

cahiers

IN CYBER

InCloud we trust ?

HIGHLIGHTS

5-7 APRIL
2023

LILLE GRAND PALAIS

THE INTERNATIONAL
CYBERSECURITY FORUM

BECOMES



summary

Highlights of the InCyber 2023 Forum



edito	1
trends	2
program	10
opening plenary	12
plenary #1 : Cloud security: pie in the sky?	16
plenary #2 : Can trust exist in a digital world?	18
plenary #3 : Cloud: should Europe start a revolution?	20
inCyber.org press review	22
Are ransomware gangs just like any other business?	24
OSINT specialists discuss the technical and legal challenges facing this discipline	28
4 key issues for surviving in the Wild West of domain names	34
How the war in Ukraine boosted the construction of Europe's cyberdefence	38
Usernames and passwords at the heart of cyber threats	42
CRQ: how to financially quantify cybersecurity risks	48
An obstacle course for Europe's sovereign Cloud	52
Cloud : Is Europe Falling Behind?	58
In the face of cybersecurity threats, Europe is getting organised, says Thierry Breton	62
Trust in Digital Technology: "We Can't Believe What We See Anymore"	66
barometers & panoramas	70
InCyber Forum in key figures	76
partners	78
contacts	80



Cloud computing:

the question(s) of trust

General of the Army (2S) Marc WATIN-AUGOUARD

CEO of InCyber Forum

Guillaume TISSIER

General director of InCyber Forum

Public cloud computing is driving the digital transformation. With an adoption rate of just 40% in Europe, the market potential for providers and productivity gains for end clients are colossal. However, the choice cannot simply come down to functional and financial criteria, since this choice constitutes a long-term commitment.

To simplify, public cloud computing means that organisations are *"using someone else's computer"*, trusting them not only with a part of their data assets, but also their most strategic business processes. Therefore, cybersecurity and trust – or lack thereof – are essential. While cybersecurity can be assessed, measured and compared, trust relies on a much more subjective appreciation that can rarely be covered by a contract. As a result, we are usually forced to trust "by default".

These two aspects entail multiple risks. Although the resource pooling that cloud computing allows is an advantage in terms of cybersecurity, the concentration of data also constitutes a weakness in terms of resilience: for example, an attack on a hypervisor can create a systemic risk.

On a strategic level, the dependency, or even "lock-in", that some contracts create can also weaken organisations and ultimately disrupt traditional value chains. Finally, trust is being strained by the increasing number of laws with extraterritorial reach, especially given the tense geopolitical environment.

With 70% of Europe's data being stored and processed outside the continent, mainly by American hyperscalers, the threat of it being held hostage by international tensions is a possibility that seems increasingly realistic.

To cope with these threats and reap the benefits of the cloud computing revolution, Europe can no longer put up with this situation of extreme dependency. All the more so because Europe has many attractions: successful and innovative companies, strong traditional industry and a large potential market, to name just three.

What strategies and policies would help Europe to accelerate the growth of its own cloud computing industry? What sectors and technologies are a priority? How can Europe reconcile the demands of a rapid digital transformation with its desire to shore up its digital sovereignty? What is the best way to guarantee the cybersecurity and resilience of cloud computing infrastructures, which are exposed in an exponentially increasing number of ways? How does the industry build trust?

Digito

the cyber threat

in key figures

THREATS

13

data leaks per day

Source: InCyber Forum / CNIL
data leak barometer 2023)

30%

of local authorities have already
been victims of ransomware

Source: CLUSIF

53%

of organizations have suffered
an attack on their cloud infrastructure

Source: Netwrix

79%

of companies have suffered at least one
data breach in the cloud in the last 18 months

Source: CapGemini

43%

of French companies affected in 2022
(compared to 54% in 2021)

Source: CapGemini

74%

of financial flows linked to
ransomware attacks point to Russia

Source: Chainalysis

13 000

vulnerabilities reported
in 2022 (-30% compared to 2021)

Source: NIST

62%

of organizations attacked by
ransomware pay the ransom

Source: Hiscox

1

France has an average of 1 cybersecurity
staff for every 1,500 employees

Source: Wavestone



ransom

the cyber threat

in key figures

ANSWERS

2024

The NIS 2 directive, which came into force in 2022, set out numerous cybersecurity requirements and will be transposed in the member states by the end of 2024

x10

The number of organizations affected by NIS 2 will increase tenfold

2022

The European Commission proposed in September 2022 a first version of the Cyber Resilience Act that will apply to all products and services containing digital content

81%

81% of companies have deployed EDR (Endpoint Detection & Response) systems

Source: CESIN

12

regional CSIRTs are being set up

700

local authorities have benefited from a cybersecurity course

in 2022

European start-ups raised €2.4 billion (+20%), i.e. 16% of the amounts raised worldwide in cybersecurity

Source: Tikehau Capital / Baromètre Forum InCyber

2023

In April 2023, during the FIC, the European Commissioner Thierry Breton announced a "Cyber Solidarity Act" and the establishment of a "cyber dome" consisting of operational cybersecurity centers



Answers
Forum

Vincent STRUBEL

General Director of the ANSSI
France's National Cyber Security Centre

INCYBER FORUM 2023



International
Cybersecurity
Forum

APRIL 5-7, 2023

LILLE GRAND PALAIS

europe.forum-fic.com

*We need to move
from high fashion
to ready-made
to expand and
massify our actions.*



**A global
market of
€250 billion
in 2022:**

of which €34 billion
for Europe

of which €3 billion
for France

MARKET

st
d
r
e
t



plenary sessions
contents

program



↘ *It is absolutely essential to coordinate cybersecurity at a European level, and you can count on me to do so with determination and without respite.*

Thierry BRETON

European Commissioner for the Internal Market

[WATCH VIDEO](#)



opening plenary

We assume fully to defend a logic of digital sovereignty in order to develop european champions of the cloud.

Jean-Noël BARROT
 Delegate Minister for Digital Affairs
 FRANCE

WATCH VIDEO



Civil preparedness starts with personal preparedness. Every single actor needs to take the responsibility of its cybersecurity. States cannot take all the responsibilities. Every single actors need to do their job.

Carl-Oskar BOHLIN
 Minister of Civil Defense
 SWEDEN

WATCH VIDEO



The strength of cybersecurity is unity. The State cannot meet the expectations of cybersecurity alone. The InCyber Forum is the ultimate public-private partnership.

Jean-Noël DE GALZAIN
 CEO of Hexatrust
 FRANCE

WATCH VIDEO



Concerning accountability of states, we have the normative framework to prevent non responsible behaviors. The diplomacy toolbox has different tools in it: the more direct process is to reach to a country but we can go all the way up to calling out a country to sanction.

Nathalie JAARSMA
 Dutch Ambassador at-Large for Security Policy and Cyber
 NETHERLANDS

WATCH VIDEO

Thanks to the InCyber Forum, the largest cyber security cybersecurity in Europe, for bringing together so many profiles and allowing them to meet.

Ludivine DEDONDER
 Minister of Defense
 BELGIUM

WATCH VIDEO



At NATO, we have set up the DIANA project. DIANA project: we pay start-ups to work with us, giving them a foothold in our strategy. We give them access to our contracts, enabling them to work in our field. It's a win-win situation: they need peace to work, we need them for peace.

James APPATHURAI
 Deputy Assistant Secretary General for Emerging Security – NATO

WATCH VIDEO





↙ *The question does not come down to good or bad cloud: it is not a turn-key solution, it does not exempt companies from having to worry about their backups, their updates...*

Vincent STRUBEL

General Director of the ANSSI

WATCH VIDEO



plenary #1
Cloud security: pie in the sky?



↘ *The difficulty with social networks is that they generate communities of interest, not of solidarity. We are in the age of surveillance coming from below: anyone can spread any information. There is so much of it that we are lost. We don't know how to find our way in this ocean..*

Jean-Gabriel GANASCIA

University Professor & Chairman of the CNRS Ethics Committee

WATCH VIDEO



plenary #2
Can trust exist in a digital world?



↙ *To those who are convinced that the battle is not lost, let's get together, let's bring the players together to compete with GAFAM.*

Alain ISSARNI

CEO of Numspot

[WATCH VIDEO](#)



plenary #3

Cloud: should Europe start a revolution?



incyber.org

press review

These articles were written by InCyber.org journalists
based on round tables and conferences at the InCyber Forum Europe 2023

Are ransomware gangs just like any other business?

CYBERCRIME

XAVIER BISEUL



In recent months, many ransomwares as a service (RaaS) groups have disappeared or scaled back their operations. Their revenues are also lower due to the downturn in cryptocurrencies, their increased maturity, and a tighter regulatory framework. This unfavourable climate casts doubt on whether this 21st century mafia is viable over the long term.

Cybercriminal organisations are businesses like any other. They are born, grow and sometimes die. In fact, their mortality rate is particularly high, judging by recent setbacks suffered by leading ransomware gangs. In September 2021, the Babuk gang scuppered itself after its ransomware decryption keys were published on the dark web.

In March 2022, the Conti group disappeared after taking a stand in support of Russia in the war against Ukraine. In January 2023, the Hive group ceased all activities after their platform was seized by the FBI and Europol. Europol also pulled off a major bust by arresting two members of DoppelPaymer in March.

Other notorious gangs are still active but have suffered a number of setbacks. In September, LockBit's builder – the kit used to create its malware – was leaked on social media after the group's leader refused to pay a developer's salary. REvil's activities dropped drastically after the May 2021 attack on Colonial Pipeline, the main US oil pipeline operator.

These events raise questions about the long-term viability of ransomware groups. These 21st century mafia gangs seem to follow the same pattern as their physical counterparts. They get rich quickly, live large, and then disappear after one too many sideswipes or one fatal misstep.

