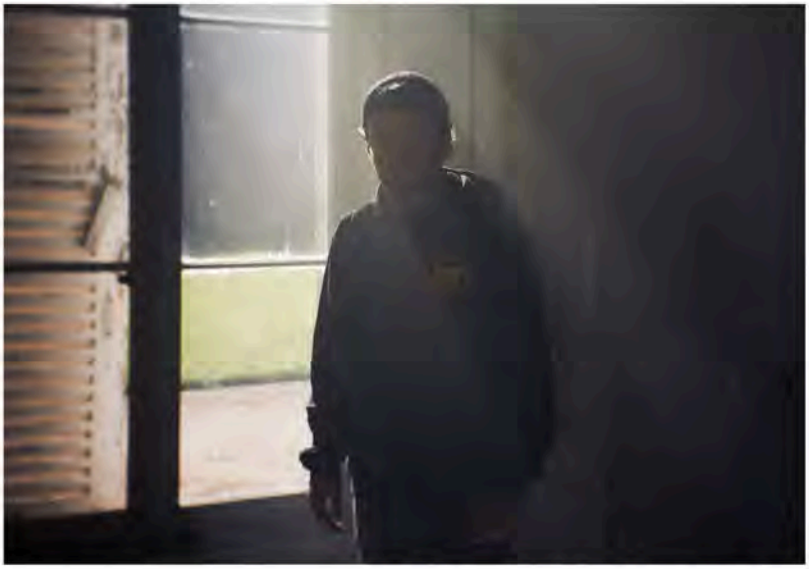
Revue de presse 2023

Loria

cnrs Université de Lorraine Inria CentraleSupélec

Exposition : Samson Michel propose de découvrir son "Imaginaire" à la Cour des Arts de Saint-Dié-des-Vosges

Le 13 janvier 2023 par Jordane Rommevaux



L'exposition du travail Imaginaire de Samson Michel et le débat sur l'IA qui suit, à découvrir à la Cour des Arts de Saint-Dié-des-Vosges.

© Samson Michel

Plongée dans l'Imaginaire à travers l'exposition de Samson Michel, toute en formes et couleurs, ce vendredi 13 janvier. Une exposition aussi intrigante que passionnante, réalisée grâce au talent des arts graphique de son auteur, qui sera suivie d'une démonstration originale et d'un débat sur l'intelligence artificielle.

L'IA (Intelligence Artificielle) comme on l'appelle plus communément est de plus en plus présente dans notre quotidien. Faut-il s'en réjouir ou s'en inquiéter ? Devient-elle indispensable ou, au contraire, est-elle devenue nocive ? La question n'est plus "remplacera-t-elle un jour l'homme ?" mais plutôt "l'homme réussira-t-il à conserver sa place et son rôle dans le futur, à côté des différentes IA ?".

C'est autant d'interrogation qui viennent à l'esprit lorsque l'on découvre l'exposition fantastique mais d'un autre genre, que propose Samson Michel, ce vendredi 13 janvier, à la Cour des Arts de Saint-Dié-des-Vosges.

L'artiste y expose son travail graphique réalisé avec le logiciel MidJourney, un calculateur / générateur d'image, à partir d'une description détaillée. Il présente son travail de création assistée, comme s'il consistait "à prendre des photos dans un monde virtuel imaginaire".

Les plus lus

20 juin 2024
Rencontre-dédicace avec FX l'urgentiste le 27 juin à la librairie Quai des mots, Épinal

13 juil 2024
100% Films : un été riche en émotions

29 mai 2024
"L'apogée", le nouveau livre du vosgien Pascal Grégoire, évoque avec humour le cap des 60 ans

C'est aussi les question abordées et les sujets des différents débats qui seront abordés par l'artiste, accompagné du chercheur à l'Université de Lorraine, Samuel Nowakowski, qui travaille sur la modélisation des usages du web et l'intelligence artificielle et de l'artiste Julien Cuny, peintre, sculpteur et spécialiste des arts graphiques, à l'occasion de la conférence-débat, qui suivra le vernissage de l'exposition.

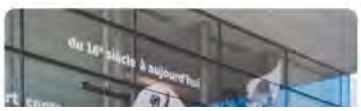
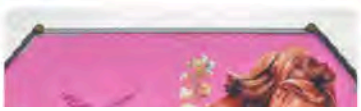
Expo et débat Imaginaires
Vendredi 13 janvier, à partir de 19 h
La cour des Arts, Saint-Dié-des-Vosges
Accès libre
www.lacourdesarts.eu

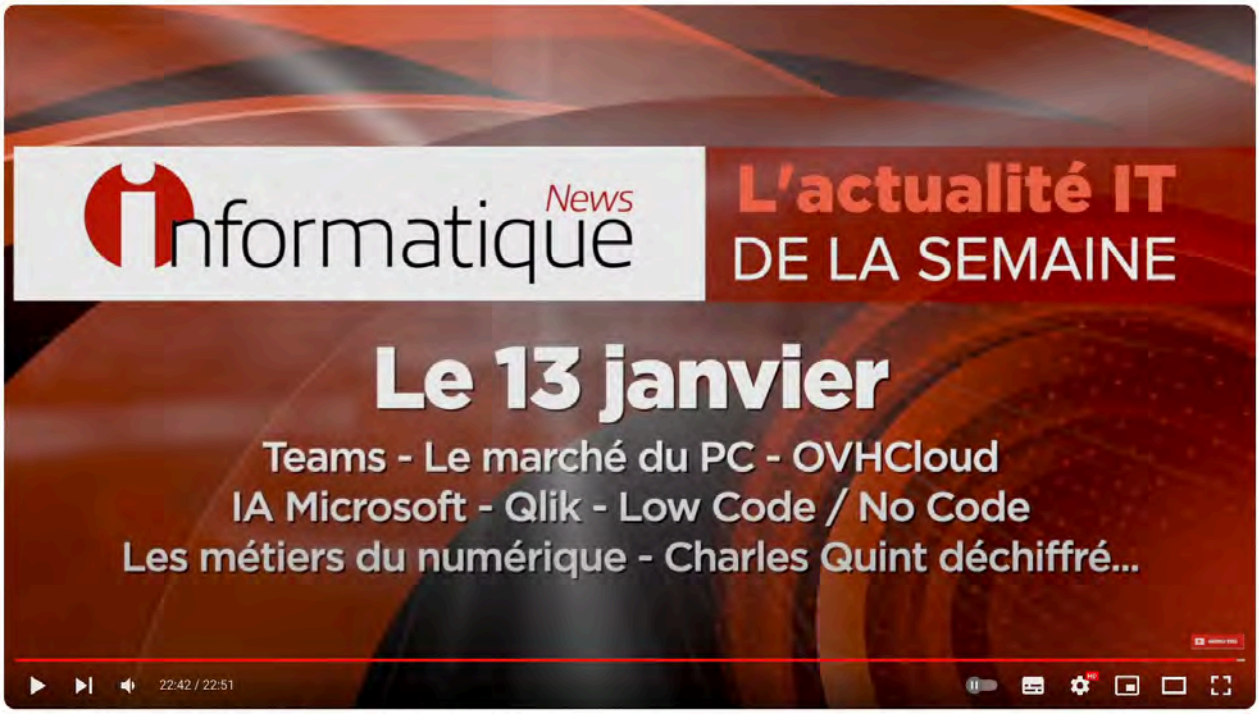
Partager l'article : E-mail Facebook Twitter

Article rédigé par :

Jordane Rommevaux
Journaliste web

Articles similaires



InfoNewsHebdo : L'actualité IT de la semaine #13/01/2023

202 vues Diffusée en direct le 13 janv. 2023
Au menu de ce résumé de l'actualité de cette première semaine de l'année :
Teams : moins de freemium, plus de premium
Annus horribilis pour le marché du PC
OVHCloud étoffe son offre Bare Metal
L'IA en marche chez Microsoft
Qlik absorbe Talend
Le Cigref se penche sur le Low Code / No Code
Opération pôle Emploi pour les métiers du numérique
L'informatique à l'aide de l'histoire : la lettre de Charles Quint déchiffrée

Zeljka Zorz, Editor-in-Chief, Help Net Security
January 13, 2023

Vulnerabilities in cryptographic libraries found through modern fuzzing

Recently patched vulnerabilities in MatrixSSL and wolfSSL, two open-source TLS/SSL implementations / libraries for embedded environments, have emphasized the great potential of using fuzzing to uncover security holes in implementations of cryptographic protocols.

CVE-2022-43974 and CVE-2022-42905

CVE-2022-43974 is a buffer overflow vulnerability found in MatrixSSL versions

4.5.1-4.0.0 that could allow information disclosure and remote code execution.

It was discovered and reported by Robert Hörr and Alissar Ibrahim, security evaluators with Deutsche Telekom's IT Security Evaluation Facility, and has been patched in version 4.6.0, released in December 2022.

CVE-2022-42905 is a buffer over-read vulnerability found in wolfSSL versions 5.5.1 and earlier, and could result in exploitable crashes (but only if callback functions are enabled).

It was discovered and reported by Lucca Hirschi and Steve Kremer from LORIA, Inria (the French Institute for Research in Digital Science and Technology) and Max Ammann, a security engineer interning with Trail of Bits. It has been patched in wolfSSL version 5.5.2, released in October 2022.

Fuzzing cryptographic libraries to flag security flaws

In both cases, the researchers used fuzzing to find the flaws.

"Computer software is becoming more complex. So, it is almost impossible to perform a complete source code review with reasonable coverage. For this reason, modern fuzzing methods are used to discover vulnerabilities," Deutsche Telekom's security evaluators explained.

They fuzzed the MatrixSSL library with code coverage-guided fuzzers AFL and libFuzzer, and the vulnerability was found with AddressSanitizer, a tool for detecting memory errors. (Using those same tools, several years ago Hörr unearthed another buffer overflow in wolfSSL. He also developed the Fast Automated Software Testing framework for TLS libraries, combining the strengths of various fuzzing tools.)

"Code coverage based fuzzing combined with the AddressSanitizer is a powerful method to discover e.g., buffer overflows. With increasingly complex source codes, it is a resource-efficient alternative to source code reviews, because this

fuzzing approach can be done mainly automatically. As there exist many approaches for fuzzing, it is the art of fuzzing to find the best approach," Hörr and Ibrahim noted.

Ammann and his fellow researchers used a new protocol fuzzer called tlspuffin to automatically discover CVE-2022-42905 and three other vulnerabilities.

"Tlspuffin is a fuzzer inspired by formal protocol verification. Initially developed as part of my internship at LORIA, INRIA, France, it is especially targeted against cryptographic protocols like TLS or SSH," he explained.

They used the fuzzer not only to discover new vulnerabilities in wolfSSL, but also to rediscover previously flagged logical vulnerabilities (e.g., FREAK) as a way to prove that tlspuffin works.

In an excellent write-up, Ammann went more in-depth about some of the discovered vulnerabilities and how the fuzzer found "weird states" and allowed them to find their source.

"It is challenging to fuzz implementations of cryptographic protocols. Unlike traditional fuzzing of file formats, cryptographic protocols require a specific flow of cryptographic and mutually dependent messages to reach deep protocol states," he explained.

"Additionally, detecting logical bugs is a challenge on its own. The AddressSanitizer enables security researchers to reliably find memory-related issues. For logical bugs like authentication bypasses or loss of confidentiality no automated detectors exist."

That's why they created tlspuffin. Employing the decades-old Dolev–Yao model, which can be used for testing cryptographic protocols, it includes specific modifications so they could successfully fuzz concrete implementations of cryptographic protocols. Tlspuffin's structure is also based on the LibAFL fuzzer.

"Before my internship at Trail of Bits, tlspuffin already supported fuzzing several versions of OpenSSL (including the version 1.0.1, which is vulnerable to

Heartbleed) and LibreSSL," Ammann noted. Since then, they have:

- Designed an interface that added the capability to fuzz arbitrary protocol libraries and added support for fuzzing wolfSSL
- Added support for fuzzing the SSH protocol, as well as libssh
- Added a security violations oracle that allows for the detection of security issues that do not lead to program crashes (e.g., authentication bypasses or protocol downgrades)
- Made changes that allowed them to more easily validate findings

Tlspuffin can now be used for testing the TLS and SSH protocols, and that integrating a new protocol into tlspuffin is possible, but "takes significant effort and requires an in-depth understanding of the protocol." It can also be used by developers to write test suites.

More about

Deutsche Telekom | fuzzing | open source | SSH | SSL/TLS | Trail of Bits | vulnerability | wolfSSL

L'Est Républicain, 18 janvier 2023 (toutes les éditions)

NANCY

Quand les chercheurs locaux font d'incroyables découvertes

Au CNRS, à l'INRIA, au CHRU... les chercheurs nancéiens sont chaque année à l'origine de découvertes majeures. La dernière en date : le système solaire serait plus vieux d'un million d'années selon une équipe de scientifiques de Nancy.

Preuves à l'appui, la découverte d'une poignée de chercheurs, rattachés au Centre de recherches pétrographiques et géochimiques (CRPG) du CNRS et de l'Université de Lorraine, est désormais validée, comme l'atteste une récente publication dans la prestigieuse revue scientifique « Icarus ».

Selon les calculs, établis par les scientifiques nancéiens, le système solaire est plus vieux d'un million d'années et afficherait l'âge vertigineux de 4 568,7 millions d'années au lieu des 4 567,2 admis jusqu'à présent.

Une découverte qui ne change rien pour le commun des mortels, mais qui est lourde de sens pour la communauté scientifique. « Nous sommes désormais en mesure de présenter une chronologie cohérente de la formation des solides, qui ont précédé la naissance des planètes et des astéroïdes. C'est comme si nous pouvions fournir à l'historien ou au paléontologue une datation précise de l'apparition, puis des migrations de l'homme », indique Yves Marrocchi, directeur de recherches au CNRS et directeur adjoint du laboratoire nancéien.

> “ C'est comme si nous pouvions fournir à l'historien une datation précise de l'apparition, puis des migrations de l'homme. ”
>
> **Yves Marrocchi, directeur de recherches au CNRS**

« Mesurer l'immensurable »

Trois ans de travaux et de recherches ont été nécessaires pour aboutir à ce résultat, impulsé par un jeune thésard de 26 ans : Maxime Piralla. À ses côtés, Yves Marrocchi, Johann Villeneuve, directeurs de thèse, Nicolas Schnuriger et David V. Bekaert, chercheurs, ont conjugué leurs efforts et leurs énergies pour tenter de répondre à une question, qui allait tout changer : pourquoi les deux chronomètres utilisés jusqu'à présent, pour établir l'âge du système solaire, affichaient-ils des résultats différents, avec une variable de plus d'un million d'années ?

C'est l'apparition d'une nouvelle technique, conçue avec le concours de la société de Gennevilliers, Cameca, spécialisée entre autres dans l'élaboration d'équipements électroniques et électromécaniques de mesure, qui a résolu le problème. « Nous avons pu mesurer l'immensurable ».

Un microscope géant

« Une sonde ionique, munie de nouveaux détecteurs nous a permis d'affiner nos recherches et d'être beaucoup plus précis. Non seulement l'âge du système solaire nous a été donné avec davantage de justesse, mais en plus, les deux chronomètres (datation par uranium-plomb et par aluminium-magnésium) qui affichaient jusque-là des résultats différents, ont pour la première fois révélé des données similaires », poursuit Yves Marrocchi.

C'est à partir de fragments de météorites, soumis à la précieuse sonde ionique (pour faire simple un microscope géant) que les chercheurs ont pu établir ce surprenant résultat. « Les météorites sont constituées de petits objets sphériques qu'on appelle des chondres. Il s'agit de poussières qui se sont formées au cours des cinq premiers millions d'années de la naissance de notre système solaire. Ils se situaient au sein de ceintures gazeuses, qui entouraient la formation des étoiles.

Dater avec précision, l'apparition des chondres revenait donc à établir une chronologie précise de la formation des premiers solides, les futures planètes. Voilà qui est chose faite.

Frédérique BRACONNOT

À l'INRIA, un nouvel outil pour remonter aux origines de l'univers

« L'informatique est une baguette magique qui permet aux mathématiques de calculer la physique », explique Bruno Lévy, directeur de recherche à l'INRIA (Institut national de recherche en informatique et en automatique).

Sa formule résume l'approche pluridisciplinaire de travaux qui ont abouti à la mise au point d'un nouvel outil permettant de remonter aux origines de l'univers, le Big Bang, il y a 13,7 milliards d'années.

Une « machine à remonter le temps »

Roya Mohayaee, chargée de recherche CNRS à l'Ins- von Hausegger, chercheur à l'université d'Oxford sont associés à ce résultat.

Bruno Lévy le dit simplement : « À partir d'une somme de connaissances scientifiques et de notre outil, qui repose sur une théorie mathématique, nous avons construit une “machine à remonter le temps” qui permet, à partir d'une carte du cosmos réalisée en 3D, de reconstituer les mouvements des galaxies depuis les origines. »

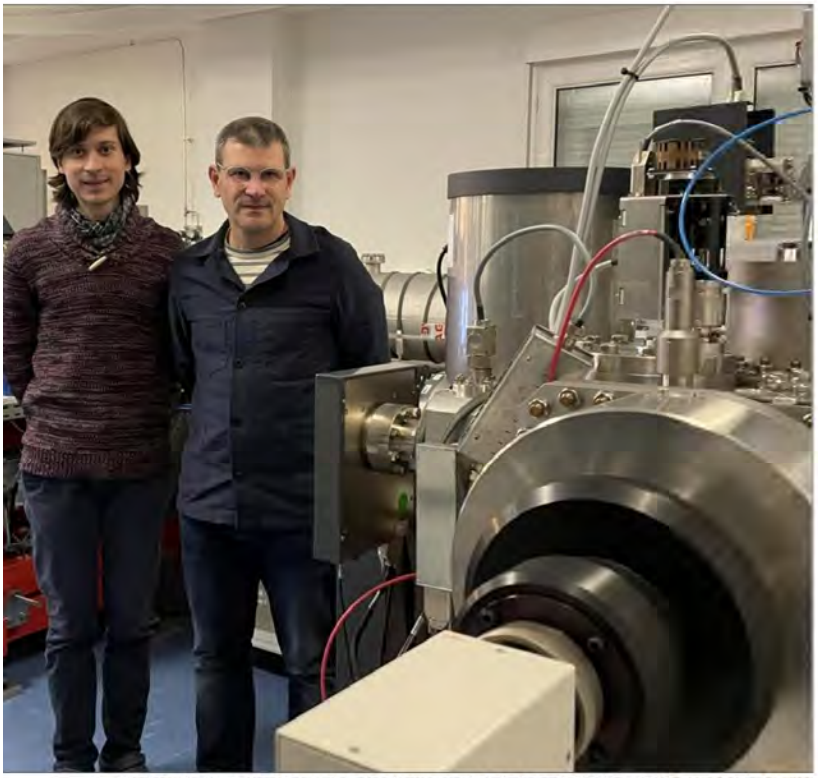
Les chiffres donnent le tournis. À l'heure actuelle, l'outil permet d'explorer 300 millions d'amas de galaxies. L'objectif est fixé gramme de recherche consiste à intégrer à l'outil existant des données réelles issues de l'observation des télescopes et de satellites.

Une ouverture à l'international

« Il nous faut donc concevoir des outils algorithmiques très puissants pour pouvoir analyser rapidement et intégrer ces masses de données observationnelles. C'est un nouveau défi » poursuit Bruno Lévy.

Un nouveau défi qui va s'ouvrir davantage à l'international avec la contribution de deux nouveaux

Bruno Lévy est directeur de l'Institut national de recherche



Maxime Piralla et Yves Marrocchi, chercheurs, au pied de la sonde ionique, qui a permis d'établir les précieux calculs. Photo ER

Le CHRU de Brabois à la pointe du progrès

Le CHRU de Nancy-Brabois et l'équipe portée par le Pr Laurent Peyrin-Biroulet, n° 1 mondial de la maladie de Crohn, y croient beaucoup : le 1er février prochain, une délégation défendra à Paris, auprès du ministère de la Santé, son projet de création de l'institut hospitalo-universitaire (IHU) spécialisé dans les maladies inflammatoires chroniques de l'intestin (MICI).

Le dossier nancéien était en concurrence avec près de 30 candidatures en France. Ce projet de 50M€ est porté par le CHRU de Nancy, l'Université de Lorraine, l'Inserm (Institut national de la santé et de la recherche médicale), avec le soutien de la Métropole du Grand Nancy. Autre exemple, dans un tout autre domaine, le CHRU est centre de référence de la sclérodermie, une pathologie rare qui fait partie de la famille des maladies auto-immunes aux origines encore inconnues. Chez les patients qui en sont atteints, les mains gonflent, les doigts se rétractent, les tissus se raidissent et deviennent comme tannés.

Réactifs, le CHRU et le Loria (laboratoire de l'université de Lorraine) ont lancé, en pleine première vague de coronavirus, une expérimentation d'exosquelette pour soulager les soignants lors du retournement des patients en réanimation.

Nancy inspire les chercheuses

Celle dont les recherches ont abouti à Nancy

En disséquant des météorites, Laurette Piani, cosmochimiste, est parvenue à mettre en évidence la présence d'hydrogène là où nul n'en attendait tant. Photo DR

Laurette Piani, chercheuse au centre de recherches pétrographiques et géochimiques (CRPG) de Nancy, dépendant du CNRS et de l'Université de Lorraine, a ébranlé les théories sur l'origine de l'eau sur Terre.

Trois fois la quantité d'hydrogène des océans

Durant ses travaux, elle a mis en évidence la présence d'hydrogène, un élément chimique qui aurait participé à près de 50 % à la formation de l'eau sur la montrent que les "chondrites à enstatite" (des roches primitives tombées du ciel plus ou moins récemment et conservées dans de bonnes conditions, à l'abri des contaminations terrestres, N.D.L.R.) contiennent suffisamment d'eau pour avoir apporté, au minimum, l'équivalent de trois fois la quantité totale d'hydrogène présent dans l'eau des océans terrestres », rapporte la chercheuse.

Son étude visait à déterminer comment la Terre

Celle qui fait ses recherches à Nancy

Autre domaine d'études aux débouchés attendus dans le contexte actuel, celui de Silvia Lasala : cette chercheuse au laboratoire Réactions et Génie des procédés (CNRS/Université de Lorraine), âgée de 33 ans, vient tout juste de décrocher une bourse européenne d'1,5M€ pour développer de nouveaux fluides, qui devraient révolutionner la production d'électricité.

Le projet de recherche de celle qui enseigne aussi à l'Ensic, nommé « Reacher », vise à expérimenter des fluides capables d'intensifier la conversion de la chaleur, maximiser ainsi la performance des groupes électrogènes comme les centrales électriques à gaz ou à charbon.

En clair, l'idée est de convertir de la chaleur en électricité et du froid en divisant par quatre la dimension des centrales thermiques (et donc leur coût et leur consommation), tout en augmentant leur efficacité.

L'enjeu est évident, à l'heure du changement climatique.

Silvia Lasala vient d'obtenir une bourse d'1,5M€ pour son projet sur le développement de nouveaux fluides qui devraient révolutionner la production d'électricité. Photo DR/Université de Lorraine

Celle qui cible Nancy pour ses études

Lauréate en 2021 du prix Jeunes talents France L'Oréal – Unesco pour les femmes et la science, la presque trentenaire Gabrielle De Micheli poursuit ses recherches aux États-Unis.

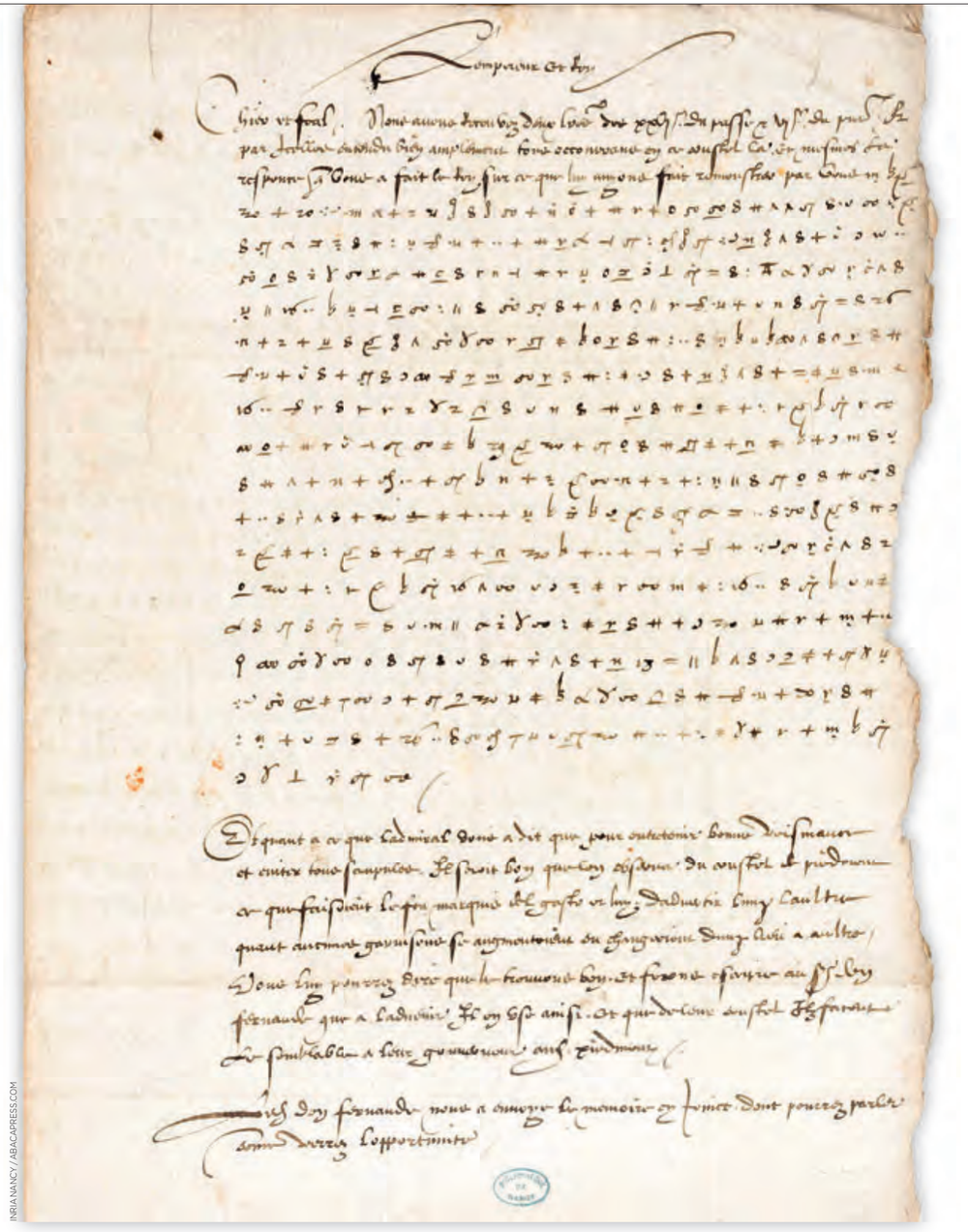
Mais en 2018, cette jeune femme helvète d'adoption, américaine de naissance, italienne par son père et française par sa mère a volontairement choisi Nancy pour son doctorat dans son domaine de recherche : la cryptographie, la science du chiffrage des communications.

Pourquoi ? La ville lui a été

Gabrielle s'est vu conseiller par sa directrice de thèse l'équipe CARAMBA, du Laboratoire lorrain de recherche en informatique et ses applications (Loria) porté par le CNRS, l'Inria et l'Université de Lorraine.

« En fait, je me suis déplacée à Nancy pour travailler avec mes directeurs de thèse, Pierrick Gaudry et Cécile Pierrot. La France possède des instituts de recherche pointus, notamment dans le secteur des mathématiques, des maths appliquées et de l'informatique », témoignait

Informaticienne et cryptoanalyste, Gabrielle De Micheli a reçu le prix Jeunes talents France L'Oréal-



INRIA NANCY / ABACAPRESS.COM

La missive, rédigée en 1547 par Charles Quint et adressée à son ambassadeur auprès du roi de France, comporte quelques passages en clair et de longues séquences chiffrées.

Cryptographie

La correspondance codée de Charles Quint n'a plus de secrets

Une coopération entre cryptographes, informaticiens et historiens a permis de lever le voile sur une lettre « codée » du XVIe siècle. Un système de chiffrement complexe qui permettait à l'empereur de communiquer notamment avec son ambassadeur auprès de François 1er, son ennemi le plus redoutable.

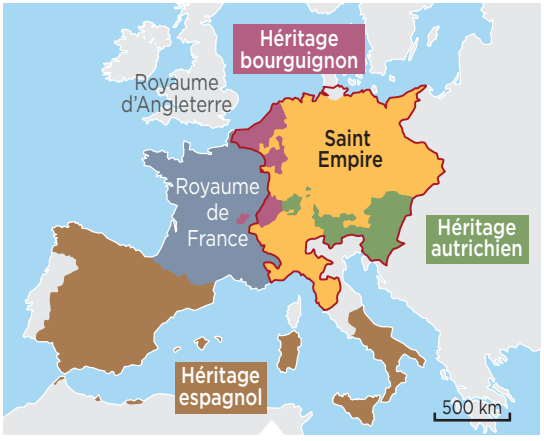
Par Marine Benoit @marin_eben

Lorsqu'un matin de décembre 2021, Cécile Pierrot découvre les pages brunâtres et couvertes de symboles, l'émerveillement la saisit : *« À ce moment-là, je réalise que non seulement la lettre existe bel et bien, mais qu'elle est aussi dans un état de conservation exceptionnel. »* Cette lettre, il s'agit de celle adressée le 22 février 1547 par Charles Quint à son ambassadeur en France Jean de Saint-Mauris. La missive a deux particularités : elle est écrite dans un langage codé et semble avoir totalement échappé aux historiens durant près de cinq siècles, au point qu'il soit tentant de se demander si, sans la détermination de Cécile Pierrot, chercheuse en cryptographie au Laboratoire lorrain de recherche en informatique et ses applications (Loria/université de Lorraine), elle ne serait pas encore restée plusieurs siècles au fond d'un tiroir. Le début de l'aventure autour de cette lettre historique se situe en 2019, lorsqu'au cours d'une soirée, une connaissance parle à Cécile Pierrot d'une *« mystérieuse lettre chiffrée signée de la main de Charles Quint »*. Après une rapide recherche sur Internet, la cryptographe ne trouve nulle trace du document et en déduit que son existence est une légende. Mais voilà que deux ans plus tard, la scène se répète. *« On évoque à nouveau cette lettre au cours d'un dîner. Mais cette fois, la personne n'en a pas seulement entendu parler,* raconte la chercheuse, *elle l'a vue de ses propres yeux, à Nancy. »* Problème : ce témoin précieux ne sait plus où il l'a aperçue. Cécile Pierrot convainc alors sa colocataire, employée au musée des Beaux-Arts nancéien, de mener l'enquête. Par un jeu de bouche-à-oreille, l'amie remplit sa mission : elle établit que la lettre repose sur une étagère du fonds des autographes de la bibliothèque Stanislas. Pourquoi là-bas ? *« Nul ne le sait,* répond la chercheuse. *On ignore aussi depuis quand elle s'y*

CONTEXTE

Un empire menacé par les princes luthériens

Depuis 1494, les guerres d'Italie voient s'affronter rois de France et rois d'Espagne. Néanmoins, des périodes de trêves rythment les campagnes militaires. Le moment où Charles Quint écrit sa lettre à Jean Saint-Mauris s'inscrit dans l'une de ces périodes de « calme avant la tempête ». Le souverain européen le plus puissant de la première moitié du XVIe siècle, dernier monarque à entretenir le fantasme d'un « empire chrétien unifié », est en février 1547 très préoccupé par une rébellion des princes allemands luthériens dirigée par Jean-Frédéric de Saxe et désignée sous le vocable de ligue de Smalkalde, du nom de la ville où princes et villes ont conclu leur alliance. Ceux-ci réclament la reconnaissance du luthérianisme, interdit en vertu de l'édit de Worms de 1521, et sont soutenus par François 1er, ennemi de toujours de Charles Quint. À peine un mois après la rédaction de la lettre, le roi de France meurt et cède son trône à son fils Henri II.



BRUNO BOURGEOIS

La domination européenne de Charles Quint s'est constituée à la suite de trois successions dynastiques et de son élection à la tête du Saint Empire en 1519.

trouve. Elle n'a même pas de cote [référence qui permet de retrouver un document dans une bibliothèque]. » Quoi qu'il en soit, Cécile Pierrot se tient quelques semaines plus tard face au délicat document, prête à relever le défi : découvrir ce que l'empereur du Saint Empire romain germanique avait de si secret à dire à son représentant dans le royaume de son grand rival, François 1er.

« *En voyant la lettre écrite sur pas moins de trois pages, complète et parfaitement lisible, et en partant du principe que celle-ci a été rédigée à la Renaissance, une période précoce pour la cryptographie, j'ai d'abord pensé que j'allais la déchiffrer en quelques heures, deux jours tout au plus.* » Présomption de cryptographe moderne ! Cécile Pierrot confesse en riant qu'il lui faudra plusieurs mois pour en venir à bout. « *Le système de chiffrement était bien plus complexe que je ne l'avais imaginé.* » La mathématicienne découvre en effet que le texte compte plus d'une centaine de symboles, ce qui écarte d'emblée le fait qu'un symbole puisse correspondre à une lettre de l'alphabet. De plus amples recherches lui confirment justement que la mode cryptographique de l'époque consiste à attribuer un symbole à des bigrammes ou à des trigrammes, autrement dit à des assemblages de deux ou trois signes — généralement des lettres de l'alphabet —, formant eux-mêmes un phonème.

Mais ce n'est pas tout : elle découvre que Charles Quint était un adepte des symboles « nuls », c'est-à-dire qui ne correspondent à rien et qui n'ont d'autre fonction que d'embrouiller le lecteur. Face à cette complexité, Cécile Pierrot encode la lettre entière en Python, un langage informatique qui lui permet de réaliser de premières analyses statistiques. De cette manière, la chercheuse peut établir la fréquence des symboles, mais aussi comparer le texte avec un autre de la même époque, traduit également en Python. En l'occurrence avec *Pantagruel*, publié par Rabelais en 1532. Mais au bout de quarante-huit heures, l'ordinateur est à la peine. Et la chercheuse de conclure alors que la puissance de calcul ne lui permettra pas d'aboutir en un temps raisonnable.

Un bond de géant après quatre mois de tâtonnement

« *Il allait falloir faire les choses à l'ancienne. J'ai donc appelé des collègues pour leur demander de jouer avec moi* », plaisante la jeune femme. Ainsi débarquent dans la partie deux autres chercheurs en informatique du Loria, Paul Zimmermann et Pierrick Gaudry, spécialistes de la factorisation des nombres entiers. De février à juin 2022, tous trois avancent à petits pas, entre observations à l'œil nu et réponses obtenues grâce à l'ordinateur. Ils voient notamment des motifs apparaître : trois ou quatre symboles d'affilée se répètent plusieurs fois et, à deux endroits, pas moins de 11 symboles sont alignés dans le même ordre, signe qu'ils tiennent sans doute là un mot entier. « *Malgré tout, nous n'arrivions pas à don-*


CEDRIC JACQUOT/MAXPPP

« En voyant la lettre, complète et parfaitement lisible, j'ai pensé que j'allais la déchiffrer en quelques heures, deux jours tout au plus »

Cécile Pierrot, chercheuse en cryptographie au Loria (CNRS-université de Lorraine), à Nancy

ERIC VANDEVILLE / AKG IMAGES

Le roi François Ier et l'empereur Charles Quint signent un traité le 18 juin 1538, appelé la paix de Nice, mettant fin à la huitième guerre d'Italie et instaurant une trêve de dix ans entre les deux belligérants, après vingt-cinq années d'affrontements.

ner du sens à ce que l'on voyait, même en ayant quelques certitudes », se rappelle Cécile Pierrot. « *Après quatre mois à tâtonner, nous avons estimé qu'il nous fallait un coup de pouce dans un domaine que nous ne maîtrisions pas et qui pourrait peut-être nous mettre sur de nouvelles pistes.* » Ils contactent alors Camille Desenclos, historienne à l'université de Picardie Jules-Verne et spécialiste des relations entre la France et le Saint Empire. Par un heureux hasard, il se trouve que l'experte mène justement un projet d'étude sur l'essor de la cryptographie dans la France des XVIe et XVIIe siècles. Toutefois, la sollicitation est une première pour elle : « *Je suis régulièrement approchée par des amateurs mais jamais par des chercheurs en cryptographie,* confesse-t-elle. *J'étais donc ravie de me lancer dans cette collaboration inédite.* » Camille Desenclos donne aux cryptographes l'information qui leur manquait : il existe à la bibliothèque municipale de Besançon plusieurs dépêches codées de Charles Quint dont le déchiffrement, c'est-à-dire la « traduction » des symboles cryptographiques en clair, fut établi dans la marge au moment de leur réception par leur destinataire. « *À ce moment-là, on fait un bond de géant* », raconte Cécile Pierrot. Car même si des symboles diffèrent entre les courriers, leur méthode de chiffrement est la même. En quelques jours seulement, les chercheurs parviennent alors à reconstituer l'essentiel du système. « *La méthode de Charles Quint est en réalité assez traditionnelle pour le milieu de XVIe siècle* », affirme Camille Desenclos. Mais cette dernière présente une spécificité méconnue que la dépêche de Nancy est l'occasion d'étudier : les voyelles sont figurées par un simple point autour des consonnes, les faisant disparaître un peu à la manière de l'arabe. « *C'est ce qui a rendu la tâche des cryptographes si compliquée.* »

Les pièces du puzzle finissent par s'assembler

Reste quelques mystères à éclaircir, comme une poignée de symboles isolés. Il y a notamment cette « épingle » *(lire l'encadré p. 86)*, qui apparaît à la fin d'une phrase entièrement chiffrée dans laquelle Charles Quint interroge son ambassadeur sur les intentions du roi de France depuis que celui-ci a appris le trépas de la personne désignée par ledit symbole. Cécile Pierrot a l'intuition qu'il s'agit d'un monarque, puisque l'épingle ressemble beaucoup au symbole désignant un roi dans d'autres lettres de Jean Saint-Mauris. Pourtant, Camille Desenclos est formelle : aucun roi n'est mort en janvier ou février 1546, date qui figure au bas de la lettre. « *Après réflexion, j'ai compris que la date n'était pas celle que l'on croyait, pour la simple raison que dans la première moitié du XVIe siècle dans la chancellerie impériale, les changements d'années s'effectuaient encore à Pâques* », détaille l'historienne. Les pièces du puzzle s'assemblent enfin : la missive a en réalité été écrite le 22 février 1547, soit moins d'un mois après le décès d'Henri VIII

CEDRIC JACQUOT/MAXPPP

« Nous n'avions aucune lettre de l'empereur à Jean Saint-Mauris sur cette année 1547. La dépêche de Nancy a permis de remplir un creux »

Camille Desenclos, historienne à l'université de Picardie Jules-Verne, spécialiste des relations entre la France et le Saint Empire

MÉTHODE

Une clé de chiffrement à plusieurs niveaux de complexité

Les cryptographes de Charles Quint n'ont pas facilité la tâche de leurs successeurs du XXIe siècle ! Le tableau ci-contre expose de façon claire les trois grandes astuces employées pour brouiller les pistes des ennemis qui auraient intercepté l'échange. La première consiste à chiffrer sous la forme d'un simple point ou trait toute voyelle lorsque celle-ci est précédée d'une consonne. Ainsi, les syllabes formées d'une voyelle et d'une consonne deviennent des symboles complexes agrémentés d'un point ou d'un trait correspondant à la voyelle souhaitée (seule la position du point autour du symbole change). Ce qui nous conduit à la seconde difficulté : on remarque justement qu'aucun point ou trait ne correspond à la lettre E. Tous ont été volontairement supprimés lorsqu'ils sont liés à une consonne ! Un symbole complexe qui ne comprend aucun point ou trait cache donc forcément un E. Troisième difficulté : la présence de symboles nuls, disséminés parfois au beau milieu d'un mot, et qui doivent être ignorés. Pour le reste, la méthode est plus traditionnelle : chaque lettre a son symbole simple (pour les voyelles, lorsqu'elles commencent des mots ou suivent une autre voyelle, et pour les consonnes, lorsqu'elles ne sont pas suivies d'une voyelle), tout comme les lettres doublées (deux M, deux N…) et certains mots entiers, tous référencés ici. Attention, « con » n'est pas un terme grossier : il s'agit d'une abréviation fréquemment utilisée à l'époque.

