CYBERSECURITY

SAFEGUARDING OUR STRATEGIC AUTONOMY

Arnaud MARTIN, Didier GRAS

THINK-TANK
DIGITAL
NEW DEAL

September 2022

NEW DEAL DIGITAL COLLECTION "TRUSTED DIGITAL"

“CYBER RISK HAS BECOME ONE OF THE THREE SYSTEMIC RISKS COMMONLY ADMITTED BY ALL INSURANCE COMPANIES (WITH PANDEMIC RISK AND GLOBAL WARMING RISK)

PLAN

PREFACE

Two major recent upheavals have brought the issue of cybersecurity to the forefront. First of all, the Covid crisis, the increasing digitalisation of uses and the exponential interconnection of systems has subsequently raised the question of their protection, each new use offersing a new opportunity for attack. Then, Ukraine of course, the media coverage of the new "hybrid wars" has made the general public aware that the threats of the virtual world have real impacts on our lives.

In such a context where cybersecurity risks are becoming more and more persistent and sophisticated, the State therefore, must educate to ensure that our companies, local authorities, and fellow citizens are well aware of the challenges and are armed to deal with increasingly regular and serious threats.

The European Union must equip itself with an ambitious strategy, making cybersecurity the fourth pillar of its strategic autonomy. It must not hesitate to question the current political and legal framework in order to do so. Europe must indeed aim for total autonomy in its ability to assess and manage cyber risk.

It is this path, beginning from awareness all the way to collective trust, that authors Arnaud Martin and Didier Gras invite us to take. Along the way, they will come up with concrete proposals that will feed this ambition, thus completing our “Numérique de confiance (Trusted digital)" collection[2], which is composed of four complementary notes. According to our think-tank, cybersecurity is the underlying element of the "Cloud, Data, AI" triptych that constitutes the trust ecosystem. For there can be no trust without security to dispel fears, and without sovereignty to ensure that we are masters of our own destiny.

> *“STRATEGIC AUTONOMY IS AN ABILITY TO GENERATE AND DEFEND AN ECOSYSTEM OF TRUST THAT ORGANISES OUR TECHNOLOGICAL INTERDEPENDENCIES”*

Arno Pons,
Digital New Deal

[1] Digital New Deal publishes a collection of four notes on the definition of "numérique de confiance (trusted digital)" as the foundation of our strategic autonomy: *Cloud de confiance* (Trusted Cloud) by Laurence Houdeville and Arno Pons in 2021, then in 2022 *Cybersécurité, vigile de notre autonomie stratégique* (Cybersecurity, the guardian of our strategic autonomy) by Arnaud Martin, *Data de confiance* (Trusted Data) by Olivier Dion and Arno Pons, and *IA de confiance* (Trusted AI) by Julien Chiaroni and Arno Pons.

INTRODUCTION

The cyber threat, is *"a potentially malicious use of digital space. It takes shape when an attacking malicious entity performs a sequence of actions via digital or physical channels to exploit the properties of the cyber space (including its technical or structural vulnerabilities) in order to achieve impacts, themselves of a digital or physical nature (particularly financial)."*[3]

This globalised threat is now part of the daily news. Recently, the physical invasion of Ukraine by Russia, combined with a widely publicised cyber conflict (i.e., attack on the ViaSat satellite, creation of the IT Army of Ukraine, sabotage actions of Ukrainian critical infrastructure, etc.), or in Costa Rica, where President Rodrigo Chavez declared a state of emergency on 10 May 2022 to combat cyberattacks attributed to the Conti group (many government agencies were ransomed by hackers, hoping to obtain the payment of several million dollars in ransom, paid by the Government).

In France, it has been gradually taken seriously: initially focused on Government intelligence, it was extended in 2009 to the defence of ministries and large administrations through the creation of the Agence Nationale de Sécurité des Systèmes d'Information (National Agency for Information Systems Security) (ANSSI); the military programming laws of 2013 and 2018 then increased the obligations of vital importans stakeholders (OIV) and essential service operators (OSE) in terms of asset protection and activity resilience, detection and reaction to attacks, as well as governance of the cyber risk.

At the same time and with the digitalisation of the world in which we live, cybercrime and manipulation of information have strongly developed, taking many forms. Starting with ransomware software that allows data to be encrypted; the theft or sale of private images subject to sextortion; or the theft of bank details by means of falsified public websites. Thus, many local authorities and University Hospitals (UH) have been deprived of their data during the Covid19 pandemic; thousands of employees have had their training credits (CPF) stolen after having communicated their passwords to counterfeit sites. The second form, a real lever of influence on populations, has developed using the technologies of synthetic imagery by the diffusion on social networks of false information and very realistic retouched videos (deepfake).

Awareness is now real in large administrations and companies, and technical and organisational measures are gradually being put in place. However, at the other end of the chain, citizens as well as small and medium-sized enterprises are too often helpless against the cyber threat.

If more effective prevention measures are not implemented in a sustainable way, the cyber threat could pose a societal risk to the further development of digital technology.

To this end, we propose an inventory of **cybersecurity in France, with eight findings and recommendations**, which aim to make it a **societal issue** and a **standardisation** issue. The first details the desirable changes in the legislative framework in order to give us the political means to preserve our strategic autonomy and thus guarantee the development of digital activities (recommendations 1 to 4). The second part identifies the actions recommended to ensure effective prevention by the population (recommendations 5 to 8).

[2] *Cybersécurité, Cyberdéfense: enjeux stratégiques* (Cybersecurity, Cyberdefence: strategic issues) Yann Salomon, Ellipses, 2021

“A COLLECTIVE AWARENESS OF THE CYBER RISK IS NECESSARY TO BUILD A TRUSTWORTHY DIGITAL WORLD.

I. ADOPTING AN AMBITIOUS AND DETERMINED STANDARDISED STRATEGY

Four recommendations for updating the European framework

1. DEROGATE FROM THE PRINCIPLE OF UNIVERSALITY OF THE CYBER DEFENCE BUDGET

FINDING 1: GROWTH IN TAX REVENUES (TAXES AND FINES) RELATED TO DIGITAL ACTIVITIES

Regulation of the digital sphere and the fight against cybercrime are above all means of securing and supervising the digital world. Taxes, fines or confiscations have collected significant income in recent years and this could be reinvested in the clean-up of the dual digital world in which every French citizen either is already a user or will more and more become a user in the future.

Let's take the example of the CNIL: created by the law on data processing and freedom of 6 January 1978, the Commission Nationale de l'Informatique et des Libertés (National Commission for Information and Freedom) is the independent administrative authority in charge of ensuring the protection of personal data both private and public, whether contained in computer files and processing or on paper. Since the implementation of the European General Data Protection Regulation (GDPR) on 25 May 2018, the CNIL has seen an exponential growth in activity. In 2020, it employed 225 agents with a budget of 20.1 million euro. It has issued 49 formal notices, 38 calls to order, and 14 penalties amounting to 138 million euro in fines (by 2021, the total amount should be even higher).

The AGRASC (Agency for the Management and Recovery of Seized and Confiscated Assets) is a public administrative institution under the joint supervision of the Minister of Justice and the Minister of Public Accounts. The agency, which is responsible for the execution of the confiscation order on behalf of the public prosecutor, also aims to meet the indispensable need for the management of the seized assets, when these require administrative acts (vehicles, buildings, business assets, boats, etc.) As a strong growth in seizures has been observed on all crypto assets, the key lever for the development of international cybercrime, the recording of these assets should eventually be entrusted to the French Government Caisse des Dépôts, which would then be able to reinvest it 100% in the sovereign digital economy via its investment bank.

The last example is the tax on digital services. In the absence of a European agreement, France adopted its own GAFAM tax on digital services on 11 July 2019. The companies concerned are those whose annual turnover for these services exceeds 750 million euro worldwide and 25 million euro in France. The amount of the tax is calculated by applying a rate of 3% on this turnover earned in France. On 1 July 2021, a more global agreement was signed at the Organization for Economic Cooperation and Development (OECD) for the implementation of a harmonised global corporate tax, with a minimum rate of at least 15%.

