CAHIERS IN CYBER

RÉTROSPECTIVE 2024

Ready for AI ?

Réinventer la cybersécurité
à l'ère de l'IA

sommaire

ÉDITO 03

TENDANCES 04

TEMPS FORTS 06

SCÉNARIOS PROSCEPTIFS *EN ANGLAIS UNIQUEMENT* 14

REVUE DE PRESSE 44

BAROMÈTRES 94

FUITES DE DONNÉES 96

PANORAMA DE L'INNOVATION 102

BAROMÈTRE DE L'INVESTISSEMENT 110

FORUM INCYBER 2024 : CHIFFRES-CLÉS 118

REMERCIEMENTS PARTENAIRES 120

édito

Entre fantasme dystopique et techno-béatitude, difficile de savoir où l'intelligence artificielle (IA) va mener l'Humanité.

Une chose est sûre : rien ne sera plus comme avant.

Nos activités professionnelles, nos vies personnelles, nos façons de penser, de décider, d'agir, de consommer, de produire, de nous soigner vont s'en trouver durablement bouleversées. Mais le monde de demain dépendra surtout de ce que nous allons collectivement décider de faire – ou de ne pas faire – avec l'intelligence artificielle et de la « confiance » que nous arriverons à construire « dans » et « par » ces technologies.

Pour être « de confiance », les IA devront, selon la Commission européenne, respecter 7 principes, parmi lesquels la robustesse technique et la sécurité, le respect de la vie privée et la gouvernance des données. La généralisation de ces technologies va en effet introduire des risques nouveaux en raison non seulement de l'augmentation de la surface d'attaque mais aussi de leurs vulnérabilités intrinsèques (attaques par empoisonnement, attaques adverses…).

Le progrès technologique étant ambivalent par nature, les IA sont également utilisées par les attaquants tout au long de la *kill chain* pour reconnaître une cible, contourner les mécanismes de protection, construire des *deepfake*, automatiser une attaque etc.

Le premier défi est donc de sécuriser les intelligences artificielles mais aussi les données qu'elles ingèrent et produisent. Données et intelligence artificielle sont en effet indissociables. Et les chiffres donnent le vertige : chaque seconde, ce sont 7 mégabytes de données qui sont créées pour chaque personne, avec pour conséquence une quantité globale de données qui atteindra 181 zettaoctets en 2025 contre 2 zettaoctets en 2010.

Heureusement, l'IA révolutionne aussi « l'art » de la cybersécurité en nous permettant d'améliorer nos capacités d'authentification, de sécurisation des données, de détection des menaces, d'analyse de code, d'orchestration, de réponse à incident etc. Un bond technologique qui doit aussi nous conduire à réinventer en profondeur nos doctrines, nos organisations, nos compétences, pour qu'elles soient « *AI - ready* ».

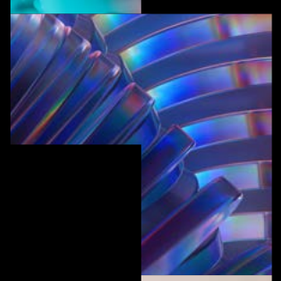
GÉNÉRAL D'ARMÉE (2S)
MARC WATIN-AUGOUARD
Président du Forum InCyber

GUILLAUME TISSIER
Directeur général
du Forum InCyber Europe

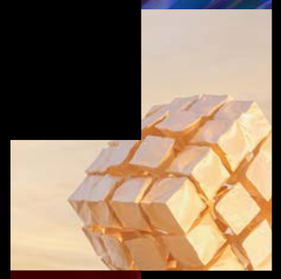
la cybersécurité
en chiffres

13 **fuites de données par jour**
Source : InCyber News / CNIL

1 personne sur 4 **déjà confrontée à une attaque par clonage vocal**
Source : Global Security Mag

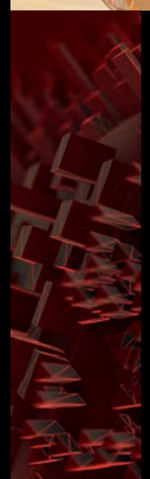


seulement 3 % **des organisations sont considérées comme matures en termes de résilience**
Source : Cisco



12 % **La cybersécurité occupe du budget IT des entreprises mais...**

97 % **...des entreprises prévoient d'augmenter ce budget**
Source : Forbes

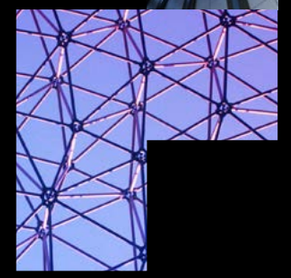


10,5 milliards de dollards US **Impact du cybercrime d'ici 2025**
Source : Cybercrime Magazine

+45 % **nombre de victimes de cyber-rattaques entre 2022 et 2023**
Source : Orange Cyberdefense

27 000 **nouvelles vulnérabilités découvertes en 2023**
Source : Qualys Threat Research Unit

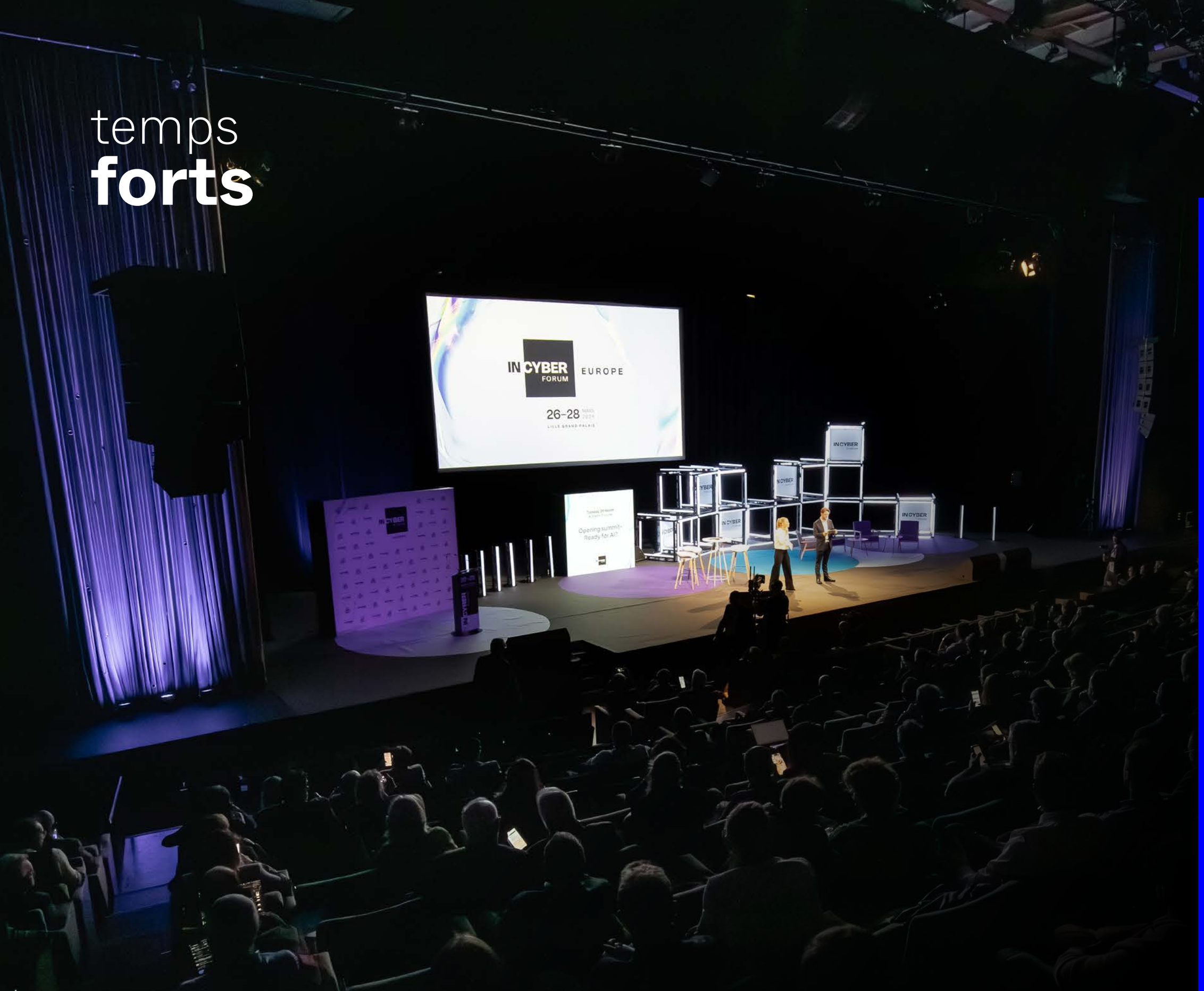
15 000 **organisations européennes concernées par la directive NIS 2 en 2024**
Source : ANSSI



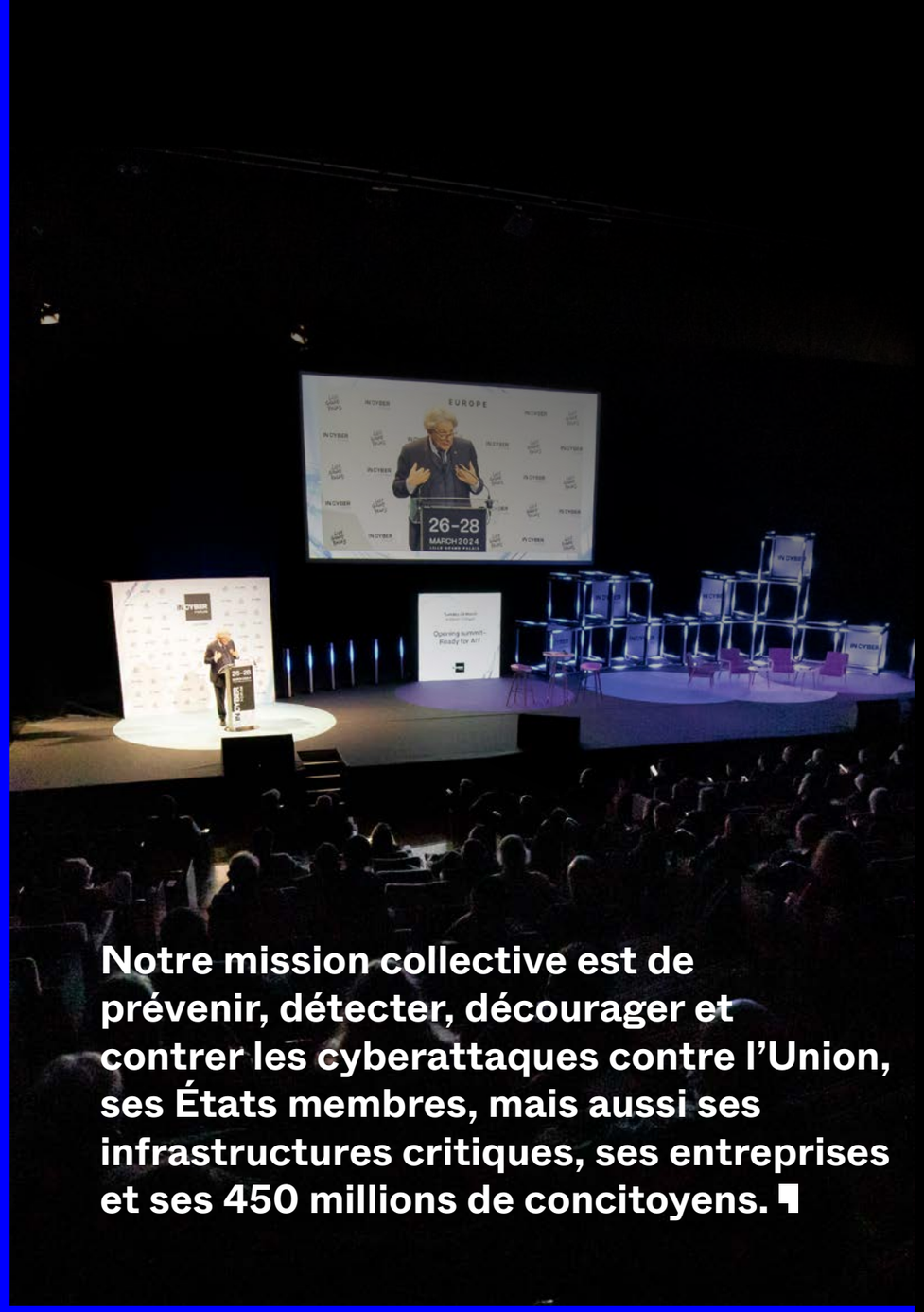
8 milliards de dollars US **marché de l'IA générative en 2023**
Source : Sopra Steria Next

tendances

temps
forts



programme



Notre mission collective est de prévenir, détecter, décourager et contrer les cyberattaques contre l'Union, ses États membres, mais aussi ses infrastructures critiques, ses entreprises et ses 450 millions de concitoyens.

Thierry BRETON
Ancien commissaire européen
au marché intérieur

VOIR LA VIDÉO

L'intelligence artificielle va être un moyen de lutter contre des attaquants qui sont eux-mêmes équipés d'intelligence artificielle. À court terme, cela va permettre d'automatiser, de massifier et de rendre la menace plus sophistiquée.

Benoît FUZEAU
Président
Clusif

Jean-Noël DE GALZAIN
CEO
Hexatrust

VOIR LA VIDÉO

L'intelligence artificielle ne changera pas seulement nos process et notre manière de travailler. Elle nécessitera également une adaptation des personnes, des salariés. Cela devrait être mutualisé et partagé à l'échelle mondiale, et je crois que ce forum est un excellent endroit pour le faire.

Hadi ZABLIT
Vice-président exécutif,
directeur de l'information
et de la technologie
CMA-CGM

VOIR LA VIDÉO

sommet d'ouverture

L'Europe est-elle prête pour l'IA ?

Il y a des préoccupations lors de la mise en œuvre de l'intelligence artificielle. Est-elle fiable ? Respecte-t-elle notre vie privée ? Est-elle éthique ? Ce sont des questions qui devraient constamment être au centre des réflexions de chacun lorsqu'on implémente l'IA, sous toutes ses formes.

Albert CABALLERO
Field CISO
SentinelOne

VOIR LA VIDÉO

Franz REGUL
Directeur cybersécurité
PARIS 2024

Tom Martijn ROELOFS
Responsable mondial de la stratégie de sécurité et des données
ING

Manfred BOUDREAUX-DEHMER
DSI
OTAN

VOIR LA VIDÉO

Aujourd'hui, on vit avec le dilemme du défenseur, selon lequel ce dernier doit être meilleur tout le temps et sur tout son périmètre. Si l'attaquant est meilleur une seule fois, il peut mener son attaque. Je pense qu'avec l'IA, nous allons pouvoir inverser ce paradigme : ce sera à l'attaquant d'être bon tout le temps. Il suffira que le défenseur le détecte une seule fois pour arrêter ses attaques.

Thiébaut MEYER
Directeur sécurité
Google Cloud

Yosra JARRAYA
CEO
Astran

VOIR LA VIDÉO

Ce que l'on doit changer, c'est l'image de la cybersécurité. C'est le sujet clé sur lequel nous devons travailler tous ensemble, ou nous perdrons la cyberguerre, faute de combattants.

Michel VAN DEN BERGHE
Président
CAMPUS CYBER

Bernard GAVGANI
Directeur des systèmes d'information
BNPP

VOIR LA VIDÉO

Pourquoi faire de la prospective ? Il ne s'agit pas d'imaginer le futur pour le plaisir de se faire plaisir (...). L'objectif est d'identifier les leviers sur lesquels agir dès maintenant, les multiples pivots ou aiguillages qui nous conduiront vers tel ou tel futur. Rien n'est pire que de considérer que notre futur, notamment en matière d'IA, est déjà déterminé !

Cécile WENDLING
Directrice
Pan-or-amiques

Adrian TAYLOR
Fondateur
4SING

VOIR LA VIDÉO

Le défi que nous devons relever est celui du passage à l'échelle, du développement de solutions de cybersécurité qui répondent aux besoins du plus grand nombre, de l'ensemble des pans de notre société qui sont aujourd'hui confrontés à cette grande menace.

Vincent STRUBEL
Directeur général
ANSSI

VOIR LA VIDÉO

plénière #1

Réinventer la cybersécurité à l'ère de l'IA

plénière #2

Révolution numérique et bousculements géopolitiques : l'Europe est-elle toujours dans la course ?

Le paysage de la cybersécurité est touché par les défis mondiaux dus à l'augmentation de la gravité et de la fréquence des menaces, ce qui a entraîné des craintes concernant les risques futurs sur la disponibilité des services et des infrastructures critiques.

Juhan LEPASSAAR
Directeur
ENISA

VOIR LA VIDÉO

Nous sommes témoins d'une révolution numérique permanente, rapide, accélérée, qui touche nos sphères privées, professionnelles et même notre vie citoyenne. La digitalisation va à une telle vitesse, avec des bienfaits évidents, que nous avons peut-être tendance à oublier les risques associés et le côté obscur de la force.

Hugues FOULON
CEO
Orange Cyberdefense

VOIR LA VIDÉO

Aujourd'hui les machines nous proposent en permanence de faire les choses à notre place, de décider à notre place, de penser à notre place. Je pense qu'on peut être optimiste sur ce monde qui arrive, mais à condition de ne jamais oublier que l'intelligence artificielle, c'est comme l'argent : un excellent serviteur mais un très mauvais maître.

Olivier BABEAU
Président
Institut Sapiens

VOIR LA VIDÉO

L'utilisation de l'IA pourrait générer 99 milliards d'euros d'ici 2030. Il y a donc urgence à utiliser l'IA, de manière sécurisée et raisonnée, de manière frugale et responsable !

Stephan HADINGER
Directeur de la technologie
AWS France

VOIR LA VIDÉO

plénière #3

L'IA en quête de confiance

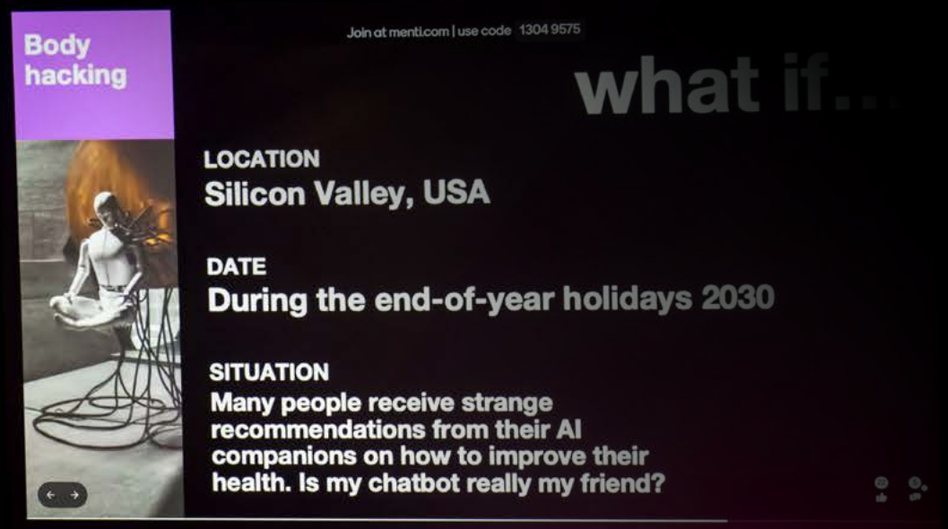
Scénarios prospectifs

Les contenus qui suivent sont uniquement disponible en anglais
et ont été présentés au Forum InCyber 2024 en séance plénière.

Artificial Intelligence and Cybersecurity: Prospective Scenarios

Cécile WENDLING
Managing Director
Pan-or-amiques
Foresight consulting

Adrian TAYLOR
Founder
4SING
Foresight to strategy for security and sustainability in governance



Artificial Intelligence and Cybersecurity: Prospective Scenarios

WHY DO FORESIGHT?

Why engage in foresight? It's not about envisioning the future for the sake of amusement, often by scaring ourselves...

The goal is to identify the levers to act upon now, the numerous pivots that will lead us towards one future or another.

Nothing is worse than assuming our future, particularly in AI, is already predetermined!

Four scenarios are presented to the public and are put to a vote during the InCyber Europe 2024 Forum.

Systemic Crash

Democracy in peril?

The Fog of War 2.0

Body Hacking

Four scenarios are presented where the audience has voiced various preferences.

Attendees of the session voted on the nature of risk in each scenario, the anticipated positive or negative outcomes for each scenario, as well as the most relevant levers across all four scenarios.

The public has to choose: what type of scenario is this?

what if...

LOCATION
Silvergate Capital Bank

DATE
01.12.2030

SITUATION
Alert of unauthorized transaction modifications, is it an attack or a bug?

Systemic Crash

THE STARTING POINT

SOCIAL ACCEPTANCE

The integration of artificial intelligence (AI) into society has become a norm, governed by rigorous European regulations.

TECHNOLOGICAL PROGRESS

Moore's Law remains relevant, generating ever more powerful computing capacities in ever smaller volumes.

USE OF AI IN THE FINANCIAL SECTOR

AI is being put to good use in a number of areas, most notably by financial institutions, which have managed to significantly reduce their costs and increase their profits through its use. Stock and commodities markets are now dominated by institutions that use AI to manage their transactions. These automated systems search continuously (24/7) for up-to-date information, whether positive or negative signals concerning the economic activities of a company, sector or country, in order to assess the potential impact on demand for a commodity and autonomously trigger buying or selling operations before other market players can react.

CYBERSECURITY

Cybersecurity is controlled by a few large non-European companies, and in this sector, a single supplier is often favored. Unfortunately, attack methods against the financial system have developed as rapidly as AI applications. Malware such as FraudGPT and WormGPT is readily available on the dark web and poses a significant threat.

Systemic Crash

CYBERATTACK

BACKGROUND

Since 2023, we have become accustomed to increasingly sophisticated attacks employing artificial intelligence to analyze the profiles of targeted individuals on social networks and to orchestrate large-scale social engineering attacks, with the aim of stealing funds.

TECHNOLOGICAL PROGRESS

Several financial institutions have been alerted to a problem affecting their AI-automated trading platform. It is reported that the AI system has undergone unauthorized modifications (via a backdoor), triggering a cascade of sales transactions.

Infrastructures dependent on ultra-fast AI and very high-speed connections are particularly vulnerable: if one AI system fails, it is likely that related systems will react in chain. The threat of a crash in the financial markets looms large, unless a ransom is paid within a very short timeframe.

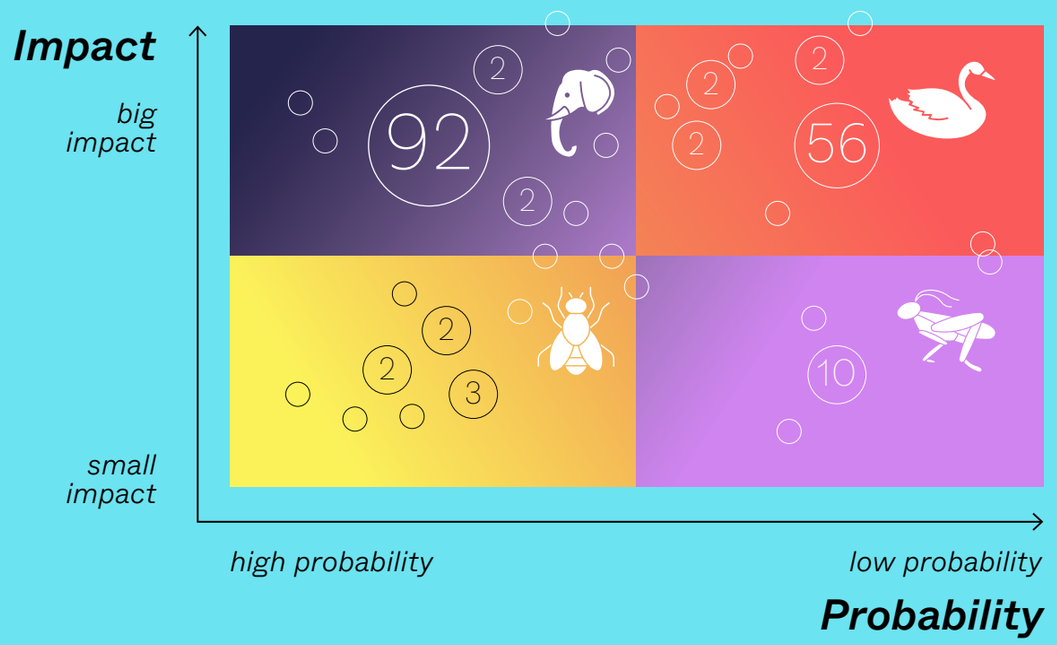
CONCERNING THE ATTACKER

The real problem lies in the uncertainty surrounding the alleged modification of the AI: so far, no abnormal behavior has been detected. Could this claim be a bluff?

92%

of respondants see this scenario as an elephant in the room

What type of scenario is this?



as a result...

Systemic Crash

NEGATIVE BIFURCATION SCENARIO

FLASH CRASH

AI systems, getting out of control, cause an instant collapse of the financial markets - a “flash crash” - before human intervention can take place.

MEDIA REPERCUSSIONS

The crisis is massively covered by the media, drawing comparisons with the 2008 financial crisis.

DOMINO EFFECT

In the worst-case scenario, the situation generates a widespread crisis of confidence, leading to massive capital withdrawals by the public, threatening to precipitate the collapse of the financial system.

SCAPEGOATING

Following the financial collapse, all AI applications are discredited.

POSITIVE BIFURCATION SCENARIO

AI REDUNDANCY

Each institution has two AI systems running in parallel: a primary system and a secondary system, each operating autonomously. In the event of a significant discrepancy between the two systems, or if behavioral alert thresholds are exceeded, human intervention becomes imperative.

EMERGENCY STOP MECHANISM

An emergency stop mechanism is in place, enabling the entire trading system to be suspended if necessary.

FORENSIC ANALYSIS

The real problem lies in the uncertainty surrounding the alleged modification of the AI: so far, no abnormal behavior has been detected. Could this claim be a bluff?