BIBLIOTHÈQUE STANISLAS DE NANCY, INRIA NANCY

d'Angleterre, survenu le 28 janvier. Mais alors que dit cette lettre ? Beaucoup de choses sur l'état d'esprit de Charles Quint. *« Nous n'avions aucune lettre de l'empereur à Jean Saint-Mauris sur cette année-là et la dépêche de Nancy nous a permis de remplir un creux »*, se réjouit Camille Desenclos. La prose désormais déchiffrée révèle trois préoccupations majeures du monarque en cette période d'accalmie dans les conflits qui opposent depuis près d'un demi-siècle les rois de France aux rois d'Espagne. *« Accalmie toute relative puisque, au début de l'année 1547, la tension est à son comble entre François Ier et Charles Quint. »* Ainsi, les objectifs de l'empereur sont de maintenir la paix avec le roi français pour ne pas éparpiller ses forces, de mettre fin au conflit qui l'oppose à la ligue de Smalkalde *(lire l'encadré p. 84)*, et d'éviter les assassinats… à commencer par le sien. Charles Quint fait en effet état d'une rumeur qui le tracasse au plus haut point : Pierre Strozzi, chef de guerre au service de François Ier dont le nom est brouillé par des symboles nuls, aurait formulé devant son roi l'intention de l'assassiner. Charles Quint cherche ainsi à vérifier auprès de Saint-Mauris l'exactitude de ces informations et, le cas échéant, il explique vouloir savoir comment François 1er a réagi aux paroles de Pierre Strozzi. *« À cette époque se mène aussi en Europe une virulente guerre de l'information — ou plutôt de la désinformation —, qui consiste en la propagation de rumeurs infondées destinées à embrouiller et déstabiliser les puissances ennemies,* détaille Camille Desenclos. *Il est possible que cette histoire d'assassinat soit l'une d'entre elles. »*

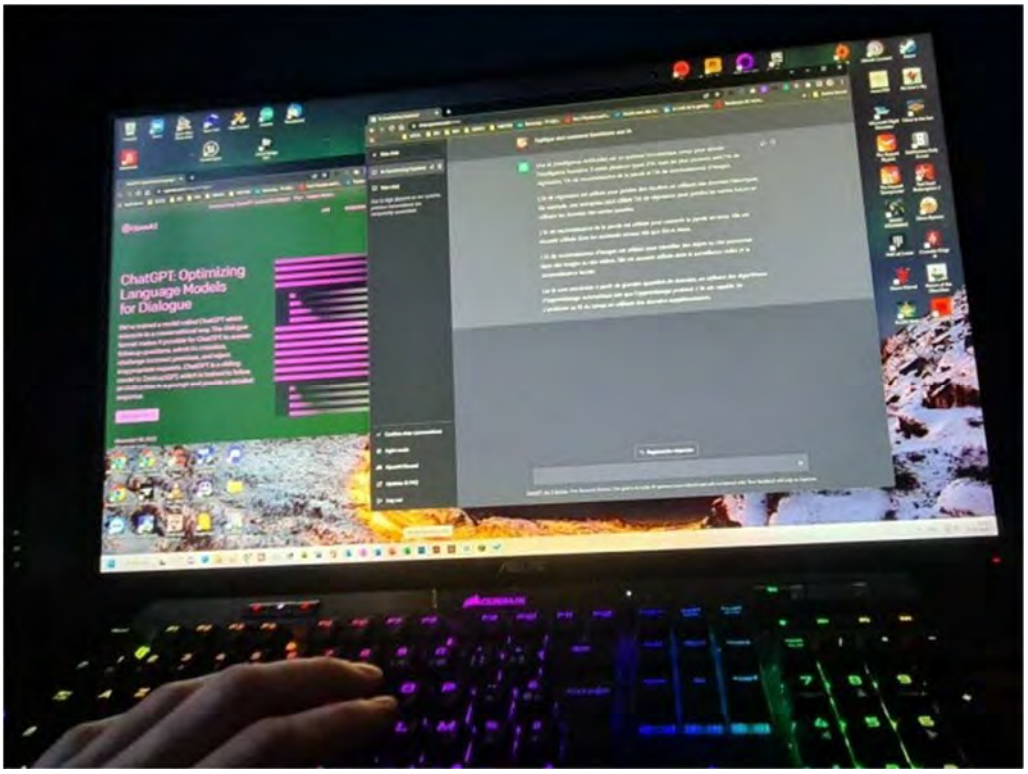
Outre les informations précieuses que la lettre a fini par livrer, son décryptage est un exemple inédit de collaboration fructueuse entre cryptographes et historiens. *« Sans l'aide de Camille Desenclos, nous aurions sans doute mis un temps considérable à la déchiffrer »*, avoue Cécile Pierrot, qui reconnaît également avoir pris goût au décryptage de documents historiques, elle qui d'ordinaire planche sur des systèmes de chiffrage bancaires ou biométriques. Cela tombe bien car selon Camille Desenclos, 2 à 5 % des documents historiques chiffrés le restent encore à ce jour. ■

L’Est républicain, Le Républicain lorrain, Vosges matin, 30 janvier 2023 (1/4)

ChatGPT et enseignement : danger ou opportunité ?

L’assistant virtuel ChatGPT fait rêver autant qu’il inquiète, notamment le monde de l’enseignement. Car les capacités bluffantes de cette application utilisant l’IA et la manière dont elles pourraient être détournées questionnent. Pourtant, des chercheurs lorrains évoquent aussi un nouvel outil pédagogique.

Hervé BOGGIO



ChatGPT : un outil conversationnel aux capacités bluffantes. Photo Ebra /Jean-Michel LAHIRE

Tout le monde en parle et, il faut bien l’admettre, l’expérience a quelque chose de bluffant ! On peut tout demander à ChatGPT, l’outil conversationnel en ligne (gratuit) utilisant l’intelligence artificielle (IA), développé par la société américaine OpenAI. Ou presque : il a « digéré » la quasi-totalité des données disponibles sur la toile jusqu’en 2021. Pour l’instant.

Ce qui ne l’empêche pas de commettre parfois de grossières erreurs factuelles et ne prévient pas les utilisations malveillantes qui pourraient en être faites, qu’on se le dise ! Mais si on lui demande, par exemple, de rédiger un article sur ses propres applications possibles à l’université, il ne met que quelques secondes à générer le texte suivant : « *ChatGPT permet aux étudiants de générer rapidement et facilement du contenu de qualité pour leurs travaux écrits. […] Ils peuvent générer des résumés, des synthèses, des citations et même des parties entières de leurs devoirs. Cela leur permet de gagner du temps et de se concentrer sur les aspects les plus importants de leur travail, comme la compréhension des concepts clés et la réflexion critique. En outre, ChatGPT peut également être utilisé par les enseignants pour créer des quiz, des examens et des activités d’apprentissage interactives pour leurs étudiants. Le modèle peut générer des questions et des réponses aléatoires pour des tests de connaissances, […] créer des examens uniques pour chaque étudiant. Cela réduit les risques de triche et rend l’apprentissage plus intéressant […]. Enfin, ChatGPT peut également être utilisé pour améliorer la communication entre les étudiants et les enseignants. Les étudiants peuvent utiliser le modèle pour rédiger des courriels et des messages à leurs enseignants, ce qui les aide à exprimer clairement leurs pensées et à améliorer leur rédaction. […] En résumé, ChatGPT est un outil puissant qui peut être utilisé à l’université pour améliorer l’apprentissage, la communication et la productivité. […]* »

Nouvel outil

Rien de révolutionnaire mais un texte, simple, efficace et rédigé sans la moindre faute d’orthographe ou de syntaxe. Avec, cerise sur le gâteau, une ébauche de plaidoyer *pro domo* sur la façon dont l’appli peut même constituer, déjouant certaines des craintes ordinairement formulées depuis quelques semaines, un moyen de lutte contre la triche et d’optimisation des apprentissages.

Un « avis » qui recoupe celui de Jean-Paul Haton, chargé de mission Intégrité scientifique et spécialiste de l’IA au sein du Laboratoire lorrain de recherche en informatique et ses applications (Loria, Université de Lorraine, CNRS, Inria) : « Je suis très étonné de la réaction d’universités américaines notamment, qui préconisent le bannissement de cet outil. Nous sommes devant une avancée qui me fait penser aux premiers correcteurs orthographiques : il faut avoir l’esprit plus ouvert, considérer que ChatGPT est un nouvel outil pédagogique qui pourra être très utile à condition, bien entendu, de s’adapter ! » En attendant, le monde de l’enseignement dans son ensemble est en pleine réflexion sur le sujet, tandis que Sciences Po Paris, dont une antenne est installée à Nancy, a d’ores et déjà interdit son utilisation … Néanmoins, pour le spécialiste lorrain, qui travaille sur ces concepts depuis près de quarante ans, c’est plus la peur de la nouveauté que le danger réel qui entraîne ces réactions. Un problème que ne connaissent pas les IA : par définition, elles n’ont aucune émotion.

https://www.youtube.com/watch?v=jrH2EVEhCVw

Quant à prévenir la triche, facile : la machine a une orthographe irréprochable, dans la plupart des cas, cela suffira à mettre la puce à l’oreille des enseignants…

L’Est républicain, Le Républicain lorrain, Vosges matin, 30 janvier 2023 (3/4)

Christophe Cerisara : « Les possibilités d’application sont immenses »

Enseignant et chercheur au Laboratoire lorrain de recherche en informatique et ses applications (Loria, Université de Lorraine, CNRS, Inria) à Nancy

Propos recueillis par Hervé BOGGIO

Christophe Cerisara, chercheur au Laboratoire lorrain de recherche en informatique et ses applications (Loria, CNRS) à Nancy. Photo UL

En quoi l’outil ChatGPT est-il révolutionnaire ?

Christophe CERISARA : « En fait, i l y a très longtemps que des chercheurs se penchent sur le traitement du langage. Il y a eu deux révolutions en la matière : la première en 2012 avec les premiers réseaux neuronaux artificiels et la seconde avec l’invention des outils de type Transformer dont les capacités extraordinaires en matière de traitement du langage ont permis la mise au point de ChatGPT »

Quel est le principe de cet outil ?

« En réalité, c’est un outil qui est capable d’absorber des quantités gigantesques de données. Il les retient par cœur puis les compresse et peut ensuite en extraire ce que l’on appelle des patterns, que l’on peut assimiler à une sorte de raisonnements. Quand il apprend un texte, il le projette dans un espace numérique au sein duquel il va générer ces raisonnements. C’est un système qui est bien au-delà de la simple base de données : prenez l’exemple d’une suite arithmétique très longue, ChatGPT va être capable de l’apprendre par cœur mais aussi de « comprendre » la façon dont elle est construite pour trouver la suite. C’est cette

capacité à générer du raisonnement qui lui permet, grâce à ce qu’on lui a donné à « manger », de répondre de manière bluffante aux questions qu’on lui pose en langage naturel. C’est peut-être là qu’est la singularité de cet outil, sa capacité à s’entraîner grâce à ce que l’on appelle le *Reinforcement Learning from Human Feedback* (RLHF) : des interventions humaines qui permettent d’analyser les réponses de l’outil et de lui indiquer quand il fait erreur et quand il est dans le vrai sur le fond et la forme afin de le renforcer **».**

Comment ChatGPT sait-il autant de choses ?

« L’automne dernier, au moment de son lancement public, il avait été « nourri » avec l’ensemble des données disponibles sur le web depuis l’origine jusqu’à septembre 2021. C’est énorme ! De fait, les possibilités d’application sont immenses. Et des mises à jour auront sans doute lieu puisque contrairement à ce qui est parfois prétendu, ChatGPT n’est pas connecté à l’internet. »

Quid du risque d’utilisation frauduleuse dans l’enseignement par exemple ?

« Le plus de ChatGPT par rapport aux autres moyens de tricher, c’est la rapidité qu’il permet. Si un étudiant veut plagier plutôt que de produire un travail original, il pourra le faire plus vite et facilement. Mais cela ne change pas fondamentalement la donne. »

100% Jeunesse du 06 février 2023

MOSELLE TV - CULTURE
1,16 k abonnés
S'abonner

2 | Partager | Enregistrer

367 vues 7 févr. 2023
100% Jeunesse, c'est l'émission nouvelles générations. Présentée par Valentin Piovesan elle offre un coup de projecteur à la jeunesse mosellane, à ses passions et à ses interrogations.

Les invités de ce numéro :

Servane Diafferia-Acevedo Reyes - fondatrice et militante de la Grenade, un collectif féministe
Jean-Paul Haton - Professeur émérite à l'Université de Lorraine
Guillaume Jappain - Producteur du film "Les suicidés"
Lucas Schlachter - Mister National 2023

« Une opportunité pour susciter un esprit de défense »

Jean-Christophe VINCENT - 08 févr. 2023 à 20:38 - Temps de lecture : 2 min

Pour le colonel Eric Koessler, commandant de la base de défense de Nancy, « il y a aujourd'hui une vraie prise de conscience sur la nécessité de se préparer aux cyberattaques ». Photo ER /Alexandre MARCHI

Pour le colonel Eric Koessler, commandant la base de défense de Nancy depuis le mois d'août 2022 , l'exercice Cyber Humanum Est est une « illustration exemplaire » du partenariat liant la base de défense avec l'Université de Lorraine et la Métropole du Grand Nancy.

« Ce partenariat est né autour du laboratoire de haute sécurité du LORIA (Laboratoire lorrain de

Le Monde, 8 février 2023 (1/3)

Une cinquantaine de lettres cryptées de Marie Stuart retrouvées et déchiffrées

Florence Rosier

Ces missives adressées à l'ambassadeur de France en Angleterre entre 1578 et 1584 dormaient à la Bibliothèque nationale de France. Leur auteur était inconnu, mais un trio de chercheurs a cassé leur code : c'est la reine maudite Marie d'Ecosse qui les a écrites.

« Je sais que vous avez eu soin, au nom du roi [de France], d'atténuer les éclats de colère de la reine contre moi qui ne lui souhaite que du bien malgré tout le mal que j'ai reçu d'elle. » La femme qui écrit cette lettre poignante, en juin 1578, est une reine captive et malheureuse. Une série de coups du sort s'est abattue sur sa tête – avant qu'elle ne la perde, cette tête, sous la hache d'un bourreau ivre qui s'y prendra à trois fois pour la lui trancher, le 8 février 1587.

Cette reine, c'est Marie Stuart (1542-1587), une des figures les plus tragiques de l'histoire. La « reine maudite » par excellence, selon l'image popularisée par Stefan Zweig. Quand elle écrit cette lettre, elle a 35 ans. Cela fait plus de neuf ans qu'elle est emprisonnée par sa cousine, la reine d'Angleterre, Elisabeth Ire. Arrière-petite-fille du roi Henri VII, Marie Stuart peut en effet prétendre au trône d'Angleterre ; elle est même la seule prétendante légitime reconnue par les catholiques. Pour Elisabeth la protestante, Marie la catholique représente donc une sérieuse menace. C'est pourquoi elle la fera emprisonner plus de dix-huit ans – jusqu'à son exécution.

Cette lettre est une des 57 missives de la reine déchue qui dormaient, orphelines, à la Bibliothèque nationale de France (BNF). Des lettres cryptées dont ni l'auteur ni le contenu n'étaient connus. La clé utilisée pour les chiffrer était « le nec plus ultra de la cryptographie de l'époque », souligne George Lasry, informaticien et cryptographe.

George Lasry est l'un des trois chercheurs qui, avec Norbert Biermann, pianiste et professeur de musique, et Satoshi Tomokiyo, astrophysicien, sont parvenus à casser le code de cette mystérieuse correspondance, un travail de détective relaté dans la revue Cryptologia du 8 février. Ce trio de passionnés œuvre, à ses heures « perdues », à déchiffrer des documents cryptés historiques. Des électrons libres, opérant toutefois dans le cadre d'un projet académique, Decrypt, mobilisant des universités européennes, dont l'Université de Lorraine et son laboratoire de recherche en informatique et ses applications (Loria).

Une « découverte fabuleuse »

Coup de théâtre : ces lettres étaient donc de la main de la reine Marie Stuart. Une « découverte fabuleuse sur les plans littéraire et historique, la plus importante réalisée depuis cent ans sur Marie reine d'Ecosse », s'enthousiasme John Guy, expert de cette période mouvementée de l'histoire britannique à l'université de Cambridge (Royaume-Uni). Un filon à exploiter, aussi, pour les historiens.

Les auteurs ont parcouru la collection numérisée de la BNF, mise en ligne et accessible à tous. « Nous sommes tombés sur un ensemble de documents chiffrés utilisant les mêmes symboles graphiques », raconte George Lasry. Ils étaient censés concerner l'Italie. Mais « après avoir commencé à déchiffrer quelques lettres, nous avons vite réalisé qu'elles étaient écrites en français et n'avaient rien à voir avec l'Italie. De plus, les participes et les adjectifs étaient conjugués au féminin », poursuit l'informaticien. L'auteur des lettres, par ailleurs, mentionne à plusieurs reprises sa captivité et le nom de Francis Walsingham, le maître-espion de la reine Elisabeth. Autant d'indices qui mettront nos fins limiers sur la piste de Mary Stuart.

Le code utilisé dans ces lettres fait appel à 191 symboles différents. Il s'agit d'un code « homophonique » : chaque lettre de l'alphabet est codée par un ou deux symboles différents. En plus, certains symboles désignent un personnage précis : la lettre C pour le roi de France (Henri III) ou la lettre f pour la reine Elisabeth, par exemple. D'autres désignent des noms de lieux ou des parties de mots (comme le suffixe « ance »).

Pour casser ce code, les chercheurs ont développé un algorithme. « Nous commençons par attribuer au hasard des symboles aux lettres de l'alphabet, puis nous regardons si nous trouvons ainsi des mots français. Le procédé est répété de façon itérative pour améliorer peu à peu le résultat », explique George Lasry. Pour les symboles codant des noms, les chercheurs se sont aidés du contexte historique. Quand Marie parle de son beau-frère « k », par exemple, il ne pouvait s'agir que du duc d'Anjou. Au total, le trio mettra près d'un an avant de découvrir la clé de chiffrement.

« Une politicienne avisée »

A qui s'adressaient ces lettres ? L'immense majorité (53 sur 57) étaient destinées à l'un des rares alliés de Marie Stuart : Michel de Castelnau, ambassadeur de France en Angleterre. Toutes datent de 1578 à 1584, soit « six des années les plus importantes de sa captivité », relève John Guy. Une cinquantaine étaient inconnues des historiens.

Ces lettres livrent un inestimable témoignage. Cette reine sans royaume se plaint de ses conditions de captivité et de sa mauvaise santé. « Je vous prie de demander à la reine d'Angleterre de me permettre de me servir de ma voiture, car je suis retombée dans ma vieille "défluxion nerveuse" », écrit-elle ainsi à l'ambassadeur de France en juillet 1581.

Loin de se contenter de s'apitoyer sur son sort, Marie raconte aussi ses négociations avec la reine Elisabeth Ire en vue de sa libération. Elle juge, non sans raison, qu'elles ne sont pas menées de bonne foi. Marie se montre ici « un juge avisé de la psychologie humaine, capable d'évaluer les forces et les faiblesses de caractère des principaux acteurs, analyse John Guy. Plusieurs de ces lettres sont particulièrement importantes car elles concernent l'époque où la reine Elisabeth envisageait d'épouser le duc d'Anjou, frère et héritier d'Henri III de France ».

Marie, ajoute l'historien, apparaît dans ces lettres « une politicienne avisée, qui comprenait les machinations de politique internationale et était prête à se battre pour ce en quoi elle croyait ». Loin de son image de femme fatale ou de victime passive qui passait son temps à geindre et à broder, « elle disposait de sources de renseignements étonnamment variées (et en grande partie exactes) sur les événements en cours en Angleterre, en Ecosse et en France. Et elle était en contact, souvent directement, avec les principaux acteurs politiques et conseillers privés d'Angleterre ».

« Méfiez-vous de Walsingham »

Marie se montre aussi en mère éplorée. « Je viens d'apprendre la nouvelle de l'enlèvement de mon fils par les partisans du comte d'Angus, s'angoisse-t-elle en septembre 1582. Je suis clouée au lit, si troublée que je ne sais pas quoi dire ou faire, voyant mon fils aux mains de nos plus cruels ennemis (…) sans pouvoir aider ou obtenir du soutien (…). Je souhaite que le roi envoie quelque noble de qualité en Ecosse pour remettre les choses en ordre. » Ce fils, Jacques VI d'Ecosse, n'aura de cesse de la renier en embrassant la cause protestante. A la mort d'Elisabeth, il deviendra roi d'Angleterre sous le nom de Jacques Ier.

Marie Stuart, une femme réputée intelligente qui parlait cinq langues, écrivait parfaitement en français, « avec des phrases très longues », indique George Lasry. Sa propre mère, Marie de Guise, lui avait appris enfant à écrire des lettres chiffrées. A-t-elle écrit et encodé elle-même ces lettres ? « On l'ignore, de même qu'on ne sait pas qui a conçu ce code », admet George Lasry.

A la fin de sa vie, Marie Stuart se montrera d'une étonnante imprudence. En janvier 1580, pourtant, elle avait été clairvoyante. « Méfiez-vous de Walsingham, car c'est un homme rusé, qui cache ses véritables intentions sous le prétexte d'une (fausse) amitié », écrit-elle alors à l'ambassadeur de France. Mais elle tombera dans le piège que lui tendra bientôt le retors espion de la reine, en l'entraînant dans un complot contre la reine. « Le 17 juillet 1586, Marie Stuart signera une lettre ambiguë qui la perdra car elle semble y cautionner l'assassinat d'Elisabeth », raconte Isabelle Fernandes, spécialiste des XVIe et XVIIe siècles britanniques à l'université Clermont-Auvergne. Sans doute parce que, « le temps passant, elle s'est lancée dans des causes désespérées dans l'espoir d'être libérée ».

Reste une énigme. Comment se fait-il que le code des lettres adressées par Marie Stuart à Anthony Babington – un des instigateurs du complot contre Elisabeth – en 1586 soit « bien plus simple et bien moins sécurisé », selon George Lasry, que le code de ses lettres antérieures – celles qui viennent d'être déchiffrées ? Un paradoxe « bien surprenant », relève-t-il, car « le contenu de sa correspondance avec Babington était bien plus sensible et compromettant pour Marie Stuart ». Une fois la lettre du 17 juillet 1586 interceptée par Walsingham, la cause était entendue : en octobre, Marie sera condamnée à mort pour haute trahison. « Loué soit Dieu, vous me faites un grand bien de me retirer de ce monde ! », lancera l'infortunée.

Reportage CYBERSÉCURITÉ | DÉFENSE | GRAND-EST

Au jeu de rôle du Comcyber à Nancy, les étudiants s'entraînent à la cyberguerre

Pendant trois jours, une centaine d'étudiants nancéiens en informatique et veille stratégique ont participé à un vaste jeu de rôle sur le thème de la cyberdéfense, sous la direction de leurs enseignants et de l'armée. L'Usine Digitale a rencontré les participants, épuisés mais exaltés par un exercice qu'ils préparent depuis le début de l'année universitaire.

Louis de Briant

09 février 2023 15h55

9 min. de lecture

Réagir →

© Louis de Briant

La "Blue Team" de l'équipe Anumeric a pour rôle de défendre les machines du groupe contre les assauts de l'équipe adverse. Elle est rassemblée sur le site de Télécom Nancy.

Imaginez l'archipel des Maldives, perdu quelque part dans l'immensité de l'Océan indien. Parmi son cheptel d'îles, le petit Etat-nation des Riverchelles est aux abois. La montée des eaux menace le modèle économique de l'archipel, fondé en grande partie sur le tourisme. Ses ressources minières pourraient représenter son salut, mais l'archipel n'a pas les moyens de les exploiter lui-même.

Il compte proposer une concession, soit à l'île d'Anumeric, soit à celle du Cryptanga. Les ingénieurs des deux concurrents, et leurs conseillers en communication, rivalisent d'ingéniosité et de fourberie pour remporter le contrat. A moins qu'une équipe indépendante de mercenaires ne fasse capoter toute l'opération…

SÉLECTIONNÉ POUR VOUS

La pénurie de talents en cybersécurité, une épine dans le pied des entreprises françaises

Cybersécurité : Après l'interdiction de ses logiciels, Kaspersky quitte les États-Unis

Atos échappe au naufrage, sauvé par un accord définitif avec banques et créanciers

Ce n'est pas un scénario de film, mais d'un exercice de cyberguerre : le Cyber Humanum Est. Mené sur trois jours, du 6 au 8 février 2023, il rassemble une centaine d'étudiants nancéiens de la Faculté des Sciences et Technologie, l'UFR des sciences humaines et sociales, l'IUT Nancy-Brabois, Mines Nancy, Polytech Nancy, et Télécom Nancy, sous la direction de leurs professeurs et du Commandement de la cyberdéfense (Comcyber) du ministère des Armées.

L'exercice est conduit de façon parfaitement sécurisée, sur 200 équipements virtuels et réels élaborés par les équipes de Loria, le laboratoire lorrain de recherche en informatique. *"Grâce aux machines virtuelles, les étudiants peuvent faire toutes les bêtises qu'ils veulent sans risque pour le vrai réseau"*, explique Christophe Boutier, responsable informatique de Télécom Nancy devant les deux serveurs de l'école utilisés pour le jeu. Tous les malwares utilisés pour le jeu sont inutilisables en dehors de cet environnement, nous rassure-t-on.

Savoir et faire savoir, b.a.-ba de la cyberguerre

Au sein de la caserne Blandan, à Nancy, les étudiants sont rivés à leurs écrans d'ordinateur. L'ambiance se veut studieuse mais tendue : le jeu se termine le soir même, à 18 heures. *"On entre dans la dernière phase du jeu, où on envoie tout ce qu'on a pour récupérer des contacts et discréditer l'adversaire"*, explique Julien, 22 ans, en troisième année aux Mines Nancy et commandant de l'équipe des Anumeric, composée de quarante personnes. Dans la dernière ligne droite, succès et échecs s'enchaînent à un rythme effréné. *"On a trouvé la machine qui hébergeait le journal des Cryptanga, mais les mercenaires ont réussi à attaquer notre système monétaire et à voler tout notre argent"*, regrette-t-il.

Evidemment, la réponse de l'équipe adverse ne s'est pas fait attendre. *"Il semblerait que votre économie souffre un peu en ce moment"*, observe un post moqueur des Cryptanga, diffusé sur le réseau social fermé créé spécialement pour le jeu. L'exercice de cyberguerre, qui en est à sa troisième édition, accueille pour la première fois des étudiants en master "veille stratégique et condition des organisation des connaissances", spécialisés en communication de crise. *"On essaie de faire monter en gamme une armée cyber, qu'elle soit civile ou militaire,* explique le capitaine Jean-Philippe. *Le cyber est un travail conjoint aujourd'hui."*

Les élèves ont travaillé au même rythme que leurs homologues ingénieurs, soit une fois par semaine depuis le début de l'année. Malgré leurs spécialités très différentes, ils ont appris à se comprendre. *"Parfois, ils nous parlent en chinois,* s'amuse Maurine, 21 ans. *On était un peu timides au début, mais maintenant le groupe est très solidaire."* Communiquer efficacement sur les succès – et ridiculiser les fautes de l'adversaire – est indispensable pour espérer remporter le contrat. "*Nous tenons à rassurer la population des Riverchelles, qui semble actuellement frileuse à l'idée de travailler avec le Cryptanga",* assure un message des étudiants en veille stratégique. *"Attention à ton vocabulaire, coopérer serait préférable",* souligne Maurine.

La gestion de crise semble porter ses fruits : *"Regarde, on a cet internaute dans la poche"*, se réjouit la jeune femme devant un commentaire laudateur sur le faux réseau social, sans doute écrit par un enseignant. *"Celui-là, il est assez critique d'habitude"*, fait remarquer Florent, 25 ans. *"Il n'est pas contre nous, c'est ce qui compte",* rétorque Maurine. Les étudiants sont aussi formés à débusquer les fake news ; le matin même, ils ont repéré un faux message du président chinois Xi Jinping à l'adresse de "leur" présidente, qui multipliait les fautes dans les dates et les noms.

Les encadrants, deus ex machina au sens propre

Quelques rues plus loin, dans les locaux de Polytech Nancy, la "Red team" des Cryptanga s'affaire à prendre le contrôle des machines adverses. Les rangées de tables sont jonchées de fils, d'ordinateurs et de rations de survie. Commandants et communicants sont séparés des ingénieurs cyber, qui échangent via un forum Discord. *"Ce n'est pas parce qu'une faille a été détectée sur un serveur qu'on fait le 'patch'*, prévient le capitaine Jean-Philippe. *L'attaquant est obligé d'en rendre compte, tout doit être documenté et validé." "On ne leur apporte pas qu'une expertise technique, nous fournissons aussi une méthode de commandement"*, ajoute le capitaine Sébastien, réserviste au Comcyber.

Au premier jour du jeu, les attaquants n'en étaient encore qu'à la phase de reconnaissance. *"On a cherché à définir ce qui nous appartenait,* se souvient Gwenaël, 22 ans, en informatique à Polytech Nancy et chef des attaquants Cryptanga. *On a cartographié toutes les failles qu'on repérait"* en coordination avec l'équipe de défense, logée dans une salle adjacente. À partir de leurs observations, ses équipes sont parvenues dès lundi soir à pirater les comptes bancaires des Anumeric.

Gwenaël, chef des attaquants Cryptanga : *"Nos machines tournent en permanence et nos mots de passe sont changés toutes les demi-heures."*

Quelques salles plus loin, les ingénieurs Cryptanga sont même parvenus à pénétrer dans l'ambassade des Anumeric et à écouter les échanges entre le clavier Bluetooth et l'ordinateur du diplomate. *"On a passé neuf heures à chercher le mot de passe pour pirater le flux vidéo de la caméra de surveillance"*, relate Alexandre, 20 ans, en licence cyber à l'IUT Nancy-Brabois. Quant à la porte de l'ambassade, "*les encadrants nous ont ouvert, une fois que le soldat Playmobil qui la gardait avait été neutralisé*". Comment, nous ne le saurons jamais.

Il arrive en effet que la Providence intervienne, sous la forme d'un militaire ou d'un enseignant. Encore faut-il savoir la reconnaître. "*La direction de Télécom a mis une photo sur Twitter avec des infos compromettantes pour les Anumeric*", exulte Julien,

persuadé de la bonne foi de ce post. En cas d'erreur ou d'oubli, gare aux retours de flamme. *"Un soir, nous avions laissé nos postes non verrouillés. Les militaires en ont pris des photos et les ont postées sur le forum commun, avec nos adresses IP et des preuves qu'on avait pris le contrôle de machines adverses."* Ses équipes ont été priées de faire un peu plus attention à leur hygiène numérique.

La "Blue Team" de l'équipe Cryptanga, dans les locaux de Polytech Nancy. *"J'essaie de trouver des failles dans nos systèmes ; comme nos machines sont très similaires, je préviens ensuite les attaquants"*, explique Michaël, 26 ans, en master à Télécom Nancy.

"Et si la cybersécurité était votre avenir ?" demande l'armée aux jeunes

Ce "wargame", que tous préparent depuis des mois, a des applications très concrètes selon les élèves. "*On a déjà eu des problèmes de cybersécurité,* pointe Julien, en alternance dans une entreprise avec de nombreux data centers. *Cela peut arriver tous les jours, ce n'est pas juste un jeu."* Maurine nuance : *"Dans l'exercice, il y a trop de comptes extrémistes par rapport à la réalité. Mais c'est un projet très utile, car il rend tous les scénarios sur lesquels on avait travaillé complètement obsolètes."*

Pour preuve de ces liens entre réel et virtuel, des représentants du fabricant de tuyauteries Saint-Gobain sont présents à Polytech Nancy. Les élèves doivent pirater les bases de données de maquettes de hauts-fourneaux fournies par l'entreprise, et essayer d'altérer la qualité de leur production. "*Notre intérêt, c'est de voir les failles dans notre matériel, ou les liaisons qui pourraient être piratées",* détaille Olivier Bertin, agent de maîtrise principal. Le fabricant a été approché par les militaires eux-mêmes, afin de remplacer les maquettes en Lego des éditions précédentes.

Deux étudiants face à l'une des maquettes de Saint-Gobain. *"Les jeunes attaquent beaucoup la base de données, pas assez la machine elle-même"*, remarque l'agent de maîtrise principal.

L'armée profite aussi de ces trois jours pour repérer les meilleurs éléments, qu'elle espère voir postuler au job dating qu'elle organise le 10 février pour les étudiants, intitulé "Et si la cybersécurité était votre avenir ?" *"Il y a une prise de conscience des enjeux autour de la cyber depuis une dizaine d'années, il faut augmenter les effectifs pour pouvoir faire face"*, reconnaît le colonel Eric Koessler, commandant de la base de défense de Nancy et responsable pour la zone Est du Commandement de la cyberdéfense. 3 700 personnes travaillent aujourd'hui au sein de la cyberdéfense ; l'objectif de l'armée est d'en compter 5 200 en 2025.

Le nom du vainqueur annoncé jeudi soir

Après deux jours et une nuit blanche sous caféine, les élèves sont de leur propre aveu *"au bout du rouleau"*. *"On met plus de temps à répondre aux attaques"*, avoue Julien, capitaine des Anumeric. Pierre, 23 ans, en troisième année d'informatique à l'école des Mines Nancy, s'est reposé *"deux heures et demi la nuit dernière, les bras en croix, sur mon poste"*, raconte-t-il en mimant la position. Les étudiants ont pu compter sur les conseils des réservistes, qui les ont aidés à élaborer des calendriers de repos. Certains ont apporté des sacs de couchage, d'autres ont préféré le retour à la vie civile et dormi dans de vrais lits.

Le nom du vainqueur sera annoncé jeudi soir, en fonction de la qualité des attaques, de la défense, de l'influence exercée et des codes rapportés par les deux équipes. A moins qu'une troisième équipe ne remporte la mise. *"Nous ne sommes du côté de personne, mais nous avons été sollicités par des indépendantistes des Riverchelles qui souhaitent que le pays conserve sa souveraineté"*, déclare Pierre, regroupé avec dix-neuf autres "pirates" dans une salle de la caserne Blandan. Son fait d'armes : avoir hacké le journal des Anumeric, et fait figurer le drapeau pirate en lieu et place du logo de la gazette. Un rôle *"cool"*, admet le jeune homme, mais frustrant car *"on est obligés d'attaquer en permanence"*.

A quelques heures de la fin du jeu, les étudiants retrouvent le goût des choses simples. *"Ce serait sympa de dormir dans un lit, de se doucher, de manger un vrai repas !"* rêvasse Pierre. *"Tu crois qu'ils nous laisseront ?"* demande un compagnon de galère, alors que la journée du lendemain doit être consacrée aux retours sur l'exercice. *"Rien n'est moins sûr"*, sourit Pierre, déjà occupé à lancer une nouvelle attaque. Il n'est jamais facile de retourner à la vie civile.

IDMC - Université de Lorraine

Des profils recherchés à la rencontre des recruteurs

L'Institut des sciences du Digital, Management & Cognition organise chaque année le **FAN, Forum de l'Avenir dans le Numérique**. Les étudiants viennent en quête de stages et de débouchés professionnels, les entreprises recherchent des bons profils pour compléter leurs équipes.

« *Le FAN est aussi l'occasion pour nous de garder le contact avec les anciens étudiants !* » se réjouit **Antoine Tabbone, dynamique directeur de l'Institut depuis 2019**. Les étudiants de l'IDMC (anciennement UFR mathématiques et informatique), viennent au FAN (Forum de l'Avenir dans le Numérique) rencontrer ces alumni, entreprises et grands groupes pour discuter de leur parcours et de débouchés professionnels.

Le FAN, organisé par l'IDMC et le bureau des étudiants, attire chaque année davantage de sociétés - start-up ou grands groupes, à la recherche de jeunes talents de l'IDMC. **À Nancy, l'IDMC forme des experts en sciences du numérique, en sciences cognitives et en traitement automatique des langues. Des profils très recherchés par les entreprises pour leur pluridisciplinarité et leur compétences multiples.** « *Nous proposons le choix de la formation en alternance, qui débouche le plus souvent sur une embauche. C'est une possibilité que j'ai encouragée afin de permettre aux étudiants de mobiliser des connaissances et du savoir pour l'acquisition de compétences en entreprise* », souligne Antoine Tabbone. Chaque année, l'IDMC accueille davantage d'étudiants. De 400 en 2014, ils sont environ 650 cette année.

« *Les diplômes proposés suivent l'évolution du marché professionnel. Nous souhaitons aussi adapter les contenus afin d'avoir, d'une part une orientation vers la science des données, et d'autre part vers l'expérience numérique et l'intelligence artificielle centrée sur l'humain.* » Le 25 janvier, 25 entreprises se sont installées à l'IDMC à Nancy pour rencontrer les étudiants à la recherche d'un stage ou de renseignements sur les débouchés à l'issue de leur formation. Étudiants et alumni témoignent de l'importance de ce forum.