This tax has already brought in 277 million euro in 2019, 375 million euro in 2020 and was expected to bring in 358 million euro in 2021 according to forecasts. It could bring in 519 million euro in 2022 for France.

RECOMMENDATION 1
DIRECTING THE BUDGETARY EQUIVALENT OF THESE TAX REVENUES TOWARDS SECURING THE DIGITAL WORLD

As cybersecurity has since 2019-2020, been identified as one of the three systemic risks (along with the pandemic risk and the risk of global warming), we recommend ensuring that the equivalent in terms of budget of all taxes, fines, confiscations related to the digital domain, be directly reinvested in securing this sector in France in the first instance, and, if possible, at the European Union level to loudly and clearly present a common goal of fighting cybercrime on our continent.

The covid 19 pandemic led to the implementation of exceptional measures in France as part of the initial "whatever it takes" policy decided by the President of the Republic.

A few days before the COP26, the Minister of Economy proposed directing the tax revenues linked to fossil fuels to the fight against global warming. A proposal that deviates from the principle of universality of the budget. Nearly 35 billion would thus be allocated to climate issues per year.

This principle could be applied to investments in cyber defence: every euro collected by the CNIL, AGRASC, GAFAM taxes, etc. would be reinvested to make access to the digital world more secure. The Cour des Comptes (French National Audit Office) could commission a mission to define the priorities for the allocation of these budgets and to monitor this measure over the long term. As a first step, the budgets of certain particularly undersized entities and/or entities that can leverage cash inflows (fines, confiscations) could be substantially increased. Concrete emergency actions would thus be financed, in particular from the resources allocated to the justice system for the fight against cybercrime. For example, the J3 section of the Paris public prosecutor's office is specialised in the fight against cybercrime. It is a key element of the French judicial system to attack the feeling of impunity that cyber attackers have long enjoyed. The J3 is currently composed of three (3) magistrates, two (2) court clerks, one (1) specialised assistant (a second one is being recruited at the end of 2021), one (1) legal assistant and one (1) police liaison officer. During 2021, J3 referral capacity increased by 540%. For example, under concurrent jurisdiction, there have been over 638 cases transferred to J3 from other jurisdictions. The assignment of additional magistrates and clerks, as well as the equipping of the J3 (with the aim of automation), would allow for a much more efficient processing of the cases that are currently late or deprioritised.

In parallel with these explicit short-term efforts, current investments under the various PIA4, France Relance 2025 and France 2030 investment plans must of course be maintained. The goal of the National Acceleration Strategy for Cybersecurity presented on 18 February 2021 and reaffirmed in February 2022, has a budget of 1,039 million euro (including 720 million euro of public money). Even if the amounts invested are significant (250 million euro per year on average over 5 years, including 180 million euro of public money), the principle of systematic earmarking would result in an overall financial leeway estimated at about 700 million euro of public money per year.

If the national cloud strategy were to be financed on the same basis, the amounts announced for the second half of 2021 (1,791 million euro, including 667 million euro of public money, 680 million euro of private funds and 440 million euro of European subsidies) would represent an investment capacity difference for cyber of at least 150 million euros per year.

Thus, it would be some €700 M (estimated budget) - €250 M (cyber plan) - €150 M€ (cloud plan) = €300 M per year left to directly finance other digital sovereignty and cybersecurity projects in France.

Obviously, the increase in tax revenue will have to be accompanied at the same time by a rationalisation of expenses through the pooling of resources. There are currently too many isolated cybersecurity initiatives, most of which are very often relevant and legitimate, but sometimes difficult to scale up and that address issues that are too targeted. This dispersal of resources, mentioned in a report by the Cour des Comptes (French National Audit Office) written in March but not published, first of all addressed *“the scattering of the jurisdictions of the public authorities in the fight against cybercrime.*[3]*"*

[3] *Letter A*, article dated 17 May 2022

“THE LEVEL OF VULNERABILITY OF ALL SOFTWARE IN THE WORLD HAS REACHED AN EXTREMELY WORRYING STAGE

2. REINFORCING EUROPEAN STANDARDS ON THE PRINCIPLES OF "SECURITY BY DESIGN"

FINDING 2: EXPONENTIAL GROWTH IN THE NUMBER OF VULNERABILITIES

The widespread introduction of digital technology has mechanically increased the number of connected solutions that we use on a daily basis, most of which are fallible in terms of security, in other words, vulnerable.

A vulnerability or flaw is a weakness in a computer system that allows an attacker to undermine the integrity of the system, i.e., its normal operation, the confidentiality or integrity of the data it contains. **These vulnerabilities are the result of weaknesses in the design**, implementation or use of a hardware or software component of the system, but they are often software anomalies related to programming errors or bad practices. These software malfunctions are usually fixed as they are discovered, but the user is still exposed to possible exploitation until the patch (temporary or permanent) is released and installed. The procedure for exploiting a software vulnerability is called an exploit.

The level of vulnerabilities in all software worldwide has reached an extremely worrying situation. The assessment of this situation is based on several reference criteria.

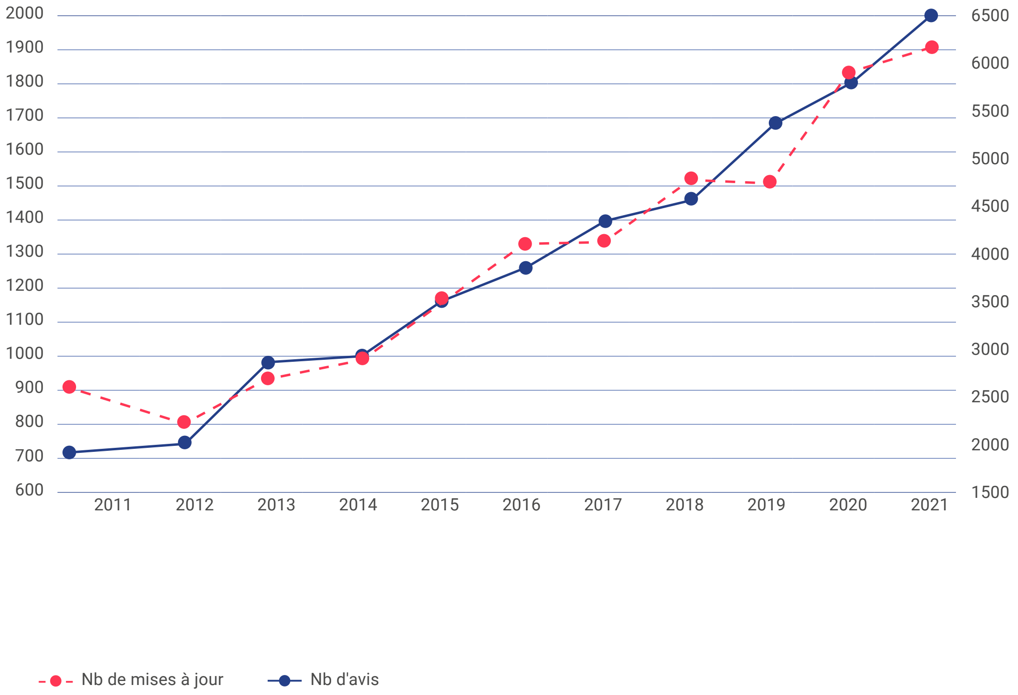

Figure 1
Cert-IST association 2021 report

(1) The number of Security Advisories issued. *They describe the new vulnerabilities discovered in the products monitored by the Cert-IST. 1,987 security advisories were published by Cert-IST in 2021. The number of advisories has been steadily increasing for several years (see the curve above), with an increase of 9% in 2021 compared to 2020. This continuous increase shows that the discovery of vulnerabilities is a constantly growing phenomenon.*

*(2) **The number of modified advisoriess.** These advisories are continuously enriched with minor or major updates. This is the case when, For example, attack programmes – known as "exploits" - are published. 5,982 minor updates and 173 major updates have been published in 2021 by Cert-IST.*