Humans are the weakest link

These groups may hide behind the Ransomware as a Service (RaaS) business model, which with its resale of creation kits to affiliates and 24/7 commercial assistance

looks similar to the legal SaaS model, but they are still vulnerable. It is ironic that the main vulnerability is still human beings.

"Their mass model is based on optimised techniques and a distribution of tasks among stakeholders. This chain cannot be 100% automated; there are always humans behind it," says Livia Tibirna, cyber threat intelligence analyst at Sekoia.io.

Although gangs list which organisations to target and which to spare, their affiliates have been known to slip up and, for example, attack healthcare facilities. LockBit reportedly apologised and sent a free decryption key to a Toronto children's hospital that was attacked by mistake. RaaS groups also brag about their misdeeds by signing their names or leaving clues on discussion forums.

A mainly Russian-speaking ecosystem

Despite the rivalries that sometimes come to the fore, such as those between LockBit and REvil, a code of honour keeps fratricidal battles at bay. *"The ecosystem is still mainly Russian-speaking, with unwritten rules of camaraderie. Most groups in former Soviet countries do not attack each other. And this situation has not changed with the war in Ukraine,"* says Tibirna.

There have even been new collaborations. For example, software publisher Sophos reported that Hive, LockBit and BlackCat orchestrated an attack targeting the same network three times.

The geopolitical situation has nevertheless destabilised the teams involved. *"To escape military mobilisation, Russian cybercriminals have relocated to Turkey or Iran, exposing themselves to the risk of being arrested by international law enforcement agencies,"* Tibirna adds.

According to Karim Abillama, International Business Pre-Sales Director at NetWitness, detecting and tracking these gangs can take years: *"These groups are very well structured and sophisticated, especially in payment method, but they still have a fairly standard method of entry based primarily on spear-phishing."*

Ransomware is just the tip of the iceberg

In terms of targeting, the threat is still primarily opportunistic. It involves knocking on every front door before breaking into the information system. *"The gangs have a choice: either attack easy prey or go after bigger fish to increase their profits. Both scenarios are possible,"* adds Abillama.

Furthermore, ransom demands are systematically coupled with the threat to disclose the exfiltrated data. Abillama even highlights an increasing trend towards re-extortion. Cyber-gangsters return to the scene of their crime by holding the victim to ransom a second time. More than a third of companies attacked by ransomware in 2022 had already been attacked in the past, according to a Barracuda Networks report.

Tibirna also notes a greater flexibility in the relationship between RaaS groups and their affiliates: *"It used to be that it was not good for affiliates to buy from different groups. Now it is more acceptable. They can use two or three different malware programs."*

She also points out that ransomware, a particularly visible and high-profile threat, is only the tip of the iceberg: *"Behind it is a whole industry that has been developed around reselling data or laundering Bitcoins."*

Lower revenues

Despite this desire to maximise profits, the experts at the InCyber Forum 2023 round table on this topic pointed to a decline in revenues generated by the ransomware industry. Several factors are contributing to this market downturn. Tibirna mentions the increased maturity of businesses that have (finally) introduced backup systems and the fall in the price of Bitcoin and other cryptocurrencies.

There have also been developments in the legal framework. The attack on Colonial Pipeline in the United States in May 2021 was a wake-up call. It showed that in addition to being profitable businesses, gangs could disrupt the way in which enemy states operate. Shortly afterwards, according to Reuters, FBI boss Chris Wray urged companies and public institutions not to pay ransom demands to prevent crime from flourishing.

More recently, on 1st March 2023, Joe Biden's administration outlined its national cybersecurity strategy. The policy is clear: any ransomware attack that targets the country's critical infrastructure will be considered a threat to national security. The strategy identifies 16 key sectors, including health and energy.

For Cody Barrow, Vice President for Intelligence and Director of Threat Intelligence at EclecticIQ, this is *"a serious warning to cyber attackers and their accomplices"*. As ransomware becomes a national security issue, more government resources will be brought to bear.

"International cooperation is also likely to increase, with the US working more closely with allied countries," says Barrow. Ransomware groups will have at least played their part in encouraging the exchange of information throughout the Western world.

[READ THE ARTICLE ONLINE](#)

These groups are very well structured and sophisticated, especially in the way they pay, but they still have a fairly standard method of entry based primarily on spear-phishing.



OSINT is on a roll

DIGITAL TRANSITION

GEORGES BONFILS



Antoine Violet-Surcouf, Managing Director and Partner of Forward, was the driving force behind a second meeting of professionals from this sector at the International Cybersecurity Forum (Forum InCyber) in Lille on 5 April. After a very well attended first meeting in 2022, the OSINT Day organisers wanted to focus this year on the collegial and community nature of open source intelligence work.

As a reminder, OSINT (Open Source Intelligence) refers to open source investigations in a variety of contexts including law enforcement, cyber protection, journalism and fact checking. The term also covers other disciplines such as GEOINT, which analyses geographical data, and SOCMINT, which analyses social media.

In a round table discussion moderated by François Jeanne-Beylot, President of the French Economic Intelligence Union (SYNFIE), Hortense Grelier, Head of SEB's Intelligence and Innovation Department, explained that open source intelligence sends information to the group's various departments for operational support purposes.

OSINT and the war in Ukraine

The day began with the account of an official from the Ukrainian State Bureau of Investigation (SBI). Established in 2015, the bureau's activities have intensified since the start of the conflict in February 2022 and it now employs almost 1,600 people. Against the exceptional backdrop of the Russian invasion, its objectives include combating corruption, identifying Ukrainian citizens who are collaborating with Russian forces, and collecting evidence on war crimes committed in Ukraine and identifying the perpetrators.

To do this, the bureau's members rely on the SBI Recognition System (a facial recognition tool), images taken by Ukrainian forces and members of the SBI network, and sometimes photos posted by soldiers from the opposing side. The work involved in reconstructing the reality of the theatre of conflict from digital traces to gain strategic knowledge was summed up by one speaker: *"OSINT works best as a collaborative tool"*.

OSINT is useful for companies too

OSINT practices are also proving to be a useful decision-making tool for companies.

Other companies have different approaches. Henri de Banizette, coordinator of economic security for Auchan Retail International, says that the main challenge is ensuring business continuity, sometimes in risky environments, when assessing third parties during mergers and acquisitions or supporting departments investigating fraud or litigation cases, for example.

Sylvain Hajri, founder of the OSINT-FR community and EPIEOS, a company specialising in OSINT, proposed a different approach to OSINT using a "red team" method. This involves playing the role of an "opposing party" to identify flaws and obtain feedback that will ultimately serve to strengthen the physical or digital defence measures of the organisation being observed.

Analysis work and legal framework

Alexis Pinon, Director of Digital Investigations at Forward, stressed the importance of OSINT analysis work. The large amount of information available and the tools available to analyse it in depth (facial recognition, information on a username or an IP address, etc.) are particularly useful in finding personal information. It is therefore essential to use the available tools wisely, and to be wary of bias and "false positives".

Marc-Antoine Ledieu, a lawyer and CISO, spoke about the legal framework for practising OSINT. According to him, the following questions should be kept in mind: Will the information system hosting the data be available to all Internet users? Do we have the right to copy the data collected? Do we have the right to use the data? He also emphasised the distinction between open data (data held by public authorities for re-use) and leaks (private information such as trade secrets, personal data or intellectual property information).

Tools and methods used in OSINT

The analyst who uses the pseudonym “Palenath” demonstrated how he finds people wanted by Interpol based on their activities on social media. Pierre-Antonin Rousseau, Coordinator of AEGE’s OSINT & Veille club, managed to trace the alleged perpetrators of a scam by bouncing back and forth between various online sources.

Emmanuel Kessler, Head of Europol’s Partnership and Outreach Team, talked about the work of the European Cybercrime Centre’s OSINT team in supporting the digital investigations carried out by its investigators. This work includes weekly newsletters on the latest cyber incidents, malware developments and legal issues in the cyber domain, along with targeted topical reports to assist investigators in their work.

Julien Métayer, co-founder of the OZINT platform, shifted the focus in his presentation, adopting the point of view of the “targets”. According to him, people who practise OSINT do not see online information in the same way as an average Internet user. Therefore, all information posted online, even the most innocuous, could for example be used in an attempted intrusion via phishing.

Jihad, Ukraine and dating sites

What links jihad, Ukraine and dating sites? OSINT, of course. Damien Ferré, founder of Jihad Analytics, described his work on analysing the propaganda of Al-Qaeda and the Islamic State (IS). His presentation provided an opportunity to contrast the highly centralised communication of IS with the decentralised communication of the various al-Qaeda cells spread around the world, which have their own communication methods and potentially exchange information with each other.

Two of the founders of the Fox project presented their research methods for obtaining information on the presence of Russian troops in Belarus. The first step involved identifying the Russian armoured vehicles that were being transported to the city of Smolensk; the second used their in-house-developed SOCMINT tool to geolocate Russian soldiers.

Emmanuelle Welch, a private investigator, described dating apps as alternative search tools. She uses software to change an account owner’s geolocation, giving her an additional tool to geolocate wanted persons. This also allows her to conduct operational security audits for sensitive organisations, checking the information that some of their registered members may disclose on these sites.

All these contributions, which were presented to a full house, give an impression of the many subjects this discipline deals with and the opportunities it offers for specialists in safety, strategic intelligence and cybersecurity. Bringing together OSINTers to discuss their work is crucial, and this was a key message repeated throughout the day. The next OSINT Day will take place in March 2024.

[READ THE ARTICLE ONLINE](#)

The large amount of information available and the tools available to analyse it in depth (facial recognition, information on a username or an IP address, etc.) are particularly useful in finding personal information.



