APRIL 2021

REPORT

CRIMINAL LAW IN THE FACE OF CYBERATTACKS

Working group chaired by Bernard Spitz,
President of the International and Europe Division of MEDEF,
former President of the French Insurance Federation (FFA)

General secretary: Valérie Lafarge-Sarkozy,
Lawyer, Partner with the law firm Altana

le club des juristes

AD HOC COMMISSION

CRIMINAL LAW IN THE FACE OF CYBERATTACKS

CLUB DES JURISTES REPORT

Ad hoc commission
APRIL 2021

4, rue de la Planche 75007 Paris
Phone : 01 53 63 40 04
www.leclubdesjuristes.com

FIND US ON

PREFACE

In the shadow of the global health crisis that has held the world in its grip since 2020, episodes of cyberattacks have multiplied. We should be careful not to see this as mere coincidence, an unexpected combination of calamities that unleash themselves in a relentless series bearing no relation to one another. On the contrary, the major disruptions or transitions caused in our societies by the Covid-19 pandemic have been conducive to the growth of offences which, though to varying degrees rooted in digital, are also symptoms of contemporary vulnerabilities. The vulnerability of some will have been the psychological breeding ground for digital offences committed during the health crisis. In August 2020, the Secretary-General of Interpol warned of the increase in cyberattacks that had occurred a few months before, attacks "exploiting the fear and uncertainty caused by the unstable economic and social situation brought about by Covid-19". People anxious about the disease, undermined by loneliness, made vulnerable by their distress – victims of a particular vulnerability, those recurrent figures in contemporary criminal law – are the chosen victims of those who excel at taking advantage of the credulity of others. During the spring 2020 lockdown, some hundred scams registered in France were committed online by individuals posing as business leaders selling stocks of masks. The digital world then has to settle for fending off contemporary examples of classic scam behaviour. The vulnerability of information systems is itself the offspring of digital. Successive lockdowns, by promoting teleworking, telemedicine and distance selling, down to what have become the most mundane acts of everyday life such as contactless payments, have helped to multiply the circumstances that can give rise to the commission of cyberattacks. The defence to these, here as elsewhere, relies on the impossibility of access. Alas! Pirated passwords, uncorrected vulnerabilities, simple human failures (such as inadvertently downloading a trojan) literally open the doors of computer systems.

What if all this revealed a structural vulnerability, that of our societies? Bound hand and foot to digital, contemporary societies draw from it what makes them both successful and fragile, in an edifying testimony to the ambivalence of digital. In fact, the Covid-19 pandemic has only exacerbated existing trends. For a long time now the risks of cyberattacks have been well identified, even where they are not already taking place. It should be recalled that the intangible dimension of cyberattacks does not mean they cannot attack, whether directly or indirectly, the bodily integrity or even the life of a person. In 2019, the US Department of Homeland Security warned of vulnerabilities in the radio communication system of certain cardiac defibrillators: if malicious

persons took advantage of such vulnerabilities, they could cause the death of a patient. In Germany, a woman in a life-threatening emergency could not be operated on at a hospital because it was being targeted by ransomware affecting around thirty of its servers: the woman died while she was being transferred to another hospital, having been admitted too late. On a larger scale, the combination of cyberattacks and terrorism represents "the" threat of the twenty-first century. In a configuration bringing the two together, "conventional" acts of terrorism such as the killings at the Bataclan could be supported by cyberattacks, for example targeting traffic-light systems: the key element being a total disruption of traffic, hampering the arrival of emergency and security forces. A further step towards dematerialisation and, as cyber war already shows us (think of the hacking of Iran's nuclear programme by the Stuxnet virus attributed to the NSA, at any rate regarded as the first cyber weapon), we need to keep in mind the spectre of cyberattacks on OVIs, operators of vital importance. But already the link between terrorism and cyberattacks is well established on another level. The financial windfall which results from them, *via* ransoms or data sales, helps to support terrorist funding networks.

Individuals are paying a high price for these attacks, but also and above all businesses. As the prime targets of cyberattacks, businesses of all sizes need to prepare for them and know how to respond when an attack occurs. A comprehensive approach to this issue has been presented to Le Club des Juristes by Valérie Lafarge-Sarkozy, a lawyer and expert of the Club. A commission was set up under the chairmanship of Bernard Spitz, the Ad Hoc Commission on Cyber Risk, bringing together experts from very different fields but whose areas of interest converge on digital. First considering it in terms of risk, a collective reflection by a sub-committee tasked with considering the insurance implications of cyberattacks led to an initial report entitled "Insuring Cyber Risk", published by Le Club des Juristes in January 2018. As a follow-up to this reflection, another sub-committee was appointed to consider the law enforcement component. Having completed its work, it is delivering this report on "Criminal law in the face of cyberattacks". The editors of the report have brought all their experience to bear as professionals working closely with cyberattacks. Valérie Lafarge-Sarkozy and Laetitia Dage, lawyers, Myriam Quéméner, prosecutor (*avocat général*) at the Paris Court of Appeal and Anne Souvira, chief superintendent (*commissaire divisionnaire*) and officer responsible for cybercrime issues at the office of the Paris Metropolitan Police Commissioner (*préfet de police de Paris*), have shared their skills and experience in drawing up the report. This author has had the privilege of following its genesis and today has the pleasure of writing the preface.

In its first two parts, the report addresses substantive criminal law and criminal procedure. As regards the first, the reader will find an informative presentation of the offences involved. Reviewing the conventional offences available (at least those which are of general application), the report recalls that it is possible to call upon both those classified as offences against property – theft and fraud – and offences against the person such as identity theft. Emphasis is also placed, of course, on the more specific offences of attacks on automated data processing systems (ADPS), combined with certain offences relating particularly to the processing of personal data. Hence a possible reversal in outlook is outlined, as businesses that are the victims of cyberattacks on their ADPS might themselves be liable for the inadequate protection of those systems. In the discussion of the offences, a call for caution should therefore be noted, which is explicitly expressed in developments designed to establish pre-emptive rules of e-governance for businesses. But when the damage is done, one must turn to the judicial response. The second part of the report offers this some very rich developments, highly practical in tone, which will be a very helpful guide for victims of cyberattacks. The first two parts of the report are not only full of various insights and advice, but also contain interviews with specialists, which give to the whole a resolutely practical and operational twist. But the report does not end there. As a conclusion, a third part offers "10 recommendations for advancing the fight against cybercrime". One can only hope that these recommendations will be heard by the various institutions to which they are addressed. Might one dare to formulate an 11th, a recommendation that in fact simply translates what runs like a watermark through this report, namely that digital should not make us forget basic common sense: discretion is the better part of valour – even in digital, especially in digital.

Agathe Lepage
Professor at Université Panthéon-Assas (Paris II)

TABLE OF CONTENTS

INTRODUCTION

1. **While cyberspace** is a powerhouse of growth and innovation, it is also plagued by malevolent exploitation of its flaws and vulnerabilities. This is the ambivalence of digital: both an economic lever – a source of value and preservation of economic activity, as we saw recently with the first health crisis in March **2020** – and also a source of cybercrime, as the same health crisis revealed, with a considerable increase in attacks, remote working having become the source of **20%** of cybercrime incidents.

In France, in **2018** **80%** of companies reported an incident of cybercrime[1]. In 2019 the rate rose to **90%**, **43%** relating to SMEs, and in **2020** the rate rose 4-fold, requiring President Macron on **Thursday, February 18, 2021** to present his cyber-defence strategy in response to the exponential growth of threats and attacks.

2. Numerous international reports measure the direct and indirect costs of digital attacks. For example, in **2017** the overall cost was **$600 billion**. In **2018** the average cost per business was **€8.6 million**[2] for French businesses and **$27.4 million** on average for US businesses.

The year **2019** confirmed the rise in indirect attacks exploiting relationships between partners. Indeed, given the current maturity level of the ultimate targets, cybercriminals bypass them by attacking a partner/supplier of digital services, internet access, outsourcing companies, etc. The scope of the attack is thereby multiplied, and in **5-year** forecasts, **23%** of the cost of attacks could result from such attacks targeting third-party information systems in order to reach the real target.[3]

As for **2020**, based on the first half of the year it will be a record year in France with, for example, a **667%** increase in phishing attacks recorded between 1 and 23 March.[4] According to a report by VMware Carbon Black[5], between February and March **2020** ransomware attacks increased by **148%** worldwide, with one attack taking place every **14** seconds.

3. Globally, cybercrime is expected to cost businesses **$6,000 billion** annually from **2021**.[6]

1. Report of the Ministry of the Interior "The state of the digital threat"
2. https://www.accenture.com/fr-fr/insights/security/etude-cout-du-cybercrime
3. https://www.accenture.com/fr-fr/insights/security/etude-cout-du-cybercrime
4. https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/
5. https://www.carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/
6. Annual Report of Cybersecurity Ventures and Herjavec Group, 2019, https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

■ **4.** The risk/cost/gain ratio of cybercrime is very advantageous to offenders who can easily obtain online and on the darknet kits for around $5 that enable them to commit denial-of-service attacks, and use digital technology to industrialise and globalise their crimes.

Changes in working methods and the massive increase in teleworking have given them new and many opportunities. In the second half of 2020, the Zoom application therefore had to slow the development of its functionality in order to focus on its security, in order to cope with the significant increase in the number of its daily users from 10 million in December 2019 to over 200 million in March 2020.

FOCUS

INTERVIEW WITH GUILLAUME POUPARD
Director General of National Agency for the Security of Information Systems (ANSSI)
by Brigitte Bouquot, AMRAE and Valérie Lafarge-Sarkozy, Altana

1/ The pandemic has increased digital use; has it developed the cyber threat?

The increase in the cyber threat is indeed very worrying, as the number of ransomware attacks handled by ANSSI increased 4-fold between 2019 and 2020, from 54 to 192.
Since the beginning of 2021, this trend has not declined and we are constantly providing assistance to some 40 victims simultaneously. Victims of importance in terms of national, economic or health security…

It is true that the health situation is a slight aggravating factor in the cyber threat, in that it complicates the lives of defenders, but not necessarily those of attackers. But it is clear that the rapid growth of the cyber threat preceded the health crisis and that the underlying trend is extremely negative. When the health crisis stops, the cyber crisis will continue. It is essential to dissociate the two subjects and deal with the cyber subject that will concern us for the long term.

2/ Could you comment on President Macron's announcements regarding the national cyber security strategy?

The strategy announced by the President has two components. A situational component linked to the cyberattacks that struck two healthcare institutions in quick succession in February, and an economic component based on France's desire significantly to

develop its industrial cyber-security ecosystem. This reflects both a strong concern for our society, under threat from cyberattacks, and also the need to enhance our industrial base to address the growing threat and assert our position as a major player in cyber security on the world stage. Indeed, we have many successful players in France which are investing heavily in cyber technology and are capable of providing trusted solutions to French, European and international stakeholders. At the international level, French solutions are particularly sought after, for they are often hallmarks of confidence. This represents real economic opportunities for French business.

The €1 billion is broken down into several major funding streams: research funding, the future investment plan (*plan d'investissement d'avenir* - PIA4), and France Recovery (*France Relance*), which includes a €136 million package to strengthen the cybersecurity of public stakeholders in a sustainable way (hospitals, local authorities, central government).

The Cyber Campus announced, very symbolically by President Emmanuel Macron, will also benefit from this funding. A true French ambition held at the highest political level, this Campus will bring together large groups, SMEs, start-ups, researchers and authorities around cybersecurity projects. It may look heterogeneous, but in reality it is a true French team. The launch of such a Campus is a major step in our cyber strategy which includes a strong European dimension, which will culminate in the French Presidency of the Council of the European Union early in 2022.

3/ How can the development of a specific criminal component reinforce the digital security policy conducted by ANSSI?

As a national authority, we cooperate with the investigation and intelligence agencies on a daily basis. We have developed a close collaboration with the intelligence agencies and investigation agencies (C3N, OCLCTIC, BL2C and DGSI) and the specialist cyber prosecution service (J3). There is a real convergence of views today on cyber issues within the State. ANSSI works very effectively with all these services to share its knowledge and methods. In future, it would help for information sharing between the intelligence and investigation agencies to be deepened further, as the sharing of technical information is essential to the fight against the cyber threat.

International judicial cooperation is increasingly working to combat cybercrime. Recently we have had some real successes with, for example, the dismantling of the Emotet and Egregor networks.

These examples change the sense of fear that is around and deliver a positive message. International judicial cooperation is developing very clearly in Europe, but also with our Western allies and even

beyond. We all have an interest in reducing the number of places where cybercriminals can act and lurk.

4/ What are your digital security tips for business leaders?
Digital risk must be integrated into the overall risk management of each business. Business leaders need to use regulatory leverage and invest 5-10% of their IT budget in cyber security in order to build efficient solutions. Our ecosystem of trusted providers, many of whom have an ANSSI Security Visa, is able to support and advise businesses effectively. Better protection for our businesses will help to limit serious attacks, raise the level of cyber security and manage residual risk effectively, including the development of insurance mechanisms. It is essential for every business to use the levers that it has to secure itself and to be accountable for this so that everyone can continue to take full advantage of the opportunities of digital.

■ **5.** In this context it seemed necessary, for a proper understanding of this report and of the challenges of cyber security for businesses, to begin by defining the concepts of cyberspace (i), cybercrime (ii), cyber security (iii) and cyber defence (iv):

(i) **Cyberspace** is a world of communication and sharing made up of infrastructures, networks and information systems (IS), as well as electronic communications, which are interconnected throughout the world, even in space. So it is an intangible space with no borders, which fuels debate about cooperation between States (e.g. in the search for digital evidence), which wield their sovereignty by complicating possible solutions at national and international levels. ANSSI ensures that European strategic autonomy in digital security is respected[7].

(ii) **Cybercrime** has been defined by the interdepartmental working group chaired by Attorney General Marc Robert[8] as acts constituting criminal offences attempted or committed against or by means of an information and communication system and the data that it holds.

(iii) **Cyber security** may be defined as the desired state that enables an information system to withstand events that might compromise the availability, integrity or confidentiality of stored, processed or transmitted data and related services that such systems offer or make accessible.

---

7. See www.ssi.gouv.fr

8. February 2014 online Cybercrime Report
http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf
http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite_annexes.pdf

To this end, the dual objective of cybersecurity is, on the one hand, to train and raise awareness in all stakeholders (businesses, communities, individuals) of cyber risks and good practices, as well as the IT hygiene to be implemented on a daily basis in order to reduce the cost of cyberattacks and, on the other hand, the acquisition of technical solutions to protect data and IS.

For businesses, cyber security is a matter of cross-business governance, entrusted to several different players such as information systems directors, heads of security of information systems, data protection officers or executive committees, under the supervision of leaders who must determine the risk acceptable given the business issues at stake and financial trade-offs.

Conscious of these difficulties, ANSSI has created "Security Visas" designed to certify and classify products or services as a security solution whose reliability is recognised following an evaluation by approved laboratories.

(iv) Thus cyber security, such as the fight against **cybercrime**, contributes to cyber defence, as they both work to prevent attacks effectively by attempting to identify and apprehend perpetrators.

Cyber defence is a "*set of technical and non-technical measures that enable a State to defend in cyberspace information systems that are deemed essential*." Since the creation of ANSSI in **2009**, Law Nº. 2013-1168 of **18 December 2013** on military programming for the years **2014** to **2019** clarified the legal framework of our cyber defence, which is organised in 4 parts: protection, military action, intelligence and judicial investigation.