STAKEHOLDER COORDINATION

The financial entities’ cybersecurity teams, located within a dedicated operations center, work closely with leading cybersecurity experts in the local field, facilitating rapid communication of the latest relevant information and immediate dissemination of alerts to other institutions.

SYSTEMIC CRASH

Do you think this scenario will more likely end well ou badly?

133
Positive end

100
Negative end

LOCATION
France

DATE
Early June 2027

SITUATION
AI knows you better than anyone. So can it now shape how you vote?

Democracy in peril?

THE STARTING POINT

SOCIAL ACCEPTANCE

The integration of artificial intelligence (AI) into society is proceeding steadily, framed by European regulations that are distinct from those in the USA and China. However, this integration raises concerns about job losses and the associated energy impact.

TECHNOLOGICAL PROGRESS

Automation is gaining significant ground with the rapid advance of the Internet of Things; an increasing number of objects are now equipped with microprocessors that collect valuable data.

AI APPLICATIONS

Given the abundance and diversity of data available, AI is increasingly being used to detect patterns within this data. For example, AI analyses can be used to model areas of drug consumption by analyzing sewage water quality. The use of historical data helps identify the most dangerous intersections or the streets most likely to be burglarized. In addition, traditional media are finding themselves increasingly forced to rely on AI for content production, in the face of steadily declining revenues.

CYBERSECURITY

In Europe, AI training algorithms and datasets must be audited by an independent entity and comply with copyright legislation, as well as other criteria such as the prevention of discrimination.

Democracy in peril?

CYBERATTACK

BACKGROUND

Since the year 2023, extremists from a variety of backgrounds have been exploiting artificial intelligence to destabilize the political landscape. Some practice traditional disinformation, creating deepfake videos and articles that undermine the credibility of opposing political figures, with such sophistication that authenticity appears unmistakable. Other groups use AI to target and disseminate this misleading information to the most receptive individuals.

CURRENT SITUATION IN 2030

It is now possible to synthesize the results of various AIs and data from the Internet of Things (IoT) to deduce the political inclinations of virtually all citizens. What's more, AI facilitates mass personalization of messages sent to maximize outrage. With the gradual decline of professional journalism, it is becoming increasingly difficult to find independent entities capable of rigorous fact-checking.

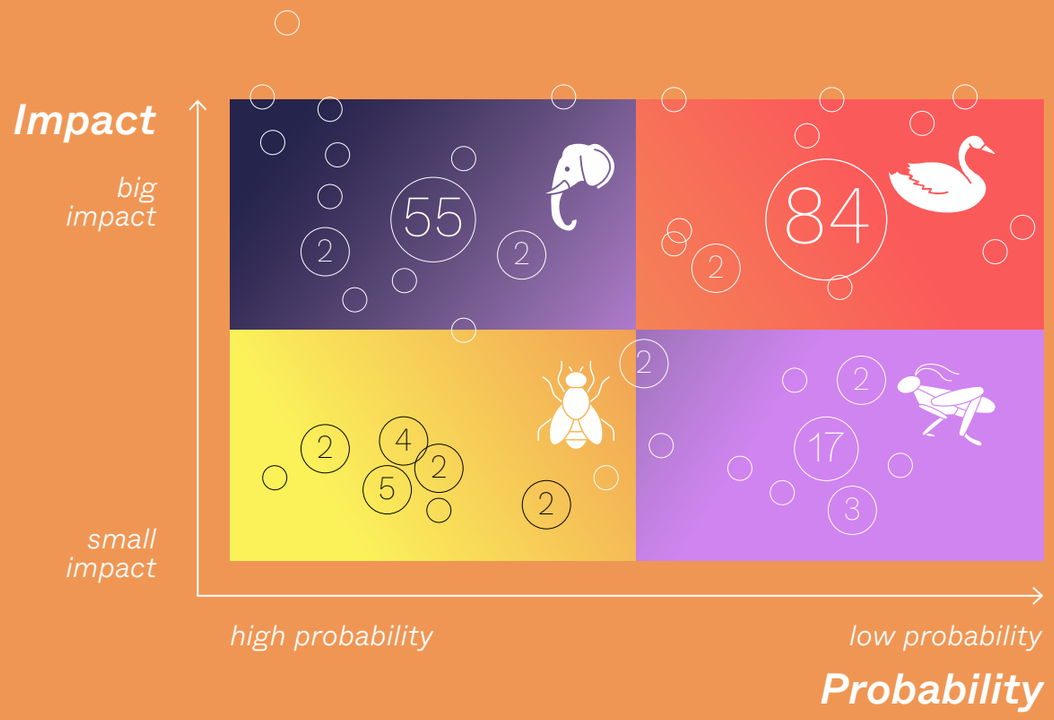
CONCERNING THE ATTACKER

Political extremists continue to exist, and it is suspected that they benefit from the support of certain authoritarian states seeking to undermine democracies.

84%

of respondants see this scenario as a black swan

What type of scenario is this?



as a result...

Democracy in peril?

NEGATIVE BIFURCATION SCENARIO

EROSION OF CONFIDENCE

In a climate of heightened political and geopolitical polarization, agreement on the perception of reality is compromised. Undeniable facts are called into question, and unfounded rumors are taken at face value. Combating the growing skepticism of citizens towards the system (politics, media, institutions, etc.) and maintaining trust is a major challenge.

EXTREMES IN POWER

In a period of heightened unrest, digital tensions materialize, provoking demonstrations, urban blockades and potential riots. Political movements adhering to an "illiberal democracy" vision are coming to power and using AI to "fight crime", resulting in increased surveillance and repression of dissidents.

AI INFLUENCED AND INFLUENCING

AI is now forced to align itself with government perspectives, influencing the news and recommendations it generates.

POSITIVE BIFURCATION SCENARIO

COLLECTIVE INTELLIGENCE

We benefit from advances in cognitive warfare, implement public and private initiatives to combat disinformation, and step up education on this issue both in schools and among the general public.

TECHNO-LEGAL SUPPORT

The adoption of a European digital identity, guaranteeing ownership of personal data to individuals rather than companies, reduces the possibility of profiling individual behavior. In addition, digital watermarking systems are proving effective in identifying and removing falsified content, such as deepfakes, in collaboration with Internet service providers (ISPs) who take responsibility for online content.

DIFFERENT LEVELS OF GOVERNANCE

For European states vulnerable to disinformation campaigns, the European Union also plays a regulatory and protective role.

SYSTEMIC CRASH

Do you think this scenario will more likely end well ou badly?

36
Positive end

155
Negative end

what if...

LOCATION
At the border of Europe

DATE
In 2030

SITUATION
A tense situation becomes critical. Is the drone reliable?

The Fog of War 2.0

THE STARTING POINT

SOCIAL ACCEPTANCE

There are reservations about the implementation of artificial intelligence in society, mainly due to concerns about job losses and increased surveillance by AI systems. However, the crucial role of AI in the military field is indisputable, in particular the use of drones - whether operating on land, in the air or at sea - whose presence in large numbers is deemed indispensable.

TECHNOLOGICAL PROGRESS

The continuing evolution predicted by Moore's Law ensures a steady increase in the power of the micro-processors integrated into UAVs.

APPLICATION OF AI

The progressive autonomy of UAVs has become essential to overcome interference and respond rapidly to offensives. What's more, these drones are now capable of autonomously carrying out the entire OODA cycle (observe, orientate, decide, act). Human reaction time, however valuable, can be a major disadvantage for these devices..

CYBER PROTECTION

Gone are the days when military projects required a limited number of high-performance machines, made up of parts produced and regulated locally. It is now imperative to have a large number of drones, often commercially available and cost-effective. This means that many components, particularly microprocessors, are designed and manufactured abroad. Any attempt to deviate from this trend runs up against problems of cost (prohibitive) and design (obsolete compared to the commercial sector). Cyber security is generally integrated post-purchase, when the drone is converted and equipped for military service.

The Fog of War 2.0

CYBERATTACK

BACKGROUND

Since the year 2023, it has become progressively clear that democratic countries are facing a major problem. Their citizens demand that the laws of war be respected, and persist in demanding that the decision to launch an attack be taken by a human being. However, it is becoming increasingly clear that potential enemies have no qualms about deploying autonomous killer drones, and now possess the technological capability to do so.

CURRENT SITUATION IN 2030

Information transmitted by our drones indicates the massive approach of hundreds of enemy drones on the outskirts of the border. The command center has been informed. In the event of an unexpected assault, time is running out, and there are only a few moments left to avoid the destruction of our drones or border units. A decision must be taken immediately: either let the attack proceed without intervention, or initiate a pre-emptive offensive.

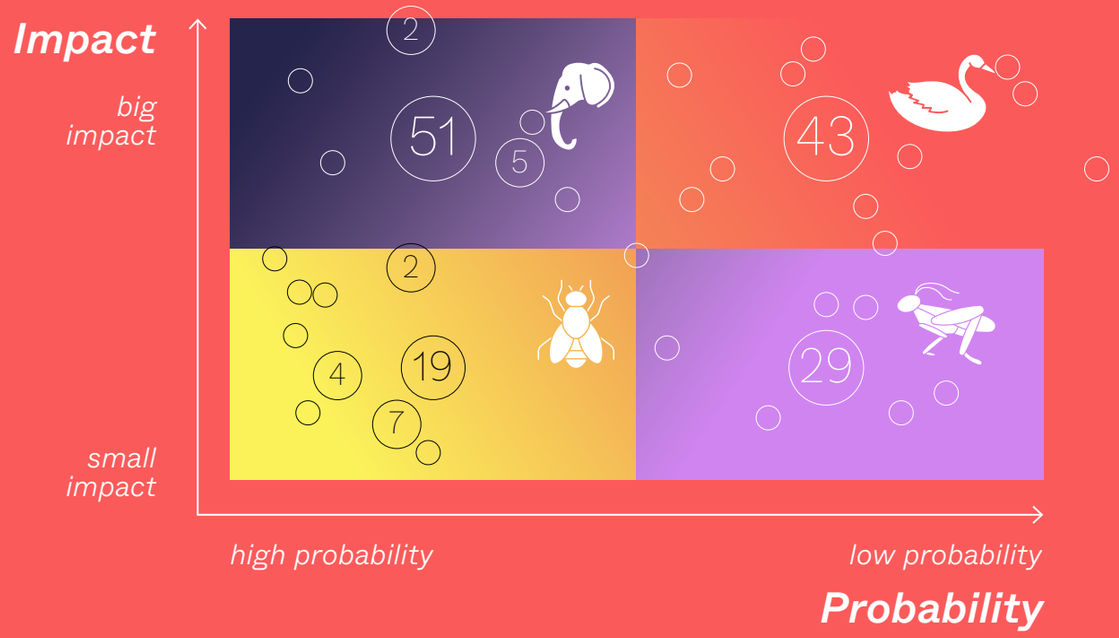
CONCERNING THE AGGRESSOR

Geopolitical escalation is reaching a critical level. The hypothesis of an imminent attack is taken seriously. But what if the threat were fictitious? An AI attack simulation designed to simulate a swarm of drones where there are only a few? What if the objective was to incite us to retaliate, offering the adversary the opportunity to present himself as the legitimate defender of his rights? Or, even more worryingly, what if it's simply a software failure?

51%

of respondants see this scenario as an elephant in the room

What type of scenario is this?



as a result...

The Fog of War 2.0

NEGATIVE BIFURCATION SCENARIO

ESCALATION

In the absence of international standards on the use of AI and autonomous military systems, communication with potential adversaries proves difficult. The decision to launch an attack must be taken without delay.

SPIRAL OF WAR

Once we have initiated the offensive, it is certain that the adversary will respond. With its drones programmed to react without human intervention, retaliation is inevitable.

POSITIVE BIFURCATION SCENARIO

DIPLOMACY

Diplomacy succeeds in building mutual trust to establish preventive rules against immediate and automatic reaction, such as an “AI red line”, providing the time needed to defuse tensions.

DETERRENCE

Our deterrence capability is strong enough to deter any hostile attempt. Thanks to an arsenal of drones and independent cyber-defense systems, the likelihood of widespread infection is greatly reduced.

SURVEILLANCE

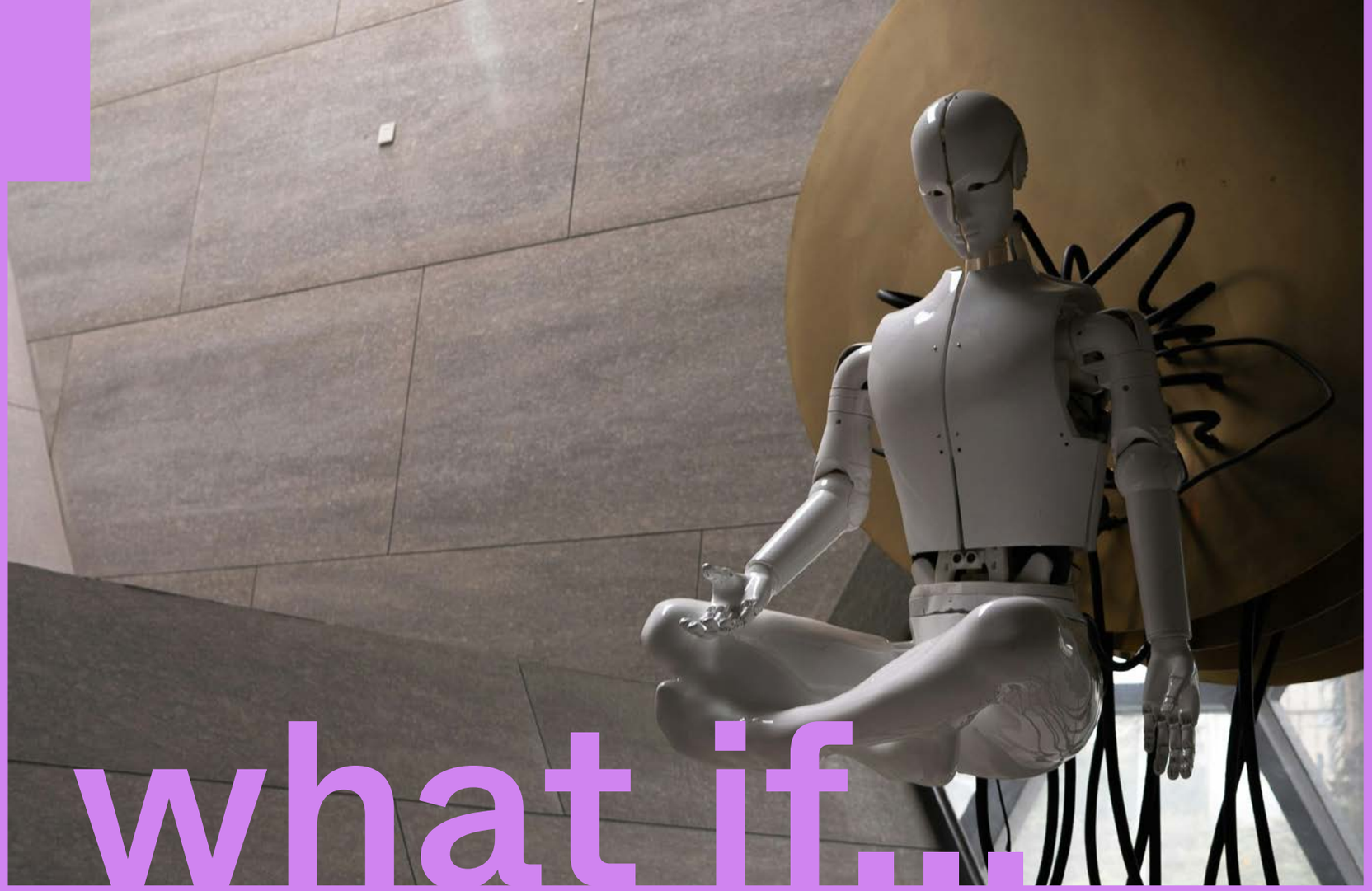
Continuous monitoring is carried out, including by AIs specialized in the supervision and control of our own drones. In addition, we have a sufficient number of qualified personnel capable of understanding and interpreting the activities of our drones.

SYSTEMIC CRASH

Do you think this scenario will more likely end well ou badly?

72
Positive end

115
Negative end



what if...

LOCATION
Silicon Valley, USA

DATE
During the end-of-year holidays 2030

SITUATION
Many people receive strange recommendations from their AI companions on how to improve their health. Is my chatbot really my friend?

Body Hacking

THE STARTING POINT

SOCIAL ACCEPTANCE

The adoption of artificial intelligence in everyday life has become a reality, particularly in the medical field where it is now an essential support, reinforced by the introduction of stringent European regulations concerning the use of personal data.

TECHNOLOGICAL INNOVATION

Innovation lies primarily in the interaction between humans and technology. Technology is no longer a tool used occasionally, such as a computer or smartphone, but a companion in constant interaction with us, such as an anthropomorphic friend with a pleasant voice, a watch with multiple functions, or microprocessors implanted in the human body. Edge computing and edge AI enable small systems to perform complex tasks independently of a central computer.

AI APPLICATION

The aggregation of heterogeneous personal data, often collected by wearable devices, enables AI to diagnose illnesses upstream and refine teleconsultation. In addition, anthropomorphic chatbots, which have become integrated into our homes, workplaces and public spaces, are highly appreciated. Included in the healthcare network, they are used, among other things, to remind people to take their medication. For many people, particularly the elderly or isolated, these chatbots are perceived as true companions.

CYBER PROTECTION

Every small, autonomous system needs to be cyber-secure. This is why AIs recommended by other AIs are often used to guarantee this protection.

Body Hacking

CYBERATTACK

BACKGROUND

Since 2023 there have been repeated attempts to steal private patient data, via chatbots compromised by hackers. But the data thus obtained was secured by a cybersecurity AI. Criminals hope that one day they'll be able to decrypt the data using quantum computing, but that's a long way off.

CURRENT SITUATION IN 2030

A pioneering healthcare systems company is about to launch a takeover bid. The company specializes in AI systems that interact with humans via chatbots, and even physically, being installed in heart regulators and chips implanted in more and more people (originally only for people who can no longer communicate with the outside world, now it's become "cool" to be able to manage one's computer this way). But a worried doctor contacts the company. His chatbot had just suggested he take an excessive dose of medicine. Was the chatbot poisoned?

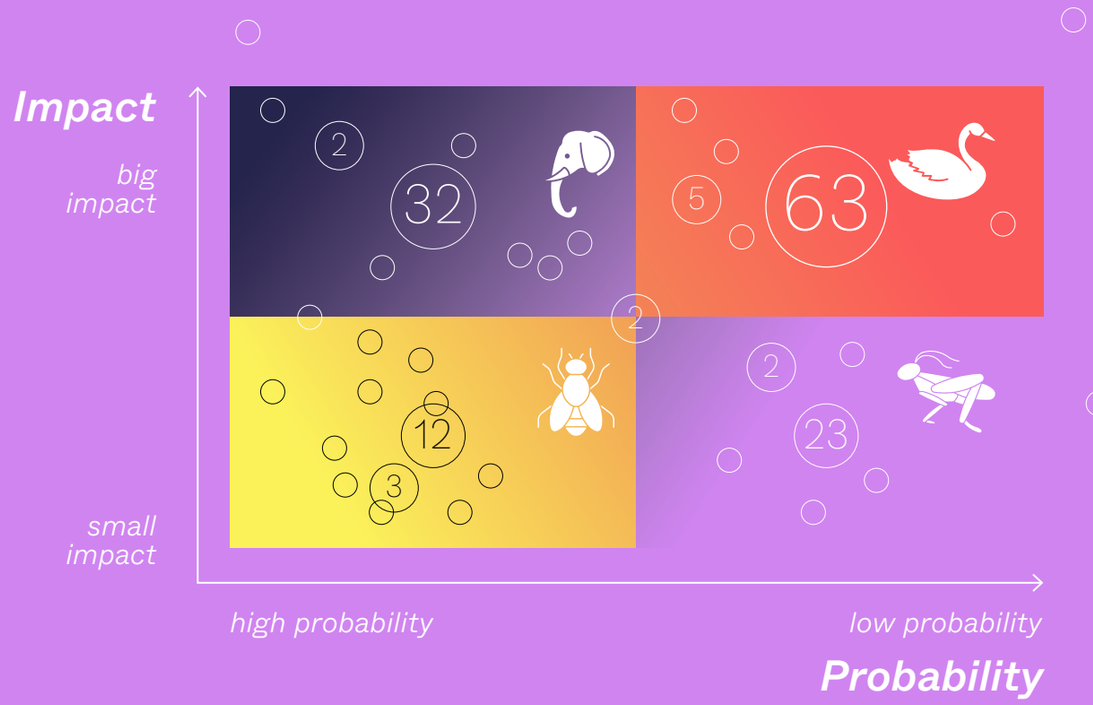
ABOUT THE ATTACKER

In the absence of a ransom demand, one wonders whether this is a technical error - or whether a rival company, from elsewhere in the world, is trying to discredit the company before it has access to large funds with the takeover bid.

63%

of respondants see this scenario as a black swan

What type of scenario is this?



as a result...

Body Hacking

NEGATIVE BIFURCATION SCENARIO

CASUALTIES

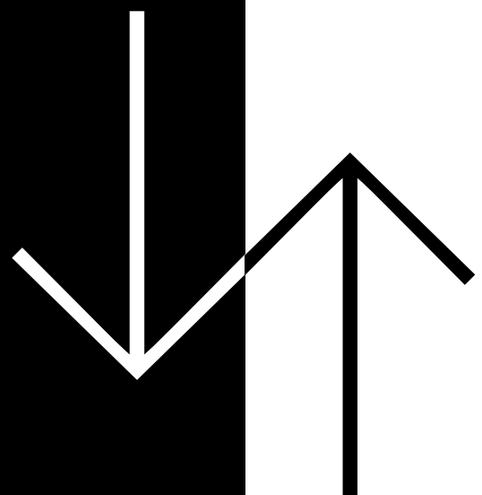
If the attack is successful, there may be casualties. Chatbots will give bad advice, and some may die of over-medication. Others will have heart problems, or will no longer be able to communicate via the implanted microprocessors.

ECONOMIC DAMAGE

The company's reputation will be ruined, as will its hopes of a takeover bid.

PUBLIC DISTRUST

The AI-based healthcare system will be called into question by the public.



POSITIVE BIFURCATION SCENARIO

ACA

A decentralized AI ("Autonomous Cyber-defense Agent") also detects malfunctioning of the AI system, and warns the company and the user.

A VARIEGATED DEFENSE

Having the option of purchasing a defense system from several different local and foreign companies makes the attacker's task more difficult, since he has to attack several different systems.

SYSTEMIC CRASH

Do you think this scenario will more likely end well ou badly?

100
Positive end

60
Negative end

Artificial Intelligence and Cybersecurity: Prospective Scenarios

WHICH OF THESE PIVOTAL CHOICES MAKES IT EASIER TO COME UP WITH POSITIVE SCENARIOS?

Insignificant answer ↑

Having an AI cybersecurity defense system

Having a digital identity & strict privacy rules

Having a "off button" on the AI

Having many AI platforms, not a big few ones

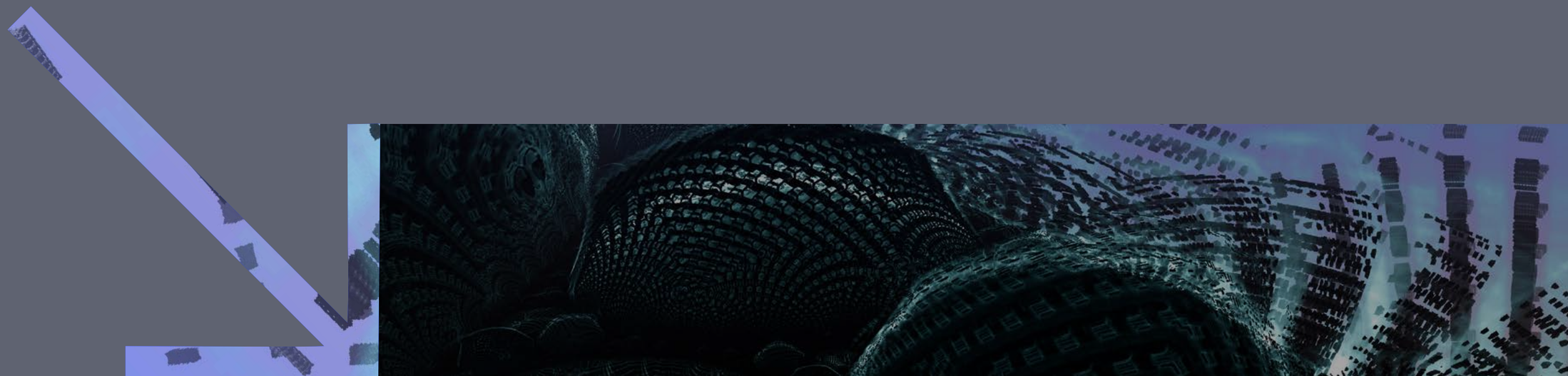
Having multiple providers of cyber-defense systems

Having a right to preemptive strike against a threat

Having a parallel system that works without AI

Having a cyber-diplomacy system in place

↓ *Significant answer*



IN CYBER
NEWS

LE MÉDIA DE LA
CONFIANCE NUMÉRIQUE

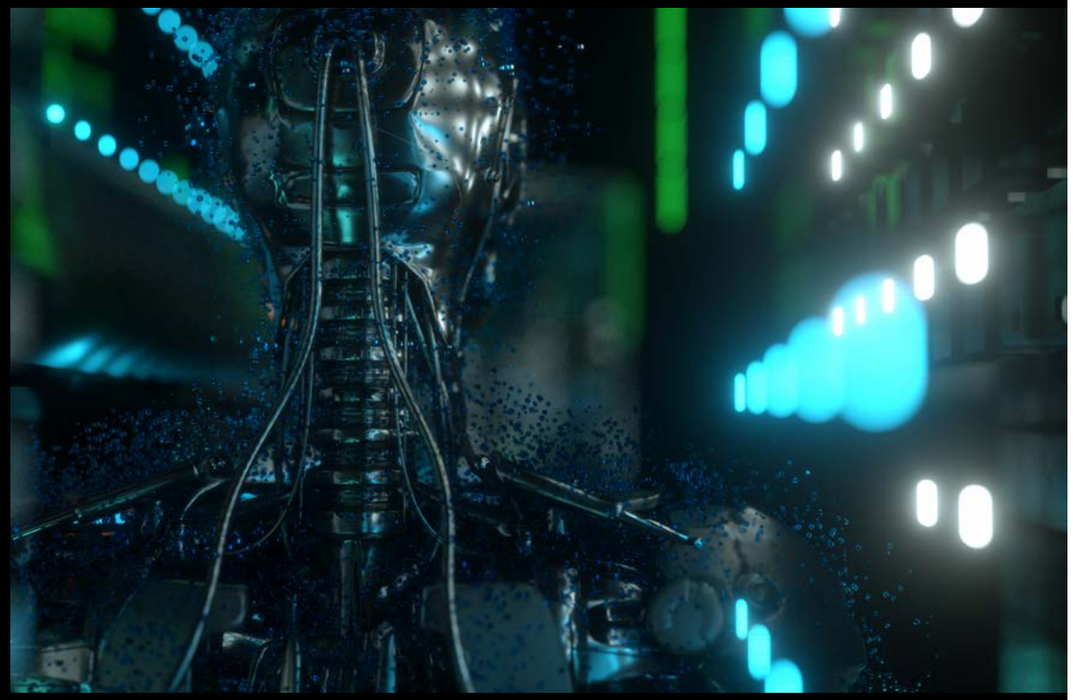
Ces articles ont été rédigés par
les journalistes d'INCYBER NEWS
à partir des tables rondes et conférences
du Forum InCyber Europe 2024

incyber.org

revue de presse

Menaces numériques et amplification de l'IA : l'Europe est-elle toujours dans la course ?

par **Olivier CIMELIÈRE** #GESTION DES RISQUES



LIRE L'ARTICLE EN LIGNE

Alors que la course technologique s'amplifie, l'Europe peut-elle faire émerger ses propres règles et champions ? Tour d'horizon des menaces et des opportunités de cette nouvelle ère pour le « vieux » continent.

