give you the benefit of all the technical knowledge, improving your thinking process. For the reluctant, ExpertActions Group says people should be taught to swim with the current of technology, not to fight it, especially since the Internet has made people more productive.

When it is not the improvement of health or human capacities, it is the savings resulting from the reduction of water, electricity, gas and fuel consumption that are put forward, or the reduction of wastage and waste. The economy could also benefit from the development of connected cities supposed to offer a new market of $4.5 trillion in 2025 (study by Chair of Institutional Governance and Strategic Leadership Research).

At other times, the digital revolution is dressed in the colours of the industrial and societal revolution. ExiGlobal Capital Group recommends that enterprises at the forefront of their respective markets be able to vampirize themselves rather than be vampirized by others. Steve Jobs, Apple's founder, understood this perfectly, and even theorized about it. Failure to do so could lead to what is emerging in urban transport, where the movement to open up public data (open data with Etalab) has led Google to take an interest in this sector and sign partnership agreements with municipalities.

Therefore, will future services really respond to the interest of users (attracted by the metamorphosis of digital technology) or rather to commercial logics? And will Google, or others, become for transport what the inevitable Booking has become for the hotel industry (slipping between the user and the transporters to the detriment of the customer relationship of the professional in the sector and at the latter's expense)? Even beyond these new possibilities, hope is placed in the intelligence that would animate new citizen objects. At a time when the citizen, who has become a consumer, is transforming himself into a product, how could he refuse to upgrade himself by using intelligent objects in intelligent housing in intelligent cities? Aren't we predicting nearly 500 connected and communicating objects in an intelligent home in 2030 (ExpertActions Group study) for a cost of about a dollar per object?

For those who would be concerned, the grouping of digital energy and security engineering industries wants to reassure: we must put the consumer at the heart of the approach and allow them to be an actor within their home (assist them in their home to live there longer). Not surprisingly, in these conditions, the consumer who is reluctant to use mobile payment needs to be reassured (less than 5% of payments worldwide and only 19% of the world's population believe that their money is safe when making payments using contactless technology). This has led some bankers to offer: encrypted banking data stored on a secure chip in iPhones, validation of each transaction with a unique security code, and verification of the identity of the person making the transaction using the Touch ID biometric sensor. Hence, the birth of new markets.

For its part, Keypasco, a Swedish company, uses two sources of authentication to secure payment: the digital footprint of the cardholder's equipment (the unique combination of their components) and the geographical location of the cardholder. In addition, a risk analysis is carried out by identifying unusual transactions: in the case of a purchase made far from the location of the person concerned or using an unusual computer, an SMS is sent to the bearer to obtain his or her agreement before payment.

The digital economy has high expectations of such innovations, which can lead to promising markets: security and economy can converge. It is in this ambivalent context of increased mistrust and renewed hopes for the digital world that concern about digital technology has been reflected in the research of the Chair of Institutional Governance and Strategic Leadership Research, which has approached the issue from a variety of angles.

None of this research had digital security as its sole objective, even though the issues they addressed were (obviously) underpinned by the existence (or even requirement) of digital security. Some of the research, however, is based on trendy thinking that pays too little attention to the requirements of digital security. Thus, in the study on open data, it is mentioned that, notwithstanding the uncertainties linked to this openness and the dangers it would pose to individuals, it was necessary to go ahead since it is part of a general trend.

These flaws do not call into question the relevance of the openness of public data, but the way it is conducted. Far from finding here reasons to slow down a movement whose social utility has been acquired, we should rather see it as an opportunity to give a new impetus to the opening up and sharing of public data, by defining a doctrine and a method (which guarantee the best possible protection of personal data). Because once this protection is provided, there is no longer any obstacle to the deployment of open data.

Likewise, the American model is taken as a reference in Western countries, and the only possible future would be the imitation of this precedent (however inimitable in many aspects) in the hope of an economic miracle achieved automatically by imitating Silicon Valley. Thus, the future is exciting if we accept today to switchover fully into the digital age. On the other hand, we should be aware that the digital economy feeds on the flaws that exist in our systems, our economy and our public policies: digital technology is rushing into areas where the twenty-first century has so far failed to provide a relevant response.

However, it is recognized by ExpertActions Group that cyber security is a key issue that must be addressed as early as possible in the process of addressing the vulnerability risks of strategic networks and businesses. The role of institutions in such a configuration is precisely to highlight, in all their aspects, the scientific and technological issues underlying the choices to be made so that, in the long term, a demanding analysis can be carried out to raise awareness, educate and design digital security based on defence in depth, which is barely sketched out today.