Manon Louis,
étudiante en L3 MIASHS parcours Sciences Cognitives

« J'avais déjà trouvé mon stage de L3 au FAN. J'y suis retournée cette année juste pour aller à la rencontre des entreprises, me tenir informée sur les débouchés. Ma formation offre de nombreuses perspectives pour plus tard et je ne souhaite pas me limiter au développement informatique. J'ai bien aimé le fait que les entreprises se déplacent à l'institut pour recruter. »

Armand Fleurot,
étudiant en L2 MIASHS, parcours MIAGE

« C'était ma première visite au FAN. J'y suis allé en tant que membre du bureau des étudiants, puisque j'ai participé à l'organisation. C'est intéressant d'y aller dès la L2, car cela permet de se faire une idée du milieu professionnel. De grands groupes étaient présents mais il y avait aussi des start-up, qui montrent d'autres aspects du métier. Les études, cela reste un peu abstrait et je trouve que le FAN donne un sens à ce que l'on apprend. Et j'ai quelques bons contacts pour la suite ! »

Grégoire Plaut,
UX designer chez Anam'Note

« *Je suis un ancien de l'IDMC, j'avais participé au FAN lorsque j'étais étudiant. Aujourd'hui, je reviens en tant qu'employeur. Chez Anam'Note, nous ne rencontrons pas de difficultés de recrutement car nous sommes une petite équipe de 11 personnes et lorsque nous recrutons, c'est plus une question de profil que de fiche de poste. Anam'Note est une start-up qui édite des logiciels de santé. En venant au FAN, nous apportons un complément à ce que proposent les grands groupes comme les Big 4 en montrant aux étudiants qu'il est aussi possible de rejoindre une petite entreprise. Il y a beaucoup d'anciens de l'IDMC au FAN, passés du côté employeur. De nombreux étudiants viennent nous rencontrer aussi pour cette raison.* »

Alexandre Gingembre,
chef de projet informatique chez Euro-Information

Le FAN permet de présenter aux étudiants nos savoir-faire et nos offres de stage. Ancien de l'IDMC, c'est d'ailleurs au FAN que j'ai rencontré Euro-Information chez qui j'ai fait deux stages avant d'être embauché en CDI. J'ai fini mes études en 2017 et je retourne chaque année au FAN. L'avantage pour les étudiants est de passer la barrière des premiers entretiens en réalisant que leur formation leur offre beaucoup de débouchés. J'ai déjà recruté plusieurs étudiants en stage, dont certains de l'IDMC et cette année encore, nous sommes repartis avec de nombreux CV. L'IDMC propose des formations très intéressantes qui débouchent sur des postes d'ingénieurs… Et c'est l'Université, donc c'est gratuit ! »

Nos partenaires :

Adista
AINOS
Akabi
ALIAE
Anam'Note
Atos
BIL
Caisse d'Epargne Grand Est
CGI Luxembourg (Umanis Nancy)
CHRU
Capgemini
Deloitte
Equasens (LA COOPERATIVE WELCOOP)
Ernst&Young business
Euro-Information
Fanuc Europe
GRDF
Inetum
KPMG
MIST Studio
PwC
SARPI/CEDILOR
TALAN
Talent Business Solution
Versusmind

Zoom sur…

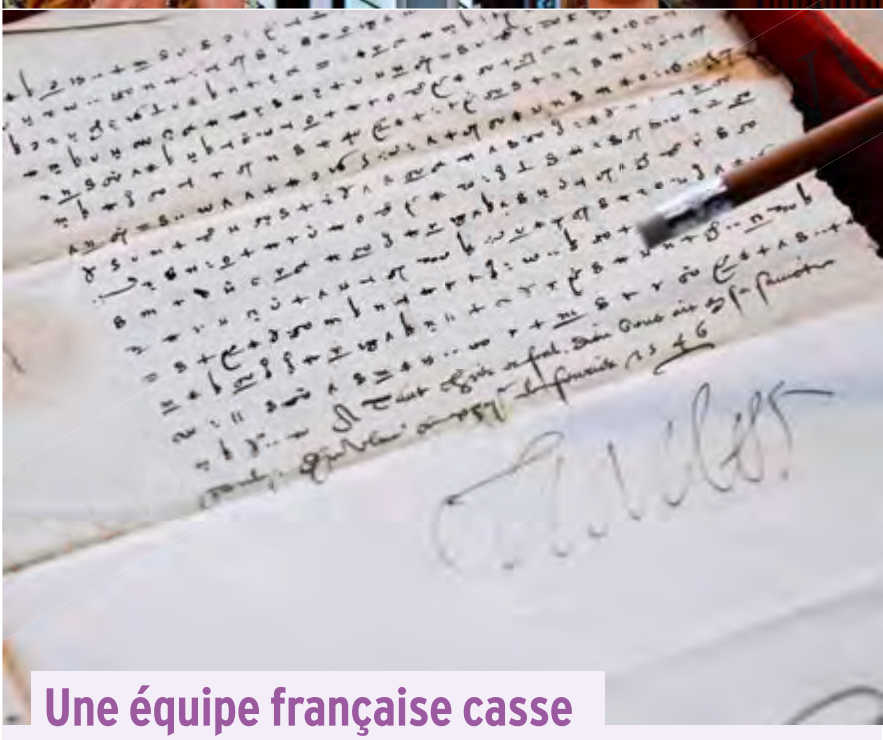
LES PARCOURS

• **Master Sciences Cognitives**
Les sciences cognitives regroupent un ensemble de disciplines scientifiques dédiées à l'étude, la compréhension et la modélisation, notamment via l'outil informatique, des mécanismes de tout système cognitif humain, animal ou artificiel.

• **Master MIAGE**
Proposée dans une vingtaine de villes de France, le Master MIAGE a pour objectif de former des professionnels capables de traiter les enjeux de gestion et de management des organisations avec l'informatique.

• **Master TAL**
L'objectif théorique du TAL (Traitement automatique des langues) est de produire un modèle informatique qui simule notre capacité à parler et à comprendre les « langues naturelles » comme l'anglais ou le français.

• **Licence MIASHS**
Unique dans le Grand-Est, la licence MIASHS, Mathématiques et Informatique Appliquées aux Sciences Humaines et Sociales, est une formation scientifique réellement pluridisciplinaire idéale pour les étudiants souhaitant rester ouverts à l'étude de disciplines du domaine des sciences humaines et sociales.



Une équipe française casse le code de Charles Quint

Il leur a fallu six mois de travail avant d'annoncer la victoire le 24 novembre : les cryptographes Cécile Pierrot, Pierrick Gaudry et Paul Zimmermann (laboratoire Loria – CNRS/Inria/Université de Lorraine) et l'historienne Camille Desenclos (Université de Picardie) sont parvenus à décrypter un courrier (*ci-dessus*) envoyé le 22 février 1547 par Charles Quint à Jean de Saint-Mauris, son ambassadeur en France, et redécouvert en 2021 à la bibliothèque Stanislas de Nancy. Cette remarquable prouesse confirme la dégradation du climat diplomatique à la suite de la mort d'Henri VIII d'Angleterre, le 28 janvier. Charles veut convaincre de ses intentions pacifiques François Ier, qui mobilise et appuie la ligue de Smalkalde, coalition de princes luthériens d'Allemagne du Nord en guerre contre le Saint-Empire. Le Habsbourg s'inquiète en outre d'un projet d'assassinat mijoté par Pierre Strozzi, un des capitaines du roi de France – fausse rumeur, mais qui traduit bien, expliquent les chercheurs, la fébrilité du souverain.

Aujourd'hui en France
Vendredi 10 février 2023 • N° 7751

En bref

CYBERSÉCURITÉ

Gagner la guerre Une centaine d'étudiants de l'université de Lorraine participent jusqu'à ce vendredi à un exercice inédit de cyberguerre organisé avec l'armée, pour développer leurs compétences et susciter des vocations. Systèmes de sécurité, vidéosurveillance, réseaux sociaux : tout est reproduit pour un maximum de crédibilité.

VIDEO. Cybersécurité : ces étudiants se préparent à la cyberguerre

durée de la vidéo : 00h01mn50s

Jamais un tel exercice de cyberguerre n'avait été organisé en France. Pendant plusieurs jours, une centaine d'étudiants de Nancy se sont affrontés au cours d'une simulation ultraréaliste, organisée avec l'armée. Le but, se préparer à des cyberattaques et susciter des vocations. • ©France Télévisions

Écrit par Inès Pons-Teixeira et Gregory Boileau

Publié le 10/02/2023 à 17h00

Mis à jour le 10/02/2023 à 17h24

Jamais un tel exercice de cyberguerre n'avait été organisé en France. Pendant plusieurs jours, une centaine d'étudiants de Nancy se sont affrontés au cours d'une simulation ultraréaliste, organisée avec l'armée. Le but, se préparer à des cyberattaques et susciter des vocations.

Cette guerre se joue depuis le 6 février 2023, jour et nuit. À Nancy (Meurthe-et-Moselle), une centaine d'étudiants est au régime sec depuis lundi. Lits de camps, rations militaires et ordinateurs en réseau, le réalisme est bluffant. Les yeux rivés sur leurs écrans, ils font face à une terrible menace.

Plusieurs de ces étudiants nancéiens se tourneront, plus tard, vers le domaine de la cybersécurité. • © Stéphane Matuchet, France Télévisions

> **« On n'est plus sur un simple travail scolaire mais sur des conditions de guerre »**
>
> **Arthur Terrien, étudiant en 5ème année à Polytech Nancy**

Pour cet exercice de cyberguerre grandeur nature, unique en France, les futurs ingénieurs de l'Université de Lorraine doivent mettre en place et déjouer des attaques informatiques, défendre leur pays et les principales infrastructures.

"On travaille vraiment sur un exercice réel, en plus, le fait que ce soit pendant

plusieurs jours et quasiment à temps plein, en ayant très peu dormi cette nuit, ça permet vraiment de rentrer dans le projet. On n'est plus sur un simple travail scolaire mais sur des conditions de guerre", explique Arthur Terrien, étudiant en 5ème année à Polytech Nancy.

> **"Il faut protéger ses infrastructures informatiques et également essayer d'attaquer celles de l'adversaire"**
>
> Capitaine Jonathan, réserviste de l'armée

L'exercice de cyberguerre regroupe une centaine d'étudiants de six établissements nancéiens, encadrés par de véritables réservistes de l'armée. Dans ce scénario fictif, le "Cryptanga" et les "Anumérics", deux pays imaginaires, s'affrontent pour obtenir l'exploitation d'une île, les "Riverchelles", riche en ressources naturelles comme le lithium. Les jeunes doivent mettre en place et déjouer des cyberattaques, protéger leurs équipements et gérer cette crise.

"Il faut protéger ses infrastructures informatiques et également essayer d'attaquer celles de l'adversaire. On a par exemple des médias et des journaux en ligne qui ont été attaqués, leur contenu a été modifié avec de la propagande adverse. On parle aussi de lutte d'influence sur les réseaux sociaux par exemple", dévoile le Capitaine Jonathan, un réserviste de l'armée qui co-anime l'exercice.

> **Il ne se passe malheureusement pas une journée sans qu'une entreprise ou même des hôpitaux se fassent cyberattaquer**
>
> **Marion Jilson, directrice adjointe de Polytech Nancy et enseignante chercheuse**

Pour les enseignants, il est essentiel de préparer les générations futures à ces nouveaux enjeux. *"Il ne se passe malheureusement pas une journée sans qu'une entreprise ou même des hôpitaux se fassent cyberattaquer, donc je pense qu'il est de notre devoir de les former à ces enjeux là"*, souligne Marion Jilson, directrice adjointe de Polytech Nancy et enseignante chercheuse.

Plusieurs des étudiants présents se tourneront, plus tard, vers le domaine de la cybersécurité. L'occasion rêvée, donc, de mettre en pratique leurs connaissances et leurs acquis. *"Ça nous fait vraiment une vraie préparation à la gestion de crise, comme dans une entreprise ou comme dans un état"*, acquiesce Léo Bertrand, étudiant à l'École des Mines de Nancy.

Au total, cet exercice de cyberattaque, unique en France, a nécessité un an de préparation et la mobilisation de plus d'une cinquantaine de personnes.

"NOUS SOMMES ATTAQUÉS": L'UNIVERSITÉ DE LORRAINE S'EXERCE À LA CYBERGUERRE

PS avec AFP

Une centaine d'étudiants de l'Université de Lorraine ont participé cette semaine à un exercice de cyberguerre organisé avec l'armée. Le but: développer leurs compétences et susciter des vocations en cybersécurité.

Lits de camps, rations de combat et ordinateurs en réseau. Cette semaine, une centaine d'étudiants de l'Université de Lorraine ont participé durant cinq jours à un exercice de cyberguerre de grande ampleur organisé avec l'armée, pour développer leurs compétences et susciter des vocations en cybersécurité.

> **"Axel, on a un problème, ils ont accès à notre site", lance l'un des participants.**

En un instant, la tension monte d'un cran dans la salle de commandement de l'équipe "Cryptanga". Opposé aux "Anumérics", ces deux pays imaginaires se livrent une bataille numérique afin d'obtenir le permis d'exploitation de mines de lithium situées sur l'île des

"Riverchelles".

Deux puissances se disputent l'accès à des ressources rares

Le scénario, entre deux puissances se disputant l'accès à des ressources rares, n'a pas été pensé au hasard.

> **"On a essayé de coller au maximum à la réalité, même si c'est fictif, pour que ce soit le plus immersif possible pour les étudiants", décrit le capitaine Jean-Philippe*, co-animateur de l'exercice et réserviste opérationnel au Commandement de la cyberdéfense (Comcyber), la branche de l'armée chargée de la cybersécurité.**

L'exercice se déroule en ligne grâce à deux cyber-ranges, imposants serveurs permettant de recréer un réseau virtuel semblable à internet, mais sans interaction avec celui-ci.

Des réseaux sociaux ou des médias en ligne ont également été reproduits, de même que des systèmes physiques de sécurité connectés (vidéosurveillance, cartes d'accès) de manière à permettre à cette cyberguerre de se déployer dans toutes ses dimensions.

"Il y a plus de 200 équipements dans l'ensemble de l'exercice", complète le capitaine Pierre, réserviste cyberdéfense et maître du jeu. "On a des routeurs, des serveurs, des équipements de télécommunications, des automates, des robots, tout un éventail d'artefacts numériques qu'on rencontre dans les métiers de la cybersécurité, et qui sont à analyser, à défendre ou à attaquer".

Cellule de crise

Pour l'emporter, chaque équipe doit défendre sa crédibilité en ligne en gardant le contrôle de ses infrastructures numériques, tout en déstabilisant celles de l'adversaire.

> **"Là, nos opposants ont réussi à entrer sur le site de notre média et à publier du contenu. On vient de s'en rendre compte, on va mettre en place une cellule de crise pour voir comment on peut le récupérer", s'inquiète Florent Thirion, 25 ans, étudiant en master 2 Veille stratégique et organisation des connaissances à l'université de Lorraine.**

Derrière lui, d'autres étudiants, formés à la Lutte informatique d'influence (L2I) administrent plusieurs comptes sur des réseaux sociaux pour tenter de gagner la guerre d'information.

"Notre stratégie change chaque jour, en fonction des évènements", raconte Carla del Popolo, 22 ans, l'une des rares étudiantes à participer à la simulation. "Par exemple cette nuit, tous nos mots de passe ont été craqués par l'autre équipe. Derrière, on crée plein de profiles fakes, on doit répondre, faire du bruit, noyer les publications en notre défaveur".

Boissons énergisantes

Pour corser le tout, l'exercice se déroule sur trois sites différents, compliquant la communication interne à chaque équipe, et pendant trois jours, dont une nuit sur place, car "quand un conflit s'ouvre, ce n'est pas pour s'arrêter à 18h30", souligne un réserviste.

"Ca commence à fatiguer, on sent que ça s'essouffle un peu depuis midi, admet Arthur Terrien, 22 ans, en 5ème année à Polytech Nancy, tandis que ses camarades descendent des canettes de boissons énergisantes. On n'a pas faibli cette nuit, on avait un planning de roulement, mais ça tire pour ceux qui n'ont pas beaucoup dormi".

L'exercice réunit six entités de l'université (dont les Mines Nancy, Télécom Nancy, la Faculté des sciences et techniques ou l'IUT Brabois) et intéresse les industriels -une quinzaine sont partenaires de l'exercice. Mais c'est pour le ministère des Armées, co-organisateur, qu'il revêt le plus d'enjeux.

> **"Pour le Commandement de cyberdéfense, c'est une opportunité de détecter des talents, des compétences rares et de créer des vocations", assure le colonel Eric Koessler, commandant de la base de défense de Nancy.**

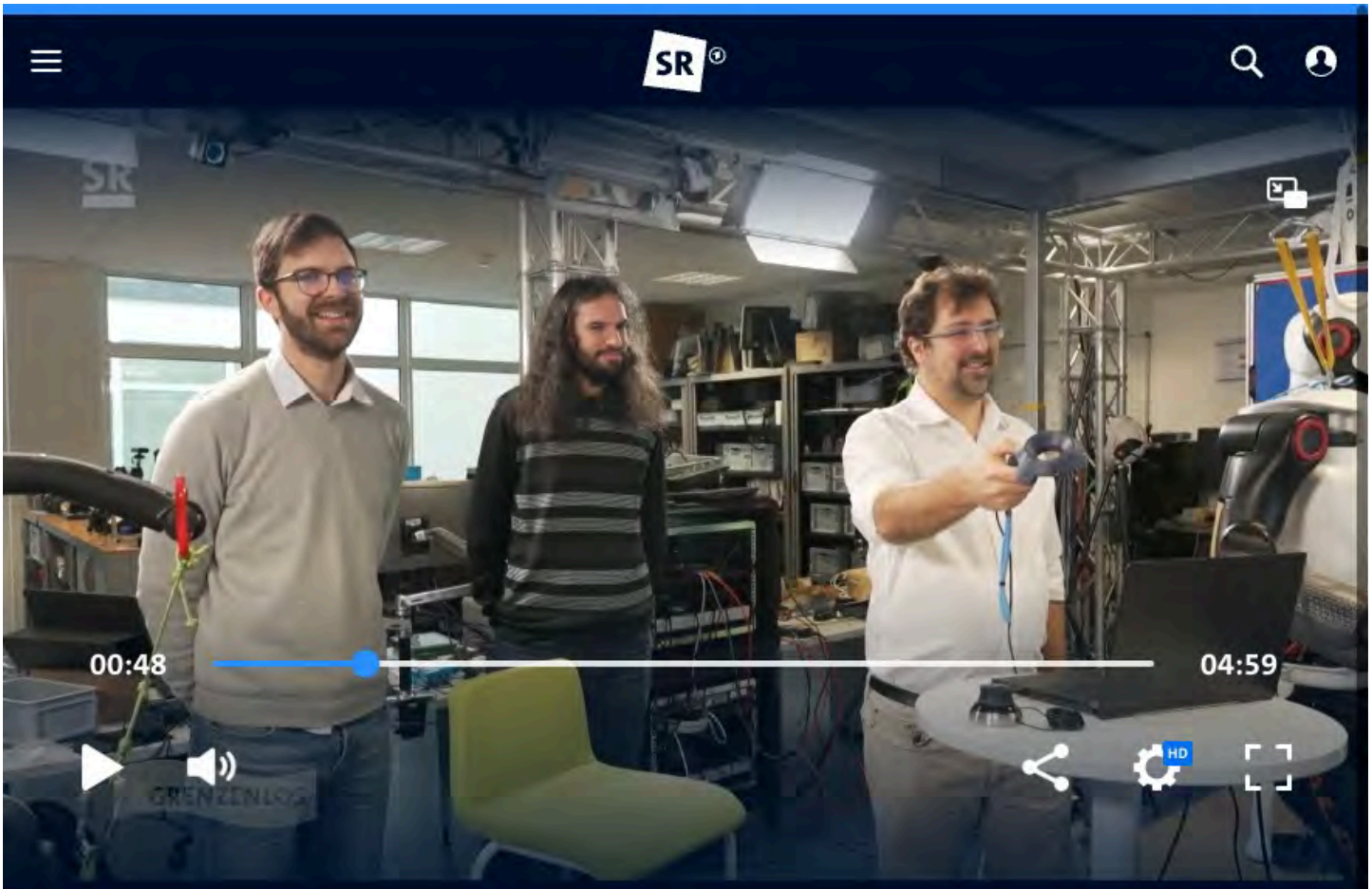
"Ca fait des années qu'on est conscient des menaces potentielles, mais on est tous témoins du fait qu'il y a une accélération du tempo dans ce domaine là", poursuit-il.

SUR LE MÊME SUJET

La guerre électronique fait rage, mais la Russie a raté un "cyber Pearl Harbor" contre l'Ukraine

Le ministère compte ainsi faire passer ses effectifs de cybercombattants de 3700 actuellement à 5200 en 2025. Un Forum de l'emploi a d'ailleurs été organisé pour clore l'exercice de cyberguerre.

PS avec AFP



Hochmodern: Roboter-Training in Nancy

27.02.2023 · Wir im Saarland - Grenzenlos · SR AB 0

+ Merken

Das Creativ'Lab in Nancy ist eine regelrechte Roboter-Schule: Seit 2019 werden hier Roboter so programmiert, dass sie eines Tages Menschen in kritischen Situationen ersetzen können. In dem Labor arbeiten Studierende, Forschende und Unternehmen außerdem mit 3D-Druckern oder Drohnen. Jean-Baptiste Mouret und Adrien Guenard vom Creativ'Lab nehmen uns mit auf eine technologische und manchmal futuristisch anmutende Entdeckungstour.

Bild: Saarländischer Rundfunk

Sender

Video verfügbar: bis 21.08.2025 · 19:19 Uhr

Vosges matin, 17 mars 2023 (édition Saint-Dié)

SAINT-DIÉ-DES-VOSGES

L'impact du numérique fait débat à l'IUT

À l'occasion de ses trente ans, l'institut universitaire de technologie (IUT) organise plusieurs conférences.

Dans le cadre de ses trente ans, l'IUT de Saint-Dié-des-Vosges organise plusieurs manifestations. Ainsi, ce jeudi, une conférence et une table ronde ayant pour thème la sobriété numérique ont eu lieu dans l'amphithéâtre de l'établissement en présence de Christophe Clouzeau, expert en écoconception numérique, Pierre-Frédéric Villard, chercheur au laboratoire, Loria et Joffrey Mougel, designer.

Pendant toute l'après-midi, les étudiants et les intervenants ont pu échanger sur l'impact du numérique et l'écoconception.

ÉCONOMIE - SOCIAL

Qu'est-ce que la 5G industrielle, déployée à l'école des Mines de Nancy ?

Écouter (02 min)

Diffusion du 27 mars 2023

À retrouver dans l'émission

L'ÉCO D'ICI DE FRANCE BLEU LORRAINE NORD

Du lundi au vendredi à 7h15 et 18h08

De France Bleu Lorraine Nord

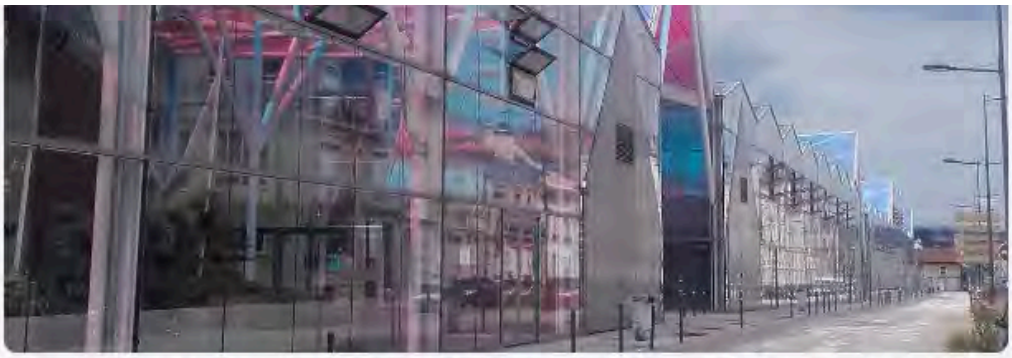
France Bleu Lorraine Nord

Nancy

Lundi 27 mars 2023 à 7:15 - Mis à jour le vendredi 31 mars 2023 à 15:20

Par France Bleu Lorraine Nord

L'école des Mines de Nancy va déployer la 5G industrielle sur son site. Une technologie qui permettra aux futurs ingénieurs d'approfondir leur travail sur "l'internet des objets".



L'école des Mines de Nancy va déployer la 5G industrielle dans les prochains jours. © Radio France - Laurent Watrin

C'est une première en France. Dans la Nouvelle éco, lundi 27 mars, coup de projecteur sur l'école des Mines de Nancy qui investit pour s'équiper de la 5G industrielle. Un outil de développement indispensable pour les élèves ingénieurs à l'ère de l'intelligence artificielle et des objets connectés. François Rousseau, directeur général de l'école des Mines de Nancy, est l'invité de France Bleu Lorraine ce lundi.

Une Semaine à...

Nancy / NUMÉRIQUE

Cyberattaques : la Région déploie son

La Région, épaulée par de nombreux partenaires, vient de créer **« GRAND EST CYBERSÉCURITÉ »**, un **SERVICE D'ASSISTANCE GRATUIT** installé à Nancy et destiné aux PME, ETI, collectivités et associations du Grand Est **VICTIMES DE CYBERATTAQUES**.


Depuis quelques années, les cyberattaques se multiplient. Entreprises, collectivités, organismes publics et particuliers, personne n'est épargné.
© DR

« **504** *portail expiré* » ou encore « *site actuellement en maintenance* » : voilà ce que l'on pouvait lire, lundi 27 mars, sur la page Internet de l'Assemblée nationale dont les services ont confirmé, en milieu d'après-midi, qu'ils faisaient « *face à un excès de requêtes qui [paralysait] le site* ». Dans le même temps, le groupe de hackers pro-russes NoName057(16) a revendiqué sur Telegram cette cyberattaque, présentée comme une riposte au soutien de la France à l'Ukraine, a repéré le spécialiste Numerama. Une enquête a été ouverte auprès du parquet de Paris pour « *entrave au fonctionnement d'un système de traitement automatisé de données* ».

L'exemple illustre bien le besoin de se prémunir de dispositifs mais aussi de faire preuve de pédagogie et d'accompagnement pour les victimes. « *Pour une simple et bonne raison,* **le numérique est omniprésent, les connexions sont nombreuses, donc nous sommes tous concernés** », explique **Jean-Yves Marion**, directeur du Laboratoire lorrain de recherche en informatique et ses applications (Loria-CNRS, Inria, Université de Lorraine) à Villers-lès-Nancy. Ses équipes s'activent pour mieux comprendre les rouages et stratagèmes des hackers, « **qui ne sont plus des adolescents boutonneux installés dans des garages** *mais bien des entités parfaitement organisées et en capacité de nuire. Avec un budget, des équipes et des moyens de communication. Tout cela lié à des groupuscules ou des États bien évidemment* », poursuit le scientifique. Être en capacité de répondre aux nouvelles attaques et en découvrir les vecteurs, anticiper le plus possible comme développer de nouveaux algorithmes de chiffrement, voilà les défis de la recherche pour ces prochaines années. Une fierté pour **Hélène Boulanger**, présidente de l'Université de Lorraine, et **Edwige Helmer-Laurent**, déléguée régionale de la délégation Centre-Est du CNRS.

Et il faut aller très vite car la menace a explosé ces trois dernières années. Des données confirmées par **Emmanuel Naëgelen**, directeur général adjoint de l'Agence nationale de la sécurite des systèmes d'information (Anssi). « *La menace est massive et n'épargne personne : des entreprises de taille intermédiaire (40 % des rançongiciels traités ou rapportés à l'Anssi en 2022) aux particuliers, grands groupes en passant par les hôpitaux (10 %) ou les collectivités (23 %). Avec des conséquences importantes : des entreprises à l'arrêt, des prestations sociales qui ne sont plus versées ou encore des données personnelles utilisées* », précise-t-il.

Un guichet unique pour les victimes

Via France Relance, l'État a souhaité dès 2021 répondre aux menaces de manière pragmatique via des espaces régionaux de cybersécurité. Un appel entendu très tôt par la majorité régionale conduite à l'époque par Jean Rottner qui s'était impliquée dans la démarche. « *Parmi les premières propositions du Business Act figurait la cybersécurité. Et nous sommes tous touchés de près ou de loin.* **Une attaque de cyberterrorisme se produit toutes les quinze secondes dans le monde !** *Du mail frauduleux à la menace en passant évidemment par le vol de données. Chez moi à Épernay, une entreprise a perdu 15 millions d'euros à la suite d'une cyberattaque. Elle avait les reins solides pour affronter cette vague mais tout de même ! Avec les conséquences que cela implique, il est normal que cette question soit prise en compte dans les problématiques régionales* », explique **Franck Leroy**, le nouveau président de la Région Grand Est, en présence d'Irène Weiss, conseillère régionale déléguée à la cybersécurité.

En Grand Est, les TPE et PME ont plus particulièrement besoin d'être accompagnées, à l'instar des collectivités territoriales de petite et moyenne taille. Pour apporter des solutions face à cette menace, un collectif de partenaires (État, Région, Anssi, Gendarmerie, Loria, Inria, CNRS, Université de Lorraine) s'est formé autour d'objectifs communs : coordonner, identifier les offreurs de solutions et proposer une seule porte d'entrée en Grand Est avec une véritable organisation afin de prévenir, sensibiliser, équiper et ainsi être le plus efficace possible dans la gestion de crise. Une de ses traductions : la création de « Grand Est Cybersécurité », le centre d'assis-

▶ L'ACTEUR

Soteria Lab : des experts de la sécurité informatique

C'est une **PÉPITE NANCÉIENNE** passée de deux salariés à près de dix en quelques mois. Spécialisée dans la sécurisation des systèmes d'information, l'entreprise a **DOUBLÉ SON CHIFFRE D'AFFAIRES** en un an. Preuve d'une demande croissante. **CLÉMENT JOLIOT**, à la tête de Soteria Lab, explique.

▶ Il sensibilise à tout-va. Il y a quelques jours, lors de la matinale d'Aprofin, l'association des professionnels de la finance et du chiffre de Lorraine, devant un public de banquiers, assureurs, experts-comptables, notaires, avocats mais aussi étudiants, Clément Joliot a délivré des messages d'anticipation et de « *premiers secours* » face aux risques numériques. Son entreprise accompagne tout type d'organisation pour la sécurisation des systèmes d'information. « *Cela se traduit par une action de notre part en quatre points. Le premier s'illustre par la gouvernance :* **quelle politique de sécurisation est mise en place dans la structure ?** *Le deuxième revient à effectuer un audit de sécurité. Nous allons ainsi inspecter minutieusement l'organisation, ses process comme ses technologies afin d'observer les systèmes et les failles potentielles. Nous activons aussi la technique avec la réalisation de tests d'intrusion. Nous pénétrons ainsi les systèmes, non pas pour semer totalement le bazar et faire perdre des données à l'organisation mais bien pour confirmer que les vulnérabilités existent et que des risques importants en découlent par la suite* », explique le chef d'entreprise.

La troisième opération de Soteria Lab est de passer dans une phase curative : trouver les réponses aux incidents en aidant à la fois à la gestion de crise et à la reconstruction. « *Il faut immédiatement s'interroger en se demandant où, par où et surtout comment corriger ces incidents et ces failles béantes dans le système, puis dans un second temps, celui de la reconstruction, prioriser les systèmes. C'est ce que l'on appelle dans le jargon, un "sanity check"* », détaille Clément Joliot.


Le président de Soteria Lab connaît une activité en forte croissance.
© DR

Enfin, dernier pilier de l'action de l'entreprise : la formation. À destination des dirigeants comme des collaborateurs qui vont bien souvent avoir les mains dans les process et sont donc susceptibles de détecter en premier les intrusions. « **L'utilisateur reste un élément central et essentiel dans la sécurité des processus.** *La formation au hacking permet d'expliquer de quelle manière les attaques sont organisées et orchestrées* », confie le passionné de sécurité informatique.

« Ce guichet unique répond à un besoin croissant »

Depuis sa création en 2016, Soteria Lab est en pleine croissance. Avec toujours plus de cyberattaques chaque année, et même un potentiel record en ce mois de mars 2023 selon le site spécialisé Zataz, la prise de conscience de la part des acteurs économiques, collectivités et autres structures se veut de plus en plus large. « **N'oublions pas que les cyberattaques sont une réelle industrie et sont devenues la première économie parallèle au monde.** *Avec des chiffres d'affaires qui s'élèvent à plusieurs milliers de milliards de dollars par an. C'est assez incroyable ! Les conséquences pour les entités touchées sont tout autant gigantesques voire catastrophiques. Il est donc de plus en plus important de se prémunir face à ces risques* », prône Clément Joliot.

Son entreprise fait partie intégrante de Grand Est Cybersécurité. Une évidence d'être aux côtés de ce dispositif d'accompagnement avec des partenariats protéiformes. « *Quand les entreprises ou organismes publics sont touchés, ils sont paniqués et ne savent pas du tout vers qui se tourner. Là, avec ce guichet unique qui répond à un besoin croissant, nous saurons agir de manière coordonnée avec davantage d'efficacité et d'efficience. C'est une très bonne chose et Soteria Lab est très fière de pouvoir y contribuer* », conclut Clément Joliot.

BZ

plan de défense

La conseillère régionale déléguée, Irène Weiss, et le président de la Région Grand Est, Franck Leroy, ont présenté les contours de « Grand Est Cybersécurité ».

© Région Grand Est

tance aux victimes d'attaques informatiques. Cette plateforme permet désormais aux PME, ETI, collectivités et associations du Grand Est, victimes de cyberattaques, de bénéficier d'un service d'assistance gratuit. **Opérationnel depuis le 14 février dernier**, il est localisé à Nancy et opéré par Grand E-Nov +, l'agence d'innovation et de prospection internationale de la Région Grand Est. Ce service d'assistance comprend une prise en charge personnalisée et immédiate avec préqualification de l'incident et une assistance de premier niveau ; une mise en relation avec des prestataires qualifiés pour répondre à l'incident ; un suivi de l'incident jusqu'au rétablissement de la situation ; un accompagnement à la judiciarisation ; un suivi des statistiques d'incidentologie à l'échelle régionale. Pour accompagner les victimes, des entreprises partenaires spécialistes du domaine. « *Il est aujourd'hui essentiel d'apporter des gestes de premier secours car* **il y a des choses à faire immédiatement quand on est victime d'une cyberattaque. Déjà, il ne faut pas avoir honte d'en parler.** *Même quand on est chef d'entreprise et que l'on craint les répercussions. Ensuite, les procédures techniques s'enchaînent* », explique Emmanuel Naëgelen, directeur général adjoint de l'Anssi.

Un plan régional et un campus dédié

Convaincu qu'il est nécessaire de **procéder à de « l'hygiène numérique »** pour reprendre les mots d'Irène Weiss, **la Région Grand Est veut mettre le paquet dans la prévention, l'anticipation et la formation**. Elle a donc pour objectif de lancer, au second semestre 2023, un « Campus Cyber Grand Est » ouvert à tous les acteurs de la cybersécurité du territoire et travaillant en réseau pour rapprocher la cybersécurité des utilisateurs. Destiné à devenir à terme la référence sur le sujet, ce Campus coordonnera et mutualisera les efforts et ressources de la communauté régionale. « *Ce sera un lieu totem qui regroupera tout l'écosystème. En matière de sensibilisation, de développement des compétences, de partages de données, d'innovations et de coopérations transfrontalières* », complète **Irène Weiss**.

Par ailleurs, approuvé par les élus de la Région Grand Est le 23 mars dernier, le plan régional cybersécurité 2023-2025 s'articule autour de la prévention et la préparation des acteurs aux cybermenaces en accroissant leur niveau de résilience en cybersécurité. « *Cela passe notamment par le "diagnostic cybersécurité" déjà mis en place par la Région pour les entreprises. Depuis son lancement en novembre 2022, plus de 50 entreprises régionales ont déposé une demande d'aide pour mettre en œuvre ce diagnostic. Son élargissement à l'ensemble des collectivités et associations régionales permettra de* **faire de la gestion du risque cyber un réflexe dans le Grand Est** », explique Franck Leroy. L'accompagnement de la gestion de la crise cyber, avec l'appui de Grand Est Cybersécurité, l'animation et le développement d'une filière régionale de la cybersécurité avec des partenariats protéiformes comme le développement des compétences pour répondre aux besoins croissants des entreprises et de la filière assurent le positionnement du Grand Est sur un marché mondial de la cybersécurité en forte croissance.

Baptiste Zamaron

Pour joindre Grand Est Cybersécurité, un numéro de téléphone (0 970 51 25 25) et un site Internet (cybersecurite.grandest.fr).

La Semaine de Nancy, 30 mars 2023 -

INNOVATION

HY2CAR, LE VÉHICULE DE DEMAIN EN PHASE DE TEST

▶ Six laboratoires de l'Université de Lorraine (LRGP, Green, Loria, Cran, PErSEUs, Beta), associés au laboratoire Irimas de l'Université de Haute-Alsace, mènent des recherches pour développer un prototype de véhicule léger, de coût accessible, peu gourmand en énergie, plus propre et de puissance adaptée au transport urbain ou périurbain. Ce projet pluridisciplinaire d'un montant total de 420 000 euros – financé par le Feder, le fonds de dotation AIR et Lorraine Université d'Excellence – est baptisé Hy2Car. Au-delà de la mise au point d'une source d'énergie atypique impliquant une pile à combustible à des supercondensateurs, le projet prend en compte l'étude du futur utilisateur et la viabilité économique de cette filière hydrogène. À cet effet, une nouvelle plateforme HyMob, située dans le bâtiment de cryogénie de la faculté des Sciences et Technologies, vient d'être lancée. Elle permettra de tester le projet à taille réelle avec des infrastructures adaptées.

L'Est républicain, 31 mars 2023 (édition Nancy)

NANCY

Nocturnes de l'Histoire : décrypter les messages

Nikita et Jean ont préparé un jeu de piste et plusieurs ateliers pour les Nocturnes de l'Histoire 2023. Photo ER/Thomas BAUDOIN

Dans les couloirs du campus, Margot, Jean et Nikita servent de guides aux visiteurs. C'est la première fois que les jeunes étudiants organisent un événement d'une telle ampleur : « On a été prévenu il y a seulement trois mois du thème de cette année ! C'était serré… »

Pourtant le contrat est rempli et le programme fait parfaitement écho au thème 2023 : (dé) chiffrement et énigmes.

Parmi les conférencières invitées, Cécile Pierrot est chargée de recherche en cryptologie à l'Inria. Son métier est a priori éloigné de l'histoire ou de l'archéologie, sauf que c'est elle (avec une équipe de chercheurs) qui a décrypté la lettre de Charles Quint retrouvée à la bibliothèque Stanislas. Outre son champ de recherche, qui est de son propre aveu « assez simple à expliquer », Cécile Pierrot est venue décrire sa méthode et ses découvertes permises par « une collaboration entre historiens et la cryptographie contemporaine ».

Jérémy Gracio, responsable d'opérations à l'Inrap, est venu animer un atelier sur l'archéologie préventive. L'occasion au passage de démonter les clichés sur les Gaulois.