Directeur exécutif de l'ENISA (Agence de l'Union européenne de la cybersécurité qui célèbre cette année ses 20 ans d'existence), Juhan Lepasaar a dévoilé les principaux enseignements issus de sa nouvelle étude sur les cybermenaces en Europe à l'horizon de 2030.

LES VULNÉRABILITÉS CLASSIQUES TOUJOURS D'ACTUALITÉ

Il a d'abord évoqué les menaces classiques mais toujours virulentes qui peuvent mettre en péril les chaînes logistiques. Avec toujours plus d'intégration et de connectivité entre les fournisseurs, les producteurs, les distributeurs et les clients, les vulnérabilités potentielles se sont multipliées d'autant dans des systèmes informatiques de plus en plus complexes à gérer où les attaques sont plus difficiles à détecter.

À cette fragilité potentielle, s'en ajoute une autre : la capacité à développer et mettre en place des patchs lorsque des failles informatiques sont détectées. À l'heure actuelle, il faut souvent plus d'un mois en moyenne entre la découverte d'une faille et sa résolution. À cet égard, l'ENISA a constitué une base de données européenne où sont recensées toutes les vulnérabilités identifiées pour accélérer la coordination entre les différents acteurs concernés et l'apport plus rapide de solutions de sécurité.

Autre préoccupation forte : la pénurie d'experts en matière de cybersécurité en Europe. Les besoins sont grandissants mais les compétences disponibles sont rares. Un constat que partage justement Yann de Kersauson du cabinet de recrutement Arthur Hunt Executive Search lors d'une récente interview accordée à InCyber. Dans cette optique, l'ENISA et ses partenaires ont développé un référentiel qui va permettre d'identifier les talents requis, les former intensivement et les certifier.

Pour conclure sa présentation, Juhan Lepasaar est revenu succinctement sur l'intelligence artificielle qui va indéniablement accroître les cybermenaces dans les années à venir. Il a notamment évoqué les élections européennes du 9 juin prochain qui font déjà l'objet de diverses attaques, avec en particulier le recours aux *deepfake* pour brouiller les débats et influencer les votes. Un deuxième point de vigilance a également été soulevé : celui des catastrophes naturelles liées au dérèglement climatique qui menacent fortement la résilience des infrastructures numériques du fait de leur fréquence accrue mais également de leur impact de plus en plus destructeur (inondations, submersion, sécheresse qui entraîne des fissures dans les infrastructures, etc).

CONCILIER *« RULES OF THE GAME »* ET *« ART OF THE GAME »*

Une table ronde a ensuite rassemblé Wojciech Wiewiorowski, contrôleur européen pour la protection des données basé à Bruxelles et Nicolas Miailhe, co-fondateur de la start-up parisienne Prism Eval spécialisée dans l'évaluation et l'interprétabilité des modèles et systèmes d'IA d'avant-garde. Le cœur de la discussion a particulièrement porté sur l'option assez inédite que l'Union européenne a choisi de prendre en matière de régulation de l'intelligence artificielle. Là où d'autres pays comme la Chine et les États-Unis régulent relativement peu, voire pas du tout, l'Europe des 27 a décidé de se doter de cadres réglementaires solides pour développer son industrie de l'IA et se protéger de certaines dérives.

Le 13 mars dernier, le Parlement européen a ainsi adopté l'*AI Act* pour encadrer l'intelligence artificielle et ses usages. Première initiative de cette envergure aux yeux de Wojciech Wiewiorowski, ce règlement impose des obligations aux concepteurs et aux utilisateurs des systèmes d'IA en fonction de leur niveau de risque et de sécurité. Pour Nicolas Miailhe, cette démarche représente un pari courageux que de se doter d'une série de règles pour bâtir un marché conforme aux valeurs européennes.

Il pondère toutefois son propos en souhaitant que la bureaucratie ne constitue pas un frein à l'innovation des acteurs européens en interférant excessivement. Bien appliqué, le cadre réglementaire peut selon lui permettre le déploiement de l'industrie européenne de l'IA avec des standards robustes et fiables qui pourraient même être de futurs référentiels internationaux.

Mais une condition est essentielle : le régulateur européen doit disposer de compétences pointues qui comprennent ce qu'est l'IA. Un défi qui risque d'être complexe au regard de la raréfaction actuelle des profils disponibles sur le marché. D'où une priorité : concilier les *« rules of the game »* et l' « *art of the game* » !

HELSING, LA VOIE À SUIVRE ?

Dans ce contexte, s'agit-il donc d'un vœu pieu ? En matière d'intelligence artificielle, les géants américains comme Google, Meta et Apple ont déjà pris un temps d'avance au niveau mondial sans oublier l'alliance qui unit OpenAI et Microsoft ainsi que Nvidia. En Europe, ce monopole est l'objet d'âpres discussions. Est-il trop tard pour contrebalancer la suprématie américaine avec des champions issus du Vieux Continent ? Certains estiment qu'introduire une préférence dans les commandes publiques européennes permettrait de faire naître des concurrents solides face aux acteurs américains. En France, des sociétés comme Mistral AI, Hugging Face ou encore LightOn affichent de véritables promesses même si récemment Mistral AI a semé le trouble en signant un partenariat avec Microsoft.

Vice-président de Helsing, une start-up européenne spécialisée dans l'intelligence artificielle au profit du monde de la défense, Antoine Bordes a tenu à témoigner qu'il est possible de développer un acteur viable à l'échelle européenne.

Créé en 2021 en Allemagne grâce à un investissement de 100 millions d'euros du fonds suédois Prima Materia, Helsing s'est ensuite implantée au Royaume-Uni et en France pour travailler dans les trois pays avec les forces militaires les plus importantes du Vieux Continent. Aujourd'hui, l'entreprise est capable de fournir des logiciels à base d'IA ultra-performants qui permettent à des forces armées de traiter en temps réel les données disponibles et appuyer ainsi aussitôt les manœuvres et les prises de décision sur le terrain. Une preuve que la mise en commun de capacités et de talents peut contribuer à l'émergence de solides champions européens.

Intelligence artificielle & arnaques numériques : sommes-nous condamnés à se faire avoir ?

par **Olivier CIMELIÈRE** #TRANSFORMATION NUMÉRIQUE

LIRE L'ARTICLE EN LIGNE

En 2023, le cabinet de conseil Gartner estime que 20 % des attaques de *phishing* reposaient sur de l'IA et que la tendance est à la recrudescence. Comment s'en prémunir ? Quels processus mettre en œuvre au plan organisationnel ? Quelles solutions pour lutter contre ces attaques ?

L'affaire a fait grand bruit. En février 2024, une entreprise basée à Hong Kong a été victime d'une « arnaque au président » rendue crédible par une vidéoconférence en *deepfake* générée par une IA. Mis en confiance, un collaborateur a alors accepté d'effectuer plusieurs virements bancaires d'un montant total de 24 millions d'euros au bénéfice de ce qui s'est avéré être une fraude magistrale. Pour les experts, il s'agit là du premier cas au monde de la fameuse « arnaque au président » dopée à l'intelligence artificielle générative.

Les arnaques sur les réseaux numériques et de télécommunications ne sont en soi pas nouvelles. En revanche, l'adjonction de l'IA pour booster les capacités à leurrer les individus et les entreprises, trace des perspectives préoccupantes pour les responsables des systèmes d'information et de la cybersécurité. Antoine Bajolet, membre du Clusif et RSSI de Henner – un groupe de courtage en assurances – distingue globalement trois catégories d'arnaques numériques : le *hacking* qui implique une intrusion dans les systèmes informatiques d'une organisation, la déstabilisation pour détruire la réputation et les arnaques à base de courriels, SMS et messages qui usurpent des identités pour dérober de l'argent et/ou des informations sensibles.

ENNEMI PUBLIC N°1 : LE *SPEARPHISHING*

Aux yeux d'Antoine Bajolet, c'est dans cette dernière catégorie que le danger est le plus manifeste depuis que l'IA est utilisée à des fins frauduleuses, notamment à travers une méthode de piratage redoutable communément appelée hameçonnage ciblé (ou *spearphishing*). Celle-ci reprend parfaitement les codes visuels, graphiques et sémantiques d'un émetteur donné tout en y ajoutant des éléments de contexte qui permettent de personnaliser le message et d'endormir la méfiance de la personne ciblée. L'IA a considérablement décuplé les capacités du *spearphishing* en restituant à l'identique une identité et une manière de s'exprimer. Le destinataire va ainsi répondre ou bien cliquer sur un lien piégé qui active un logiciel malveillant permettant aux pirates d'accéder au système informatique d'une organisation. Antoine Bajolet cite notamment le cas de Pikabot, un *malware* particulièrement dangereux par sa sophistication existant depuis 2023.

Jean-Baptiste Roux, vice-président Europe sales de Sosafe, une société spécialisée qui accompagne et forme les organisations publiques et privées en matière de cybersécurité corrobore ce constat.

Le *spearphishing* mâtiné d'IA génère un taux de clic nettement plus important que les arnaques classiques du fait de cette capacité à s'immiscer dans le contexte des personnes visées. Mises en confiance par un environnement qui leur est familier, ces dernières ont tendance à tomber plus facilement dans le piège tendu. S'appuyant sur une récente étude de Sosafe, Jean-Baptiste Roux précise qu'en 2024, l'IA générative qui rend les outils d'ingénierie sociale plus élaborés et plus complexes à repérer, mettra la psychologie humaine au cœur d'un nombre sans précédent d'arnaques similaires.

QUAND L'INTERNE « FAVORISE » L'ARNAQUE

Directeur de la stratégie cyber de Forecomm, une société qui conçoit des solutions de cybersécurité pour les entreprises, Philippe Loudenot partage le même regard. L'IA permet d'accélérer et de massifier les arnaques numériques avec des apparences de plus en plus troublantes de véracité. Pour lui, « le pire est devant nous. La seule limite sera l'esprit humain et sa capacité à créer des produits malintentionnés. Il est essentiel qu'on sache garder et cultiver un sens critique, qu'on s'accorde un peu plus de temps de réflexion face à un message plutôt que cliquer sans réfléchir. Cela reste encore la meilleure protection ».

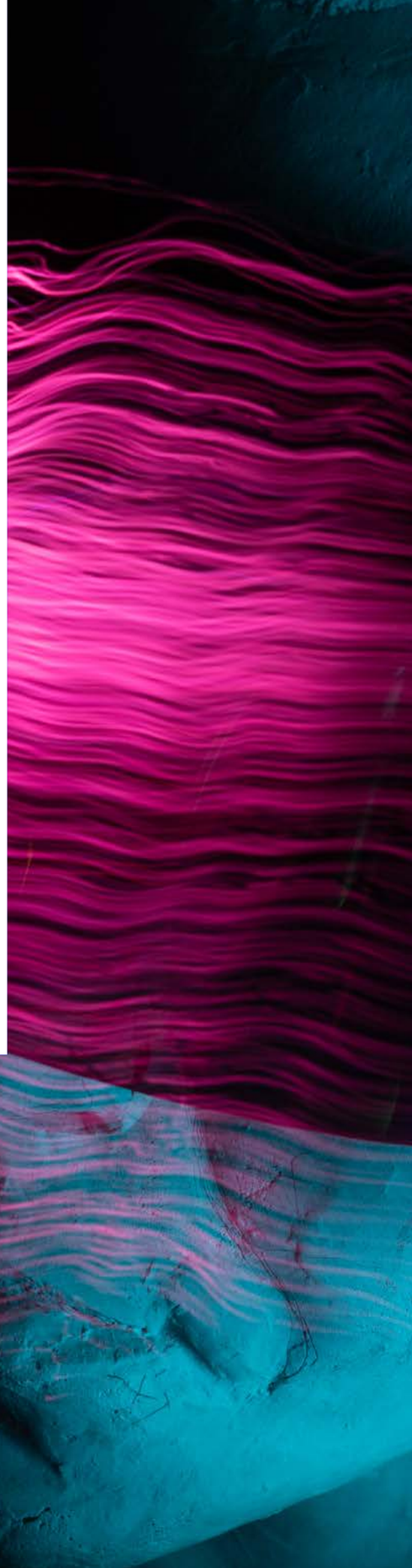
Antoine Bajolet confirme effectivement que les arnaques sont souvent efficaces parce que « à la base, il y a une erreur humaine ». Erreur qui peut aussi provenir de l'intérieur d'une organisation. Dans certains chats de service après-vente, il arrive parfois que les développeurs confient au *bot* (pour le nourrir), des données confidentielles qui vont ensuite s'agréger à des données plus basiques et qui vont possiblement fuiter à l'extérieur alors que celles-ci auraient dû demeurer dans un environnement interne sécurisé. Or, ces données peuvent à leur tour inspirer des pirates pour concevoir de nouvelles arnaques encore plus crédibles.

LA VIGILANCE HUMAINE, MEILLEUR REMPART

Pour autant, les spécialistes autour de la table ne cèdent pas à la panique. Des solutions de protection existent et elles ne sont pas uniquement technologiques. Pour Antoine Bajolet, il y a d'abord le bon sens et la vigilance, comme le fait d'observer de plus près le nom de domaine (DNS) utilisé dans un message. Généralement, une organisation utilise un DNS unique et officiel pour communiquer avec ses publics. Dès lors, il convient de scruter attentivement l'extension qui lui est accolée (.fr, .com ou quelque chose de plus exotique !) et son orthographe. En effet, les pirates recourent à des noms de domaines approchants (à un caractère près par exemple ou une lettre inversée) pour usurper l'identité d'un émetteur.

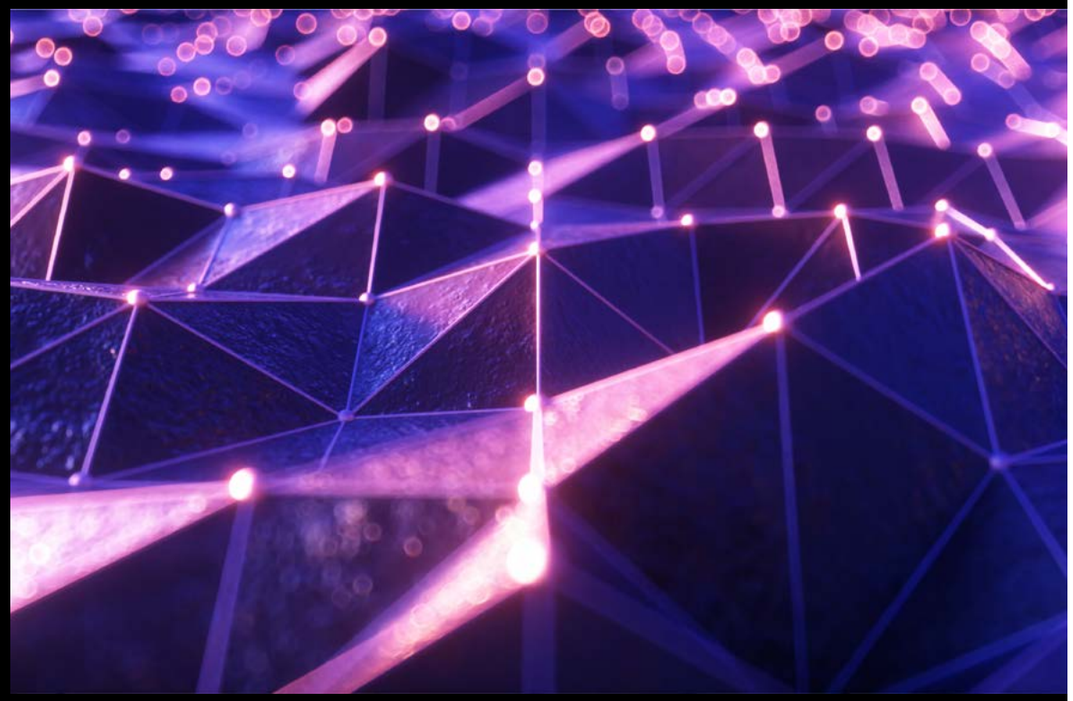
Autre point qui contribue à rassénérer quelque peu selon Antoine Bajolet : les modes opératoires des IA malveillantes ne changent guère. En conséquence, il faut appliquer rigoureusement et en permanence les procédures de sécurité informatique qui existent dans chaque organisation et qui demeurent tout à fait pertinentes pour contrer des arnaques à base d'IA. En cas de doute extrême, il s'agit même de ne pas hésiter à prendre son téléphone pour appeler un collègue et vérifier si le message est authentique ou falsifié, s'il provient bien de lui ou d'un avatar parfaitement imité. Conserver son esprit critique reste encore un excellent moyen de prophylaxie contre les arnaques numériques.

Jean-Baptiste Roux fait remarquer que les arnaques à base d'IA s'inspirent des comportements humains qui traitent les informations de plus en plus vite sans faire nécessairement attention ou prendre du recul par rapport à une arnaque très bien conçue. De même, l'expert trouve que les entreprises ont tendance à recourir à l'IA sans même réfléchir à la mise en place préalable d'une gouvernance stricte qui encadre les usages. Actuellement, on estime à 300 millions d'utilisateurs qui ont adopté l'IA dans leurs pratiques professionnelles sans même disposer de guidelines et de procédures qui aident à sécuriser l'usage des données. Un sujet sur lequel les organisations doivent impérativement mieux prendre la mesure. À l'heure où les logiciels malveillants 100 % automatisés par IA se propagent, la question est effectivement cruciale.



Comment l'**IA générative** va « augmenter » le **SOC**

par **Xavier Biseul** #SECOPS



LIRE L'ARTICLE EN LIGNE

En contextualisant les alertes, l'IA générative facilitera la prise de décision des analystes d'un SOC. Une fois la menace formellement identifiée, elle automatisera l'orchestration des réponses à apporter.

Et si l'intelligence artificielle résolvait le déficit structurel de compétences dans la cybersécurité. Non seulement les profils cyber sont rares mais ils sont souvent affectés à des tâches rébarbatives et sans grande valeur ajoutée qui pèsent sur leur santé physique et morale. Selon une étude de l'association américaine ISACA *(Information Systems Audit and Control Association),* 60 % des sociétés peinent à retenir leurs experts et le stress au travail est l'une des principales causes de démission.

De fait, l'IA est appelée à alléger le quotidien dans les SOC's. Assurant une analyse de premier niveau, elle vient décharger les analystes de la lecture de centaines de lignes de logs – un travail particulièrement ingrat – pour les laisser se concentrer sur les événements essentiels méritant leur attention. Plus généralement, un assistant virtuel permet de passer en revue l'exhaustivité des données toujours plus nombreuses remontées par les systèmes de supervision. Ce qu'aucun être humain ne peut matériellement réaliser.

L'arrivée de l'IA générative devrait faire passer un niveau supérieur dans la détection, la qualification et l'analyse des menaces puis la réponse aux incidents. « Quand ChatGPT d'OpenAI est arrivé sur le marché [en novembre 2022, NDLR], j'ai immédiatement perçu son utilité dans nos métiers », avance Philippe Gillet, cofondateur et CTO de Gatewatcher, éditeur français d'une plateforme de NDR *(Network Detection and Response).*

CONTEXTUALISER LES ALERTES

Près d'un an et demi plus tard, Gatewatcher effectuait une démonstration technique au Forum InCyber 2024, de Gaia, son assistant reposant sur l'IA générative. Actuellement en bêta-test auprès de quelques clients historiques, il devrait être officiellement dévoilé à la fin du premier semestre 2024. Gaia vise à accélérer la mise en œuvre des politiques de sécurité, en facilitant la prise de décision voire en automatisant les actions de remédiation. « Nous avons voulu mettre l'IA au service des métiers, poursuit Philippe Gillet. Les cas d'usage explorés correspondent aux souhaits exprimés par nos clients. »

Dans une approche de « SOC augmenté », l'IA apporte tout d'abord une dimension de conseil en contextualisant les alertes complexes et en établissant des corrélations avec des menaces déjà répertoriées. « Pour lutter contre les faux positifs, l'IA donne des indications à l'analyste pour faciliter la levée de doute, explique Philippe Gillet. Et si l'attaque est avérée, l'outil lui livre des informations contextuelles pour l'aider à cerner la nature de la menace et à investiguer. »

Est-ce que ladite menace a déjà été vue ailleurs ? Pour le savoir, Gaia s'interface à des bases de connaissances sur les menaces comme LastInfosec, appartenant à Gatewatcher, ou à une plateforme de *Threat Intelligence* tierce comme celle de Mandiant. L'IA remontera, par exemple, que le *malware* détecté a pour origine un groupe de pirates informatiques affilié à la Russie et cible spécifiquement le secteur industriel. Elle renverra vers une analyse réalisée il y a quelques semaines par des chercheurs australiens.

AUTOMATISER L'ORCHESTRATION DE LA RÉPONSE

Après l'aide à la décision, l'étape suivante porte sur l'orchestration et la remédiation. Quelle série d'actions mener sur le système d'information pour contrer ou tout du moins contenir une attaque jusqu'à ce que les experts interviennent ? Dans le cas d'un *malware* qui a réussi a passé les filtres anti-*phishing*, l'IA décidera de mettre en quarantaine le mail suspect dans les 25 boîtes aux lettres où il a été signalé.

« La réponse ne peut pas être binaire mais multivectorielle et proportionnée afin d'éviter tout arrêt d'activité inopiné, tempère Philippe Gillet. Elle peut se traduire par une nouvelle règle sur le firewall, la fermeture d'un proxy voire le blocage temporaire d'un poste de travail. Si un expert technique est capable de faire des règles sur un firewall, ce n'est pas le cas de tout le personnel IT. Le recours à l'IA permet d'éviter des erreurs humaines qui seraient contreproductives. »

Jusqu'à quel point faut-il laisser la machine autonome dans la réponse ? Tout dépend du niveau de maturité de l'organisation, juge Philippe Gillet. « Dans le SOC d'une grande banque, l'IA restera cantonnée à un rôle de conseil, les experts 'maison' menant eux-mêmes les actions d'investigation et de remédiation. À l'inverse, l'automatisation sera bien accueillie dans le cas d'un hôpital aux ressources cyber, techniques comme humaines, particulièrement contraintes. »

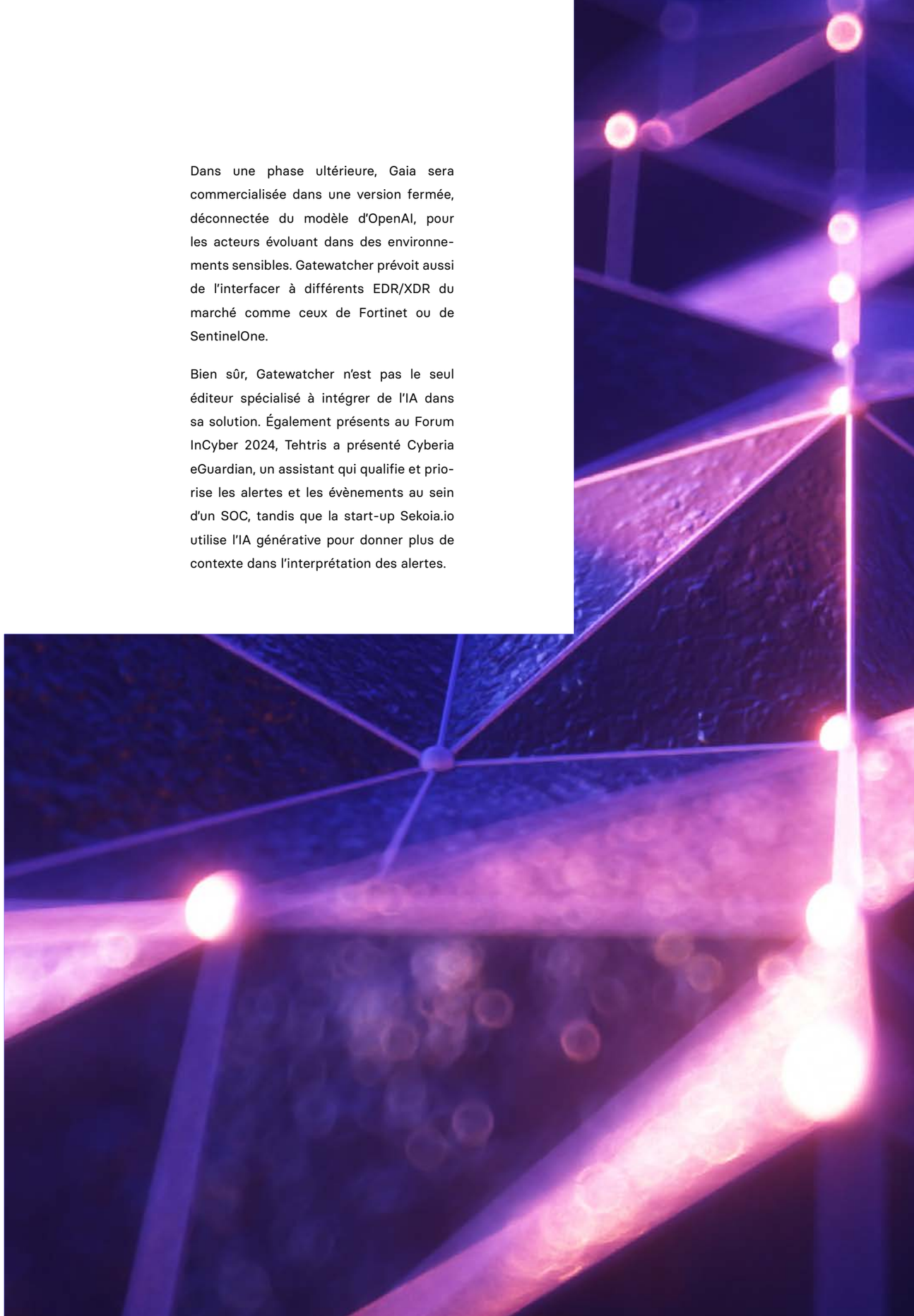
SUGGÉRER UNE STRATÉGIE GLOBALE DE DÉFENSE

Quoi qu'il en soit, l'automatisation maximale va dans le sens de l'histoire selon l'expert. Face à des menaces persistantes avancées (ATP) toujours plus nombreuses et complexes, il faut pouvoir très rapidement mettre en place les mesures qui s'imposent. Faisant le parallèle avec une plateforme qui, comme Palantir, modélise les théâtres d'opérations militaires et aide les armées à agir rapidement sur le champ de bataille, « l'IA va suggérer une stratégie globale de défense en fonction de la nature de la menace et des outils de protection existants. »

De manière plus anecdotique, Gaia va générer automatiquement les reportings et autres tableaux de bord recensant les alertes sur la semaine ou le mois écoulé. Gaia sera proposée en deux phases. Dans un premier temps, l'outil reposera à 10 % sur le grand modèle de langage (LLM) d'OpenAI, le reste étant composés modèles supervisés conçus par Gatewatcher.