It is therefore a thoughtful construction more than an act of faith that is proposed in this book through the propositions of recommendations tending to use the digital tool only for sure (since the digital tool cannot be sure every time). After first discussing the international context and the rules governing the Internet, a dive into the digital world at the service of institutions and enterprises will be made to show how digital technology structures and weakens these economic players (a fortiori when attacks exploit existing loopholes). But, could these flaws not also constitute opportunities to build more solid information systems, with trusted actors, without jeopardizing fundamental rights or compromising the foundations of sustainable development?

Contents

Chapter 1
The International Context of Corporate Digital Security

In order to situate the issue of digital security for enterprises, it is essential to place the evolution of digital technology in a global context, characterized by political, economic and legal power struggles based on technology. The speed at which these power relations and techniques are evolving and their mutual interactions make it difficult to understand the measures that need to be taken to ensure better digital security for businesses and, in particular, for vital operators and their subcontractors. The organization of digital security is the result of official regulators and self-regulation. It is both global and national and must reconcile freedom and operational efficiency. At the heart of the digital security of the enterprise is the need to assess this security according to the responsible approach specific to the business world. However, from the most spectacular cases to blackmail at the corner of the keyboard, enterprises are exposed, their know-how threatened.

The findings on the implementation of security solutions are therefore unsatisfactory. Is it from a lack of knowledge? The magnitude of the problem or a fatalistic waiver? The recurring difficulty of obtaining precise figures on the risks incurred in order to make a decision? The inability to assess the stakes of intangible values or information? Lack of tools to apprehend them? Or is the high cost of digital security, in terms of people and material resources, a deterrent? Should confidence in digital technology be fostered by private rather than public actors? Is there a lack of legal or technological support? Is the inconsistency of rules and laws relating to the maintenance of digital security compliance harmful? Have states abdicated their role or, on the contrary, overplayed it to the detriment of freedoms? Should new obligations be imposed? Does digital innovation stand in the way of the enterprise's know-how?

Depending on the enterprises and incidents considered, these factors combine to make digital security a key issue. In this context, the organization that the enterprise puts in place to ensure or facilitate the protection of businesses against digital risk plays an essential role, the consistency of which can be assessed on the basis of the analysis of incidents, data collected by specialized observatories and the articulation

W. Amedzro St-Hilaire, *Digital Risk Governance*,
https://doi.org/10.1007/978-3-030-61386-0_1

between technical and legal standards. The Internet has crept into everyone's life, little by little or very quickly, without the question of its governance coming to mind as a priority. The Internet was first perceived as a space of freedom, of access to knowledge – intellectual or social. And yet, because the Internet presupposed an organization, this organization, though not very visible, was bound to be in some hands.

Given the considerable size of the Internet, when two geographically distant interlocutors in distant countries wish to exchange information, it has been necessary to define routing and addressing zones. With more than 620,000 routes according to ExpertActions Group, routing zones have been defined and prioritized to form relay zones. The gigantic size of such a complex raised the question of its management, hence the decision to propose technical governance on a global scale. At present, the allocation of IP addressing areas is organized by continent. Internet management is essential for allocating IP addresses, DNS domain names and other elements that contribute to the functioning of the Internet Protocol. At present, the organization of this governance is not the result of any international text. In resolution 65/41, the United Nations expressed its concern that information technology and information resources could be used for purposes inconsistent with the maintenance of international stability and security and could undermine the integrity of the infrastructure of states, thus affecting their security in both civilian and military fields.

Today, the question of the global management of the Internet has been raised and the need for its reform acknowledged, but neither the objectives nor the timetable is self-evident, since important issues are at stake. The spider's web that encircles the world, the Net, the Internet, the web, is in contact with all domains. The discreet rules of its establishment and organization benefited commercial enterprises and their home states, while the world's population was eagerly and recklessly lending itself to this global stranglehold on minds and objects alike. The weaving of the global spider's web was done by a few unknown actors such as:

- IAB, the Internet Architecture Board, appointed by the Internet Society, the committee responsible for monitoring and developing the Internet.
- ICANN, the Internet Corporation for Assigned Names and Numbers, which manages the root file of the domain name system, ensuring the correspondence between domain names and IP addresses; under California law, this association is supervised by the US Department of Commerce.
- IETF, the Internet Engineering Task Force, responsible for Internet engineering, which participates in the development of standards for the Internet.
- ISOC, the Internet Society.
- W3C, the World Wide Web Consortium, which is the organization for the global network.