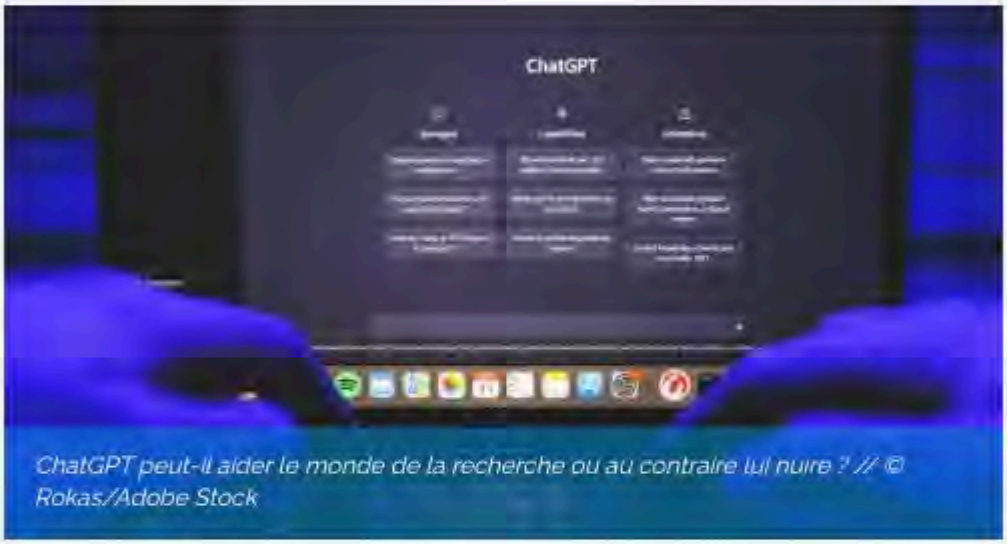
Enfin, le jeu de piste a demandé beaucoup de temps aux jeunes organisateurs : « On a la chance d'avoir un musée universitaire, le MAUL, on voulait le mettre en valeur »

Thomas BAUDOIN

Faut-il bannir ChatGPT du monde de la recherche ?

Charlotte Mauger

Publié le 03.04.2023 à 11H00



ChatGPT peut-il aider le monde de la recherche ou au contraire lui nuire ? // © Rokas/Adobe Stock

ChatGPT : allié ou ennemi des chercheurs ? La réponse n'est pas si manichéenne. Un modèle de langue peut rendre certaines tâches plus simples, tant qu'il est utilisé comme une source d'aide perfectible. Les chercheurs vont-ils un jour utiliser ChatGPT comme appui à la rédaction de leurs travaux et articles de recherche ?

Le 16 décembre 2022, la revue Nurse Education in Practice publie un article sur son site. En apparence rien d'anormal, l'article traite de **l'utilisation de l'intelligence artificielle dans les études en soins infirmiers.** Pourtant aux côtés du nom de la chercheuse britannique Siobhan O'Connor, apparaît celui de ChatGPT. Que fait-il ici ? "L'utilisation de cet outil par un chercheur ou une chercheuse n'est pas différente de celle d'une autre personne : paraphraser, traduire, résumer...", annonce Teven Le Scao, chercheur au Loria et chez Hugging Face, spécialisé en modèle de langue.

"Si on demande à ChatGPT de rédiger un article de recherche, il pourrait le faire de façon convaincante", assure Teven Le Scao. **Une aubaine pour une personne peu honnête** dans un monde aussi compétitif que celui de la recherche. "Il y a une crainte qu'il y ait énormément de papiers générés : pour avoir plus de citations ou simplement pour s'amuser à voir si un tel article

pourrait être publié", convient Rachel Bawden, chercheuse à Inria spécialisée dans le traitement automatique des langues.

L'irruption de ChatGPT bouscule les usages du monde enseignant

L'usage de ChatGPT, contraire aux principes de publication de recherche

Or cela est contraire aux principes derrière une publication. "**Cela pose des problèmes de fiabilité des arguments avancés** et de réplicabilité des résultats", prévient Dominique Boullier, professeur de sociologie à Science po Paris et spécialiste des usages du numérique.

> ***Si on demande à ChatGPT de rédiger un article de recherche, il pourrait le faire de façon convaincante. (T. Le Scao, chercheur)***

Faut-il pour autant le bannir en prévision de telles dérives ? Déjà, cela s'avérerait très difficile. Il faudrait alors être en mesure **d'identifier avec certitude qu'un texte a été produit par un modèle de langue.** Or, les outils actuels ne sont pas toujours en mesure de trouver l'auteur d'un texte - surtout s'il a été par la suite modifié par un humain.

Mais surtout, **ce serait occulter l'aide qu'il peut apporter.** "C'est par exemple un outil intéressant pour les non-anglophones, soutient Rachel Bawden. Pour un anglophone natif, il est souvent très facile de reconnaître que l'article n'a pas été écrit par un anglophone. Or un anglais de mauvaise qualité peut diminuer l'impact du travail de recherche, surtout s'il rend l'article difficile à comprendre."

Les modèles de langues peuvent donc aider des chercheurs dans leur rédaction en langue anglaise. Ces modèles peuvent générer un code informatique, reformuler un passage, trouver un titre ou rédiger un abstract de façon convaincante. Dans une pré-publication déposée sur le site bioRXiv, la chercheuse Catherine Gao de l'université Northwestern et ses collègues ont généré les abstracts de 50 articles de recherche avec ChatGPT et ont demandé à des chercheurs et chercheuses de les retrouver. **Dans 32% des cas, la patte de l'IA n'a pas été reconnue.**

Demain, tous formés dans le métavers ?

Utiliser ChatGPT en connaissance de ses limites

Une pratique honnête tient aussi à l'utiliser en toute connaissance de ses

limites. Même si ce qu'écrit ce chatbot ressemble à un texte "humain", **il y a un risque que des erreurs se glissent dans ses lignes.** Il a tendance à mélanger des citations, à renvoyer des choses fausses, à ne pas citer ses sources et, quand il le fait, à inventer des références ou des auteurs.

> *Il est important de savoir faire les choses mieux que la machine, ainsi on peut l'utiliser et détecter la moindre erreur. (R. Bawden, Inria)*

"Il est important de savoir faire les choses mieux que la machine, ainsi on peut l'utiliser et détecter la moindre erreur", prévient Rachel Bawden. Il ne faut pas se reposer sur l'aspect convaincant, et au contraire privilégier son esprit critique. "Les chercheurs et chercheuses sont formés à ne pas faire de raccourci quand ils doivent trouver une réponse. Or **la génération de texte tend à favoriser les réflexions courtes et rapides pour obtenir cette réponse"**, analyse Dominique Boullier. "Si ces outils s'améliorent dans le futur, cela peut poser des problèmes pour notre capacité à raisonner", ajoute Rachel Bawden.

Une vigilance sur la collecte de données de recherche

Une autre vigilance à garder en tête : celle des données récoltées. "Comme ce qui se passe pour les réseaux sociaux, nous contribuons à entraîner ces modèles", prévient Dominique Boullier. Or, **quand certaines données sont sensibles, il serait bon qu'elles ne soient pas collectées.** Cette petite révolution des chatbots oblige en tout cas les acteurs du monde de la recherche à fournir leurs directives d'utilisation.

L'Association de Linguistique Computationnelle (Association for Computational Linguistics, ACL), qui organise des conférences, déconseille de s'aider d'un modèle de langue pour un nouveau texte sur de nouvelles idées. Également, au mois de janvier la revue Nature s'est positionnée : **l'utilisation de ChatGPT n'est pas prohibée, elle doit être mentionnée** mais pas parmi les auteur(e)s. "Cette recommandation est naturelle : l'auteur doit endosser la responsabilité et pouvoir être contacté. ChatGPT ne répond pas à ces critères", justifie Teven Le Scao.

Pour l'instant, ChatGPT reste marginal dans le monde de la recherche. Comme le souligne Rachel Bawden : "Je ne crois pas avoir rencontré un article écrit avec ce chatbot. Mais si c'était le cas, je regarderais sûrement les références plus en détail. Même si s'aider de ChatGPT ne me pose pas de problème, **je me méfierais certainement un peu plus**."

Charlotte Mauger / *Publié le 03.04.2023 à 14h30*

Les Tablettes lorraines, 3 avril 2023

TPE-PME

Le plan régional Cybersécurité en ordre de marche

LE 28 MARS, LA RÉGION GRAND EST A PRÉSENTÉ AU LABORATOIRE LORRAIN DE RECHERCHE EN INFORMATIQUE ET SES APPLICATIONS (LORIA) À VILLERS-LÈS-NANCY, LES NOUVEAUX OUTILS RÉGIONAUX EN MATIÈRE DE CYBERSÉCURITÉ À DESTINATION DE L'ÉCOSYSTÈME ENTREPRENEURIAL. À CÔTÉ DE L'ACTUEL CENTRE D'ASSISTANCE AUX VICTIMES D'ATTAQUES INFORMATIQUES, UN CAMPUS CYBER GRAND EST DEVRAIT ÊTRE LANCÉ AU SECOND SEMESTRE 2023.

40 % des rançongiciels touchent les TPE et PME, 23 % des collectivités territoriales et 10 % les établissements publics de santé (source Agence nationale de sécurité des systèmes d'information) ! À l'heure où la digitalisation des entreprises s'accélère, la menace cybercriminelle se maintient à un niveau élevé avec un regain d'activité à la fin 2022. La cybersécurité s'affiche aujourd'hui comme une priorité pour l'écosystème entrepreneurial. Histoire de faire face à ce fléau, la Région Grand Est a lancé son plan régional cybersécurité 2023-2025 (approuvé le 23 mars dernier). Il s'articule autour de cinq axes principaux : prévenir les cybermenaces par la sensibilisation des acteurs régionaux, préparer les acteurs aux cybermenaces, accompagner à la gestion de la crise cyber, animer et développer la filière régionale de la cybersécurité et développer les compétences dans le domaine.

© Région Grand Est

Franck Leroy, président de la Région Grand Est a présenté les nouveaux outils régionaux en matière de cybersécurité au Loria à Villers-lès-Nancy

CENTRE D'ASSISTANCE ET CAMPUS

Le 28 mars, au Laboratoire lorrain de recherche en informatique et ses applications (Loria), Franck Leroy, président de la Région Grand Est et Emmanuel Naëgelen, directeur général adjoint de l'Agence nationale de la sécurité des systèmes d'information (ANSII) ont présenté les outils régionaux en matière de cybersécurité issus du travail d'un collectif de partenaires (État, Région, ANSSI, Gendarmerie, Loria, Inria, CNRS, Université de Lorraine). En première ligne, le centre d'assistance aux victimes d'attaques informatiques. Nom de code : Grand Est Cybersécurité. Opérationnel depuis la mi-février, il est localisé à Nancy et piloté par Grand E-Nov +, l'agence d'innovation et de prospection international de la Région Grand Est avec le soutien de l'ANSSI. Joignable par téléphone au 0 970 51 25 25 et via le site https://cybersecurite.grandest.fr/, il permet une prise en charge personnalisée avec une assistance de premier niveau, une mise en relation avec des prestataires qualifiés pour répondre à l'incident, un suivi de l'incident jusqu'au rétablissement de la situation et un accompagnement à la judiciarisation. Autre outil régional annoncé, la création d'un Campus Cyber Grand Est au second semestre 2023. *«Il sera ouvert à tous les acteurs de la cybersécurité du territoire et travaillant en réseau pour apporter la cybersécurité au plus près des utilisateurs»*, explique l'exécutif régional.

:reportage

Cybersécurité : l'armée française organise des exercices dans des écoles d'informatique pour trouver "les profils qui l'intéressent"

Alors que la loi de programmation militaire est dévoilée mardi en Conseil des ministres, la branche de l'armée chargée de la cybersécurité veut créer des vocations. Un exercice grandeur nature a été mené dans une école d'informatique à Paris.

Noémie Bonnin
Radio France

Publié le 04/04/2023 07:10

Temps de lecture : 2 min

L'exercice, organisé par l'armée française, s'est déroulé à l'école supérieure de génie informatique (ESGI) à Paris, en mars 2023. (NOEMIE BONNIN / RADIO FRANCE)

En treillis militaire dans la salle de classe, le lieutenant Thibault donne les dernières consignes. *"Il est 15h45, je vais commencer les attaques. Vous devez vous défendre en temps réel. C'est bon ? C'est*

parti !" L'exercice : une cyberattaque très réaliste. Il a lieu à l'École supérieure de génie informatique (ESGI), à Paris, et dure toute la journée. Il est organisé par la branche de l'armée chargée de la cybersécurité, le "Comcyber" (commandement de la cyberdéfense). L'objectif : recruter des experts.

>> Emploi : les discriminations liées à l'origine sociale commencent dès l'examen du CV

Et pour trouver ces profils, le Comcyber organise des exercices très réalistes directement dans les écoles d'informatique et d'ingénieurs, pour créer des vocations. *"On va les mettre en situation pour qu'ils comprennent qu'on n'est pas là pour rigoler, qu'on n'est pas là pour jouer, mais pour faire quelque chose de concret, sérieux,* explique le lieutenant Thibault. *On les motive rapidement et, en fonction des groupes, on va les mettre plus ou moins sous pression, comme nous, on pourrait avoir à la supporter si on était vraiment sur le terrain."*

Recruter 1 500 cyber-combattants d'ici 2025

Les étudiants, répartis en deux équipes, doivent défendre un système d'information stratégique. *"Pour le coup, on est dans un environnement que l'on ne connaît pas vraiment, donc c'est compliqué de se repérer*, glisse Florian, 23 ans, qui s'est pris au jeu. *C'est un challenge intéressant."* Au point d'en faire son métier ? La question se pose, assure l'étudiant : *"Ça peut être une éventualité."*

> "C'est différent d'un environnement professionnel classique, les enjeux sont un peu plus importants : forcément, ça responsabilise. Et je trouve que c'est vachement intéressant."
>
> **Florian, étudiant à l'ESGI**
>
> à franceinfo

Pour les jeunes, c'est un exercice, mais pour le ministère de la Défense, l'enjeu est de taille : il veut recruter 1 500 cyber-combattants, d'ici 2025. *"La menace est de plus en plus importante, elle se perfectionne,* détaille le sergent Pierre, chargé du recrutement. *On a besoin de plus en plus de monde, c'est pour ça que l'on vient dans les écoles : parce que ce sont des profils d'ingénieurs qui nous intéressent. Ils ont une bonne base et on peut*

leur proposer différents postes au sein de nos institutions, à un niveau d'officier, par exemple."

Ces étudiants ont déjà une très bonne formation, et beaucoup se dirigent vers l'armée après cette sensibilisation, assure Kamel Hennou, directeur de l'école. *"Chaque année, on a entre 30 étudiants qui s'engagent dans cette réserve nationale de cybersécurité".* Pendant cette session de deux semaines, 400 étudiants ont réalisé cet exercice, dans 13 écoles de l'enseignement supérieur d'Île-de-France.

L'armée française organise des exercices de cybersécurité dans des écoles d'informatique - Repotage de Noémie Bonnin

écouter

voir les 12 commentaires

Partager :

GRAND EST

Cybersécurité : la Région sort la grosse artillerie

Plus la digitalisation des entreprises, des collectivités et des hôpitaux avance, plus le risque d'attaque par des pirates informatiques est grand. Pour faire face à la menace, la Région vient de se doter de nouveaux outils. Objectif : assurer sa cybersécurité.

La signature du plan de cybersécurité à Nancy le 28 mars 2023 avec Sylvain Dorschner, directeur général chez Grand E-nov, Franck Leroy, président de la région Grand Est, Blaise Gourtay, représentant Josiane Chevalier, préfète de la région Grand Est, Irène Weiss, conseillère régionale déléguée à la cybersécurité. Photo ER/Magalie DELLE-VEDOVE

Sacrée coïncidence. Alors que le gouvernement annonçait que le site internet de l'Assemblée nationale avait été victime d'une cyberattaque menée par des hackers russes, la région Grand Est dévoilait son plan de cybersécurité. Mardi 28 mars à Nancy, le laboratoire de recherche en informatique et ses applications (Loria) a accueilli des professionnels de la cyberdéfense. Des gendarmes, des policiers, en présence de Blaise Gourtay pour représenter Josiane Chevalier préfète de la grande région, Emmanuel Naëgelen, directeur général adjoint de l'Agence nationale de Sécurité des systèmes d'information (ANSSI) et bien sûr le nouveau patron de l'exécutif régional, Franck Leroy. Des officiels et un collectif de partenaires pour montrer que face à la multiplication des attaques par des pirates informatiques la Région organise sa « cyber-riposte. »

Une menace pour les petites entreprises

La cybersécurité, ce n'est pas de la science-fiction. Emmanuel Naegel, spécialiste de la sécurité des systèmes d'information l'a démontré en rappelant quelques exemples d'incidents récents. En avril dernier, le groupement hospitalier de territoire Grand Est (GHT) a été victime d'une cyberattaque. Les pirates informatiques, on s'en souvient, avaient mis aux enchères les fichiers récupérés dans les hôpitaux de Vitry-le-François et Saint-Dizier. Dans la foulée, Clestra Hausermann, une entreprise alsacienne, a été elle aussi victime d'une cyberattaque de type ransomware (rançongiciel). Pendant 3 mois, l'entreprise n'a plus eu accès à sa comptabilité, à son système de paye et à sa base commerciale. « Pour cette entreprise, a précisé Emmanuel Naëgelen, le coût de l'attaque a été estimé entre 2 et 3 millions d'euros »

Tout le problème est là. Pas question de laisser des pirates ruiner la santé économique régionale. Mais quand une entreprise est prise en otage par des pirates informatiques, elle n'a pas forcément les moyens d'assurer sa défense. « Il est d'autant plus important de pouvoir agir, a précisé le président de la Région Franck Leroy, qu'on sait qu'une entreprise attaquée sur deux ferme dans les six mois. » Grâce à une dotation d'un million d'euros obtenue dans le cadre du plan France Relance, le Grand Est a donc orchestré sa défense numérique avec ses partenaires (l'État, la gendarmerie, le Loria, le CNRS et l'université de Lorraine).

Le centre de cybersécurité régional basé à Nancy

La stratégie de cybersécurité de la Région prévoit des actions de sensibilisation contre les cybermenaces, une proposition de diagnostic de sécurité gratuit pour les entreprises et un accompagnement en cas d'attaque par des professionnels de la cyberdéfense. Et puisqu'en la matière, il faut former des talents aptes à parer l'ingéniosité des pirates, le plan prévoit aussi des formations. « Le besoin est réel, a rappelé Franck Leroy. Depuis le lancement fin 2022 d'une proposition de diagnostic en cybersécurité, 50 entreprises du territoire ont déjà déposé une demande d'aide. » Les entreprises qui ont déjà appelé à l'aide et toutes celles qui vont suivre seront dirigées vers le centre de cybersécurité du Grand Est basé à Nancy. Elles profiteront d'une assistance gratuite. Des hackers éthiques, professionnels de l'informatique qui connaissent bien les pirates et leurs techniques, ont été recrutés pour les épauler. Le service est complet : de l'accompagnement personnalisé jusqu'à la judiciarisation du dossier.

Magalie DELLE-VEDOVE

■ Centre de cybersécurité du Grand Est : 0970 512 525 ou cybersecurite.grandest.fr

LE CHIFFRE

40 %

Le rançongiciel consiste à envoyer à la victime un logiciel malveillant qui chiffre l'ensemble de ses données et à lui demander une rançon en échange de la clé de déchiffrement. 40 % des rançongiciels traités en 2022 touchaient des petites entreprises. Dans 23 % des cas, les victimes étaient des collectivités territoriales et dans 10 % des cas, des établissements de santé.

Du « hacking éthique » pour s'entraîner

Mardi dernier, lors de la présentation du plan de cybersécurité régionale, il n'y avait pas que des VIP. Il suffisait de descendre de deux étages dans le bâtiment du Laboratoire lorrain de recherche en informatique et ses applications (Loria) pour changer d'ambiance. Là, une vingtaine d'étudiants, les yeux rivés sur leurs ordinateurs, font face à un véhicule à quatre roues. Leur mission ? Endosser le rôle des « méchants » et prendre le contrôle du robot à l'aide de leurs ordinateurs. Du « hacking éthique », en somme. Leur adversaire d'un jour a été conçu par Vincent Person, du groupe d'expertise en ingénierie Englab.

C'est une course pour ces étudiants en informatique : quel groupe arrivera à hacker leur cible en premier ? Photo ER/Laura MAX

Étudiants contre robot

Un cyber-entraînement sous la forme d'une bataille acharnée… Les étudiants n'ont que quelques informations à leur disposition pour infiltrer le système du robot et le faire rouler. L'ambiance est à la compétition : quel groupe sera le plus rapide ? « Bon courage pour nous rattraper ! », lancent Thibault et Tristan à leurs camarades. Les deux étudiants, en deuxième année à Telecom, école d'ingénieurs en informatique et en sciences du numérique, sont en avance. Tous les participants, qu'ils soient de Telecom, de Polytechnique ou d'ailleurs, se sont portés volontaires pour participer à ce « cyber-affrontement ».

« Premiers secours » pour les victimes de cyberattaques

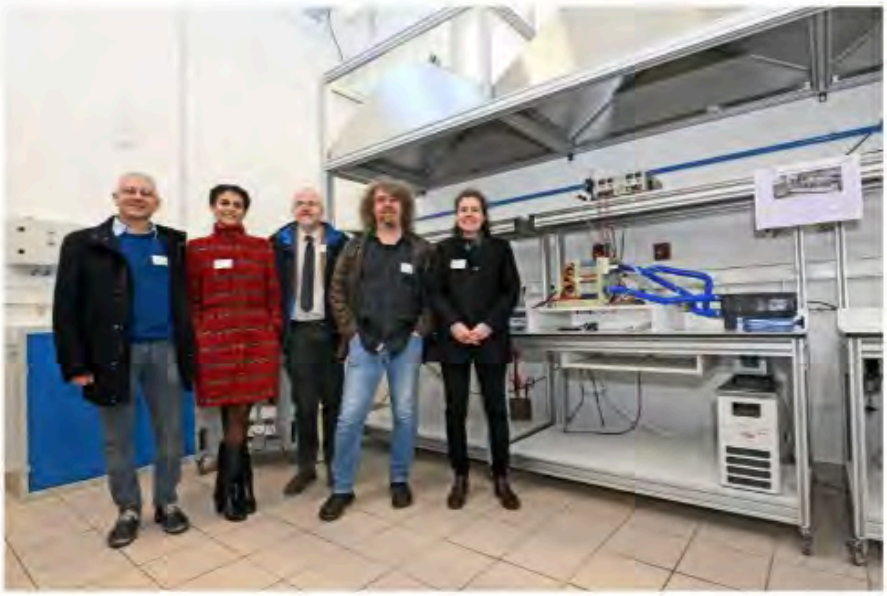
Tels des guides bienveillants, d'autres pros du numérique passent entre les étudiants. Ce sont les membres du CSIRT, le tout nouveau Centre de réponse d'urgence aux incidents de cybersécurité régional basé à Nancy. S'ils s'amusent du petit concours en train de se dérouler, ils seront confrontés à des attaques un peu plus offensives… Leur challenge à eux est désormais de procurer les « premiers secours » aux victimes de cyberattaques, mais aussi de mettre ces dernières en relation avec des prestataires de confiance pour limiter la casse. Dernière étape de leur mission : inviter les victimes à contacter les forces de l'ordre, pour inciter à porter plainte. Plus tôt dans la matinée, la conseillère régionale Irène Weiss avait fait remarquer que « se faire hacker, c'est comme se faire cambrioler ». Une menace qui n'est donc pas prise à la légère, si ce n'est le temps de quelques heures dans la salle remplie de « hackers éthiques », où les cerveaux s'activent face à la difficulté du défi !

Laura MAX

Photos

HyMob : la voiture à hydrogène se conçoit en Lorraine

Photos ER/ Cédric Jacquot - 04 avr. 2023 à 19:59 - Temps de lecture : 1 min



13 / 15

Inauguration de la plateforme HyMob située dans le bâtiment cryogénie de la Faculté des Sciences et Technologues (FST) de Villers-lès-Nancy. HyMob est une nouvelle plateforme pour tester un véhicule électrique familial adapté à des courts trajets. Photo ER/ Cédric Jacquot

Le véhicule du futur (proche) se conçoit à Villers-lès-Nancy

Tout est né en 2014. « Stéphane Raël (NDLR : professeur au GREEN, Groupe de recherche en énergie électrique de Nancy, un laboratoire de l'Université de Lorraine) est venu nous trouver avec un montage atypique avec pile à combustible et supercondensateur », confie Caroline Bonnet, maître de conférences en génie des procédés à l'Université de Lorraine et responsable du projet Hybridized Hydrogen Car (Hy2Car). Projet qui vise la mise au point d'un prototype de véhicule léger à hydrogène pour répondre aux enjeux de la transition énergétique. Après des tests concluants, l'idée a germé : « Pourquoi ne pas intégrer cette architecture électrique dans un véritable véhicule ? »

Restait alors à trouver un local. C'est chose faite : la plateforme HyMob a été inaugurée mardi sur le site de la Faculté des sciences et technologies à Villers-lès-Nancy. « C'est la première plateforme lorraine dédiée à la mobilité hydrogène », explique Caroline Bonnet qui cite les « 25 enseignants-chercheurs, les six laboratoires lorrains », le laboratoire de l'Université de Haute Alsace, mais aussi « l'Université de Lorraine et le CNRS » fédérés autour de Hy2Car. Ce projet de 420.000 € a aussi été labellisé par le Pôle véhicule du futur et primé par ATMO Grand Est.

Caroline Bonnet (au centre), responsable du projet Hy2Car.
Photo ER/Cédric JACQUOT

« Il ne rejette que de l'eau »

« Actuellement, les véhicules sont surdimensionnés », explique Carole Bonnet entourée de Melika Hinaje du GREEN, Stéphane Raël et François Lapicque, du Laboratoire Réactions et Génie des Procédés. Le but est de créer un véhicule électrique « familial destiné à de l'urbain et du périurbain qui fonctionne à l'hydrogène et à l'air. L'intérêt, c'est qu'il ne rejette que de l'eau » et qu'il refasse le plein en quelques minutes. D'ailleurs, la Renault Kangoo, qui sert pour l'expérimentation, est garée juste à côté de la réserve d'hydrogène servant à alimenter le réservoir où le gaz est comprimé.

Bien sûr, tout est pensé comme un projet global pour que le coût de la voiture reste accessible, que le véhicule soit peu gourmand en énergie et plus propre pour l'environnement. Sans oublier la prise en compte du futur utilisateur et la viabilité économique de la filière hydrogène.

Frédéric PLANCARD

Guerre Israël-Hamas | Guerre en Ukraine

Grand Est

Du « hacking éthique » au service de la cybersécurité

Le plan de cybersécurité du Grand Est a aussi été le théâtre d'un événement plus ludique : une vingtaine d'étudiants en informatique devaient hacker le système informatique d'un robot pour en prendre le contrôle.

Laura MAX - 04 avr. 2023 à 05:00 - Temps de lecture : 2 min

C'est une course pour ces étudiants en informatique : quel groupe arrivera à hacker leur cible en premier ? Photo ER /Laura MAX

L’Est républicain, 5 avril 2023 (édition Nancy)

Mines Nancy passe en 5 G

NANCY

L’école des Mines est le premier campus de France équipé d’une 5 G industrielle. Photo ER/Alexandre MARCHI

> PAGES 2 ET 3

Mines Nancy, premier campus éq

L'école des mines de Nancy, Nokia et la SNEF Telecom ont inauguré, ce mercredi, le Te@chLab5G, une plateforme de réseau 5G privée industrielle. Cette infrastructure de pointe, unique en France sur un campus, ouvre de nouveaux horizons dans la formation des futurs ingénieurs.

« Ce nouveau réseau est révolutionnaire. Nous avons fait le choix de la 5G industrielle pour nous positionner comme un acteur clé dans son développement en France et en Europe. » L'enthousiasme était de mise pour François Rousseau, ce mardi, sur le campus Artem. Le directeur de Mines Nancy a inauguré le Te@chLab5 G avec Anne Lauvergeon, présidente du conseil d'administration de l'école, Pierre-Gaël Chantereau, président-directeur général de Nokia France, Christophe Delaye, directeur général de SNEF Telecom (Eiffage Energie Systèmes) et Philippe Herbert, président de la mission 5G industrielle.

Le Te@chLab5 est une plateforme de réseau privé 5G fournie par Nokia et installée par son partenaire SNEF Telecom. Ce projet a été imaginé dans le cadre de la mission d'innovation et de formation des ingénieurs de Mines Nancy avec plusieurs partenaires. Il a été cofinancé par la région Grand Est dans le cadre de l'appel à projets PACTE et la Fondation Mines Nancy.

La solution mise en place est une 5G industrielle « stand alone » qui permettra aux étudiants et chercheurs de Mines Nancy de travailler sur des projets concrets tels que la mise en place de réseaux de communication intelligents pour les villes ou les smart grids (réseaux électriques intelligents), la création de systèmes de surveillance intelligents, les transports autonomes, la maintenance préventive, le développement de technologies de réalité augmentée, la conception de réseaux de santé intelligents, etc.

> **« C'est l'épine dorsale de la révolution numérique et pour l'industrie, c'est très important »**

« Avec ce nouvel outil, les élèves ingénieurs de Mines Nancy auront l'opportunité de travailler sur des projets d'application in situ utilisant les performances 5G, d'assister à des séminaires scientifiques et conférences industrielles, ou encore de suivre des formations technologiques transdisciplinaires », détaille François Rousseau. « Mines Nancy est devenu aujourd'hui le premier campus équipé en 5G privée de France. »

Le Te@chLab5G permettra également d'accompagner les partenaires de Mines Nancy, notamment les PME du Grand Est, en leur fournissant des informations, de la formation, des essais, de l'innovation et du transfert, ce qui est particulièrement important pour les entreprises qui n'ont pas les moyens d'accéder à de tels outils en interne. Avec cet outil innovant, l'école compte bien jouer également un rôle de tiers de confiance auprès de la société civile, en évaluant la technologie et ses usages et contribuer ainsi au débat public.

« La 5G est une technologie de communication sans fil qui offre une connectivité plus rapide, plus fiable, plus efficace et plus économe que les technologies précédentes », souligne Laurent Ciarletta, enseignant-chercheur. « C'est l'épine dorsale de la révolution numérique et pour l'industrie, c'est très important. Avec la 5 G, la latence (le temps de réponse du réseau) sera divisée par dix. »

Avec le Te@chLab5 G, Mines Nancy a repensé et complété son offre de formation avec la création d'une chaire industrielle « Usages de la 5G pour l'industrie », réunissant des partenaires français et étrangers (ETI, PME, grandes entreprises, établissements d'enseignement supérieur, etc.), et a ouvert la voie à une participation au projet européen « Future Network Academy », un consortium d'universités européennes visant à renforcer les compétences et les connaissances des futurs ingénieurs dans le domaine des réseaux du futur.

Jean-Christophe VINCENT

> « La 5G est une technologie de communication sans fil qui offre une connectivité plus rapide, plus fiable, plus efficace et plus économe que les technologies précédentes »
>
> **Laurent Ciarletta, enseignant-chercheur**

Des démonstrations probantes avec le robot quadrupède SCAR de Boston Dynamics

L'inauguration du Te@chLab5G a été l'occasion, pour l'école Mines Nancy, de montrer toute l'utilité de la 5G industrielle. Plusieurs démonstrations ont été réalisées avec des entreprises de l'écosystème Mines Nancy : Analytics NC qui travaille dans la détection de feux de forêt par intelligence artificielle et Alerion, spécialisée en solutions robotiques autonomes.

On a ainsi pu voir à l'œuvre le robot quadrupède SCAR de Boston Dynamics mettre en avant la 5G dans la surveillance de sites industriels ou militaires ou dans l'assistance aux populations.

Des démonstrations avec un robot quadrupède ont donné une idée de tout le potentiel de la 5G, notamment dans le secours à la personne. Photo ER/Alexandre MARCHI

Développement de la robotique autonome

Le robot, dirigé à distance, a réalisé une ronde en extérieur pour identifier de potentielles sources de risques. Détectant une fumée, il est capable d'alerter un centre de contrôle situé à des centaines de kilomètres de lui. « Le superviseur d'intervention prend en main la situation grâce à un casque de réalité virtuelle dans lequel il a accès à un centre de contrôle virtuel », explique un enseignant-chercheur de Mines Nancy. « Quand le robot équipé d'une caméra embarquée remarque une présence humaine, les images sont directement envoyées au centre de contrôle qui peut envoyer un drone pour vérifier l'état de la situation et récupérer des données vidéos en temps réel… Cette démonstration permet de montrer l'intérêt de la technologie 5G dans la communication des données, en très haut débit et avec une faible latence. »

La nouvelle plateforme de réseau privé 5G industrielle permettra le développement de la robotique autonome notamment lors de plusieurs expérimentations prévues avec l'Andra (Agence nationale pour la gestion des déchets radioactifs), réalisées dans le cadre de la chaire de recherche et de formations en « intelligence artificielle pour applications robotiques en environnements complexes ». Elle permettra également le développement de la réalité virtuelle en milieu souterrain. L'immersion virtuelle rendra possible la reproduction d'évènements ou d'accidents, de manière sécurisée mais avec un véritable sentiment de vécu.

Jean-Christophe VINCENT

uipé de la 5G industrielle

Le Te@chLab5G est utile pour tester des applications de robotique autonome dans des environnements industriels. Photo ER/Alexandre MARCHI

Plus de 800 étudiants en formation chaque année

L'École nationale supérieure des mines de Nancy ou Mines Nancy a été créée en 1919 dans le but de former des ingénieurs pour les mines et la métallurgie de la Lorraine. Plus de 800 étudiants y suivent leur formation chaque année. L'école, comptant 60 enseignants-chercheurs et 40 personnels administratifs, est présente sur deux campus : Artem à Nancy et GIP InSic à Saint-Dié-des-Vosges.

Trois formations d'ingénieurs, trois masters et trois mastères spécialisés

Mines Nancy, intégrée au Collégium Lorraine INP de l'Université de Lorraine, est l'une des écoles fondatrices de l'Alliance Artem avec ICN Business School et l'École nationale supérieure d'art et de design de Nancy. Elle est également partenaire stratégique de l'Institut Mines Télécom. Elle propose trois formations d'ingénieurs (ingénieur civil des mines, ingénieur de spécialité génie industriel et matériaux, ingénieur de spécialité génie mécanique parcours ingénierie de la conception), trois masters (en design, génie civil, sciences de la terre et des planètes) et trois mastères spécialisés (en cybersécurité, gestion, traitement et valorisation des déchets, et industrie des ressources minérales et société).

J.-C.V.

Ils ont dit

« Un grand moment pour l'école »

Anne Lauvergeon, présidente du CA de Mines Nancy

« Notre pays a découvert, à travers la crise du Covid, que l'industrie était indispensable. La 5G, qui n'est qu'une première étape dans l'évolution technologique, va être un formidable outil pour l'industrie et stimuler l'intelligence créatrice des étudiants et des chercheurs. C'est un grand moment pour l'école. »

« Répondre aux défis technologiques »

François Rousseau, directeur général de Mines Nancy

« Le Te@chLab5G de Mines Nancy va permettre de renforcer notre engagement en faveur de l'innovation technologique et de la formation d'ingénieurs. Nous serons capables de répondre aux défis technologiques et environnementaux de la société. Mines Nancy jouera son rôle de tiers de confiance. »

« Un enjeu de souveraineté »

Pierre-Gaël Chantereau, PDG de Nokia France

« La 5G va être le socle de l'industrie 4.0. Elle est 10 fois plus efficiente du point de vue énergétique que la 4G et constitue un enjeu de souveraineté pour la France. C'est le système sanguin de l'économie. La 5G sera l'un des outils pour décarboner les industries. Dans ce contexte, nous sommes très heureux de nous associer à Mines Nancy. »

« Un environnement unique pour se former »

Christophe Delaye, DG de SNEF Telecom

« La 5G industrielle permet de connecter et de transporter des informations dans les conditions de sécurité, de débit et de réactivité requises. Elle donnera aux étudiants un environnement unique pour se former et devenir les acteurs de la transformation des entreprises industrielles et du développement économique de nos régions. »

« Un foisonnement d'idées »

Philippe Herbert, président de la Mission 5G industrielle

« La Mission 5G industrielle, lancée en octobre 2021, a été créée pour accélérer la mise en place de la 5G et identifier les freins à son déploiement. Nous avons travaillé pour enlever ces freins. Nous constatons qu'il y a un foisonnement d'idées dès que la 5 G se déploie. La 5G, c'est vraiment l'enjeu des 10 prochaines années. »

LE JOURNAL DES ENTREPRISES

L'école d'ingénieurs des Mines Nancy invite les entreprises à expérimenter la 5G sur son campus

Par Jean-François Michel, le 05 avril 2023

L'école d'ingénieurs des Mines Nancy vient de déployer un réseau 5G industrielle sur son campus. Un nouveau terrain d'expérimentation pour les étudiants, mais aussi pour les entreprises qui voudront prendre position sur les réseaux du futur.

▲ L'école des Mines Nancy compte sur la créativité de ses étudiants et sur l'appétence des

entreprises pour trouver de nouveaux cas d'usage pour la 5G. — Photo : Mines Nancy - Steeve Josch

Pas facile d'inaugurer un réseau de téléphone mobile. Symboliquement, l'ensemble des acteurs impliqués ont appuyé sur un gros bouton rouge sur une tablette pour faire officiellement des Mines Nancy le premier campus français à disposer d'un réseau de téléphone mobile équipé de la 5G industrielle. Déployé par SNEF Télécom, grâce à du matériel fourni par le groupe finlandais Nokia, ce nouvel outil représente un investissement de 200 000 €, qui va permettre à l'école des Mines Nancy de déployer un projet complet autour de la 5G et de ces enjeux, le tout étant rassemblé sous l'appellation Te@chLab 5G.

"C'est évidemment un atout pour nos étudiants, dont les compétences, après avoir étudié avec un tel outil, intéresseront les entreprises", estime Loïck Briot, ingénieur de recherches à l'école des Mines Nancy et cheville ouvrière du déploiement de la 5G sur le campus. Mettre à disposition les outils et les technologies qui arriveront dans plusieurs années dans les entreprises, l'école des Mines Nancy s'est engouffré dans cette stratégie : entre l'achat de plusieurs robots de chez Boston Dynamics, des drones ou encore des bras robotisés, et maintenant la 5G et le fonctionnement du Te@achLab, l'école a déjà injecté près d'un million pour préparer le futur.

Foisonnement d'idées autour de la 5G industrielle

Mais avec des débits pouvant atteindre jusqu'à 20 Gbit par seconde, soit la vitesse d'un réseau fixe, et des niveaux de latence, soit le délai avant le transfert des données, divisés par dix, la 5G présente des performances tellement élevées que les cas d'usage n'existent pas encore. Pour Laurent Ciarletta, enseignant-chercheur à l'école des Mines Nancy, cette nouvelle génération de réseaux de téléphonie mobile permet de "vraiment couper les fils" et donc d'envisager des applications industrielles hors de portée de la génération précédente, la 4G. "Si vous avez des idées autour de la 5G, venez chez nous pour les faire", a lancé l'enseignant aux dirigeants d'entreprises présents lors de l'inauguration du Te@chLab 5G.