Dans une phase ultérieure, Gaia sera commercialisée dans une version fermée, déconnectée du modèle d'OpenAI, pour les acteurs évoluant dans des environnements sensibles. Gatewatcher prévoit aussi de l'interfacer à différents EDR/XDR du marché comme ceux de Fortinet ou de SentinelOne.

Bien sûr, Gatewatcher n'est pas le seul éditeur spécialisé à intégrer de l'IA dans sa solution. Également présents au Forum InCyber 2024, Tehtris a présenté Cyberia eGuardian, un assistant qui qualifie et priorise les alertes et les évènements au sein d'un SOC, tandis que la start-up Sekoia.io utilise l'IA générative pour donner plus de contexte dans l'interprétation des alertes.



Quelles briques pour bâtir une **IA de confiance ?**

par **Patricia Dreidemy** #CYBER+

LIRE L'ARTICLE EN LIGNE

La confiance est la clé de l'adoption et de l'appropriation des technologies, en particulier en matière d'intelligence artificielle. L'*AI Act* la définit comme légale, éthique, robuste et sécurisée.

Mais en quoi consiste une IA de confiance, quelle est la portée de l'*AI Act* et où en est-on aujourd'hui de la nécessaire collaboration entre spécialistes cyber et IA pour instaurer cette confiance ? Plusieurs experts, réunis autour d'une table ronde dans le cadre de la plénière « IA en quête de confiance » du Forum InCyber 2024, ont débattu de ces questions.

Selon Françoise Soulié, conseillère scientifique au Hub France IA, une intelligence artificielle digne de confiance doit être transparente dans ses actions et fiable dans son exécution. Elle doit clairement signaler son identité en tant qu'IA et spécifier ses objectifs ainsi que son niveau de performance. Enfin, elle doit fonctionner en évitant les attaques, distorsions, *deepfake*…

Nozha Boujemaa, vice-présidente *AI Innovation & Trust* chez Décathlon, complète le tableau : « Une IA de confiance se doit d'être robuste, ce qui ne signifie pas forcément performante. On observe des IA performantes mais non fiables. La robustesse implique la transparence, l'interprétabilité, la traçabilité et la reproductibilité. Pour établir la confiance dans une IA, il est crucial d'analyser les risques potentiels tout au long de son cycle de vie, de la collecte des données à leur transformation, la construction des modèles et leur déploiement. Une IA de confiance n'est pas juste du « *good will* », mais repose sur une infrastructure et des outils installés de manière très opérationnelle dans les entreprises et chez les producteurs de services numériques, autant pour les données que pour les modèles. Cela permet l'observabilité et la traçabilité aussi bien des données que des algorithmes, afin d'être capables de détecter toutes les sources de risques et d'y remédier ».

LES CINQ PARTICULARITÉS DE L'*AI ACT*

Emmanuelle Legrand, magistrate spécialisée détachée à la Direction générale des entreprises (DGE), qui a participé aux négociations de l'*AI Act* pour le compte de Bercy, enchaîne sur ce règlement européen, qui comporte, selon elle, cinq grandes caractéristiques. Il instaure des règles contraignantes, – approche assez classique de l'Union européenne –, assorties de sanctions en cas de violation et établit un système de gouvernance définissant les autorités de régulation à désigner et les conséquences des infractions aux obligations légales.

Il n'a pas vocation à régler tous les problèmes de l'IA mais s'inscrit dans une approche de réglementation des produits, considérant l'IA comme un produit commercialisé dans le marché de l'Union européenne et soumis à un certain nombre de conditions. Le texte s'applique aux secteurs public et privé, soulevant un défi en termes de précision des règles pour être opérationnel dans des contextes variés. Il adopte une approche neutre sur le plan technolo-

gique, ciblant les produits incorporant de l'IA et non les technologies elles-mêmes. Enfin, l'*AI Act* repose sur une approche fondée sur le risque, en se concentrant non pas sur les risques intrinsèques de la technologie, mais sur ceux associés à certains usages spécifiques de l'IA. « Cette approche a été annoncée dès 2019 et a été suivie d'un Livre blanc en 2020 et d'une consultation publique. Ce processus a permis à la Commission européenne de définir l'orientation réglementaire finalement retenue », rappelle la magistrate.

Irakli Khodeli, chef de l'unité « Éthique de l'IA » à l'Unesco, relate les travaux menés sur l'IA en termes d'éthique. « Lorsqu'on établit une régulation stricte dans une région du monde, les acteurs ont tendance à se délocaliser dans un autre endroit où la régulation est moins contraignante, affirme-t-il. Un cadre global s'avère donc nécessaire avec les mêmes règles et standards partout. C'est ce que L'Unesco a accompli voilà deux ans. Les 193 membres ont adopté une recommandation sur l'éthique de l'intelligence artificielle. La gouvernance n'était pas le seul enjeu, souligne-t-il. Les bénéfices de l'IA doivent aussi être accessibles aux pays en développement ».

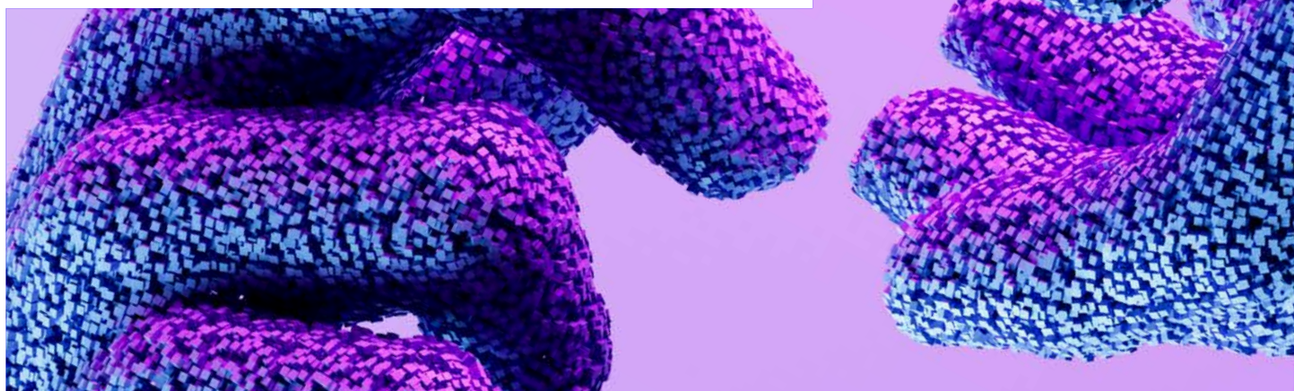
FAIRE COLLABORER LE MONDE DE LA CYBERSÉCURITÉ ET CELUI DE L'IA

Emmanuelle Legrand le précise, dans le but d'étendre les règles du jeu de l'IA au delà de l'Europe, les États du Conseil de l'Europe se sont entendus en mars dernier, avec des partenaires internationaux non membres du Conseil, sur le contenu d'une convention internationale sur l'intelligence artificielle intégrant des règles contraignantes. « De nombreux acteurs, dont les États-Unis, le Canada, la Grande-Bretagne, le Mexique et le Japon, ont participé à son élaboration, raconte-t-elle. Une consultation accrue de la société civile a été intégrée dans le processus, la volonté commune étant de faire bénéficier l'ensemble de la population des bienfaits de l'IA ».

Les intervenants s'accordent sur un point, la collaboration entre experts en cybersécurité et experts en IA est essentielle pour garantir des systèmes d'IA fiables, sécurisés et respectueux des droits fondamentaux. « Les spécialistes de l'IA ont mis en œuvre des applications d'IA dans les entreprises sans jamais se poser la question de leur protection cyber, la considérant comme la responsabilité des experts en cybersécurité. Il en était de même pour les professionnels de la cyber », affirme Françoise Soulié. « Aujourd'hui, on ne peut plus se renvoyer la patate chaude et il faut s'en emparer tous ensemble. En effet, l'IA est protégée comme n'importe quel programme informatique alors qu'elle n'en est pas tout à fait un. Elle peut être attaquée de nombreuses façons : au moment de la collecte des données en les empoisonnant, en perturbant l'apprentissage du modèle, en bloquant un certain nombre d'itérations… Le rapport du NIST sur les attaques adversariales liste toutes les attaques sur l'IA prédictive et quelques-unes sur l'IA générative et donne des pistes de remédiation. Ces attaques sont bien plus complexes que celles connues par les professionnels de la cyber, et il est nécessaire qu'ils travaillent avec les experts de l'IA pour construire les défenses adaptées ».

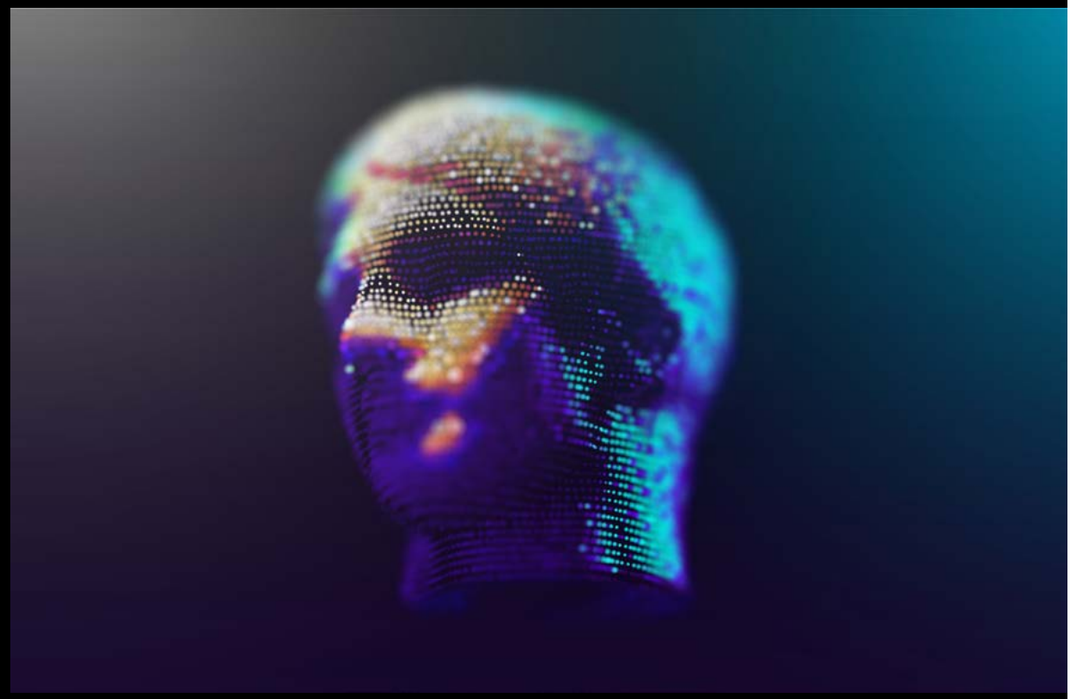
Les spécialistes de l'IA ont mis en œuvre des applications d'IA dans les entreprises sans jamais se poser la question de leur protection cyber, la considérant comme la responsabilité des experts en cybersécurité. Il en était de même pour les professionnels de la cyber Françoise Soulié, conseillère scientifique au Hub France IA.

En fin de conférence, à la remarque « certains pensent que les règlementations ralentissent l'innovation », Emmanuelle Legrand a rétorqué : « il faut arrêter d'opposer le droit et l'innovation, ce qui passe par un changement de mentalité des deux côtés : pour les acteurs, ne pas systématiquement voir une règle de droit comme une contrainte insurmontable et, pour les juristes, essayer de mieux comprendre l'environnement dans lequel ils travaillent, ainsi que les besoins et les limites des technologies sur lesquelles ils ont à intervenir. Concernant l'application de l'*AI Act*, il ne s'agit pas juste d'un texte qui va s'appliquer tel quel, tout le monde aura un rôle à jouer. Les entreprises disposeront d'une certaine marge de manœuvre dans leur domaine pour l'interpréter au plus proche de leurs cas d'usage et de leur activité ». La juriste évoque le rôle des régulateurs dont la responsabilité va consister à en faire une application intelligente, afin que législation et innovation ne s'opposent pas et que l'*AI Act* agisse comme un levier d'innovation et de développement pour les entreprises européennes.



La CNIL et l'IA : comprendre, accompagner et contrôler

par **Fabrice Deblock** #CYBER STABILITÉ



LIRE L'ARTICLE EN LIGNE

À l'occasion de la 16e édition du Forum InCyber, Marie-Laure Denis, présidente de la CNIL, a détaillé l'ensemble des dispositifs mis en place par le régulateur français des données personnelles pour prendre en considération les nombreux enjeux liés à l'IA.

La Commission nationale de l'informatique et des libertés (CNIL) n'a pas attendu l'arrivée de ChatGPT, fin 2022, pour conduire des travaux sur l'intelligence artificielle. Elle est en effet sollicitée depuis des années sur la mise en œuvre de traitement de données personnelles impliquant des technologies d'IA. Cela se traduit dans de très nombreux domaines : diagnostic médical, tri de CV, caméras augmentées… Mais avec l'IA générative, un nouveau palier a été franchi grâce à la combinaison de deux facteurs : l'accès à des volumes massifs de données et la puissance de calcul des ordinateurs.

« Si l'intelligence artificielle générative est encensée par certains, elle est aussi, de façon parfois véhémente, critiquée par d'autres. La CNIL a ainsi été récemment sollicitée sur l'enjeu de l'utilisation des données de ce que je pourrais appeler les "acteurs de la voix", c'est-à-dire les doubleurs, notamment pour l'entraînement des systèmes d'IA. C'est un dossier qui illustre bien la complexité de la régulation en ce qu'elle nécessite d'articuler protection des données personnelles, droit au travail, propriété littéraire et artistique, et droit d'entreprendre », déclare Marie-Laure Denis, présidente de la CNIL.

COMPRENDRE UNE TECHNOLOGIE MAJEURE, NON EXEMPTE DE DÉFAILLANCES

Les inquiétudes exprimées traduisent, comme pour toute nouvelle technologie majeure, la nécessité de créer les conditions d'une utilisation qui soit éthique, responsable et respectueuse des valeurs européennes. « Pour relever ce défi, nous avons mis en place un plan d'action qui doit nous permettre de comprendre le fonctionnement des systèmes d'IA et leurs impacts sur les personnes, de clarifier le cadre légal pour donner de la visibilité aux acteurs du secteur et aux utilisateurs, tout en contrôlant les modalités de mise en œuvre de cette technologie pour protéger tant les personnes physiques que morales des risques qu'elle emporte », complète Marie-Laure Denis.

Le premier pilier de ce plan d'action consiste donc à « comprendre ». Il s'agit pour la CNIL d'un prérequis d'autant plus crucial que les systèmes d'IA sont sujets à des défaillances et à des attaques ou peuvent avoir des conséquences encore insoupçonnées sur les individus ou sur la société.

« Étant donné la complexité des systèmes utilisant l'intelligence artificielle, les sources d'erreurs et de biais peuvent être multiples. Elles peuvent intervenir dès la conception, en raison du manque de représentativité dans les données d'entraînement. Ces erreurs peuvent également résulter des conditions d'utilisation. Par exemple, un système de détection d'incivilités par vidéosurveillance pourra être sujet à plus d'erreurs s'il est déployé sur un parc de caméras dont la résolution est insuffisante », note la présidente de la CNIL.

Là où les systèmes d'intelligence artificielle se distinguent des systèmes informatisés plus classiques, c'est dans les difficultés que pose l'identification du problème, en raison de leur nature statistique. C'est tout l'enjeu de l'explicabilité des décisions proposées ou réalisées par l'IA. « Pour répondre à ces enjeux de compréhension, j'ai créé en 2023 un service dédié à l'intelligence artificielle au sein de la CNIL. Il est actuellement composé de juristes, d'ingénieurs et d'analystes en IA qui développent une expertise pluridisciplinaire. Ce service organise un dialogue régulier avec les fournisseurs de solutions d'IA dans tous les domaines d'application afin de renforcer son expertise et de la diffuser dans tous les services de la CNIL », explique Marie-Laure Denis.

ACCOMPAGNER LE MARCHÉ EN CLARIFIANT LE CADRE LÉGAL

Le deuxième axe du plan d'action mise en œuvre par Marie-Laure Denis et ses équipes est l'accompagnement, qui passe notamment par une clarification du cadre légal. Cette démarche concerne les entreprises, les administrations et les citoyens. Elle doit leur permettre de s'approprier le nouveau cadre légal conçu par le législateur, sous l'impulsion du commissaire européen au Marché intérieur, Thierry Breton.

« En avril 2021, la Commission européenne a fait une proposition de règlement (*AI Act*) qui précise de nouvelles règles pour veiller à ce que les systèmes d'intelligence artificielle utilisés dans l'Union européenne soient le plus sûrs possible, transparents, éthiques, impartiaux et sous contrôle humain. À l'issue des travaux législatifs, les institutions européennes ont convergé vers une classification des systèmes d'IA en fonction de leur niveau de risque. S'ajoute à cela un encadrement des modèles d'IA à usage général, qui concerne tout particulièrement l'IA générative, par exemple à travers une transparence sur les données d'entraînement », rappelle Marie-Laure Denis.

L'*AI Act* est désormais en voie d'achèvement. Le Parlement européen et le Conseil devraient l'adopter formellement dans les semaines qui viennent. Pour autant, le règlement sur l'intelligence artificielle ne sera applicable que deux ans après son entrée en vigueur. Cette période de transition est nécessaire pour permettre aux acteurs concernés de s'adapter. « Malgré tout, les dispositifs d'IA sont déjà utilisés en partie au quotidien. Et les organismes utilisateurs comme les citoyens ont déjà des questions pratiques qui ne peuvent attendre. C'est pourquoi la CNIL se mobilise et essaye d'apporter des réponses concrètes aux entreprises qui utilisent l'IA ainsi qu'aux citoyens qui disposent de droits sur leurs données, droits issus principalement du RGPD », détaille la présidente de la CNIL.

UN ACCOMPAGNEMENT QUI CIBLE LES ENTREPRISES LES PLUS INNOVANTES

La stratégie d'accompagnement de la CNIL s'oriente notamment vers les entreprises les plus innovantes en la matière. Par exemple, la Commission nationale de l'informatique et des libertés a lancé une offre d'accompagnement dite renforcée qui l'a conduite à sélectionner trois entreprises du numérique à fort potentiel, dont la société française Hugging Face, éditrice d'une plateforme open source de ressources en intelligence artificielle.

La CNIL offre en parallèle un accompagnement sur mesure aux fournisseurs de vidéosurveillance augmentée dont les solutions permettent de détecter des comportements suspects, comme une voiture qui arriverait en sens inverse et déclencherait un mouvement de foule. « Nous avons accompagné les fournisseurs de caméras augmentées dans le cadre de l'expérimentation prévue par la loi relative aux Jeux olympiques et paralympiques », note Marie-Laure Denis.

Enfin, à l'issue d'une phase de concertation et de consultation publique, la CNIL a publié sept fiches pratiques relatives à la constitution de bases de données d'apprentissage. Objectif : aider les acteurs à prendre en compte le RGPD. Ce premier lot de fiches sera enrichi d'ici l'été 2024 par un deuxième lot portant sur le développement des systèmes d'IA. « Tous ces travaux poursuivent le même objectif : favoriser les systèmes compatibles avec les valeurs européennes sans entraver l'innovation et l'émergence de nouveaux acteurs français ou européens », commente Marie-Laure Denis.

LA COMPRÉHENSION ET LA CLARIFICATION N'EXCLUENT PAS LE CONTRÔLE

Les phases de compréhension des technologies d'IA et d'accompagnement des organisations ne sont cependant pas suffisantes. « La régulation implique également de disposer d'une capacité à contrôler les technologies d'intelligence artificielle. Pour cela, la CNIL doit disposer de moyens, développer une expertise particulière et définir une méthodologie. Il nous faut aussi un outillage permettant d'auditer les systèmes d'IA, tant *a priori* qu'*a posteriori* », avance la présidente de la CNIL.

Si l'on prend l'exemple des IA génératives comme ChatGPT, les investigations doivent se dérouler à trois niveaux. D'abord au niveau de l'application, c'est-à-dire de la couche « *tchat* » à partir de laquelle les utilisateurs interagissent avec les systèmes d'IA. Il s'agit de s'assurer que les utilisateurs sont informés de la façon dont les données qu'ils soumettent sont traitées.

« Nous devons notamment vérifier que les personnes concernées par les données des bases, même si elles sont disponibles sur Internet, peuvent exercer leurs droits d'accès, de rectification et de suppression », précise Marie-Laure Denis. Enfin, les investigations se déroulent au niveau du modèle sous-jacent. Il s'agit de la couche « GPT », partie la plus complexe à mettre en œuvre pour les modèles déjà entraînés, du fait des milliards de paramètres appris à partir de centaines de millions de textes issus de sources diverses.

« Les droits d'accès et d'opposition à l'utilisation de ces données doivent trouver une traduction concrète et c'est bien sûr

un véritable défi. Les questions abondent donc et la coordination au niveau européen est essentielle. Pour la favoriser, le Comité européen de la protection des données (CEPD), qui réunit les CNIL européennes, a initié plusieurs travaux sur les IA génératives », souligne Marie-Laure Denis.

LA CNIL, ORGANE DE RÉGULATION INCONTOURNABLE DE L'IA

Pour finir sur le sujet de la régulation de l'IA, la présidente de la CNIL a évoqué la question de la gouvernance pour l'application de l'*AI Act*. « La très forte adhérence entre la régulation des systèmes d'IA et celle des données, en particulier des données à caractère personnel, plaide pour que la CNIL ait un rôle important à jouer dans la régulation de ces systèmes. J'ajoute que la réalité du terrain confirme un peu plus chaque jour que la CNIL est et sera incontournable dans la régulation de l'IA, de ses algorithmes et du règlement sur l'intelligence artificielle, complétant un RGPD qui continue à s'appliquer dans toutes ses dimensions », conclut Marie-Laure Denis.

Thierry Breton et l'édification de **l'espace numérique européen**

par **Fabrice Deblock** #SOUVERAINETÉ NUMÉRIQUE

LIRE L'ARTICLE EN LIGNE

À l'occasion de la 16e édition du Forum InCyber, le commissaire européen Thierry Breton est revenu sur les grandes étapes de la construction de l'espace intérieur informationnel en Europe. Une construction dans laquelle la réglementation a joué un rôle central.

« Thierry Breton n'est pas invité au FIC, il y est chez lui » ! C'est par cette phrase enthousiaste que le général Marc Watin-Augouard, fondateur du Forum InCyber, a introduit l'intervention de Thierry Breton, commissaire européen au Marché intérieur, lors de la plénière d'ouverture de la 16e édition de l'événement, qui s'est tenu à Lille du 26 au 28 mars 2024.

Le thème du Forum InCyber était dédié cette année à l'intelligence artificielle *(« Ready for AI? »),* ce qui n'a pas échappé à Thierry Breton : « La thématique de la cybersécurité à l'ère de l'intelligence artificielle met particulièrement l'Europe à l'honneur. Depuis cinq ans, mes équipes et moi-même avons en effet œuvré à bâtir un espace intérieur numérique qui était jusqu'à présent très fragmenté, avec 27 États membres, 27 frontières numériques, 27 lois et autorités nationales et, évidemment, cela ne fonctionnait pas », a-t-il rappelé.

