New Perspectives in the Fight against Cyberattacks

Thomas Cassuto

Magistrate
Doctor of Law
Vice-President of the Institut Présaje

Abstract

Cyberthreats, including cybercrime, constitute a major challenge on two levels. They pose a risk to the critical infrastructure that is vital if France is to function properly, severely testing its resilience. They also threaten democracy. Personal data are exploited to collectively influence individuals in order to guide their political choices. The risks to democracy are much stronger given that manipulation of opinion is carried out without individuals' knowing and at the instigation of foreign powers.

Keywords: cyberattacks, cyberthreat, cybercrime

Nuevas perspectivas en la lucha contra los ciberataques

Resumen

Las ciber amenazas, que incluyen al ciber crimen, constituyen un desafío mayor en dos niveles. Representan un riesgo a la infraestructura crítica que es vital si Francia quiere funcionar de manera apropiada, lo cual pone a prueba severamente la resiliencia del país. También amenazan la democracia. Los datos personales son explotados para ejercer una influencia colectiva sobre los individuos para guiar sus elecciones políticas. Los riesgos a la democracia son mucho más fuertes dado que la manipulación de la opinión se lleva a cabo sin el conocimiento del individuo y con la instigación de poderes extranjeros

Palabras clave: ciber ataques, ciber amenazas, ciber crimen

doi: 10.18278/ijc.7.1.2

打击网络攻击之新视角

摘要

包括网络犯罪在内的网络威胁从两个层面形成一个重大挑战。网络威胁对那些于法国正常运转而言至关重要的关键基础设施造成风险，严重挑战基础设施的韧性。它们还对民主造成威胁。个人数据被滥用，以期集体性地影响个人，进而影响他们的政治选择。考虑到在个人不知情和外部势力的煽动的情况下对舆论进行操纵，民主遭遇的风险会更加强烈。

关键词：网络攻击，网络威胁，网络犯罪

Introduction

One hundred and sixty-three zettabytes[1]: that was the quantity of digital data produced in 2017.[2] Fifteen billion connected devices across the world. These two figures should be compared against the estimated cost of cybercrime to the world economy in 2017: 400 billion euros.[3]

Cyberthreats, including cybercrime, constitute a major challenge on two levels. They pose a risk to the critical infrastructure that is vital if France is to function properly, severely testing its resilience. They also threaten democracy. Personal data are exploited to collectively influence individuals in order to guide their political choices. The risks to democracy are much stronger given that manipulation of opinion is carried out without individuals' knowing and at the instigation of foreign powers.

This is nothing new; cybercrime stems simultaneously from organized crime and from confrontations between cyberpowers. Some current conflicts confirm this. The border between cyberwar and cybercrime is therefore a blurred one. In this context, from a legal point of view, improvements in the fight against cybercrime rely on a strengthening of network security, legal instruments, and operational capabilities.

1. Strengthening Network Security

France's law of January 6, 1978 on information technology and liberties introduced a number of obligations upon persons who process personal data. Noncompliance with some of these obligations, in particular security

1 163 billion terabytes.

2 The number doubles every eighteen months.

3 Communication from the European Commission.

breaches or the unlawful collection and processing of personal data are punishable under articles 226-16 et seq. of the Penal Code.

The 1978 law, a living and evolving text, prefigured the creation of a European legal order. EU law has now established in its treaties the right to protection of personal data and has codified approaches to the protection of this right. Over several decisions, the Court of Justice of the European Union (CJEU) definitively enshrined this fundamental right in practice.[4]

The last steps to date are the General Data Protection Regulation[5] (GDPR) and its accompanying Police Directive[6]; these constitute the general framework for the protection of personal data. In parallel, on January 10, 2017, the Commission presented a proposal for a regulation on "privacy and electronic communications."[7] These standards were also reflected in several conventions of the Council of Europe.

In this intensifying regulatory context, network actors, internet service providers, platforms, search engines, and software publishers must face up to their responsibilities. The fight against various forms of cybercrime unquestionably requires the security of the physical and virtual networks administered by globalized companies. There is therefore an urgent need to systematically and forcefully sanction these companies' failure to comply with their obligations arising from the European law on the protection of personal data. At this juncture, it would be appropriate to extend to this category of offenses the scope of the judicial public interest agreement provided for in article 41-1-2 of the French Code of Criminal Procedure,[8] including, in addition to fines, the obligation to submit to enhanced monitoring from the CNIL (National Commission on Informatics and Liberty).

Second, it is necessary to admit that cybercrime widely benefits from breaches committed by the main actors within information networks, whether in the form of their involuntarily breaching their obligations or of their compromising data for commercial purposes—for example, through the unlawful sale of personal data. In this regard, the transmission of personal data over a social network to a company that performs profiling for electoral purposes,[9] or even to companies

4 Judgment C-135-12 of May 13, 2014 (Google Spain), enshrined the right to be forgotten on the basis of the right to data protection set out in the Charter of Fundamental Rights of the European Union; Judgment C- 162/14 of October 6, 2015 (Maximillian Schrems v Data Protection Commissioner), canceled the safe harbor established with the United States under EU Directive 95/46/EC.