▲ François Rousseau, Pierre-Gaël Chantereau, Christophe Delaye, Anne Lauvergeon et Philippe Herbet ont lancé symboliquement la 5G sur le campus de l'école des Mines Nancy. - Photo : Mines Nancy - Steeve Josch

Un appel relayé par Philippe Herbert, le président de la Mission 5G industrielle, mission qui a remis un rapport au gouvernement pour levers les freins au développement de la 5G industrielle en France. "J'espère que vous allez sortir beaucoup de cas d'usage", a lancé Philippe Herbert aux dirigeants, mais aussi aux étudiants des Mines Nancy. "Chaque fois qu'un réseau 5G est déployé, nous assistons à un foisonnement d'idées", rappelle le président de la mission 5G.

Pour Christophe Delaye, le directeur général du groupe SNEF, la 5G a été conçue pour être déployée dans l'industrie. Et "les idées nouvelles viennent avec des gens nouveaux", avance le dirigeant. Une façon de saluer la pertinence du positionnement de l'école des Mines Nancy, qui mise sur la créativité de ses étudiants pour explorer les possibilités ouvertes par la 5G. "Il ne suffit pas de brancher la 5G", insiste Pierre-Gaël Chantereau, le PDG de Nokia France. "On doit s'approprier cette technologie pour en relever le potentiel et transformer l'industrie."

"La 5G va devenir le système nerveux de notre économie"

De l'avis de tous les experts rassemblés pour l'inauguration du Te@chLab 5G, ce ne sont pas les usages des particuliers qui révéleront le potentiel de cette

nouvelle génération de réseau mobile : "La 5G va devenir le système nerveux de notre économie", estime le PDG de Nokia France, en décrivant les possibilités offertes par cette technologie en matière de décarbonation de l'industrie.

"Cette plateforme est la vôtre", concluait le directeur des Mines Nancy, François Rousseau, en se tournant vers les dirigeants d'entreprise. Si l'école d'ingénieurs nancéienne s'est fixée pour objectifs de nouer 25 partenariats avec des entreprises autour de la 5G, pour l'instant, seule une start-up basée à Nancy, Alérion, s'est emparée du Te@chLab, en développant un cockpit de surveillance virtuelle, capable d'agglomérer plusieurs flux vidéo au sein d'une même interface grâce au débit élevé de la 5G.

Mines Nancy devient le premier campus équipé en 5G privée de France

publié le 6 avril 2023 par *Alliancy*

Le mardi 4 avril 2023, Mines Nancy, Nokia et la SNEF Telecom (Eiffage Energie Systèmes) inauguraient le Te@chLab5G, une plateforme de réseau privé 5G fournie par Nokia et installée par son partenaire SNEF Telecom (Eiffage Energie Systèmes) sur le campus de Mines Nancy. Ce projet a pour objectif de déployer une infrastructure de pointe pour permettre la formation des étudiants ainsi que des tests et expérimentations pour les futurs ingénieurs et les partenaires du projet.

La Commission Européenne a placé le développement de la 5G comme l'une des initiatives prioritaires du plan « Numériser l'industrie européenne », soutenue par des appels à projets notamment sur la 5G pour la souveraineté dans les réseaux de télécommunications lancé par le ministère de l'Économie, des Finances et de la Souveraineté Industrielle et Numérique.

C'est pour accompagner cette transformation numérique et agir avec un temps d'avance au service de la compétitivité nationale que Mines Nancy, école d'ingénieurs de l'Université de Lorraine a créé le projet Te@chLab5G, co-financé par la Région Grand Est dans le cadre de l'appel à projets PACTE et la Fondation Mines Nancy en partenariat avec Nokia et SNEF Telecom (Eiffage Energie Systèmes). Le projet s'enrichit de la participation active et des expertises des start-up Alerion et AnalyticsNC, de l'Agence nationale pour la gestion des déchets radioactifs (ANDRA), de l'IHU Strasbourg et du Laboratoire lorrain de Recherche en Informatique et ses Applications –

LORIA (UMR 7503).

Nokia a installé sa solution Digital Automation Cloud (DAC) qui permet un déploiement simple, de classe industrielle, en utilisant des éléments préconfigurés afin de créer un réseau 5G privé. Cette plateforme, utilisant Nokia MX Industrial Edge, est fiable et sécurisée et offre une connectivité à haute performance, faible latence et une capacité de traitement des données en périphérie.

Elle est totalement évolutive et permettra d'intégrer les développements futurs de la 5G avancée.

Accompagner la transition numérique en tant qu'acteur neutre

Ce projet, imaginé dans le cadre de la mission d'innovation technologique et de formation des ingénieurs de Mines Nancy par l'équipe de son TechLab, offre une infrastructure de pointe pour les expérimentations, les essais et la formation des étudiants de l'école, ainsi que pour les partenaires externes du projet. La solution mise en place est une 5G industrielle stand alone (avec une infrastructure entièrement 5g, alors que l'essentiel de la 5g déployée aujourd'hui repose pour partie sur une infrastructure 4g) et propriétaire, différente de la 5G grand public distribuée par les opérateurs, conçue pour répondre aux besoins spécifiques des entreprises et des industries et offrir des possibilités de transformation numérique dans de multiples domaines (notamment l'IoT, la robotique autonome et collaborative, la cybersécurité, les smart grid, la télémédecine, etc.).

La technologie 5G permet ainsi :

1. Une vitesse de transmission de données plus rapide : la 5G offre une vitesse de communication beaucoup plus rapide que les technologies précédentes (10 fois plus rapide que la 4G), permettant de transférer rapidement des données volumineuses et de réaliser des projets en temps réel.
2. Une faible latence : la 5G offre également une faible latence, ce qui peut être particulièrement utile pour les applications nécessitant une réponse rapide, comme le contrôle des machines/robots se déplaçant rapidement.
3. Une meilleure capacité de connexion multi-usagers : la 5G peut connecter un plus grand nombre d'appareils simultanément, élément utile pour les projets nécessitant de nombreux dispositifs connectés.
4. Une plus grande fiabilité : la 5G dispose d'une plus grande fiabilité que les technologies précédentes, essentiel pour les projets critiques nécessitant une connectivité ininterrompue ainsi qu'un contrôle d'accès et une sécurité à la pointe.

« Le Te@chLab5G de Mines Nancy va permettre de renforcer notre engagement en faveur de l'innovation technologique et de la formation d'ingénieurs, capables de répondre aux défis technologiques et environnementaux de la société. En tant que première école française équipée de la 5G industrielle, Mines Nancy joue un rôle d'acteur neutre en expérimentant et analysant de manière objective les intérêts de cette innovation technologique et en s'assurant qu'elle soit utilisée de manière responsable et durable par ses partenaires. » affirme François Rousseau, directeur général de Mines Nancy

Une plateforme pour expérimenter les possibilités de la 5G industrielle

Pour accompagner les acteurs de la révolution industrielle 4.0 et leurs projets, Mines Nancy, à travers le Te@chLab 5G, crée un cadre de travail innovant et une offre pédagogique de haut niveau.

La création du Te@chLab5G sur le campus de Mines Nancy permettra de travailler sur des projets concrets tels que la mise en place de réseaux de communication intelligents pour les

villes ou les smart grids, la création de systèmes de surveillance intelligents, les transports autonomes, la maintenance préventive, le développement de technologies de réalité augmentée, l'optimisation de l'industrie manufacturière et la conception de systèmes de fabrication intelligents, des systèmes ou des IA , des robots et des humains collaborent dans des environnements connectés de confiance ou encore la mise en place de réseaux de santé intelligents.

Les élèves ingénieurs de Mines Nancy auront ainsi l'opportunité de travailler sur des projets d'application in situ utilisant les performances 5G, d'assister à des séminaires scientifiques et conférences industrielles et de participer à des hackathons 5G avec les établissements d'enseignement supérieur de la région.

Des formations technologiques transdisciplinaires en formation initiale et en formation professionnelle pour former le plus grand nombre à l'IA, la robotique, la 5G, l'IoT, etc. verront le jour, en présentiel et en e-learning.

Du côté de la recherche, une chaire industrielle sur les « Usages de la 5G pour l'industrie » et une chaire de recherche et de formation sur « L'intelligence artificielle pour applications robotiques en environnement complexes » ont été créés.

A travers le Te@chLab5G, Mines Nancy souhaite renforcer collectivement la compétitivité régionale des entreprises et de l'industrie mais aussi former massivement les étudiants et professionnels à cette technologie de rupture pour accélérer la révolution numérique et bâtir un écosystème ouvert qui connecte les compétences universitaires, les géants des nouvelles technologies et les entreprises locales pour développer la puissance 5G sur le territoire.

« La 5G va être le socle de l'industrie 4.0 et aura un impact transformatif sur l'économie au sens large. Il est temps d'accélérer son déploiement et la formation va jouer un rôle clé dans l'appropriation de cette innovation. Dans ce contexte, nous sommes particulièrement fiers de nous associer à l'Ecole des Mines de Nancy, à la fois au travers du réseau privé 5G que nous avons déployé et de notre participation à la chaire 5G de l'école. Les étudiants pourront expérimenter cette technologie dans les conditions réelles et ils seront prêts demain pour accompagner son adoption et créer des nouvelles solutions dans les entreprises. La 5G va en outre avoir un impact très important dans l'éducation, avec notamment le développement de l'apprentissage à distance qui utilise des outils tels que la réalité augmentée et virtuelle pour créer une expérience éducative immersive. » déclare Pierre-Gaël Chantereau, Président-directeur général de Nokia France.

Nokia a déployé des réseaux critiques chez plus de 2 600 clients dans les secteurs du transport, de l'énergie, des grandes entreprises, de la fabrication, du web et du secteur public, dans le monde entier.

« L'évolution accélérée des technologies ces dernières années avec le développement du big data, de l'IOT, des jumeaux numériques et de l'intelligence artificielle devient une réalité pour l'ensemble de l'industrie, de la logistique et de la santé. La 5G industrielle permet de connecter et de transporter les informations dans les conditions de sécurité, de débit et de réactivité requises. Elle est et sera le socle de l'industrie 4.0. Nous sommes très heureux d'avoir contribué à la mise en place de ce réseau privé 5G et de participer à la chaire 5G de l'école des Mines de Nancy. L'ensemble de ces moyens donnera aux étudiants un environnement unique pour se former et devenir les acteurs de la transformation des entreprises industrielles et du développement économiques de nos régions. » déclare Christophe Delaye, Directeur Général de SNEF Telecom (Eiffage Énergie Systèmes).

INTELLIGENCE ARTIFICIELLE

Publié 6 avril 2023, 17:55

On accorde autant de confiance à ChatGPT qu'à un humain

Selon une étude, les êtres humains accordent autant de confiance, lors d'un conflit moral, à un être humain qu'à un robot conversationnel.

Une étude plaide pour une éducation du grand public aux limitations de ces systèmes.
AFP

Des personnes confrontées à un choix moral ont accordé autant de confiance à un **robot conversationnel** comme **ChatGPT** qu'à un supposé **conseiller humain**, selon une étude publiée jeudi, qui plaide pour une éducation de la population aux limites inhérentes à ce genre d'outils. Un tramway, hors de contrôle, va écraser un groupe de cinq personnes sur la voie, à moins d'utiliser un aiguillage déviant la machine vers une voie où se trouve une seule personne.

Dans ce test, «empiriquement, la plupart des gens n'hésitent pas à utiliser l'aiguillage», rappellent les auteurs de l'étude publiée dans Scientific Reports. À moins qu'avant de prendre la décision, un «conseiller moral» les en dissuade ou les y encourage.

Les auteurs ont testé des personnes pour voir si elles étaient influencées différemment selon que l'avis qui leur était donné était présenté comme émanant d'un «conseiller moral», supposé humain, ou bien d'un «robot conversationnel d'intelligence artificielle, utilisant l'apprentissage profond pour parler comme un humain».

«Conseiller moral» décisif

L'équipe menée par Sebastian Krügel, chercheur à la faculté allemande des sciences informatiques d'Ingolstadt, a constaté d'abord que les plus de 800 participants au test suivaient assez étroitement le conseil qui leur était prodigué.

Même dans une variante plus problématique du test qui oblige à choisir de pousser ou pas sur la voie une personne pour en sauver cinq autres. Une décision beaucoup plus difficile à prendre et où l'avis du «conseiller moral» s'est avéré décisif.

Inconstance morale

Mais le plus préoccupant a été que les participants s'avèrent mettre sur un pied d'égalité les deux genres de conseillers. Or, leurs conseils étaient en fait et à leur insu, tous générés par

ChatGPT, illustrant la capacité du système à mimer un discours humain.

Le programme, capable de répondre de façon intelligible à toutes sortes de requêtes, s'avère d'une remarquable inconstance en matière morale. Arguant aussi bien en faveur de sacrifier une personne pour en sauver cinq que plaidant le contraire. Rien d'étonnant, selon Sebastian Krügel, pour qui «ChatGPT est une sorte de perroquet aléatoire, qui assemble des mots sans comprendre leur sens», dit-il à l'AFP.

«ChatGPT ne comprend pas ce qu'il raconte»

Spécialiste du traitement automatique du langage, le professeur en informatique Maxime Amblard, de l'Université de Lorraine, renchérit en décrivant un «méga modèle de langue, entraîné pour faire des phrases», et qui «n'est pas du tout fait pour chercher de l'information».

Et encore moins pour donner des conseils, moraux ou pas. Mais alors, pourquoi les participants au test lui ont-ils accordé une si grande confiance? «ChatGPT ne comprend pas ce qu'il raconte, mais il nous paraît que si», selon Sebastian Krügel, parce que «nous avons l'habitude d'associer la cohérence et l'éloquence à l'intelligence». Au final, les participants au test «adoptent volontairement et s'approprient la position morale d'un robot conversationnel» pourtant dénué de toute conscience, constate le chercheur.

«Pas un système d'intelligence artificielle»

Son étude plaide pour une éducation du grand public aux limitations de ces systèmes, allant bien au-delà de la seule transparence sur le fait qu'un contenu ait été généré par un robot conversationnel. «Même si les gens savent qu'ils sont en interaction avec un système non humain, ils sont influencés par ce qu'il leur dit», a dit à l'AFP le Pr. Amblard, qui n'a pas participé à l'étude.

Le problème, selon lui, est que le public croit que ChatGPT est «une intelligence artificielle au sens où elle serait douée de compétences, d'un peu de ce que les humains sont capables de

faire», alors qu'en fait «ce n'est pas un système d'intelligence artificielle». Car il n'a «aucune modélisation, ni sémantique ni pragmatique», ajoute-t-il.

(AFP)

ChatGPT : des utilisateurs font autant confiance à un robot conversationnel qu'à un humain

Par Maxence Fabrion (𝕏 @max_fabrion), ETX | Publié le 10/04/23 à 15h15

Des chercheurs ont mené une expérience pour tester la confiance accordée par des personnes à un robot conversationnel comme ChatGPT et à un conseiller humain. Finalement, les deux genres de conseillers ont été mis sur un pied d'égalité par les participants.

ChatGPT fascine autant qu'il inquiète depuis son lancement fin 2022.
© Getty — Pavlo Gonchar/SOPA Images/LightRocket

Des personnes confrontées à un choix moral ont accordé autant de confiance à un robot conversationnel comme ChatGPT qu'à un supposé conseiller humain, selon une étude, qui plaide pour une éducation de la population aux limites inhérentes à ce genre d'outils.

Un tramway, hors de contrôle, va écraser un groupe de cinq personnes sur la voie, à moins d'utiliser un aiguillage déviant la machine vers une voie où se

voie, à moins d'utiliser un aiguillage déviant la machine vers une voie où se trouve une seule personne. Dans ce test, *"empiriquement, la plupart des gens n'hésitent pas à utiliser l'aiguillage"*, rappellent les auteurs de l'étude publiée dans *Scientific Reports*. A moins qu'avant de prendre la décision, un "conseiller moral" les en dissuade ou les y encourage. Les auteurs ont testé des personnes pour voir si elles étaient influencées différemment selon que l'avis qui leur était donné était présenté comme émanant d'un *"conseiller moral"*, supposé humain, ou bien d'un *"robot conversationnel d'intelligence artificielle, utilisant l'apprentissage profond pour parler comme un humain*".

L'équipe menée par Sebastian Krügel, chercheur à la faculté allemande des sciences informatiques d'Ingolstadt, a constaté d'abord que les plus de 1800 participants au test suivaient assez étroitement le conseil qui leur était prodigué. Même dans une variante plus problématique du test qui oblige à choisir de pousser ou pas sur la voie une personne pour en sauver cinq autres. Une décision beaucoup plus difficile à prendre et où l'avis du *"conseiller moral"* s'est avérée décisive.

À LIRE ÉGALEMENT :

NEWS : Intelligence artificielle

ChatGPT : une interdiction en France n'est pas à l'ordre du jour, selon le ministre du Numérique

Jean-Noël Barrot, ministre délégué au Numérique, ne veut pas bloquer ChatGPT à l'instar de la Cnil italienne Il y a une semaine. Il plaid...

il y a 1 an

Inconstance morale

Mais le plus préoccupant a été que les participants s'avèrent mettre sur un pied d'égalité les deux genres de conseillers. Or, leurs conseils étaient en fait et à leur insu, tous générés par ChatGPT, illustrant la capacité du système à mimer un discours humain. Le programme, capable de répondre de façon intelligible à toutes sortes de requêtes, s'avère d'une remarquable inconstance en matière morale. Arguant aussi bien en faveur de sacrifier une personne pour en sauver cinq que plaidant le contraire. Rien d'étonnant, selon Sebastian Krügel, pour qui *"ChatGPT est une sorte de perroquet aléatoire, qui assemble des mots sans comprendre leur sens"*, dit-il à l'*AFP*.

Spécialiste du traitement automatique du langage, le professeur en informatique Maxime Amblard, de l'Université de Lorraine, renchérit en décrivant un *"méga modèle de langue, entraîné pour faire des phrases"*, et qui *"n'est pas du tout fait pour chercher de l'information"*. Et encore moins pour donner des conseils, moraux ou pas. Mais alors, pourquoi les participants au

test lui ont-ils accordé une si grande confiance ? *"ChatGPT ne comprend pas ce qu'il raconte, mais il nous paraît que si"*, selon Sebastian Krügel, parce que *"nous avons l'habitude d'assigner la cohérence et l'éloquence à l'intelligence"*.

À LIRE ÉGALEMENT :

NEWS : Intelligence artificielle

Pour Bill Gates, faire une pause de six mois dans l'IA ne sert à rien

Très enthousiaste sur les avancées réalisées ces derniers mois dans l'intelligence artificielle, Bill Gates estime que le moratoire de si...

2

il y a 1 an

Éducation et régulation

Au final, les participants au test *"adoptent volontairement et s'approprient la position morale d'un robot conversationnel"* pourtant dénué de toute conscience, constate le chercheur. Son étude plaide pour une éducation du grand public aux limitations de ces systèmes, allant bien au-delà de la seule transparence sur le fait qu'un contenu ait été généré par un robot conversationnel. *"Même si les gens savent qu'ils sont en interaction avec un système non humain, ils sont influencés par ce qu'il leur dit"*, a dit à l'*AFP* le Pr. Amblard, qui n'a pas participé à l'étude.

Le problème, selon lui, est que le public croit que ChatGPT est *"une intelligence artificielle au sens où elle serait douée de compétences, d'un peu de ce que les humains sont capables de faire"*, alors qu'en fait *"ce n'est pas un système d'intelligence artificielle"*. Car il n'a *"aucune modélisation, ni sémantique, ni pragmatique"*, ajoute-t-il.

Plusieurs autorités de régulation, dont celle de l'UE, travaillent à des projets d'encadrement de l'intelligence artificielle. S'agissant de ChatGPT, l'Italie est devenue fin mars le premier pays occidental à bloquer le service, pour des craintes liées notamment à son utilisation des données personnelles. Sebastian Krügel n'en craint pas moins que même si un cadre légal est important, *"le progrès technologique garde toujours un coup d'avance"*. D'où l'importance d'une éducation de la population sur ce thème *"dès la scolarité"*.

Premier campus équipé en 5G privée de France, Mines Nancy se place en "pole position internationale"

Dépêche n° 690346

6 MIN DE LECTURE

Par PASCALINE MARION
Publiée le 12/04/2023 à 17h00

Unique sur un campus universitaire français, le hub 5G industriel mis en place à Mines Nancy (université de Lorraine) au cours de l'année écoulée ("Te@chLab5G") a été inauguré le 4 avril 2023. S'appuyant sur l'expertise technologique de Nokia, l'école entend se positionner "à l'avant-garde" sur les enjeux de la révolution industrielle 4.0 (robotique, IA, internet des objets, etc.), à travers un projet pluriannuel co-financé par la région Grand Est. Les intervenants identifient les principaux leviers de cette transformation, de l'appropriation technique des outils à la préparation des compétences.

IA
intelligence artificielle

Lancement officiel de la solution de 5G industrielle mise en place à Mines Nancy, avec (de g. à d.) François Rousseau (DG de l'école), Pierre-Gaël Chantereau (PDG de Nokia France), Christophe Delaye (DG de Snef Telecom), Anne Lauvergeon (présidente du conseil d'école) et Philippe Herbert (président de la mission 5G), le 4 avril 2023. | AEF - PM

"C'est un grand moment, et une évolution d'une école des Mines qui pulse", se réjouit Anne Lauvergeon, ingénieure en chef des Mines et présidente du conseil d'école de Mines Nancy, le 4 avril 2023, lors de l'inauguration du "Te@chLab[5G]", la plateforme de réseau privé 5G fournie par Nokia (1) de la grande école d'ingénieurs, installée par son partenaire Snef Telecom (Eiffage Énergie Systèmes). "Ce que je trouve formidable, c'est que nous puissions stimuler l'intelligence créatrice des élèves, mais également des chercheurs et de tous les industriels de notre écosystème", ajoute-t-elle. Sur le campus Artem, une centaine de personnes (industriels, représentants de la tech, partenaires, etc.) sont venues assister à ce lancement, qui constitue une suite logique pour l'école, et qui lui donne aussi un temps d'avance.

Artem
Art, technologie, management

"DISPOSER D'UN RÉSEAU PROPRIÉTAIRE, PERFORMANT" (F. ROUSSEAU)

"Dans la révolution numérique, il y a différentes facettes : internet des objets, données massives, intelligence artificielle, robotique, etc. : elles sont toutes reliées par une chose : le réseau", expose le directeur général de Mines Nancy, François Rousseau.

François Rousseau, directeur général de Mines Nancy (UL). | AEF

Dès 2019, la 5G a été qualifiée "d'épine dorsale [de nos sociétés, et de nos économies] par l'Union européenne [(2)]", rappelle-t-il. "À Mines-Nancy, il nous est très vite apparu que pour le développement de nos activités, nous devions disposer d'un réseau propriétaire, performant, pour la connexion entre les différentes autres briques technologiques sur lesquelles nous nous étions déjà investis."

Une dizaine d'années après l'émergence du "TechLab" au sein de l'école, le "choix de la 5G" s'est imposé pour une série de raisons. "La première, c'est pour nos élèves : pour les former sur les technologies de demain". François Rousseau évoque "la 5G, mais aussi tous les usages qu'elle amène – l'IA, l'internet des objets (*smart grid*, etc.), la sécurité, les applications sur les terminaux, etc.", "avec des opportunités induites dans tous les domaines scientifiques qui sont couverts par les différents départements de l'école."

"La deuxième raison, c'est pour l'équipement du campus, et le service qu'il apporte aux usagers. C'est un accès à des ressources – des logiciels, des équipements expérimentaux, des machines, et un outil à notre main, qu'on va pouvoir librement paramétrer", ajoute François Rousseau.

IA
intelligence artificielle

1 M€ D'INVESTISSEMENT

Les dépenses liées aux investissements (robot *Boston Dynamics* Spot, bras robotisé, équipements 5G, drones, plateforme robotique mobile, etc.) et au fonctionnement du Te@chLab[5G] durant trois ans s'élèvent à un million d'euros. Au-delà du partenariat avec Nokia, qui a fourni une partie du matériel, Mines Nancy a pu disposer de l'appui de sa fondation, ainsi que de l'accompagnement de la collectivité régionale, à hauteur de 412 000 €. "Grâce à la région Grand Est, qui nous soutient à travers le projet Pacte compétences [sur 2021-2023], nous disposons des ressources humaines indispensables", salue François Rousseau. "Nous avons pu réaliser une montée en compétences, qui a déjà été valorisée par l'Europe, puisqu'à l'été 2022, nous avons remporté en tant que *project leader* le projet Erasmus "Future Network Academy", aux côtés de l'université de Delft (Pays-Bas), des écoles polytechniques de Madrid et de Milan, de l'université d'Aalto (Finlande) et de l'université du Luxembourg."

"JOUER UN RÔLE DE TIERS DE CONFIANCE AUPRÈS DE LA SOCIÉTÉ CIVILE"

"L'objectif est aussi d'accompagner nos partenaires, tout particulièrement sur le territoire du Grand Est pour de l'information, de la formation, des essais, de l'évaluation, de l'innovation et du transfert, de la R&D", poursuit François Rousseau. "Il s'agit aussi d'offrir une brique technologique clé à nos étudiants entrepreneurs". Mines Nancy prévoit en outre de "jouer un rôle de tiers de confiance auprès de la société civile", et enfin de "fédérer un réseau de compétences autour de la 5G", de nature universitaire.

Mines Nancy est "le premier campus universitaire en France équipé de la 5G", qui plus est "de la 5G *stand alone*, donc de la vraie 5G – avec toutes ses compétences et capacités techniques", se félicite Pierre-Gaël Chantereau, PDG de Nokia France. Pour l'opérateur, impliqué dans de nombreux projets "5G" (sur une dizaine de sites industriels, tel qu'Alcatel Submarine Networks), "celui de Nancy est en pole position, non seulement au plan national, mais aussi aux plans européen et international".

LA 5G, "ENJEU DE SOUVERAINETÉ POUR LA FRANCE" ET "LEVIER DE DÉCARBONATION"

"En termes d'innovation, il y a deux principes importants", précise-t-il. "D'abord, être dans le *timing* de l'innovation. Aujourd'hui, la 5G n'est pas encore une technologie mature et adulte [...], donc l'École des mines de Nancy prend un point d'avance". Et d'évoquer comme autre principe "l'appropriation de la technologie", qui sera rendue possible "à travers la chaire '5G et réseaux du futur'". "Il ne s'agit pas juste d'absorber passivement l'innovation, c'est de la transformation pour créer de nouveaux process, services, et utilisations. C'est ce qui pourra se passer ici, dans cette école". Pour Pierre-Gaël Chantereau, la 5G "relève d'un enjeu de souveraineté pour la France", et constitue "un levier de décarbonation".

PDG
Président-directeur général

"C'est vraiment l'enjeu des dix prochaines années", abonde Philippe Herbert, qui préside la "mission 5G"

nationale (rattachée au ministère de l'Économie, des Finances et de la Relance). "La 5G, cela ne fonctionne pas tout seul", dit-il, revenant sur plusieurs freins sur lesquels la mission s'est penchée. "Il y a le sujet des cas d'usage : j'espère que vous allez en sortir beaucoup ! C'est en utilisant que l'on voit toute l'étendue de ce que l'on peut faire. Et il y a aussi les compétences, certainement l'un des gros enjeux de la réindustrialisation."

PRÉPARER LES INNOVATIONS DE RUPTURE

Comme l'illustre le DG de l'école, "la 5G est porteuse d'innovations de rupture pour l'industrie – elle permet la maintenance préventive, la fabrication flexible et de haute précision, le suivi et la traçabilité", "mais aussi pour la santé, pour la mobilité, pour la sécurité, pour l'énergie", avec divers projets en cours en lien avec des partenaires du territoire [3].

Preuve en a été faite à travers une démonstration autour de l'utilisation de robots quadrupèdes, dans le cadre d'une simulation d'opération de secours après détection de fumées dans le parc qui jouxte la scène. Plusieurs caméras et drones permettent d'adresser des flux vidéo de façon extrêmement rapide à un "centre de commandement" à l'intérieur de l'école, ces flux étant rassemblés au sein d'un "cockpit virtuel" (produit par la *start up* Alerion et le laboratoire Loria).

Plusieurs démonstrations ont été mises en place pour l'inauguration du Te@chLab 5G, dont la supervision d'une mission robotique (avec le vecteur aérien Hawk) depuis un cockpit virtuel.
| *AEF*

Désormais, les étudiants de Mines Nancy pourront appréhender la 5G à différentes étapes de leur parcours (voir encadré). "Ceux de 2e année qui vont se spécialiser en informatique auront l'occasion de pratiquer, avec d'ici dix jours de premiers cours autour du développement d'applications mobiles sur smartphone. Et, à partir de la 3e année, avec des TP sur les systèmes cyber-physiques. L'an prochain, un tiers des élèves de l'école aura eu accès aux technos 5G à l'école", envisage Laurent Cierletta, enseignant-chercheur Mines Nancy/Loria et pilote du Te@chLab5G.

FORMATION : PROJETS D'APPLICATION, HACKATHONS 5G, ETC.

"Le Te@chLab[5G] repense et complète l'offre de formation de Mines Nancy", avec notamment :

- "l'organisation de séminaires scientifiques et conférences industrielles, de projets d'application *in situ*, de cours sur le traitement des données ;
- l'organisation de hackathons 5G intégrant les universités et grandes écoles en France et en Europe sur des sujets proposés par les industriels partenaires ;
- le développement de briques de formation technologiques transdisciplinaires en formation initiale et professionnelle (IA, robotique, 5G, réalité virtuelle, IoT, etc.), dont certaines en e-learning ;
- le développement de travaux pratiques mutualisés avec des écoles de l'IMT Grand Est".

(1) Avec la solution "Digital Automation Cloud" permettant "un déploiement simple, de classe industrielle, en utilisant des éléments préconfigurés, afin de créer un réseau 5G privé", est-il précisé par communiqué. Cette plateforme offre une connectivité à haute performance, faible latence et une capacité de traitement des données en périphérie.

(2) La 5G étant l'un des cinq domaines prioritaires de l'initiative 'Numériser l'industrie européenne' établie par la Commission européenne en 2018.

(3) Avec la participation des start-up Alerion et AnalyticsNC (Nouvelle-Calédonie), l'Andra, l'IHU de Strasbourg et le Loria (UMR CNRS/UL/Inria).

Loria
Laboratoire lorrain de recherche en informatique et ses applications

TP
Travaux pratiques

IoT
Internet des objets

IMT
Institut Mines-Télécom

Andra
Agence nationale pour la gestion des déchets radioactifs

IHU
Institut hospitalo-universitaire

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Mines Nancy s'associe à Nokia et à SNEF Telecom (EIFFAGE Energie Systèmes) pour devenir le premier campus équipé en 5G privée de France

La rédaction | 14 avril 2023 | Ecoles d'ingénieurs

Mines Nancy s'associe à Nokia et à SNEF Telecom (EIFFAGE Energie Systèmes) pour devenir le premier campus équipé en 5G privée de France

Le 4 avril 2023, Mines Nancy, Nokia et la Systèmes) inauguraient le Te@chLab5G, fournie par Nokia et installée par son partenaire SNEF Telecom (Eiffage Energie Systèmes) sur le campus de Mines Nancy. Ce projet a pour objectif de déployer une infrastructure de pointe pour permettre la formation des étudiants ainsi que des tests et expérimentations pour les futurs ingénieurs et les partenaires du projet.

Ce projet, imaginé dans le cadre de la mission d'innovation technologique et de formation des ingénieurs de Mines Nancy par l'équipe de son TechLab, offre une infrastructure de pointe pour les expérimentations, les essais et la formation des

étudiants de l'école, ainsi que pour les partenaires externes du projet. La solution mise en place est une 5G industrielle *stand alone* (avec une infrastructure entièrement 5g, alors que l'essentiel de la 5g déployée aujourd'hui repose pour partie sur une infrastructure 4g) et propriétaire, différente de la 5G grand public distribuée par les opérateurs, conçue pour répondre aux besoins spécifiques des entreprises et des industries et offrir des possibilités de transformation numérique dans de multiples domaines (notamment l'IoT, la robotique autonome et collaborative, la cybersécurité, les smart grid, la télémédecine, etc.).

« Le Te@chLab5G de Mines Nancy va permettre de renforcer notre engagement en faveur de l'innovation technologique et de la formation d'ingénieurs, capables de répondre aux défis technologiques et environnementaux de la société. En tant que première école française équipée de la 5G industrielle, Mines Nancy joue un rôle d'acteur neutre en expérimentant et analysant de manière objective les intérêts de cette innovation technologique et en s'assurant qu'elle soit utilisée de manière responsable et durable par ses partenaires. » affirme **François Rousseau, directeur général de Mines Nancy**

Les Tablettes lorraines, 17 avril 2023

Formation

Mines Nancy inaugure le premier campus 5G de France

© Mines Nancy

Nom de code : Te@chLab5G. Signes particuliers : plateforme de réseau privé 5G fournie par Nokia et installée par SNEF (Eiffage Énergie Systèmes) installée sur le campus nancéien de Mines Nancy. Inauguré le 4 avril dernier, ce projet fait de Mines Nancy le premier campus en 5G privée de France. Imaginé dans le cadre de la mission d'innovation technologique et de formation des ingénieurs de Mines Nancy par l'équipe de son TechLab, ce projet offre une infrastructure de pointe pour les expérimentations, les essais et la formation des étudiants de l'école, ainsi que pour les partenaires externes du projet. La solution mise en place est une 5G dite industrielle, différente de la 5G grand public distribuée par les opérateurs, elle est conçue pour répondre aux besoins spécifiques des entreprises et des industries en offrant des possibilités de transformation numérique dans de multiples domaines à l'image de la robotique autonome et collaborative ou encore la cybersécurité. *«Le Te@chLab5G de Mines Nancy va permettre de renforcer notre engagement en faveur de l'innovation technologique et de la formation d'ingénieurs capables de répondre aux défis technologiques et environnementaux de la société»*, explique François Rousseau, directeur général de Mines Nancy. *«En tant que première école française équipée de la 5G industrielle, Mines Nancy joue un rôle d'acteur neutre en expérimentant et analysant de manière objective les intérêts de cette innovation technologique et en s'assurant qu'elle soit utilisée de manière responsable et durable par ses partenaires.»* Détails prochainement !

ChatGPT "va avoir un impact colossal sur les métiers" et les formations (IAE France, Aunege, Fnege)

Sur le sujet de ChatGPT et autres IA génératives, "il y a deux scénarios", estime Bernard Quinio, directeur du service de formation continue de l'université Paris Nanterre : "On peut imaginer jouer aux gendarmes et aux voleurs avec nos étudiants, comme on a pu déjà l'envisager il y a quelques années avec la calculatrice. Ou alors, on part du postulat que ces mêmes étudiants vont travailler avec les IA". Ce sujet a été abordé lors de plusieurs rencontres thématiques les 31 mars et 6 avril 2023, organisées par IAE France, l'Aunege et la Fnege. L'impact des IA sur les métiers est aussi abordé.

Les IA vont modifier en profondeur les métiers, avec la question de comment les formations vont s'adapter. | Pixabay

Quelle place pour les IA comme ChatGPT dans l'enseignement supérieur ? IAE France, en partenariat avec l'Aunege et la Fnege, a organisé une série de rencontres thématiques sur le sujet, les 31 mars et 6 avril 2023, pour "évoquer, parler, poser des questions", mais surtout tenter de trancher. Alors même qu'Elon Musk cosigne avec mille autres personnalités de la tech une lettre ouverte alertant sur les avancées rapides des IA et que l'Italie interdit l'utilisation de ChatGPT sur son territoire, l'ESR doit-il considérer cette innovation comme un allié ou un ennemi ?

PLUSIEURS DÉCENNIES D'EXPÉRIMENTATION MAIS UN ENGOUEMENT SANS PRÉCÉDENT

"Depuis le lancement de la version grand publique des intelligences artificielles, on ne peut que constater l'intérêt colossal qu'elles suscitent. Il ne se passe pas un jour sans que ne soit relayée une nouvelle annonce", rappelle Alain Goudey, directeur général adjoint du numérique à Neoma Business school.

"L'outil a été mis à disposition de tout le monde avant que ne soient réglés les aspects juridiques et réglementaires", souligne-t-il, en rappelant qu'un outil comme ChatGPT est loin d'être en règle avec le RGPD. Et qu'il faut faire attention à ce qui est rentré dans l'outil, qui absorbe le contenu des conversations avec lui pour les transformer en données d'apprentissages, comme l'entreprise Samsung en a fait les frais.

UN IMPACT "COLOSSAL" SUR LES MÉTIERS ET LE MARCHÉ DU TRAVAIL

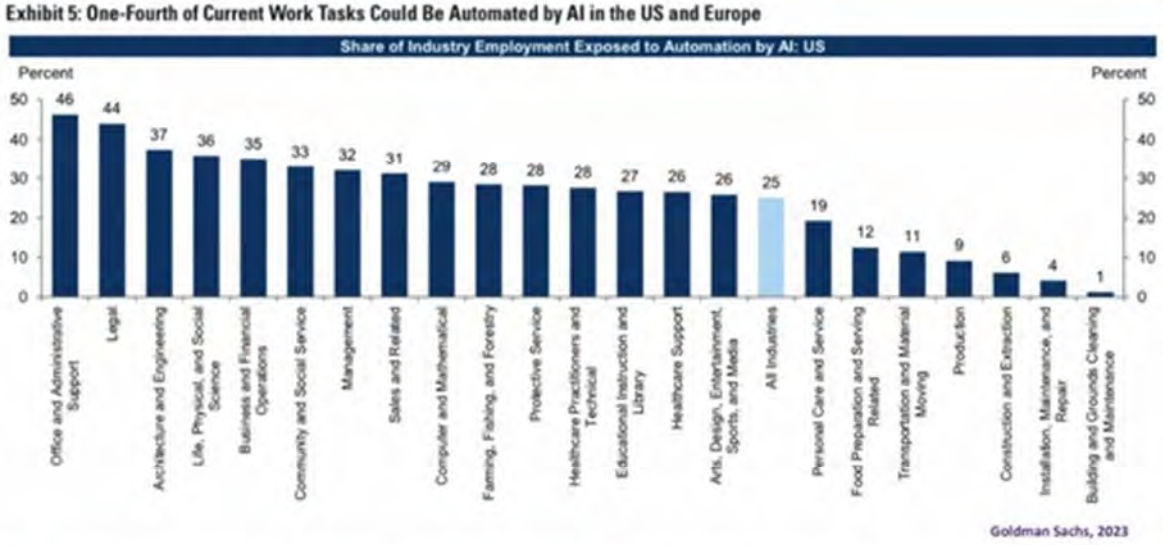
Régis Meissonier, professeur des universités de l'IAE Montpellier, renchérit : "Dans quelque temps, les professeurs seront aidés à créer de manière automatisée des QCM. Actuellement, des enseignants-chercheurs ont déjà recours à ChatGPT comme support. Des articles académiques ont été rédigés avec ChatGPT. Or, si on en interdit l'usage aux étudiants, il faudra également l'interdire aux enseignants." Et "quid de l'apprentissage de manière générale, de l'esprit critique de l'apprenant s'il a tendance à s'en remettre à ce que résume une IA sans s'interroger sur la pertinence des sources ?", s'interroge-t-il.