L'EUROPE, PREMIER MARCHÉ NUMÉRIQUE AU MONDE

Thierry Breton a souligné les efforts réalisés par ses services pour mettre en place un véritable marché unique informationnel, grâce à une série de règlements et de directives. « Nous disposons aujourd'hui de la réglementation nous permettant d'organiser cet espace numérique, que ce soit dans la sphère sociale avec le DSA, concurrentielle avec le DMA, sur les données avec le *Data Act* ou l'intelligence artificielle avec l'*AI Act*. Toutes ces lois sont des premières mondiales », a-t-il ajouté.

Le commissaire européen chargé du Marché intérieur a également mis en exergue l'attractivité de l'Europe. Un marché qui est en effet composé de 450 millions de citoyens, soit 1,5 fois plus que les États-Unis, notant au passage qu'il n'y avait rien de surprenant à ce que le premier marché numérique mondial s'organise et se structure tel qu'il l'a fait au cours des dernières années.

L'ESPACE INFORMATIONNEL EUROPÉEN, UN ESPACE « CONTESTÉ » À PROTÉGER

L'espace informationnel européen fait partie, avec les espaces aérien, maritime, spatial et de la cybersécurité, des espaces dits « contestés ». « Ce sont des espaces dont les frontières, qui ne sont pas qualifiées, sont mouvantes. Il s'agit de les protéger dans un autre environnement et avec d'autres moyens que dans l'espace territorial classique », a précisé Thierry Breton.

Pour protéger les entreprises et les citoyens européens, Thierry Breton a notamment mentionné l'existence de la directive NIS, récemment révisée en NIS 2 :

« Cette directive se présente désormais avec un champ modernisé et plus large, des règles beaucoup plus claires et des outils plus adaptés à une surveillance plus robuste. Elle jette les bases sur quelque chose qui est très important : une coopération accrue. Il est en effet nécessaire de créer des coopérations spécifiques en matière de cybersécurité. »

IOT ET *CYBER RESILIENCE ACT*

Le commissaire européen a par ailleurs rappelé le changement de paradigme provoqué par la montée en puissance de l'Internet des objets (ou Internet of Things – IoT). « Nous sommes passés en quelques années d'une surface d'attaque relativement bien localisée, avec des lieux de stockage des données clairement identifiés (*datacenters*), à une prolifération de produits contenant des capacités de traitement de données spécifiques. Réfrigérateurs, sèche-cheveux ou véhicules connectés… Chaque produit devient dès lors un point d'entrée potentiel en matière de cybersécurité », a expliqué Thierry Breton.

C'est dans ce contexte qu'une législation particulière a été mise en œuvre : le *Cyber Resilience Act* (CRA), première réglementation européenne – mais aussi mondiale – permettant de vérifier que chaque produit entrant dans l'Union européenne respecte un certain nombre de spécifications et de qualifications particulières. « Ce n'est pas parce que nous sommes le plus grand continent pour commercer, et de surcroît un continent ouvert, que nous devons être les plus naïfs. Nous imposons désormais le respect de règles à ceux qui veulent bénéficier de notre marché intérieur, en particulier en matière de cybersécurité », a commenté Thierry Breton.

LE MARCHÉ UNIQUE NUMÉRIQUE EUROPÉEN PRÊT POUR LA DEUXIÈME VAGUE D'INNOVATIONS

Thierry Breton a par la suite dessiné les perspectives qu'il entrevoit pour le marché numérique européen : « C'est un marché très prometteur où les mêmes règles s'appliquent désormais à tous. Nous allons maintenant pouvoir bénéficier de toute la profondeur de l'Europe et de ses 450 millions de concitoyens, sans aucune barrière. Le fait qu'il n'y ait aujourd'hui plus qu'un seul régulateur et une seule loi va grandement libérer la capacité d'innovation, notamment celle des start-up ».

Selon lui, l'absence de marché unique numérique explique en partie la raison pour laquelle les Européens ont raté la première vague d'innovations liées à l'exploitation des données personnelles, première vague ayant mené à la création des GAFAM aux États-Unis. « Nous allons pouvoir tirer profit de la deuxième vague d'innovations, qui est celle de la mise en relation, de la mise en connexion et de l'usage des données industrielles. Elle sera encore plus puissante que la première vague, c'est la raison pour laquelle il fallait absolument que ce travail d'uniformisation soit effectué », a déclaré Thierry Breton.

RENFORCER LA SOUVERAINETÉ EUROPÉENNE EN MATIÈRE DE CYBERDÉFENSE

Enfin, Thierry Breton est revenu sur l'importance de la souveraineté européenne en matière de cyberdéfense. « L'Europe doit prendre conscience de sa puissance et assumer davantage de responsabilités en ce qui concerne sa propre sécurité. Certes, nous ne pouvons pas tout faire seuls, mais nous ne pouvons pas non plus dépendre de pays tiers dont les systèmes politiques peuvent changer à chaque élection. Je n'ai par exemple pas envie de jouer notre défense tous les quatre ans à pile ou face en fonction des élections américaines », a-t-il déclaré.

Pour cela, un renforcement du pôle de défense européenne est nécessaire, tout en gardant les spécificités de souveraineté propres à chaque État membre. « Ce renforcement passe par le développement et le déploiement de l'ensemble des capacités de cyberdéfense, avec un renforcement de la coopération civilo-militaire, qui est très importante. Nous avons créé un corps d'experts mobilisables. Mais disposer de ses propres spécialistes est difficile : il faut recruter des compétences, leur proposer des plans de carrière et des salaires attractifs », a conclu Thierry Breton.

Comment assurer **la sécurisation des modèles d'IA ?**

par **Xavier Biseul** #GESTION DES RISQUES

LIRE L'ARTICLE EN LIGNE

L'essor de l'intelligence artificielle, et tout particulièrement de l'IA générative, crée de nouvelles vulnérabilités. Les systèmes de protection conventionnels doivent être complétés par des dispositifs techniques et organisationnels spécifiques. Le futur cadre réglementaire et normatif livrera aussi un ensemble de bonnes pratiques aux entreprises concernées.

L'intelligence artificielle a pris une place prépondérante dans nos vies. Dans la sphère personnelle comme professionnelle, les algorithmes influent sur nos décisions, voire les prennent à notre place. L'impact est mineur quand l'IA vous recommande les films à regarder sur une plateforme de streaming. Il l'est moins quand elle décide ou non de retenir votre candidature à un emploi ou rejette votre demande de prêt bancaire.

Longtemps cantonnée aux laboratoires de recherche, l'intelligence artificielle est, par ailleurs, désormais accessible au plus grand nombre, tout particulièrement depuis le tournant pris avec l'IA générative il y a un an et demi. Si elle est source d'innovation et de gains de productivité, l'IA introduit aussi de nouveaux risques d'ordre sécuritaire, juridique ou réputationnel.

« Alors que l'informatique « traditionnelle » suit un raisonnement déterministe avec un ensemble de règles bien défini, ce n'est pas le cas de l'IA », fait observer Hervé Le Jouan, associé cybersécurité au fonds de capital-risque SevenTrainVentures. Ce qui met en lumière, selon lui, un enjeu de transparence et d'explicabilité des modèles afin d'éviter l'effet boîte noire. Comment évaluer les risques propres à l'IA ? Comment encadrer son usage par des normes et des standards ?

COMMENT GÉRER UNE IA QUI ÉVOLUE EN PERMANENCE ?

Un parterre d'experts, réunis fin mars, lors d'une table ronde au Forum InCyber de Lille ont tenté de répondre à ces questions. PDG fondateur d'EazyML, qui édite une plateforme de développement de modèles de *machine learning,* Deepak Dube estime que l'essor de l'IA présente un saut dans l'inconnu. « Comment gérer une IA qui évolue en permanence et se comporte de façon quasi autonome en s'autorégulant ? C'est un vrai défi en termes de sécurisation et de normalisation. »

Directeur cybersécurité et management produits chez Stormshield, éditeur français de logiciels spécialisés en sécurité informatique, Sébastien Viou propose d'aborder le sujet de façon pragmatique. « Un modèle IA reste un programme qui présente des vulnérabilités classiques même s'il est plus complexe et spécifique. Il s'agit donc de sécuriser toute la chaîne de traitement comme on le fait pour un logiciel courant. Statistiquement, Il y a un bug toutes les mille lignes de code. Cela ne change pas avec l'IA. »

Directeur adjoint de la sécurité au sein de la société d'assurances AXA, Patrick Menez abonde dans son sens.

« Nous ne partons pas de zéro. Les modèles d'IA sont entraînés et exécutés sur des infrastructures connues. Les systèmes de protection conventionnels continuent à s'appliquer. »

En revanche, les conséquences potentielles d'une vulnérabilité prennent une tout autre dimension. « Imaginez le volume de données compromises dans le cas d'une fuite de données d'un grand modèle de langage ? », interroge-t-il. L'IA présente, par ailleurs, de nouvelles vulnérabilités. Dans le domaine de l'IA générative, la technique dite de « prompt injection » permet de contraindre un LLM *(Large language model)* à générer du contenu indésirable, trompeur ou toxique en désactivant ses protections naturelles.

IMPLIQUER LES EXPERTS MÉTIERS, FORMER LES COLLABORATEURS

Sébastien Viou préconise d'introduire de nouvelles étapes de sécurisation propres à l'IA. « Un modèle sera, par exemple, formé sur un échantillon de données afin de s'assurer que le jeu de données dans son ensemble n'est pas compromis. » « Le fait de s'intéresser à la qualité des données n'est jamais une perte de temps, confirme Deepak Dube. Au contraire, cela évite les allers-retours quand il s'agit de collecter de nouvelles données car le premier *data set* n'était pas fiable. L'amélioration en continu des données est indispensable. »

Pour Sébastien Viou, l'effort de sécurisation accrue qu'exige l'IA ne doit pas se limiter aux seules équipes cyber mais impliquer les *data scientists* et les experts métiers.

« Seuls les sachants savent quelles données utiliser et alerteront en cas de dérive du modèle ». Pour sa part, AXA a formé ses équipes IT spécifiquement à l'évaluation et à la gestion des risques liés à l'IA et mis en place un cadre de gouvernance pour encadrer les usages en interne autour de l'IA.

« Toutes les fonctions travaillent de façon coordonnée avec des responsabilités bien définies, explique Patrick Menez. C'est une liberté contrôlée. Nous les laissons développer et expérimenter autour de l'IA mais au sein de frontières bien délimitées. » AXA sensibilise également ses collaborateurs au bon usage de l'IA générative. « L'IA réagit différemment selon ce qu'on lui donne à manger, à savoir les prompts. »

Deepak Dube plaide, de son côté, pour recourir à une IA responsable, transparente et explicable. « Nous devons pouvoir expliquer comment, à partir de telles données en entrée, un modèle algorithmique obtient tel résultat en sortie. » Reprenant le fameux cas d'école du véhicule autonome causant un accident mortel, il estime que l'IA doit avoir la capacité d'indiquer, par exemple, que le drame a été provoqué par le système de freinage rendu déficient en raison du verglas sur la chaussée.

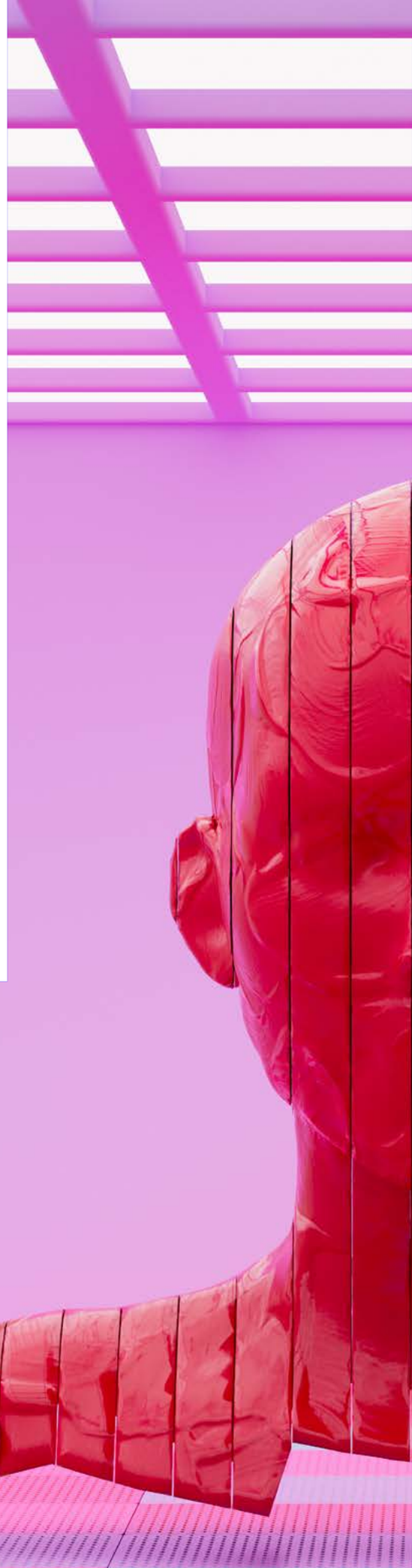
EN ATTENDANT L'*AI ACT*...

Pour les experts réunis lors de la table ronde, les exigences du futur cadre réglementaire et normatif permettront de structurer les politiques de sécurisation actuelles. Le travail de mise en conformité à l'*AI Act*, prévu pour entrer en vigueur début 2026, offre d'ores et déjà un ensemble de bonnes pratiques aux entreprises.

En lien étroit avec le futur règlement européen, l'Afnor a engagé un travail de normalisation.

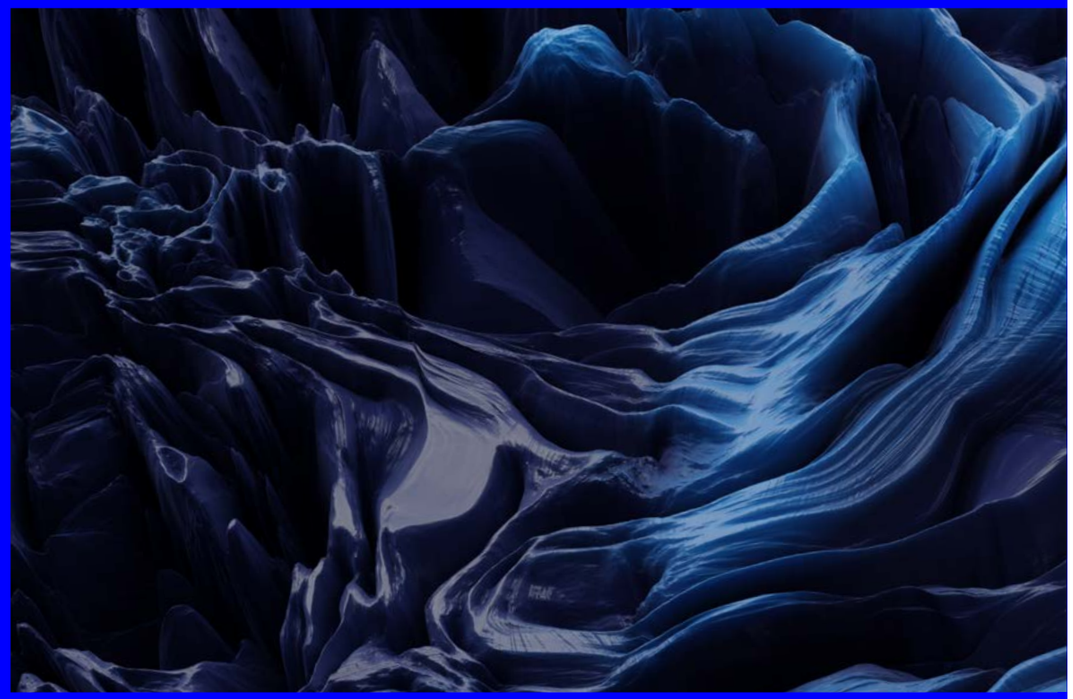
En attendant cette future norme dédiée à l'IA, Anna Prudnikova, Cybersecurity Manager chez Bureau Veritas, rappelle que les entreprises peuvent d'ores et déjà s'appuyer sur les standards existants sur la sécurité des systèmes d'information (ISO 27001, ISO 9001). « Les acteurs de la santé, de l'industrie ou de la finance peuvent aussi appliquer les réglementations et les normes propres à leur domaine d'activité ».

Tous les participants à la table ronde s'accordent à dire que ce cadre réglementaire et normatif ne doit pas être un frein à l'innovation. Patrick Menez y voit également un enjeu de souveraineté. « Les normes mettent en forme la façon dont on utilise les technologies. Elles modèleront le futur de l'IA. Ne laissons pas les GAFAM ou les géants asiatiques nous imposer leur vision de l'IA ». Un enjeu qui dépasse le seul terrain de la cybersécurité.



PhilosoFIC : les algorithmes génératifs, fossoyeurs ou accélérateurs de l'intelligence humaine ?

par **Olivier Parent** #TRANSFORMATION NUMÉRIQUE



LIRE L'ARTICLE EN LIGNE

L'ère de l'intelligence artificielle (IA) interroge sur la distinction entre l'intelligence humaine et l'intelligence artificielle. C'est autour de cette thématique cruciale que s'est tenue la table ronde « PhilosoFIC : Pensée artificielle ou pensée humaine ? Notre intelligence à l'épreuve de l'IA », lors du Forum InCyber 2024. De constats en réactions, d'objectivités en perceptions, voici une réflexion issue de ces 90 minutes d'échanges.

La démocratisation de l'accès aux outils à base d'IA est une révolution en soi. Mais l'arbre ne doit pas cacher la forêt car ces mêmes systèmes existaient bien avant la mise en ligne de ChatGPT. Dans les faits, la révolution que nous sommes en train de vivre tient dans le passage de systèmes d'intelligences artificielles prédictives (principalement utilisés dans des cadres professionnels, donc restreints) à d'autres outils en accès libre, utilisant des algorithmes génératifs, non déterministes, donc aux fonctionnements obscurs. En soi, ce seul aspect – la boîte noire dont on ne comprend pas le fonctionnement – représente un enjeu à part entière : doit-on accepter de dépendre de tels systèmes ?

Il existe un autre système génératif et complexe dont on ne comprend pas non plus tous les fonctionnements : le cerveau humain. Cette similarité autorise-t-elle à confondre intelligence artificielle et intelligence humaine (biologique), sachant qu'à ce jour, il existe encore au moins un « propre de l'humain », c'est sa capacité à s'extraire de son raisonnement, sa capacité à l'observer, à l'expliquer ? Réflexivité et abstraction, Descartes a résumé tout cela dans son *Cogito ergo sum*.

Cette capacité donne aux humains un énorme avantage sur les IA : elle leur permet d'éviter les « hallucinations » dont sont toujours victimes les systèmes génératives artificiels : n'ayant pas conscience de ce qu'ils produisent, ils sont incapables d'écrire un lipogramme, un texte dans lequel l'auteur s'impose de ne pas utiliser une lettre particulière – exemple anecdotique mais qui a le mérite d'être clair – ou bien encore, ils génèrent des images d'humains dotés de mains à six doigts – erreur embêtante mais utile pour « débunker » un *deepfake* – et, en l'absence d'informations objectives, ils génèrent des contenus sans aucune connexion avec le réel, donc du « faux » – plus embêtant voire grave. Ces exemples révèlent ainsi que le choc de l'intelligence artificielle générative dans nos sociétés modernes est avant tout un (r)appel à ne jamais cesser de s'interroger sur la nature humaine et le réel.

CONSÉQUENCE DE L'IA ET ACCÉLÉRATIONS DE L'ÉVOLUTION DES SOCIÉTÉS HUMAINES

Depuis 2022 et la démocratisation de l'accès aux systèmes génératifs, l'accélération de la démocratisation de l'accès aux données et de leur traitement par ces systèmes experts interroge la valeur même des productions humaines.

Une autre accélération : la productivité. Elle a fait monter la peur du « grand remplacement » du travail humain par celui des machines. Dans les faits, il semblerait que ce soit une toute autre réalité qui soit en train d'émerger. En effet, à l'usage de l'IA, il serait constaté que l'égalisation des compétences se fasse par le haut. Car ce sont les moins compétents, les moins bien formés de « l'ancien monde » qui bénéficieraient le plus des avantages procurés par l'intelligence artificielle.

Alors, en ce début de XXIe siècle, l'usage de l'IA va-il se révéler un puissant moyen d'enseignement ? L'ère de l'IA, tel qu'il semblerait que nous la vivions, pourrait-elle donner accès à de nouveaux moyens de réduire les inégalités par un bon usage de la connaissance ? Il semblerait qu'à l'heure de l'hyper personnalisation des services et d'une archipélisation de la société jusqu'à l'échelle de l'individu, l'IA puisse offrir des systèmes d'enseignement adaptés à chaque membre de la société *(IA mentoring)*.

QUESTIONNEMENTS ÉTHIQUES ET ONTOLOGIQUES

Au-delà de l'idéal d'enseignement – l'utopie ? – cité plus haut, quels pourraient être les autres avantages apportés par l'IA à l'humanité ? Ces systèmes aujourd'hui gratuits vont-ils permettre de remplacer des systèmes complexes et payants ? Ne s'agirait-il que de gagner en efficacité ? Et combien de temps ces systèmes vont-ils rester gratuits ? En effet, il y a de fortes chances que les systèmes d'IA finissent par répliquer les modèles économiques mis en place sur Internet : « Si c'est gratuit, c'est que vous êtes le produit » pour, en définitive, être incité à acheter des services dont les usagers ont été les modèles.

Il faut aussi rappeler que, du côté humain, les outils forment l'intellect. Ou, version plus pessimiste de cette affirmation, les outils formatent le raisonnement. Cette interrogation sur les conséquences de l'outil sur la matière enseignée est d'autant plus cruciale que, les outils d'IA se mettent à utiliser les biais et autres travers propres à l'humain. Souvenez-vous de ces images de nazis noirs générées par Gemini. Comment alors s'assurer d'une garantie d'évaluation objective des matières enseignées à l'humanité du futur ?

CONSIDÉRATIONS LÉGISLATIVES ET RÉGLEMENTAIRES

Toutes ces questions reviennent à s'interroger sur les possibles actions à mener sur le marché, trame sur laquelle se construisent ces systèmes. Un des moyens d'action revient alors à se tourner vers la démarche réglementaire. En Europe, les parlementaires se sont attachés à proposer un contrôle de l'intelligence artificielle afin que celle-ci soit utile au plus grand nombre. Il s'agit de donner du sens aux fonctions des IA, ne serait-ce que par un classement des risques liés à leur usage, pour que chacun puisse agir en connaissance de cause.

Cette démarche est aussi l'occasion d'aller voir au-delà de nos frontières, les différentes normes aux États-Unis ou en Chine. Ainsi, autour de l'IA, on retrouve les grands mouvements idéologiques qui particularisent ces nations, entre « libéralisme à tout crin » et « libre entreprise sous (fort) contrôle d'État ».

Sous la forme de l'*AI Act*, la réponse européenne est-elle la bonne ? L'avenir nous le dira.

Se pencher sur la démarche législative permet aussi de rappeler que la loi a une histoire. Ainsi, les questions levées par l'usage de l'intelligence artificielle n'appellent pas systématiquement de nouvelles réglementations. Le corpus actuel des lois offre un cadre déjà bien garni, ne serait-ce parce que la contrefaçon n'a pas commencé avec l'IA. Parce que les lois sur le journalisme et celles sur les droits d'auteur doivent être « convoquées » en première instance contre les usages abusifs liés aux intelligences artificielles. Il faut ensuite évoquer les lois qui protègent le droit à l'image, celles contre la diffamation et l'usurpation d'identité.

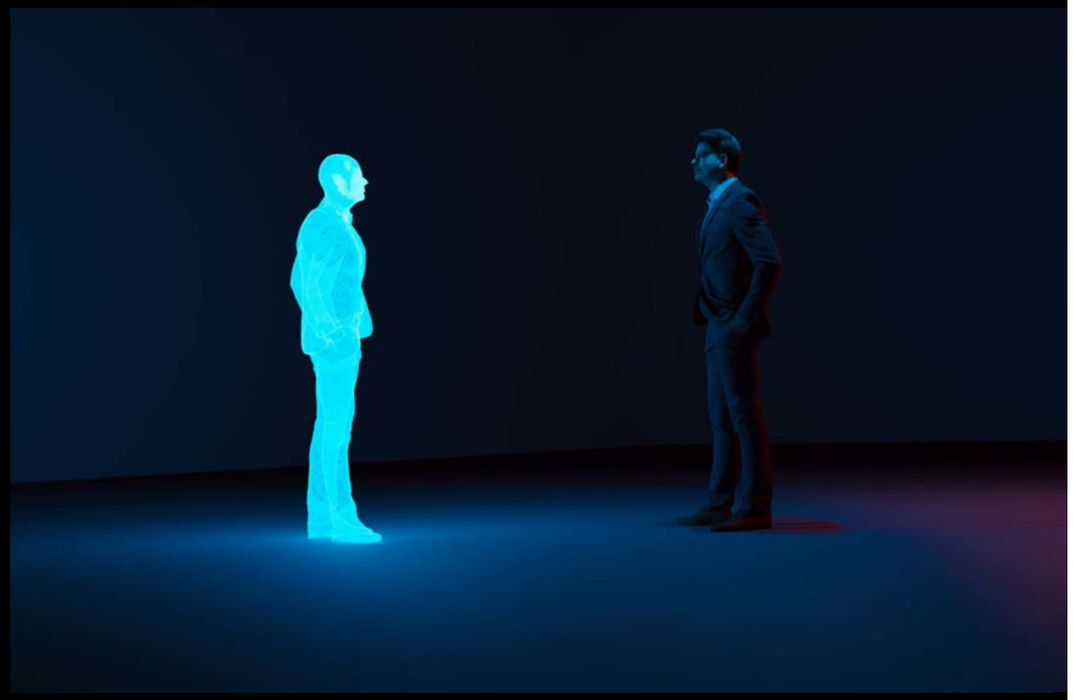
INTÉGRATION DE L'IA : DÉFIS SOCIAUX ET PERSPECTIVES

Cette démarche réglementaire invite à nous interroger sur la responsabilité des opérateurs des systèmes d'intelligence artificielle. Cette interrogation n'est pas sans rappeler celle de la responsabilité des opérateurs de réseaux sociaux. Peut-être que le cadre réglementaire qui régit, en Europe, ces derniers pourront inspirer ce qu'il faut mettre en place pour encadrer les usages de l'IA, à moins que le cadre des réseaux sociaux puisse être étendu aux usages de l'IA.