*(3) **The number of so-called 0Day vulnerabilities.** A 0Day or zero day vulnerability is a computer vulnerability that has not been published or has no known patch. The existence of such a flaw in a computer product implies that no protection exists, whether as a stop-gap or definitive. The terminology "zero day" does not qualify the severity of the flaw: like any vulnerability, its severity depends on the amount of damage that can be caused, and on the existence of an exploit i.e., a technique that "exploits" this flaw in order to carry out undesirable actions on the product concerned.*

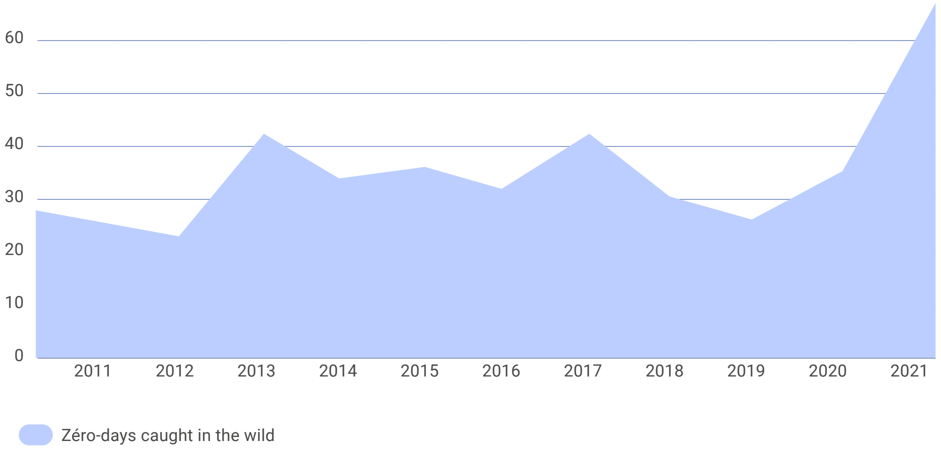

Figure 4
MIT study - 0Day vulnerabilities over the year 2021

*(4) **All publishers involved.** In short, all publishers are concerned. It is interesting to note that publishers with the largest market capitalisations have some of the highest number of discovered vulnerabilities in the world. This leads us to consider that the software industry is unable to provide trustworthy services.*

To date, administrations and companies are faced with an exponential number of vulnerabilities to deal with (patches or stopgap measures) and must mobilise resources at their own expense and regularly (and sometimes urgently) apply the patches developed by the publishers.

RECOMMENDATION 2.A.
IMPOSE A CYBER EU STANDARD LISTING THE FUNDAMENTAL PRINCIPLES TO BE ADHERED TO BY THE INDUSTRY.

Before any connected solution can enter the EU market, we recommend that it must meet a number of commitments in terms of a "vulnerability discloser policy". Sanctions, in case of serious malfunctioning, could be applied (or recalls at the expense of publishers and manufacturers for remediation, as is imposed on car manufacturers).

In addition, we recommend imposing on digital professionals, an obligation of transparency or information allowing each user to have the necessary reference points to understand the security issues associated with the products or solutions offered and to promote responsible use.

RECOMMENDATION 2.B. MAKE A FLASH CYBERSECURITY DIAGNOSIS MANDATORY

Companies should be obliged to have an annual flash audit (e.g., lasting one day) on a few inspection points of the essential safety measures just like the motor vehicle inspection or the verification of a fire protection system. No one doubts that a system of fire detection devices is necessary to protect people and property. The same perception does not yet exist about immaterial things. A cyberattack can have major operational, financial and/or reputational impacts, and can go from paralysing a company severely to even permanently. How many companies know about firewall, detection or isolation mechanisms in the digital domain?

3. EXTEND THE LEGAL SCOPE OF ATTACK DETECTION TO CERTAIN SUPERCRITICAL OPERATORS

FINDING 3: EXISTENCE OF CERTAIN PRIVATE STAKEHOLDERS WITH A PRIVILEGED ROLE IN THE FIGHT AGAINST CYBERCRIME

In the 12 February 2018 Strategic Cyber Defence Review, an in-depth analysis was made on protecting Operators of Vital Importance (OIVs) and Critical Activity Protection (CAP). Amongst the OIVs, because of their role as service providers to other OIVs, the electronic communications and electric power supply sectors can be qualified as supercritical (a cyber attack on one of these stakeholders having a domino effect on all OIVs). In fact, these stakeholders (notably the historical stakeholders Orange and EDF) very early on, developed advanced cyber detection capabilities and the level of maturity of their CERTs is recognised by all private and public stakeholders.

In Article 34 (L.33-14) of the Military Programming Law 2018-607 of 13 July 2018, telecommunications operators have also seen their role increased: the ANSSI is now able to share technical markers (indicators of compromise) with them so that they can monitor the possible presence of these markers on their networks. ANSSI is able to have detailed information on these streams only in the case where the presence of these markers is detected on OIV or OSE. This process is very strictly regulated by ARCEP (French Electronic Communications, Postal and Print media distribution Regulatory Authority).

On a more ad hoc basis and on the basis of classified investigations *(which we will therefore not be able to detail in this report*), in-depth research operations have been carried out by certain telecom operators. The network equipment of victims had been infected by an attack by state actors and the analysis of network streams on all the network equipment in France, allowed us to precisely confine the scope of the victims. Concretely and in a very specific way, some operators have been able to "illuminate" all the Internet streams in a sequential manner, which corresponds to a very precise search for a few frames at speeds of around ten terabits per second.

Unlike the centralised interconnection of the Chinese network to the global Internet, the architectures of the European networks and particularly the French networks are decentralised. There are a few dozen Global Internet eXchanges (GIX) in France and about a hundred GIXs in Western Europe. Even if these interconnections are not unique and therefore make the principle of the Great Digital Wall of China impossible to apply in Europe, their number remains nevertheless finite.

RECOMMENDATION 3
CONSIDER GIVING TELECOM OPERATORS A GREATER ROLE IN DETECTING CYBER ATTACKS

Internet neutrality is a fundamental principle of our Western democracies. Without revising this neutrality, we propose to substantially increase the capacity to detect cyber activities on telecom operators' networks by inspecting duplicated (mirrored) streams at choke points so as to never offer a private stakeholder or any State, the capacity to filter certain Internet information streams (and thus avoid any temptation for private or State censorship).

We suggest first of all to widen the legal scope of detection at the French or European level. Even if the markers currently provided are detected on companies (excluding OIV or OSE), the ANSSI is not entitled to obtain the details of this information. A parliamentary mission (assisted by engineers from technical bodies, lawyers and experts from the CNIL) could be set up to review the legal scope of applicability of the search for technical markers to all companies and citizens on the French territory. A specific government stakeholder member of the C4 committee (ANSSI for example) could be in charge of selecting the shared markers and be the guarantor of the use and direct notification of companies or citizens of alerts concerning them.

But even if these legal constraints can be relaxed, dedicated and standardised, technical infrastructures will have to be built and financed. Current probes (neither those approved by the ANSSI within the framework of the LPM, nor any other commercial probe) are incapable of absorbing streams of several hundred gigabits per second (or even a few terabits per second). Most of them also offer a cut-off mode of operation (which, as a matter of architectural principle, should be prohibited). This dedicated applied research project could become one of the flagship projects of the newly inaugurated Cyber Campus. These probes would have several modes of operation:

- *sampling* mode, with alerts on markers by sampling (one frame every 10,000 frames for example); this general mode could provide a global cyber weather forecast in France;
- *deep inspection* mode, with more targeted detailed searches (over shorter periods of time, on much more precise types of Internet traffic) compared to information consolidated by the ANSSI (after agreement from the intelligence services within the framework of the C4 committee);
- graduated inspection modes between the broad-spectrum vision and the very precise field vision described above, allowing zooming in on certain attack typologies (depending on the current events or the research target (APT group X or Y)

From a more technical point of view, the shared markers are mostly IP addresses of identified Command and Control (C&C) servers belonging to attackers. Any source or destination IP traffic with these C&Cs would identify a public IP address of a potential victim (past, current or future). Resolving this public IP address into a person's name (physical person or entity) and/or an email address, would allow the potential target to be alerted in an appropriate way. For citizen alerts, we can even imagine a system that allows the *AllCyberPlayers* application to be used to convey alerts to potentially any equipment on the home LAN. Indeed, the application connected to a domestic WiFi would have the same public IP application as that detected in the malicious traffic and an alert such as "Contact at risk", like in the *AllAgainstCovid* app, could be generated with a link to easy-to-understand explanations of the risk incurred and the various actions to be taken.