4 key issues for surviving in the Wild West of domain names

ANTIFRAUD ACTION

OLIVIER CIMELIÈRE



A company's domain name is one of the primary components of its digital identity and online presence. Paradoxically, it is still one of the most confusing areas to manage due to changing rules, intermediaries who are not always reliable and the lack of governance in companies. At In-Cyber Forum Europe 2023, a round table of experts examined all the technical, legal and marketing issues involved in owning a domain name.

A domain name is anything but an innocuous gimmick. It is what conveys the name of a company or a product brand on the web. It is what translates the encrypted IP address of a website into an understandable, memorable name for every internet user. Domain names also have an extension, which categorises websites by geographical area (.fr for France, .de for Germany, .it for Italy or .com for the world) or by sector (.org for NGOs, .tv for media outlets, and so on). Ultimately, a domain name becomes the digital signature of an economic, governmental, non-profit or other stakeholder.

ISSUE 1: Registering domain names. Okay, but which ones?

Virginie Brunot, a lawyer specialising in industrial property at Lexing Alain Bensoussan Avocats, is very familiar with this first step: registering a domain name to prevent it from being registered by a third party (and thereby making it unusable by you) or, worse, by someone with malicious intent who diverts web traffic to a fake site for illegal purposes. For many years, companies have therefore adopted a simple (but relatively expensive) strategy: register as many domain names as possible to limit the risks of spoofing and protect themselves.

This strategy has now become economically unsustainable following the recent flood onto the market of new domain extensions – some 1,500 worldwide. Virginie Brunot therefore recommends looking at only those domain names that are essential to the company, usually .com, .fr for a French company and possibly .tv or .media for media outlets, for example.

Once you have registered your domain name with an approved registrar, Virginie recommends keeping a close eye on any new registrations for the domain names your company chose not to register. The aim here is to find out who is behind the registration and preempt any potential risk of malicious intent if the address subsequently becomes active.

ISSUE 2: Minimising the risk of domain name spoofing

This is undoubtedly the most crucial point in managing a domain portfolio. If those domain names a company leaves available (because it considers them non-essential) should not go unmonitored, then the same is true of those domain names that are similar (to within one character, for example). The risk of becoming a victim of typosquatting is particularly high, and many fraudsters exploit this technique. Muriel Bochaton, sales director at domain registrar NameShield, says that this practice accounts for almost 15% of domain name disputes. And the consequences are not insignificant: internet users may fall victim to ransomware or have their devices infected with malware as soon as they connect to the pirate site.

The risk is even greater given that there is no requirement to check the identity of applicants wishing to register a domain name. In France, apart from "gouv.fr", which is strictly off limits to anyone outside the French state, all extensions are available to anyone. They are assigned on a "first come, first served" basis according to the rules laid down by the global internet regulatory authority, ICANN (Internet Corporation for Assigned Names and Numbers).

Even in France, AFNIC (the French Association for Internet Naming Cooperation), which is responsible for the .fr domain, has relaxed its requirements and aligned itself with the international position. Identity checks on registrants are therefore very minimal, based only on their good faith and character, often without the need to provide a contact name, postal address or phone number.

This is why it is important to choose the right registrar when registering a domain name. Most registrars are private companies with a commercial interest. Some strongly encourage their customers to register their domain names with the new extensions they create and sell, but then shirk responsibility when an attack such as cybersquatting occurs and stay conspicuously quiet.

ISSUE 3: Protecting your domain names

According to Nicolas Pawlak, who keeps a daily watch on malicious domain names on his "Red Flag Domains" website, there is one vital thing to check that is often forgotten: the domain name registration expiry date. And this is before you even think about hacking or cybersquatting attacks. If you fail to renew your registration by the deadline, the domain name is once again available to anyone. It is therefore important to carefully manage these deadlines to avoid this happening, as it could leave you with an unusable website.

If an attack is subsequently detected, a company has several courses of action to take down the offending site. In France, it can request that AFNIC initially block the site and then delete it if the offence is proven. The process takes between two and seven days depending on the complexity of the case. This is especially true since cases are not always clear-cut. For example, Nicolas Pawlak told the amusing anecdote of "mamie est chaude.fr" domain name. At the time, this set alarm bells ringing, just as "granny is hot.com" would in English. Could it be a pornographic site? In the end, the domain name was linked to the website of a baker in Versailles!

The registrar through which you registered the domain name may also be a useful ally when taking steps to deal with a proven attack.

You could also approach the hosting provider for the suspicious site, although there is no guarantee of quick resolution. Lastly, once the offending or spoofed domain name has been delisted, you can also ask for it to be transferred to you, especially if deemed essential for managing your domain name portfolio.

ISSUE 4: Committing to consistent naming and proper governance


As important as it is for a company to have meaningful and memorable domain names, it is just as important to have a consistent naming strategy for your domain name portfolio. Jérôme Guihal from the French National Cybersecurity Agency (ANSSI) laments the fact that some companies are rather lax in naming the domain names they then go on to use.

La Poste is a case in point. For its various online services, France's number one postal service has no problem registering domain names that no longer include "la poste.fr". This is the case in particular for its Colissimo services, where the domain name is completely different.

In this expert's view, this is certainly less of a risk in terms of security alone, but it can lead to confusion among users. They could think it was yet another phishing scam or fraudulent site and decide not to click on the genuine notification they received.

Companies must, therefore, put governance in place to manage their domain names. This is essential to guard against losing the use of domain names, prevent them from being pirated or spoofed, or even avoid causing confusion among users. In addition, it is important to choose the right registrar so that you have a reliable partner in all circumstances.

[READ THE ARTICLE ONLINE](#)



As important as it is for a company to have meaningful and memorable domain names, it is just as important to have a consistent naming strategy for your domain name portfolio.



hexatrust

cocktail



HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

WEDNESDAY, APRIL 5, 2023



How the war in Ukraine boosted the construction of Europe's cyberdefence

SECURITY AND STABILITY IN CYBERSPACE

XAVIER BISEUL



The return of war to Europe's borders sent shockwaves throughout the European Union. It has stepped up initiatives in recent months to boost its cyberdefence capabilities and foster better cooperation between Member States.

For the first time in modern history, a cyberwar preceded a so-called "traditional" war. In the night of 13-14 January 2022, a few weeks before Russian troops crossed into its territory, Ukraine suffered a wave of cyberattacks targeting its vital infrastructure and government sites. Since cyberspace knows no geographical borders, Russia used "wiper" attacks. This type of destructive malware caused collateral damage to European businesses and institutions.

Long before it sent tanks, the European Union came to Ukraine's aid in cyberspace at the start of the conflict. Outside its borders, it deployed its Cyber Rapid Response Team (CRRRT), which works under the Permanent Structured Cooperation (PESCO) that structures cooperation between Member States in security and defence.

A European "cyber shield" in 2024

"Ukraine has been a wake-up call for our cyberdefence," Thierry Breton said in November 2022. The European Commissioner for the Internal Market pointed out Europe's lack of sovereignty in the area. "We had to obtain resources that were not European to defend ourselves," he said.

Five months later, Thierry Breton could see the work that had been done. Before his speech to InCyber Forum 2023, he officially launched the European "cyber shield". This mechanism will be operational in early 2024 with an allocated budget of €1 billion to identify attacks more quickly and ahead of time.

It will rely on a network of five or six security operations centres (SOCs).

Allied countries must work together

The EU's cyberdefence efforts are not limited to the cyber shield. In recent months, Europe has taken a number of initiatives to try to catch up. France's Presidency of the European Union in the first half of 2022 made progress in governance. One such initiative was the creation of the European Cyber Commanders Strategic Conference (CyberCo).

More recently on 10 November, the European Commission presented the EU's cyberdefence policy and the Action Plan on Military Mobility 2.0 "to address the deteriorating security environment following Russia's aggression against Ukraine".

In addition to boosting its protective capabilities, the plan mentioned the necessary coordination effort between "national and EU cyber defence players, to increase information exchange and cooperation between military and civilian cybersecurity communities". It also plans to create an emergency fund and a reserve of cyber resources to mobilise certified service providers.

A few days later, 18 Member States, including France, launched MICNET (Military Computer Emergency Response Team Operational Network). Managed by the European Defence Agency (EDA), it aims for greater cooperation between national CERTs.

“The war in Ukraine has caused a paradigm shift”

At a round table at InCyber Forum 2023, Wiktor Staniecki, Deputy Head of Division at the European External Action Service (EEAS), stressed that cooperation between Member States and an increase in bilateral relationships between cyber diplomatic services are necessary. *“Our resilience requires exchanging information and sharing best practices.”*

He also mentioned potential cooperation with NATO, which has its Cyber Defence Centre of Excellence based in Tallinn, Estonia. In a joint statement on 10th January 2023, the EU and NATO acknowledged the need to cooperate in *“countering hybrid and cyber threats”*.

Alessandro Cignoni, head of the *“Information Superiority”* unit at the European Defence Agency, also spoke in favour of a *“unified approach in the cyber strategy”*. *“The war in Ukraine is a paradigm shift for us. Actions must be triggered more quickly. This requires long-term efforts,”* he said.

