Introduction:
Responding to cybermenaces

Côme Berbain,
Direction Interministérielle du Numérique et du système d'Information de l'État (DINSIC)

The widespread view of cyberthreats is warped. Several years ago, Hollywood seized on the character of the hacker as a young white male in a hooded sweatshirt who, assisted by more or less magical tools, could control computers and plunge the world into an apocalypse by stopping a country's production of energy, wiping out banking data or massively circulating fake news. Deprived of the least conscience of his acts, this hacker is usually manipulated by another character, ultimately more human because his intentions are easier to understand. Nothing is both farther from reality as regards the intentions and methods but more realistic as regards the potential consequences.[1]

The digital transformation is making our lives and societies dependent on data and on ever more connected and open information systems. We need but think of banking accounts, hospitals (where computers contain the list of daily treatments for patients), or cities (where smartphones can steer the management of street lighting). This openness is a source of innovations that make the technology and its uses evolve together. It generates innovations in rapid cycles linked to an international competition involving both nation-states and firms. This speed leaves little time for new technology to mature, nor for us to fully understand the issues — whence a permanent challenge to regulations and security.

This new world's security is not all that new. This problem area lies at the crossroads of traditions about the security of information and its transmission, of counterespionage and propaganda. However the issue of security has become more important owing to the broad scope of eventual actions, the technical and organizational immaturity of the very large majority of organizations (public or private), and the availability of offensive techniques.

As approached in this special issue, cybersecurity is a component of digital security. Its purpose is to protect data and information systems, to see to their confidentiality, integrity, authenticity and availability. Despite its technical underpinnings, cybersecurity also entails taking account of human aspects, both individual and collective. As has frequently been said, the principal vulnerability in a computer system is located "between the chair and the keyboard".

Cybersecurity is a problem distinct from the protection of personal data, the manipulation of algorithms or fake news. Unlawfully collecting data does not necessarily imply breaching an information system. Circulating fake news on a social network, such as Twitter, is a normal operation that does not entail attacking the platform's servers. Nevertheless, the questions of protection and manipulation are interrelated, since sophisticated attacks combining both have occurred in recent years.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France).

This special issue presents the current state of thought about cybersecurity and describes the trends under way, as closely as possible to the field and to the persons whose everyday practices are in this field — and thus far from Hollywood scenarios and moving pictures. We want to provide keys for helping readers concretely understand this phenomenon, levers that citizens, employees or decision-makers can put to use in the many dimensions of cybersecurity:

● SEEING AND UNDERSTANDING. It is hard to mount a defense against an invisible enemy. While the media have paid attention to a few emblematic cases (TV5Monde, Saint-Gobain, Airbus…), most victims of cyberattacks want to attract as little attention as possible. Detecting an attack is the indispensable first step, but it is also necessary to understand the motivations, ranging from the cybercriminality of mafia organizations to actions blamed on governments, and to gauge whether an attack is local or systemic, an action against individuals or a "cyberstorm" sweeping over the Internet.

● THE RIGHT BALANCE BETWEEN PREVENTION AND REACTION. Once there is an awareness of the actual menace, the temptation is strong to focus on reacting to it, even more so since reacting involves meaningful activities. As with major fires or industrial catastrophes however, reacting does not suffice by itself. It is also necessary to devote effort to the long tasks of standardizing and certifying solutions, raising stakeholders' level of awareness and of education, and organizing and regulating the ecosystem. All this is necessary to keep our cyber "firefighters" from being exhausted in a contest where the hacker always has the upper hand for launching actions and, too, a natural advantage: after all, destroying is simpler than building or repairing.

● MOVING BEYOND TECHNICAL PROCEDURES. Cybersecurity's technical complexity should not keep us from perceiving nontechnical issues and problems. The questions raised in the past few years about training, organization and regulation must be approached by enlarging our thoughts to encompass the state's role, the responsibility of big high-tech firms, the behavior of private parties, the forms and bounds of regulations, and the adaptation of activities, such as justice, to cybersecurity.

For these reasons, this issue presents the current state of cybersecurity threats, describes motivations, discusses the question of detection, and then turns to examine the array of possible responses from both the public (nation-states, European Union) and private sectors. Given the importance of this issue, nation-states have, of course, intervened. They have responded to major attacks and are trying to set up, at the national and European levels, regulatory frameworks for cybersecurity, which has become so essential to the operation of our society and, too, of the state itself. The media have drawn attention to a few well-known attacks, and this framework should set the conditions for developing products, services or insurance activities in the private sector (in both startups and big industrial groups). In the field of cybersecurity, France still holds its own in worldwide competition. It has also played an active part in defining the details of the European regulatory framework, which will have a long-term impact on the competitiveness of our industries.

New issues related to cybersecurity will also be brought under discussion in these pages: the technical challenges of artificial intelligence, the cloud or connected devices; and the regulation of the comportment of big high-tech firms and even nation-states.

Enjoy!