5 Regulation (EU) 2016/679 of April 27, 2016.

6 Directive 2016/680/EU of April 27, 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data.

7 COM(2017) 10 final.

8 Established by the law of December 9, 2016.

9 "Le 'scandale Facebook' pousse Cambridge Analytica à la faillite," *Le Figaro*, May 2, 2018.

in China—a country where the state collects personal data, in particular biometric data,[10] on a massive scale—constitutes a major failure and a form of cybercrime. Such abuses must be punished under criminal law in accordance with the applicable European legislation, especially when the personal data have transited across Europe or relate to European nationals.

The security of personal data has ceased to be an issue of individual freedom alone now that big data, the black gold of AI, can be used for criminal purposes or to impair democracy. In this regard, information and guarantees of individuals' rights must be further improved.

2. Strengthening the Legal Instruments

It is self-evident that cybercrime is a form of organized crime with transnational dimensions and vectors. It stimulates coordination and cooperation between multiple actors in technical, financial, social, and other areas. The international level is therefore where we must strengthen instruments and transpose them efficiently to the national level.

In this regard, the Council of Europe Convention on Cybercrime,[11] known as the Budapest Convention, serves as the principal international instrument, as it has been ratified by nonmember states, including the United States, Canada, Japan, Australia, and Senegal. The convention, adopted in 2001, is unfortunately dated. It scarcely includes technological developments and the arrival of new actors. It also suffers from the fact that Russia has not signed it and that China opposes it; these two countries consider the convention to be too focused on repression. In any event, this instrument must still be modernized, as part of a third protocol, in order to define new offenses, strengthen network security, and extend liability to new actors.[12]

At the European level, the GDPR is the general framework imposed on those who process personal data. However, it is necessary to strengthen the means of action that aim to suppress forms of cybercrime targeting such data. In this regard, the Directive on the European Investigation Order[13] implements the principle of mutual recognition for the collection of evidence. However, the time frames it imposes, which are drastically shorter than those observed in terms of classic mutual assistance in criminal matters, are too large for combating cybercrime, especially when it comes to financial fraud, which gives rise to significant movements of funds in short periods of time.

10 "Données personnelles: Facebook les a partagées avec des groupes chinois," *Le Figaro*, June 6, 2018.

11 Convention of November 23, 2001, which entered into force on July 1, 2004.

12 A second protocol on the fight against terrorism is still in development.

13 Directive 2014/41/EU, implemented in France by order 2016-1636 of December 1, 2016. See Thomas Cassuto, "La Directive concernant la Décision d'enquête européenne," *AJ Pénal Dalloz* (July-August 2014): 338.

The establishment of joint investigation teams[14] must be made easier to ensure that they can be structured and deployed in a very short period of time. The possibility of having these teams work remotely must contribute to this. Setting up such teams could be encouraged among services that specialize in the fight against cybercrime.

It would be useful for the European Investigation Order to be supplemented by the regulation proposal presented on December 21, 2016 on the mutual recognition of freezing and confiscation orders.[15] The adoption of this regulation could allow fraudulent financial transactions undertaken by cybercriminals to be followed and countered, thus depriving them of their gains.

In the future, the European prosecutor[16] should have the capacity to combat cybercrime, which, in various forms, finds fertile ground in fraud affecting the EU's financial interests.

This is the context in which, on April 17, 2018, the European Commission presented, on the one hand, a proposal for a regulation[17] on European production and preservation orders for electronic evidence in criminal matters, and, on the other hand, a proposal for a directive[18] laying down harmonized rules on the appointment of legal representatives responsible for gathering evidence in criminal proceedings. These proposals aim to facilitate national judicial authorities' access to electronic evidence, particularly by requiring the holders of such data to respond directly to the requesting authority. The regulation proposal, which implements the principle of mutual recognition, should allow the transmission of data to be ordered in less than ten days, or even in less than six hours in an emergency, when a requesting state makes such an application. It also provides for a preservation order to prevent the deletion of data, which obliges a service provider offering services in the EU and established or represented in another member state to retain certain data for their transmission at a later date. These measures also seem to be a response to the enactment on March 23, 2018 of the United States' CLOUD Act. This was itself adopted in response to the Microsoft case, which gave rise to a decision by a court of appeals to the effect that the *Stored Communications Act of 1986* only applied to data stored in the United States and did not have any extraterritorial effect.[19]

14 Framework Decision 2002/465/JHA of June 13, 2002.

15 COM(2016) 819 final.

16 Art. 86 TFEU, regulation 2017/1939/EU implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office.

17 COM (2018) 225 final.

18 COM (2018) 226 final.

19 See Sylvie Peyrou, "Le projet de règlement 'E-evidence' (preuves électroniques) présenté par la Commission européenne: un 'Cloud Act' européen," http://www.gdr-elsj.eu.