■ **6. Having set out this framework of context and definitions, we must look at the circumstances in which our criminal law has adapted to respond to multifaceted cyberattacks.**

In France, cybercrime has been taken into account legally since the law on computer science, files and freedoms of **6 January 1978**, then by the visionary Godfrain Law 88-19 of **5 January 1988** on computer fraud, which introduced Articles **323-1 et seq into the Criminal Code** to punish all attacks on automated data processing systems (ADPS), such as hacking and distributed denial-of-service (DDOS) attacks, and now ransomware data encryption.

The Law on trust in the digital economy (*la loi pour la confiance dans l'économie numérique* - LCEN) of **21 June 2004**, with its **Article 6** on internet service providers, webhosts and publishers of manifestly illicit content, should also be mentioned. The LCEN also introduced a new article into the Criminal Code (**323-3-1**), aimed directly at the

possession and provision of equipment designed to commit acts of intrusion into a system or of interference with its functioning.

The Law of **30 September 1986** known as "CANAL+" for the reception of audio-visual programmes, the **Intellectual Property Code (Articles L. 335-1 et seq)**, and the Monetary and Financial Code **(Article L. 163-4-1 of the Monetary and Financial Code)** provide for numerous offences: for example, fraud and counterfeiting, which in some cases make use of a telecommunications network in aggravating circumstances (Articles L. 521-10, L. 615-14, L. 623-32 and L. 716-9 of the Intellectual Property Code).

The Lemaire Law Nº. **2016-1321** of 7 October 2016 for a digital Republic also has a criminal dimension and, most recently, the Law of **23 March 2019** on programming for **2018-2022** and judicial reform (LPJ) provides for the extension of the use of investigations under pseudonym and the harmonisation of special investigative techniques tailored to the fight against cybercrime.

Lawmakers are therefore continually adapting the criminal arsenal with regard to the constant and rapid evolution of cyber threats.

■ **7.** A Europol IOCTA report **of 2018**[9] describes **seven particularly pervasive types of cyber threats** of which businesses can be the victim, to which conventional crime should be added:

(i) **Ransomware** that encrypts data on both workstations and servers while requesting a payment, particularly in cryptocurrency such as bitcoin or Ethereum, in exchange for a decryption key that will restore access to the data. Although it is estimated that **80%** of data is recovered, it is not always reusable, as it is often returned in a disordered state and/or still encrypted.

In **2019, 2020 and 2021**, ransomware attacks[10] were the most troubling IT threat, targeting businesses and public bodies as well as critical information systems such as those relating to health, often resulting in data theft as well as encryption.

A major attack will live on in the memory: the self-replicating data encryption ransomware **WannaCrypt**, which in June 2017 infected thousands of computers worldwide (300,000 victims in 150 countries) and was apparently facilitated by a security breach that was not corrected by available updates[11].

9. (IOCTA), https://www.europol.europa.eu
10. https://www.zdnet.fr/actualites/ransomware-des-operateurs-d-egregor-interpelles-en-ukraine-39917907.htm
11. https://tribune.com.pk/story/1423609/shadow-brokers-threaten-release-windows-10-hacking-tools

More recently, in **May 2019** hackers took hostage the computer system of the city of Baltimore. They blocked **10,000** computers in the city with ransomware, demanding a ransom of **$100,000 (€89,410)** in bitcoin to unlock all the files concerned, or alternatively a lower ransom per file.[12]

In **2020**, the attack by the Maze ransomware which raged across the world (affecting both Bouygues Construction in France, Southwine, PitneyBowes or Cognizant in the USA as well as Asco in Belgium) should be mentioned, particularly as it required ANSSI and its international partners to reconsider previously delineated borders between cybercrime and national security.[13] In **the autumn of 2020** the Egregor ransomware raged in similar circumstances.

The foreign intelligence agencies of North Korea, China and Russia were identified as attackers and their assets frozen by an order of the Minister of Economy, Finance and Recovery dated **30 July 2020**[14].

On the night of January **15 to 18, 2021**, the Mayor of Angers and the urban community of Angers Loire Métropole were the victims of ransomware that blocked their entire information system. One month later, the situation had still not returned to normal.

In **2020** and early **2021**, a real spate of it hit French cities (for example La Rochelle, Aix, Marseille, Vincennes), but also hospitals: French hospitals were the subject of **27** major cyberattacks.

(ii) **Denial-of-service (DDoS) attacks**, which saturate a network or online service with traffic, making it unavailable (the site goes down).

For example, in **June 2019**, during the protests that were then rocking Hong Kong, the encrypted messaging service Telegram was the victim of a denial-of-service attack that prevented its use by protesters to arrange meetings anonymously. It turned out that the attack originated from IP addresses located in China.[15]

In **September** of the same year, it was the online encyclopaedia Wikipedia that was hit by a massive attack in Europe, Africa and the Middle East, before spreading partly to the United States and Asia.

12. https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html
13. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/ ; https://www.lefigaro.fr/secteur/high-tech/qu-est-ce-que-maze-ce-rancongiciel-qui-seme-la-terreur-dans-les-entreprises-20200206
14. JORF N°. 0188 of August 1 , 2020
15. https://www.pcmag.com/news/chinese-ddos-attack-hits-telegram-during-hong-kong-protests

This attack altered the proper functioning of the service for at least **nine hours**.[16]

In **October 2020**, Google was targeted by the largest DDoS attack ever recorded of 2.54 TB.

(iii) **Cryptojacking** attacks allow the clandestine use of a computer previously infected with a virus to instal cryptocurrency creator (mining) software.

Cryptojacking uses the computing power or bandwidth of a computer or device to create and extract currencies without the knowledge of the user who does not properly perform antivirus updates. There are few reports of cryptojacking cases, as victims often do not notice the attack (which simply causes a slowdown of their machine) and are rarely sufficiently harmed to file a complaint.

(iv) **Fake computer support fraud**, such as posing as a software company for troubleshooting and updating, is the second leading cause of financial loss in the US (as a result of cyberattacks), according to an FBI report of **11 February 2020**, which details the attacks and their cost[17].

(v) **Phishing**, which, particularly through viruses with machine learning capabilities, enables digital identity theft by sending massive amounts of trick messages.

Thousands of potential victims are thus targeted and referred, for example, to corrupt sites which steal their "login/password" details, or any other personal data that can easily be converted into cash on the darknet. The data will then be used to attack bank accounts or e-shops, etc.

For example, in the United States in **2015** cyber criminals used personal information stolen from US citizens to answer security questions on the website of the tax authorities (IRS) and thereby to access their tax returns, which contained their addresses.[18]

The Covid-19 pandemic has encouraged the development of *phishing*. Teleworking by employees who are not sufficiently suspicious and do not have the appropriate security tools is an open door to phishing emails.

16. https://nakedsecurity.sophos.com/2019/09/11/wikipedia-fights-off-huge-ddos-attack/
17. https://pdf.ic3.gov/2019_IC3Report.pdf
18. https://www.nytimes.com/2015/05/27/business/breach-exposes-irs-tax-returns.html

(vi) **Economic espionage**, an ever-increasing threat that aims to reach the information assets of companies. These very discreet computer attacks can only be detected very late in the day, with consequences that are sometimes difficult to assess in terms of economic loss.

For example, the French aeronautical supplier SAFRAN was the victim of a cyberattack orchestrated by the Chinese intelligence services, an attack unveiled by the US Department of Justice in **October 2018**[19].

In **May 2019**, Europol announced the dismantling of a gang of cybercriminals who had stolen nearly **€90 million** from **41,000 victims**[20] using the spyware Goznym, which recorded everything its victims were typing on their keyboards.

The victims were robbed of their bank details by hackers accessing their accounts, transferring the funds to accounts which they controlled, then laundering the proceeds, particularly through bitcoin portfolios.

The ANSSI Annual Report for **2019** reveals that espionage continues on an upward trend - the search for strategic information on foreign and defence policies, as well as access to industrial and commercial secrets or the theft of personal data, and also influence through fake news being the main motives. [21]

(vii) **Sabotage**, which causes the failure of a computer system.

The attack on TV5 Monde [22] was a sabotage emblematic of the ease of committing large-scale crimes capable of completely paralysing access to information.

One could also mention the NotPetya cyberattack, which infected accounting software used by many businesses around the world. According to ZDNet, the French company Saint-Gobain estimates that the ransomware campaign which it suffered cost it **1%** of its

19. https://www.reuters.com/article/us-usa-china-hacking/u-s-charges-chinese-intelligence-officers-for-jet-engine-data-hack-idUSKCN1N42QG
20. https://www.lemonde.fr/pixels/article/2019/05/16/demantelement-d-un-gang-de-cybercriminels-aux-41-000-victimes_5463030_4408996.html
21. Annual Activity Report, ANSSI, 2019, https://www.ssi.gouv.fr/uploads/2020/06/anssi-papiers_numeriques-2020.pdf
22. https://www.lemonde.fr/pixels/article/2017/06/10/le-piratage-de-tv5-monde-vu-de-l-interieur_5142046_4408996.html

income, or at least **220** million euros [23]. This sabotage affected the core of computer hardware operations.

(viii) We must also mention **software hacking**, which allows a business's information system to be entered unnoticed *via* a software update that has had malware implemented in its source code.

The always-active Solarwinds cyberattack is a major example of this: it is one of the largest and most sophisticated attacks to date.

By updating Solarwinds software used as a vector of delivery to "hackers", it enabled the information systems of **18,000,000** critical organisations (large companies, infrastructure and government institutions) to be infiltrated.

This panorama of cyber threats that is growing exponentially, and their economic and social consequences, demand effective judicial treatment. Hence, in particular, the importance for investigators to have the necessary technological and human resources to enable them to establish the constituent elements of the offences and identify the cybercriminals. This also requires effective international cooperation at the European level and beyond. In this threatening context, an overriding need in the public interest is the availability of responsive and competent services, able to take action rapidly for businesses in order to give them the best advice, take account of the challenges of the attack, secure the situation and conduct investigations. In this respect, ANSSI constitutes a recognised asset in the economic sphere, particularly by the businesses that have called on its services.

23. https://www.zdnet.fr/actualites/notpetya-a-coute-cher-a-saint-gobain-39855594.htm

PART I

LEGAL TREATMENT OF CYBERATTACKS AND ECONOMIC AND SOCIAL CONSEQUENCES

While offences targeting automated data processing systems must of course be considered first (Chapter I), it should also be stressed that more traditional offences are also committed in cyberspace (Chapter II).

CHAPTER I

OFFENCES TARGETING AUTOMATED DATA PROCESSING SYSTEMS (ADPS)

This chapter will cover the definition of ADPS and automated data processing (I), the particular case of connected devices (II), attacks on ADPS, their punishment (III) and their consequences for businesses (IV), which are advised to draw up e-governance rules (V).

SECTION I
DEFINITION OF ADPS AND DATA PROCESSING

■ **8.** An ADPS is a set of processing units, memories, software, data, I/O components and connections, which must be protected by safety devices.

■ **9.** This automated data processing corresponds to different processes of collection, registration, organisation, preservation, adaptation, modification, retrieval, consultation, use, communication by transmission or dissemination or any other form of provision, and reconciliation of personal or non-personal data.

Such systems and data are protected by Law N°. 88-19 of 5 January 1988 known as the Godfrain Law and also, so far as personal data is concerned, by the *Informatique et Libertés* (data protection) Law, as well as by the GDPR, which defines the concepts of personal data, processing, filing system and controller[24].

Specifically, for a business, it concerns its information assets, know-how and data about its staff, customers, prospects and suppliers.

This corporate data is an asset to be protected, since it is what cybercriminals want.

24. GDPR/EU 679/2016

■ **10.** Almost everything, from household appliances to vehicles to toys for children, is in the course of being provided with network and communication connectivity.

The peculiarity of an ADPS is that it develops constantly since the devices that, in the execution of a programme, ensure automated data processing multiply and invade the daily life of a business, including through connected devices.

SECTION II
THE SPECIFIC CASE OF CONNECTED DEVICES

■ **11.** A connected device may be defined as *"a physical object in which technical means are integrated enabling it to collect, store, process and transmit data using wireless technologies."*[25]

These intelligent devices, capable of collecting, analysing and transmitting information relating to their environment, have been deployed within businesses through the prism, in particular, of home automation and mobile telephony.

Hence, any of the following may be classified as ADPS in so far as they store and process digital data: video surveillance cameras, photocopiers, scanners, printers or internal telephone networks.

The expansion of these connected devices multiplies businesses' exposure to attacks and has therefore led to a massive increase in organised or "independent" cybercrime.

■ **12.** Such devices may be classified in three categories by nature:

- sensor-actuator devices that communicate data over a network;
- sensor-actuator, storer, transmitter devices that communicate a significant amount of data to software;
- sensors-actuators, transmitters, storer devices that interact with one another through relay gateways connected to several networks.

Accordingly, the security challenges of free or licensed connected devices that communicate *via* wifi, 5G or RFID are different and dependent on the communicating interconnection.

■ **13.** These devices are not only exposed to the general risks of digital such as physical access to the device and its USB port, allowing

25. Bernheim-Desvaux S., The connected device under contract and consumer law, Contrats, conc., consomm. 2017, étude n°. 1)

modification or access to its memory. They are also exposed to particular risks owing to their nature as devices connected to a network with which they communicate.

The connected device may therefore be attacked because of its purpose, because of the value of the information it receives or gives, as well as the value in taking control of it.

■ **14.** This makes connected devices particularly vulnerable, requiring special attention that is often overlooked within businesses.

This is particularly demonstrated by the "Shodan" search engine, designed by John Matherly, which lists vulnerable devices and devices connected to the internet: webcams, water treatment installations, alarms, wind turbines, licence plate readers, smart TVs, sensitive industrial installations such as power plants, refineries or reactors…[26]

■ **15.** Cybercriminals thus have an infinite number of possibilities for infecting systems *via* connected devices, as demonstrated by the attack on DYN Managed DNS in the United States in **October 2016**, using among other things the online source code which enabled **100,000** connected devices to be infected.[27] Or in **2016** the attack on MIRAI which was conducted from the establishment of a botnet of public cameras, control of which had been taken remotely.[28]

SECTION III
DIFFERENT ATTACKS ON ADPS AND THEIR PUNISHMENT

■ **16.** Attacks on the ADPS of a business may be multiple, including:

- sabotage of networks and infrastructure by alteration, modification, entering, deletion, extraction of data, interference, improper data transmission;
- access to an information system for the deposit of a virus and other software:
  - a CryptoLocker virus that will encrypt data, or even servers, in order to ransom the poorly secured business;
  - espionage software;
- impeding access to systems of messaging, telephony or data-sharing servers, whether through spamming or taking advantage of a vulnerability to deposit a virus encoder;

26. https://money.cnn.com/2013/04/08/technology/security/shodan/index.html
27. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
28. https://www.zdnet.com/article/mirai-ddos-botnet-powers-up-infects-sierra-wireless-gateways/

- interfering in communications between one or more machines to intercept data, correspondence, or to send data by impersonating the owner of the machine.

■ 17. **Offences of attacks on ADPS are provided for by Articles 323-1 et seq of the Criminal Code which render illegal:**

- fraudulently accessing or remaining in an ADPS;
- impeding or distorting the operation of an ADPS;
- fraudulently entering data into an ADPS;
- without lawful grounds importing, holding, offering, transferring or making available a piece of equipment, instrument, computer programme or any data, designed or specially adapted to commit one or more of the offences.