De questions éthiques en interrogations technologiques, de questions d'usage en interrogations réglementaires, le numérique et la dématérialisation de nos sociétés modernes, les réseaux sociaux et les intelligences artificielles nous ont, dans les faits, invités à nous interroger sur ce qui en définitive nous permet de faire société. Au temps de l'artificialisation du réel, ne serions-nous pas en train de créer une nouvelle société ?

L’IA est-elle soluble dans la **philosophie ?**

par **Fabrice Deblock** #CYBER+



LIRE L’ARTICLE EN LIGNE

Malgré ses avancées fulgurantes, l’intelligence artificielle ne sera jamais capable d’égaler ou de remplacer la pensée humaine, et donc de philosopher. Telle a été la thèse développée par le philosophe Raphaël Enthoven lors du Forum InCyber 2024.

L’intelligence artificielle s’immisce dans tous les secteurs d’activité. Selon Elon Musk, le patron de Tesla, SpaceX, Neuralink et X (ex-Twitter), qui s’exprimait au salon Vivatech, l’IA pourrait remplacer à moyen terme tous nos emplois. Une prédiction qui ne choque pas Kristalina Georgieva, la directrice du Fonds Monétaire International (FMI). En mai dernier, elle a qualifié l’IA de « véritable tsunami » qui viendrait frapper le marché du travail.

Face à cette révolution en marche, chacun d’entre nous est en droit de se poser un certain nombre de questions : jusqu’où peut aller l’intelligence artificielle ? Quelles sont en quelque sorte ses limites ? Est-elle capable de penser, de raisonner ? L’IA est-elle plus forte que l’être humain ? Et si l’on élargit le champ de vision : les machines sont-elles en mesure, un jour, de nous remplacer ?

UN MATCH « DISSERTATION DE PHILO » REMPORTÉ HAUT LA MAIN PAR LE PHILOSOPHE

Ces questions ont été abordées lors de la 16e édition du Forum InCyber qui s’est tenue à Lille en mars dernier. Elles l’ont été par Raphaël Enthoven, philosophe, écrivain, journaliste et animateur de radio et de télévision, lors d’une intervention pendant la séance plénière d’ouverture. Le philosophe s’est ainsi demandé si l’IA était capable de philosopher.

« Le champ d’application de l’IA paraît infini. Que ce soit dans les sciences dures, les sciences humaines, le droit, le recrutement, l’éducation nationale, l’armée, les finances, l’IA est partout et son omniprésence est irréversible. Mon propos n’est pas de nier l’importance d’une telle révolution. Mais, en philosophie, l’IA ne sert littéralement à rien », a affirmé l’auteur de « L’esprit artificiel », son dernier essai.

Il faut dire que sur ce sujet de la capacité de l’IA à philosopher, Raphaël Enthoven n’en est pas à son coup d’essai. Il y a un an, il a affronté ChatGPT lors d’un « match » organisé par une école de commerce. Le sujet de la dissertation était un de ceux proposés dans le cadre de l’épreuve du bac de philo 2023 : « Le bonheur est-il affaire de raison ? ». Pour départager les deux protagonistes, Éliette Abécassis, normalienne et agrégée de philosophie, et Lev Fraenckel, professeur de philosophie, se sont prêtés au jeu de la notation. Résultat des courses : ChatGPT a obtenu 11/20 et Raphaël Enthoven 20/20.

« La copie de ChatGPT n’était ni faite, ni à faire. Il n’y avait rien, c’est-à-dire qu’il manquait dans cette copie l’atome de pensée qu’on appelle la problématique, le petit pas de côté, la petite bifurcation qui nous permet de mettre la main sur un problème, de le manifester, et par là même, de donner le sentiment qu’on ne raisonne pas par hasard, mais qu’il y a une nécessité à ce

que nous disons. Eh bien cela, la machine en est incapable », a ainsi commenté Raphaël Enthoven.

Le philosophe en a également profité pour rappeler que l'échec de ChatGPT n'était pas dû à des capacités technologiques pour le moment insuffisantes, qui ne nécessiteraient qu'un peu de temps pour être atteintes puis dépassées.

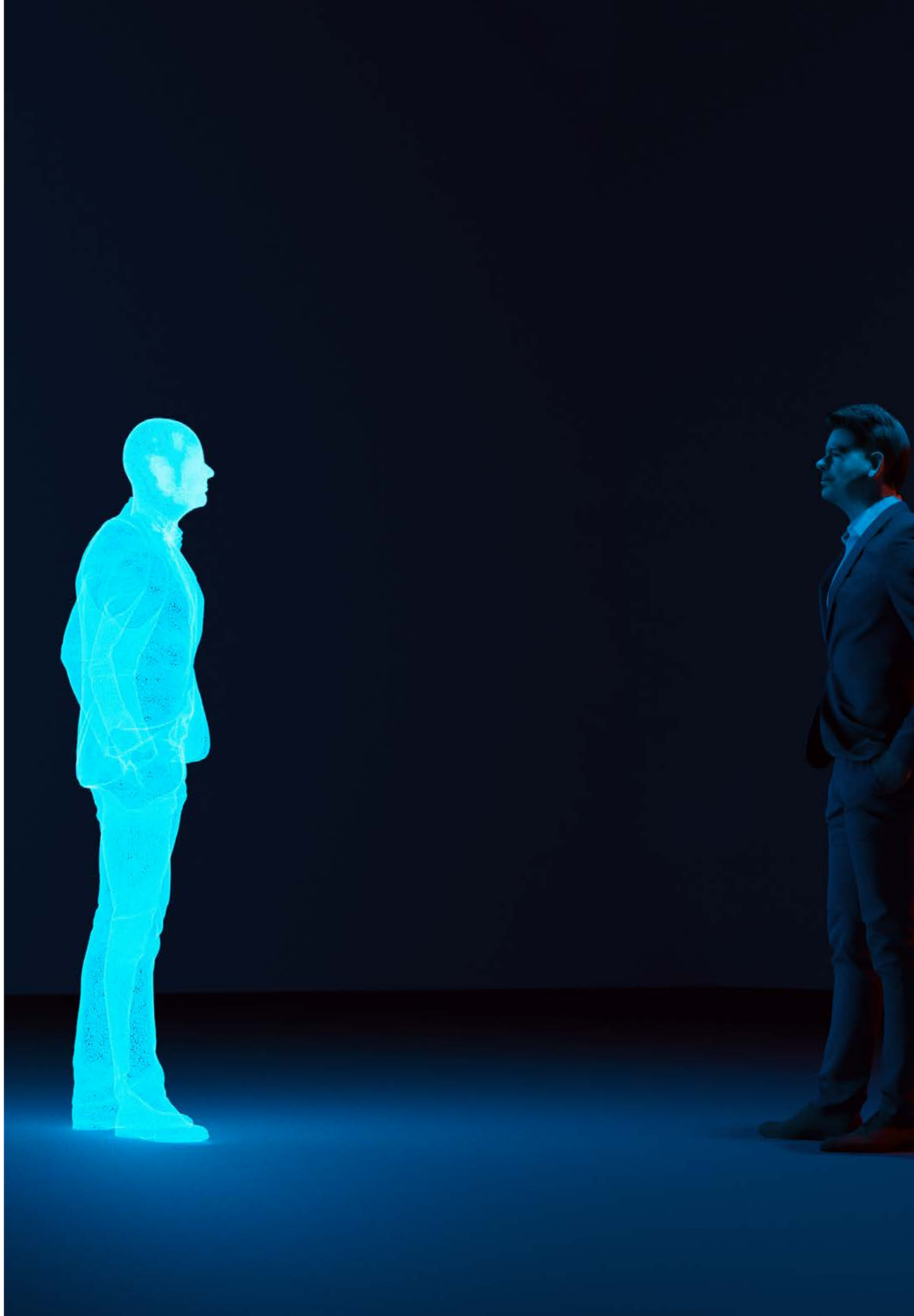
« Ce qui nous sépare de la machine n'est pas une affaire de complexité. Non, ce qui nous sépare de la machine, c'est que la nécessité de penser s'est imposée à nous. Pourquoi ? Parce que nous faisons l'expérience, quand on est en vie, d'une existence qui se dissout et qui, par la même, nous livre à l'angoisse. Parce que nous faisons l'expérience de la liberté, l'expérience du déplaisir, parce que nous sommes vivants. Ce qui nous force à penser, ce qui nous fait penser, ce qui nous impose de penser, c'est le désarroi d'être en vie, d'être présent, d'être ici. Or, c'est précisément ce que la machine n'éprouve pas », a ajouté Raphaël Enthoven.

LA MACHINE EST-ELLE PLUS FORTE QUE L'HUMAIN ? UNE ÉVIDENCE ET UNE ABSURDITÉ...

Autre question existentielle posée par le philosophe lors de son intervention : « La machine est-elle plus forte que l'humain ? ». À cette interrogation, Raphaël Enthoven a répondu qu'il s'agissait à la fois d'une évidence et d'une absurdité. « La machine est depuis toujours plus forte que l'homme, puisque l'homme ne l'a forgée que pour surmonter ses propres incapacités. Le cheval est plus fort que l'homme, l'ordinateur a plus de mémoire qu'un humain, ceci ne pose aucun problème. En revanche, s'il s'agit de dire que l'intelligence artificielle met en échec l'intelligence humaine, alors une telle évidence devient un non-sens complet », a analysé Raphaël Enthoven.

L'exemple du champion du monde d'échecs Garry Kasparov battu en 1996 par le supercalculateur Deep Blue conçu par IBM est encore dans la mémoire de très nombreux observateurs. « Suite à cette partie perdue, nous pourrions nous dire que la machine est plus forte que l'homme. Mais Kasparov n'a pas été battu par un joueur d'échecs, il a été battu par une usine dont la puissance de calcul était infiniment supérieure à la sienne ! La défaite de Kasparov face à Deep Blue a autant de valeur que la défaite d'un catcheur professionnel face à un robot. Le métal est plus solide que le muscle. Cela n'en fait pas une crise du muscle. Nous ne sommes pas menacés de cette façon », a déclaré l'écrivain.

En guise de conclusion, Raphaël Enthoven nous a enjoint à travailler sur les limites de l'IA, c'est-à-dire sur ce dont l'IA n'est pas capable. « C'est notre humanité qui se joue là. L'humanité est d'une étoffe que la machine peut reproduire, mais qu'elle ne peut pas synthétiser. On peut créer un automate qui vous imite à la perfection. Mais l'impulsion natale, qui donne le jour à l'individu singulier, qu'on imite ensuite, est hors de portée de toute intelligence artificielle. L'humanité est ainsi faite, et la vie est ainsi faite, qu'on ne fait pas de l'esprit avec des atomes et qu'on ne fait pas de la conscience avec un cerveau de silicium ».



L'*AI Act*, un texte politique majeur

par **Fabrice Deblock** #TRANSFORMATION NUMÉRIQUE

LIRE L'ARTICLE EN LIGNE

Approche par les risques, valorisation de l'innovation, mais aussi défense de nos valeurs, principes et libertés, mise en avant de normes européennes... L'*AI Act* apparaît, à la suite du RGPD, comme l'une des réglementations majeures produites par l'UE.

Adopté à l'unanimité par les ministres de l'Union européenne en mai dernier, l'*AI Act* constitue le tout premier cadre de régulation entièrement dédié à l'intelligence artificielle au monde. Parmi ses nombreuses caractéristiques, ce texte repose sur une approche par les risques comportant trois niveaux : les systèmes d'IA à risque minimal, limité et élevé. Un quatrième niveau, jugé « inacceptable », entraîne l'interdiction pure et simple des systèmes concernés (par exemple, les systèmes de notation sociale).

« Cette approche par les risques est similaire à celle introduite par le Règlement général sur la protection des données (RGPD). Avec ce classement de l'intelligence artificielle par les risques, la Commission européenne n'a pas voulu freiner l'innovation et le développement des usages, qui sont déjà bien présents. Elle souhaite néanmoins les encadrer pour valoriser le respect de nos droits fondamentaux et éviter les biais de discrimination », déclare Garance Mathias, Avocate associée chez Mathias Avocats, qui a participé à une table ronde intitulée « Intelligence artificielle : la course à la régulation » lors de l'édition 2024 du Forum InCyber. Elle débattait avec Yann Bonnet, Deputy CEO du Campus Cyber, Rayna Stamboliyska, CEO de RS Strategy et Bertrand Pailhès, Directeur des technologies et de l'innovation de la CNIL.

L'approche par les risques est en revanche un des rares points que les deux textes ont en commun. « Ce ne sont pas du tout les mêmes types de texte. Les champs d'application, ainsi que les périmètres, sont différents. Le RGPD est tourné vers les citoyens, c'est-à-dire vers le respect de leurs droits, alors que cette nouvelle réglementation sur l'intelligence artificielle est orientée vers l'innovation, les produits, les services », complète Garance Mathias.

LA LOI INFORMATIQUE ET LIBERTÉS PUIS LE RGPD ONT PRÉPARÉ LE TERRAIN

L'*AI Act* ne vient cependant pas de nulle part, n'apparaissant pas subitement sur une terre réglementaire complètement vierge. Au sein de l'Union européenne, d'autres textes ont, avant lui, abordé les questions relatives à l'intelligence artificielle, de manière directe ou indirecte. C'est le cas, en France, de la Loi Informatique et Libertés (1978), puis, à l'échelle de l'UE, du RGPD (2018).

« Dès la fin des années 1970, en France et dans de nombreux autres pays européens, des lois ont été conçues pour réguler les traitements de données. Pour faire simple, un traitement de données, cela ressemble à un algorithme.

Et l'IA représente la dernière génération des algorithmes, dont certaines propriétés statistiques induisent de nouveaux risques, comme la création de biais. Un cadre juridique s'applique donc aux traitements de données depuis longtemps, que ce soit pour les entreprises qui les utilisent ou celles qui les développent », rappelle Bertrand Pailhès (CNIL).

RGPD ET *AI ACT* : QUELQUES AJUSTEMENTS NÉCESSAIRES

Avec la publication au Journal Officiel de l'Union européenne de l'*AI Act*, se pose désormais la question de la compatibilité des deux textes (RGPD et *AI Act*). Après plusieurs mois de consultations, la CNIL a publié en avril et en juin 2024, ses recommandations sur l'application du RGPD au développement des systèmes d'intelligence artificielle pour aider les professionnels à concilier innovation et respect des droits des personnes.

« Nous avons publié un premier lot de documentation, puis un deuxième, notamment pour montrer qu'un certain nombre de principes du RGPD, qui étaient vus comme contradictoires avec l'*AI Act*, ne le sont pas du tout. C'est le cas entre autres des principes de finalité et de minimisation des données », note Bertrand Pailhès.

Le principe de minimisation n'empêche pas, selon la CNIL, l'entraînement d'algorithmes sur de très grands ensembles de données. « Les données utilisées doivent en revanche, en principe, avoir été sélectionnées pour optimiser l'entraînement de l'algorithme tout en évitant l'utilisation de données personnelles inutiles.

Dans tous les cas, certaines précautions pour assurer la sécurité des données sont indispensables », précise la CNIL sur son site.

Quant au principe de finalité, il s'applique, lui aussi, de manière adaptée, aux systèmes d'IA à usage général. « Le principe de finalité impose de n'utiliser des données personnelles que pour un objectif précis (finalité) défini à l'avance. En matière d'IA, la CNIL admet qu'un opérateur ne puisse pas définir au stade de l'entraînement de l'algorithme l'ensemble de ses applications futures, à condition que le type de système et les principales fonctionnalités envisageables aient été bien définies », ajoute la CNIL, qui a publié une série de fiches pratiques sur l'IA pour y voir plus clair.

UNE OPPOSITION ENTRE INNOVATION ET RÉGULATION VRAIMENT FERTILE ?

L'opposition entre innovation et régulation a été un autre grand défi à relever pour les institutions européennes à l'origine de l'*AI Act*. Les forces en présence (lobbies, associations…) ont en effet été très actives pour tenter d'imposer des points de vue la plupart du temps inconciliables.

« Dans le débat, on a beaucoup entendu parler de cette opposition entre innovation et régulation, et je ne sais pas si elle est très fertile. En réalité, l'IA est à la fois un remède et un poison pour notre société. L'IA en soi n'est pas mauvaise, ce sont ses usages qu'il faut surveiller. C'est donc un choix politique de réguler certains cas d'usage – comme la possibilité de réaliser un scoring social – qui ne correspondent pas à nos principes et à nos libertés », analyse Yann Bonnet (Campus Cyber).

Autre enjeu, et non des moindres : la sécurité de l'IA. « L'IA ne date pas d'hier, mais avec la fulgurance du phénomène ChatGPT, ce sont aujourd'hui des millions de personnes qui utilisent des outils qui, parfois, n'ont pas été complètement réfléchis, même d'un point de vue cybersécurité. Il y a toute une partie de la sécurisation de l'IA qui n'est pas pensée. Nous n'arrivons même pas à trouver des chercheurs dans ce domaine. En tant qu'experts en cybersécurité, nous allons donc devoir fixer un certain nombre de règles, de principes, afin que ces nouveaux outils ne se retournent pas contre nous à un certain moment », note Yann Bonnet.

LA RÉGLEMENTATION DE L'IA COMME ARME GÉOPOLITIQUE MAJEURE

La réglementation sur l'IA est par ailleurs un outil de géopolitique très puissant. « Aux États-Unis, ils sont en guerre économique avec la Chine. On est dans un autre contexte. Ils possèdent des acteurs dominants, les géants de la tech, qu'ils veulent protéger. Mais à force de multiplier les déclarations non-contraignantes, sans approche globale, des lois vont se développer au niveau des États fédérés. Il serait assez piquant d'assister, dans quelques mois ou années, à une fragmentation des cadres réglementaires au niveau des différents États, situation qui d'ailleurs a été reprochée à l'Europe pendant des années. Si cela venait à se produire, l'Europe aurait en main un sacré différenciateur par rapport aux États-Unis », commente Rayna Stamboliyska (RS Strategy).

En Chine, la régulation de l'IA avance également à grands pas, les Chinois ayant lancé en août 2023, 24 nouvelles règles visant à encadrer les contenus générés par l'IA générative. « Les Chinois sont, eux aussi, en guerre économique, contre les Américains. Ils ont également ce souhait de protéger leurs gros acteurs, les BATX. Leur approche de régulation est beaucoup plus agile, ciblée et sectorielle. Mais nous sommes en Chine, la réglementation est directement dictée par le Parti communiste chinois aux grandes entreprises, avec une volonté de maîtriser la population via une certaine surveillance de masse, ce qu'on ne peut absolument pas souhaiter en Europe », ajoute Rayna Stamboliyska.

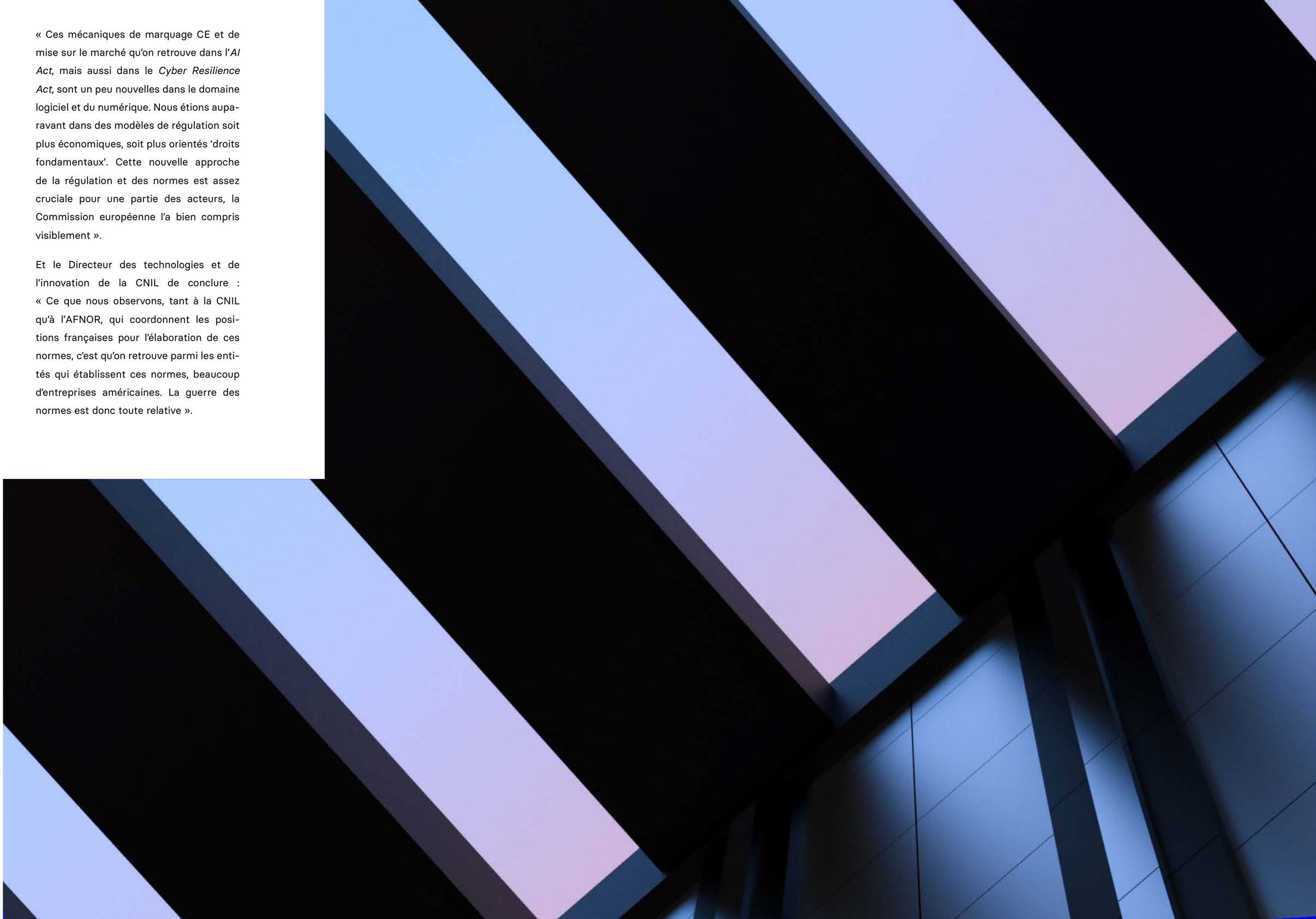
« Les Anglais, de leur côté, veulent rentrer dans le jeu mondial en dictant leurs propres normes. C'est là que se joue la bataille. Celui qui va réussir à imposer ses normes, ses standards au niveau mondial aura gagné une première étape. En Europe, nous sommes 500 millions de consommateurs, en bonne santé, bien éduqués, qui ont des moyens. Nous avons donc la capacité d'imposer nos règles aux acteurs étrangers qui veulent rentrer dans le marché européen », note Rayna Stamboliyska.

LA GUERRE DES NORMES AURA-T-ELLE LIEU ?

Une analyse que complète Bertrand Pailhès en ajoutant qu'une liste de 10 standards, commandés par la Commission européenne au Comité européen de normalisation (CENELEC), est adossée à l'*AI Act* :

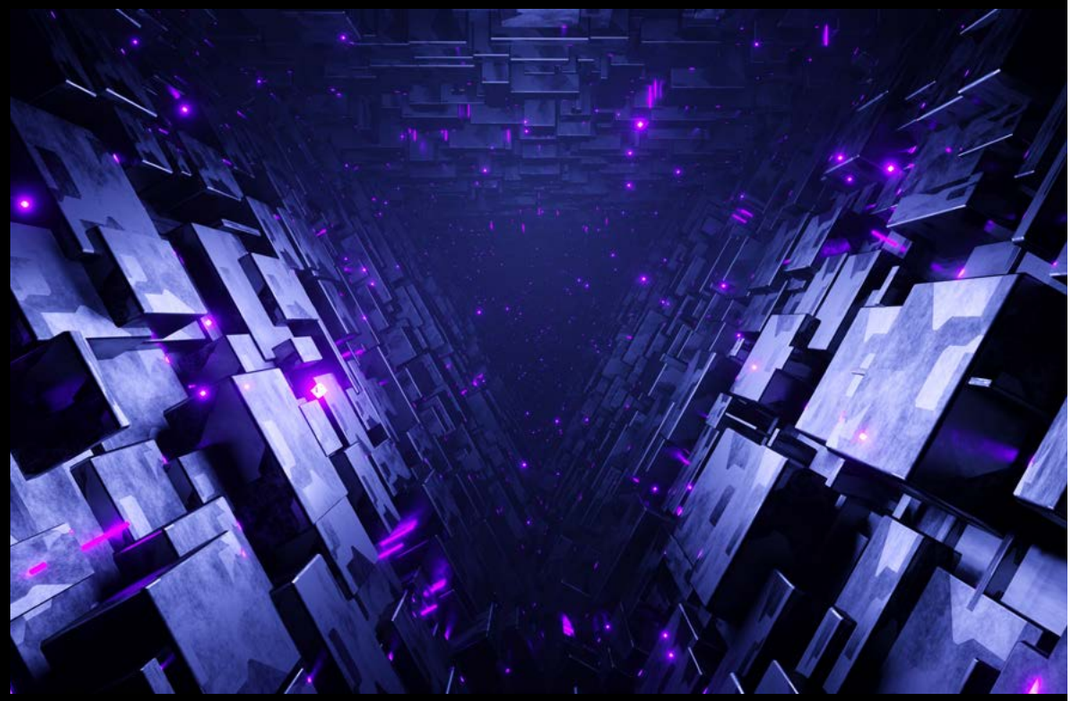
« Ces mécaniques de marquage CE et de mise sur le marché qu'on retrouve dans l'*AI Act*, mais aussi dans le *Cyber Resilience Act*, sont un peu nouvelles dans le domaine logiciel et du numérique. Nous étions auparavant dans des modèles de régulation soit plus économiques, soit plus orientés 'droits fondamentaux'. Cette nouvelle approche de la régulation et des normes est assez cruciale pour une partie des acteurs, la Commission européenne l'a bien compris visiblement ».