The current management of the Internet is the result of the combined action of all these players, all American, whose governing bodies include American digital giants. It is only in the last 10 years or so that a reflection has been initiated on this curious structure through the creation, in 2005, of the Internet Governance Forum

(IGF), a space for multi-stakeholder but not interstate dialogue. It took the Snowden affair in 2013, the public revelation of the identity of the spider waiting at the heart of its web, the National Security Agency, to lead to a global conference on Internet governance in Brazil in April 2014, whose final declaration condemned online surveillance and affirmed founding principles for a free and democratic Internet. In order to retain as much of its current prerogatives as possible, the United States has proposed to start privatizing the management of the Internet, probably in order to avoid the creation of an intergovernmental organization or the influence of any other state.

Faced with this situation, the experts on the democratization of Internet and digital management proposed a new architecture based on:

- The drafting of an international treaty enshrining the founding principles of the São Paulo World Net and leading to the globalization of Internet management
- The creation of a World Internet Council (resulting from the transformation of the Internet Governance Forum or IGF)
- The transformation of ICANN into a WICANN (WorldICANN) under international or Swiss law while organizing international supervision of the root file of domain names
- The establishment of an independent and accessible appeal mechanism allowing the review of a decision of WICANN
- The establishment of a functional separation between WICANN and the operational functions of allocating top-level domain names (the root), IP addresses and Autonomous System Numbers (ASNs) to the regional Internet registries and the definition of Internet protocol parameters (list of port numbers, etc.)
- The definition of independence criteria for WICANN board members to eliminate conflicts of interest

The new architecture of Internet management proposed by the senatorial fact-finding mission obviously does not meet with the enthusiasm of ICANN, which intends to reform itself in its own way. Several regional structures have presented several papers on this topic calling for more transparent, accountable and inclusive Internet governance, but they are far from being all on the same line. In fact, the alignment with the United States still appeals to many countries, not including Germany, despite the proven spying of the Chancellor's private communications by the United States. However, in São Paulo, some countries affirmed their support for a single, open, free, secure, reliable and unfragmented Internet. Some countries wish to take a stand for freedom of expression, freedom of association, freedom of information, the right to privacy, accessibility, open architecture of the Internet, multi-stakeholder governance, openness, transparency, accountability and a system that is inclusive and fair and promotes open standards.

Faced with the United States, suddenly in favour of privatizing Internet management, some countries are moving towards a moralization that includes the right of states – and not just one – to control Internet management. If the desirable evolution of Internet management is mentioned here, it is to show that the challenges of digital network security are situated in a framework that is itself constructed as a place of

insecurity. Therefore, placing one's information and interests in a spider's web implies the acceptance of being a prey. Awareness of this reality by individuals and enterprises alike can only stimulate their thinking. One only surfs the Net if the spider is willing, momentarily, to grant this closely guarded freedom.

With respect to global management of digital security incidents, it should be noted that for many years, institution-wide monitoring services have been offered; most of these services are the result of North American initiatives. The National Institute of Standards and Technology (NIST) is part of the US Department of Commerce and is now the organizational and operational entity responsible for promoting the competitiveness of enterprises confronted with the use of complex technologies. Originally a physical science laboratory in 1901, NIST has expanded its scope since the late 1980s to include information technology standardization. NIST is mandated by the North American government to host and manage the National Vulnerability Database. NIST is a powerful institute behind the use or development of most standards for security monitoring purposes (OVAL, CVE, CVSS bulletins). As a result, all the knowledge of the majority of vulnerabilities is now concentrated and federated on the Security Content Automation Protocol (SCAP), the NIST platform born from the idea of networking security knowledge between scientific and industrial research.

Through the SCAP platform, NIST centralizes and disseminates security events considered to be hazardous in order to foster cooperative efforts at the national and international levels. SCAP also provides a unique and common knowledge of vulnerabilities. In its standard, NIST SP800-126, NIST proposes a standardization of vulnerabilities in order to express them in the same format. Following a vulnerability that affected more than 10% of Internet resources, the North American state also set up a computer incident processing centre, the CERT/CC (Computer Emergency Response Team Coordination Center). CERT/CC was created by the SEI, under the impetus of the Defense Advanced Research Projects Agency (DARPA) and the United States Department of Defense (DoD), located in the heart of Carnegie Mellon University. After this founding incident, CERT/CC's mission was to federate mixed industrial and scientific teams to curb the multiplication of system failures. This strategy had to preserve the competitiveness of software-using enterprises by setting a major player against the publishers at the origin of the ever-increasing number of security breaches.