Offence concerned	Penalty incurred	Law creating the offence
Fraudulently accessing or remaining in all or part of an ADPS	Two years' imprisonment and a fine of €60,000. Where it has resulted in either the **deletion or modification of data contained** in an ADPS or an **alteration of the functioning** of the ADPS in question, the penalty is increased to **three years' imprisonment and a fine of €100,000, five years and a fine of €150,000** for a personal ADPS used by the State and, if committed by an organised group, **10 years and a €300,000 fine**.	Article 323-1 of the Criminal Code
Impeding or distorting the operation of an ADPS	Five years' imprisonment and a fine of €150,000. Where the offence has been committed on a **personal ADPS used by the State**, the penalty is increased to seven years' imprisonment and a fine of €300,000 and, if committed by an organised group, **10 years and a fine of €300,000**.	Article 323-2 of the Criminal Code

Offence concerned	Penalty incurred	Law creating the offence
Fraudulently entering data into an ADPS	Five years' imprisonment and a fine of €150,000. Where the offence has been committed on a **personal ADPS used by the State**, the penalty is increased to seven years' imprisonment and a fine of €300,000 and, if committed by an organised group, **10 years and a fine of €300,000**.	Article 323-3 du Code pénal
Fraudulently extracting, holding, damaging, reproducing, transmitting, deleting or modifying data contained in an ADPS	Five years' imprisonment and a fine of €150,000. Where the offence has been committed on a **personal ADPS used by the State**, the penalty is increased to seven years' imprisonment and a fine of €300,000 and, if committed by an organised group, **10 years and a fine of €300,000**.	Article 323-3 of the Criminal Code

■ **18.** These offences against property require the free and conscious will to commit the acts whose attempt is punishable (Criminal Code, Article 323-7), **and the legal entity that has benefited from the fraud may be held liable**.

In practice, identifying the perpetrators of these offences is complex owing to the international dimension of cybercrime and the inherent difficulties in obtaining evidence using digital traces and clues mostly located abroad.

SECTION IV
CONSEQUENCES FOR BUSINESSES OF ATTACKS ON THEIR ADPS

The main aim of attacks on ADPS is, in addition to malicious damage, the fraudulent appropriation of intangible assets (personal data, industrial and commercial secrets etc.). They have major financial and image consequences for businesses, which can even have penalties imposed.

IV-1.
"THEFT" OF PERSONAL DATA, INDUSTRIAL AND COMMERCIAL SECRETS

■ **19.** The appropriation of its data is a major risk to businesses in the event of a breach of their ADPS, as both their industrial and commercial secrets and the personal data of their customers or employees may be stolen.

Article 323-3 of the Criminal Code was supplemented in this respect in **2014**, in order to create the offence of copying personal data where it has not been deleted, since the act of *"fraudulently extracting, holding, reproducing, transmitting, deleting or modifying data (…)"* contained in an ADPS is punishable with **5 years'** imprisonment and a fine of **€150,000**.

In **2011**, PlayStation Network, the Japanese brand Sony's multiplayer gaming, online gaming store and live content service, had the personal data of **77** million users stolen, as well as the bank details of tens of thousands of players. [29]

In **2013**, *Vodafone GmbH*, Germany's second-largest mobile operator, had the personal contact details of nearly two million subscribers hacked. [30]

In **2014**, the computer attack on Orange's website also made it possible to steal the personal data of several hundred thousand customer accounts. [31]

In **November 2014**, the *Sony Pictures Entertainment* subsidiary was attacked by malware, the scale of the impact leading to the departure of the chief executive of the company.

29. https://www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html
30. https://www.bbc.co.uk/news/technology-24063621
31. https://www.theregister.com/2014/05/08/orange_france_hacked_13_million_seeing_red/

The hackers (the *Guardians of Peace*) had stolen **100** terabytes of data containing a great deal of confidential information. Examples of what was stolen included the plot of the James Bond film under preparation, the personal data of **47,000** employees (names, addresses, e-mails, social security numbers, salaries etc.) as well as various email exchanges.

Owing to the content of some of her emails (in particular considered offensive to the then president, Barack Obama), Sony Pictures Entertainment's Director, Amy Pascal, left office and paid the equivalent of $**8** million in damages to its employees and ex-employees following a cyberattack that resulted in the disclosure of their personal details. [32]

Between **March and July 2019**, US bank Capital One had the personal data of **106** million customers stolen from it. This was one of the largest computer hacking events affecting a large US bank, Capital One being the fifth largest issuer of bank credit cards in the US. [33]

IV-2.
FINANCIAL AND IMAGE CONSEQUENCES

■ **20.** Interference with systems of messaging, telephony or data sharing servers, whether through spamming or taking advantage of a vulnerability, directly impacts the activity of business which may find itself slowed down, stopped completely or continuing under downgraded conditions.

As early as **2011**, the attack suffered by EDF known as a "distributed denial of service" attack, which was part of a major offensive by the "Anonymous" organisation appearing under the title "Operation *Greenrights*", resulted in EDF's websites being put out of action three times between **April and June**. [34]

The attack in **November 2016** on German government services which affected the Deutsche Telekom telephone network caused difficulties in connecting to the network for nearly **900,000** people. [35]

32. https://www.theguardian.com/film/2015/feb/04/guardians-peace-revenge-hack-sony-finances-unscathed
33. https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html
34. https://www.lefigaro.fr/flash-actu/2014/11/07/97001-20141107FILWWW00322-juge-pour-avoir-bloque-le-site-d-edf.php
35. https://www.bbc.com/news/technology-38130352

21. The result of this interruption/slowdown of activity is among other things financial.

For example, according to a report by IBM, the average global cost of an IT attack for a business was estimated at $3.62 million in 2017, $3.86 million in 2018 and $3.92 million in 2019. The report also notes that the cost to businesses of a data breach has increased by 12% over the last five years. [36]

These figures take into account not only the costs associated with possible damage to the devices and systems affected by the attack, but also all indirect costs such as the impact on the business's image, loss of revenue and the costs of any legal proceedings, whether relating to the amount of damages awarded to victims, fines or lawyers' fees. Saint-Gobain assessed the cost of the attack it suffered in 2020 at €220 million [37]. The cost of an attack *via* ransomware, suffered in June 2019 by the French group Eurofins, a specialist in bioanalytical testing, was estimated at €62 million. [38]

A cyberattack may also cause a loss of confidence among the business's partners, shareholders and customers by reflecting an image of weakness or lack of reliability.

The US payment processing company *Heartland Payment Services* offered a specific example of this when, following a data leak in 2009, it saw its relationship with one of its main customers, Visa, being called into question. [39]

In March 2017, the US credit analysis agency Equifax, in turn, was the victim of a large-scale attack that enabled hackers to obtain the personal data of more than 145.5 million customers. The company, which acknowledged that it had not reacted even though it had detected a breach, only revealed the attack to its customers in July 2017. By September of the same year, Equifax shares had lost 28% of their value on Wall Street. [40]

22. This damage to image and reputation can also have a significant impact on the business's employees and its ability to attract talent.

36. https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years#assets_all
37. https://www.zdnet.fr/actualites/notpetya-a-coute-cher-a-saint-gobain-39855594.htm
38. https://www.silicon.fr/ransomware-75-millions-e-perdus-pour-eurofins-scientific-335439.html
39. https://www.bankinfosecurity.com/heartland-breach-inside-look-at-plaintiffs-case-a-1844
40. https://www.capital.fr/entreprises-marches/le-pdg-dequifax-demissionne-apres-le-piratage-informatique-1246206

Neither is a business which is the victim of an attack exempt from the risk of penalties, both administrative and legal, in the case of theft and/or disclosure of personal data of customers, suppliers or employees.

IV-3. RISK OF PENALTIES IN THE EVENT OF FAILURES OF SECURITY OF ADPS

■ **23.** Since **25 May 2018**, the European General Data Protection Regulation (GDPR) has introduced new rules for the use and dissemination of personal data concerning all individuals and legal entities that hold and process personal data.

Article 32 of the GDPR and Article **4 paragraph 6** of the *Informatique et Libertés Law* as amended by the Law on adaptation to the GDPR of **20 June 2018** and by Order N°. 2018-1125 of **12 December 2018**, specify that the controller must implement appropriate technical and organisational measures **to ensure a level of security appropriate to the risk**.

■ **24.** The imprudence and negligence of businesses when processing sensitive data are therefore now directly and heavily sanctioned by the GDPR, and failure to take the necessary measures to protect personal data constitutes misconduct for which a business that is the victim of a cyber-incident and its chief executive may be liable.

Two kinds of penalties, administrative and criminal, of different types – and thus cumulative – are provided for if businesses breach the provisions of the GDPR and of the *Informatique et Libertés* Law codified in the Criminal Code.

(i) Administrative penalties

Breaches of the data security provisions may be punished by an administrative fine of up to **€10** million or **2%** of the total annual worldwide turnover of the previous financial year, whichever is greater.

It is in this context that Dailymotion and Uber were sanctioned by the CNIL in **July and December 2018**, for security breaches of their customers' data, to fines of **€50,000** [41] and **€400,000** respectively. [42]

It should be stated that the use of a data management provider does not relieve the company of its obligation to guarantee the security of

41. https://www.lemonde.fr/pixels/article/2018/08/02/la-cnil-sanctionne-dailymotion-pour-un-piratage-de-comptes-d-utilisateurs-en-2016_5338652_4408996.html

42. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000037830841/ ; https://www.lesechos.fr/industrie-services/tourisme-transport/piratage-de-donnees-uber-mis-a-lamende-en-france-par-la-cnil-240511

the data processed on its behalf. This was accepted by the CNIL [whose decisions may be published] on **8 January 2018**, by imposing a penalty of €**100,000** on Darty.

(ii) Criminal penalties referred to in Articles 226-16 et seq of the Criminal Code

Despite improvements in the security policies of information systems and networks, businesses are regularly victims of cyberattacks and data "thefts", owing to lack of effective protection of their systems.

The realisation that such a risk exists outside the organisation imposes a greater obligation on companies to protect their information systems and data…

Thus, in the event of a security breach resulting in the destruction, loss, disclosure or unauthorised access to personal data of customers or employees processed by the business, the business may be subject to criminal liability.

The origin of "such breaches" of personal data may be:

- unlawful or malicious, particularly in the case of cyberattacks or malicious conduct; or
- accidental: inadvertent disclosure by an employee of data, etc.

Their common denominator is a flaw in the protection of information systems and data.

Several offences are aimed at punishing such misconduct by a business in safeguarding its systems and protecting personal data. They are provided for in Articles 226-16 et seq of the Criminal Code:

- Hence, processing or having someone process personal data without implementing the measures prescribed in Articles **24, 25, 30, 32** of the GDPR or paragraph 6 of Article **4** and Articles **99 to 101** of the *Informatique et Libertés* Law may be punished by a penalty of up to **five years' imprisonment and a fine of €300,000** (Article **226-17** of the Criminal Code).
- Failure on the part of a provider of electronic communications services or a controller to notify a breach of personal data to the National Commission for Information Technology and Freedoms or to the person concerned, in disregard of Articles 33 **and 34** of the GDPR or of the provisions of Article 83 and Article 102 of the *Informatique et Libertés* Law, is punishable by **five years' imprisonment and a fine of €300,000** (Article **227-17-1** of the Criminal Code).

- A processor who fails to notify such a breach to the controller, in disregard of Article 33 of the GDPR or Article 102 of the *Informatique et Libertés* Law, is liable to the same penalties (Article 226-17-1 paragraph 2 of the Criminal Code).

In the event of criminal proceedings for failure to protect information systems and personal data, either or both of the company and its lawful representative may be prosecuted, at the option of the public prosecutor.

Either way, if the chief executive of the company is prosecuted, he may avoid criminal liability if he can demonstrate that he had effectively delegated his authority in this specific area.

To be valid, a delegation of authority must meet the following three conditions, namely that the delegate must be competent, independent and have the necessary resources to carry out his role.

As regards the criminal offences under Articles 226-16 et seq of the Criminal Code, the person given such delegation of authority could thus incur criminal liability not only for himself but also for the business, on the same basis as its lawful representative.

Yet it is important to remember that the GDPR's general principle of "accountability[43]" tends **to limit the possible areas of delegation of authority by business leaders to purely operational, rather than strategic, aspects of implementing the measures prescribed by the GDPR or the *Informatique et Libertés* Law.**

FOCUS

COMMENT ON THE DELEGATION OF POWERS RELATING TO DATA PROTECTION

The data protection officer (DPO), whose appointment is provided for by the GDPR, may not be liable for any breach of the Regulation.

As a result, the mechanism of delegating authority in criminal matters is not possible with respect to the DPO, in particular because delegation is incompatible with the independence of the delegate and with the fact that the controller (who, in turn, may benefit from a delegation of authority) must ensure that there is no conflict of interest with the DPO (Article 38.6 of the Regulation).

43. Obligation for all businesses to implement a set of internal mechanisms and procedures to demonstrate compliance with data protection rules.

Such prohibition is deduced:

- from the provisions of Article 38.6 of the GDPR, which provides that the tasks and duties of the data protection officer must not result in a conflict of interests;
- from the G29 guidelines which specify that the delegate is not liable for non-compliance with the Regulation, and that **only the controller or processor may be liable**;
- from the CNIL guide "*Becoming a Data Protection Officer*".

The CNIL had already considered, pursuant to the provisions of Article 46 of the decree implementing the *Informatique et Libertés* Law, that the former data protection correspondent (correspondant informatique et libertés - CIL) could not be the subject **of a delegation in criminal matters which would amount to confusing his role with that of the controller.**

This approach may therefore be applied to the new data protection officer.

In the case of criminal proceedings against the legal entity, it is the lawful representative of the company or the data controller, if he benefits from a delegation of authority, who will be prosecuted, and not the DPO.

In order to avoid liability, the lawful representative of the company will have to **justify the effective implementation of this delegation of authority to the data controller.**

It should be specified that the GDPR's general principle of "accountability" tends to limit the areas of delegation by business leaders to non-strategic operational aspects.

This suggests that **the information systems director of a company could only be a delegate with regard to the operational compliance of systems** and not to the drawing up of personal data policies.

Either way, in the event of a valid delegation, the lawful representative may avoid liability in the area covered by the delegation, unless he has personally taken part in the breach.

(iii) Cumulation of penalties

Finally, it should be recalled that a cumulation is possible between the administrative penalties imposed by the CNIL and the criminal penalties, these being of different types.

On the other hand, under the principle of proportionality, in the event of a cumulation of such penalties the overall amount of the penalties imposed may not exceed the higher amount of one of the two fines incurred, which are already very high.

(iv) Examples of businesses being convicted for failures of security of their ADPS

• Penalties imposed in France

FOCUS

PENALTIES IMPOSED BY THE CNIL

Following a security incident on the website of the Alliance Française Paris Île-de-France association, the data of those enrolled in their courses became accessible.

The CNIL found that basic security measures had not been taken with regard to the procedure for identifying users of the website and for the predictability of URLs and, on **6 September 2018**, imposed a penalty of **€30,000**.[44]

Dailymotion also received a penalty from the CNIL in respect of insufficient data security for users of its video content hosting platform.

Hackers were able to obtain the login details of an administrator account in the company's database, which they were able to access by this means and extract users' personal data.

Despite the technical nature of this type of attack, the CNIL took the view that it would not have been able to succeed had sufficient security measures been put in place and, on **24 July 2018**, it therefore imposed a financial penalty of **€50,000** on Dailymotion.[45]

On **7 May 2018**, the CNIL imposed a penalty of €250,000 on Optical Center for insufficient security of its customers' data, as it considered that the company had failed to fulfil its obligation to secure personal data, disregarding Article 34 of the *Informatique et Libertés* Law.[46]

On **28 May 2019**, the CNIL similarly imposed on Sergic a fine of **€400,000**.[47]

44. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000037435170/

45. https://www.lemonde.fr/pixels/article/2018/08/02/la-cnil-sanctionne-dailymotion-pour-un-piratage-de-comptes-d-utilisateurs-en-2016_5338652_4408996.html

46. https://www.solutions-numeriques.com/rgpd-1ere-sanction-de-la-cnil-contre-optical-center/

47. https://www.cnil.fr/fr/sergic-sanction-de-400-000eu-pour-atteinte-la-securite-des-donnees-et-non-respect-des-durees-de

• Penalties imposed abroad

In **2013**, the "Target" supermarket chain suffered a massive theft of its customers' personal data, including banking details.