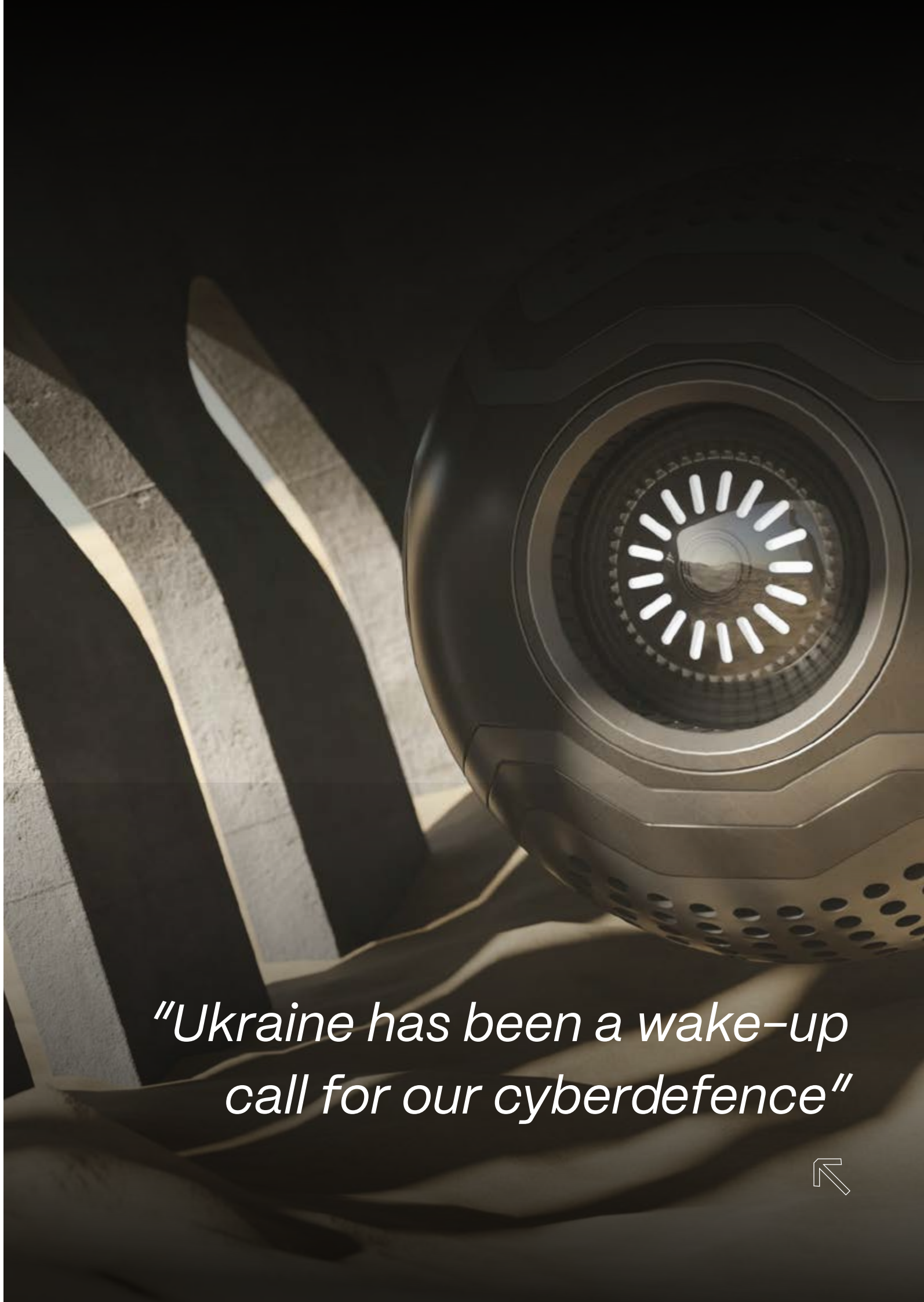
European Affairs Director at Rasmussen Global Arthur de Liedekerke agrees. *“Ukraine’s current cyber resistance hasn’t come from nowhere; it took years of preparation. EU Member States must work together to prepare themselves.”*

A stricter regulatory framework

The experts at this round table also stressed the need for private sector involvement in the (cyber) war effort. The support for Ukraine from America’s big tech companies has been widely reported in the media. The Kiev administration migrated its sensitive data to AWS and Microsoft’s cloud computing servers to ensure its activities could continue should its datacentres be destroyed. However, *“European cybersecurity companies have also helped Ukraine with donated software licences,”* said Arthur Liedekerke.

Europe’s cyber-resilience will also require a stricter regulatory framework. Unveiled on 16 December 2022, the EU’s new cybersecurity strategy mentions two new directives, one of which (revised NIS or NIS 2) aims to protect companies’ networks and IT systems more effectively. The second directive will be dedicated to the resilience of critical entities.

[READ THE ARTICLE ONLINE](#)



“Ukraine has been a wake-up call for our cyberdefence”

Username and passwords at the heart of cyber threats

CYBER RISKS

OLIVIER CIMELIÈRE



Now more than ever, hackers' activities revolve around usernames and passwords. If companies fail to remedy this vulnerability as a priority, their activities could be crippled. This is the key message to emerge from a conference at InCyber ForumEurope 2023 given by Sébastien Baron, Technical Director at cybersecurity solutions publisher CrowdStrike, and Franck Perillier, Group CISO at real estate services provider Emerica.

80% of security vulnerabilities originate from compromised user accounts, as demonstrated by two recent, convergent studies carried out by Forrester Research and telecoms operator Verizon, respectively. Hackers adopt a chain of attack in which usernames and passwords are an Achilles heel whose security requires special attention.

For Sébastien Baron, Technical Director at CrowdStrike, this combination is indeed crucial. It cannot necessarily be detected by traditional EDR solutions installed in companies' IT infrastructure to combat DDoS attacks, viruses, and ransomware. It therefore requires an entirely different approach to security.

Username black markets are prized among hackers

The CrowdStrike representative insists this point since usernames and passwords are sold by brokerage platforms on the dark web, where hackers can purchase entire leaked databases which they can then use for their own attacks. These databases generally include usernames, passwords, configuration data and session cookies, which are then used to gain undetected access to the systems of target companies.

Once this crucial information has been obtained, the tried-and-tested intrusion technique rolled out. The hacker logs into an existing account. Once inside, they can move around easily and target the Active Directory

used to store information about a domain's network resources. They can then create new user accounts with more extensive administration rights, which they can use to take over one or more of the company's IT architecture domains. In the meantime, they can also tap into the most sensitive databases.

Network complexity increases the threat level

According to CrowdStrike's 2023 Global Threat Report, 12% of intrusions are carried out using a valid account and 73% with a newly created account. For Franck Perillier, CISO at Emerica, the Active Directory is a particularly critical asset to a company's IT security. It authenticates users and allows them to access various features according to their profile and assigned authorisation levels.

The larger and more international the company, the more complex its systems architecture, with a wider variety of applications, not all of which may be up to date, and with different technologies. Such companies also have multiple actors, both internal (such as developers, maintenance staff and ordinary users) and external (including suppliers, customers and service providers).

Observing behaviour while constantly raising awareness

This multiplicity makes computer systems vulnerable, especially if hackers manage to

sneak into them. For Franck Perillier, one strategy is to analyse the behaviours of active, connected accounts in the system using tools such as the solution developed by CloudStrike, which enables the identification of suspicious accounts (especially by observing logs) and means that action can be taken before the intruder can mount a more extensive attack on the IT network and resources.

However, Emeria's expert reminds us of that cyber-hygiene also requires users to apply security rules and protocols. Humans are a random factor that can cause breaches in the system when they use weak passwords like the typical "Company-Name123" that hackers know by heart.

If raising awareness does not work, then a more coercive approach is needed. CrowdStrike's solution can also identify accounts with weak passwords and force them to be changed, denying users access to the system for as long as the vulnerability remains. Even at the heart of technology, humans continue to play a fundamental role.

[READ THE ARTICLE ONLINE](#)

Humans are a random factor that can cause breaches in the system.



CRQ: how to financially quantify cybersecurity risks

OPERATIONAL SECURITY

FABRICE DEBLOCK



At a 2023 InCyber Forum workshop, C-Risk presented the Factor Analysis Information Risk (FAIR) standard. Here is an overview of this method of quantifying cybersecurity risks and the benefits for companies.

There are several methods for assessing cybersecurity risks: not analysing the risks at all, analysing them qualitatively, or quantifying them (Cyber Risk Quantification, or CRQ).

"In companies, cybersecurity decisions – where they exist – rely on essentially qualitative analyses. These analyses are influenced by cognitive biases, mental shortcuts that help us take quick decisions in situations that we recognise or believe we have already encountered. In most cases, these intuitions, experiences and expertise can be helpful. However, in truly complex and strategic situations, they can make for poor advisors," says Christophe Forêt, co-founder and CEO of C-Risk.

To cope with this complexity, there are models that facilitate the financial quantification of cybersecurity risks, more or less accurately and easily. "These models use mathematical methods to weigh the pros and cons and look for contradictory opinions. The aim is to reach more objective, justifiable decisions that would lead to statistically comparable solutions if they were replicated by other people," says Christophe Forêt.

FAIR, a standard created by a CISO in 2005

The Factor Analysis of Information Risk (FAIR) is one such CRQ model. It is an Open Group standard devised in 2005 by Jack Jones, then CISO of insurance company Nationwide. Its taxonomy describes a menu of components that contribute to the frequency of an

event and the extent of financial losses that may be incurred if this event were to happen.

"The FAIR model uses estimated data ranges and matching levels of confidence to make use of uncertain information. It models the frequency of events, the inspections and the scale – in both impact and financial terms – of claims," says Christophe Forêt.

The model helps break down the risk into variables that can be estimated not in discrete values, but in ranges that reflect the "minimum", "most likely" and "maximum" values. Using Monte Carlo simulations, the same formula can be evaluated thousands of times using values selected from among the intervals. This generates a probabilistic distribution of the amounts of potential future losses.

"Ranges have the advantage of saying, for example, that the risk of ransomware represents between €500,000 and €4 million for a given company. It's much more specific than saying "it will cost you a lot" or "it's a red risk". This helps us correctly define what a risk is: a financial loss from an event involving an asset," says Christophe Forêt.