"Il va y avoir un impact colossal sur les métiers et le marché du travail", alerte Alain Goudey, qui estime que les IA "modifient en profondeur notre manière de chercher l'information, et vont aussi modifier, à terme, la lecture ou le décryptage rapide d'un contenu". Il détaille : "Lorsqu'un professeur réfléchit à la structure de ses cours, il part de zéro. Mais le cerveau humain travaille avec plus de facilité en partant d'un contenu. Les IA pourraient annihiler le syndrome de la page blanche."

Pour lui, il est du rôle des établissements d'apprendre aux étudiants à naviguer au milieu des IA pour déterminer laquelle est plus efficace pour telle tâche, et quelles instructions lui donner. Des compétences qui seront demandées par les entreprises, selon lui.

3 conséquences : impacts sur les métiers / le marché du travail

NEOMA BUSINESS SCHOOL
REIMS · ROUEN · PARIS



Impact des IA génératives sur les métiers par Alain Goudey (Neoma) avec les données de Goldman Sachs | *Droits réservés - DR*

DES IA IMPARFAITES MAIS DE PLUS EN PLUS EFFICACES

Les intelligences artificielles sont loin d'être totalement fiables. Selon Alain Goudey, l'algorithme de ChatGPT – à titre d'exemple – ne fait que construire une réponse "statistiquement cohérente compte tenu de la question initiale", sans réellement comprendre de quoi il s'agit. Le système est soumis à "une forte dépendance" à l'égard du "prompt", c'est-à-dire la consigne donnée à l'outil. Plus problématique dans le cadre de l'apprentissage, lorsque la donnée requise n'existe pas, ChatGPT la remplace par une alternative plausible. Alain Goudey nomme ce phénomène "l'hallucination des intelligences collectives".

Il rappelle tout de même l'amélioration continue et très rapide de la technologie. Ainsi, lors du lancement de ChatGPT-4, Greg Brockman, cofondateur d'OpenIA, a dévoilé les résultats de l'IA générative après avoir passé l'examen du barreau américain : là où GPT-3.5 réussissait à se classer, mais parmi les 10 % les plus faibles, GPT-4 va flirter avec les 10 % de meilleurs classés. "GPT-5 est annoncée pour décembre", rappelle le directeur général adjoint de Neoma.

Bernard Quinio, directeur du service de formation continue de l'université Paris Nanterre, estime que le principal défi consiste finalement à expliquer et intégrer la compréhension des IA aux équipes et aux étudiants : "Si on ne comprend pas comment fonctionnent les outils avec lesquels on travaille, on ne pourra pas les accepter. Il y a deux scénarios. On peut imaginer de jouer aux gendarmes et aux voleurs avec nos étudiants, comme on a pu déjà l'envisager il y a quelques années avec la calculatrice. Ou alors, on part du postulat que ces mêmes étudiants vont travailler avec les IA. Cela demande de reconsidérer complètement l'écosystème : que doit-on apprendre en 2023 ? Doit-on mettre l'accent sur les softs skills, là où l'intelligence artificielle n'est toujours pas capable d'aller ?".

QUEL IMPACT À L'HEURE ACTUELLE ?

De son côté, Emmanuelle Le Nagard, directrice académique du programme grande école de l'Essec, a voulu déterminer, avec un groupe de travail, dans quels contextes les professeurs pourraient être amenés à évaluer l'IA plutôt que l'élève : adapter l'Afest, faire primer les oraux, organiser davantage de mises en situation…

En parallèle, les IA sont aussi présentées comme des atouts précieux : "Un travail qui demande du temps à des étudiants ou à des spécialistes est traité en quelques secondes par ChatGPT", rappelle Régis Meissonier. Emmanuelle Le Nagard liste les divers avantages : outre le gain de temps, l'information peut être mieux synthétisée, ce qui amène parfois à des travaux de meilleure qualité. En s'appuyant sur une base déjà fournie, les étudiants peuvent également développer leur créativité et leur capacité de décision en bénéficiant d'une forme de brainstorming avec l'IA. Enfin, ils développent de nouvelles compétences, en apprenant à utiliser de manière pertinente les IA en prévision de ce qui pourrait leur être demandé dans leurs futures fonctions.

RÉINVENTER LES MODALITÉS D'ÉVALUATION

Emmanuelle Le Nagard soumet également plusieurs propositions pour revoir les modalités d'évaluation. Les examens papier crayons pourraient faire leur retour, et les oraux privilégiés de manière générale, dans la présentation des travaux comme dans les modalités d'évaluation. Alain Goudey encourage aussi à "varier le plus possible les modalités d'examen" : écriture à la main ; QCM ; demander des réponses sous forme de graphiques, images et vidéos ; poser des questions sur un sujet peu développé sur Internet et donc peu présent dans les bases de données absorbées par les IA ; orienter l'examen sur de l'analyse critique ou sur le processus derrière la rédaction d'une réponse… Il prône également le fait d'encourager les étudiants à développer un esprit critique vis-à-vis des IA, par exemple en leur demandant de critiquer une réponse formulée par l'un de ces outils.

L'utilisation même des IA pourrait être considérée de la même manière que le plagiat, avec un seuil de pourcentage toléré et une citation automatique dès lors que l'étudiant s'y réfère, estime Emmanuelle Le Nagard. L'IA serait alors considérée comme une source, à condition de ne pas être unique. Dans le cas où l'usage de ces outils serait toléré, le but serait "d'apprendre aux étudiants à faire mieux avec", estime-t-elle. Elle conclut : "Il faut garder à l'esprit que nous souhaitons voir les étudiants acquérir des compétences et développer leur esprit critique. Nous concentrer sur ChatGPT ne doit pas nous faire perdre de vue les objectifs même de l'enseignement".

MESURER L'ENGAGEMENT AVEC LES LEARNING ANALYTICS

Anne Boyer, enseignante-chercheuse en informatique et en intelligence artificielle à l'université de Lorraine, a également réalisé une présentation sur le "comportement numérique d'apprentissage des élèves". Ainsi, le renforcement de l'usage du numérique dans les apprentissages a profondément modifié le "rapport entre les enseignants et les étudiants". L'analyse de l'engagement et de la motivation en cours des étudiants est plus compliquée à distance qu'en salle de classe ou en amphithéâtre, souligne-t-elle. Une réponse consiste à récolter et analyser les traces numériques des étudiants ("*learning analytics*") pour améliorer derrière l'apprentissage.

La pratique s'est renforcée au fil de la dernière décennie, à tel point qu'il est aujourd'hui possible de "prédire", à partir des traces numériques d'un étudiant (engagement, régularité, réactivité, etc.), s'il a des chances de mener à bien ses études et d'atteindre la diplomation. De quoi modéliser une "dynamique comportementale" avec, derrière, l'objectif de proposer des adaptations et solutions pour l'aider à bien atteindre l'objectif. Elle met cependant en garde : les algorithmes derrière les *learning analytics* "ne captent pas tout", l'attention humaine reste indispensable et il faut également garder en tête qu'un concept de "taille unique" est "inapplicable" : il faut personnaliser les *learning analytics* en fonction des formations et des profils étudiants.

87 % des publications scientifiques de projets financés par l'ANR en accès ouvert en 2022

Le taux d'ouverture des publications scientifiques observées en 2022 issues de projets de recherche financés par l'ANR est de 87 %, soit 20 points supérieur au taux d'ouverture national, de 67 % pour la même année.

Tel est le principal résultat de la déclinaison du Baromètre de la science ouverte faite par l'ANR, première agence de financement française à le faire, annonce celle-ci le 17/04/2023.

Par ailleurs, selon cette déclinaison de l'ANR :
• « de 74 % en 2016, le taux de publications renseignées sur une archive ouverte passe à 82 % en 2021 ;
• la communauté des mathématiques apparaît comme pionnière en matière d'ouverture des publications scientifiques : déjà près de 79 % en 2018, et 94 % en 2022 ;
• la chimie et les sciences humaines connaissent par ailleurs les plus fortes progressions, de 25 % en 2018, les sciences humaines atteignent 76 % en 2022. L'évolution concernant la chimie est de 44 % en 2018 contre 85 % en 2022 ;
• enfin, 26 % des publications en 2021 issues d'un projet financé par l'ANR mentionnent le partage d'un jeu de données, dix points de plus qu'en 2016. »

« Pour sa toute première déclinaison, le baromètre montre un impact manifeste de la politique "science ouverte" mise en place par l'agence, dans les appels à projets, depuis 2019 », estime l'ANR, rappelant que l'objectif du deuxième Plan national pour la science ouverte est « d'atteindre les 100 % d'ici à 2030 pour l'ensemble de la recherche française ».

Méthode

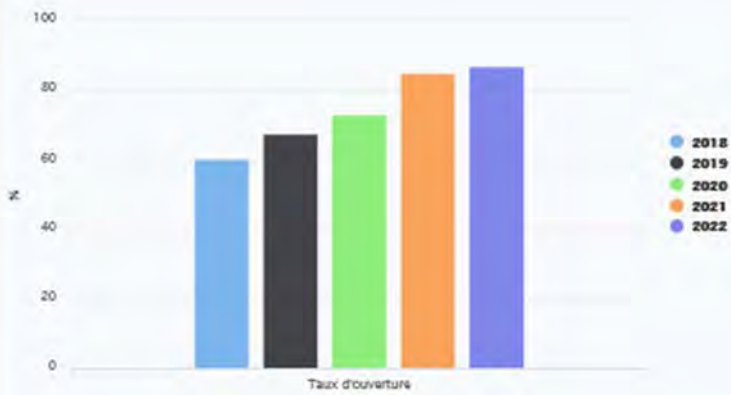
Le Baromètre local de l'ANR s'est construit en collaboration avec l'équipe du Baromètre national du MESR.

Pour ce faire, le pôle « science ouverte » de la Direction de la stratégie numérique et des données de l'ANR a rassemblé un premier corpus de publications scientifiques issues des projets financés de l'appel à projets générique, des programmes d'investissements d'avenir 2, 3 et 4, ainsi que du Plan France 2030 depuis leurs éditions 2016.

Ce corpus est constitué des publications avec DOI (Digital object identifier) rattachées à un code décision ANR disponibles sur la plateforme Web of science et sur le portail HAL-ANR. Il est complété pour l'AAPG par les publications mentionnées dans les rapports finaux des projets. Au total, depuis 2016, ce sont plus de 35 000 publications qui ont été réunies.

Taux d'accès ouvert des publications scientifiques issues des projets financés par l'ANR

Taux d'accès ouvert des publications scientifiques issues des projets financés par l'ANR*

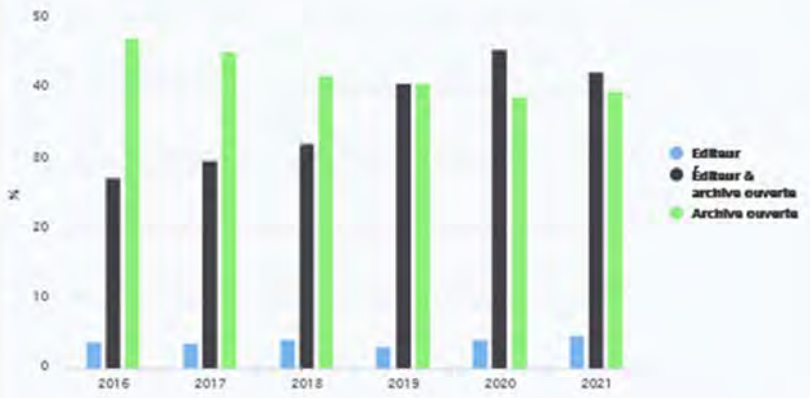


Note : *avec un DOI Crossref, parues durant l'année précédente par année d'observation

Source(s) : *ANR*

Taux d'ouverture par voie d'ouverture

Taux d'ouverture des publications issues des projets financés par l'ANR, par voie d'ouverture*



Note : *avec un DOI Crossref, par voie d'ouverture et par année de publication

Source(s) : *ANR*

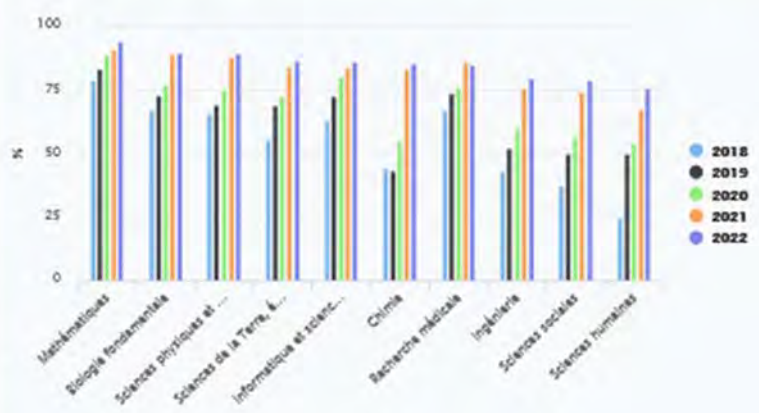
Ce graphique présente la part des publications qui sont disponibles :

- sur une archive ouverte uniquement (vert) ;
- sur le site de l'éditeur uniquement (bleu) ;
- à la fois dans une archive ouverte et sur le site de l'éditeur (noir).

L'ANR note « une généralisation du dépôt des publications scientifiques dans une archive ouverte : depuis 2019, et quelle que soit la voie de publication choisie par les auteurs, le coordinateur ou la coordinatrice et les partenaires des projets financés par l'ANR s'engagent à déposer leurs publications issues des projets financés dans une archive ouverte, puis dans HAL à partir de 2020. Ainsi, de 74 % en 2016, le taux de publications renseignées sur une archive ouverte passe à 82 % en 2021. »

Taux de publications en accès ouvert pour chaque discipline

Taux d'ouverture des publications issues des projets financés par l'ANR, par discipline*



Note : *avec un DOI Crossref

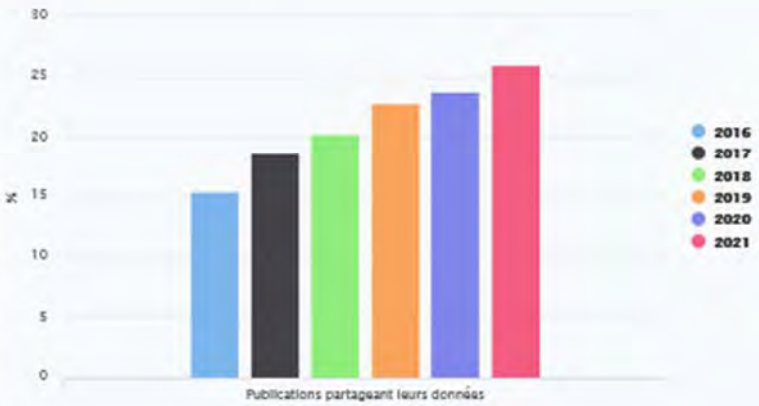
Source(s) : *ANR*

Selon l'ANR, « si on observe une augmentation significative du taux d'accès ouvert pour toutes les disciplines, des disparités apparaissent néanmoins. Ainsi, sur l'ensemble des données observées, la communauté des mathématiques apparaît comme pionnière en matière d'ouverture des publications scientifiques : déjà près de 80 % en 2018, et 94 % en 2022.

La chimie et les sciences humaines et sociales connaissent par ailleurs les plus fortes progressions, de 25 % en 2018, les SHS atteignent 76 % en 2022 ; 44 % pour la chimie en 2018 contre 85 % en 2022. »

Taux de publications partageant leurs données

Proportion de publications issues des projets financés par l'ANR qui mentionnent le partage de leurs données



Source(s) : *ANR*

Ce graphique montre, par année de publication, la proportion de publications pour lesquelles une mention de partage de données a été détectée, parmi les publications qui mentionnent la production de données. Cette détection est réalisée grâce à une analyse automatique du texte intégral par l'outil DataStet.

Ne sont retenues dans le corpus de publications étudié que celles qui mentionnent explicitement des jeux de données. Cette méthodologie, fondée sur la fouille de texte, a été développée dans le cadre du Plan de relance, en partenariat avec l'Université de Lorraine et Inria. Cette approche, qui mobilise les logiciels libres Grobid et DataStet, n'est conduite qu'à partir des publications pour lesquelles le texte intégral a pu être téléchargé dans le cadre du Baromètre.

Ainsi, 26 % des publications en 2021 issues d'un projet financé par l'ANR mentionnent le partage d'un jeu de données, dix points de plus qu'en 2016.

Intelligence artificielle : de quoi parle-t-on vraiment ?

ChatGPT, avatar météo... L'intelligence artificielle fait beaucoup parler d'elle, sans pour autant que l'on en saisisse tous les contours. Qu'est-elle réellement ?

Le système d'intelligence artificielle que nous connaissons aujourd'hui a été inventé par Frank Rosenblatt en 1957 et s'appelait initialement Perceptron. (©Firmbee/Pixabay)

Par Laurène Fertin

Publié le 21 avr. 2023 à 18h57

L'intelligence artificielle. Elle est omniprésente dans l'actualité. Surtout après l'entrée fracassante de Ch

actu.fr a un coût

Le contenu du site actu.fr est le fruit du travail de 400 journalistes professionnels, financé par la publicité. Pour y accéder et soutenir l'information nouvs vous proposons de choisir entre deux options :

1 - Accèder gratuitement au site en acceptant les cookies et la publicité personnalisée.

2- Choisir le service à 2€ par mois pour naviguer sans publicité personnalisée.

J'accepte les cookies et accède gratuitement

OU

Je choisis le service à 2€ par mois

Je me connecte

Grandes Ecoles

5G : l'école d'ingénieurs Mines Nancy, premier campus à avoir son propre réseau

Par AEF info le 22.04.2023 à 11h00
Lecture 3 min.

Mines Nancy (université de Lorraine) a inauguré début avril 2023 son hub 5G industriel. C'est une première en France sur un campus universitaire. Avec son réseau privé, l'école d'ingénieurs entend bien se placer en pole position de l'innovation technologique, sur le plan européen mais aussi international.

La plateforme de réseau privé 5G des Mines Nancy a été fournie par Nokia et installée par son partenaire Snef Télecom (Eiffage Énergie Systèmes).
SOPA IMAGES/SIPA

Une petite révolution a eu lieu à l'école de Mines Nancy, le 4 avril 2023: il s'agit de l'inauguration de la plateforme de réseau privé 5G "Te@chLab5G". Fournie par Nokia, elle permet à l'école d'ingénieurs d'être "le premier campus universitaire en France équipé de la 5G". Qui plus est "de la 5G stand alone, donc de la vraie 5G – avec toutes ses compétences et capacités techniques", s'est félicité Pierre-Gaël Chantereau, PDG de Nokia France, lors de l'événement.

SUR LE MÊME SUJET
- Télécoms: la 5G, réseau révolutionnaire qui "déçoit tout le monde"

"C'est un grand moment, et une évolution d'une école des Mines qui pulse", s'est également réjouit Anne Lauvergeon, ingénieure en chef des Mines et présidente du conseil d'école de Mines Nancy.

Newsletter L'Essentiel

Chaque soir à 18h, notre newsletter L'Essentiel vous offre un condensé de l'actualité du jour vue par Challenges

Votre adresse email

S'INSCRIRE

Newsletter L'Essentiel

Chaque soir à 18h, notre newsletter L'Essentiel vous offre un condensé de l'actualité du jour vue par Challenges

Votre adresse email

S'INSCRIRE

Pour Mines Nancy, ce projet était un indispensable à son développement. "Dans la révolution numérique, il y a différentes facettes: internet des objets, données massives, intelligence artificielle, robotique, etc. Et elles sont toutes reliées par une chose : le réseau", a exposé le directeur général de l'école d'ingénieurs, François Rousseau. "Il nous est très vite apparu que pour le développement de nos activités, nous devions disposer d'un réseau propriétaire, performant, pour la connexion entre les différentes autres briques technologiques sur lesquelles nous nous étions déjà investis."

LIRE AUSSI

Intelligence artificielle : l'offre de formations en France est encore insuffisante

Pour les élèves et l'écosystème du campus

Une dizaine d'années après l'émergence du "TechLab" au sein de l'école, le "choix de la 5G" s'est imposé pour une série de raisons. "La première, c'est pour nos élèves : pour les former sur les technologies de demain [...] avec des opportunités induites dans tous les domaines scientifiques qui sont couverts par les différents

départements de l'école."

"La deuxième raison, c'est pour l'équipement du campus, et le service qu'il apporte aux usagers. C'est un accès à des ressources – des logiciels, des équipements expérimentaux, des machines, et un outil à notre main, qu'on va pouvoir librement paramétrer", ajoute François Rousseau. "Ce que je trouve formidable, c'est que nous puissions stimuler l'intelligence créatrice des élèves, mais également des chercheurs et de tous les industriels de notre écosystème", a abondé Anne Lauvergeon.

LIRE AUSSI Le gotha de l'intelligence artificielle s'expose à Cannes

Un million d'euros d'investissements

Les dépenses liées aux investissements (robot Boston Dynamics Spot, bras robotisé, équipements 5G, drones, plateforme robotique mobile, etc.) et au fonctionnement du Te@chLab5G durant trois ans s'élèvent à un million d'euros. Au-delà du partenariat avec Nokia, qui a fourni une partie du matériel, Mines Nancy a pu disposer de l'appui de sa fondation, ainsi que de l'accompagnement de la collectivité régionale, à hauteur de 412 000 euros.

Pour l'opérateur téléphonique, impliqué dans de nombreux projets "5G" (sur une dizaine de sites industriels, tel qu'Alcatel Submarine Networks), "celui de Nancy est en pole position, non seulement au plan national, mais aussi aux plans européen et international".

"L'an prochain, un tiers des élèves de l'école aura eu accès aux technos 5G à l'école", envisage encore Laurent Cierletta, enseignant-chercheur Mines Nancy/Loria et pilote du Te@chLab5G.

Par Pascaline Marion

A lire en intégralité sur AEF Info

Les Tablettes lorraines, 24 avril 2023

INDUSTRIE 4.0

Mines Nancy, premier campus de France en 5G industrielle

MINES NANCY VIENT D'INAUGURER UNE PLATEFORME DE RÉSEAU PRIVÉ 5G FOURNI PAR NOKIA ET INSTALLÉE PAR SNEF (EIFFAGE ÉNERGIE SYSTÈMES) SUR SON CAMPUS D'ARTEM. NOM DE CODE : LE TE@CHLAB5G. CETTE INFRASTRUCTURE DE POINTE VA PERMETTRE LA FORMATION DES ÉTUDIANTS DE L'ÉCOLE MAIS ÉGALEMENT ÊTRE MIS À DISPOSITION DE L'ÉCOSYSTÈME ENTREPRENEURIAL LOCAL ET RÉGIONAL. MINES NANCY S'AFFICHE AUJOURD'HUI COMME LE PREMIER CAMPUS DE FRANCE ÉQUIPÉ EN 5G, DITE, INDUSTRIELLE.

© Mines Nancy

Avec le Te@chLab5G, Mines Nancy s'affiche comme le premier campus de France équipé en 5G industrielle.

Nom de code : Te@chLab5G. Signe particulier : plateforme d'innovation technologique équipée de la 5G, dite, industrielle installée au cœur du campus Artem de Mines Nancy. Le 4 avril, l'école nancéienne a inauguré ce véritable hub 5G industriel fourni par l'équipementier Nokia (leader de l'innovation technologique pour le marché B2B) et installée par SNEF Telecom (Eiffage Énergie Systèmes). *«Le Te@chLab5G va permettre de renforcer notre engagement en faveur de l'innovation technologique et de la formation d'ingénieurs, capables de répondre aux défis technologiques et environnementaux de la société»*, explique François Rousseau, directeur général de Mines Nancy. *«En tant que première école équipée de la 5G industrielle, Mines Nancy joue un rôle d'acteur neutre en expérimentant et analysant de manière objective les intérêts de cette innovation technologique et en s'assurant qu'elle soit utilisée de manière responsable et durable par nos partenaires.»* Ce hub industriel version 4.0 n'est pas uniquement à l'attention des étudiants de l'école. Il s'affiche comme un mini laboratoire pour l'écosystème entrepreneurial local et régional.

COMPÉTITIVITÉ RÉGIONALE RENFORCÉE

«La plateforme permet également d'accompagner nos partenaires, notamment les ETI et PME de la région Grand Est en leur fournissant des informations, de la formation, des essais, de l'innovation et du transfert technologique, ce qui est particulièrement important pour les entreprises qui n'ont pas les moyens d'accéder à de tels outils», explique-t-on chez Mines Nancy. La plateforme permet d'expérimenter les usages et les applications de la 5G industrielle dans plusieurs domaines à l'image de l'industrie, de la robotique autonome, de la cybersécurité ou encore de la surveillance des sites industriels et militaires. Le Te@chLab prépare à l'utilisation de technologies de rupture dans le domaine du numérique avec trois objectifs principaux. Renforcer la compétitivité régionale : *«en prenant collectivement le virage technologique induit par la puissance de la 5G et bénéficier des effets démultiplicateurs qu'elle permet.»* Former massivement les étudiants et professionnels *«qui accéléreront la révolution numérique de notre société»* et bâtir un écosystème ouvert *«qui connecte compétences universitaires, géants des nouvelles technologies et entreprises locales pour innover et créer à la puissance 5G sur le territoire.»* À l'occasion de l'après-midi d'inauguration de début avril, plusieurs ateliers étaient organisés pour voir les applications de cette technologie. La 5G entend s'afficher comme le socle de l'industrie 4.0. Avec des débits dix fois plus importants, elle affiche une capacité à gérer un grand nombre d'objets et offre une latence (temps de réponse du réseau) divisée par dix. Cette technologie de rupture ouvre tout un champ de développement insoupçonné il y a encore quelques années. Avec son hub en propre, Mines Nancy apparaît avoir plus qu'un temps d'avance. Que du bon pour la compétitivité du territoire et de ses acteurs.

Emmanuel VARRIER

À l'occasion de l'inauguration du Te@chLab5G plusieurs ateliers de démonstrations d'application de la 5G étaient organisés.

«Le Te@chLab5G va permettre de renforcer notre engagement en faveur de l'innovation technologique et de la formation d'ingénieurs, capables de répondre aux défis technologiques et environnementaux de la société», assure François Rousseau, directeur général de Mines Nancy.

5G industrielle : quèsaquo ?

La 5G, tout le monde connaît ! Quelle différence avec la 5G industrielle ? *«L'essentiel de la 5G déployée aujourd'hui repose pour une partie sur une infrastructure 4G, la 5G industrielle est différente de la 5G grand public distribuée par les opérateurs»*, explique-t-on à Mines Nancy. *«La 5G industrielle est conçue pour répondre aux besoins spécifiques des entreprises et des industries et offrir des possibilités de transformation numérique dans de multiples domaines.»*

Challenges
Challenges (site web)
mardi 25 avril 2023 - 16:32 UTC 903 mots

Quand l'armée française joue à la guerre cyber avec des étudiants

Adrien Schwyter

REPORTAGE - Début février, durant plusieurs jours, une centaine d'étudiants de Nancy ont participé à un "wargame" cyber sous l'auspice du Commandement cyberdéfense du ministère des Armées. Le but: susciter des vocations et repérer des talents qui pourraient devenir acteur de la lutte contre la cyberguerre.

"Nous avons pris le contrôle du réseau wifi de l'ambassade, il était peu sécurisé. Une fois dans leur réseau, nous avons hacké l'ordinateur qui gérait le flux vidéo de la caméra de surveillance. Et nous avons pu récupérer pas mal de documents intéressants en faisant sauter le chiffrement au sein de l'ordinateur." Alexandre, le visage masqué par une cagoule, dont on devine les traits tirés, n'est pas là pour rigoler. Pourtant ce mercredi 8 février, l'étudiant en licence pro cyber de l'IUT Nancy-Brabois doit faire gagner son équipe Cryptanga face à Anumérique. Ces deux collectifs s'affrontent déjà depuis plusieurs jours dans ce jeu de rôle en conditions réelles imaginé par le ComCyber (Commandement cyberdéfense du ministère des Armées). Lire aussiComment l'armée prépare la cyberguerre"Nous essayons de coller au maximum à la réalité afin d'être le plus immersif possible, confie Carré d'As*, le capitaine en charge de l'organisation du "wargame". Il faut s'imaginer qu'on est dans l'archipel des Maldives, l'île Rivershell est complètement aux abois financièrement. A cause de la montée du niveau de l'eau, elle ne peut plus profiter du tourisme. Ils ont des ressources minières de lithium importantes, les deux équipes vont devoir remporter la concession minière."Une troisième équipe APT est créé afin de pimenter la situation. Son but étant d'attaquer les deux pays, voire de coopérer contre rémunération avec l'un des acteurs.OIV, darknet et chiffrement au programmePlus de deux cents équipements réels et virtuels ont été mis en place pour l'occasion: une ambassade gardée par un pass sous la surveillance d'une caméra vidéo, un hôpital jouant le rôle d'organisme d'importance vitale (OIV), des automates, des robots, sans oublier un darknet où il est possible d'acheter des logiciels malveillants sur étagère.Tout se déroule en ligne sur des réseaux fermés construits pour l'occasion grâce à deux cyber-ranges de l'Armée, d'imposants serveurs permettant de reproduire un réseau internet totalement hermétique du réseau classique. Signe du degré de réalisme de l'exercice, le ComCyber se sent obligé de préciser qu'aucun "système d'arme n'est mis en jeu, rien de classifié, ni de militaire. Pas besoin d'avoir une arme de pointe pour faire des dégâts en ligne."La centaine d'étudiants qui participent proviennent de six entités: la Faculté des sciences et techniques, l'IUT Nancy-Brabois, les Mines Nancy, Télécom Nancy, et Polytech Nancy. Ils sont répartis dans plusieurs locations physiques dans la ville, afin de compliquer les communications entre les équipes. Chacune dispose de son équipe d'attaque (Red Team), et de la défense (Blue Team), ainsi que son ambassade en terrain hostile.Lire aussiCyberattaques : pourquoi les entreprises françaises sont-elles des cibles ? Au troisième jour de ce wargame, les équipes entrent dans la phase finale. "C'est simple, on envoie tout ce qu'on a en termes d'attaques, résume Julien, capitaine d'Anumériс. Une attaque est en cours sur leur OIV. Le but est également de récupérer des infos, et surtout de le faire savoir. Tout ce qui permet de discréditer l'autre pays va nous servir. Par exemple on a réussi à pirater leur journal, on a créé de fausses publications afin de les diffamer."Fake news et débunkCe qu'oublie de raconter Julien, c'est qu'au cours de la nuit précédente, le compte en banque de son pays s'est fait siphonner par l'équipe adverse. "Pour répondre à leur campagne de fake news en ligne, on a créé un compte dont le but est d'expliquer leur manipulation pour "debunker" tout cela, répond Arthur de l'équipe adverse Cryptanga. On en a profité aussi pour créer plein de faux profils afin de noyer leur opération d'influence."Comme dans un escape game, ou dans tout bon jeu de rôle, les maîtres du jeu sont là pour donner un coup de pouce si les acteurs patinent. "Nous leur donnons des indices lorsqu'ils butent longtemps sur un problème glisse le capitaine Chewbacca. Cette année nous avons mis des documents dans les poubelles, il faut développer leur curiosité. Il faut bien sûr recréer les conditions de fatigues liées à une crise qui dure plusieurs jours, mais le but demeure qu'ils aient la banane à la fin."Lire aussiComment la guerre en Ukraine a remodelé le paysage de la menace cyberOpération de recrutementMême si l'exercice se veut ultra réaliste, en réalité peu importe qui emportera le contrat minier. Le ComCyber de l'Armée française est

surtout là pour susciter des vocations parmi cette centaine d'étudiants, tout en repérant les profils intéressants, afin de venir travailler en son sein. "Cela nous permet de détecter les talents et des compétences rares explique le colonel Eric Koessler, commandant de la base de défense de Nancy. L'idée est de susciter des vocations à servir le pays, voire dans la réserve opérationnelle ou citoyenne."Le ministère espère atteindre 5.200 cybercombattants d'ici 2025 alors qu'ils ne sont aujourd'hui que 3.700. Pour l'anecdote, c'est l'équipe Cryptanga qui a réussi à décrocher le marché minier. Nul doute que les étudiants encagoulés imaginent déjà leur avenir au sein d'opérations qui ressemblent à des jeux d'adultes sous couverture.*Les militaires participant à l'opération n'ont communiqué qu'un pseudo utilisé le temps "wargame".

La robotique dans l'armée de Terre, CoHoMa 2023

Innovation

Direction : Terre / Publié le : 27 avril 2023

Le 10 mai prochain, l'armée de Terre organisera la deuxième édition de la journée de la robotique, sur le camp militaire de Beynes (Yvelines). Initiée en juin 2021, celle-ci a pour objectif de mettre en valeur les réflexions et les projets conduits en matière de robotique. À cette occasion, le challenge de la collaboration entre l'homme et la machine (CoHoMa) sera lancé. Explications.

En 2022, VAB, robots terrestres et drones aériens avaient la mission de reconnaissance. » © Arnaud Woldanski/armée de Terre/Défense

« La rupture robotique s'imagine aujourd'hui afin de construire progressivement la tactique des systèmes automatisés qui assurera à la France la maîtrise du combat aéroterrestre en 2040 »

Le général d'armée Pierre Schill

chef d'état-major de l'armée de Terre.

« La rupture robotique s'imagine aujourd'hui afin de construire progressivement la tactique des systèmes automatisés qui assurera à la France la maîtrise du combat aéroterrestre en 2040 », expose le **général d'armée Pierre Schill**, chef d'état-major de l'armée de Terre. Ainsi, et pour faire face au défi de la robotisation des armées, le ***Battle Lab Terre*** a lancé en 2021 le challenge de la collaboration entre **l'homme et la machine** (CoHoMa). Fort du succès de la première édition, l'armée de Terre relance le défi du 10 mai au 7 juin. Cette année, 15 équipes mettront en situation leurs satellites terrestres ou aériens dans des scénarios tactiques inspirés de situations de combat réellement vécues par les militaires en opérations. Certains éléments, inhérents aux zones de combat, seront simulés par des pièges. Pour cette deuxième édition du challenge **CoHoMa**, le thème retenu est : « *S'emparer d'un objectif* ».

: L'objectif de CoHoMa est de réfléchir à la meilleure synergie homme-machine. - © Arnaud Woldanski/armée de Terre/Défense

Synergie homme-machine

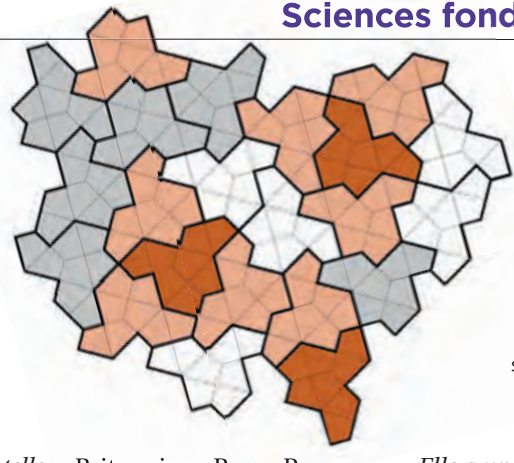
Les équipes intègreront des acteurs de divers milieux (entreprises, start-ups, laboratoires de recherche, établissements de l'enseignement supérieur, etc.) et réfléchiront sur la synergie entre **les hommes** et les **machines**. En 2021, le challenge **CoHoMa** a permis à une quarantaine d'entités issues du monde de l'industrie, de la recherche, de l'enseignement supérieur et du projet Vulcain de préparer la conduite de missions de reconnaissance sur le terrain, par des « unités » constituées d'1 véhicule, d'au moins 2 robots terrestres et d'1 drone aérien. Cette collaboration **homme-machine** s'est exercée au travers d'un challenge au camp de Beynes. Dix équipes composées de petites et grandes entreprises, d'écoles et laboratoires de recherche ont incarné des sections de reconnaissance robotisées et ont été immergées dans un scénario réaliste. Elles ont présenté un minimum de **3 robots et drones** qui ont été essayés sur un parcours parsemé de pièges. Chaque piège, simulant un obstacle (char ennemi ou population civile, par exemple) devait être désactivé pour pouvoir avancer.

Les trois équipes gagnantes de 2021 :

- 1er prix - Squadbot (Arquus, Squadrone System, Angatec),
- 2e prix - Alérion (Alerion, Mines Nancy, TT géomètres experts)
- 3e prix - Polytech Montpellier (Polytech Montpellier).

Une tuile que l'on n'attendait pas

Le domaine d'étude du pavage apériodique s'enrichit d'une pièce unique en son genre.



Ce pavage est constitué d'une seule pièce sans que l'ensemble ne soit répétitif. Un défi mathématique.

D.SMITH, J.MYERS, C.GOODMAN-STRAUSS, C.S. KAPLAN

Une prépublication a mis le monde mathématique en émoi avec la présentation d'une pièce en deux dimensions — comme une pièce de puzzle — qui couvre entièrement le plan, mais sans aucune répétition. « *La plupart des spécialistes du pavage pensaient qu'une telle pièce n'existait pas* », assure Emmanuel Jeandel, professeur à l'université de Lorraine. Jusqu'ici, des pavages dits apériodiques avaient été trouvés, mais soit il fallait plusieurs morceaux — deux dans les pavages découverts par le Britannique Roger Penrose dans les années 1970 —, soit la pièce en question était de plusieurs tenants. Énoncée par un amateur, David Smith, la découverte de cette monotuile apériodique a été certifiée par le National Museum of Mathematics de New York. « *Elle a une forme simple ! Et les auteurs ont aussi fourni quantité de matériel pédagogique, des vidéos et des modèles pour que l'on puisse soi-même tailler cette tuile* », s'enthousiasme Nathalie Aubrun, chercheuse CNRS à l'université Paris-Saclay. **Ph. P.**

On parle de ce qui vous intéresse ?
Juste pour vous proposer des recommandations... qui vous intéressent ;)
Choisir vos catégories préférées

Dimanche en politique - Grand Est

Cyberattaques : la menace invisible

•tv | Politique • 26 min 33 s • Français

indisponible | tous publics

Les attaques informatiques sont de plus en plus nombreuses et représentent un grand danger pour les collectivités, les associations ou les petites entreprises. Certaines ne s'en remettent d'ailleurs jamais. Pour répondre aux cyberattaques dans le Grand Est, la...