More than **80** lawsuits and class actions were brought, including actions against the directors.

The latest estimate of the cost of these claims in October **2017** was **$65 million** in defence and investigation costs. [48]

In the same vein, Yahoo was fined **$35 million** for concealing a massive hacking of users' personal data in **2016**. [49]

On **25 October 2018**, British Airways announced that it had been the victim of a cyberattack. The investigation carried out by the Information Commissioner's Office (ICO) revealed that data, including payment details for **500,000 clients**, had been hacked. In July 2019 the British agency imposed a record fine of **€206 million** on the airline. [50]

The establishment of a system of liability for business victims of a cyber incident owing to the insufficient **safeguarding** of their ADPS by the European General Data Protection Regulation (GDPR), as well as the administrative and criminal penalties that may be imposed by the CNIL, **must encourage businesses to invest in prevention, particularly in respect of personal data, by putting in place security measures within their information systems.**

SECTION V
THE NEED TO ESTABLISH PREVENTIVE RULES OF E-GOVERNANCE WITHIN OVERALL BUSINESS RISK MANAGEMENT SYSTEMS

■ **25.** Today the observation is twofold:

- **zero risk does not exist -** the question is not whether one is at risk of being attacked, but when and how to limit such risk;
- **information systems must be secured** by optimising their ability, using reasonable means, to resist actions that compromise the availability, authenticity, integrity or confidentiality of data and related services.

48. https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031
49. https://www.lesechos.fr/tech-medias/hightech/yahoo-indemnise-les-victimes-du-hack-du-siecle-142766
50. https://www.bbc.com/news/business-48905907

■ **26.** Spreading a culture of cyber security under the leadership of senior management, with the help of the risk manager, is therefore necessary in all businesses and often indispensable to their survival, and may be required by insurers as a precondition for any contract.

FOCUS AND ADVICE

E-GOVERNANCE RULES IN BUSINESS

I. Establish cross-business governance for data and information assets:

- identify the information, as well as the sensitive and strategic data to protect;
- carry out a vulnerability audit;
- draw up a security policy for information systems;
- designate one or more points of contact to take responsibility for these issues;
- establish a crisis management procedure, immediately operational in the event of a cyberattack, including a business continuity and recovery plan;
- comply with the GDPR;
- develop a personal data protection policy, especially in the light of the invalidation of the privacy shield, and have the right binding rules;
- establish procedures to identify security incidents and required notifications (to the CNIL and/or ANSSI, if applicable);
- secure the use of teleworking and, in general, remote working;
- integrate the e-governance rules in the internal regulations;
- draw up an IT charter.

II. Review contracts:

- of data outsourcing and IT protection with service providers so that they comply with the new rules for responsibility between controller and processors;

- of insurance and, in particular, cyber insurance;
- of employment, updating them to include standard clauses relating to data protection or any other source of information about employees and strengthening confidentiality clauses in employment contracts.

III. Train the staff of the business:

- carry out a training and communication plan regarding IT security, the valuing of information assets and the management of personal data, involving all occupations, trades unions and employers' organisations;
- carry out tests at least twice a year.

IV. Have a communication and crisis management plan

- have language ready for internal and external communications;
- have up-to-date contact information for potential contacts that can be reached at any time (ANSSI, police services, communications agency, lawyers, bailiffs).

■ **27.** In the face of the growing and multifaceted threat of cyberattacks to national security, the economy, local authorities, hospitals, citizens and businesses, digital security has become a priority in France. Essential tools for protection include, in the first place, means of cryptography and in particular information encryption technologies.

These tools provide security at the right level when transmitting, storing and accessing sensitive digital data. The applications are manifold: exchanges covered by national defence secrecy, the data of health or regulated professions, technical, commercial and strategic data of businesses, the personal data of citizens, etc.

■ **28.** In this context, French law does not limit the means of cryptology.

Law N°. 2004-575 of 21 June 2004 "*on confidence in the digital economy*" establishes the principle of freedom of use of cryptology, but regulates its use, in particular by requiring prior declarations (*Law N°. 2004-575, 21 June 2004, Article 30*). *Means of cryptology consist of any hardware or software designed or modified to transform data, whether information or signals, using secret conventions or to perform the reverse operation with or without a secret convention. The main purpose of such means of cryptology is to guarantee the security of the storage or transmission of data,*

by ensuring their confidentiality, their authentication or the control of their integrity (...) ».

In this respect, the GDPR presents encryption in a relevant way as "an appropriate guarantee".

FOCUS

CYBERCRIMINALS DO MARKET RESEARCH ON THEIR TARGETS. ONCE THESE HAVE ACHIEVED A HIGHER LEVEL OF PROTECTION, THEY CONCOCT SOPHISTICATED ATTACKS *VIA* THEIR "INTERMEDIARIES" WHO ARE WEAKER IN TERMS OF CYBER SECURITY. HOW CAN WE FIGHT THIS FLAW?

PHILIPPE COTELLE
Head of Insurance Risk Management Airbus Defence and Space
Director of AMRAE, Chairman of the Information System Commission

The rise of digital during the Covid-19 lockdown period has significantly increased the attack surface and created a dependence on digital.

As a result, the bombardment of attacks that took place in the first half of 2020 is, unfortunately, likely to continue. So we rapidly need to find firewalls, or cyber will be tomorrow's pandemic.

The new generation of cybercriminals is conducting market research that has led to a surge in big game hunting, forcing businesses to verify and secure all stages of the supply chain, which first requires an audit of the dependence and penetration of each data processor in the internal organisation of the business.

To deal with this real threat and to remain competitive, businesses must work with partners who are armed and attentive.

Cybercriminals are also “trawling” ransomware campaigns, which target small and medium-sized businesses indiscriminately. These campaigns require few resources for a substantial gain.

SMEs are therefore very concerned, either independently in the context of these attacks or because they are the flaw in the system of other businesses of which they are partners.

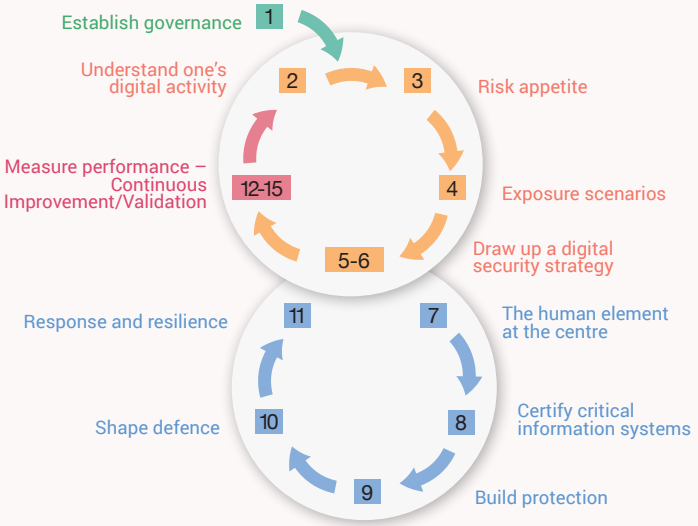
But most of them still do not realise the risk they face which is, quite frankly, the impossibility of overcoming the financial and image loss caused by the attack.

Small businesses must therefore safeguard their information systems and protect their assets by making the necessary investments, including in training, because it will be those who have learned how to adapt that will survive.

Regardless of the size of the business, this safeguarding requires breaking down silos and defining cross-business strategic risks that may affect the existence of a business.

Based on the strategic risk that has been defined and specified in terms of cyber risk, the business will prioritise which protections to deploy in order to defend itself.

The chart below, based on the AMRAE/ANSSI joint report entitled "Digital Risk Control – the Trust Advantage", describes this step-by-step approach aimed at maximising the resilience of the business while minimising the investment effort.



The first of these steps, as part of a digital risk management policy, is the implementation of e-governance and the creation of a risk committee made up of representatives of the business and security teams, to provide a cross-business view of the assets to be protected. The aim is to identify and protect the vulnerabilities of the business, since cyber risk is a threat that may affect them and thus have a major negative impact on the business.

CHAPTER II

TRADITIONAL OFFENCES IN CYBERSPACE

Since acts traditionally punishable under the Criminal Code may be committed in cyberspace, we should study such of these offences as affect the property and reputation of a business.

SECTION I
DAMAGE TO PROPERTY

■ **29.** While crime against automated data processing systems (ADPS) is sanctioned under the criminal law by specific offences and aggravating circumstances, in practice cybercrime corresponds to a list of offences and a way of operating.

Traditional classifications such as fraud, including fraud by an organised gang, abuse of trust, money laundering either alone or by an organised gang (Criminal Code, Article 324-1) also allow many fraudulent acts to be punished in their digital guise.

■ **30.** The list of offences involving damage to property may thus be summarised as follows:

INTERNET FRAUD 313-1 et seq	Domain name fraud	▸ *Typosquatting:* creation of a similar domain name to deceive the victim (amendes-gouv.fr and amendes.gouv.fr) and persuade him to make a remittance	Criminal Code, Article 313-1: 5 years' imprisonment €375,000 (Criminal Code, Article 313-2, paras 1 to 6: 7 years' imprisonment and €750,000 where there are various aggravating circumstances, sentences increased to 10 years' imprisonment and €1 million where the fraud is committed by an organised gang (Criminal Code, Article 313-2, final paragraph).

FORGERY AND USE OF FORGED DOCUMENTS BY INTERNET		▸ *Phishing* : sending fraudulent emails for the purposes of: - Advertising or sales of prohibited products - Fraudulent collection of personal data (codes and bank details etc, e.g. for carding) - Virus infection to control the system and commit fraud	The retailer becomes a victim of the fraud and the bank pays the individual for the fraudulent use of his bank card number which he has not parted with (Monetary and Financial Code). But the criminal case survives for the individual and the retailer.
	Bank card fraud	▸ *Carding* : hacking of a bank card number resold on deep web sites inaccessible to the police (except to organised crime and organised gangs).	
FRAUD (continued)		▸ *Skimming* : retrieving a bank card number by reading the magnetic strip in an ATM. Fraud in respect of housing, rentals etc., and all types. Fake bank transfer instructions by socially-engineered computer manipulation, more rarely using previous malware or taking control of a computer.	
	PBX (telephone exchange) fraud, *phreaking*	Fraud on telephone switches, fraud on communications made to a business's account in order to benefit from gains or services *via* premium-rate numbers.	

EXTORTION 312-1 et seq	These are cyber offences in the strict sense of blocking computers through malware, committed for the purpose of a cyber offence in the broad sense, cf. INTERFERENCE 323-2 and encryption of data.	- Forcing the delivery of characters from video games or units of account *via* the internet to unlock the computer (bitcoin, Ethereum…). -Forcing a business to pay in bitcoin to recover access to its computers that have been encrypted by a virus (also interferes with the system).	Difficulty relating to the material component. Constraint is an element of the offence. 7 years' imprisonment and €100,000 (Criminal Code, 312-1, para. 2). 10 years' imprisonment and €150,000 where there are various aggravating circumstances, including the particular vulnerability of the victim (Criminal Code, Article 312-2).
BLACKMAIL 312-10 et seq	THE SAME, but threat to ruin reputation through revelations, through disclosure of technical vulnerability.	- Threatening to reveal or impute facts likely to impugn a person's honour or esteem in order to obtain a secret, with a transfer of funds from the victim (blackmail).	The distinction of blackmail. The threat of revelation 5 years' imprisonment and €75,000 (Criminal Code, 312-10, para. 310-10). If the threat is carried out, 7 years' imprisonment and €100,000.
ABUSE OF TRUST ABUSE OF WEAKNESS 314-1	*Via* the internet.	Various modes of operation and laundering and concealment of something, etc.	Up to 10 years' imprisonment and €1,500,000.
Any offence committed by the internet or by means of information and communication technologies is intended to be brought within the scope of cybercrime in the broad sense. This table is therefore not exhaustive.			

SECTION II
IDENTITY THEFT THAT DAMAGES THE REPUTATION OF A BUSINESS

■ **31.** Digital identity theft, online identity theft or the use of data of any kind may take many forms. It aims to impersonate someone else (an executive, a business, an authority) to access data or bank accounts and divert funds, or to damage the reputation of a business or its leaders or commit so-called fraud "*à la carambouille*" (the reselling of unlawfully owned goods). (A real supplier is taken in by someone pretending to be his client business and makes a delivery on an industrial estate; he never gets paid, etc.).

■ **32.** The techniques most often used to extract data that enable identity theft to take place are *phishing or the use of keyloggers* (malware that records keystrokes).

Identity theft has been established, for example, in the case of the creation of email addresses, fake Facebook profiles and fake advertisements in order to harm a business leader[51].

■ **33.** 33. In the face of the increase of such attacks on identity *via* the internet, by the law of **14 March 2011** known as "Loppsi[52] 2", the government established the offence of identity theft, which punishes with one year's imprisonment and a fine of €15,000 "*the act of impersonating a third party or making use of one or more data of any kind enabling him to be identified with a view to disturbing his peace*[53] *or that of others, or to impugn his honour or esteem*" (CP 226-4-1).

The rapporteur of the Law of 14 March 2011 stressed that the term "identity" should be understood as "covering all the electronic identifiers of the person, i.e. not only his name but also his nickname or pseudonym used on the internet"[54].

■ **34.** The factual element of the offence of identity theft is either the impersonation of a third party or the use of data enabling a third party to be identified. The mental element involves, in addition to general malicious intent, wishing to disturb the peace of others or to impugn the person's honour or esteem.

■ **35.** The offence of identity theft may be invoked by a legal entity. Indeed, case law considers that in the event of damage to its reputation on the internet, a business, represented by its leader, may act on the basis of the digital identity theft. This text may avoid bringing the discussion into the field of exceptions to the general law, namely the Press Law of **1881** with, in particular,

---

51. Ca Paris, Oct. 10 2014, #13/7387: Comm. 2015, comm. 9).
52. Law of policy and programming for the performance of internal security)..
53. Article 226-4-1 of the Criminal Code.
54. E. Ciotti, NA Report N°. 2271, 1streading, 27 Jan. 2010,.

defamation that is more difficult to characterise and has a short limitation period.

■ **36.** All these legal and regulatory developments reflect a real awareness, very significant on the part of the institutions, of the challenges associated with digital security as a whole, by adjusting the European legal framework to the radical changes that it introduces and by implementing appropriate measures for a successful digital transition.

Risk is the new key concept of the GDPR and NIS. These two texts also shed light on methods capable of limiting the occurrence of risks and minimising them. In the age of the internet and big data, risk is ubiquitous.

FOCUS

WHAT IS THE ROLE OF TELECOMS OPERATORS IN CYBERSECURITY?

NICOLAS ARPAGIAN
Vice President, Strategy and Public Affairs, Orange Cyberdefense

Hackers use communication networks to infect the data servers and information systems of their targets. Detection as far upstream as possible of the equipment concerned becomes a condition for better overall digital security. Guillaume Poupard, the Director General of the National Agency for the Security of Information Systems (ANSSI), made the following observation in **October** 2017[55]: "*In my opinion, the only place where we can act effectively is at the level of the operators who carry these things [malware]. They probably have the capacity to act at that stage.*"

This analysis was put into perspective in the Cyber Defence Strategic Review[56] published by the General Secretariat of Defence and National Security (*Secrétariat général de la défense et de la sécurité nationale* - SGDSN) in **March 2018**, which called on telecoms operators to strengthen their cooperation with the State in order to detect cyberattacks in progress. Its operational application is contained in Law N°. 2018-607 of 13 July 2018 on military programming for the years 2019 to 2025.