Many benefits for companies

One of the main benefits of this method is being able to quantify a significant number of scenarios. *"When we look at a group of risks, we start by sorting. After a few hours, we will be able to give an estimate before going further into detail depending on the use cases."*

And from the moment we realize there's a loss, we try to assess whether there could be domino effects, with both internal and external costs, and timeframes that aren't always those of solution vendors," says Christophe Forêt.

Quantification supports an insurance director who is looking to see if the coverage they have taken out reflects their true exposure to cybersecurity risks. "Sometimes, companies say they have €5 million of coverage, with a deductible of 'only' €500,000. But if we look deeper, we can see that the €5 million covers all the claims in a tax cycle, whilst the deductible is by type of loss. With quantification, we know that none of the risks, by loss category, will reach the deductible amount," says Christophe Forêt.

Another example: operational security teams working on certain protective solutions that struggle to find common ground. "Generally, for encryption, these teams may not agree on which method to use. Should they encrypt the data, the database, the operating system? What are the related costs? Going further down the taxonomy, we can provide more comprehensive analyses to guide decision-makers. In some large companies, this can represent millions of euros of investment," says Christophe Forêt.

[READ THE ARTICLE ONLINE](#)

From the moment we realize there's a loss, we try to assess whether there could be domino effects, with both internal and external costs, and timeframes that aren't always those of solution vendors.



cyberleaders gala



CYBER+LEADERS
THE STRATEGIC CYBERSECURITY REVIEW

THURSDAY APRIL 6, 2023



An obstacle course for Europe's sovereign Cloud

DIGITAL SOVEREIGNTY

STANISLAS TARNOWSKI

Despite formidable progress, the European Cloud seems to be struggling in the face of American Big Tech's overwhelming dominance. The analysis by regulators and cloud and cybersecurity professionals during a roundtable at InCyber Forum 2023 did little to dispel this impression. Is a storm on the horizon for the European cloud?

Despite the optimism and willingness displayed by public and private European sovereign Cloud players, there is still many a slip 'twixt cup and lip for this highly strategic project. This is what emerged from the "Towards a European alternative to US Cloud standards?" roundtable held at InCyber Forum 2023 in Lille.

The assessment made by Solange Viegas Dos Reis, head of legal at OVHcloud, was unequivocal: "In 2017, the share of European players in the European Cloud market was 27%. Five years and a market boom later, the same European players represent only 13%." Americans are head and shoulders above their European competitors in terms of market share and technology.

And the challenges are not just commercial, as explained Hugues Foulon, CEO of Orange Cyberdefense. "One of the main issues for some of our customers is extraterritoriality, as it relates to the Cloud Act and the Patriot Act. It is our duty at Orange not to be naive, to convey the consequences of choices, whatever they may be."

US legal extraterritoriality? It means you are subject to US jurisdiction upon using American goods or services, whether it's a measly dollar or a Gmail address. A direct consequence is that any US company Cloud user falls under American law and the confidentiality of his data is no longer guaranteed.

Let's "not be naive" in the face of challenges from the Cloud

"We're talking about data protection and its significance, but let's not forget the right to privacy. And privacy does not only extend to individuals residing in the European Union, but also to legal persons, such as corporations," explained Peter Sund, the CEO of FISC (Finnish Information Security Cluster, the Finnish cybersecurity interbranch organization).

The Cloud in Europe? A market totally dominated by sometimes intrusive foreign players, whose governments can claim the right to access the data of any citizen or business; the opposite of a "trustworthy Cloud". A very French expression emphasized Rayna Stamboliyska, uncertainty management specialist for RS Strategy, who was hosting the round table. She then asked speakers "what trust in the Cloud means, and how they implement it on a daily basis in technical, technological and operational terms."

"This comes down to the fact that the user has freedom of choice thanks to technological interoperability and reversibility. Moreover, data will be protected and will not be used for purposes other than those he has specified," answered Solange Viegas Dos Reis.

Hugues Foulon subscribed to these operational principles, pleading for “pragmatic solutions that make it possible to move forward and gain strategic autonomy. And that’s what we did with ‘Bleu.’” This joint venture between Orange and Capgemini, in partnership with Microsoft, will be operational in 2024 and aim to provide a “trustworthy” and “sovereign” Cloud to public and private players in search of the highest level of security and privacy.

“Schrems II”, Cloud players backed into a corner

The solution has *“the advantage of being compliant by design. This was the only way to be compliant with the GDPR,”* underlined Bertrand Pailhès, head of IT and innovation at the CNIL (French data protection authority). Indeed the technical aspect alone is not enough; a legal and regulatory framework is also essential in guaranteeing trust in the Cloud. And in this regard the EU seems to have grabbed the bull by the horns. *“Europe has included a fairly strong principle everyone agrees on, I think, which is that the protection of Europeans’ data must be guaranteed everywhere, at all times,”* said Bertrand Pailhès with satisfaction. The GDPR, which is very protective of personal data, is thus elevated to the rank of a de facto standard which the rest of the world should follow.

This was the sentiment behind the “Schrems II” decision, which the Court of Justice of the European Union (CJEU) rendered on July 16, 2020. Considering personal data protection in the United States wasn’t up to snuff, the CJEU voided the “Privacy Shield”, the data transfer system set up between Washington and Brussels. The problem is that nothing was agreed upon to replace it and that the market is not ready, according to the head of IT and innovation at the CNIL.

“The CJEU’s decision will come into force on July 17. Starting tomorrow, it will be forbidden to transfer data to the United States. There is no transitional period,” lamented Bertrand Pailhès at FIC.

“Sometimes it’s completely unrealistic to think that because a judge in Luxemburg has decided the market wasn’t compliant with basic rights, everyone will immediately agree and get up to speed,” he added. And in this case, the regulator must be flexible until enough *“alternative solutions (sic) come about.”*

Legislative wheeling and dealing

European legislature is thus full of good intentions, but they sometimes clash with reality... Unless they are *“regulatory issues that are in some way complete opposites of one another,”* pointed out Peter Sund, for whom “it is always difficult to strike a balance” between contradictory objectives. Thus, the protection of personal data may seem at odds with the powers granted to authorities and courts to investigate. He used the example of the series of measures called “a better internet for children”, designed to combat child sexual abuse material.

To do so, the European Commission enables authorities to access images and other material hosted by online service providers, in particular encrypted messaging services. This measure renders useless data encryption, which security in the Cloud relies heavily on. *“This runs the risk of spreading confusion and fostering a situation that goes against the Cloud’s objectives,”* worried Peter Sund, while acknowledging the importance of the fight against child sexual abuse.

According to Bertrand Pailhès, the United States relied on solid legislation to develop the Cloud: *“It was launched ten years ago and is now exhaustive, the industry is highly regulated, and this has in fact allowed the American Cloud ecosystem to grow, as there were clear rules about what was expected of it.”*

“Europe must breed champions”

This favorable framework is just one of the expressions of strong political will, agreed Solange Viegas Dos Reis: *“when we look at American or Chinese Cloud leaders today, we realize that they solidified their position on their domestic markets thanks to strong government support, with public contracts, and funding and research grants.”*

This willpower was long lacking this side of the Atlantic, insofar as the Commission’s liberal principles (no market intervention) held strong. This could change however: *“we support the ‘Buy European Act’, which would provide for tangible, financial support, and give all Cloud players the necessary means to grow,”* further stated Solange Viegas Dos Reis.

It is indeed time to shake things up, deemed the CEO of Orange Cyberdefense France. *“Europe must breed champions in this area,”* pleaded Hugues Foulon, who also emphasized that we shouldn’t stop here. The Cloud is not just about datacenters, it also entails rapidly evolving software solutions, cybersecurity, maintenance, in short, an entire environment. And according to him, *“Europe is not fully aware of the scale of the training required.”* The EU still lacks developers and experts of all sorts. Without these skills, *“it will be difficult to operate a strategically autonomous system.”*

“We’re going to have a hard time creating an ecosystem as high-performance as those of market leaders, from scratch. I think it is more a matter of decades,” warned Hugues Foulon, who argued for a practical approach, just like with the partnership between “Bleu” and Microsoft. Will it even be possible to one day do without American Big Tech? European professionals want to believe so.

[READ THE ARTICLE ONLINE](#)



Europe is not fully aware of the scale of the training required.

Cloud : Is Europe Falling Behind?

DIGITAL SOVEREIGNTY

MARC AUXENFANTS



To successfully transform in the face of its competitors, the EU must come together, build a shared ecosystem and shore up its resilience and regulations. But above all, it must believe in its strengths, talents and skills.

"Enormous financial stakes, a long-term view of investments and profitability, being fiercely determined to succeed and always striving for operational excellence." For John Dinsdale, chief analyst at American research and studies group Synergy Research, these are the conditions required of aspiring leaders in the global cloud computing market. However, "no European company comes close to fulfilling all these criteria, and the six leaders are all American companies," he notes.

Amazon, Microsoft and Google now combine to make up 72% of the EU cloud computing market, currently worth €10.4 billion. However, their main European competitors, such as OVHcloud and Orange, each only take 2% of the pie.

Given this, what challenges should Europe address? What solutions should it put forward to overcome its weaknesses? Jean-Claude Laroche, President of Cigref, explains this shortcoming by the European companies' lack of presence in the cloud computing market. "Our situation is: we are dependent on American hyperscalers, which is detrimental however you look at it, whether in terms of protecting data and processing, in terms of finance or in our business relationships with these players. The challenge is to have our own industrial champions!" he says.

"There is no time to waste!"