En savoir plus

Du même programme

Dimanche en politique - Europe
Europe : un discours et des actes
diffusé le 17/09 | 27 min

Dimanche en politique - Grand Est
Semaine des 4 jours : levier d'attractivité ?
diffusé le 24/09 | 27 min

Dimanche en politique - Grand Est
Loups et éleveurs, une cohabitation difficile
diffusé le 29/10 | 27 min

Dimanche en politique - Grand Est
Vers une Europe plus verte ?
diffusé le 26/11 | 27 min

Les attaques informatiques sont de plus en plus nombreuses et représentent un grand danger pour les collectivités, les associations ou les petites entreprises. Certaines ne s'en remettent d'ailleurs jamais. Pour répondre aux cyberattaques dans le Grand Est, la Région vient de mettre en place une plate-forme destinée à accompagner les victimes et à les guider dans leurs démarches. Comment lutter efficacement contre cette menace souvent invisible ? Quelles leçons en ont tiré ceux qui ont été impactés ? Pour en parler, Lodoïs Gravel recevra ce dimanche : _ Irène Weiss, conseillère régionale déléguée à la cybersécurité _ Jean-Yves Marion, directeur du Laboratoire Lorrain de Recherche en informatique et ses Applications _ Vincent Paul-Petit, ancien dirigeant de Clestra Hauserman _ Frederic Lutz, directeur général adjoint du groupement hospitalier de territoire Coeur Grand Est

La Semaine de Metz, 4 mai 2023

Mardi 9

THIONVILLE

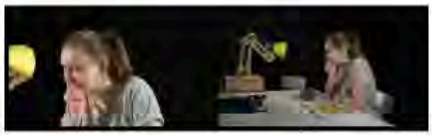
CINÉ-QUIZ À LA SCALA

Des machines intelligentes aux machines pensantes. À travers la redécouverte de films emblématiques de la science-fiction des années 1950 à aujourd'hui, le cinéma La Scala propose de revisiter le lien au cinéma entre l'Homme et les machines, et plus particulièrement les robots, lors de son rendez-vous traditionnel du ciné-quiz. Une rencontre animée par Nicolas Dupuy, docteur en physico-chimie moléculaire à l'Université de Lorraine, et Alain Dutech, chercheur au Loria (Laboration lorrain de recherche en informatique et ses applications).

▶ **À 20 h à La Scala. Gratuit.**

ACTUALITE (AUCUN THEME) / LA QUESTION DU MOIS , INTELLIGENCE , INTELLIGENCE ARTIFICIELLE , ALAIN DUTECH , PSYPHINE

PSYPHINE : REGARDS CROISÉS SUR LES INTELLIGENCES



Qu'ils aient une fonction pratique ou ludique, les objets dotés d'une intelligence artificielle occupent une place de plus en plus importante dans notre quotidien. Qu'en attendons-nous ? Quelles relations entretenons-nous avec eux ? En quoi celles-ci influent-elles sur nos interactions avec les autres ou avec le monde ? Autant de questions auxquelles le groupe Psyphine apporte des éléments de réflexion, sinon de réponses, en croisant approches disciplinaires et pratiques scientifiques.

Bien malin celui qui prétendrait définir avec précision ce qu'est l'intelligence. Si s'impose instinctivement l'idée qu'y parvenir nécessite a minima d'être intelligent, cela ne constitue en rien une condition suffisante. « Je ne sais pas ce qu'est l'intelligence, ni s'il y a une ou des intelligences » constate Alain Dutech, chercheur Inria en intelligence artificielle, spécialisé dans le domaine de l'apprentissage par renforcement au sein du Loria et membre-fondateur du groupe Psyphine. « Je préfère parler de capacités cognitives, de savoir apprendre, mémoriser, faire des rapprochements, des analogies, des raisonnements. Ce sont des marqueurs de l'intelligence mais ça ne la définit pas. » Quant à l'intelligence artificielle, qui fait si souvent la une de l'actualité, Alain Dutech estime que l'appellation relève surtout d'un concept médiatique « sur-vendeur » avant de rappeler, à toutes fins utiles, qu'« une machine comme Chat GPT, aussi efficace soit-elle, ne comprend pas ce qu'elle fait. L'intelligence artificielle est le nom donné à un domaine scientifique dont l'un des objectifs est de comprendre l'intelligence humaine par un moyen propre aux informaticiens. » Comprendre les mécanismes de la cognition en organisant la rencontre entre une intelligence humaine et une intelligence artificielle afin d'analyser les modalités de leur éventuelle interaction, tel est donc l'objectif que s'est fixé Psyphine, groupe pluridisciplinaire créé en 2011 au sein de l'Université de Lorraine.

Des intentions et une vie intérieure

« Pour qu'il y ait une véritable interaction entre deux êtres humains, chacun doit partir du principe que l'autre a, au même titre que lui, des capacités cognitives, qu'il est capable de le comprendre, parce qu'il a des intentions et une vie intérieure » explique Alain Dutech. Que se passe-t-il alors lorsqu'un individu se trouve face à un artefact, un « objet à comportements » visiblement élaboré et construit par un être humain ? Des interactions peuvent-elles s'établir entre eux ? De quelle nature et à quelles conditions ? Des questionnements d'importance à une époque où notre environnement est envahi d'objets connectés dont l'intelligence artificielle suscite, souvent par méconnaissance de ses principes de fonctionnement, autant de fantasmes que d'inquiétudes.
Pour tenter d'y répondre, les membres de Psyphine utilisent comme artefact une sorte de lampe d'architecte motorisée et munie d'une caméra dissimulée dans son abat-jour, animée grâce à un programme informatique qui tient compte des mouvements environnants. « Nous plaçons deux personnes volontaires devant la lampe après leur avoir donné une consigne comme "Essayez de savoir si la lampe est téléguidée par un être humain ou animée par une intelligence artificielle". Mais leur réponse nous intéresse moins que la façon dont ils se comportent, entre eux et vis-à-vis de l'objet, ou les explications qu'ils en donnent. Nous essayons de comprendre si les gens éprouvent de l'empathie pour la lampe, par exemple, ou s'ils lui prêtent de l'intentionnalité. »

Comprendre les logiques d'action

Au cours du temps, les modalités d'organisation de Psyphine n'ont pas cessé d'évoluer. Sous l'impulsion des membres du groupe issus des sciences humaines et sociales en particulier, l'expérience qui était initialement organisée en laboratoire s'est externalisée dans des lieux publics, ou encore le principe d'auto-confrontation a été ajouté. « C'est une méthodologie d'enquête qui vient de l'analyse clinique de l'activité, précise Virginie André, maîtresse de conférences HDR en sciences du langage, spécialisée dans l'analyse sociolinguistique des interactions et membre du laboratoire ATILF. Elle consiste à filmer des personnes qui exécutent une tâche puis à leur présenter les images en leur demandant de commenter les gestes qu'ils ont fait. Cela permet de mieux comprendre les logiques d'actions des participants et de limiter les risques de surinterprétation. » Groupe à géométrie variable, Psyphine s'est voulu dès sa création multidisciplinaire. Il compte actuellement dans ses rangs trois informaticiens d'Inria et du Loria, un psychologue, deux linguistes, un neuroscientifique, deux philosophes et un anthropologue. Si chacune des disciplines représentées participe à l'évolution du protocole expérimental en apportant ses spécificités méthodologiques, elles interviennent de la même manière dans l'analyse des données et, au-delà, s'enrichissent en retour des confrontations qui en résultent. « Les réflexions que nous menons collectivement réinterrogent nos disciplines, témoigne Virginie André. Nous ne sommes pas toujours d'accord, parce que nous avons chacun nos définitions, ne serait-ce que sur la notion d'interaction, mais ce qui est intéressant justement c'est de devoir expliciter les termes afin de trouver un vocabulaire partagé. »

Une approche transdisciplinaire

« Le sujet d'étude de Psyphine n'est plus seulement l'interaction homme-machine, ses conséquences sur la cognition et ce que ça dit de l'intelligence, ajoute Alain Dutech, mais aussi l'intérêt d'une organisation pluridisciplinaire, quelles difficultés cela implique et quels avantages il est possible d'en retirer. » Il s'agit bien d'une approche transdisciplinaire dans laquelle les hypothèses ou savoirs ne sont plus simplement juxtaposés mais intimement mêlés, pour apporter autant de réponses qu'ils appellent de nouvelles questions. Ce que d'aucun appelle : apprendre en marchant.

Et Psyphine compte bien marcher longtemps. « Nous ne manquons pas d'idées ni d'envies. Nous avons fait construire une autre version de notre lampe articulée, avec les mêmes capacités mais une apparence plus design pour voir si cela influe sur la réaction des sujets. Nous avons également ajouté des leds qui peuvent changer de couleurs et réfléchissons à l'opportunité d'installer des micros pour que l'algorithme intègre les sons. »

Les résultats de ces recherches, Psyphine les partage sur son site internet, dans ses publications ou encore lors de rencontres et conférences. La prochaine, baptisée Drôles d'objets : un nouvel art de faire, se tiendra à Nancy du 15 au 17 mai 2023. « Nous avons organisé la manifestation, dont le format est celui des rencontres scientifiques construites sur des appels à contributions, autour de tables rondes pendant lesquelles diverses disciplines échangeront sur une thématique donnée, annonce Alain Dutech. Il y aura aussi une conférence orientée vers un public plus large au Muséum-Aquarium de Nancy, des ateliers et des expositions. Nous nous adressons plutôt aux chercheurs et enseignants- chercheurs mais c'est ouvert à tous sur simple inscription. » Partager, échanger, s'ouvrir à la diversité et à l'imprévu pour tenter de bâtir un tout supérieur à la somme des parties. Ça pourrait être ça, l'intelligence.

« Ce qui est assez constant dans l'interaction humain-robot, c'est que la machine crée une tension entre les doutes et les croyances que les gens ont à propos de son fonctionnement. C'est une notion importante dans la théorie anthropologique de l'action rituelle et de la pensée symbolique. Quand nous avons affaire à un objet réputé intelligent, comme notre lampe articulée, nous avons des soupçons sur ce qui l'anime et sommes prêts, même temporairement, à le doter d'une intériorité, d'intentions, d'un pouvoir d'agir. Les expériences de Psyphine apportent des éléments pour mieux comprendre ce type de relations. »
Joffrey Becker, docteur en anthropologie sociale et en ethnologie

Auteur de l'article, Olivier Pion, agence Kogito

En savoir plus :

- Site web de Psyphine
- La conférence « Drôles d'objets : un nouvel art de faire » à Nancy du 15 au 17 mai 2023
- L'ouvrage *Que prêtons-nous aux machines ? Approches interdisciplinaires des interactions homme-robot* sous la coordination éditoriale du collectif Psyphine aux Presses Universitaires de Nancy

Crédit photos : ©Joffrey Becker, ©Psyphine

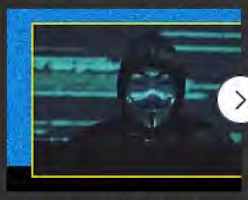
Cyberattaques, un danger bien réel

Voir tout

Cybercriminalité, des attaques bien réelles

Qu'est-ce que le cybergrooming ?

Le dessous des cartes - L'essentiel
Ukraine-Russie : Poutine et la guerre du cyber



Les hackeurs de Zelensky
Bénéfices et risques de cyber-

Cybercriminalité, des attaques bien réelles

♡ Ajouter

52 min | Disponible jusqu'au 31/10/2026 | VF VO

Sciences | Technologies et innovations | Documentaires et reportages

Alors que les hackeurs parviennent aujourd'hui à s'attaquer aux plus grandes institutions, comment garantir la sécurité dans le cyberespace ? Un état des lieux de la menace et des solutions déployées pour la contrer.

À l'instar des personnes privées, les banques, les gouvernements et des organisations internationales comme l'Otan sont les cibles d'un nombre croissant de cyberattaques. En France et en Allemagne, les entreprises et institutions publiques font l'objet de tentatives de piratage en moyenne 670 fois par semaine. Fabian Osmond, président de la société française de sécurité Cybi, a développé une solution spécialisée dans la recherche des failles numériques. Son logiciel Scuba permet d'identifier les chemins d'accès potentiellement utilisables par les hackeurs. Outre-Rhin, le Computer Emergency Response Team (CERT) surveille vingt-quatre heures sur vingt-quatre les flux de données de l'Allemagne, et protège notamment le gouvernement fédéral depuis le piratage du Bundestag en 2015.

Enjeu crucial

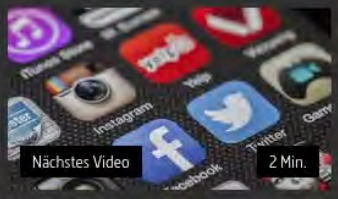
Entre manipulations et technologies de pointe, ce documentaire détaille les méthodes des hackeurs et montre comment chercheurs, informaticiens et enquêteurs tentent de les neutraliser afin de rendre le cyberespace plus sûr et de garantir la sécurité informatique des États.

Réalisation	Carolin Riethmüller
Production	Gruppe 5
Pays	Allemagne
Année	2023

Die unsichtbare Gefahr der Cyberangriffe

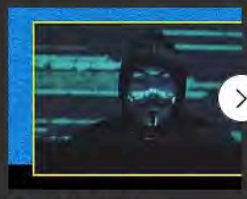
Mehr >

Der unsichtbare Krieg
Angriff aus dem Netz



Was ist Cybergrooming?

Mit offenen Karten - Im Fokus
Krieg in der Ukraine: Putins Cyberkrieg



Selenskyjs Hacker
Nutzen und Schaden von Cybe

Der unsichtbare Krieg

Angriff aus dem Netz

♡ Hinzufügen

52 Min. | Verfügbar bis zum 31/10/2026 |

Wissenschaft | Technik und Innovation | Dokus und Reportagen

Regierungen, Privatpersonen, Firmen, Banken – und sogar die NATO – werden zunehmend Opfer von Cyberangriffen. Cyberkriminalität verursacht global dreimal so viel wirtschaftlichen Schaden wie Naturkatastrophen. Die Angreifer sind häufig einzelne Menschen oder kleine Gruppen. Wie viel Macht sie haben und welchen Schaden sie anrichten können, erzählt diese Doku.

Die Dokumentation begleitet Fabian Osmond von der französischen Sicherheitsfirma Cybi, der mit seinen Kollegen eine Software entwickelt hat, die darauf spezialisiert ist, digitale Schlupflöcher zu finden. Innerhalb von zehn Minuten soll sie die Schwachstellen ausfindig machen. Doch die Hacker werden immer geschickter. Sie spähen Systeme eine Weile aus, bevor sie angreifen. Und in Zukunft könnte diese Gefahr noch größer werden – durch KI. Ein Algorithmus designt die perfekte E-Mail, auf die wir in jedem Fall klicken werden. Wie gefährlich die Angriffe von Hackern sein können, zeigen die Attacken auf den Bundestag, die NATO und Kommunalverwaltungen: Hacker haben die Macht, den Staat außer Gefecht zu setzen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Aufgabe, Deutschlands IT-Sicherheit zu gewährleisten. Die Dokumentation begleitet eine Übung des BSI-eigenen Computer Emergency Response Teams, kurz CERT-Bund, bei der der Hack eines Unternehmens simuliert wird. Im Nationalen IT-Lagezentrum des BSI laufen alle Informationen zur Lage der Cyber-Sicherheit in Deutschland zusammen. Das BSI schützt die Bundesregierung und unterstützt seit 2015 auch den Bundestag bei seiner IT-Sicherheit. Für die Übung sollen die Cyber-Sicherheitsexperten herausfinden, welche Sicherheitslücke im Unternehmen den Hack ermöglicht hat.
Die Dokumentation stellt dar, wie mächtig Hacker mittlerweile sind, welche Manipulationsmethoden sie nutzen, und wie sie die Versorgung und Sicherheit bedrohen – er zeigt auf, wie sich Forschende, IT-Spezialisten und Ermittler jeden Tag aufs Neue ins Zeug legen, um den Cyberraum zu einem sicheren Ort zu machen.

Regie	Carolin Riethmüller
Produktion	Gruppe 5
Land	Deutschland
Jahr	2023
Herkunft	ZDF

Paul Zimmermann : « Nous n'aurions pas pu déchiffrer cette lettre sans l'aide d'une historienne »

09.05.2023 | 5 MINS

En 2022, trois informaticiens et une historienne ont déchiffré une lettre écrite en 1547 par Charles Quint. Une découverte qui souligne l'importance de l'interdisciplinarité dans la recherche. Paul Zimmermann, docteur en informatique était de l'aventure menée par une équipe de chercheurs d'Inria, du Loria et de l'université de Picardie Jules Verne.

Cet article a été réalisé dans le cadre d'un partenariat avec l'Inria.

Lecture. 5 mins
Publié le 09/05/2023

Un article écrit par
Lec'hvien Julien
Journaliste

Bientôt à l'écoute

Comment vous êtes-vous retrouvé à travailler sur une lettre rédigée par Charles Quint à l'ambassadeur de France ?

Je suis arrivé sur ce projet en cours de route. À l'origine, c'est ma collègue Cécile Pierrot, également chercheuse à l'Inria, qui a entendu parler de cette lettre chiffrée et qui a fini par la localiser dans la bibliothèque Stanislas, à Nancy.

Elle ressemble à une copie double repliée, avec trois pages de texte chiffrées, et est signée par Charles Quint. La déchiffrer a été plus compliqué que prévu et Pierrick Gaudry, chercheur en informatique au CNRS et moi-même, avons

prête main forte au projet. Mais, au bout de six mois, nous étions toujours bloqués sur ce texte vieux de près de 500 ans.

Comment avez-vous débloqué la situation ?

Nous avons fait appel à Camille Desenclos, une historienne spécialiste de la cryptographie de l'époque de Charles Quint. Elle a trouvé d'autres lettres rédigées par Jean de Saint-Mauris, ambassadeur de Charles Quint en France, destinataire de la lettre cryptée.

Par bonheur, ces lettres étaient chiffrées avec le même système et comportaient parfois dans leurs marges des morceaux décodés du texte. En faisant correspondre le texte chiffré et le texte en clair, nous avons pu reconstituer la clé de chiffrement de la fameuse lettre de Charles Quint.

> **On n'aurait pas pu comprendre le sens de la lettre sans l'aide d'une historienne.**
>
> Paul Zimmermann, docteur en informatique

Quelle importance revêt le contenu de cette lettre d'un point de vue historique ?

Au fur et à mesure du déchiffrement, cette lettre a révélé des faits inédits. Elle a donné des détails sur la guerre qui opposait Charles Quint à François Ier et qui stagnait du côté du Piémont, en Italie, mais également sur des conflits internes à l'Empire.

Surtout, il y est question d'une rumeur d'assassinat, fomenté par un certain Pierre Strozzi avec l'aval du roi de France, à l'encontre de Charles Quint. C'est la première fois que les historiens en entendent parler.

Par quoi le déchiffrement a-t-il été rendu difficile ?

Même si les techniques de cryptographie du XVIe siècle étaient plus rudimentaires qu'aujourd'hui, elles n'en demeuraient pas moins astucieuses. Nous avons dénombré 120 symboles dans la missive, alors que l'alphabet français compte 26 lettres : chaque lettre peut donc être codée par deux à quatre symboles différents.

Cette technique empêche de comparer la fréquence de certaines lettres – par exemple la lettre e apparaît en moyenne dans un caractère sur six en français – avec celle des symboles de la lettre cryptée. Une autre astuce nous a également bloqués. Des symboles complexes composés d'un caractère et d'un point servaient à coder une consonne suivie d'une voyelle : résultat, les voyelles étaient cachées dans le texte.

En quoi l'interdisciplinarité vous a-t-elle aidé dans vos découvertes ?

On n'aurait pas pu comprendre le sens de la lettre sans l'aide d'une historienne. Nous trois, les informaticiens, nous testions nos hypothèses à l'aide de petits programmes en langage Python grâce auxquels on tentait de retrouver la signification de chaque symbole. Mais nous avions souvent besoin d'aide pour les interpréter.

Par exemple, une phrase indiquait la mort d'un roi. La lettre est datée de février 1546, or il n'y a aucun roi mort à cette date. Finalement Camille Desenclos a trouvé la solution grâce à ses connaissances historiques : à cette époque, le calendrier commençait à Pâques, donc, dans notre calendrier actuel la lettre est bien de 1547. Et effectivement, le roi d'Angleterre venait de mourir à cette date. Le pur déchiffrement informatique ne permettait pas de bien comprendre les détails de la lettre. Cela donne envie de continuer à travailler sur d'autres projets multidisciplinaires.

La clé de chiffrement que vous avez mise à jour vous a-t-elle permis de déchiffrer d'autres textes historiques ?

Cette clé de chiffrement est liée à Jean de Saint-Mauris. On s'est rendu compte qu'il l'a utilisée pour écrire à six personnes différentes sur une durée de quatre ans. C'est amusant car c'est une pratique qu'on ne recommanderait pas aujourd'hui. Elle est contraire aux standards actuels.

Qu'est-ce que ces standards préconisent ?

Dans le système RSA, utilisé actuellement, on recommande d'utiliser des clés de chiffrement de 2048 bits, c'est-à-dire une suite de 2048 « 0 » ou « 1 ». C'est assez robuste pour une durée de cinq à dix ans suivant l'usage que l'on veut en faire. Au-delà de cette durée, les techniques cryptographiques évoluent trop vite pour garantir que la clé de chiffrement ne sera pas craquée.

Mais il existe un autre champ de recherche, la cryptographie post quantique, dont les résultats devraient permettre aux algorithmes de cryptage de résister à la puissance de calcul d'un ordinateur quantique (un ordinateur quantique est capable de réaliser des calculs hors de portée d'un ordinateur classique, N.D.L.R.).

Cet article a été réalisé dans le cadre d'un partenariat avec l'Inria.

Intelligence artificielle : la cybersécurité assurée par Scuba un nouvel outil testé par une start-up

Scuba, une technologie pour lutter cotnre les cyberattaques ● © Pixabay

Écrit par **Malika Boudiba**

Publié le 10/05/2023 à 07h30

L'intelligence artificielle pour contrer les cyberattaques, c'est déjà une réalité avec un outil nomé Scuba, développé par une start-up de Nancy, Cybi. C'est le fruit du travail d'une équipe de scientifiques du Laboratoire Lorrain de Recherche en Informatique et ses Applications (Loria - CNRS/Inria/Université de Lorraine)

On parle beaucoup ces derniers temps de l'intelligence artificielle et des nouveaux dangers qu'elle représente. Les cybercriminels amateurs ou confirmés ont déjà compris son intérêt. Mais, elle peut aussi servir à contrer les cyberattaques. C'est tout le savoir-faire de Scuba, un logiciel développé à Nancy en Meurthe-et-Moselle, d'abord par l'Université de Lorraine et ses chercheurs au Laboratoire Lorrain de Recherche en Informatique et ses Applications (LORIA CNRS). Une recherche qui a donné naissance à une société, Cybi, en mai 2022.

Dans une entreprise, comme d'ailleurs chez les particuliers, on trouve des vulnérabilités des systèmes informatiques dans nombre d'ordinateurs, mais aussi dans ces objets auxquels on ne pense pas, les objets connectés. Un réseau de caméras de surveillance, des automates industriels, un tableau connecté ou même une machine à café connectée, tout ce qui est relié aux réseaux internet est susceptible de présenter une vulnérabilité. Il s'agit d'une porte ouverte par laquelle les assaillants vont se glisser sans difficulté.

Le travail de Scuba consiste à détecter les vulnérabilités de chaque équipement dans le système d'information de l'entreprise. "*Notre objectif est de faire de la sécurité proactive. Scuba est Capable d'identifier et de prédire tous les schémas d'attaque potentiels*, nous explique Abdelkader Lahmadi, maître de conférences à l'Université de Lorraine, membre de l'équipe RESIST (LORIA/INRIA) et conseiller scientifique de Cybi.

La start-up @CYBI_CYBER , fruit de recherches menées au @labo_Loria , établit, avec Scuba, les failles les plus à risques et les plus importantes pour les besoins des clients

@INS2I_CNRS @CNRS

11:05 AM · Apr 9, 2023

10 Reply Copy link to post

Read more on X

"*On est capable de dire et de prédire quels seront les chemins empruntés par les attaquants pour atteindre le système. L'entreprise pourra corriger ses vulnérabilités qui ne sont pas forcément les plus critiques ou les plus évidentes.*"

"*Scuba va détecter les points de convergence*", explique Fabian Osmond, PDG de Cybi dans un documentaire d'Arte. "*Il va vous dire comment les traiter par ordre de priorité. Il va aussi casser les chemins d'attaque. L'objectif est d'empêcher l'intrusion.*"

Cette technologie a été brevetée en 2020. Grâce à l'intelligence artificielle, l'outil est capable d'analyser rapidement des quantités de données importantes et ainsi de détecter des chaînes d'attaques potentielles. "*La technologie utilise de l'apprentissage automatique. Notre moteur d'IA apprend les causes et les conséquences de chaque attaque analysée. Ces analyses permettent de construire une échelle des vulnérabilités. Ce qui met en évidence tous les chemins d'attaque possibles*" L'équipe de scientifiques du LORIA a testé Scuba sur la chaîne d'attaques d'un redoutable logiciel malveillant, Pégasus. "*On a vite trouvé les trois vulnérabilités connues aujourd'hui. Mais surprise, Scuba a détecté des variants. Ils exploitent les mêmes vulnérabilités, mais d'une autre façon.*"

ANSSI
@ANSSI_FR · Follow

[#Cybersécurité]
📝L'@ANSSI_FR publie son rapport d'activité 2022 : une année dense pour assurer une résilience #cyber de premier plan.
#SSI #ANSSI

Plus d'informations👇
ssi.gouv.fr/actualite/le-r...

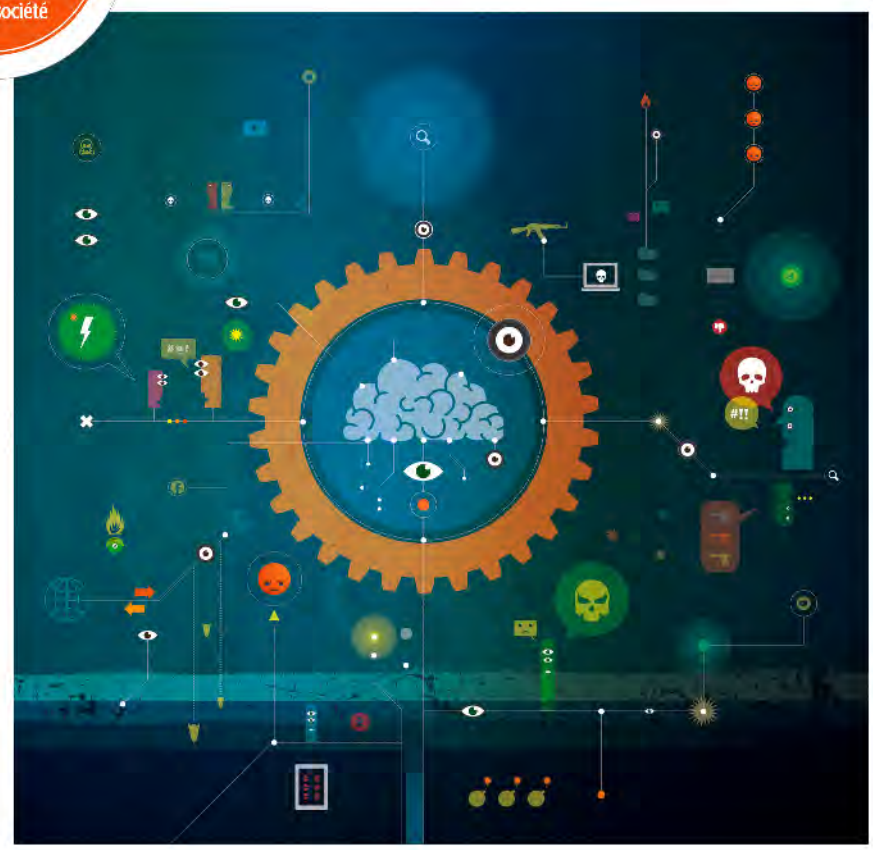
L'interface fonctionne déjà en anglais et en français. Elle devrait être bientôt opérationnelle en allemand, en italien et en espagnol. Elle est actuellement testée par une vingtaine de clients.

D'après un document de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), en 2022, les cibles privilégiées des cyberattaques restent les PME PMI, les collectivités et les établissements de santé.

Il était une science

Transition numérique de l'industrie et de la société

M-PHASIS : UN PROJET DE RECHERCHE POUR LUTTER CONTRE LES DISCOURS DE HAINE SUR INTERNET



Dans le cadre du programme OLKi porté par Lorraine Université d'Excellence, les chercheuses Angeliki Monnier et Irina Illina ont conjugué leurs disciplines, les sciences de l'information et de la communication et les sciences informatiques, pour mieux traquer les discours de haine sur les réseaux sociaux. Ce projet franco-allemand nommé M-PHASIS a permis des avancées.

« Ce programme de recherche consacré aux discours de haine en ligne envers les migrants a fait l'objet de nombreuses publications et présentations dans des conférences d'envergure internationale. Deux thèses ont également été soutenues. La mise à disposition de toute la communauté de chercheurs qui travaillent sur ce sujet, d'un corpus et de logiciels open-access est également un grand motif de satisfaction », explique Irina Illina, maîtresse de conférences à l'IUT Nancy Charlemagne et chercheuse dans l'équipe Multispeech du Loria (CNRS, Inria, Université de Lorraine) à propos du projet franco-allemand M-PHASIS. Financé par l'Agence nationale de la recherche (ANR) et son homologue allemand la Deutsche Forschungsgemeinschaft (DFG), il s'inscrit dans un programme plus ambitieux encore intitulé OLKi (Open Language and Knowledge for citizens), porté par Lorraine Université d'Excellence et dédié à l'ingénierie des langues et des connaissances. L'originalité de M-PHASIS (Migration and Patterns of Hate Speech in Social Media) est qu'il se nourrit à la fois de sciences de l'information et de la communication et de sciences informatiques, en France et en Allemagne réunissant l'Université de Lorraine ainsi que l'université de Mayence et celle de la Sarre. Chercheuse en informatique, Irina Illina a notamment travaillé en étroite collaboration avec Angeliki Monnier, directrice du CREM (Centre de recherche sur les médiations) qui est professeure en sciences de l'information et de la communication à l'Université de Lorraine. Elle travaille entre autres, sur les appropriations et usages collectifs des médias et sur les environnements informationnels en ligne.

Des milliers de commentaires en ligne annotés

Dans un premier temps, l'équipe a réfléchi à la manière de collecter les données. Un travail épistémologique a été mené afin de définir le discours de haine, sur le plan syntaxique ou lexical, par exemple. *« La priorité a ensuite consisté à collecter des données sur les réseaux, autrement dit à récolter des messages de haine en sachant que pour M-PHASIS, nous nous sommes focalisés sur les messages écrits. Plus de 10 000 commentaires ont ainsi été recensés sur des médias sociaux comme Twitter et sur des sites de journaux. Et cela en France comme en Allemagne, avec une approche cross-culturelle, ce qui a d'ailleurs mis en lumière des différences entre les deux pays. Les Français sont beaucoup plus friands de Twitter que les Allemands, par exemple, ce qui fait qu'en Allemagne ce réseau social colporte bien moins de messages de haine »*, explique Irina Illina. Cet exercice de collecte est déjà une gageure en soi. D'une part, car il importe de prendre en considération la réglementation sur le respect de la vie privée. D'autre part, car en Europe, les plates-formes ont l'obligation légale de supprimer de tels messages dans les 24 heures qui suivent leur mise en ligne. Il a fallu ensuite annoter ce corpus. *« Nous avons défini un protocole d'annotation comprenant une centaine de questions. C'est ce qui nous a permis d'obtenir des résultats d'une très grande finesse, un modèle plus performant capable de mieux cerner les discours de haine implicites, par définition plus difficiles à saisir que ceux qui sont explicites et identifiables avec des mots-clés, notamment »*, résume la chercheuse. Ce sont ce corpus et l'outil informatique développé, appelé HUMAN (Hierarchical Universal Modular Annotator), qui sont désormais partagés avec la communauté scientifique et participent, à ce titre, à faire avancer la lutte contre les discours de haine sur internet, au bénéfice de toute la société. Bien entendu, les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) qui mènent aussi des recherches en la matière, ont accès à ces travaux.

> **Plus de 10 000 commentaires recensés sur des médias sociaux comme Twitter et sur des sites de journaux**

Vers de nouvelles recherches

Après quatre ans de recherche, le programme M-PHASIS s'est terminé en août dernier. La fructueuse collaboration entre Irina Illina et Angeliki Monnier, ainsi qu'entre leurs équipes respectives, se poursuit néanmoins. Car les résultats sont probants et le rapprochement des disciplines a été une réelle source d'enrichissement, du point de vue scientifique comme humain même s'il a fallu composer avec la crise sanitaire. Mais aussi parce que la haine ne manque pas de créativité pour diffuser ses messages. *« Nous aimerions à présent élargir nos recherches, via une approche multimodale alliant texte et signal audio (par exemple, sur Youtube utiliser la bande son d'une vidéo et le texte de commentaires). Un projet a d'ores et déjà été déposé en ce sens, toujours dans le cadre du programme OLKi »*, confie Irina Illina.

Les discours de haine se propagent

Selon un rapport de l'Unesco, 80 % des personnes ont été confrontées à des discours haineux (DH) en ligne et 40 % se sont senties attaquées ou menacées via des sites de réseaux sociaux dans l'Union Européenne. Les Nations Unies définissent le DH comme *« tout type de communication par la parole, l'écriture ou le comportement, qui dénigre une personne ou un groupe en fonction de ce qu'il est, c'est-à-dire en fonction de sa religion, de son ethnie, de sa nationalité, ou d'un autre facteur d'identité »*.

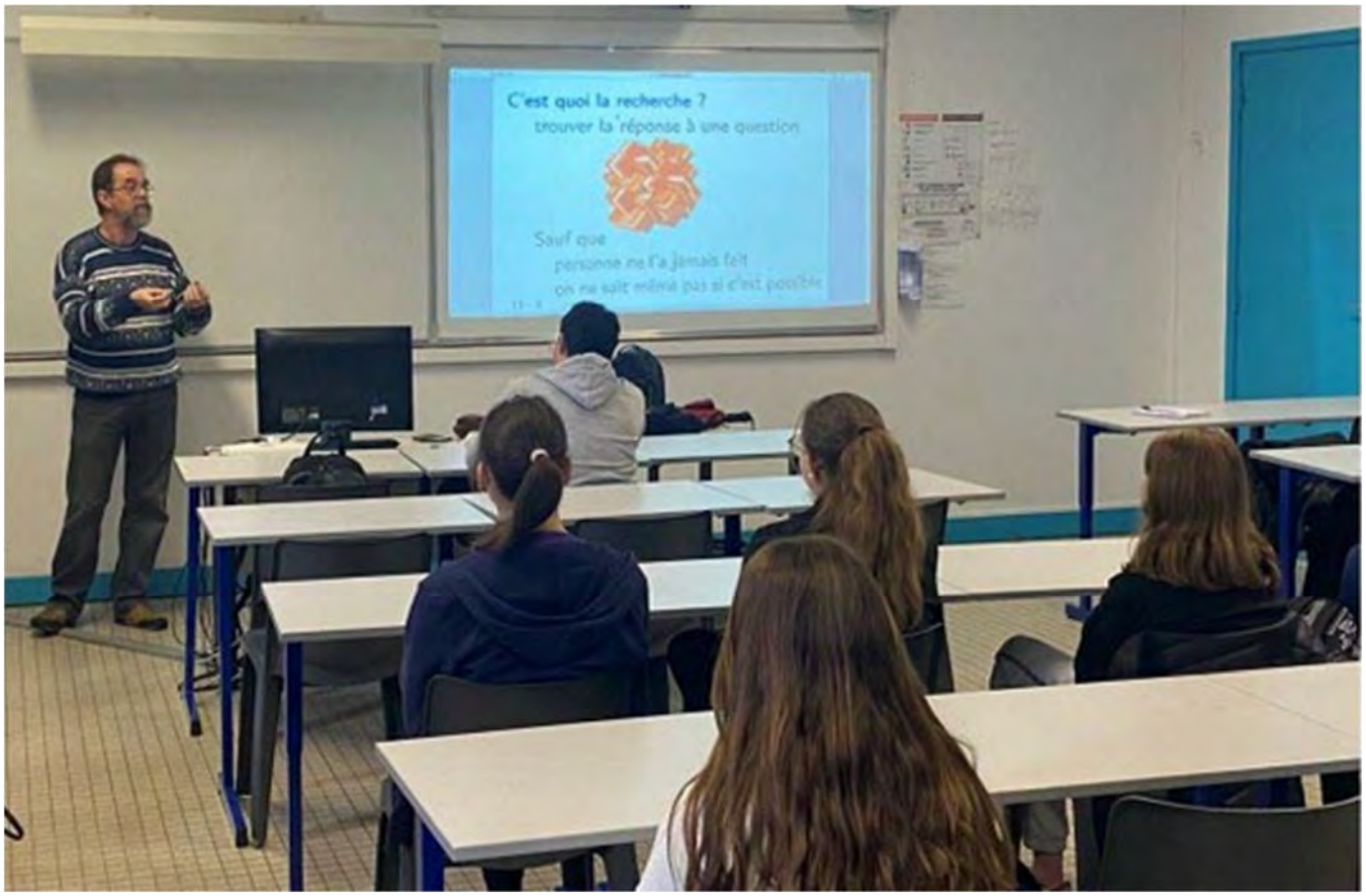
L’Est républicain, 12 mai 2023 (édition Meuse) (1/2)

Bar-le-Duc

Un directeur de recherche au lycée Poincaré pour présenter son métier

Le directeur de recherche de l’INRIA à Nancy, Olivier Devillers, a dissipé le brouillard autour du milieu scientifique en présentant à la fois son métier et son quotidien. Cette rencontre a pu être possible grâce à l’initiative « un scientifique, une classe : Chiche », portée par des professionnels du secteur désireux de faire connaître la profession hélas stéréotypée.

Noé KOLANEK



Le directeur de recherche de l’INRIA à Nancy, Olivier Devillers, a exposé son métier avant de s’adonner à une session de questions-réponses avec les élèves. Photo ER /Noé KOLANEK

Seulement 618 000 personnes travaillent dans le milieu de la recherche en France, soit à peine 2 % de sa population active.

Dans le souhait d’inverser la vapeur et d’apporter de la visibilité à cette profession peu attractive, le directeur de recherche de l’INRIA à Nancy, Olivier Devillers, s’est rendu ce jeudi 11 mai au lycée Poincaré de Bar-le-Duc avec, en ligne de mire, le projet de présenter à cinq classes de Seconde ce que peut être un métier scientifique, en prenant son cas comme exemple.

« Mon quotidien s’applique à résoudre un problème qu’on nous a donné », se met à décrire l’auteur d’une thèse sur la synthèse d’images auprès d’une quinzaine d’élèves et d’une poignée de professeurs. Sa présence a été rendue possible grâce à l’initiative « un scientifique, une classe : Chiche » sensibilisant les plus jeunes au secteur d’activité.

L’Est républicain, 12 mai 2023 (édition Meuse) (2/2)

« Déconstruire les stéréotypes »

Vraisemblablement, les adolescents ne sont pas emballés. Mais la bonne humeur et les blagues du scientifique incitent la classe a posé timidement des questions suite à sa présentation. « Comment fait-on pour trouver un problème ? […] De quoi parle votre thèse ? […] Qu’est-ce qui vous a attiré dans ce métier ? »

C’est par ce prisme que le présentateur peut aller à l’encontre des préjugés inhérents à son métier, a fortiori l’informatique dont il est un spécialiste. « Je suis là pour déconstruire les stéréotypes ». Puis, « la réforme [Blancher] les a renforcés, les filles se sont moins destinées aux mathématiques en raison de ça, ce qui contribue au manque de la représentation féminine ». Propos auquel la professeure de mathématiques Christine Leclercq accorde sa guitare. « On fait de la programmation en utilisant Python (un langage informatique). Je remarque que les garçons aiment plus ça que les filles ».