55. "ANSSI wants operators to protect the Internet from cyberattacks", Nextépact, Guénaël Pépin, October 12, 2017 - https://www.nextinpact.com/news/105385-lanssi-veut-que-operateurs-protegent-internet-cyberattaques.htm

56. http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

Article 34 of that Law complements the Postal and Electronic Communications Code by establishing an Article L. 33-14 which explains the nature of such cooperation:

> *"Article L. 33-14.- For the purposes of the security and defence of information systems, electronic communications operators may, having informed the National Agency for the Security of Information Systems, use on the electronic communications networks which they operate devices that implement escalating technical markers for the sole purpose of detecting events that may affect the security of their subscribers' information systems.*
>
> *"At the request of the National Agency for the Security of Information Systems, where it is aware of a threat likely to affect the security of information systems, electronic communications operators (having put in place the devices provided for in the first subparagraph) shall proceed to operate them in order to prevent the threat, if appropriate using the technical markers supplied to them by the Agency".*
>
> *"By way of derogation from Article L. 34-1, electronic communications operators are authorised to keep, for a maximum of six months, the technical data strictly necessary for the identification of an event detected by the devices mentioned in the first paragraph of this Article.*
> *Data collected in the course of operating these devices other than those directly needed for the prevention and identification of threats shall be immediately destroyed. »*
>
> *"Where events that may affect the security of information systems are detected, electronic communications operators shall inform the National Agency for the Security of Information Systems without delay. »*
>
> *"At the request of the National Agency for the Security of Information Systems, electronic communications operators shall inform their subscribers of the vulnerability of their information systems or of the attacks that they have suffered.*
>
> *"The detailed rules for the application of this Article shall be specified by decree in the State Council (Conseil d'État). In particular, this will identify the categories of data that may be kept by electronic communications operators. »*

These provisions should allow better anticipation of attacks and be helpful in serving to inform the CERT (Computer Emergency Response Teams) networks that are used by cybersecurity professionals to share information confidentially about the characteristics of detected malware and according to standard protocols. The technical characterisation of such malware will be integrated into

the databases of the information systems' monitoring tools, in order to spot their presence and block as soon as possible their access to the servers of the entity concerned.

Telecoms operators are also on the front line in responding to denial-of-service (DDoS) attacks that lead to overloading access to a website, preventing legitimate internet users (visitors or customers) from connecting to the service. Dishonest service providers offer turn-key solutions, with tens of thousands of infected computers available which may, for paltry sums, be enlisted in a few clicks and result in the unavailability of retail or institutional websites. Operators can, at the request of their customers, filter the connection flow and thus restore the use of the site placed in difficulty.

One of the strengths of a telecom operator that owns its infrastructure, like Orange, whose networks are deployed globally, is to have relays and sensors throughout the world. While attackers support their attack mechanisms from interconnected facilities in several countries, an international cybersecurity provider's presence is an asset for being informed upstream of how hackers intervene, in order to document detection tools quickly. The same is true for the capacity to mobilise operational teams to respond to incidents. Finally, it is advisable that a consideration of cybersecurity should naturally accompany the deployment of digital services offered by telecom operators.

PART II

CYBERATTACK: WHAT JUDICIAL RESPONSE?

CHAPER I

THE PLAYERS AND THEIR INSTITUTIONAL FRAMEWORK

SECTION I
THE FRENCH SYSTEM

The specific nature of cybercrime and the technical nature of cyberoffenders' methods of operation have required the creation of dedicated investigative services and a progressive specialisation of the judicial authorities.

I-1.
SPECIALISATION OF THE INVESTIGATIVE SERVICES

■ **37.** Local complaints and simple cases are handled by police stations and gendarmerie brigades.

■ **38.** Cases requiring further investigation are dealt with by police forces of the *départements*, the investigative units of the gendarmerie and the criminal investigation department in Paris and its inner suburbs.

■ **39.** The most complex cases, for example because of their technical nature and international dimension, fall under the jurisdiction of specialist central services or those assisting a traditional service.

The creation of such specialist services has resulted from the need to adapt arrangements to the strategies used by cybercriminals and has taken place in a general context of mobilising public institutions to enhance the effectiveness of the fight against cybercrime.

These specialist services thus have a vital role in the fight against cybercrime.

Examples include:

- **the Anti-Cybercrime Branch (SLDC)** of the Central Directorate of the Judicial Police, which plays a preventive and law enforcement role: on the one hand, it defines the strategies to be implemented in the areas of operations, training and prevention and, on the other hand, it contributes to the search for evidence of cybercrime offences;

- its Central Office for Combating Crime relating to Information and Communication Technology (*office central de lutte contre la criminalité liée aux technologies de l'information et de la communication - OCLCTIC*) which is responsible for:

  - dealing with illicit content on the internet, its recovery and use;

  - centralising, for the benefit of investigators, information useful for facilitating operational exchanges with internet service providers;

  - the punishment of offences relating to attacks on automated data processing systems, fraud on electronic communications operators, internet scams and attacks on payment systems.

- in Paris and its inner suburbs, for dealing with the specific litigation of offences involving ADPS and data:

  - The Anti-Cybercrime Brigade (*Brigade de lutte contre la cybercriminalité - BLCC*), formerly the Information Technology Fraud Investigation Brigade (*Brigade d'enquêtes sur les fraudes aux technologies de l'information - BEFTI*), has jurisdiction to deal primarily with offences relating to fraudulent access or retention in an automated data processing system (ADPS offences). For the sake of consistency, it absorbed the group of the Means of Payment Fraud Brigade (*Brigade des fraudes aux moyens de paiement - BFMP*) to combat this new economic and financial crime and, in particular, cyber-laundering carried out through dematerialised transactions using cryptoassets.

  It contributes to the dissemination of a culture of cybervigilance and cybersecurity to the general public, IT professionals and, more broadly, the digital world. The Smart Crime Enforcement Brigade (*Brigade de répression de la délinquance astucieuse - BRDA*) deals with online fraud, forgery and abuse of trust.

  - The Juvenile Protection Brigade (*Brigade de protection des mineurs*) deals with cases of child pornography and grooming (meetings offered online to children under false pretexts, often giving rise to serious offences).

  - The Crimes against the Person Enforcement Brigade (*Brigade de répression de la délinquance envers la personne*) deals with defamation, justification of terrorism and criminal labour law *via* the internet.

- The Centre for Combating Digital Crime (*Centre de lutte contre les criminalités numériques - C3N*) is responsible for providing guidance and specialist support for the work of the gendarmerie against cybercrime and digital crime, for conducting or coordinating national investigations of the gendarmerie relating to cybercrime, and carrying out a permanent monitoring of the internet to detect and collect evidence of offences that may be committed there. The network of specialist investigators within the gendarmerie forms a comprehensive and coherent chain of 3,500 gendarmes. Only its Pontoise investigators have national jurisdiction and are trained in investigations on the internet using a pseudonym.

▸ Customs, in particular the National Directorate for Customs Intelligence and Investigations (*la direction nationale du renseignement et des enquêtes douanières - DNRED*) has since 2009 had a body to combat cybercrime known as the e-Customs Service (*Service des cyberdouanes*), otherwise known as the Cybercustoms Cell (*cellule Cyberdouane*). The service collects and uses any information that may be helpful in the fight against internet fraud relating to the trafficking of prohibited, regulated or heavily taxed goods. Its agents conduct an internet watch to establish links between different sites, forums or keywords and to map complex fraud. They seek to identify individuals or entities hiding behind an online sales site, email address or pseudonym on a classified advertisements website, a forum, a blog or a social network. They conduct enquiries into cyber counterfeiting and investigations, including on the darknet.

■ **40.** These services have been heavily mobilised in recent years to meet the challenges of knowing the cyberoffender, developing human resources in intelligence, coordinating information and innovation networks, training of more investigators and international cooperation.

FOCUS ON C3N

“ MEETING WITH COLONEL FABIENNE LOPEZ AND CAPTAIN PAUL-ALEXANDRE GILLOT

Based in Pontoise (Val d’Oise), within the judicial centre of the gendarmerie, C3N is a cutting-edge unit of the gendarmerie in the fight against cybercrime. This specialist service, which was recently demonstrated in Operation EMMA95 against the Encrochat encrypted communication network, or in the dismantling of several networks of machines infected by the Retadup botnet in the summer of 2019, is led by Colonel Fabienne Lopez.

Could you introduce us to C3N, its origin and role?
Established in 2015, C3N is historically heir to the Department of Combating Cybercrime (*département de lutte contre la cybercriminalité*) established in 1998 within the Technical Service for Judicial Research and Documentation (*Service technique de recherches judiciaires et de documentation*), which later became the STRJD. C3N is an investigative unit with national jurisdiction whose main role is to investigate cybercrime, namely attacks on automated data processing systems, traffic on the darknet or through other communication systems (WhatsApp, Telegram, Snapchat, etc.), scams in various forms (SPAM, *phishing*, or fake technical assistance), etc.

C3N consists of 42 people in 4 departments with well-defined roles:

- the coordination department, which organises and coordinates the Cybergen chain, a community of around 3,500 gendarmes;
- the technical department: research and development, a rare centre of expertise for the benefit of investigations and support in terms of digital investigations;
- the department of cyber design and development, which works to create and develop cyber tools that all investigators can use in the field (open source research);
- the investigations department, which is divided into 5 groups. It conducts C3N's investigations and supports and coordinates the action of the 11 C3N branches located across the country.

The **C3N investigations department**, which is dedicated to conducting **the most complex cybercrime investigations**, either alone or in co-operation with regional units, on **matters of national and international scope, is headed by Captain Gillot. As such, C3N is, in particular, responsible within the gendarmerie for the fight against:**

- criminal organisations using, among other things, botnets (Retadup in 2019), encrypted communication systems (Encrochat since 2017));
- illegal trafficking on the darknet, in particular massive sales of drugs and arms trafficking;
- attacks on ADPS, particularly in the form of ransomware. **With regard to ransomware attacks, C3N's jurisdiction to conduct investigations will depend on the malware used for the attack.** Ransomware is allocated by families, themselves distributed between the specialist services;

- complex scams such as fake computer repairs;
- sexual attacks against minors on the internet;
- investigations involving all cryptoassets. Indeed, cryptocurrencies are at the centre of all cybercrime cases and are becoming a true horizontal theme. The main challenge is the de-anonymisation of criminals by tracing cryptocurrency flows and demixing transactions.

Also, in connection with the J3 section of the Paris Public Prosecutor's Office, which specialises in cybercrime, C3N works in consultation with international institutions (Europol, Interpol, etc.), but also with many private companies, in order to obtain intelligence (access providers, telephone operators, antivirus developers, etc.). C3N also provides technical support to field units in terms of cybercrime, and takes part in the training of specialist investigators on specific aspects, such as investigations using a pseudonym.

Can you tell us about a completed investigation and a dismantled network?

C3N has recently been successful in neutralising the international computer virus "Retadup".

Created in 2016, the Retadup botnet had 11 different versions and 20 embedded domain names. Its potential for trouble-making was due in particular to a remote control tool (cryptocurrency mining), massive theft of personal data (theft of medical data from an Israeli hospital, seizure of stored passwords) and the implementation of coordinated offensive action.

In total, the botnet controlled more than 1.327 million softwares without their owners being aware.

On 25 March 2019, the antivirus company Avast reported a wave of infections on 200,000 PCs worldwide, including a C&C server in France, which enabled C3N to be instructed by the cybercrime section of the Paris Public Prosecutor's Office to conduct the investigation.

Upon judicial requisition, a copy of the C&C server was made at the host and 11 versions of the malware were discovered during its analysis. A flaw in the implementation of the Retadup botnet was also updated, allowing C3N to create its own C&C server with a view to replacing Retadup's server and thus enable the neutralisation of the bot software.

On 1 July 2019, acting very discreetly in order not to be detected by the cybercriminals, C3N replaced the C&C server with the one which

it controlled. The FBI supported their work by taking charge of the redirection of the domain names.

The C3N server then recorded more than one TB of logs, which enabled the progressive disinfection of the 1.327 million Retadup-controlled machines to be managed live.
The investigations continued with the opening of a judicial investigation at the Paris Regional Court (*Tribunal de Grande Instance - TGI*).

What is your opinion on international cooperation in respect of cybercrime? Has it progressed in recent years and in what way is it essential in the fight against cyber attackers?
As regards cyber litigation, the latest cases of C3N and other specialist services have highlighted more than ever the exponential need for international cooperation.

Today, it is common to face opponents who have infrastructure spread across different countries. International cooperation is therefore essential, first for practical reasons such as the need to obtain a copy of the servers quickly before the evidence disappears. In terms of the investigation itself, if another foreign agency is investigating the same group we conduct a 'deconflicting' upstream, which is helpful for the next stage of the investigations, etc., and even divide up the tasks to be carried out.

Moreover, when planning an operation, it is not uncommon for cyber litigation to take place in a coordinated manner involving different countries.

There are several modes of cooperation:
- bilateral police to police;
- in the context of more comprehensive cooperation involving Europol and/or Interpol;
- more fully in the context of an ECE.

In the fight against ransomware, for example, the last family to be taken on by C3N required cooperation from the outset with 5 countries to cross-reference the elements of the attack, obtain copies of the servers brought to light in the course of negotiation, then carry out a 'deconflicting' of the investigation itself. While the first crime in France dates back to September 2020, the first coordination meetings have already taken place with Europol and Interpol, in the course of which France has been in a position to take the lead in the investigations.

Referrals of the J3 cybercrime section of the Paris Public Prosecutor's Office now systematically mention the authorisation to share details of the investigation with Europol and its Member States. »

I-2.
THE SPECIALISATION OF JUDGES

■ **41.** The specialisation of judges and public prosecutors, whatever their level of jurisdiction, has also proved necessary.

Law N°. 2016-731 of 3 June 2016 thus strengthened the provisions of Part XXIV of Book IV of the Code of Criminal Procedure.

Article 706-72-1 of the Code of Criminal Procedure thus gives the Paris Public Prosecutor, the prosecution centre and the Court of Justice and Assize Court of Paris **concurrent national jurisdiction** in respect of attacks on ADPS and on the fundamental interests of the nation (cybersabotage), as regards complex and geographically extensive matters.

The referral of a matter to the Paris Public Prosecutor's Office and Court of Justice, based on their concurrent national jurisdiction for offences relating to ADPS, may not be made by a party claiming damages but only by the public prosecutor's office of another court with territorial jurisdiction that wishes to transfer it to the court in Paris.

■ **42.** Such specialisation was reinforced by Law N°. 2019-222 of 23 March 2019 which established a new jurisdiction for the Paris Court of Justice, which became the national court responsible for combating organised crime (*juridiction nationale chargée de la lutte contre la criminalité organisée - JUNALCO*). It brings together specialist judges responsible for conducting large-scale investigations, frequently involving national or international investigations, particularly in the field of cybercrime [57, 58].

The creation of JUNALCO also led to the reorganisation of the Paris Public Prosecutor's Office into 3 divisions by specialisation, J3 being made responsible for the fight against cybercrime.

---

57. Circular of 17 December 2019 on the concurrent national jurisdiction of the Paris Regional Court and Assize Court in the fight against highly complex organised crime and on explaining the role of the various judicial players in the fight against organised crime.

58. Interview with R. Heitz, Gaz. PAL. feb 4 vol. 2020, n°. 369 x 4, p. 10.

FOCUS

MYRIAM QUÉMÉNER
Prosecutor (*avocat général*) at the Paris Court of Appeal

What do you think of the specialisation of judges in respect of cybercrime?
"It is indispensable in my view, not only in order to have a vision and knowledge of the operating methods of offenders, which are increasingly sophisticated, but also in order to manage the international dimension and have contacts within Interpol, Europol and the FBI, for example.