If we take a step back from this recommendation, the notification of potential alerts will be a key point of the system: it will have to be industrialised but personalised by type of potential victim, automated and non-anxiety causing, all this within a framework that preserves individual liberties protected by the CNIL.

4. DEVELOP A CYBER RISK RATING AGENCY BASED ON A EUROPEAN STANDARDISED MODEL FOR ALL PUBLIC PURCHASES.

Since the middle of the 20th century, financial rating has been widely extended to non-financial rating. Nowadays, it is a must-have, as it meets the growing obligation for companies to report on the inclusion of ESG objectives in their investment strategy. Cyber risk appears in the form of a specific rating. The rating responds to the need for comparative management indicators, since, although digital risk is now considered by all to be a major factor, it is dealt with very unevenly in companies. Investors, insurers and decision-makers are the primary consumers. Since 2011, an average of one dedicated rating agency per year has been created worldwide. At a time when the search for new "geo/eco-political" equilibrium is leading governments to demand a certain strategic autonomy, most of the cyber rating agencies are North American and there are no major players in Europe. The French presidency of the EU is focusing on European "sovereignty" and the implementation of a development model that supports the growth of European digital stakeholders defining their own rules (data, artificial intelligence, cyber, processors). In this context, we believe that it must consider the development of an autonomous, external and automated cyber risk assessment capability for European companies.

“THE LEVEL IT IS CRUCIAL TO CHANGE OUR PERCEPTION : THE PASSIVE MAJORITY MUST REPORT THE ATTEMPTS THEY ARE BEING TARGETED WITH.

FINDING 4.A: LACK OF AUTONOMOUS CAPACITY TO ASSESS CYBER RISK

There is an oligopoly of US rating agencies (95% of the rating market) that publish more and more ESG indicators and create de facto standards. These agencies impose a dependency or submission to a unilateral cyber rating. These assessments expose European companies to the risks of the delocalisation of laws, distortion of competition or conflict of interest.

As an illustration, BitSight, the American company leader in the market, is gaining a foothold in Europe. The company, which already has 2,400 customers in 30 countries, has just acquired Moody's in its capital holding. It already has a substantial portfolio of that carries out measurements on European companies, a development centre in Portugal and sales offices in France. Its sales teams deploy aggressive conquest strategies based on unsolicited sectoral evaluation and comparison.

To date, there is no large-scale European alternative, no guarantee of the independence and reliability of the measurements made, and no consensus on the value of the widely published ratings.

RECOMMENDATION 4.A. CREATION OF A EUROPEAN ACCREDITATION SYSTEM FOR CYBER RATING.

Given the strategic nature of cybersecurity, we recommend the implementation of a European cyber rating accreditation system for non-financial rating stakeholders.

The objective of this accreditation would be to guarantee the reliability of the measurements, the independence of the published ratings, and the fair treatment of European companies when it comes to investment or insurance choices related to the external assessment of cyber risk. The requirements for obtaining this accreditation should include the governance and financing of the measurement operator and the conformity of its practices to shared European standards.

FINDING 4.B: UNEVEN AND OPAQUE CYBER RISK ASSESSMENT METHODS

Each rating agency has its own method of measurement and evaluation and these are rarely published. Moreover, non-financial rating agencies are subject to the same remarks as their predecessors: lack of transparency and professional inadequacy.

In the case of cyber rating, the testimonies collected mainly concern the uncertainty relative to the relevance of the scope evaluated, the opacity of the measurement methods and the rating rules, the interpretation of the rating and the level of associated risk at the level of executive managements.

In France, there is no consensus on the cyber rating methods used by the rating agencies within the professional bodies of the cybersecurity professions. The lack of reference limits the use of the scores currently attributed by the agencies to the sole act of communication.

RECOMMENDATION 4.B. DEFINITION OF A STANDARDISED EUROPEAN MODEL FOR CYBER RATING

We recommend dialogue on the development, validation and publication, within the European authorities, of a standardised measurement method that can offer instant visibility on the exposure to an explicit cyber risk portfolio.

The published standard must provide objective and aggregated information in terms of performance management, maturity measurement (according to European laws, regulations, norms and standards: NISv2, GDPR, DORA) and cyber risks for stakeholders (shareholders, investment funds, M&A firms, banks, insurers, principals).

It would be based on the technological ability of European stakeholders to address, analyse, visualise and share multiple digital footprints to compare them to increasingly "intelligent" multifaceted threats, using current data management and AI techniques.

FINDING 4.C: DISCREPANCIES IN THE INTERPRETATION OF THE CYBER RATING

Beyond the rating, there are significant differences in the interpretation of the ratings given between the different stakeholders (decision-makers, cyber specialists, insurers or investors). These discrepancies are due to the lack of a reference framework for measurement and to the divergences linked to the individual perceptions of stakeholders with different backgrounds and expertise.

RECOMMENDATION 4.C. IMPLEMENTATION OF A EUROPEAN CERTIFICATION FOR CYBER ANALYSTS

We recommend the establishment and training of cyber analysts, with a view to producing accompanying reports on cyber rating with regard to the reality of the measures and the impacts in the European context (political, economic, societal, ecological and regulatory).

The cyber sector is essentially technical, and given the stakes involved, it seems essential to train a new group of analysts who know how to assess these impacts, which have become major factors for Europe.

Beyond the standardised aspect of this European cyber rating approach, this recommendation would directly serve to confirm that all public investments in the digital domain are subject to a European sovereignty clause, guaranteeing a "native and explicit level of cyber security" of the investments proposed under Recommendation 5.

EU MUST DEVELOP AN AUTONOMOUS AND AUTOMATED CYBER RISK ASSESSMENT CAPABILITY FOR EUROPEAN COMPANIES.

II. MAKING CYBERSECURITY A SOCIETAL ISSUE

Four recommendations to ensure that the public is well protected

5. RAISING AWARENESS AMONGST THE GREATEST NUMBER OF PEOPLE

FINDING 5: LOW AWARENESS OF CYBER RISKS AND DISMAY OF VICTIMS

We have all been targeted or victimised by a fraud attempt in the last two or three years (either ourselves or those close to us). The three most common scams are[4] :

- computer breakdown fraud, which consists of blocking the victim's device by making them think of a serious problem in order to push them to call a fake technical support that bills them for a pseudo breakdown of several hundred euro; the realisation and then the resulting investigations led to the arrest of 3 individuals in early 2019 and the seizure of 1.9 million euro of criminal assets;

- crypto porn blackmail: this is a message from an alleged "hacker" who informs them that they have hacked into the targets' device and blackmails them by threatening to publish compromising information if they do not pay a ransom of several hundred to several thousand euro in crypto-currency (bitcoin); 30,000 reports and 2,000 complaints have been filed

- the "Mon Compte Formation" (My Training Account) scams, where French citizens have their training credits siphoned off through identity theft mechanisms and/or complicity within training organisations; the estimated loss is several tens of millions of euro.

How do we react most of the time? Fortunately, most of us can see that it is a fraudulent attempt and the email or SMS in question is simply destroyed. Sometimes you get a phone call from your parents or grandparents, anxious about receiving this type of solicitation. We reassure them by telling them to ignore it.