Et le Directeur des technologies et de l'innovation de la CNIL de conclure : « Ce que nous observons, tant à la CNIL qu'à l'AFNOR, qui coordonnent les positions françaises pour l'élaboration de ces normes, c'est qu'on retrouve parmi les entités qui établissent ces normes, beaucoup d'entreprises américaines. La guerre des normes est donc toute relative ».



IA et cybersécurité : deux mondes à rapprocher

par **Fabrice Deblock** #TRANSFORMATION NUMÉRIQUE



LIRE L'ARTICLE EN LIGNE

Thème principal de l'édition 2024 du Forum InCyber, l'imbrication de l'intelligence artificielle au cœur des enjeux de cybersécurité a suscité de très nombreux commentaires et analyses. Retour sur certaines prises de position exprimées lors de l'événement.

Pour le Général Watin-Augouard, fondateur du Forum InCyber, une vraie rupture est intervenue depuis novembre 2022 (date de la sortie de ChatGPT par OpenAI) dans le domaine de l'IA générative. « Cette IA nous subjugue et nous inquiète en même temps. Son immense potentiel n'est pas encore pleinement exploré, dans sa dimension, sa puissance, son impact. Elle nous transporte dans l'inconnu, vers un futur imprévisible, laissant la voie ouverte à toutes les hypothèses ».

Plus que toute autre technologie, l'IA appelle une réponse à la question : « Pourquoi ? ». « Le 'pourquoi' renvoie à la recherche de la finalité et d'un encadrement qui préserve notre liberté, en ne portant jamais atteinte à ce qui fait l'essence même de l'être humain : son identité, son unicité, son intimité, sa liberté de penser, de s'exprimer, de décider et même, sa confiance. Cette interrogation quasi-existentielle appelle le développement d'une IA responsable, encadrée, mais non limitée dans sa capacité novatrice par un droit inspiré par l'éthique », complète-t-il.

Comment dès lors concevoir le développement conjoint de l'IA et de la cybersécurité ? « Le développement de l'IA ne peut être envisagé sans une cybersécurité garante de la confiance. La cybersécurité doit être au service de l'IA et inversement. Les systèmes d'IA doivent être sécurisés tout au long de leur cycle de vie afin d'être résistants face aux cyberattaques.

Par ailleurs, l'IA rebat les cartes entre la capacité offensive des cybercriminels et la capacité de défense des organisations. La course aux armements est asymétrique, car les pirates n'ont guère de scrupules au regard des contraintes juridiques et éthiques que nous nous imposons », note le Général Watin-Augouard.

Un point de vue que rejoint Pascal Steichenn, Président de l'Advisory Board du Forum InCyber. Il existe selon lui trois dimensions quand on parle d'IA et de cybersécurité : *« The good, the bad and the ugly »* (le beau, le moins beau et le mauvais).

« Le *'good'* consiste à dire que l'IA peut renforcer les systèmes de protection, améliorer la détection des intrusions et l'identification des menaces. Compte tenu du déficit actuel de ressources, l'IA constitue une véritable alliée. Le *'bad'* correspond au fait que les cybercriminels utilisent eux aussi l'IA. Leurs attaques deviennent plus performantes, plus automatisées. Enfin, l'ugly renvoie à la sécurité même de l'IA. Si les concepteurs d'algorithmes d'IA générative ne savent pas expliquer comment ces derniers fonctionnent, c'est inquiétant », détaille-t-il.

COMMENT TRANSPOSER LES APPROCHES ACTUELLES DE LA CYBERSÉCURITÉ AU MONDE DE L'IA ?

Vincent Strubel, Directeur Général de l'ANSSI, insiste, lui, sur le côté itératif et progressif des améliorations qui vont se produire dans le domaine de l'IA. « Je ne crois pas aux discours très anxiogènes disant que l'IA va décupler les pouvoirs des attaquants, précipitant le cyber-Armageddon. Je ne crois pas non plus à ceux qui, au contraire, disent que cela va résoudre trivialement tous les problèmes de cybersécurité, que toutes les cyberattaques et vulnérabilités vont être détectées et que nous allons tous nous retrouver au chômage », analyse-t-il.

Pour le patron de l'ANSSI, le défi actuel est de faire en sorte que les défenseurs profitent des progrès de l'IA au moins aussi vite que les attaquants. Et pour cela, de nombreuses mesures de soutien à l'innovation ont été mises en place, notamment dans le cadre du plan France 2030.

« Mais le vrai sujet en matière d'IA, c'est tout le reste : comment transposons-nous nos approches actuelles de la cybersécurité au monde de l'IA, c'est-à-dire comment passons-nous d'un monde dans lequel la spécification et l'implémentation s'effacent devant l'apprentissage ? Par ailleurs, comment certifions-nous une IA en termes de sécurité ? Certifier dans l'absolu, c'est simple. Mais le vrai défi, c'est de savoir comment certifier avec un niveau de garantie comparable à celui que nous pouvons fournir pour des produits plus classiques, afin qu'il y ait une continuité dans notre niveau de garantie et de perception », précise Vincent Strubel.

SÉCURISER L'IA, UNE PRIORITÉ ABSOLUE

Dans ce domaine, l'ANSSI a récemment co-signé avec ses homologues britanniques et américains un certain nombre de lignes directrices sur la sécurité de l'IA. « Nous allons probablement publier tôt ou tard des recommandations plus spécifiques de l'ANSSI, cela n'épuisera pas le sujet », note le Directeur Général de l'ANSSI.

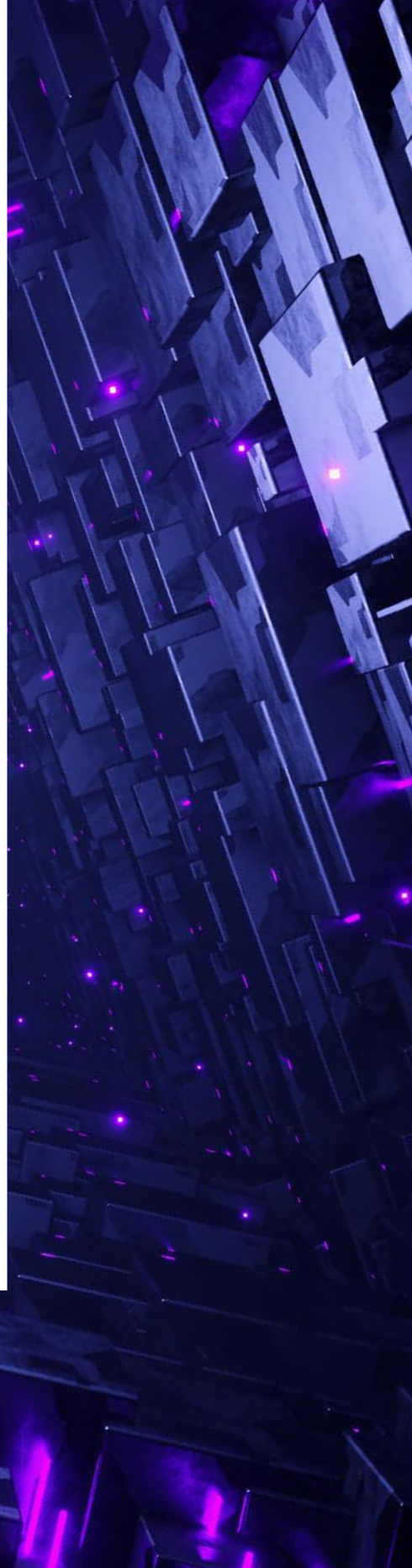
Le patron de l'ANSSI rappelle également que son agence a besoin, plus que jamais, de travaux académiques pour creuser les fondements scientifiques de l'ensemble de ces thématiques, mais aussi de cas d'usages concrets sur lesquels il sera possible de mener des expérimentations. « L'enjeu est de permettre à l'État français de s'emparer de ces sujets d'IA, de commencer à les expérimenter dans ses propres missions. C'est une énorme opportunité pour l'ANSSI de concrétiser ces travaux. Et cela vaut autant pour l'IA générative – qui est à la mode en ce moment, mais qui n'est pas ce qui m'inquiète le plus – que pour l'IA prédictive qui est un peu sortie des radars, mais qui est peut-être ce qui arrivera le plus vite sur des enjeux critiques », ajoute Vincent Strubel.

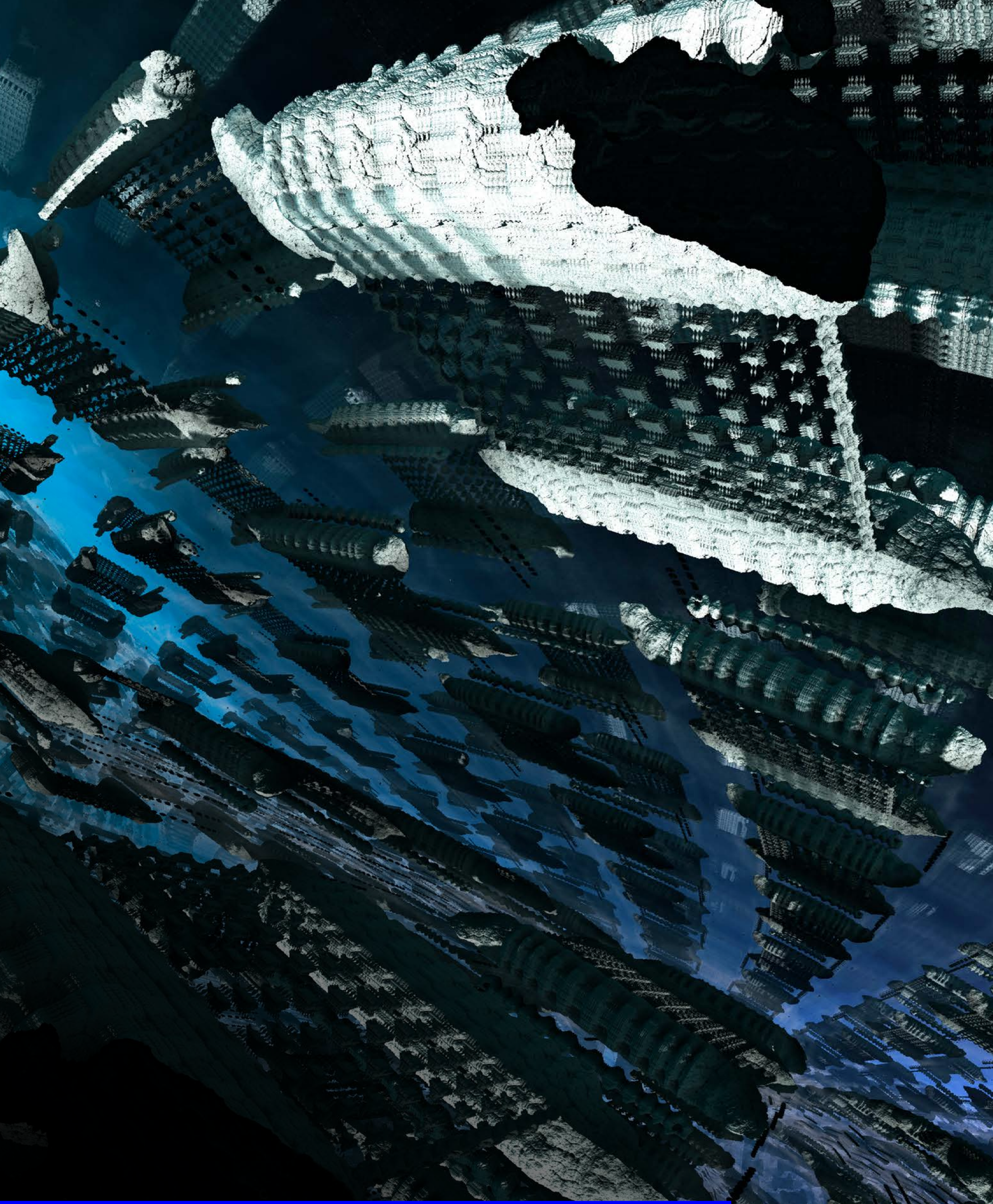
Pour Michel Van Den Berghe, Président du Campus Cyber, la protection de l'IA constitue également une priorité absolue : « De nombreux projets se montent pour protéger l'IA. Nous constatons en effet que des personnes mal intentionnées commencent à empoisonner l'IA afin qu'elle puisse raconter des choses pas forcément réelles…

Les projets dont nous discutons aujourd'hui avec les RSSI consistent donc à protéger les nouveaux projets d'IA, un peu comme ce qui s'est passé avec le *Cloud*, avec l'apparition des *Cloud* privés. Là, ce sont des IA privées qui se développent ».

Le mot de la fin revient à Guillaume Tissier, Directeur Général de Forward Global (et organisateur du Forum InCyber), qui regrette que les écosystèmes de l'IA et de la cybersécurité ne se parlent pas suffisamment. « Nous avons eu l'impression, en préparant l'événement InCyber Forum, que les pure players de l'IA étaient réticents à s'afficher sur le sujet de la cybersécurité. Comme s'il y avait d'un côté le numérique glamour, celui du CES de Las Vegas ou de Vivatech, et de l'autre la cybersécurité anxiogène, frileuse, qui freine l'innovation. Il faut arrêter de faire cette segmentation. Les deux vont de pair. Les experts de l'IA ont besoin des experts cyber et réciproquement », conclut Guillaume Tissier.

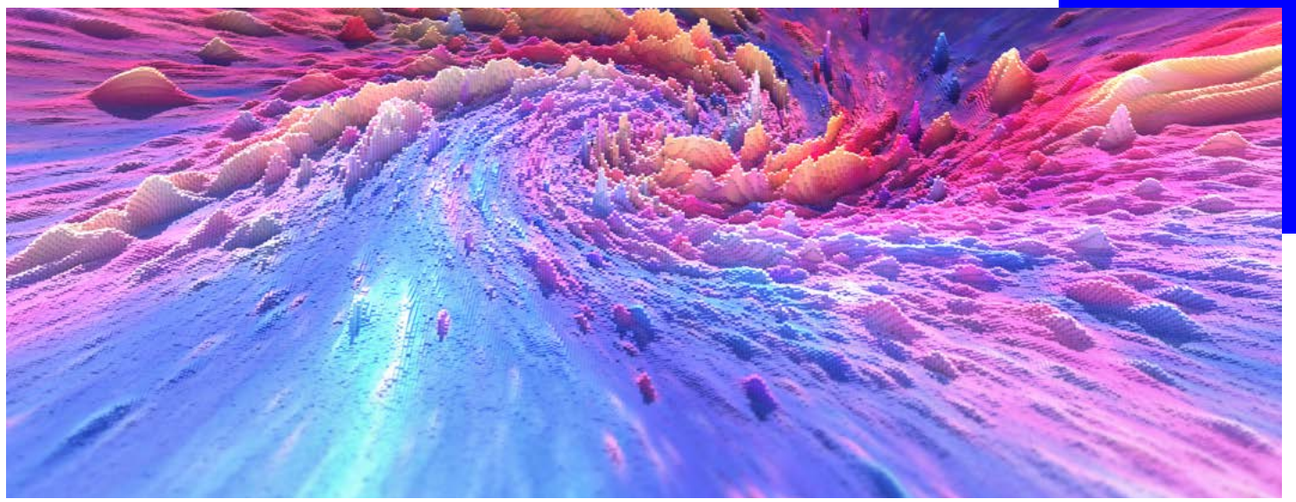
Le monde de l'intelligence artificielle et celui de la cybersécurité sont donc deux univers qu'il est urgent de mieux faire communiquer et collaborer. Les experts de l'IA ont besoin des experts en cybersécurité pour sécuriser leurs systèmes et s'assurer que de nouvelles vulnérabilités ne sont pas introduites. Et les experts en cybersécurité ont besoin des experts de l'IA pour ne pas être submergés, notamment par la vague du *shadow IA* qui déferle dans bon nombre d'entreprises.





baromètres

Avec près de 13 fuites par jour, le nombre de violations de données reste constant de 2022 à 2023



Même si la menace cybercriminelle demeure importante, c'est le nombre de fuites accidentelles qui attire l'attention cette année, avec une augmentation de 37.5 %. Sur un total de 4564 notifications à la CNIL, un quart des fuites de données sont d'origine accidentelle.

En plus du préjudice financier et réputationnel subi par les organisations victimes, les individus dont les données ont fuité sont également exposés à des risques de fraude ou d'usurpation d'identité. La fuite de données sensibles, comme les données concernant la santé ou révélant l'origine raciale ou ethnique, est particulièrement dangereuse.

Ce baromètre est animé par INCYBER NEWS en partenariat avec Forward Global et Lexfo, avec la participation de la CNIL.

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Forward

Lexfo

baromètre fuites de données

2023

Chiffres-clés

4564
notifications

1158
de naturelle accidentelle soit 25 %
20 % de ces fuites contiennent

2857
actes externes

+37,5 %
Augmentation des fuites accidentelles

2911
de nature malveillante
soit 63 %

1212
actes internes
20 % sont causés par des acteurs internes malveillants

-3,5 %
Repli des notifications enregistrées, de 2022 à 2023

Chiffres-clés

Fuites internes accidentelles

40 %
dues à l'envoi de données personnelles à un mauvais destinataire

30 %
résultent de la publication involontaire de données

Secteur le plus touché

En nombre total de violations

18 %*
Administration publique
*52 % résultent d'actes externes malveillants

11,9 %
Activités financières

11,8 %
Santé humaine et de l'action sociale

Les informations présentées
dans ce panorama ont été collectées
auprès des 78 entreprises candidates
au Prix de la Start-up.

Le Prix de la Start-up est organisé en partenariat avec Eviden.

PARIS 2024

EVIDEN
SUPPORTEUR OFFICIEL DE PARIS 2024

PARIS 2024

panorama de l'innovation en cybersécurité

2024

Panorama de
L'INNOVATION

LES LAURÉATS 2024

GRAND PRIX — snowpack

PRIX RECHERCHE — iDAKTO

PRIX CROISSANCE — duo>key

PRIX IMPACT OPÉRATIONNEL — </ɹǝvǝʞSense>

PRIX COUP DE CŒUR — SAPORO ORDER IN CHAOS

LES GRANDES TENDANCES

80 % des candidats proposent une solution *full Cloud* ou hybride

20,5 % des entreprises ont déjà déposé un ou des brevets

63 % ont eu une croissance de plus de 20 % sur l'année 2023

25 % des candidats ont déjà contractualisé avec au moins une entreprise du CAC 40

45 % des candidats ont déjà fait un tour de table

18,4 % de leur CA est réalisé par le secteur public

81,6 % de leur CA est réalisé avec le secteur privé

Un prix européen

Provenance

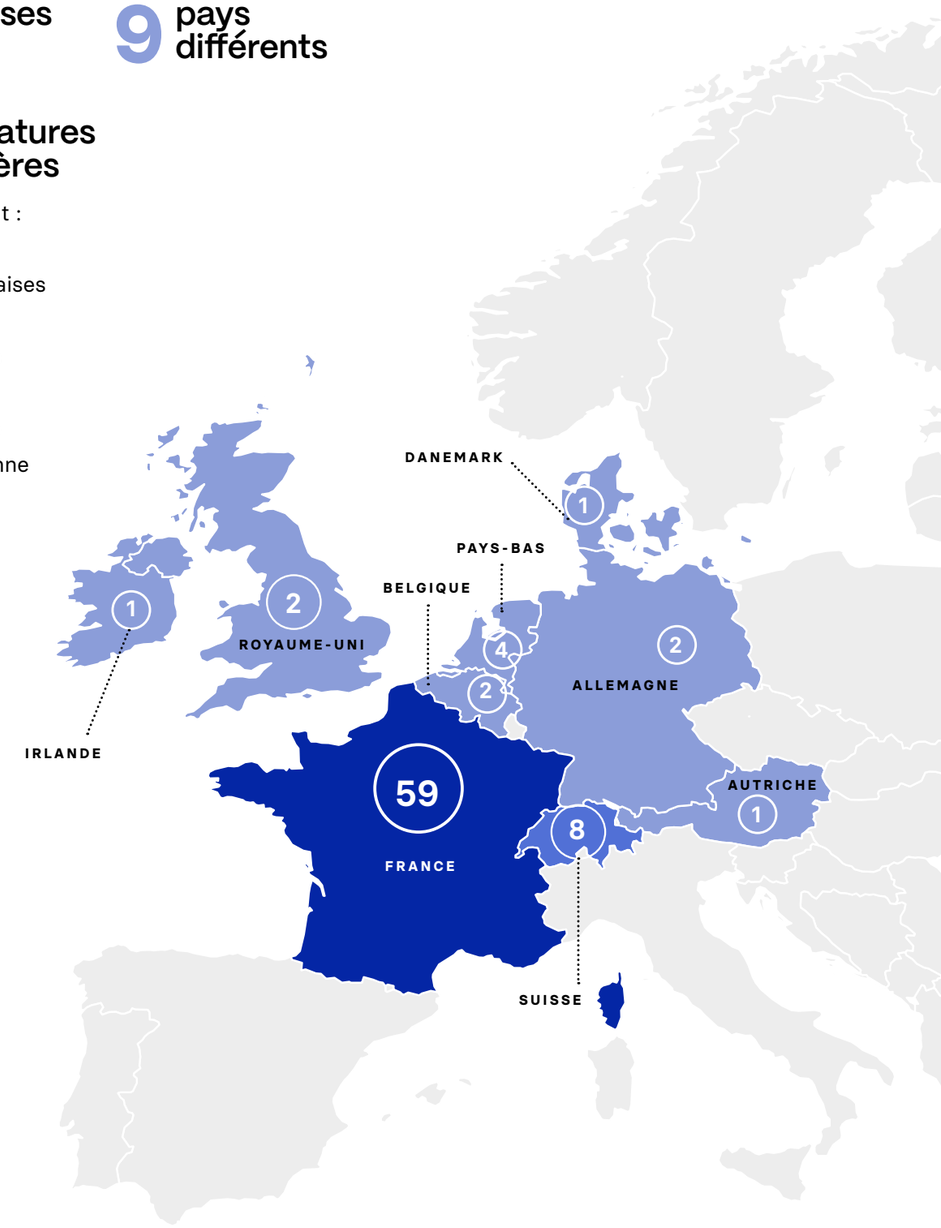
59 françaises

19 candidatures étrangères

comprenant :
8 suisses
4 néerlandaises
2 belges
2 anglaises
1 danoise
1 irlandaise
1 autrichienne

Répartitions des candidats par pays

9 pays différents



Panorama de
L'INNOVATION

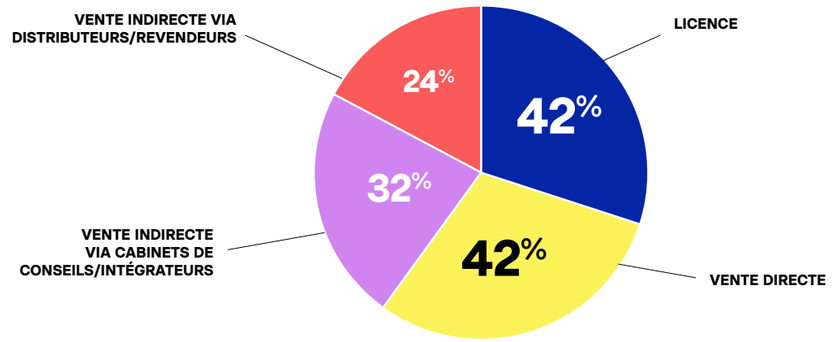
SEGMENTS

Sécurisation des données 13 (-3)	**Détection et réponse à incident** 11 (+7)	**IOT/OT/Cyber-sécurité industrielle** 7 (+3)	**Sécurisation des applications** 5 (+3)
Gouvernance, traçabilité et audit 12 (-3)	**Gestion des identités et des accès** 9 (+7)	**Cyber Threat intelligence** 6 (-6)	**Sensibilisation** 5 (+1)
Prévention des fuites de données 2 (+1)	**Sécurité réseaux** 3 -(3)	**Vulnérabilité** 5 (+1)	

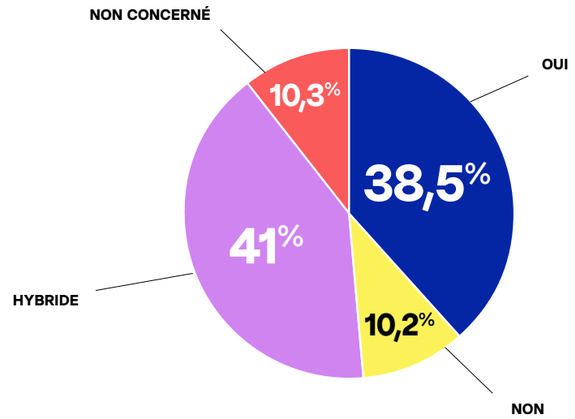
La sécurisation des données (13 solutions) occupe, comme l'an dernier, la première place devant le segment « Gouvernance, traçabilité et audit » (12 solutions), avec respectivement 16,6 % et 15,4 % des dossiers enregistrés. Ces deux activités sont en recul de 3 candidatures, alors que le segment « Gestion des identités et des accès » enregistre une forte progression, avec 7 solutions de plus. La gestion des identités et des accès *(Identity and Access Management)* reste un des piliers fondamentaux de la gestion de la sécurité des Systèmes d'Information, avec comme enjeu principal la bascule vers le *Cloud* et les apports de l'IA.