However, for Michel Paulin, head of OVHcloud, the weakness is not just technological. *"If we look at all the ecosystems of European players in cybersecurity, cloud computing and software, today we have all the building blocks we need for champions, but we do not have players as big as the Chinese and the Americans, players that can become one-stop shops offering a complete range of solutions."*

Can Europe still become a major player in cloud computing? For Thierry Breton, European Commissioner for the Internal Market, the solution first requires resilience. *"While we are building an internal market of industrial data, cloud computing is a matter of digital and industrial sovereignty. More than ever, Europe must ensure the development of a secure, trusted digital space. For this, we need innovative but secure data management systems. Our systemic rival partners are investing massively. There is no time to waste!"*

American hyperscalers' monopoly also raises the issue of transparency between cloud computing providers and customers, says Shahmeer Amir, a Pakistani ethical hacker.

In response to this, he suggests that the EU require strong, clear transparency with solid data protection regulations, especially for cloud computing environments. *"These legal frameworks would guarantee that all this cloud infrastructure is monitored, that it will be able to securely solve these problems,"* he says.

"Europe must be strategic"

To ensure that intellectual property and sensitive information is effectively and securely protected, Shahmeer Amir recommends a European policy that promotes smart, healthy diversity and competition between cloud computing providers. *"Monopoly implies a lack of transparency. And when there is a lack of transparency, sensitive data and information can be hacked or leaked."*

For Jean-Claude Laroche, a pan-European trusted cloud is necessary. It must fulfil four basic requirements: *"it balances the relationship between the service provider, transparency, portability of solutions and interoperability; there are secure cybersecurity solutions; there are solutions that address social and environmental problems while mastering the environmental aspect of digital technology in the cloud; it protects against interference from non-European intelligence services"*.

These requirements are listed in the standards developed by Cigref and included in France's SecNumCloud certification. *"Now, we want there to be equivalent requirements at the European level. It's absolutely essential if we want a trusted European cloud provider with a high level of certification and to be protected against extra-territoriality,"* says Jean-Claude Laroche.

For Michel Paulin, European requirements in traceability and transparency, such as EUCS and the Digital Market Act, give European operators a competitive advantage that benefits customers. Furthermore, Europe is clearly the leader when it comes to data protection.

Nevertheless, how can we create a shared ecosystem that can rival those from China, the United States, South Korea and Israel? *"These countries supported champions with strategic government that set a long-term ambition with regulations, certification and funding for support. In all these areas, Europe must be strategic,"* he says.

He also says that there must be financing. *"Without a Nasdaq, we must help companies obtain their own funds and lines of financing in order to grow. The IPCEIs (Important Projects of Common European Interest) are one of the mechanisms to achieve this."* We must also expand public contracts and private contracts from large companies to build this European ecosystem, boost research and development through public-private exchanges like those at Stanford, Harvard and MIT, and resolve the shortage of talent.

"We don't have enough engineers in Europe. So, instead of spreading our subsidies too thin, we should reinvest in universities to train more engineers and PhD students who will want to stay in Europe," says Michel Paulin.

"The war is not lost"

For Shahmeer Amir, raising awareness among people, users, companies and the government is fundamental. *"We often think that we know, but we don't. Also, it's always a good idea to get together, ask questions, listen and then gather and combine all these needs and expectations into a verified policy recognised by at least 90% of people, which will then be applied."*

"Europe needs to pull itself together. It's an absolute necessity. There needs to be a real strategy and industrial policy at the European level. We need to set priorities and keep to them!" says Jean-Claude Laroche. For Alain Issarni, CEO of NumSpot, however, the war is not lost. *"There are fatalists, and there are those who do not believe it to be lost: we should target the latter!"*

He suggests starting small and with great ambition. *"Does Europe want to start a cloud computing revolution? I hope so. Can it do it? Definitely yes. Can it avoid it? No. Therefore, we need to develop credible alternatives in cloud computing and be a part of this revolution. Otherwise, we will be left behind!"*

[READ THE ARTICLE ONLINE](#)



While we are building an internal market of industrial data, cloud computing is a matter of digital and industrial sovereignty.

EUROPEAN CYBER CUP

25 teams 250 players 6 challenges



APRIL 5 & 6, 2023



In the face of cybersecurity threats, Europe is getting organised, says Thierry Breton

DIGITAL SOVEREIGNTY

FABRICE DEBLOCK



At InCyber Forum2023, the European Commissioner for the Internal Market spoke at a plenary session. He detailed all the measures taken since he took up his role three years ago.

Thierry Breton began his speech by reminding us that cybersecurity issues can no longer be addressed by Member States on their own—they must be handled at the European level.

He also highlighted the fact that the “European internal digital market” was the leading market in the free, democratic world: “This internal digital market is now structured by an organisation and regulations such as the DSA, the DMA and the Data Act. For the first time, we have a single market for data that operates with the same rules for everyone.”

For Thierry Breton, the industrial data revolution will be a much bigger wave than that seen in personal data. “This will generate a much bigger volume of data that will be the basis for changes to come, bringing new jobs and services,” he said. But in this field, we are only as strong as our weakest link. Our cyber-resilience must become an issue for Europe as a whole.

“The European Union, as a political and economic player as well as a player in global security, is becoming a growing target for all kinds of cyberattacks, with—for those behind these attacks—the goal of destabilising our systems,” Thierry Breton said.

Cyberspace is now an integral part of Europe’s defence doctrine

The Commissioner for the Internal Market also said that cybersecurity was now recognised as a contested space in the new European defence doctrine, just like maritime space

and outer space. Like any contested space, we must all work together to protect it.

“This is a major paradigm shift. Cyberspace is now a part of our defence doctrine. To better handle cyber threats, we need cutting edge technologies, secure shared infrastructure, improved operational cooperation and structures of governance and effective sanctions,” he said.

This is the context behind Thierry Breton’s goal to establish a European shield to protect, detect, deter and defend.

Technology and regulation: the two pillars of protection

The “protection” aspect revolves around a clear aim to improve the European internal digital market’s resilience and security through an ambitious approach to technology and regulation. “In terms of technology, we are working to roll out a clear roadmap to identify our cybersecurity dependencies and to concentrate national European funding, notably through the European Defence Fund,” said Thierry Breton.

On the regulatory side, the NIS Directive introduced cybersecurity requirements for all key economic players in critical sectors, including data centres and public administrations.

Another key regulatory component is the “Cyber Resilience Act” proposed by Thierry Breton in November 2022. “This bill lays out minimum cybersecurity requirements for all products and software sold within the internal market.

Self-certifications of compliance will be possible for 90% of products. But for thirty or so of the most critical products, such as industrial firewalls, routers and operating systems, we have set up a compliance test that will be carried out by third parties," the European Commissioner said.

Increased detection and defence

With regard to detection, Thierry Breton reiterated the aim of drastically reducing the time taken to detect an attack, so that in the long term it will only take a few hours and not several months, like the current average of 190 days for sophisticated attacks.

In this regard, the European Commission proposed a "Cyber Solidarity Act" last April. This text provides for an infrastructure of six or seven SOCs (Security Operations Centres) to be set up to create a global detection system at the European level. *"In terms of governance, this "cyber shield" will be a bit like a cyber version of our Galileo satellite connectivity and positioning architecture,"* he said.

Regarding "Defence", Thierry Breton recalled the importance of the "cyber emergency mechanism" which will also be covered in the Cyber Solidarity Act. This mechanism will be based on the principles of joint crisis management and mutual assistance. It draws inspiration from how European civil protection works in a spirit of solidarity to provide assistance in the event of a major disaster in an EU country, such as a fire or earthquake.

"It is a response branch that will rely on a pool of several thousand responders to mobilise certified, trusted, volunteer public and private service providers to support defence and mobilisation efforts in the face of an attack. This reserve will stand ready to respond upon request from any Member State," he said.

An active policy of direct sanctions for better deterrence

Finally, to become a credible global player in the continent's cybersecurity, or even cyberdefence, Europe must devise a genuine doctrine on cyberattacks and cyberdefence. *"The aim is to increase Europe's cyber deterrence capabilities. There can be no cyberdefence without deterrence. This doctrine must come with an active policy of direct sanctions. The EU already has a cyber diplomacy that allows it to impose tough sanctions, especially when there is strong evidence for who is responsible,"* said Thierry Breton.

The European Commissioner for the Internal Market concluded, *"However, to be credible, any deterrence must be supported by a genuine strategy on active, i.e., offensive, response capabilities, which remain in the hands of the Member States. We have committed considerable resources, for example in the European Defence Fund, to intervene upstream and help Member States finance key technologies."*

In the face of threats, Europe is organising its technology regulations of its shared infrastructure and solidarity to improve its defence and deterrence capabilities. This approach involves all Member States as well as its NATO allies, the first of which is the United States.

[READ THE ARTICLE ONLINE](#)



*There can be no
cyberdefence without
deterrence.*

Trust in Digital Technology: “We Can’t Believe What We See Anymore”

DIGITAL TRANSITION

FABRICE DEBLOCK

Social networks, AI, big data: digital technology has upended social structures and undermined what holds them together: trust. How can we redefine it? To answer this question at an InCyber Forum plenary session, Jean-Gabriel Ganascia, Michel Bauwens and Éric Salobir referred to history, philosophy, sociology and their digital expertise.

When three intellectuals tackle the topic of trust in the digital world, the outcome opens up dizzying perspectives. For those who were unable to attend the two-hour plenary session at InCyber Forum 2023 devoted to this issue, InCyber is pleased to offer you a quick synopsis. We give the floor over to Jean-Gabriel Ganascia, professor at the Sorbonne and president of the CNRS ethics committee, Michel Bauwens, computer scientist and cyberphilosopher, and Éric Salobir, priest and founder of the OPTIC network, which promotes technology for the benefit of humanity and the common good.

Jean-Gabriel Ganascia: Do trust and digital technology go together? This is ambiguous; it can mean “can digital technology absorb trust?” So, is there more trust, or does it mean we want to create digital technology we can trust? Careful, trust does not mean fidelity and neither is it proof: when you trust someone, you risk being wrong. There are several types of trust. There is trust in

individuals, there is trust in institutions, and then there is trust in machines.