How many of us make a report (to the authorities or to the mechanisms in place for reporting spam in large French companies *(for example abuse@orange.fr for the historical operator or the 33700 for unwanted SMS)?* Amongst the most vulnerable French citizens, how many have actually reacted and been swindled? Finally, among this last category, what proportion of people too ashamed of the idea of having been deceived, fails to speak about it either to their relatives or to the authorities: *"After all, I only lost a hundred euro and it's my fault, I should have been more careful..."*

Cybercriminals have understood that when they remain below the thresholds of acceptability (individual and/or collective), the probability that they will never be investigated is almost zero. The official statistics on cybercrime in France are therefore probably largely underestimated. Worse still, victims very regularly feel responsible for their e-credulity.

It is therefore crucial to change the perception of citizens, so that real victims are no longer ashamed of having been defrauded and systematically file complaints. The trend must be reversed: the passive majority of French people must report the attempts they are being targeted with.

[4] Source: *Cybermalveillance, rapport d'activité 2021* (Cyberbullying, Activity Report 2021)

RECOMMENDATION 5
CONDUCT A MULTI-YEAR NATIONAL CYBERSECURITY AWARENESS RAISING CAMPAIGN

In the digital ecosystem, the ease of use of technology prevails over potential risks. We have to admit that our fellow citizens have never been taught how to securely use the digital tools that are so widely promoted. If we draw a parallel with the world of transportation, the technical complexity of the operation of a car is certainly totally hidden from the driver. On the other hand, every driver is aware of the dangers of the road: they are trained (driving licence), have regular reminders (road safety messages) and are subject to monitoring (speed cameras, traffic cameras, traffic police, etc.)

We therefore propose to carry out a "road safety" type awareness raising programme on cyber risk prevention. The preferred target of this campaign would be adults between the ages of 18 and 60, taking into account the leverage effect they will have on other categories of the population. They will be able to spread the right messages to their children: 11-18 year olds are connected to social networks earlier and earlier (60% of 11-12 year olds have an account on a social network) and the time spent behind the screens has further increased over this age group during the periods of lockdown in 2020 and 2021. The 18-60 year olds will also be ambassadors of best practices to seniors (more cautious than young people, the latter rely heavily on their family circle, especially their children and grandchildren, for all technical and computer-related matters, including matters of cybercrime).

A synthesis of the studies conducted on this subject shows that this approach should be more like a programme than a simple campaign. We need to be part of a permanently accessible, long-term process, and we need to build on the reputation gained by the October European Cyber Security Month. The often complex messages of cyber security experts will have to be transformed into simple, strong and even amusing messages in order to encourage their active adoption and dissemination. A formal media plan will have to be established; it will be by definition multi-channel: TV (adverts and dedicated programmes), social networks (personal and professional), with messages adapted to the segmentation of targeted citizens. This programme may also promote the *TousActeursCyber (AllCyberPlayers)* app presented in Recommendation 4.

The budget for this type of programme has been estimated by an in-depth study to be around 4 million euro. It will probably be necessary to release a multi-year budget to repeat the same messages over the long term in order for this recommendation to bear fruit and lead to a real awareness among citizens. However, the following years' campaigns could be considered in a more targeted manner.

6. TRAINING AT ANY AGE - PART 1, TRAINING BY THE NATIONAL EDUCATION SYSTEM

FINDING 6: EXISTENCE OF MULTIPLE CYBERSECURITY AWARENESS INITIATIVES FOR 6-18 YEAR OLDS

The Internet Permit for Children, launched in 2013, is a nationwide programme to empower fifth graders and their parents to be vigilant, safe and responsible users of the Internet. The French Gendarmerie Nationale and the AXA Prévention association are joining forces and pooling their expertise in protection and prevention against digital risks for children aged 9 to 11. At the end of 2019, two new themes will be integrated: cyber harassment, in collaboration with the Gendarmerie's digital mission, and hyper-connection in addition to the resulting attention and concentration disorders. In 2020, 72,529 elementary school students were educated by the Gendarmerie through this programme. The details of the Internet Permit can be found on www.permisinternet.fr

Initiated by the state in 2016, Pix is a non-profit structure constituted as a public interest group with the mission of supporting the raising of the general level of digital skills. Rapidly promoted in secondary education, the Pix certification will replace the B2i in 2021, in particular by highlighting the digital skills of 9th grade students via a compulsory assessment.

Cybersecurity is addressed in the "Protection and Security" skills around two themes:

- **Securing the digital environment:** Securing equipment, communications and data to protect against attacks, traps, nuisances and incidents that can affect the proper functioning of hardware, software, websites, and compromise transactions and data (with protection software, encryption techniques, mastery of best practices, etc.).
- **Protecting personal data and privacy:** Controlling your browsing history tracks and managing personal data to protect your privacy and that of others, and adopting an informed practice (by adjusting privacy settings, regular monitoring of your browsing history by alerts or other tools, etc.)

Since April 2019, ANSSI, in partnership with the Ministry of National Education, Youth and Sports (MENJS), has been launching the CyberEnJeux experiment to train young people in cybersecurity through the creation of games[5]. Cybermalveillance (Cyberbullying) also has a page dedicated to raising the awareness of young people[6]. For 7-11 year olds, it includes "Les Incollables (The Unbeatables)", "Deviens un super-héros du Net (Become an Internet Super hero)", "Les As du Web (WWW aces)" and the "Permis Internet (Internet Permit)", for 11-14 year olds, "1,2,3 Cyber", and for teenagers, "La Hack Academy (Hacking School)".

[5] All the details of the experimentation are given in this link

[6] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/dossier-accompagnement-sensibilisation-des-jeunes

RECOMMENDATION 6
CONCENTRATE ALL THESE INITIATIVES AROUND THE NATIONAL EDUCATION PIX PROJECT

Even if we should welcome the different initiatives for training young French citizens, it would be more efficient to combine the efforts of all the stakeholders around a single common project (even if it means that several stakeholders contribute to the development of the different modules). The dissemination of messages by the National Education system via Pix seems to be the right lever for several reasons.

First of all, it is a programme that is now recognised and that can be scaled up (1.2 million agents and 12 million students).

Moreover, it deals with the concept of digital acculturation globally and is and not just a solution dedicated to cyber security. Cyber issues must be addressed in the context of digital use, the use of tablets, computers, smartphones, and the use of social networks that are part of our children's daily lives from elementary school onwards so as to be relevant and reassuring.

Finally, in the same way that Moral and Civic Education (EMC) is taught within the framework of school programmes by a History and Geography teacher, it is key to make our young generations aware of their responsibility to use the Internet in a reasoned way within schools by teachers trained within the framework of a pedagogical programme defined and validated by the Ministry of National Education.

Pix could be scaled up by gradually defining the knowledge to acquire in terms of cybersecurity:

- cycle 1 (nursery school) seems a bit early to deal with these concepts - it is better to limit ourselves to digital uses with a playful approach;
- cycle 2 (primary school) would address the main risks associated with the discovery of the Internet (bad encounters);
- cycle 3 (primary school-secondary school) would allow students to develop autonomy through good practices (choice of a password, creation of an email address, use of avatars or pseudo, online purchases);
- cycle 4 (secondary school) would focus on the consequences of digital footprints (personal data, cyber harassment, fraud, identity theft).

Each step would be validated by the awarding of a coloured belt (like in judo) that the student could upload to his or her AllCyberPlayers application presented in recommendation 4.

High-school and higher education could develop specific modules adapted to the level and specialties of the different students: the popularisation of the notions of encryption, password hashing and brute-force attacks could be a good illustration of the mathematics programme in any scientific curriculum.

Finally, as part of the National Cybersecurity Strategy of the Future Investment Programme, the process of supporting and adopting cyber solutions by individuals, companies, communities and the Government could very well be hosted by Pix for all online initiatives. It is expected that this initiative will be financed in the amount of €176 million, of which €156 million is public funding.

Pix would thus make it possible to federate two important and inseparable issues throughout the schooling process:

- on the one hand, mandatory training in new information and communication technologies (NICT) for students from nursery school (fun aspect) to the end of high school (more scientific aspect);
- on the other hand, the risks associated with these uses by emphasising the awareness of possible manipulations on social networks and the dangers of the Internet.