This training must also focus on the special investigative techniques harmonised by the 2019 Law, which are very regulated from the legal point of view and need to be safeguarded in order to ensure that the procedures are carried out. This is particularly so in respect of investigations using a pseudonym, geolocation and remote data capture.

Given the constant evolution of the subject matter and the ceaseless imagination of cybercriminals, such training must be continuous.

It should include monitoring of the case law of the European Courts and a permanent legal watch.

Judges would also need to be integrated into the cyber community and to participate in think tanks and various major events on the subject bringing together professionals in the field.

It also requires the establishment, not only for public prosecutors but also for judges and at every level of jurisdiction, of a sophisticated digital and cyber department, made up of judges and executives specialising in digital technology."

■ **43.** Dealing with cybercrime requires knowledge of the evolving operating methods of cybercriminals. This requires strong partnerships with key players upstream from the courts, particularly the National Agency for the Security of Information Services (ANSSI) which acts on the front line in identifying the damage resulting from cyberattacks and is able to detect, for example, which ransomware has been used by cybercriminals.

FOCUS

RÉMI HEITZ
Public Prosecutor of Paris

How is the Paris Public Prosecutor's Office organised to respond to the increase in the number and magnitude of cyberattacks?
*"The Paris Public Prosecutor's Office is a central player in the fight against cybercrime, as it has concurrent national jurisdiction in respect of attacks on automated data processing systems. It is therefore designed to deal with large-scale cybercrime cases committed in France and to centralise procedures, working alongside local public prosecutors in whose regions the attacks may have taken place. As a result, the recent proliferation of cyberattacks has direct effects on its work. For the year **2020**, for example, the J3 section dedicated to cybercrime recorded 397 references under its national jurisdiction, compared to only **62** in **2019**.*

*To respond to this phenomenon of national importance, this section has since **1 February 2020** been absorbed into the public prosecutor's office of the national court responsible for combating organised crime (JUNALCO). This organisation enables judges and officials to liaise with other sections specialising in large-scale organised crime (organised crime, financial crime) to establish possible links and develop synergies that enhance effectiveness in action. The section is also more easily identifiable, both by other public prosecutors' offices and by its foreign partners. The international ramifications of this de-territorialised crime require strong international collaboration, and the Paris Public Prosecutor's Office continually looks outward in order to respond.*

*In addition, the three judges in this section are now assisted, since the end of **2020**, by an assistant lawyer specialising in international mutual assistance in criminal matters, a liaison officer of the national gendarmerie and an assistant from the national police specialising in the handling of ransomware.*

Beyond these staffing reinforcements, which will continue to increase over the coming years, the decision has been taken to establish an out of hours office dedicated to cybercrime that is open in the evenings and at weekends. As a result, specialist judges can now respond immediately, at any time of the day or night, to any major cyberattack anywhere in the country."

What criminal strategy are you putting in place to combat cybercrime?
"To combat cybercrime effectively by reducing the number of attacks, we need to establish criminal liability, unmask the perpetrators of the attacks and punish them. We are not dealing with computer geniuses who want to play with the authorities, these are primarily offenders. Our strategy must therefore be responsive, adaptable and resolute.

In order to limit the scale of attacks, we must look very closely at the techniques used by the hackers. To do this, the centralisation of case files is a real asset. In particular, the Paris Public Prosecutor's Office takes on all ransomware, computer repair fraud and jackpotting cases. It instructs the central offices to investigate them (the Central Office for Combating Crime relating to Information and Communication Technology – OCLCTIC – and the Centre for Combating Digital Crime or C3N). This provides an overview of organised crime networks and a fine-tuned, cross-referenced observation of the mechanisms implemented, and it means that attacks are not suffered passively. By mapping the technical infrastructure of cybercriminals, we can move up more quickly through the modus operandi to the perpetrators when there are new outbreaks of an attack. The recent dismantling of the Egregor ransomware in Ukraine, with the participation of the Paris Public Prosecutor's Office, confirms that these efforts are paying off.

To confront a multifaceted crime that regularly reinvents itself, you must also be trained and informed. In this respect, we have strengthened our ties with the private sector and the research sector. We frequently work with incident recovery companies to obtain their response reports and the technical information in their possession. They intervene rapidly with victims to put a stop to the effects of an attack and thus have know-how whose sharing helps us in our investigations. We are also in contact with a PhD student at the École Normale Supérieure who helps us rethink our techniques of investigation in the field of cybercrime. This openness beyond the traditional borders of the judicial world is essential if we wish to be effective and to be able to convict increasing numbers of cybercriminals. In order to benefit all stakeholders from our reflections, we will distribute in 2021 a template for making a complaint and an emergency form for all police and gendarmerie services. It is essential to be able to act quickly by freezing data with foreign authorities as soon as possible after an attack.

Once individual liability has been established, we obviously send a message of resolve. This is the only way to put an end to cybercriminals' sense of impunity. Our resolve is first expressed in the conduct of enquiries or judicial investigations. At this stage, we regularly apply for the seizure of criminal assets where they exist. We cannot accept that some people are getting rich through these crimes. Next, at the criminal hearing, the same firmness is applied and prison sentences are requested. However, for our submissions to be accepted, it is essential to work at educating the court, because we are presenting mainly technical files involving experienced criminals and very complex modus operandi."

Do you think that the current body of law is sufficient to respond to this scourge?

"Cyberattacks have multiple modus operandi and are constantly developing. They call for a permanent adaptation of the judicial system,

*but the flexible framework of the Law of **5 January 1988** known as the Godfrain Law, which established the offences of attacks on automated data processing systems, enables us to get to grips with new phenomena in the field of cybercrime. Indeed, it punishes all actions capable of harming an automated data processing system, without laying down a precise and binding list.*

However, in the face of the increase in cybercrime, the police and gendarmerie services have had to adapt their investigative techniques. Some technical processes are not available in France. Moreover, some other techniques are still not provided for in the Code of Criminal Procedure, because the legislature were not able to anticipate their creation. So we are in a form of technology race that requires ever more effective human and material resources."

What advice can you give businesses in this area?
"The fight against cybercrime requires everyone's commitment in order to reduce our exposure to the risk of cybercrime. However, if a business experiences a cyberattack despite taking internal precautionary measures it should, first of all to stop the attack, prevent the system from being further infected by disconnecting the infected machines from its network and the internet and by calling in a technician, a computer incident response company or the National Agency for the Security of Information Systems (ANSSI), depending on the size of the system affected.

More specifically, in order to ensure the effectiveness of the criminal response, in the event of a ransomware attack people are strongly advised against paying the ransom. Such payments do not guarantee the recovery of data or protect against new attacks, and help to fund the cybercriminal ecosystem. It is also essential to retain the evidence, or to have it retained by a professional, such as an example of a booby-trapped message or the ransom note. Finally, it is essential to file a complaint with the police or gendarmerie service that has jurisdiction in the region. If the attack is massive, the Paris Public Prosecutor's Office, which will have been informed by the public prosecutor to whom the case was initially referred, will be able to deal with the case under its concurrent national jurisdiction."

I-3. THE ROLE OF THE NATIONAL AGENCY FOR THE SECURITY OF INFORMATION SYSTEMS AND THE INDEPENDENT ADMINISTRATIVE AUTHORITIES

■ **44.** ANSSI, the National Agency for the Security of Information Systems, coordinates government action on the protection of information systems and has strengthened links with other independent administrative authorities such as the Financial Markets Authority (*Autorité des Marchés Financiers - AMF*), since

February 2018, which has warned about the risks of cybercrime for financial and stock markets. In its 2018-2022 Strategic Plan, the AMF recalls the significant challenge that cybercrime has become, as well as its willingness to develop new expertise to respond to it.

■ **45.** An agreement of 19 January 2018 between ANSSI and the Prudential Control and Resolution Authority (*Autorité de contrôle prudentiel et de résolution - ACPR*) also provides for a regular exchange of information concerning incidents affecting the security of information systems, as well as cooperation in the management of possible crises and, more generally, in the field of digital security.

■ **46.** TRACFIN, the administrative service for the processing of financial intelligence, has a "cybercrime" cell whose work is mainly devoted to blockchains, the darknet and child pornography.

SECTION II
INTERNATIONAL POLICE AND JUDICIAL COOPERATION

■ **47.** Cybercrime, by its essence global and borderless, demandsinternational cooperation.

II-1.
THE PLAYERS AT EUROPEAN AND INTERNATIONAL LEVEL

■ **48.** At the European level, Europol, the European agency specialising in criminal law enforcement, which supports the 27 Member States of the European Union in their fight against cybercrime through the establishment of an information channel between Europol and the Member States.

In 2013, the European Centre for Combating Cybercrime (EC3) was established to facilitate European operational and analytical cooperation between law enforcement agencies, universities and the private sector.

At the end of 2019, Europol adapted its so-called "2020+" strategy, which includes several aspects relating to cybercrime: strengthening the agency's analytical capacity, the management of information, defining an innovation strategy, establishing a laboratory for innovation and emerging technologies which will enable experts from law enforcement agencies, universities and the private sector to be brought into contact.

Europol's work resulted in January 2021 in the dismantling of the Safe Inet network, one of the largest virtual private networks

(VPNs) in the world.

This network was used by cybercriminals, including for ransomware attacks and the hacking of bank card data. The security forces, under the command of the Rentlingen police in southern Germany, confiscated this Safe Inet VPN service on Monday, **11 January 2021**, disabling its servers that had been active for more than a decade. Safe Inet was used by some of the world's largest cybercriminals, responsible for ransomware attacks, hacks of data, bank cards and other forms of cybercrime.

■ **49.** At the international level, **Interpol** provides a platform for cooperation enabling police authorities to work directly with their counterparts.

For example, in **December 2020** Interpol's cybercrime unit sent a warning message to its **194** member countries, calling on them to prepare for organised crime actions focused on vaccines against the coronavirus. In an Orange secure warning notice, the international police cooperation organisation based in Lyon warned of "potential criminal activity linked to counterfeiting, theft and illegal promotion of Covid-19 vaccines". Today, sites selling these fake vaccines have multiplied.

■ **50.** A cooperation agreement between Interpol and Europol was signed in **2001** and approved by the Council of the European Union on **27 June 2001**, and by the Interpol General Assembly at its 70th session held in Budapest on **26 September 2001**, organising co-operation in the fight against international crime, in particular with regard to the exchange of information.

And Interpol for Innovation (CMII), specialising in the fight against cybercrime, was established in **April 2015** in Singapore and works to improve the technical skills of the investigative services and the development of transnational tools.

II-2.
TEXTS CURRENTLY UNDER DISCUSSION

■ **51.** E-evidence

On 17 April 2018, the European Commission presented a draft regulation and directive on cross-border access to electronic evidence in criminal matters: "E-evidence".

This draft regulation aims to facilitate the obtaining of electronic evidence (such as e-mails or other documents located in the cloud), necessary for investigations by the judicial authorities. Having an extraterritoriality effect, it appears as a response to the

promulgation of the "Cloud Act" in **March 2018**.

The draft "E-evidence" directive lays the groundwork for EU-US cooperation and provides a model for coordination of access to electronic evidence. It has created the obligation for legal entities established outside the EU to appoint lawful representatives on European territory.

II-3.
THE 2ND PROTOCOL TO THE BUDAPEST CONVENTION

■ **52.** Negotiations on the conclusion of a second Additional Protocol to the Budapest Convention of 27 November 2001 began in June 2017 and are expected to be concluded shortly [59].

■ **53.** The aim of this Protocol is to strengthen international cooperation among the **67** signatory countries, in particular with regard to access to electronic evidence, the improvement of mutual legal assistance and the organisation of joint investigations through measures intended to improve:

- international cooperation between law enforcement and judicial authorities, including legal assistance between authorities;
- cooperation between authorities and service providers in other countries;
- conditions and guarantees of access to information for authorities in other countries;
- data protection requirements.

FOCUS

INTERNATIONAL ACTION AGAINST ORGANISED CYBERCRIME MUST BE A PRIORITY

by BERNARD BARBIER[60], JEAN-LOUIS GERGORIN[61] and ÉDOUARD GUILLAUD[62]

France, like other democracies, faces an exponential growth in organised cybercrime.

59. The Budapest Convention on Cybercrime is the first international treaty to, in particular, establish international police cooperation to obtain data held in another country.

This is based on the existence of mafia groups established in countries, clearly identified, that have not ratified the Budapest Convention on Cybercrime. These groups have no difficulty in recruiting talented computer scientists naturally attracted to the core business of cybercrime, ransomware attacks, which is probably the most rewarding and least risky criminal activity in history.

Indeed, these groups, at least tolerated by the authorities of the countries concerned, enjoy near-total impunity. The result is an ecosystem in which large groups of cybercriminals, comfortably located in safe haven countries, are developing increasingly sophisticated malware that they offer, with ad hoc access, in the form of "ransomware as a service" to direct attackers.

Against this background, it is no wonder that only an infinitesimal proportion of the world's leading cyber criminals are being brought to justice. In the face of the explosion of cyber hacking, we are advocating active international action at national or European levels to encourage safe haven States to end impunity for cybercriminal groups. This policy should be accompanied by a deterrent, to be spelt out in the French academic law of cyber defence and, where appropriate, implemented, the possibility of retaliating through information technology to cyberattacks against the nation's economic or survival potential, as theoretically provided by Article L. 2321-2 of the Defence Code. Interestingly, the United Kingdom recently created a National Cyber Force to retaliate digitally against not only States, but also cybercriminals digitally attacking the "realm".

Finally, the explosion of cyber threats seems to us to justify the creation of a national cyber coordinator alongside the President of France, like the national intelligence and counter-terrorism coordinator who has demonstrated his effectiveness [63].

60. Bernard Barbier is a former Technical Director of the General Directorate of External Security (*Direction Générale de la Sécurité Extérieure - DGSE*) and a former Director of the Laboratory of Electronics and Information Technology (*Laboratoire d'Électronique et de technologies de l'information - LETI*). He is a member of the Academy of Technologies.

61. Jean-Louis Gergorin, Lecturer at Sciences Po, former head of the Centre for Analysis and Forecasting at the Quai d'Orsay, is co-author of "Cyber - the permanent war" (Éditions du Cerf 2018).

62. Admiral Edward Guillaud is a former military Chief of Staff. He is a member of the Marine Academy.

63. The World 5/01/2021 "*Cyber coercion must be combated by a national and global strategy*"

CHAPTER II

THE IMPLEMENTATION OF CRIMINAL PROCEEDINGS AND THE MEANS OF EVIDENCE

SECTION I
THE COMPLAINT

I-1.
THE FILING OF A COMPLAINT

■ **54.** The simple complaint is the preliminary stage to the commencement of a judicial investigation.

Any natural or legal person, or any organisation that is the victim of a cyberattack, may file a complaint, whether or not the perpetrator is identified. In the latter case, the complaint is filed against X.

■ **55.** Since the majority of cyber-attack offences are lesser offences (*délits*), in order to be admissible the complaint must be filed within a maximum of 6 years from the date of commission of the offence, but in reality it must be filed as soon as possible, for when it comes to cybercrime it is essential to proceed quickly and to be responsive.

A complaint filed promptly results in the opening of an investigation which, in turn, allows the preservation of evidence, the use of service providers and technical experts by the investigators and the deployment of international cooperation, etc.

(i) At a police station or gendarmerie

FOCUS

FILING OF A COMPLAINT

To file a complaint **with the law enforcement agencies**, it is enough to go to the police or gendarmerie station nearest to the business or to the place where the facts were discovered. By way of reminder, police officers and staff or gendarmes are obliged to receive complaints, even if the facts of the case do not fall within their geographical area of jurisdiction. Only in exceptional cases will the complaint be filed with a specialist service geared to cyberattacks.