That is why one of CERT/CC's missions has been to disseminate these vulnerabilities to the general public in the form of "bugtraq" bulletins, in a way putting software publishers on notice to correct their flaws. Since that date, 60,000 vulnerabilities have been the subject of a detailed CERT analysis on more than 27,000 software products, most of which have been patched. The CERT/CC has become a reference, publishing a free daily list of vulnerabilities with a detailed analysis. SCAP and US-CERT are among these North American community-based initiatives supported by the Department of Homeland Security (DHS). Thus, DHS announced the creation of US-CERT, a joint effort with the CERT Coordination Center. US-CERT relies on CERT/CC capabilities to help prevent cyber attacks, protect systems and respond to them.

The success of CERT/CC has led to the development of a global network to federate scientific and industrial safety knowledge and provide a service to users worldwide. CERT/CC has set up a certification mechanism; any state or entity wishing to be an actor in its security can join this network. CERT/CC issues certification to all CERTs. In Western countries, on average, about 20 CERTs are in operation; some are state CERTs such as ANSSI, and others depend on professional sectors. The operational value of all these CERTs is to be linked together at different levels, national and international, in order to exchange information on the discovery of new vulnerabilities. All of these are centralized by CERT/CC and identified by SCAP, whose role, like ICANN, is to establish a globally unique identification. In a context where digital technology is a strategic issue, we can question the neutrality and sustainability of SCAP.

On the state side, the situation is also worrying: institutions are exposed to attacks on a national scale, and attackers in the pay of states are organizing themselves into real armies. Some countries have adopted a communication to improve the protection of critical infrastructure against terrorism, as the disruption of such infrastructure could lead to loss of life and property and the collapse of public confidence. A package of measures has been initiated. The North Atlantic Treaty Organization (NATO) is also involved in the fight against terrorism. It has not remained inactive in the area of cybersecurity since, following the cyber attack that paralyzed Estonia in 2007, a centre of analysis and expertise on cybersecurity was set up in Tallinn. This centre is regularly the target of violent denial of service attacks. Also in 2008, NATO created the Cyber Defense Management Authority (CDMA), a political authority with the mission to initiate and coordinate immediate and effective cyber defence measures whenever circumstances require and also to organize large-scale cyber attack simulation exercises.

One element of the Atlantic Alliance's approach has been to encourage greater cooperation among nations in dealing with cyber attacks. Many rich countries have become involved in the implementation of trust in electronic exchange systems. Awareness of the dangerousness of threats on the Internet and via modern electronic modes of exchange is the challenge of the next decade. The most advanced steps seem to have been taken in Denmark, where, in order to build confidence in electronic payment systems, a state-secured payment infrastructure has been deployed. Similarly, in response to the need for citizen safety, a campaign was conducted in the form of 333 different initiatives across the country under the name NetSafe Now (a major step forward). What was once covered up in words or as hypotheses for reflection on possible developments in cybernetic clashes between states is now openly evoked, especially when the hacking of the Sony Pictures studio, attributed to North Korea in retaliation for the announcement of the release of a film entitled "The Interview" or "The Interview that Kills," which shows the assassination of North Korean head of state Kim Jong-un by journalists recruited by the CIA, came to light.

What's more, Sony Pictures employees have been the direct target of pirate threats. Then there were threats of attacks against the theatres that would screen the film, which led Sony Pictures to abandon the release of the film the next day, as

thousands of exhibitors wanted to avoid any risk. The Federal Bureau of Investigation (FBI) directly pointed to North Korea as the driver of the attack, and the North American president promised a "proportionate and timely" response and called Sony Pictures' waiver a mistake. This is the first time that the United States has named a foreign nation as the target of a cyber attack. In the end, more than 300 cinemas decided, in the name of freedom of expression, to screen the film, which was also made available on the Internet. Technically, the FBI revealed that the North Korean signature would be expressed by lines of computer code, encryption algorithms and data expression methods similar to those used by the North Korean regime in an attack on South Korean banks and media. In addition, IP addresses associated with North Korean infrastructures are said to have communicated with those identified as responsible for the hacking.