The user perceives only a small part of the path that his or her personal data take. Data are used to **individualize product recommendations**, or to estimate the price a customer is willing to pay for a product, and therefore whether it is relevant to offer him or her a discount on the price: this is a form of **price discrimination**. For the user, the output data of these algorithms, i.e. the advertisements he sees, the products that are recommended to him ,and the prices that are proposed to him are the only manifestation of the generalized use of his data by the various digital actors.

ALL PUBLIC INVESTMENTS IN THE DIGITAL DOMAIN SHOULD BE SUBJECT TO A EUROPEAN SOVEREIGNTY CLAUSE, GUARANTEEING A "NATIVE AND EXPLICIT LEVEL OF CYBER SECURITY".

7.TRAINING AT ANY AGE - PART 2, PROFESSIONAL TRAINING

FINDING 7: PREVIOUSLY TRAINED GENERATIONS DON'T HAVE A BACKGROUND IN CYBERSECURITY

Academic training is not sufficient to ensure that generations trained twenty years ago, regardless of their academic level, have skills that are in line with the changes in the world today. Typically, Generation X has heard very little about cyber security during their studies, even for engineers who specialised in computer programming. Professional training throughout one's career or in the context of retraining is therefore a key lever for forward-looking management of jobs and skills (GPEC).

Since 2015, the personal training account (CPF) allows you to acquire training rights that can be used throughout your professional life. It is a tool aimed at skills in companies and for citizens, during the changes and transformations they encounter, especially those related to ecological and digital transitions. Among the major upcoming issues for My Training Account one can mention three:

- increasing the commitment of companies to their employees by expanding the range of services offered to companies through matching contributions;
- strengthening quality controls on professional certifications;
- combating endemic fraud and abusive canvassing on the system.

The success of the system is an asset that we can capitalise on[7] : 4 million downloads of the mobile application, 16.7 million unique visitors to the site, 3.87 million training applications accepted for an educational cost of €5.06 billion. However, the current offer in cybersecurity on MCF is low. Among the distance learning courses, there are only four courses, including one related to cybersecurity law. For physics courses, the statistics are a little better, but there are only five courses in Rennes and Paris, which are nevertheless the two leading regions in terms of cybersecurity in France.

In order to broaden the scope of this observation, the French government has introduced a general obligation to provide training in certain areas: for example, Article L. 4141-2 of the French Labour Code stipulates that the employer must organise practical and appropriate training in occupational health and safety. It covers several modules: traffic conditions (R. 4141-13), working conditions (R. 4141-13), what to do in the event of an accident or disaster (R. 4141-17) and the usefulness of the prevention measures prescribed (R. 4141-4). Caisse des Dépôts, in conjunction with the Ministry of Labour, Employment and Integration, is currently working to position My Training Account at the heart of this compulsory company training scheme.

RECOMMENDATION 7
USING MY TRAINING ACCOUNT AS A LEVER FOR E-LEARNING

As a first step, we propose to promote the use of My Training Account for all cyber training and certification in France.

[7] Data as of 22/02/2022

Initially, it will be necessary to expand the range of services offered by encouraging French digital training organisations (Formind, Advens, Atos, H2S, OCD, etc.) to register their training courses and certifications (ISO27001 Lead auditor, ISO27001 Lead Implementor, ISO27005 Risk Manager, CISSP, etc.) on My Training Account.

In a second phase, a major campaign to promote the approach among HR departments of companies could be organised in order to highlight the company's sponsorship in a key area of skills management: cybersecurity training. A recent study by the firm PWC, reported a shortage of talent in the cyber industry with around 5,000 positions needing to be filled. Company sponsorship in the amount of 25 million euro in the cyber sector alone would be very reasonable to imagine, given the matching funds already allocated by the ANCT (Agence Nationale de la Cohésion des Territoires) to the digital sector two years ago.

Finally, as part of the France 2030 programme, 140 million euro have been earmarked to set up cybersecurity training programmes via a call for expressions of interest (AMI CMA). The MCF system could naturally become the portal for linking training supply and demand, in the same way as the matching funds already implemented as part of France Relance 2025.

A second, more disruptive step would be to integrate cybersecurity into the legal framework for workplace safety in the same way as psychosocial risks. The labour code (and in particular the collective agreements in the fields most exposed to cyber risks) could be amended to include cyber risks in the articles dealing with working conditions (R.4141-13), and conduct to follow in case of accident or disaster (R.4141-17). Thanks to its initiative in the non-regulatory context described above, the MCF system would be positioned as a natural lever for the implementation of a training programme on a large scale so that the French industrial and economic fabric can become more resilient to a targeted or more global cyber attack.

8. OFFER A SINGLE SERVICE ACCESSIBLE TO ALL

FINDING 8: MULTIPLICITY AND COMPLEXITY OF THE DEMATERIALISATION OF GOVERNMENT SERVICES TO FIGHT AGAINST CYBERCRIME

For the past two decades, the Government has invested heavily in the dematerialisation of citizens' procedures. The Ministry of Finance was a precursor with the implementation of the website impots.gouv.fr now used by all French people at least once a year. The development of the France Services one-stop shop also provides access to the main public service organisations in a single location: the Ministry of the Interior, the Ministry of Justice, the Public Finance Department, Employment Centre, Retirement Insurance, Health Insurance, Family Allowance (CAF), the Farmer’s Social Security (MSA) and the Post Office.

Cyber crime being in essence digital in origin, has not be ignored in the initiative to digitalise public services following the explosion of these crimes. The French government has commissioned different services which are all very successful: Pharos, Percev@l and cybermalveillance.gouv.fr.

The Percev@l platform (opened in 2018) allows any citizen to report fraudulent use of their bank card, to law enforcement agencies. If a citizen detects a credit card transaction that they did not initiate and is still in possession of their card, they can enter an alert based on the transactions identified on their bank statement. In concrete terms, the person must provide

THERE IS NO GUARANTEE OF THE INDEPENDENCE AND RELIABILITY OF THE MEASUREMENTS MADE, AND NO CONSENSUS ON THE VALUE OF THE WIDELY PUBLISHED RATINGS BY THE OLIGOPOLY OF AMERICAN AGENCIES.

their bank card number, the name of the bank, the date, the wording and the amount of the fraudulent expenses noted, as well as any additional comments that may help the investigating authorities in their research. Reporting facilitates and expedites the reimbursement of fraudulent transactions upon presentation of a receipt to your bank.

Percev@l has a purely judicial aim and is used to correlate different transactions whose individual loss is small but which, once correlated between different victims, can represent substantial amounts and therefore give rise to referrals to the investigation services of the police. In 2020, Percev@l received nearly 320,000 reports, an 86% increase over 2019. On average, this represents 873 alerts per day for a total loss in the amount of 136,604,730 euros (i.e., 428 euros on average per alert).

Pharos is the acronym for Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Platform for Harmonisation, Analysis, Cross-checking and Orientation of Alerts). It is a website created in 2009 to report illegal on-line content and behaviour. The central role of this platform was reaffirmed following the terrorist attack on the school-teacher, Samuel Paty with the addition of staff so that this service is now available 7 days a week, 24 hours a day. In 2020, 289,590 reports were made online. The majority of the reports concern scams and extortion. After that, come the offences against minors (child pornography, sexual predators, etc.), the reports of discrimination and finally those concerning the support for acts of terrorism.

The Public Interest Group CyberMalveillance.gouv.fr was created in 2017 (following an incubation within the ANSSI services in 2016-2017). It constitutes an observatory of the digital threat but also assists victims of cyber-malware. 173,000 requests for assistance were triggered in 2021, with a total number of individual visitors of 2,482,700. The main types of scams (fake technical support, crypto porn, My Training Account, etc.) are explained to French citizens.

The digitally agile citizen will undoubtedly find the right online site to effectively and quickly alert the government services about the fraud or cyber crime of which they are the victim. But the citizen who is not so well versed in digital tools and who is already highly perturbed by the loss they have just suffered, may quickly become discouraged by the complexity of the decision tree they are confronted with in order to report the incident.