Éric Salobir: Indeed, and the whole challenge with trust in digital technology is creating the conditions for trust in things that we cannot see, whereas by definition, we always tend to trust what we see. With generative AI, for example, we are now saying, “I can’t believe my eyes” and in fact, we cannot believe our eyes anymore. Digital technology has completely upended the conditions for trust.

Michel Bauwens: As society has become more complex, people have lost their ability to trust those around them, their direct acquaintances, the famous Dunbar’s number.

Distributed trust with the blockchain

Today, we are in a different sort of peer-to-peer environment: we must coordinate non-locally. We have to trust people with

whom we share a project or belief, but who are not nearby. So, we are forced to connect with our peers via proprietary platforms for whom we are more or less livestock for data extraction. This is fundamental. There is no institution representing this new sociology. Our institutions are essentially geographical, such as the nation-state.

É. S.: The question is why these business models have emerged. Ultimately, we did not want to be customers, so we became a product. And the question is, “how will we think about these new business models?”

J-G. G.: In ancient times, trust was based on one’s word, and a witness was worth more than writing. As groups expanded, writing became more important. Now, the major transformation is that it will be machines. With blockchain, for example, there will be new types of trust, and this trust will be distributed since it will no longer rely on trusted third parties, an institution, a central bank for currency, or a government.

É. S.: What is disturbing is that this trust in machines comes at the expense of trusting people: “trust the blockchain so you no longer have to trust your neighbours”.

ChatGPT, the avatar of the “golden calf”?

The trust we had in fiat currency, from “fides” or faith, was both trust in the person and trust in the economy, in the group. All of this is disappearing in a rather Hobbesian perspective: if man is wolf to man, then I prefer the blockchain.

How will we build a society on this type of technology? How will we benefit from these technologies? I don’t want to get to a point where smart contracts end up killing the social contract.

J-G. G.: When I was talking about the blockchain, it wasn’t about trust in the machine, but trust through the machine. Trust in the machine, that’s ChatGPT, which is seen as an oracle. It has a special status, like divination. When you say, “I asked ChatGPT”, that’s exactly what we mean.

É. S.: Yes, we anthropomorphise this machine by asking it questions. It appears to be endowed with speech, with a discrepancy between its formal perfection – it speaks well, gives the impression of being well-argued – and its complete lack of common sense. ChatGPT can say any number of things, it’s a gasbag, but that’s not a problem. People put their trust in AI in the same way that the people made the golden calf their god in the Hebrew tradition. The goldsmiths didn’t make it an idol, the people did. Are we all building the same relationship with technology?

“Capitalist” American tech firms

M. B.: to avoid this, we need to build new institutions that reflect this virtual reality. These are actually being created in the open source community, such as the FLOSS Foundations, which manage collective infrastructure in a non-territorial and often democratic way. One example I can think of is the Linux Foundation. I call these magistrates of the commons. This could also apply to data, with data trusts, data commons and data cooperatives, to partially escape those “capitalist” American tech giants that capture our attention and our data.

É. S.: We are indeed witnessing an impoverishment of pre-existing institutions while new ones are struggling to be established. These foundations are great, but unfortunately, they are too marginal. To create new trusted third parties, I think we need three characteristics. The first is independence, including financial independence, which open foundations lack.

The second is transparency, where experts can verify algorithms, ChatGPT metaprompts and how our data is used. Thirdly, this governance needs to be participative. And here, I greatly agree with you. The problem is that the scale is global. There will not be one, but many trusted third parties. The question is, *“what architecture do we need so they can all talk to each other?”*

Social media and mob psychology

J-G. G.: These pillars that you have listed seem perfectly essential to me. Trust is being completely rewritten in our digital societies, and it is up to us to redefine all these criteria. You talked about data. The challenge is that it can be duplicated and falsified. So, we need to think about the processes that we are going to put in place so that we can rebuild trust independently of its very fluid nature.

M. B.: Beyond these issues, I think we need to introduce the notion of online civility, because the online world is very fragmented. Everyone is in their own little tribe of affinities that has access to different information. Each community is battling against the information coming from another tribe. You can't create a society with this attitude.

J-G. G.: We do have communities, but no longer in the old sense, i.e., communities of people condemned by fate to live in the same place, with a duty of solidarity. Today, these online communities are communities of interest. The problem is collective deliberation. Within these groups, we can see concepts from mob psychology in action, as per Gustave Le Bon and Freud. In a mob or on social media, people become sensitive, aggressive, or get excited about nothing. There is no longer one public space, but spaces that are somewhere between public and private.

Covid-19, a “painful” crisis of trust for scientists

É. S.: We have gone from a world of received identity (*“I am so-and-so, son of so-and-so”*) to a world of chosen identity and multi-identities. Everyone is forging their own paths. While this gives us a lot of freedom, it happens a bit by force and contributes to this rather agitated, violent dimension of the public space.

J-G. G.: We could see this during the Covid crisis, when trust withered away, and it was particularly painful for us scientists at the time. By nature, scientists have doubt, but here we were faced with the wider public who made scientists hostages to their own doubts. They said that if we couldn't say for sure, that meant we had no idea, etc.

M. B.: I don't want to be too negative, but we have entered an era of digital surveillance. When I am on Facebook, I feel a bit like I'm in China, where you can't even share scientific articles, they're filtered.

On the one hand, there is the “monotheistic” media in the sense that they follow a dominant narrative, and online, algorithm controls work against you. Even if we get the impression of fragmentation, we are really having trouble getting the word out. And the danger, of course, is where there is no speech, there is violence. Will we end up like the Romans with a breakdown of our structures, or will it be like the 16th century, where we found a capital solution in the nation-state?

“Monotheist” medias versus a “fragmented” Internet

J-G. G.: Besides this fragmentation by groups within societies, digital technology also brings out divisions between cultural zones. For example, I participated

in UNESCO's ethics committee when it was setting up its ethics on artificial intelligence. I read a certain number of charters, and I can tell you that how Europeans see it is not how the Americans or the Chinese do.

É. S.: Exactly. For the Chinese, chaos is the absolute evil. It's not dictatorship, and that says a lot about their social organisation. The Americans have a very consequentialist view. Basically, as long as there's no class action, everything's fine. In Europe, we apply Kant's principle where *“your maxim should become a universal law”*, i.e., if you do something, you should want everyone to do the same.

M. B.: Even the technological system is being divided in two. Huawei can no longer invest here, and the Americans have a law that punishes Americans with up to fifteen years of prison for working for Chinese microchip companies. Even the Internet is breaking up.

Trust in digital technology needs to be reinvented at the regional and national levels, so at the global level it seems very hypothetical.

[READ THE ARTICLE ONLINE](#)

Each community is battling against the information coming from another tribe. You can't create a society with this attitude.





barometers & panoramas

Panorama of cyber innovation

2023 INCYBER FORUM STARTUP AWARD

The information presented in this panorama was collected from the 81 companies that applied for the award. The award is organised in partnership with Atos and with the support of ECSO. Each year, it rewards the most innovative companies in the field of cybersecurity.



Candidates by segment



Trends

65% of first-time applicants

+88% participation since 2019

3/4 of the applicants had growth of more than 20% in 2022

71% of them have already completed at least one round of financing

57% plan to raise funds within six months

56% of companies have fewer than 10 employees

83% of the offered solutions are SaaS/Cloud compatible

The information presented here covers the main lessons learned from this panorama. To view the document in full, visit incyber.org, the InCyber Forum community media.

THE NUMBER OF BREACHES REMAINS AT A HIGH LEVEL

VARIATION IN THE NUMBER OF BREACHES



Key figures

+35 % DPO
(data protection officers)

i.e. **17,432**
people appointed
to this key function

-3,11 %

decrease in recorded notifications

This stabilisation can be credited to **organisations maturing** in terms of cybersecurity.



x2

number of breaches

between 2019 and 2021

After a very sharp increase in the number of breaches between 2019 and 2021, there was a slight decrease in notifications recorded over the last year.

Focus

After a very sharp increase in the number of breaches between 2019 and 2021, there was a slight decrease in notifications recorded (-3.11%) over the last year. This stabilisation can be credited to organisations maturing in terms of cybersecurity.

Media coverage of a growing number of cyberattacks with ransomware affecting not only private companies of all sizes but also hospitals and local authorities saw awareness grow faster among executives. Organisations increased the budget dedicated to cybersecurity and boosted their levels of defence.

Protective measures did not focus solely on investments in software and hardware. Personal data confidentiality policy is increasingly being backed up with fresh appointments. The number of data protection officers (DPO) increased by 35% in one year with 17,432 people appointed to this key function. As a reminder, the GDPR makes it mandatory to appoint a DPO for public organisations and private businesses carrying out large-scale sensitive data processing (article 37).

In spite of these encouraging signs, the number of breaches remains at a particularly high level. With the sanitary crisis, the level of threat went up a notch, as cybercriminals made the most of the vulnerabilities caused by both the disorganisation of businesses and the widespread adoption of remote working. The number of breaches more than doubled between 2019 and 2021. This pressure does not seem to have fallen since.

The potential consequences of a data leak are varied. The first risk is the illegitimate use of exfiltrated data. This type of fraud can take varied and uncontrolled forms.

CNIL indeed reiterates that in the event of a data leak “liable to cause a high risk for rights and liberties”, the organisation liable has “the obligation to individually inform the data subjects of the fact that their data has been compromised and published online”.

A data breach can destabilise the organisation of a business and partially or totally paralyse its activity. This causes a reduction in productivity and, de facto, a financial loss. An organisation that falls victim to ransomware is also not guaranteed to recover the entirety of its information system.