Within these services, investigators generally specialise in the fight against cybercrime and, failing this, they will direct the business to the specialist service - see Part **I.1.**

The representative of the business, if possible bringing a copy of its registration details (*extrait KBIS*) less than **3** months old and a power of attorney if he is not the business leader, goes to file a complaint, describe the facts found and, with as much detail as possible, discuss any modus operandi identified.

If the business has dedicated resources for digital protection, either internally or through a service provider, it is important that these professionals attend the filing of the complaint and provide technical details establishing the facts. It may therefore be appropriate to be accompanied by the IT security officer or the person appointed to handle the incident.

The information to be produced may be:

- the exact description of the incident;
- contact details for all stakeholders or service providers who may be able to provide information to the investigators;
- all the technical details it has been possible to collect: computer traces of the attack (for example, connection logs), the exact address of the machine(s) attacked (specifying whether it is an office workstation, a mobile or an attack on the website, or the server hosted by an internet service provider);
- emails relating to the infringement, the organisation chart of the company, a list of personnel, contact details of the various **service providers** (e.g. host, security company).

It is essential, upon discovering the offence, to preserve (or have preserved by any service provider, particularly a bailiff) all traces of the attack, including a copy of the state of the servers and networks.

■ **56.** It is also possible to file a complaint with the public prosecutor of the court of justice within the territorial jurisdiction of the business's registered office by post **(ii)** or online **(iii)**.

(ii) At the public prosecutor's office which has territorial jurisdiction to investigate the cyberattack, the complaint being formalised by filing it in person or sending it by registered letter with acknowledgement of receipt.

This is usually done through a lawyer who will draft and document the complaint before filing it in person with the public prosecutor's office.

After the complaint has been registered, the public prosecutor will refer it to the appropriate investigation service.

(iii) Online complaint

Law N°. 2019-222 of 23 March 2019 on programming and judicial reform introduced **the possibility of filing a simple online complaint**[64] for certain offences[65].

The first public prosecutor deemed to have jurisdiction is that of Nanterre (the place of receipt of the online complaint). In the light of the first investigations carried out by OCLCTIC, the Nanterre Public Prosecutor will forward the complaint to the public prosecutor who has territorial jurisdiction to continue the investigation.

(iv) A complaint that includes an application to join the proceedings as a civil party

A complaint that includes an application to join the proceedings as a civil party, lodged with the senior investigating judge, may be filed at the end of three months of ineffective investigation following the filing of a simple complaint (Article 85 of the Code of Criminal Procedure) or if the simple complaint has been discontinued.

This will result in the appointment of an investigating judge who must call for the file, to take note of it. Sometimes he will need to wait for responses to submissions previously made in the preliminary investigation.

I-2. THE HANDLING OF A COMPLAINT

■ **57.** As soon as a complaint is filed, the offence that has been committed or attempted is brought to the attention of the public prosecutor, who assesses the judicial action to be taken.

Where investigations require special technical assistance and/or where the damage is significant, the public prosecutor may decide to entrust the investigation to a specialist service, or that the investigations should be carried out in partnership with a specialist cybercrime investigator.

---

64. Article 15-3-1 of the Criminal Code.

65. http://www.textes.justice.gouv.fr/art_pix/Article_14_Plainte_en_ligne_190324_V1.pdf

■ **58.** The investigators may be required to travel to the business's premises and request access to employees' computers with their consent (particularly in order to detect a malware infection), make a copy of the digital media that are of interest to the investigation or access certain locations or offices of the business, especially where the attack or offence was committed by a person within the business or a subcontractor.

They may also summon qualified individuals (computer technicians, security officers of information systems, etc.), witnesses or, possibly, suspects in order to interview them.

I-3.
THE INVESTIGATION

■ **59.** The Code of Criminal Procedure provides that investigations may be conducted under three legal frameworks that confer different coercive powers on the investigators:

- an expedited investigation, where the facts are revealed very soon after taking place;
- a preliminary investigation, where the conditions for an expedited investigation are not met;
- a warrant (*commission rogatoire*) by the investigating judge who has been appointed.

■ **60.** The public prosecutor and the investigating judge may respectively issue an application for international criminal assistance (*demande d'entraide pénale internationale - DEPI*), an international warrant to conduct investigations abroad or a request for a European investigation (*demande d'enquête européenne - DEE*). Exchanges will then take place, in particular between the French agencies, ANSSI, Europol, Interpol, foreign police forces, and/or foreign judges.

I-4.
POSSIBLE JUDICIAL FOLLOW-UP TO THE INVESTIGATION

■ **61.** At the end of the investigations, the entire investigation file is forwarded to the public prosecutor who decides the direction of the case, because he has the discretion to prosecute.

■ **62.** He may thus decide:

- **that the case should be discontinued**, for various reasons such as:

- the lack of an offence (the facts cannot be characterised as criminal)
- the offence is insufficiently characterised
- the perpetrator has not been identified
- the facts are statute-barred
- on discretionary grounds (where there is minor damage that has been repaired, etc.);

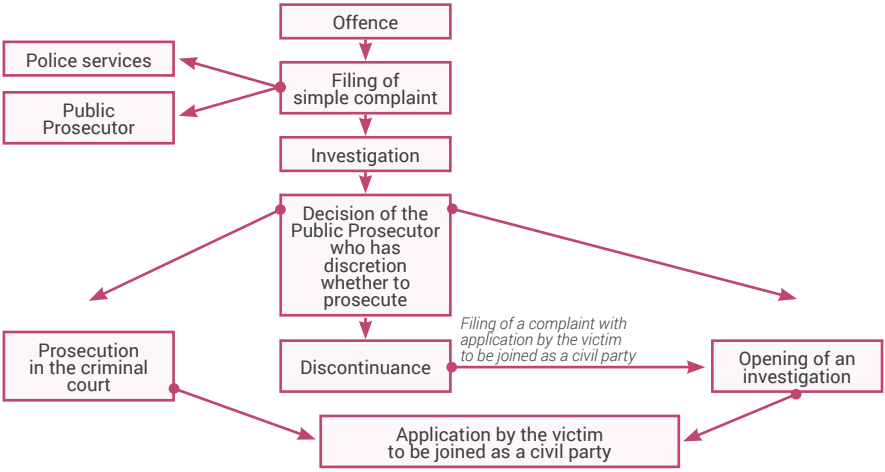
▸ that alternative measures to prosecution should be taken;

▸ **that the perpetrator should be prosecuted in the criminal court**;

▸ **that an investigation should be opened** and an investigating judge appointed where required by the complexity of a case, particularly from a technical point of view, or by its media coverage.

Where a case has been discontinued, the victim may challenge this by applying to the Attorney General (40-3 of the Code of Criminal Procedure) or by filing with the investigating judge a complaint that includes an application to be joined as a civil party. This possibility is also available to the complainant if no investigative act has been taken within three months or if the public prosecutor has not taken a decision within the same period.

■ **63.** In the event of a prosecution in court or the opening of an investigation, the victim may apply to join the proceedings as a civil party, either simply to support the prosecution or to make a claim for damages.



FOCUS

ANNE SOUVIRA
Chief Superintendent, Officer Responsible for Cybercrime Issues at the office of the Paris Metropolitan Police Commissioner;
Head of the new "Cyber" Task Force of the Police headquarters since 2021 in the Directorate of Innovation, Logistics and Technology

Do you think businesses are sufficiently informed and know how to respond in the event of a cyberattack?
"Although some businesses have made progress, often the largest ones are not sufficiently informed or prepared to respond to a cyberattack. They are still under-equipped in cybersecurity from a technical point of view through lack of dedicated budgets, as well as in the training/ awareness of managers and employees, which are the two cornerstones - technical and human - of cybersecurity.

Businesses, which are all subject to cyber threats, must learn to anticipate and consider how they would respond to the types of attack that they may experience. For example, a phishing email that with one click lets in ransomware data encryption bringing down the whole system, and therefore the business, is not the same as a phishing email sent to a supplier in a sales scam whereby a business is asked to change the bank account details to which an invoice is to be paid, or forged transfer instructions sent in a so-called fake president fraud, which are still fashionable.

Businesses really need to raise awareness, conduct cyber risk analyses (on data and networks) and integrate cyber security into their business plans. This means being prepared to finance the technical, organisational and human resources needed to anticipate and manage an attack. No system is inviolable, and attacks may be direct or even indirect by way of service providers, business suppliers or people with access to the extranet, all of which are gateways for attackers (e.g. NotPetya, collateral damage originating from the Ukraine, or a legitimate update that includes a code modified by hackers such as the Solarwinds case, the imagination is limitless)."

What information is most often requested by businesses that are the victims of cyberattacks?
"Most often, businesses wish to know who to file a complaint with.

For the filing of complaints, it is usually the system of single windows that will apply, i.e. the victims will go to the gendarmerie brigade or police station that best suits them, which will notify the public prosecutor, who will choose the investigative service.

Sometimes a slightly different treatment may be reserved for certain cyberattacks. For example, in the case of ransomware attacks, the number of these is such that they have been distributed by type between different specialist services of the national police (OCLCTIC and BL2C, the former BEFTI of the Police headquarters) and the national gendarmerie (C3N). Therefore, depending on the name of the ransomware concerned (Egregor, Ryuk, M88P, etc.), the complaint will be taken by the specialist service already working on the same ransomware.

The Public Prosecutor's Office at the Paris Court of Justice, cybercrime section (J3) which has concurrent national jurisdiction, organises the distribution and monitors the investigations.

It is always possible to address a complaint directly to the public prosecutor, who will refer it to the investigation service.

It should be noted that, in the case of vital operators, the matter will always be referred to the judicial section of the DGSI. Organisations within this category normally have a correspondent at the DGSI who will guide them in respect of their complaint."

Do you think that the current law enforcement system and existing investigative techniques are suitable for combating cybercrime?
"Yes, the law enforcement system as such is suitable for distributing and attributing resources from the simple to the most complex, despite the length of time it has been in place. This field appears as recent and reserved for technicians. It is more the training of technicians in specialist criminal law that deserves to be improved and promoted, as well as that of judges. My impression is that everyone is making heavy weather of this area, which is detrimental to its attractiveness and thus its handling.

Progress has been made, as there is now the cybercrime centre at the Paris Court of Justice, which has just been strengthened by three specialist judges and will need to be expanded further. The police also make available to public prosecutors and judges specialist assistants, who provide them with help and facilitate liaison and work with specialist or non-specialist services.

As regards legislation and investigative techniques, the legal arsenal exists: it includes traditional techniques such as requisitions, searches, interviews, visits to premises, or an investigation using a pseudonym, which allows a police officer who is trained, qualified and authorised, at the suggestion of his director by the Attorney General, to go onto the darknet to find offences being committed through electronic communications and to collect evidence.
The only limitation, however, in my view concerns the retention of personal data by electronic service operators and access to digital

evidence, which have not been consolidated at the European level following the ECJ's Tele2sverige judgment prohibiting the retention of data in a general and indiscriminate manner. Only the preservation of data earmarked for future use is possible. This does not currently allow for a quality investigation, as the evidence may never have existed. You cannot work up the chain of a piece of data if you do not know whether it will be needed… you cannot expect miracles."

SECTION II
EVIDENCE AND ITS LIMITATIONS

■ **64.** In the field of digital evidence, law and technology combine to ensure procedural efficiency, determined by the search for a necessary balance between the preservation of privacy and the protection of public order.

Indeed, there are recurring difficulties in obtaining digital evidence:

- its dematerialised and extra-territorialised location;
- the lack of data retention or the use of Virtual Private Networks (VPN) or TOR, designed to keep network users anonymous. These means of anonymisation, as well as encryption tools, require investigators to carry out extra investigative work in order to find the perpetrator of a crime.

II-1.
PROCEDURES FOR ACCESS TO DIGITAL EVIDENCE

Investigators may usually obtain evidence through a requisition **(I)**, computer searches and seizures **(ii)**, or an investigation using a pseudonym **(iii)** or accessing stored correspondence **(iv)**.

(i) Requisitions that are typically used in the search for digital evidence

■ **65.** The public prosecutor, the investigating judge or, on with the approval of the latter two in a preliminary investigation or under a warrant (*commission rogatoire*), a judicial police officer and, under his supervision, a more junior colleague, may thus request from any business holding documents relating to the inquiry to pass data to him, or to keep content data, including data from a computer system or normative data processing (Articles 60-1 and 60-2, 77-1-1, 77-1-2, 99-3 and 99-4 of the Code of Criminal Procedure).

Requisitions make it possible to obtain subscription, connection and sometimes accessed content data, which are often

declarative, financial and technical information addressed to telecommunications operators or companies (name, address, telephone number, means of payment), and data that in particular enable an automated data processing system to be identified, such as a computer and its location.

(ii) Computer searches and data seizures

■ **66.** Judicial police officers carrying out a search may, in the context of the expedited investigation provided for by Article 57-1 of the Code of Criminal Procedure, access through a computer system located in the premises where the search is taking place, or from their own office, data that is of relevance to the investigation and is stored on that or another computer system, provided such data is accessible from the original system or available to the original system.

The search then allows access to the data stored on the computer or, provided it is not known beforehand that the data is located abroad, to the data that is online or on another computer, provided it is accessible from the computer being searched.

■ **67.** Law N°. 2014-1353 of 13 November 2014, on the fight against terrorism, extended the powers of investigators by adding the possibility of access, by means of a computer system at the premises of a service or unit of the police or gendarmerie, data relevant to the current investigation and stored on another computer system.

■ **68.** All these provisions also apply to all investigative frameworks.

■ **69.** The original data collected is handed over to the court, if necessary after being copied onto any medium that may be placed under seal after analysis by specialist investigators or an expert. Preserving the integrity of the original data, the seal guarantees the authenticity and unaltered nature of the data being analysed. In addition, a new copy of the original data will allow an alternative expert's report to be made in the event of a challenge to the validity of the evidence obtained.

(iii) Investigations using a pseudonym

■ **70.** Pursuant to Article 230-46 of the Code of Criminal Procedure, which was introduced by Law N°. 2019-222 of 23 March 2019 on programming for 2018-2022 and judicial reform, this procedure is now applicable to offences attacking automated data processing systems and is limited *"for the sole purpose of detecting crimes and offences punishable by imprisonment committed by means of electronic communications".*

Such investigations enable the following acts to be carried out:

- *"taking part in electronic exchanges using a pseudonym"*,
- being in contact, by electronic means, with the suspects of offences,
- by this means, extracting or retaining evidence and data about suspects,
- acquiring any content, product, substance, sample or service, including unlawful ones,
- transmitting a response with an express request for illicit content.

■ **71.** An investigation using a pseudonym must not, on pain of being held void, constitute an incitement to commit offences.

(iv) Access to stored correspondence

■ **72.** Until the Law N°. 2019-222 of 23 March 2019, access to stored correspondence was **limited to organised crime**. The legislature allowed the public prosecutor, with the prior approval of the liberty and custody judge (**juge des libertés et de la détention**), and the investigating judge to retrieve, remotely and without the knowledge of the person concerned, stored electronic correspondence accessible by means of a computer identifier[66].

■ **73.** The legislature **extended the scop**e of Articles 706-95-1 and 706-95-2 of the Code of Criminal Procedure to **cover all crimes**. Thus a liberty and custody judge (Article 706-95-1 of the Code of Criminal Procedure) or an investigating judge (Article 706-95-2 of the Code of Criminal Procedure), or a judicial police officer may authorise access, remotely and without the knowledge of the person concerned, to stored electronic correspondence for any type of crime.

II-2. RETENTION OF DATA BY OPERATORS

■ **74.** The requirement for data retention that is imposed in France for one year on telecommunications operators is a means of obtaining evidence. However, the rules for the retention of digital data vary according to the laws of different States, which makes international cooperation chaotic.