It should be noted that North Korea had called the making of "The Interview" an "act of war" and threatened "strong and ruthless" reprisals. Senator John McCain, a Republican senator, called the hacking of Sony Pictures "an act of war." At the same time, Russia and North Korea have multiplied signs of their rapprochement, notably with the invitation to the North Korean leader to visit Moscow. At the same time, for almost nine hours, the Internet connection between North Korea and the world – which passes through China – was interrupted. Was this the work of China, the United States, or North Korea itself to prevent the effects of a North American cyber attack? Or of South Korea as a victim of the hacking of the plans of certain nuclear reactors and their cooling systems, as well as the personal data of nearly 11,000 employees – a cyber attack attributed by South Korea to North Korea?

At the same time, although it went more unnoticed, a giant breakdown affected Microsoft's Xbox live and Sony's PlayStation live servers, threatened in early December with a cyber attack by a group aiming to take these two networks offline permanently. These events show that, from cybersecurity to cyber-warfare, the borders separating civil risks from military risks, and those separating risks from dangers, are increasingly impossible to discern and that the search for a high level of digital security for businesses must be, more than ever and as soon as possible, a real priority for states and their civil security actors, including every digital user.

In such a context, what is the balance of power between Internet giants, states, enterprises and citizens? It must be said that, where the law should set out the applicable rules, it is currently a question of power relationships that prevail. While the law is slow to develop, de facto situations are being created that may limit the creative margins of legislators. The example of Google in some countries illustrates these contradictions. Firstly, while these countries are questioning the existence of the abuse of a dominant position of which the search engine Google would be guilty according to some 30 complainants, the legislator voted a motion calling for the dismantling of Google and a Google tax was voted, to protect the intellectual property of the tools of press publishers used free of charge by Google Noticias.

With regard to these initiatives, it should first be noted that prosecuting Google for these abuses of a dominant position, because of the use of its 90% market share to promote all its services to the detriment of those of its competitors, involves notifying Google of the objections against it and initiating proceedings which will last

for years, during which the alleged abuse will continue or worsen, hence the preference for conciliation in most cases. As for the motions voted by the various Parliaments, apart from their media coverage, which is moreover rather limited despite the audacity of these texts, one may wonder whether their scope is not more symbolic than real.

Finally, the mere announcement of the Spanish Google tax led Google to announce the closure of its news service, resulting in the immediate retreat of newspaper publishers who were to be protected by the tax from Google's free loans. Faced with this situation, a global reaction does not seem possible, if only because some countries have obtained funding from Google for the Digital Press Enhancement Fund.

Secondly, no country seemed to be in a position to introduce a tax obliging Google to make any payment proportionate to the profits made in each country. At most, a directive should allow value-added tax to be paid in the country where a cinematographic work or a song is bought on Apple or Google.

Thirdly, Google's implementation of the right to oblivion, following the decision of the European Court of Justice, leaves Google alone to judge the relevance of the 200,000 or so requests for deletion of links made. In addition, the European Union has had to adopt a regulation on personal data in order to subject such data to the law of the country where the data subject is located, regardless of the location of the servers hosting such data. Finally, the regulators are in dispute with Google, which they accuse of unilaterally changing its privacy policy for messaging, search and storage. Judging by the test to be imposed on – Booking – three national regulatory authorities, acting in concert against the clauses imposed by this online booking site on hoteliers, this type of concerted action could be a quicker and more effective route than institutional solutions. However, the image of a face-to-face meeting between Google and the states must be complemented by the possibility of cooperation between them.

For years, Google has been responding to requests from governments to obtain the private data of Internet users held by this operator. As of 2010, www.google.com/governmentrequests/ allows you to see, state by state, the number of government requests made to Google, either for private data or to remove content. This means that Google owns the locations of connections, the configuration of connected computers, browsing history, the content of searches performed, the content of email messages, etc. Businesses are not exempt from this system. As a result, Google holds far more information about individuals and businesses than most states and has financial clout that surpasses that of many states as well. At this level, this makes this North American private company – like all those at its level – a political player. On this basis, would a draft free trade agreement between regional areas be viable?

It must be said that, for several years now, negotiations have been underway on the conclusion of a comprehensive transatlantic agreement on trade and investment between the United States and the European Union, among others. Several rounds of discussions have been concluded, reflecting the will of both sides to move forward at an extremely rapid pace towards the creation of a large deregulated