RECOMMENDATION 8
CREATE AN ALLCYBERPLAYERS APP CENTRALISING ALL THE CYBER FEATURES AND INFORMATION THAT THE PUBLIC NEEDS

Following the example of the *TousAntiCovid* (AllAgainstCovid) application, which centralises all information on the pandemic crisis in France, we propose to develop a unique online information and reporting solution in the form of an Android and IOS app: *TousActeursCyber (AllCyberPlayers)*.

For the past two years, cyber risk has become one of the three systemic risks commonly admitted by all insurance companies in their annual reports - *along with pandemic risk and global warming risk* - thus a user-friendly public pathway should be devised and implemented in order to address and react early on to any potential cyber crime aggravation in the coming months and years.

First of all, in terms of the percentage of the French population potentially targeted, this application would potentially address all French citizens. As a reminder, *AllAgainstCovid* has had 52 million initial downloads and 42 million activations since its inception in June 2020. Obviously, it is unlikely that the *AllCyberPlayers* application will experience such a high level of downloads (unless France suffers a massive cyber attack in the near future, which of course nobody hopes for). Nevertheless, assisting the implementation of *AllCyberPlayers* by the proposed training measures (with the youngest, via promotion in Pix, with the entire French population in the context of a road safety type campaign and globally via a pop-up in *My Training Account* when searching for training in the cyber domain) would increase its recognition, particularly with the Y and Millennium generations.

In terms of features, the app will above all promote the services provided to French people:

- The mandatory integration of reporting features (Percev@l, Pharos, Signal-Spam, etc.). In addition to the centralisation of all services, improvements could be made to some of them: for example, for Percev@l, Banks could be required to provide a feature for selecting fraudulent bank card transactions and exporting them in the form of a pivot format that can be directly downloaded by the *AllCyberPlayers* app (thus automating a certain number of manual re-entries that have no added value and are even a source of errors).

- The availability of cyber news: like the CERT FR bulletin of the ANSSI, summaries popularising information on cybersecurity could be consulted through this app. This part, which initially is very neutral, could also be a Viginum relay over the long term, in order to provide Lutte Informatique d'Influence (L2I) (Digital Influence Control) features in the event of fakenews or attempts to influence the population during major events in France (e.g. national elections, organisation of the Olympic Games in Paris in 2024, etc.)

- Direct contact with the police services in the event of a proven attack, as well as the possibility of being informed about local private stakeholders (those who have obtained the cyber expert label from CyberMalveillance.gouv.fr) that can provide assistance, especially to small structures or individuals.

- Although more complex to delineate in terms of personal freedom and CNIL compliance, we can consider the possibility of sending alerts through the application in case of cross-referencing of information obtained by supercritical operators (see recommendation 7): for example, a smartphone connected from a private WiFi network with a public IP address having been the target of a scan or an attack from a identified Command and Control (C&C) server belonging to a cybercriminal group, could be warned of an imminent or past potential risk.

- More anecdotally, the storage of cyber passports, especially those obtained through Pix (see recommendation 2)

A key point in the success of this recommendation will be to verify the feasibility under French law of concentrating all these services in a single application. It can be recalled that the Council of State has made several changes to *AllAgainstCovid* since its introduction. It is important that this application can respect the privacy and individual liberties of citizens, but that it can be nominative, regardless of the place of connection, for example, by using FranceConnect for identification.

CONCLUSION

The digitalization of the EU member states' government, society and economy is a key challenge of our time, and the French government deserves praise for the way they used their EU presidency term in the first half of 2022 to try and address it. Yet, the EU's member states still have a long way to go, especially the biggest countries such as Germany, France and Italy. Moreover, even in those countries that are acknowledged leaders in e-government and pride themselves on their highly digitalized economies such as Denmark much remains left to do in regards to cybersecurity.

The ongoing ransomware epidemic remains unanswered, and the hacks of major companies by cybercriminals have become a normal feature of our news programmes. At the same time, large-scale attacks such as the recent SolarWinds case have proven the ongoing vulnerability of our most critical infrastructure and government networks to hostile state hackers. It will require an enormous effort by all sectors of society to change our culture towards an approach that ensures that basic cybersecurity measures are implemented everywhere and all of our critical networks are equipped with more sophisticated protection. This report is to be welcomed as a contribution to this debate over just how we are going to reach this goal in the whole EU within the next few years.

One of its key recommendations is to take a closer look at cyber security rating agencies, a novel but fast-growing sector that is rarely given the attention it deserves. These agencies scan the internet-facing parts of company networks for unpatched vulnerabilities, misconfigured port settings and other weaknesses a hacker might exploit. This is a sensible service to offer since it is exactly how cybercriminals work when looking for their next victims. There are obvious limitations to this approach as it is blind to anything that happens internally within company networks, but having the score is way better than nothing: a company with a bad score is highly likely to be bad at managing its cyber security risk. A company with a good score may have hidden flaws and gaps in its cybersecurity setup but short of a full risk audit there is no way of finding out.

Most of these rating agencies started out about ten years ago as service providers for the insurance industry, offering to solve a fundamental problem: as cyber insurance established itself as a successful line of business, how could insurers understand the level of cyber risk they were accepting by insuring a given company without investing the time and money necessary for a full audit? As a deep cyber audit only made financial sense when insuring larger companies, insurers embraced rating scores as a fast and cheap substitute.

Their huge growth in recent years is explained by the fact that the dilemma first encountered by cyber insurers (how do you find out whether a company has reasonable cyber security without a full audit?) is now being recognized as a general problem of the modern economy. Ransomware attackers increasingly focus on supply chains to infect their targets, either by hacking service providers with direct access to their target company's network or by sending manipulated emails from the email server of a known (and trusted) supplier. Therefore, the question whether you can trust the cyber security measures of a company you work with or even allow into your network is now a key problem of corporate risk management. But how do you establish whether your business partners are good or bad at managing cyber risk, especially when you are a sizable company working in direct business relationships with hundreds of other companies? With the upcoming introduction of the NIS 2 regulation that will require all EU member states to implement new cybersecurity requirements to protect their critical infrastructure, this will become a huge issue. Art. 18 of NIS 2 requires all organisations within the scope of the new legislation to demonstrate that they are running sophisticated programmes to manage the cyber risk in their supply chains. For companies in industries such as food production that have no experience with cyber security regulation this will be a very tough challenge. The lure of a service that offers to distil the entire complexity of company cyber security into a single figure – the company's overall cyber risk score – will prove irresistible to risk managers and CEOs in every EU member state.

In short, cyber risk scores sold by rating agencies offer a quick, cheap and scalable solution to the supply chain cyber risk problem, and my prediction is that the scores set by the leading rating agencies will become one of the key figures used by others to assess whether to work with a company or not.

Therefore, the question how these scores are made and by whom will become hugely important, and it is an overlooked part of the current struggle for the EU's digital sovereignty: as it stands, these ratings are made by a handful of US companies that do not face any strict legal requirements to explain how their scores are generated. As Europe found out during the 2008 financial crisis, being economically dependent on ratings created by private US companies does come with a certain risk. Therefore, I have argued elsewhere that we should think seriously about establishing a European cyber risk rating agency[8] and I applaud the efforts of the drafters of this report to bring this important but largely overlooked issue to the attention of European policymakers.

Jan Martin Lemnitzer

Jan Martin Lemnitzer teaches cyber security at the Department of Digitalisation, Copenhagen Business School. He holds a PhD from the London School of Economics. He was co-organiser of the 2018 Odense Cyber Security conference funded by the Danish Tech Ambassador and researches the emergence of cyber norms, national cyber strategies, the potential of cyber security ratings and insurance, and the question of neutrality in cyber space.