---

66. Circular of 2 December 2016 introducing the provisions of Law N°. 2016-731 of 3 June 2016 strengthening the fight against organised crime, terrorism and their financing, and improving the effectiveness and guarantees of the criminal procedure relating to strengthening the measures for combating organised crime NOR: JUSD1635582C.

■ **75.** Directive 2006/24 of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services provides for a minimum data retention period of 6 months.

Article 15 of the Directive provides that Member States may adopt measures limiting the rights and obligations laid down in the Directive *"where such limitation constitutes a necessary, appropriate and proportionate measure within a democratic society to […] ensure the prevention, research, detection and prosecution of criminal offences"*.

■ **76.** The room for manoeuvre left by European texts to the Member States has the effect that there are different approaches to data retention.

As regards the French legislation, the period of retention of technical data is set at one year[67].

■ **77.** Some States provide for a retention period of only a few weeks to protect their citizens' personal data, at the expense of proceedings and therefore of victims.

It should be specified that by a judgment dated 8 April 8 2014 in the "Digital Rights Ireland" case, the Court of Justice seems to have removed all normative scope from Article 15, since it found that legislation providing for *"widespread and indiscriminate retention of all data relating to traffic and localisation of all registered subscribers and users"* could only be justified by the fight against serious crime and therefore, for the future, since no one can know whether he will need such or such data, and for a serious offence not yet known…

■ **78.** This judgment thus reveals the legal insecurity that surrounds the length of data retention since its scope is interpreted differently by the legislation of the Member States.

■ **79.** In the United States there is no general requirement for minimal data retention to allow for possible use by the police or judicial services.

Despite the cooperation of the permanent contact group between the Ministry of the Interior, the judiciary and the various operators of these services, the processing of applications (for example relating to GAFAM - Google, Amazon, Facebook, Apple, Microsoft) sent by the French judicial authorities to the US judicial authorities sometimes takes several weeks, except in cases of vital

67. Article L. 34-1, III of the Postal and Electronic Communications Code.

emergency, and may not succeed, especially where a freedom of expression less restrictive than France's legal analysis is at stake.

II-3.
MEANS OF ACCESS TO ENCRYPTED DATA

The judicial authorities may require any person who is likely to be aware of the measures applied to protect the data to which access is permitted in the search. These provisions, introduced in 2014, also allow investigators to **request third parties who hold codes that lock access to computer content** to provide them with the information enabling them to access the data. This is in order to provide for the possible absence of a holder of computer content or his refusal to provide such codes.

On this point, it is interesting to recall that Article 434-15-2 of the Criminal Code punishes with 3 years' imprisonment and a fine of **€270,000** "the fact, for anyone who knows the secret convention for decrypting a means of cryptology that may have been used to prepare, facilitate or commit a crime or offence, to refuse to surrender it to the judicial authorities or to implement it", upon requisitions by those authorities issued pursuant to Parts II and III of Book I of the Code of Criminal Procedure.

In practice, it turns out that this offence is sometimes used in the event of a refusal by those arrested to give the access code of their mobile phone. As it stands, this interpretation of Article 434-15-2 of the Criminal Code appears to be incorrect and has led to the setting aside of several proceedings. In fact, the offence is aimed at means of cryptology such as certain applications (e.g. Signal or Telegram, Law N°. 2004-575, 21 June 2004, Article 29) that are not telephone access codes, which are a mechanism for authentication and not of cryptology. In this area, the law is confronted with technology that is particularly subject to change and therefore constitutes a source of legal insecurity.

■ **80.** **In addition, the use of judicial experts** is provided for in the Code of Criminal Procedure which enables the judicial authorities, for the purpose of "*putting encrypted data into plaintext*", to use **"external" expertise** to carry out technical operations that allow access to encrypted data, to their plaintext version or to the secret convention for decryption.

For example, they call upon a "encryption expert" to "decipher" information at their disposal.

PART III

10 RECOMMENDATIONS FOR ADVANCING THE FIGHT AGAINST CYBERCRIME

The following recommendations aim, following those concerning cyber insurance referred to in Book I, to improve the legal treatment of cyberattacks which must be the subject of a comprehensive and cross-cutting judicial response.

FOCUS

WHAT DEVELOPMENTS HAVE THERE BEEN IN CYBER RISK INSURANCE SINCE THE PUBLICATION OF BOOK I OF THIS REPORT IN JANUARY 2018?

CHRISTOPHE DELCAMP
Deputy Director of general and liability insurance, FFA

Recent developments relating to cyber risks amply demonstrate the relevance of dealing with cyber risk in a multidisciplinary manner. This method of working enabled Book I of the report from the Club des Juristes, dedicated to cyber insurance, to pose the key challenges of the insurability of these risks.

Three years later, where are we?

The context of cyber insurance has evolved in a positive way, but has not yet dispelled all the threats to its development.

On 12 November 2019, the ACPR (*Autorité de contrôle prudentiel et de résolution* - prudential and resolution supervisory authority) issued a press release drawing the attention of insurers to the inadequacy of the measurement of their exposure to this risk, notably through the implied warranties contained in contracts for RC (*responsabilité civile* - civil liability) and property damage. Recommendations 2 and 6 of Book I had anticipated this subject. Since then, major insurers have done in-depth work analysing their exposure to this risk. It will be up to each insurer whether or not to develop its offering on the basis of this work.

On 7 June 2019, the Council of the European Union adopted the European Regulation known as the "Cybersecurity Act". This Regulation aims at strengthening the European Union Agency for Cybersecurity (ENISA) and establishing a single European framework for cybersecurity certification.

On 18 February 2021, Cybermalveillance.gouv.fr announced the launch of the ExpertCyber label. This label enables micro businesses/SMEs/Authorities to identify quickly a recognised IT service provider for supporting victims in the fields of websites and professional information systems.

Recommendations 4 and 7 called for this technical framework, aimed at both large businesses and smaller structures at the European and national level, to enable real preventive and remedial tools to be provided to all economic stakeholders.

On 18 February 2021, President Emmanuel Macron set out a €1 billion plan to strengthen the country's cybersecurity between now and 2025, including €720 million of public funding.

Recommendation 10 emphasised the need to guide public investment plans to foster the development of sectors of excellence in the field of cybertechnology, the only way to anticipate future challenges and not be overtaken by other countries.

On 16 July 2019, Michel Van Den Berghe, Director General of Orange Cyberdefense, received his letter of engagement from Prime Minister Édouard Philippe to set up a cyber campus in France. In his January 2020 report, Michel Van den Berghe identified data sharing as one of the challenges which this campus had to face.

Recommendation 5 highlighted this need for data sharing for insurers.

While these measures contribute to a positive development in the insurability of these risks, there are still many threats to the proper transfer of these risks to insurers.

The combination of the Covid-19 crisis, the proliferation of large-scale attacks, and severe losses affecting data storage sites (Solarwinds in December 2020, Microsoft Exchange and OVHCloud in March 2021), have raised fears that "a pandemic" could affect information systems.

The lack of clarity on the insurability of ransoms and administrative fines, already identified in Book I, does not permit the necessary transparency for insurance buyers.

The lack of a culture of cyber risk among micro businesses/SME/local authorities, as well as insurance professionals, does not provide a salutary awareness for developing prevention against these risks and their transfer to insurers.

The year 2021 will be marked by the race between the short time needed for annual renewals of insurance and reinsurance contracts and the long time needed for the establishment of foundations for the proper treatment of these new risks.

RECOMMENDATIONS INTENDED FOR THE GOVERNMENT

RECOMMENDATION 1:

Make the fight against cybercrime a national cause for 2022

- Launch recurrent targeted information and awareness campaigns through traditional and social media, including with the support of chambers of commerce, companies and professional bodies.
- Enter into an agreement to this effect between the Ministry of Justice and the Cybermalveillance.gouv.fr platform.

RECOMMENDATIONS INTENDED FOR THE MINISTRY OF JUSTICE

RECOMMENDATION 2:

Encourage the specialisation of judges and public prosecutors and their continuing education

- Create a branch of cyberjudges, if necessary through graduate education (a university Cyber degree, for example).
- Strengthen the Cyber centre at the Paris Public Prosecutor's Office.
- Strengthen the specialisation of a chamber of the Court of Justice in the field of digital law and cybercrime.
- Create a Digital and Cyber department at the Paris Court of Appeal, made up of judges and public prosecutors.
- Enhance the joint ENM/EFB and PN/GN/Customs training on digital law and the fight against cybercrime, with practical training courses in the specialist services.
- Designate one cyber point of contact per court of appeal, regularly updating the list.

RECOMMENDATION 3:

Strengthen public/private cooperation and guide public and private investment toward the emergence of a French and European sector of excellence in cyber technology

- French and European public investment plans should promote the development of a European sector of excellence in the field of cyber protection and support market efforts to reduce the cyber threat.

  This recommendation, already formulated in Book I, is also valid for the legal handling of the cyber threat since it aims to reduce it.

  It also aims, in order to avoid their expatriation, to help researchers become entrepreneurs in line with the cyber campus and the investments of the *William Levat Cyber Challenge*".

RECOMMENDATION 4:

Strengthen judicial services in the fight against cybercrime

- Recruit specialist cybersecurity managers and assistants, both at the level of the Court of Justice and the Court of Appeal in Paris.
- Develop regular exchanges with the companies of judicial experts.
- Review the nomenclature of judicial experts in order to introduce a specialisation in digital and cybersecurity.
- Sign Justice/Bar/Interior agreements on these issues of cyber security and cybercrime, and plan for information sharing between those in charge.

RECOMMENDATION 5:

Simplify investigation procedures using a pseudonym on the "darknet"

- Provide realistic resources for the investigators who have to conduct them.

RECOMMENDATIONS INTENDED FOR EUROPEAN BODIES

RECOMMENDATION 6:

Adoption of a European data retention regime to meet the operational needs of law enforcement and judicial services.

- This regime should provide for the enabling of investigations by taking into account data retained for up to one year.

RECOMMENDATIONS INTENDED FOR ANSSI

RECOMMENDATION 7:

Encourage safe haven States to end the impunity of cybercriminal groups

- The aim is to end the comfortable installation of major cybercriminal groups in safe haven countries by developing solidarity between States to force the safe haven States to take legal and economic measures for this purpose

RECOMMENDATION 8:

Signature of protocols with all independent agencies and administrative authorities involved

- This recommendation applies to all independent agencies and administrative authorities, in order to encourage them to systematise reporting procedures.

  This recommendation is linked to Recommendation 5 of Book I: pooling data collected from cyber incidents and to the creation of the cyber campus.

RECOMMENDATIONS INTENDED FOR BUSINESSES

RECOMMENDATION 9:

Invest in cyber-attack prevention

- Such investments take place in the context of the global risk management scheme.

  They must be human (for example, cyber security training), technical (software investment, backup tools, audits, etc.), organisational (implementation of e-governance), and insurance-related.

RECOMMENDATION 10:

In the event of a cyberattack, file a complaint immediately

- The complaint enables all the services mentioned in the booklet to be brought in and to be able to identify sources, particularly in order to dismantle networks.

These 10 concrete proposals, intended to strengthen the protection of businesses and citizens, are all additional instruments in the service of freedoms. They also represent the conditions for France to possess essential advantages of competitiveness and sovereignty for our country in the context of technological developments that are embarked in the 21st century upon a path towards digital and artificial intelligence. It is rare that challenges of such importance do not require investments that are out of reach. These proposals are within our financial reach. All they need is to be able to rely on real political will."

Bernard Spitz

COMPOSITION OF THE COMMISSION

■ CHAIRMAN:

Bernard Spitz, President of the International and Europe Division of MEDEF, former President of the French Insurance Federation (FFA)

■ GENERAL SECRETARY:

Valérie Lafarge-Sarkozy, Lawyer, Partner with the law firm Altana

■ MEMBERS:

Nicolas Arpagian, VP Strategy & Public Affairs, Orange Cyberdefense

Brigitte Bouquot, former Chairperson of the Association for Corporate Risk and Insurance Management (AMRAE), VP Scientific

Philippe Cotelle, Head of Insurance Risk Management Cyberdefense, Airbus Defence and Space, Director of AMRAE, Chairman of the Information Systems Commission

Christophe Delcamp, Deputy Director of general and liability insurance, FFA

Émilie Dumérain, Legal Deputy, Syntec Numérique

Agathe Lepage, Professor at Université Pantheon-Assas (Paris II)

Charles-Henry Madinier, Director of Consulting Solutions, Marsh Advisory

Alexandre Menais, Executive Vice President and Group Head of M&A, Strategy & Development, Atos

Séverine Oger, Mission Head / Staff of the Operations Sub-Directorate, National Agency for the Security of Information Systems (ANSSI)

Martin Pailhes, Head of the Legal Team "Information Technology – Intellectual Property", BNP Paribas

Christian Poyau, Chairman of Micropole, President of the MEDEF Digital Transformation Commission

Myriam Quéméner, Prosecutor (*avocat général*) at the Paris Court of Appeal

Anne Souvira, Chief Superintendent (*commissaire divisionnaire*), Officer Responsible for Cybercrime Issues at the office of the Paris Metropolitan Police Commissioner (*préfet de police de Paris*)

François Weil, Member of the Council of State (*Conseil d'État*)

Leigh Wolfrom, Policy analyst, Directorate for Financial and Enterprise Affairs at OECD

■ EDITORIAL CONTRIBUTORS:

Valérie Lafarge-Sarkozy, Lawyer, Partner with the law firm Altana

Myriam Quéméner, Prosecutor (*avocat général*) at the Paris Court of Appeal

Anne Souvira, Chief Superintendent (*commissaire divisionnaire*), Officer Responsible for Cybercrime Issues at the office of the Paris Metropolitan Police Commissioner (*préfet de police de Paris*)

Laetitia Daage, Lawyer, Counsel with the law firm Altana

■ WITH INTERVIEWS AND PARTICIPATION FROM:

Nicolas Arpagian, VP Strategy & Public Affairs, Orange Cyberdefense

Bernard Barbier, former Technical Director of the DGSE – Member of the Academy of Technologies,

Mariette Bormann, Director of the Legal, Compliance, Tax and Distribution Division of the FFA (French Insurance Federation)

Brigitte Bouquot, former Chairperson of the Association for Corporate Risk and Insurance Management (AMRAE), VP Scientific

Philippe Cotelle, Head of Insurance Risk Management Cyberdefense, Airbus Defence and Space, Director of AMRAE, Chairman of the Information Systems Commission

Christophe Delcamp, Deputy Director of general and liability insurance, FFA

Jean-Louis Gergorin, former Head of the Centre for Analysis and Forecasting at the Quai d'Orsay,

Paul-Alexandre Gillot, Head of the Investigations Department at C3N

Admiral Édouard Guillaud, former Chief of Staff of the Armed Forces – Member of the Naval Academy

Rémy Heitz, Public Prosecutor at the Paris Court of Justice

Agathe Lepage, Professor at Université Panthéon-Assas (Paris II)

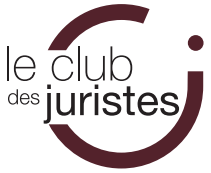
Fabienne Lopez, Colonel, Commander of C3N

Haritini Matsopoulou, Professor at Université Paris-Sud

Séverine Oger, Mission Head / Staff of the Operations Sub-Directorate, National Agency for the Security of Information Systems (ANSSI)

Guillaume Poupard, Director General of National Agency for the Security of Information Systems (ANSSI)

Élisabeth Rolin, Legal Adviser at the National Gendarmerie


le club
des juristes

4, rue de la Planche 75007 Paris
Phone: 01 53 63 40 04

www.leclubdesjuristes.com

FIND US ON