Furthermore, disclosure of a data leak harms the reputation of a business and can have a lasting effect on the trust placed in it.

DATA BREACH BAROMETER



This barometer is coordinated by the Cyberleaders strategic review in partnership with Bessé and Almond and with the participation of CNIL.



There was nothing exceptional about 2021. Though there was a slight decrease in the number of personal data breaches notified to CNIL (-3.11%) last year, it remained at a particularly high level. After making the most of the disorganisation of both businesses and public organisations during the health crisis, cybercriminals are continuing to pose a constant threat with wave after wave of increasingly sophisticated campaigns.

For the organisations that fall victim to a data breach, there's nothing insignificant about it. They can have more or less serious financial, operational, reputational, legal and/or regulatory consequences. Based on the data published by CNIL, this barometer is designed to assess the issue and its consequences.

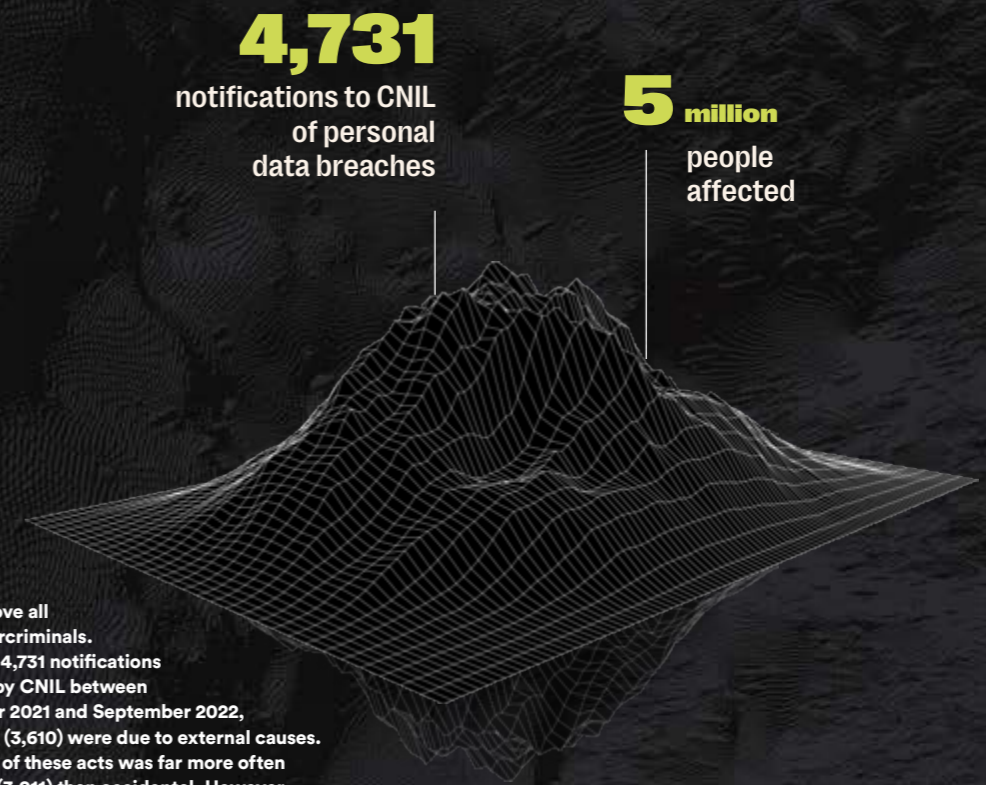
2022, A NEW RECORD YEAR

[ANALYSIS OF GLOBAL TRENDS]

With nearly 13 data breaches per day and 4,371 incident notifications received by CNIL last year, 2022 was a new record year. Overall, these personal data breaches affected a very large number of individuals in France. Based on the average number of people affected per breach, it can be estimated that approximately five million French people were affected in 2022. Though this method is far from scientific, it demonstrates the scale of the issue.

As a reminder, according to article 4.12 of the GDPR a personal data breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted".

The GDPR has also introduced a notification obligation for data controllers in the event of a data breach. They must alert CNIL as quickly as possible, if possible within 72 hours of learning of the breach. Failure to meet this obligation can result in a fine of up to €10 million, or 2% of the business's global annual sales revenue.



The threat comes above all from cybercriminals. Out of the 4,731 notifications recorded by CNIL between September 2021 and September 2022, two-thirds (3,610) were due to external causes. The origin of these acts was far more often malicious (3,011) than accidental. However, the proportions were the other way round for the 1,049 breaches of internal origin at an organisation. The causes of these internal acts were mainly of accidental (842) rather than malicious origin (207).

This data confirms, in absolute figures, that cybercriminality is mainly the doing of individuals external to an organisation. This is an increasing issue as, in one year, the number of malicious acts of external origin increased by 10.6%. Malicious acts of internal origin increased by an equivalent proportion (+11.89%). This must make organisations question the processes to be implemented to counter these "enemies within".

Regarding internal acts of accidental origin, it is legitimate to think that the widespread adoption of remote working since the COVID-19 pandemic has accentuated risk factors.

At home, employees' devices do not have the same level of protection as in the office.

Remote working also reduces the level of alertness. Sitting on their own in front of their screen and without the benefit of sound advice from colleagues located on the same premises, employees more easily fall prey to phishing campaigns.

However, the number of leaks "of unknown origin" fell by 49% in one year. As we prepare to celebrate five years of the implementation of the GDPR next May, businesses and administrative authorities have visibly matured. Over the years, they have progressively put in place tools to track the origin of incidents.



SECTORS PARTICULARLY AFFECTED

VARIATION IN THE NUMBER OF BREACHES

Key figures



The administrative and support service sector

accounted for

30 %

of total data breaches

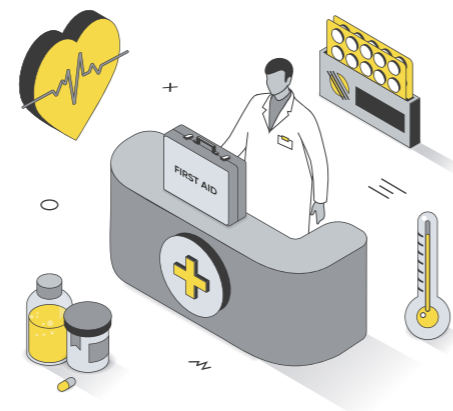
next came

overseas activities

(embassies, consulates, international institutions), accounting for

10 %

of data breaches



Ransomware particularly affected

regional authorities

23 %

and

public healthcare facilities

10 %

Source: ANSSI

Focus



One business sector accounted on its own for nearly 30% of total personal data breaches: the administrative and support service sector. This INSEE NAF code (i.e. French National Institute of Statistics and Economic Studies' acronym referring to business sector identification code) covers activities relating to rental, travel, employment, safety and more generally business service companies.

Next, around and under the 10% bar, came overseas activities - i.e. embassies, consulates, and international institutions -, followed by financial institutions, insurance companies, real estate professionals, and law, accounting and architectural firms, as well as scientific and technical activities.

Public organisations, which are spread across different business sectors, are particularly exposed. In its "2022 cyberthreat panorama", ANSSI (i.e. French National Cybersecurity Agency) underlined that ransomware particularly affects regional authorities (23%) and public healthcare facilities (10%)

The list of public organisations that have fallen victim to cybercriminals is long. The most recent cases covered by the media include the Versailles and Corbeil-Essonnes hospital centres, the Beuzeville residential care home, Brunoy and Chaville town halls, and the Seine-et-Marne and Alpes-Maritimes departmental councils.

What do these private businesses and public organisations have in common? They are a step ahead in terms of their digital transformation. The down side of this is that the widespread digitisation of their processes inevitably increases their exposure to data breach risks.

On the contrary, only marginally digitised activities such as construction, hotels & catering, and the manufacturing industry only fell victim to a low number of breaches. N.B. the order of the ranking did not change between 2021 and 2022. The administrative and support service activities sector even consolidated its first place with a 34% increase in one year.



InCyber Forum

in key figures



INCYBER FORUM 2023

20 000	attendees including
+16 000	unique attendees on site (+10,7%)
4 000	online participants
2 700	internationals
650	private and public partners
530	speakers
+1 800	business meetings via the networking platform
82	represented countries
11	minutes: average online viewing time (+22%)
+700 000	views on InCyber Forum social network accounts and 50 millions impressions on the topic



thanks

to our 650 partners!

MAIN PARTNERS

H E X A T R U S T
CLOUD CONFIDENCE & CYBERSECURITY

DIAMOND PARTNERS

EVIDEN THALES

PLATINIUM PARTNERS

AIRBUS  **BRETAGNE**
LA CYBERSECURITE A SON TERRITOIRE  **CROWDSTRIKE**

DARKTRACE  **EXCLUSIVE NETWORKS** **Orange Cyberdefense** 

   **sopra steria** **<TEHRIS>**

GOLD PARTNERS

abbakan  **.AGORIA**  **aws** **BITSIGHT**  **CAMPUS CYBER**

    **EGERIE** **EURATECHNOLOGIES** **FLANDRIN TECHNOLOGIES** **FORTINET**

FORTRA    **kaspersky**  **neoVAD** **OneTrust**

opentext    **GrandEst**   **CYBERKOCC** **SANS**

Schneider Electric  **TANIUM**  **tenable**  **txOne**

photos credits

Adam Jicha
Adrien Vin
Cash Macanaya
Christian Lue
Daniel Lincoln
Efe Kurnaz
FLY:D
Hesam Link
Kristaps AoM3
Maximalfocus
Nathan Watson
Nick Brunner
Romuald Charpentier
Shubham Dhage
Timon Studler

Security is a game

**THE INTERNATIONAL
CYBERSECURITY FORUM**

BECOMES