The objective of the European Commission's two proposals, which happen to be essential for effectively combating cybercrime, is to be able to directly obtain, from any representative in the EU, data held or administered by any person, including when these data have been transmitted outside the EU—for example, to the United States.[20]

In parallel, at the European level, it is necessary to update the common minimum standards relating to definitions of offenses in order to adapt them to new forms of cybercrime. This harmonization must as a minimum promote the mutual recognition of investigation measures and prevent difficulties related to dual criminal liability. Directive 2013/40/EU contributes to this.[21] It should be adapted to take account of new forms of fraud such as the unlawful processing of personal data, the use of cryptography, the unlawful refusal to reveal an encryption key, and fraud related to blockchain technology.

At the national level, the legislator regularly adapts definitions of offenses in order to take new developments into account. On the level of criminal procedure, however, it seems necessary to streamline the rules in order to reduce the time between decision making and access to useful data. Therefore, the general structure of the rules relating to perquisitions of information; requisitions; seizure of computer data; and decryption through national-defense, geolocation, or computer data capture processes[22] should be simplified in order to ensure that they are effective on a day-to-day basis. As a matter of urgency, the state should also develop technical tools to enable the implementation of these provisions, in particular those from articles 706-102-1 et seq of the Code of Criminal Procedure relating to computer data capture, and it should commit to the development, on the basis of articles 230-6 et seq of the same code, of files that allow the systematic analysis of the facts and data collected.

3. Strengthening Capabilities

This sounds obvious. In the face of a form of crime that continues to grow, adapting legislative frameworks is necessary but not sufficient.

First, there is an urgent need to strengthen material and human resources and to train services that specialize in cybercrime, whether at the national or regional level, in connection with Europol, which has set up a center of expertise in this area. These services must accommodate interdisciplinary skills and establish

20 Regarding the United States, there is a framework agreement, the EU-US Privacy Shield, which came into force on August 1, 2016. It sets out a system of certification and self-certification for companies that transfer personal data to the United States. This mechanism has several limitations.

21 Directive of August 12, 2013, on attacks against information systems and replacing the framework decision.

22 See in particular articles 57-1, 77-1-1, 99-5, 230-1, 230-32, 706-102-1 et seq of the Code of Criminal Procedure.

or strengthen partnerships with researchers and key internet actors, in particular public actors. Moreover, the fight against cybercrime requires fast and continuous innovation with the goal of developing technical solutions to constantly evolving problems. This innovation should lead to closer ties between investigators and researchers.

Second, it is also necessary to create an electronic registry system to store and preserve pieces of digital evidence in order to reduce the physical management of materials that are cumbersome, in terms not only of computer units and storage but also of data volume. Moreover, it is now a given that developments in artificial intelligence will have an impact on the criminal sphere. New forms of crime will appear—for example, autonomous drones[23] that are armed or involved in the logistics of trafficking. Artificial intelligence has already been hijacked, and the threat of its misuse spreading across all networks is growing.

Faced with this threat, and taking into account more generally the exponential growth of the amount of digital data produced, we must develop artificial-intelligence capabilities and applications that focus on the processing of mass data and the fight against all forms of crime, especially cybercrime. Indeed, I would argue that, in the near future, only artificial intelligence will be able to solve forensic issues related to the hijacking of artificial intelligence.[24] The development of these capacities should be based on a strong partnership between the public, private, and university sectors. In this respect, it is particularly important to extend the ability to implement—within a strict framework and according to perfectly defined rules of usage —cyberdefense measures when certain forms of cybercrime are able to threaten national sovereignty, territorial integrity, and our critical infrastructure.

Conclusion

By definition, cybercrime is the form of crime that requires the greatest capacity to adapt and evolve on the part of the authorities. A threat in terms of its purposes, its means, and its substance, cybercrime is creating a danger to France's vital interests.

For several years, the fight against cybercrime has been the subject of special attention, and resources have been developed to this end. It remains the case that the evolution of this form of crime, which numerous terrorist organizations have seized upon, requires heightened protection of networks and personal data, as well as a speeding up of the development of capabilities and competences. This fight should also be placed within the context of the rapid construction of a transnational legal order related to information and communications technologies.

23 Lethal autonomous weapon systems (LAWS) are now the subject of intense work within the Conference on Disarmament. See the statement made by the Permanent Representative of France on November 15, 2017, https://cd-geneve.delegfrance.org.

24 See Thomas Cassuto, "Justice et intelligence artificielle," *L'ENA hors les murs* (June 2018).

CYBERATTACKS – CYBERTHREATS – CYBERCRIME

Cyberthreats, including cybercrime, constitute a major challenge on two levels. They pose a risk to the critical infrastructure that is vital if France is to function properly, severely testing its resilience. They also threaten democracy. Personal data are exploited to collectively influence individuals in order to guide their political choices. The risks to democracy are much stronger given that manipulation of opinion is carried out without individuals' knowing and at the instigation of foreign powers.