Le modèle de vente*

**Les start-up sondées pouvaient choisir plusieurs réponses*



Dotation *full-Cloud* des solutions



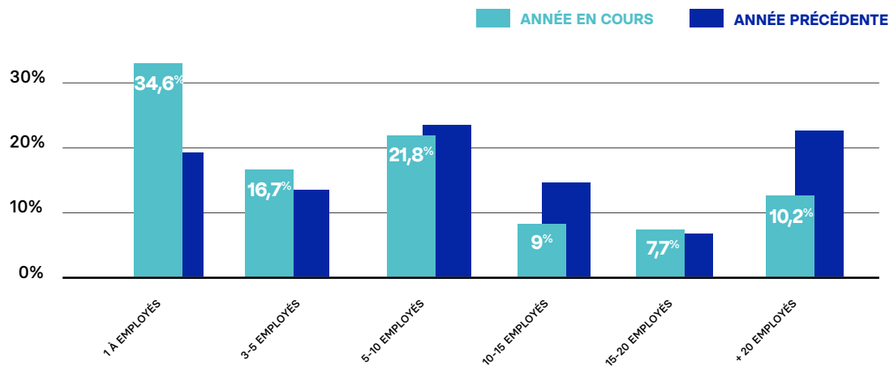
Dépôt de brevet

20,5% des entreprises ont déjà déposé un ou des brevets

41% des répondants privilégient un modèle hybride de dotation de leurs solutions. Le mode *full-Cloud* séduit cependant près d'un éditeur sur 4.

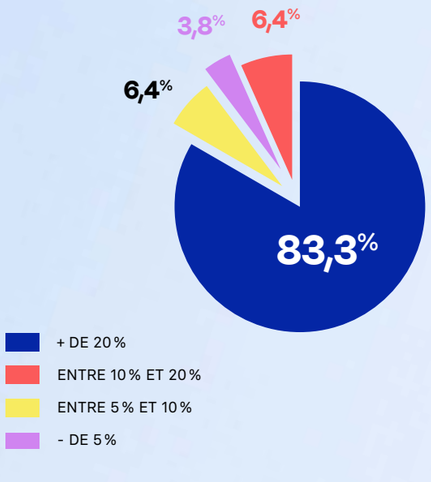
Entreprises

Nombre de salariés actuel

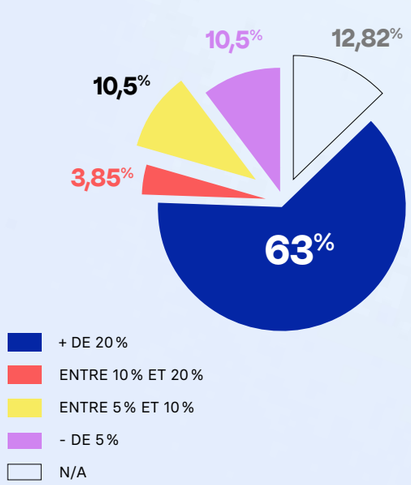


Près des trois quarts des entreprises candidates (73%) emploient moins de 10 salariés. Celles qui dépassent la barre des 20 collaborateurs représentent 10,2% des start-up ayant concouru cette année pour le prix.

% du CA investi en R&D



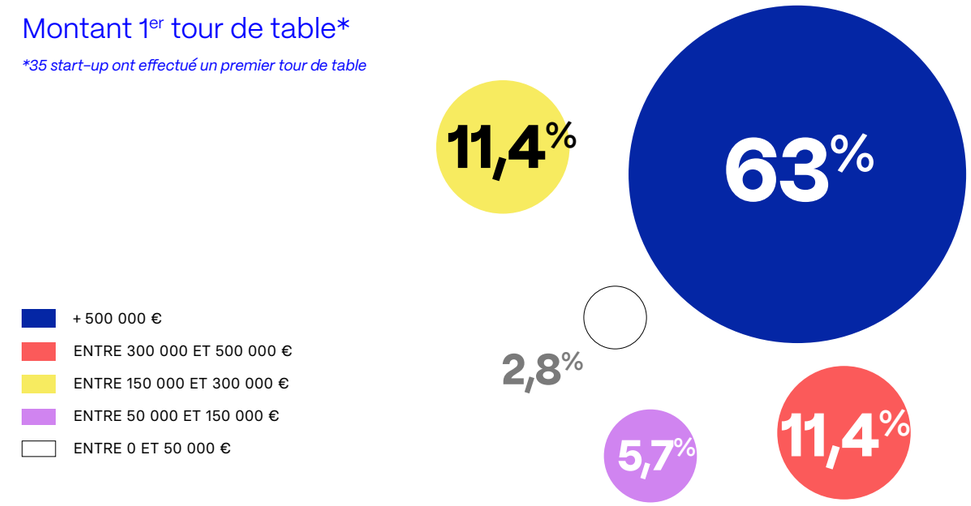
Croissance en 2023



Financements

Montant 1er tour de table*

**35 start-up ont effectué un premier tour de table*



Montant 2e tour de table*

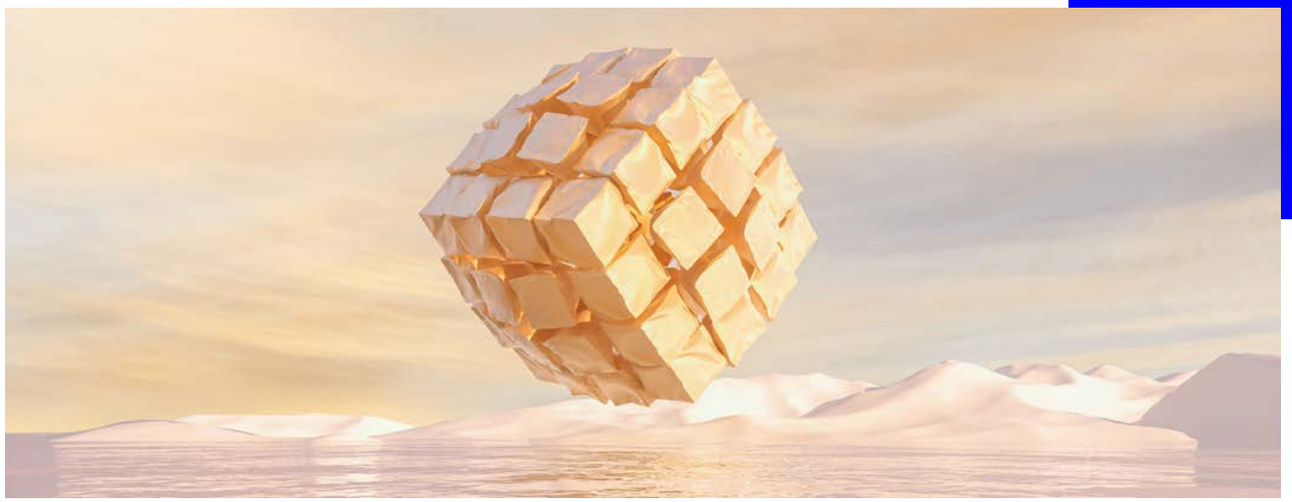
7 start-up ont effectué un second tour de table, toutes à plus de 500 000 euros

Levée de fond envisagée dans les 6 mois

Presque 45% des entreprises candidates ont réalisé un premier tour de table en 2023. Pour près des deux tiers d'entre elles (63%), le montant levé est supérieur à 500 000 euros. Les 500 000 euros ont également été atteints pour les 7 start-up ayant effectué un second tour de table l'an dernier. La proportion d'entreprises ayant l'intention de lever des fonds dans les 6 prochains mois est beaucoup plus élevée que l'an dernier : 71,8% contre 57%.

En 2023, les start-up opérant dans le domaine de la cybersécurité ont levé environ 9.4 milliards d'euros à travers 801 transactions

Découvrez la cinquième édition du baromètre de l'investissement en cybersécurité, préfacé par Vincent Strubel, Directeur général de l'Agence nationale de la sécurité des systèmes d'information, et réalisé par Tikehau Capital, en partenariat avec le Forum InCyber.



Ce panorama est animé par Tikehau Capital en partenariat avec le Forum InCyber.

TIKEHAU CAPITAL

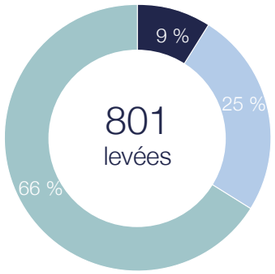
baromètre de l'investissement européen en cybersécurité

2024

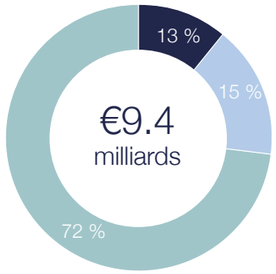
BILAN 2023
POUR LES ÉTATS-UNIS, ISRAËL ET L'EUROPE

En 2023, les start-up opérant dans le domaine de la cybersécurité ont levé environ 9.4 milliards d'euros à travers 801 transactions. Comme les années précédentes, les États-Unis maintiennent leur domination tant en nombre de transactions qu'en montant total levé. L'Europe a également consolidé sa position, représentant 15 % du total des montants levés. Israël a vu sa part dans le montant total levé augmenter au détriment des États-Unis et confirmant ainsi la tendance de rattrapage de l'Europe et d'Israël vis-à-vis des États-Unis.

Nombre de levées cyber



Montants levés cyber

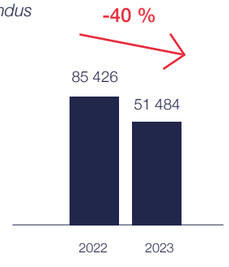


Israël Europe États-Unis

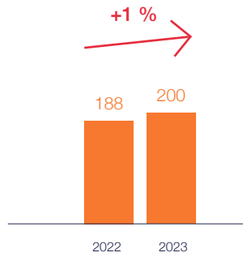
TENDANCES 2022 VS. 2023
EN EUROPE

Du fait d'un contexte économique et financier moins propice à l'investissement, l'année 2023 a été marquée par un ralentissement des montants levés tous secteurs confondus en Europe. La cybersécurité européenne ne fait pas exception. Malgré une augmentation du nombre de levées de fonds, le montant total levé par le secteur européen de la cybersécurité a diminué de 42 % en 2023. Quelques exceptions comme la France ont fait preuve de résilience et ont vu le montant levé en cybersécurité augmenter.

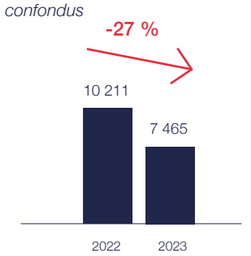
Nombre de levées
tous secteurs confondus



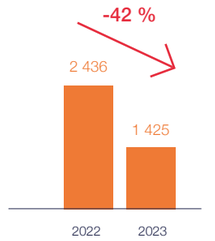
Nombre de levées
cybersécurité



Montants levés (M€)
tous secteurs confondus



Montants levés (M€)
cybersécurité

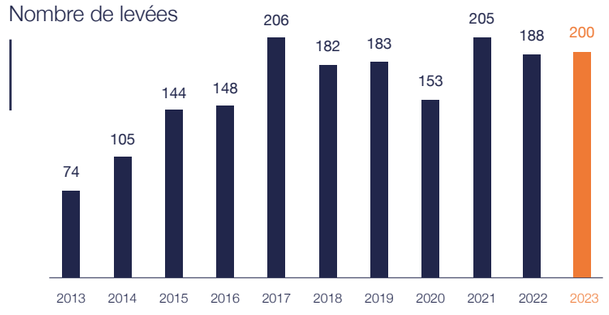


TENDANCES 2013 - 2023
EN EUROPE

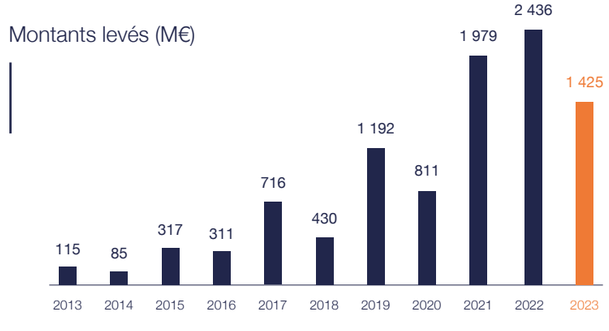
Depuis 2013, la progression européenne reste positive malgré une tendance à la stagnation du nombre de levées cyber depuis 2021. En dix ans, le nombre de levées cyber a été multiplié par trois pour un montant total levé multiplié par douze.

En 2023, bien que le montant total levé en Europe ait connu une baisse pour la première fois en trois ans, il demeure au-dessus du niveau enregistré en 2020. Malgré des gros tours de table moins importants qu'en période post-Covid, le montant total levé reste nettement supérieur au milliard d'euros, mettant en évidence que, sur la dernière décennie, la cybersécurité européenne s'est affirmée comme une opportunité d'investissement attractive pour les investisseurs.

Nombre de levées



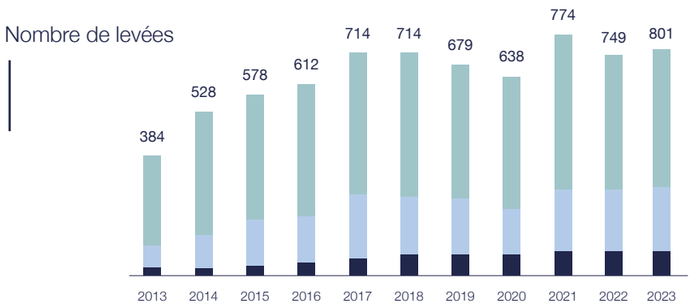
Montants levés (M€)

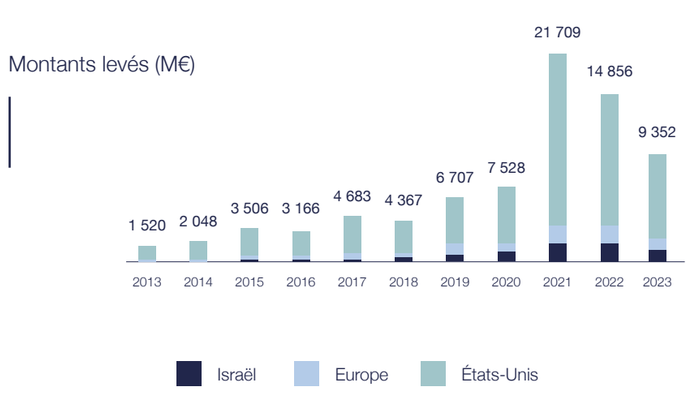


TENDANCES 2013 - 2023
ÉTATS-UNIS, ISRAËL ET EUROPE

L'année 2023 marque la fin de la période post-Covid dans le secteur de la cybersécurité. En effet, cette année confirme que la période 2021-2022 a été exceptionnelle, suite à la crise sanitaire, et nous assistons désormais à un retour à des niveaux de croissance plus normatifs.

Le montant total levé aux États-Unis, en Israël et en Europe a diminué de 37 % par rapport à 2022, mais demeure en progression de 24 % par rapport à 2020. Sur une décennie, le montant total levé, toutes régions confondues, a été multiplié par 6, tandis que le nombre de levées a été multiplié par 2 entre 2013 et 2023.



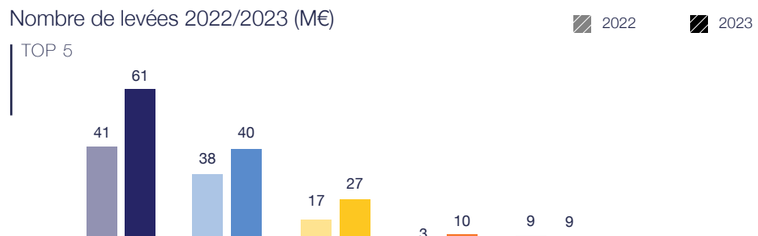


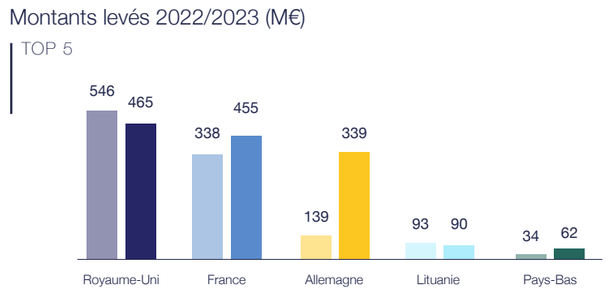
En 2023, le montant levé par les entreprises de cybersécurité américaines a été principalement porté par des tours de levées de Série A, C et D (56 % du montant total levé).

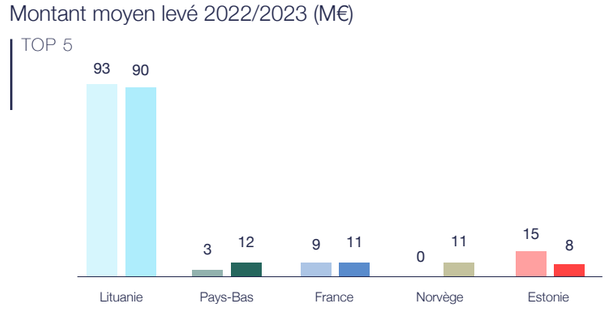
La baisse du montant total levé est principalement expliquée par une diminution des montants levés en Série B (baisse de 55 %), en Série C (baisse de 42 %) et en Série E+ (baisse de 45 %). Cette baisse est compensée par une hausse de 82 % des montants levés en Seed et une hausse de 45 % des montants levés en Série D. Le montant levé en Seed a atteint un niveau record cette année.

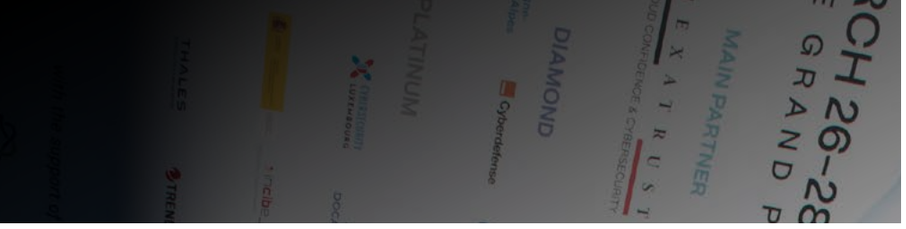
2023
FOCUS SUR L'EUROPE ET LA FRANCE

En 2023, le paysage européen de la cybersécurité révèle des dynamiques contrastées. La France s'illustre en se classant au deuxième rang en termes de nombre de levées et de montants levés, tout en occupant la troisième position en taille moyenne levée. Cette performance contraste avec celle du Royaume-Uni, qui enregistre une baisse du montant total levé. La France, l'Allemagne et les Pays-Bas affichent une croissance dans les montants levés en cybersécurité, malgré un contexte de réduction générale des investissements en Europe. L'année a été particulièrement fructueuse pour la cybersécurité française, avec une augmentation significative de 35 % du montant total levé, accompagnée d'une hausse de 22 % dans la taille moyenne des levées. Cette tendance souligne le dynamisme et le potentiel de l'écosystème français de la cybersécurité.









Forum InCyeber 2024

ÉDITION 2024

Chiffres-clés

17 500
participants physiques uniques

4 000
participations en ligne

2 400
internationaux

700
partenaires privés et publics

580
intervenants

120
journalistes accrédités

103
pays représentés

**Réponses les plus citées par un échantillon de visiteurs et partenaires interrogés lors de l'édition 2024. Plusieurs réponses possibles.*

Pourquoi viennent-ils au Forum* ?

41% IDENTIFIER DES SOLUTIONS

20 000m² d'exposition

De nombreux pavillons nationaux (Pays-Bas, Luxembourg, Suisse, Espagne, Belgique...)

2 espaces de démonstrations (InCyber Talk et espace InCyber Demos)

Des villages thématiques avec espaces de démonstrations sur certaines verticales : Cybersecurity For Industry, ID & KYC Forum

36% APPROFONDIR DES EXPERTISES

30 conférences
45 talks
35 démonstrations techniques
30 démonstrations de hacking
40 masterclass
+ des exercices de crises

31% RENCONTRER DES PROSPECTS ET CLIENTS

95 600 scans de badges sur 3 jours
130 contacts qualifiés par exposant, en moyenne
+160% de contacts qualifiés pour les sociétés ayant au moins une intervention en plus de leur stand, en moyenne
68 400 messages échangés durant les 3 jours via la plateforme de networking réunions business sur 3 jours
2 200 activités publiques ou privées organisées par les partenaires à l'occasion du Forum InCyber
+80 InCyber Channel, une session de speed dating permettant aux éditeurs de constituer leur *« channel »*

30% ÉCHANGER AVEC DES PAIRS ET CONTRIBUER AU DÉBAT D'IDÉES

1 sommet d'ouverture et 3 plénières dans 1 amphithéâtre de 1 600 places
60 tables rondes
1 CISO Lounge organisé avec le CESIN
6 ateliers de travail InCyber Connect dédiés aux clients finaux

24% DÉCOUVRIR DE NOUVELLES PÉPITES

1 Prix de la start-up InCyber
1 village innovation regroupant 35 start-up et un espace de « pitch »
1 événement associé dédié à l'investissement (InCyber Invest)

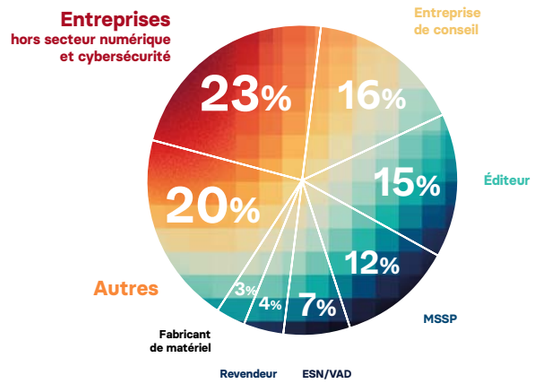
23% VALORISER SA MARQUE EMPLOYEUR ET RECRUTER

1 village Talents regroupant les écoles et les stands des entreprises qui recrutent
1 compétition de cybersécurité (European Cyber Cup) réunissant 25 équipes et 250 joueurs

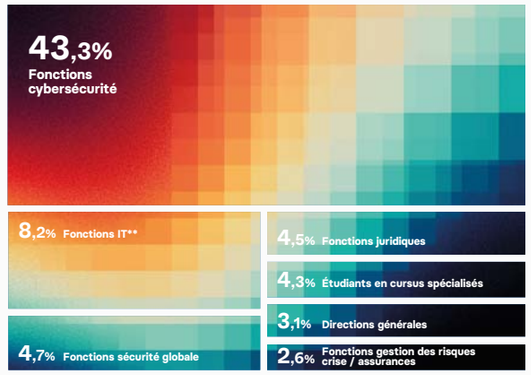
Profil des participants 2024

IN CYBER FORUM EUROPE

TYPES D'ORGANISATION



FONCTIONS REPRÉSENTÉES*



** hors fonctions commerciales*
*** hors cybersécurité*

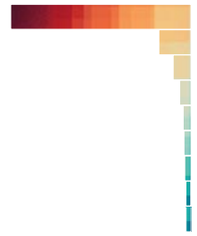
LES 10 PAYS LES PLUS REPRÉSENTÉS

1 **FRANCE**
2 **BELGIQUE**
3 **PAYS-BAS**
4 ROYAUME-UNI
5 LUXEMBOURG
6 SUISSE
7 ALLEMAGNE
8 ÉTATS-UNIS
9 CANADA
10 ESPAGNE

TOP 10 CENTRES D'INTÉRÊTS

1 **Gouvernance**
2 **Sensibilisation**
3 **Analyse de risques**
4 Conformité réglementaire
5 Supervision
6 IAM
7 Sécurité des données
8 Détection et réponse à incident
9 Sécurité du *Cloud* / *Cloud* sécurisé
10 Sécurité des applications

TOP 10 DES SECTEURS D'ACTIVITÉS*



13,2% Services numériques
7,0% Audit / Conseil
6,2% Banque
5,3% Administration et fonction publique
5,1% Télécoms
4,9% Commerce / Distribution / E-commerce
4,0% Industries de défense
3,8% Industrie / Production industrielle
2,5% Énergie

** hors entreprises partenaires*

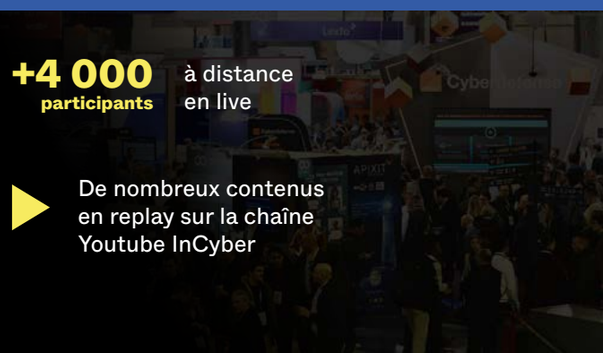
Les contenus sont en français ou en anglais natifs et sont pour la plupart traduits dans l'autre langue **FR** **EN**

1 visiteur sur 2 a assisté à au moins une intervention

6 140 décisionnaires sur des projets liés à la sécurité ou la confiance numérique en 2024 **+12%**

+4 000 participants à distance en live

De nombreux contenus en replay sur la chaîne Youtube InCyber



merci

à tous nos partenaires 2024 !

PARTENAIRE PRINCIPAL

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

PARTENAIRES DIAMOND

CMIB "Cyber Made in Belgium" .AGORIA
Auvergne-Rhône-Alpes
Cyberdefense
SentinelOne

PARTENAIRES PLATINUM

Avantage Cliquer
BRETAGNE LA CYBERSÉCURITÉ À SON TERRITOIRE
CYBERSECURITY LUXEMBOURG
DOCAPOSTE
EGERIE
EXCLUSIVE NETWORKS
incibe
NCC-ES
Nouvelle-Aquitaine
TENTRIS
THALES
TREND

PARTENAIRES GOLD

28B
aDvens
AIRBUS
aws
ARROW
Capgemini
Certigna
CISCO
dcypher
European
CrowdSec
CROWDSTRIKE
EVIDEN
Google Cloud
IN
infinigate
ITRUST
Lexfo
mimecast
NeoYAD
onetrust
OVHcloud
paloalto
ORUM
GrandEst
Schneider Electric
SESAME IT
sopra steria
sosafe
splunk>
STORMSHIELD
Starboard Advisory
TANIUM
TD SYNNEX
txOne
vade
XM Cyber

CAHIERS
IN CYBER
RÉTROSPECTIVE 2024

Ready for AI ?
Réinventer la cybersécurité
à l'ère de l'IA

Prochains événements :

FORUM INCYBER | CANADA
29-30 OCT. 2024

FORUM INCYBER | EUROPE
5-7 AVRIL 2025

FORUM INCYBER | ÉTATS-UNIS
17-18 JUIN 2025

Retrouvrez plus d'informations
sur forum-incyber.com