[8] Jan Lemnitzer, 'Do we need an EU Cybersecurity Rating Agency?', EU Cyber Direct Blog, 10 November 2020, available at https://directionsblog.eu/do-we-need-an-eu-cybersecurity-rating-agency/

SUMMARY OF OUR RECOMMENDATIONS

ISSUE 1: ADOPTING AN OFFENSIVE STANDARDISED STRATEGY

TO MAKE THE CURRENT EUROPEAN FRAMEWORK EVOLVE, VIA 4 PROPOSALS:

1. Derogate from the principle of universality of the cyber defence budget	Growth in tax revenues (taxes and fines) related to digital activities	Directing the budgetary equivalent of these tax revenues towards securing the digital world
2. Reinforcing European standards on the principles of "security by design"	Exponential growth in the number of vulnerabilities	6.a. Impose a Cyber EU standard listing the fundamental principles to be adhered to by the industry 6.b. Make a flash cybersecurity diagnosis mandatory
3. Extend the legal scope of attack detection to certain supercritical operators	Existence of certain private stakeholders with a privileged role in the fight against cybercrime	Consider giving telecom operators a greater role in detecting cyber attacks
4. Develop a cyber risk rating agency based on a European standardised model for all public purchases.	8.a. Lack of autonomous capacity to assess cyber risk 8.b. Uneven and opaque cyber risk assessment methods 8.c. Discrepancies in the interpretation of the cyber rating	8.a. Creation of a European accreditation system for cyber rating 8.b. Definition of a standardised European model for cyber rating 8.c. Implementation of a European certification for cyber analysts

ISSUE 2: MAKING CYBERSECURITY A SOCIETAL ISSUE

ENSURING THAT THE POPULATION IS WELL PROTECTED, VIA 4 PROPOSALS:

SUJET	FINDING	RECOMMANDATION
5. Raising awareness amongst the greatest number of people	Low awareness of cyber risks and dismay of victims	Conduct a multi-year national cybersecurity awareness raising campaign
6. Training at any age - part 1, training by the National Education system	Existence of multiple cybersecurity awareness initiatives for 6-18 year olds	Concentrate all these initiatives around the National Education Pix project
7. Training at any age - part 2, professional training	Previously trained generations don't have a background in cybersecurity	Using My Training Account as a lever for e-learning
8. Offer a single service accessible to all	Multiplicity and complexity of the dematerialisation of Government services to fight against cybercrime	Create an AllCyberPlayers app centralising all the cyber features and information that the public needs

DIDIER GRAS

Trained as an engineer (EPITA, Télécom Paris) with over 25 years of dedicated professional experience in the field of Cybersecurity, allowing him to investigate all the components of this sensitive field in a number of activity sectors. With his unique career path, he currently holds the position of CISO (Chief Information Security Officer) and IT Risk Officer at BNP Paribas - Banque Commerciale in France.

He has been elected several times by his peers as a director and secretary general of CESIN - Club des Experts de la Sécurité de l'Information et du Numérique (gathering together more than 800 French CISOs from companies of all sizes, administrations and local authorities).

This organisation participates in the professionalisation of the Cyber industry and has created a platform for secure exchanges within the framework of the cross-sector management of alerts on critical Cyber vulnerabilities and incidents.

ARNAUD MARTIN

Arnaud Martin, Director of Cybersecurity for the Caisse des Dépôts Group, is a graduate of Ecole Polytechnique (X98) and the Technische Universitaet Muenchen (2003).

He has been working for 19 years on information technologies and their security: at Siemens (in Germany), then in France within the Orange group and now at the Caisse des Dépôts.

He was a member of GITSIS (Groupement Interprofessionnel pour les Techniques de Sécurité des Informations Sensibles) between 2015 and 2019, and then of CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) since 2019, where he leads the work of the College A body.

He is also an auditor for the national session of the IHEDN 2021 - 2022 (Digital Sovereignty and Cybersecurity major)

ACKNOWLEDGEMENTS

This publication was written in conjunction with the work carried out at the IHEDN national session 2021 - 2022 - major digital sovereignty and cybersecurity. It is based on interviews conducted with the session's auditors and external speakers, as well as discussions on specific themes with CESIN peers or colleagues from the Caisse des Dépôts Group. This work would not have been possible without our discussions with Cyril, Céline, Philippe, Gautier, Johanna, Jérôme, Laurent, Hélène, William, Antoine. And a very special thanks to François Marchessaux and Jean-Claude Tapia.

We would like specifically to thank IHEDN and CESIN for allowing us to reflect on global cybersecurity issues in privileged ecosystems and to work on securing a digital France and a digital Europe.

Finally, a big thank you to Arno Pons and Olivier Sichel for their advice and proofreading prior to publishing this note!

DIGITAL NEW DEAL
THE THINK-TANK OF THE NEW DEAL

Digital New Deal accompanies private and public decision-makers in the creation of an Internet of the Enlightenment, European and humanistic. We are convinced that we can offer a 3rd digital way by aiming at a double objective: to defend our values by proposing a new regulation against the centralization of powers; and to defend our interests by creating the conditions of cooperation against the capture of value by the "Big Tech".

The purpose of our publication activity is to shed as much light as possible on the developments at work within the issues of "digital sovereignty", in the broadest sense of the term, and to develop concrete courses of action, even operative via the Do Tank, for economic and political organizations.

THE BOARD OF DIRECTORS

Olivier Sichel (founding president) and Arno Pons (general delegate), steer the strategic orientations of the think-tank under the supervision of the board of directors.

Strengthened by their common interest in digital issues, the members of the Board of Directors have decided to deepen their debates by formalizing a framework for production and publication within which the complementarity of their experiences can be put at the service of public and political debate. They are personally involved in the life of Digital New Deal, especially in the choice of reports and their editors. They are the guarantors of our academic and economic independence.

SÉBASTIEN BAZIN
PDG AccorHotels

NATHALIE COLLIN
General Manager, Consumer and Digital Division La Poste Group

NICOLAS DUFOURCQ
DG of Bpifrance

AXELLE LEMAIRE
Former Secretary of State for Digital Technology and Innovation

ALAIN MINC
President AM Conseil

DENIS OLIVENNES
DG Libération

YVES POILANE
DG Ionis Education Group

ARNO PONS
General Delegate of the Digital New Deal think tank

JUDITH ROCHFELD
Associate Professor of Law, Panthéon Sorbonne

OLIVIER SICHEL
President Digital New Deal
DGA Caisse des Dépôts

BRUNO SPORTISSE
PDG Inria

ROBERT ZARADER
PDG Bona fidé

OUR PUBLICATIONS

RGPD, acte II : la maîtrise collective de nos données comme impératif | Julia Roussoulières, Jean Rérolle – *May 2022*

Fiscalité numérique, le match retour | Vincent Renoux - *September 2021*

Défendre l'état de droit à l'ère des plateformes | Denis Olivennes et Gilles Le Chatelier - *June 2021*

Cloud de confiance : un enjeu d'autonomie stratégique pour l'Europe | Laurence Houdeville et Arno Pons - *May 2021*

Livres blancs : Partage des données & tourisme | Fabernovel et Digital New Deal - *April 2021*

Partage de données personnelles : changer la donne par la gouvernance | Matthias de Bièvre et Olivier Dion - *September 2020*

Réflexions dans la perspective du Digital Services Act européen | Liza Bellulo - *March 2020*

Préserver notre souveraineté éducative : soutenir l'EdTech française | Marie-Christine Levet - *November 2019*

Briser le monopole des Big Tech : réguler pour libérer la multitude | Sébastien Soriano - *September 2019*

Sortir du syndrome de Stockholm numérique | Jean-Romain Lhomme - *October 2018*

Le Service Public Citoyen | Paul Duan - *June 2018*

L'âge du web décentralisé | Clément Jeanneau - *April 2018*

Fiscalité réelle pour un monde virtuel | Vincent Renoux - *September 2017*

Réguler le « numérique » | Joëlle Toledano - *May 2017*

Appel aux candidats à l'élection présidentielle pour un #PacteNumérique | *January 2017*

La santé face au tsunami des NBIC et aux plateformistes | Laurent Alexandre - *June 2016*

Quelle politique en matière de données personnelles ? | Judith Rochfeld - *September 2015*

Etat des lieux du numérique en Europe | Olivier Sichel - *July 2015*

contact@thedigitalnewdeal.org

THINK-TANK DIGITAL NEW DEAL

September 2022

www.thedigitalnewdeal.org