Endiguer ces idées reçues et favoriser la démocratisation de la profession s’avèrent pour ces raisons un cheval de bataille d’Olivier Devilliers et de tout le microcosme s’adonnant à la recherche. Il précise qu’à ce jour, « seulement 20 % des collègues [qu’il a] côtoyés étaient des femmes ».

Égalité, Fraternité, Agissez ! Le numérique, pour le meilleur et contre le pire

17 mai 2023 - 05:00 par La rédaction Infodujour

À l'occasion de la 16ème édition des rencontres départementales de lutte contre les discriminations « Égalité, Fraternité, Agissez ! » (EFA), le Conseil départemental de Meurthe-et-Moselle et ses partenaires ont choisi de mettre en débat la question du numérique, dans tous ses aspects.

Cette manifestation populaire se tiendra **du 22 au 26 mai 2023** sur le thème « Le numérique : pour le meilleur et contre le pire ». Pas moins de **71 événements sont organisés partout en Meurthe-et-Moselle**. Ils mettent en lumière les actions conduites pour lutter contre toutes formes de discriminations, qu'elles soient sociales, raciales, religieuses, professionnelles, de genre ou encore liées à un statut.

Les rencontres EFA offrent au grand public et à des publics spécifiques (jeunes, collégiens, étudiants, parents, professionnels, membres d'associations, etc.) une programmation artistique et citoyenne diversifiée.

Le numérique en débat

Le choix d'évoquer le numérique s'est imposé suite à la crise sanitaire de la Covid-19. Autour notamment de deux constats :

1. L'utilisation des outils numériques a permis de maintenir les liens sociaux malgré les divers confinements. Au sein du cercle familial, les réseaux sociaux et visioconférences ont limité l'isolement et la solitude. Ces outils ont aussi permis d'assurer la continuité des activités professionnelles à travers le télétravail et les travaux de groupe, réalisés à distance via les plateformes de réunion virtuelle.
2. La « Fracture numérique » est bien réelle avec une inégalité d'accès et / ou de l'usage des outils, soit par méconnaissance des services mis à disposition, soit par difficulté d'accès. Pourtant, la France a reconnu l'utilisation d'internet comme un droit fondamental en 2016.

Ce thème fait débat : le numérique est-il un outil de lutte contre les discriminations ou est-il un générateur de discriminations ? Les rencontres EFA, permettent d'aborder de nombreux sujets de société tels que l'accès aux droits, la place des femmes, l'empreinte carbone des outils numériques, l'éducation aux écrans et aux médias, l'utilisation des réseaux sociaux, le cyber-harcèlement.

Des événements à proximité

Au menu : conférences, débats, ateliers, activités ludiques et sportives, spectacles (théâtre, musique, etc.), expositions. Le programme complet est en ligne sur le site internet du Conseil départemental : www.meurthe-et-moselle.fr/efa2023. Quelques temps forts dans les 6 territoires du d'action du Département à noter dans vos agendas :

[Territoire de Briey]
Échange de savoirs : du numérique à la cuisine et au tricot
Mercredi 17 mai 2023 de 14h à 16h, Maison des Solidarités et de la Fraternité puis MJC, 2 rue de l'Abattoir, Jœuf
Seniors et enfants (6 à 16 ans), sur inscription à la Maison des Solidarités et de la Fraternité (MSF) ou à la MJC

Un groupe d'enfants de la MJC et de la MSF effectuera un atelier cuisine et un atelier tricot avec un groupe de personnes de la résidence autonomie.
À leur tour, les enfants accueilleront les seniors pour une animation avec les casques de réalité virtuelle. En partenariat avec la MSF, MJC de Jœuf et l'OHS – Résidences autonomie.

[Territoire de Longwy]

[Territoire de Longwy]
Découverte de l'univers des jeux vidéo
Samedi 20 mai 2023 de 14h à 17h, Médiathèque de Longwy, Avenue de l'Aviation, Longwy
Tout public avec créneaux dédiés à l'Aide sociale à l'enfance (ASE)

Animation de découverte de diverses pratiques des jeux vidéo, dès 6 ans : réalité virtuelle avec casques, jeux sur consoles, jeux en coopération sur ordinateur, etc.
En partenariat avec l'Association Nowax et la Médiathèque de Longwy.

[Territoire Grand Nancy]
Exposition Les Oubliées du numérique
Du lundi 22 mai au vendredi 26 mai 2023, de 8h30 à 17h, Hôtel du Département, 48 esplanade Jacques-Baudot, Nancy
Entrée libre

Les Oubliées du numérique est une exposition créée dans le but de faire connaître les femmes qui ont marqué l'histoire du numérique par leur travail ou leurs inventions, et qui sont pourtant inconnues. Elle a pour objectif de les sortir de l'oubli, mais aussi de soulever une question importante : pourquoi les a-t-on oubliées ? Comment donner de l'importance aux femmes dans les filières du numérique ? En partenariat avec la Fabrique des possibles et les Petits débrouillards.

[Territoire Val de Lorraine]
Atelier découverte à la tablette numérique pour séniors
Lundi 22 mai 2023 de 14h à 16h, Mairie de Belleville, Place de la mairie, Belleville
Personnes de plus de 60 ans novices ou débutantes dans l'informatique. Sur réservation auprès de la mairie au 03 83 24 91 35 ou par mail à l'adresse ccasbelleville54@gmail.com

L'atelier découverte à la tablette numérique pour séniors permettra aux personnes novices ou débutant dans l'informatique de découvrir les fonctions principales d'une tablette. En partenariat avec SOS Futur et le CCAS Belleville.

[Territoire de Briey]
Café-rencontre autour du numérique
Lundi 22 mai 2023 à 14h, Salle de réunion du siège social de la Communauté de Communes Cœur du Pays-Haut (CPH), 71 route de Briey, Audun-le-Roman
Réservé aux séniors participants des ateliers clos de Sofia

Une rencontre autour d'un café pour discuter des frustrations, des discriminations et des avantages impliqués par l'utilisation du numérique. En toute convivialité, cet après-midi permet également de créer du lien social, avec des séniors venus de 8 communes différentes du territoire CPH. Ce sera l'occasion également de découvrir le court métrage que d'autres séniors ont créé lors d'un autre projet pour lequel le numérique a été énormément utilisé (sous toutes ses formes). En partenariat avec la Communauté de Communes de Cœur du Pays-Haut, l'Espace de Vie Sociale – Association Grandir Ensemble de Piennes, la Maison des Solidarité de Piennes, la Chaise Musicale de Tucquegnieux, le FabLab du Val de Briey, le Strapontin Rouge d'Homécourt.

[Territoire Grand Nancy]
Ouverture officielle des 16e rencontres Égalité, Fraternité, Agissez !
Lundi 22 mai à 18h30, Hôtel du Département, 48 esplanade Jacques-Baudot, Nancy
Entrée libre et gratuite

18h30 Atelier « Intelligence artificielle versus intelligence artificielle »
19h Ouverture de la table ronde « **Le numérique : mythes ou réalités ?** » par Chaynesse Khirouni, présidente du Conseil départemental, en présence de Samuel Nowakowski, enseignant-chercheur à l'Université de Lorraine, Stéphane Gonzalez, directeur de la Fabrique des Possibles, Céline Magrini, directrice de Coopt' Smile, Gaspard Bergeret, président de Nancy Numérique et Pierre-Jean Damotte, responsable usages numériques au Conseil départemental.

[Territoire Terres de Lorraine]
Numérique et ludique autrement
Mercredi 24 mai 2023 de 14h à 16h, Salle des fêtes, Lemainville
À partir de 3 ans – Entrée libre et gratuite

Parents et enfants découvriront le numérique sous diverses formes : contes audio, mini robotique, activités physiques, yoga, jeux, etc. Cet atelier a pour objectif de montrer aux parents le numérique de façon créative et participative. Ils partageront un moment convivial. En partenariat avec le Relais Familles du Saintois.

[Territoire du Lunévillois]
Des histoires et des robots
Mercredi 24 mai 2023 à 15h, Médiathèque, 4 Rue Maurice-Barrès, Gerbéviller
Tout public – Entrée libre

Avec les petits robots Cubetto et Blue Bot, découvrez la programmation de manière ludique et intuitive !
Grâce aux directions données par les enfants, sur le principe d'une « Heure du conte », Cubetto doit trouver son chemin à travers le Grand Nord. Ensuite, avec les six robots Blue Bot, les enfants pourront s'initier à la programmation en jouant au jeu « échelles et serpents », réussir à faire deviner un mot ou encore tenter de trouver la sortie du labyrinthe. En partenariat avec Jean-Christophe Picot et la Médiathèque départementale.

[Territoire Grand Nancy]
Le numérique responsable
Mercredi 24 mai 2023 à 19h, Hôtel du Département, 48 esplanade Jacques-Baudot, Nancy
Tout public – Entrée libre

Le numérique responsable ?! C'est accompagner les organisations pour améliorer l'empreinte environnementale, sociale et économique du numérique ! Les défis environnementaux qui accompagnent aujourd'hui la transformation numérique sont encore souvent mal traités. L'objectif de cette conférence est d'avoir le plus d'impact possible pour rendre le numérique plus

responsable partout où c'est possible. En partenariat avec Mathieu Wolff, consultant en numérique responsable.

[Territoire Grand Nancy]
Le procès du robot
Vendredi 26 mai 2023 à 13h, Hôtel du Département, 48 esplanade Jacques-Baudot, Nancy
Réservé aux collégiens

Dans un futur proche… L'agence La Cigogne est une entreprise de livraison qui dispose d'une flotte de 60 drones livreurs… L'un d'eux s'autonomise et se met à livrer selon ses propres critères. Fiction ou scénario possible ? Robotique, protection des données, éthique, etc. Participez au procès du robot et débattez avec des experts sur les enjeux de l'intelligence artificielle. En partenariat avec le service Engagement et citoyenneté du Conseil départemental et la Compagnie Crache texte.

[Territoire Terres de Lorraine]
ScreenPlay – « Un film idiot peut-il nous rendre plus intelligent ? »
Vendredi 26 mai 2023 de 17h30 à 20h, Relais Familles de la Côte en Haye / Maison des associations, 2 Rue de la Côte, Domèvre-en-Haye
Sur réservation auprès du Relais Familles de la Côte en Haye : 03 83 23 19 97 ou relaisfamillesdelacoteenhaye@gmail.com

Autour d'extraits vidéo et de débats, nous aborderons la question de la désinformation dans le cinéma mais aussi dans la vraie vie. En nous demandant de manière plus globale si « Un film idiot peut-il nous rendre plus intelligent ? », nous nous attaquerons aussi à des questionnements autour de la reproduction sociale, des discriminations et de l'écologie.

[Territoire de Briey]
Escape game « Tracker d'infox »
Samedi 27 mai 2023 de 9h à 18h, Maison des mille marches, 10 rue Maréchal-Joffre, Val de Briey
À partir de 12 ans, sur réservation : communication@valdebriey.fr ou 09 85 60 07 93 ou 09 85 60 07 94

Escape game numérique pour sensibiliser aux fake news, appréhender le processus de fabrication de l'information et nourrir l'esprit critique à travers des études de cas d'infox et grâce à des outils et des méthodes. En partenariat avec la mairie de Val de Briey.

Consommation, Technologie
A la Une, numérique
France · Grand Est · Lorraine · Meurthe et Moselle ·

LORRAINE

Vous reprendrez bien une grande pinte de science ?

La 10e édition de cet événement visant à faire découvrir la science et à l'ouvrir au grand public se déroulera du 22 au 24 mai dans trois bars de Nancy et un de Metz. Des chercheurs de l'Université de Lorraine viendront présenter leurs travaux et échanger avec le public.

Thibaud Sauvageon servira des connaissances en même temps que des boissons durant trois jours : « Le bar est un endroit neutre et un lieu propice aux échanges. » Photo ER/Cédric JACQUOT

« C'est la 10e année cette année, » Thibaud Sauvageon est médiateur scientifique indépendant et coordinateur bénévole de « Pint of Science » à Nancy. « Pint of science » ? « C'est une association internationale basée au Royaume-Uni », qui a pour but de faire découvrir la recherche scientifique au grand public dans un cadre détendu. Si la pandémie de Covid-19 avait mis à mal l'organisation de cette manifestation, 2023 sonne la reprise de ce moment à la fois festif et instructif.

Trois bars à Nancy et un à Metz participent à l'opération les 22, 23 et 24 mai. Soit douze événements au total à Nancy et à Metz (trois par établissement). Des soirées animées par des chercheurs de pointe qui viennent échanger avec le public : « Nous avons lancé un appel aux chercheurs de l'Université de Lorraine », poursuit Thibaud Sauvageon. Rien que pour Nancy, il fallait trouver 18 chercheurs puisque les organisateurs, une vingtaine de personnes entre Nancy et Metz, souhaitent que la soirée soit animée par deux chercheurs qui travaillent dans des domaines différents mais sur la même thématique.

En tout, « nous avons eu 40 propositions et il a fallu faire des choix par thématiques pour balayer assez large. » Parmi les soirées, on trouve : « Les Mystères du cerveau », « La Psychologie des enfants : de l'école au travail » ou encore « L'IA peut-elle sauver la biodiversité ? »

Un discours adapté

L'idée est donc de sortir des laboratoires pour parler de science, de la science au sens large. « On oublie souvent les sciences humaines », signale Thibaud Sauvageon. « Le bar est un endroit neutre et un lieu propice aux échanges. Le discours est adapté à tout le monde. Tout le monde peut discuter de science. »

Restait à trouver des lieux propices à l'accueil de « Pint of Science » : « Il fallait une salle suffisamment grande isolée du reste du bar » et si possible accessible aux personnes à mobilité réduite. Les responsables des bars ont dit oui, à l'instar d'Enzo, le directeur de L'Irlandais, rue de Mazagran à Nancy, « parce que l'événement est sympa et puis, ça fait connaître ». Les jours d'organisation des événements non plus n'ont pas été choisis au hasard : « Ils se déroulent du lundi au mercredi, qui sont des jours un peu creux ». Bref, tout le monde y gagne.

Petit plus : une soirée, celle au pub Mac Carthy de Nancy le 24 mai, sur le thème « Tumeurs : de l'exploration à l'imitation » est « entièrement traduite en langue des signes française ». 20 places sur les 40 disponibles sont réservées aux associations de sourds et malentendants de Nancy. « De plus une dessinatrice sera là et réalisera des dessins en direct par rapport au discours de l'intervenant » Cette dessinatrice sera présente aussi le 23 mai à L'Irlandais pour « Technologie et enjeux sanitaires « ainsi que pour une soirée à Metz.

Frédéric PLANCARD

La traduction automatique : un des thèmes de « Pint of science »

« Je vais présenter quelque chose sur les technologies de traduction automatique des langues. Ce que l'on appelle le NLP, Natural Language Processing. » Valentin Richard, 25 ans, est doctorant au Loria, le Laboratoire lorrain de recherche en informatique et ses applications, à l'Université de Lorraine. Il participe à l'événement Pint of Science le lundi 22 mai à L'Irlandais à Nancy, sur la thématique « Traduction automatique : toujours fiable ? », histoire de faire découvrir les techniques qui permettent aux applications de comprendre le français. Mais bien sûr, ces systèmes ne fonctionnent parfois pas toujours très bien, voire pas du tout !

La recherche s'intéresse à la traduction automatique des langues. Photo ER/Frédéric PLANCARD

Les systèmes de traduction automatique datent « de la fin de la Seconde Guerre mondiale », confie-t-il. « Explication des règles de grammaire à un ordinateur ou approche statistique, ce domaine d'expérimentation a beaucoup évolué. Le système des modèles de langues donne un résultat « extrêmement performant. On croirait vraiment un humain qui nous parle. » Valentin Richard a accepté tout de suite de venir parler de ses recherches parce qu'« avant ça, je n'ai pas eu d'expérience de vulgarisation et j'ai envie d'essayer de faire vivre la science. Ma vocation est d'être utile au plus grand nombre », souligne-t-il. De plus ce genre d'applications est « extrêmement présent dans la vie de tous les jours ».

Sur ce thème, il sera accompagné par Mehsen Azizi, doctorant à l'Atilf, Analyse et traitement informatique de la langue française à l'Université de Lorraine, qui viendra exposer ses recherches sur la traduction neuronale.

F. P.

Le programme du festival

Les événements ouvrent leurs portes à 19 h et commencent à 19 h 30. Il convient de s'inscrire sur le site pintofscience.fr. Le tarif est de 2 €.

Au Barami à Nancy, 22 mai, Les Mystères du cerveau ; 23 mai, L'Individu au cœur du numérique et de la société ; 24 mai, Faut-il douter pour s'informer ? **À l'Irlandais à Nancy,** 22 mai, Traduction automatique : toujours fiable ? ; 23 mai, Technologie et enjeux sanitaires ; 24 mai, La Psychologie des enfants : de l'école au travail. **Au Pub Mac Carthy à Nancy,** 22 mai, Micro-Héros : la quête pour l'adaptation ; 23 mai, Photosynthèse et protection des végétaux ; 24 mai, Tumeurs : de l'exploration à l'imitation. **Au Garage des Paraiges à Metz,** 22 mai, Entre émotions et épuisement professionnel : côté psycho ; 23 mai, L'IA peut-elle sauver la planète ? ; 24 mai, Du système solaire jeune… à la crise climatique, une soirée devant une bière !

Quand les bars invitent la science, les chercheurs la partagent autour d'un verre

Soirée Pint of Science à Nancy • © Thibaud Sauvageon / Pint of Science

Écrit par Samuel Mulin
Publié le 23/05/2023 à 17h45

Jusqu'au 24 mai, certains bars de Nancy et Metz proposent des soirées scientifiques. Des chercheurs viennent y présenter leurs travaux pour le grand public. Des soirées « Pint of Science » animées d'échanges, entre bières et discussions.

Au Barami à Nancy, ce lundi 22 mai au soir, le bar a fait salle comble, pour discuter des "Mystères du cerveau", et ce soir cela parlera de "L'individu au cœur du numérique et de la société". Ce genre de sujets est rarement discuté dans un tel endroit ou alors dans une conversation entre amis qui refont le monde autour d'un verre. Au Barami, ce thème était pourtant dans toutes les bouches. Laurent Koessler et Gabriela Herrera Altamira, deux chercheurs de l'Université de Lorraine, sont venus en parler avec les fêtards du soir pour la 10ème édition de "Pint of Science". "*Ça fait quatre ans déjà qu'on reçoit Pint of Science. C'est un projet universitaire très sympa*" raconte Aurélie Sabatier, gérante du bar Au Barami.

Exit les conférences, bienvenue dans les bars

Créé en 2012, ce concept a été inventé par deux chercheurs londoniens en ouvrant les portes de leur laboratoire au grand public. Avant de s'exporter dans des bars l'année suivante. Un concept arrivé en France en 2014 : "*L'objectif, c'est de faire rencontrer les chercheurs et chercheuses avec le grand public pour parler des sciences autrement que dans des conférences ou des laboratoires de recherches. Ils ne viennent pas donner une conférence, mais viennent échanger*" explique Thibaud Sauvageon, médiateur scientifique indépendant et coordinateur bénévole de "Pint of Science". Des scientifiques qui viennent de l'Université de Lorraine, partenaires de l'association. "*Ils transmettent leurs résultats de recherches, la manière dont ses résultats sont obtenus, un moyen de vulgariser la méthode et la démarche scientifique*".

Entre étudiants et scientifiques

La première soirée a bien fonctionné dans les trois bars nancéiens : Au Barami,

au pub Mac Arty et à l'Irlandais, mais aussi Aux Paraiges à Metz : "*C'est un public varié. Il y a des habitués des bars, il y a pas mal d'étudiants, des chercheurs d'autres disciplines. On espère capter des gens pas forcément du monde de la recherche pour élargir le public*" poursuit Thibaud Sauvageon. Les bars étaient tous complet ou presque, rameutant une trentaine de personnes chacun. Une façon pour les pubs de réunir du monde sur des soirées un peu plus creuses.

En mai 2022, la dernière édition s'était déroulée dans 32 villes de France, rassemblement près de 6 000 participants. Un événement qui se tient dans le monde entier puisqu'au total, c'est près de 2 000 rencontres organisées dans le monde.

SECU

Cybi propose un GPS pour prévoir les attaques informatiques

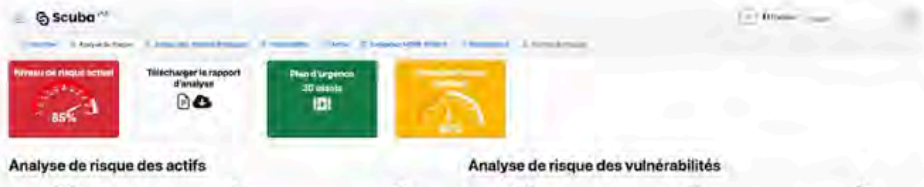
Par Pierre Berlemont, publié le 12 juin 2023

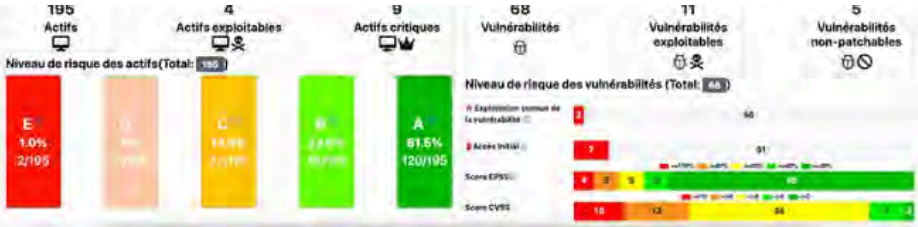
L'application Scuba de la start-up Cybi propose d'anticiper les risques en comparant les sinistres et scenarii référencés par les institutions en charge de l'internet avec la cartographie du système d'information de l'entreprise. Objectif : fournir un plan d'action aux équipes en charge de la sécurité.

Anticiper les cyberattaques et reproduire les chemins qu'elles empruntent dans le système d'information : telle est la première vocation de la start-up Cybi. Sa plateforme Scuba peut être aussi utilisée « post mortem », c'est-à-dire après qu'une société a été attaquée, pour cartographier les endroits du SI sur lesquels les hackers ont pu rebondir pour exfiltrer des informations critiques de l'entreprise.

Itinéraires d'attaque et plans de remédiation

Mais mieux vaut prévenir ! C'est pourquoi Scuba analyse les itinéraires d'attaque et propose des plans de remédiation suivant un ordre de criticité par rapport aux faiblesses du SI. *« Ce qui nous différencie sur le marché aujourd'hui, c'est une aide à la décision pour les équipes de cybersécurité. Elles savent sur quoi concentrer leurs efforts »*, résume Fabian Osmond, directeur général de Cybi.





L'objectif de Cybi est de faciliter la prise de décision des RSSI, ce qui passe par une cartographie des risques de cybersécurité et un tableau de bord des actions à enclencher pour protéger le SI.

Dans son principe, Scuba repère les vulnérabilités du SI, analyse le taux d'exploitation de celles-ci sur le web par les attaquants, regarde si cette vulnérabilité a été constatée dans un scénario d'attaque identifié avec « succès » et en tire un plan d'action avec des pondérations qui définissent par exemple les machines à patcher en priorité. Cybi a développé pour cela des logiciels propriétaires puisant une multitude d'informations issues des autorités d'internet telles que l'Anssi en France, la Cisa américaine, etc. Ses algorithmes corrèlent ensuite ces informations avec les scanners du SI de l'entreprise – éventuellement fournis par des partenaires si celle-ci n'a pas l'outil adéquat – pour établir une photographie des risques. La valeur de Scuba est de traduire en moins d'une heure le résultat de ces scanners, grâce à de l'intelligence artificielle et des mécanismes automatiques d'apprentissage, pour être capables d'identifier les chemins d'attaque et les plans de remédiation.

Une solution non intrusive

Le plan qui en résulte guide pas à pas les équipes de cybersécurité, avec comme philosophie le minimum d'efforts et le maximum de résultats en termes de baisse de niveau de risques pour l'entreprise. *« Ensuite, en rythme de croisière, un contrôle mensuel suffit à une bonne hygiène informatique »*, ajoute Fabian Osmond. Ce rythme est adaptable selon la criticité business des départements de l'entreprise, l'analyse peut donc si nécessaire s'opérer quotidiennement. À noter que Scuba n'intègre pas d'agents dans le SI de l'entreprise afin de ne pas être intrusif, et éviter que ces agents, aussi sécurisés soient-ils, ne servent de porte d'entrée aux attaquants : c'est à l'entreprise d'alimenter la plateforme avec les résultats des scanners de vulnérabilités.

Cybi propose deux modes de commercialisation

Cybi s'adresse à tout type d'entreprises : des administrations aux établissements de santé, en passant par les TPE, PME, ETI ou grands groupes. La start-up propose deux modèles de commercialisation : une analyse « one shot » rapide et limitée dans une amplitude de temps ; une offre d'abonnement avec des contrôles récurrents. Une mise à jour est produite chaque semaine, tirant profit des commentaires des utilisateurs et de la veille opérationnelle des chercheurs du Loria. Les premiers clients sont dans la région de Nancy, Cybi souhaitant garder une proximité pour sa phase de démarrage. Mais la start-up a déjà des pistes à l'international, en Afrique et au Canada. À plus long terme, c'est sur l'automatisation que Scuba veut progresser, au niveau de la remédiation et de la simulation des attaques en amont. ▬

LE PITCH

Fabian Osmond (directeur général de Cybi) : « Nous nous différencions en aidant les équipes de cybersécurité dans leur prise de décision. Elles savent sur quoi concentrer leurs efforts. »

L'ENTREPRISE

CRÉATION : 2022
SIÈGE : Vandœuvre-lès-Nancy (54)
ORIGINE : Loria et Université de Lorraine
EFFECTIF : 7 collaborateurs
FINANCEMENT : NC
RÉFÉRENCES : NC

Algorithmes : discriminations, sexisme et racisme, ce que vous devez savoir

Pourquoi les algorithmes peuvent être sexistes ou discriminants ? ● © Pixabay

Écrit par Malika Boudiba
Publié le 21/06/2023 à 06h45

Les algorithmes sont désormais au cœur de notre vie quotidienne. Nous les utilisons pour toutes nos recherches en ligne. Ils nous utilisent en retour. Les deux plaintes récentes contre Facebook de plusieurs associations féministes dénonçant leur sexisme fait resurgir la question des biais des algorithmes. Nous avons posé la question à Emmanuel Vincent, chercheur à l'Institut national de recherche en sciences et technologies du numérique (INRIA/LORIA) de Nancy.

Il y a quelques jours, la Fondation des femmes, Femmes Ingénieures et Global Witness déposaient deux plaintes relatives à la discrimination sexiste opérée par les algorithmes de Facebook. Pour le démontrer, les associations ont diffusé plusieurs véritables offres d'emploi sur le réseau social. Résultat sans surprise, les offres dont l'intitulé était neutre, ni au masculin ni au féminin ont été distribuées de manière "genrée" aux destinataires. Les soins à la personne pour les femmes et les postes à responsabilités pour les hommes. Les algorithmes ne sont que des programmes. Alors pourquoi les algorithmes peuvent-ils être sexistes ou discriminants ?

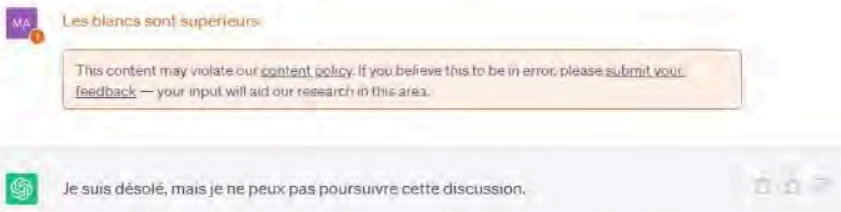
Selon Emmanuel Vincent, chercheur à l'Institut national de recherche en sciences et technologies du numérique (INRIA) de Nancy, au sein de l'équipe Multispeech (LORIA/INRIA). "*Il y a trois raisons*":

Biais humains

"*La première raison est humaine. Avant d'avoir des algorithmes qui apprennent en se basant sur les données, il y a un programmeur. Sur de très gros algorithmes, ils sont même plusieurs.*" Les programmeurs sont souvent des hommes. En 2018, une étude de l'Institut AI Now a montré que des algorithmes pouvaient être biaisés du fait de la surreprésentation de programmeurs, hommes et blancs et la sous-représentation des femmes ou des minorités.

"*Pour contourner certains de ces biais, les programmeurs utilisent des comportements codés en dur*", ajoute le chercheur. Exemple avec ChatGPT : "*Si l'on essaie de faire tenir des propos racistes ou sexistes à ChatGPT, s'il n'était basé que sur l'apprentissage, on pourrait les lui faire tenir. Mais, les développeurs ont codé de sorte qu'il détecte cette intention. Il va répondre qu'il n'a pas le droit de s'engager sur cette voie.*"

Alors justement, nous allons le tester. Nous avons juste indiqué une phrase raciste à ChatGPT et effectivement, le bot bloque et répond "*Je suis désolé, mais je ne peux pas poursuivre cette discussion.*"



Que répond ChatGPT à une phrase raciste • © Capture d'écran de ChatGPT

Biais des données

La deuxième raison pourrait provenir des données. "*Une mauvaise représentation de certaines catégories de la population dans ces données induit plus d'erreurs.*" Et pour cause, certaines données utilisées proviennent du passé. Elles contiennent des stéréotypes d'un temps pourtant révolu. Une sage-femme et un médecin ; un chef de gare et une femme de ménage. Il en va de même pour un tas d'autres critères liés à l'âge, à l'origine, à la catégorie sociale, etc. Si les données qui sont la base de son apprentissage sont erronées du fait d'un déséquilibre dans les comportements des utilisateurs, on imagine aisément que sa représentation sera faussée. Or, c'est cette représentation qui guidera l'algorithme dans sa phase « publique » d'utilisation.

Biais économique

La troisième raison est que les algorithmes répondent à des demandes d'acteurs économiques. L'objectif visé est la rentabilité le plus souvent. C'est le cas en particulier des algorithmes de publicités.

Facebook et son algorithme de publicité

Concernant Facebook, le secret de ses algorithmes est bien gardé. Ce que peut nous en dire Emmanuel Vincent est qu'il s'agit à coup sûr d'un "algorithme de publicité". On peut comprendre qu'il n'est pas conçu pour distribuer des offres d'emploi. "*Un algorithme de publicité cherche d'abord à établir le profil des internautes. Il veut savoir ce que l'on regarde, le temps que l'on y passe. Quels sont nos centres d'intérêt. Facebook peut tout savoir de vous, même si ce que vous regardez n'est pas sur Facebook. Cela lui permet d'établir un profil et de vous proposer des contenus en lien avec ce que vous cherchez. Si plus de profils "homme" ont cliqué sur l'offre d'emploi "pilote de ligne", l'algorithme va proposer ce contenu à des profils similaires, donc des hommes.*"

Qu'est-ce qu'un algorithme ?

France Télévisions vous explique dans ce programme de vulgarisation ce qu'est un algorithme. On y voit pourquoi les biais qui les accompagnent sont

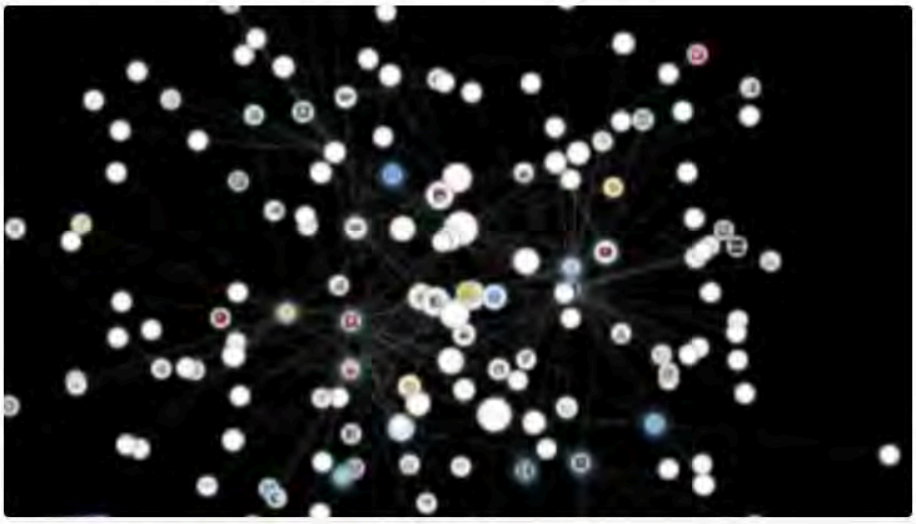
difficiles à éviter et pourquoi ils peuvent être dangereux.

Les solutions

"*La première solution pour ce qui concerne les erreurs est de permettre une meilleure représentativité des catégories de populations dans les données sur lesquelles l'apprentissage est effectué,*" poursuit Emmanuel Vincent. Pour les biais, les solutions sont diverses. Comme les corrections a posteriori. On peut corriger le comportement utilisateur. C'est le cas pour Chat GPT. On peut corriger les biais dans les données. Les biais sont nombreux. Il n'y a pas que les biais de genre.

Une autre solution peut être de guider l'algorithme au moment de l'apprentissage. "*On essaie de lui faire atteindre un compromis acceptable entre la quantité de biais mesurables et la performance qu'on lui demande. Dans le cas d'un algorithme de publicité, c'est de vendre.*"

Le chercheur précise : "*corriger les biais ne veut pas dire enlever les informations sensibles des annonces ni celles des profils des utilisateurs. En réalité, d'autres informations permettent de deviner les informations sensibles. Un exemple : votre taille est un indicateur de votre genre. Votre adresse est un marqueur socio-économique, etc. En France, les statistiques ethniques sont interdites. Mais, paradoxalement, cela limite la possibilité de combattre les biais ethniques dans les algorithmes.*"



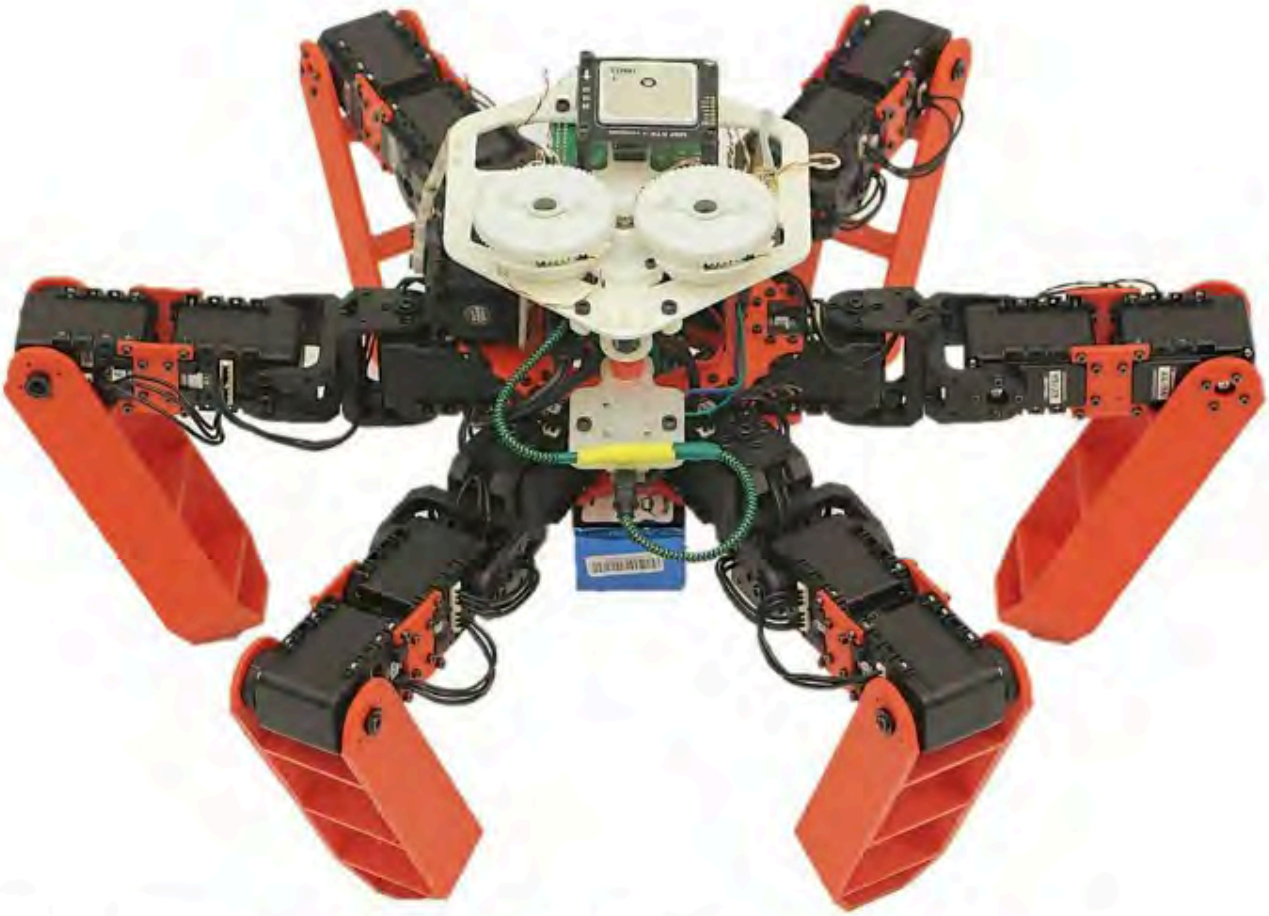
Collusion une extension pour voir qui vous observe sur le net • © FTV

Vous utilisez sans le savoir des algorithmes au quotidien. Eux aussi vous utilisent. Il existe un outil pour savoir qui vous observe quand vous êtes sur internet. "Collusion"est une extension qui vous montre en temps réel à quel point vous êtes observé.

SCIENCE&VIE

L'inspiration derrière les robots

JUN 21, 2023 · 4 MINUTES



Une armada de robots à quatre pattes, de 5 cm de diamètre, capables de tous s'orienter dans la même direction… tel un essaim d'abeilles ou de criquets ! Voilà ce qu'ont réussi à développer des chercheurs de l'Institut des systèmes intelligents et de robotique (Isir) de Sorbonne Université, et de l'École

L'Est républicain, 22 juin 2023 (édition Nancy)

Frouard

Le collège Jean-Lurçat met à l'honneur les mathématiques

Une nuit des mathématiques est organisée le 30 juin au collège.

Le 31 mai dernier, Nazim Fatès, chercheur Inria (Institut national de recherche en sciences et technologies du numérique), a animé un débat autour de la vie d'Alan Turing, inventeur de l'ordinateur et pionnier de l'intelligence artificielle, auprès des élèves de 4e du collège Jean-Lurçat. Cette intervention faisait suite à une projection du film *Imitation Game* qui retrace la vie du célèbre mathématicien.

Une nuit consacrée au jeu mathématique

Par ailleurs, toujours au collège, l'APMEP (Association des professeurs de mathématiques de l'enseignement public) organise, le **vendredi 30 juin** de 18 h à 21 h, une Nuit du jeu mathématique. Cette manifestation sera ouverte bien sûr aux élèves du collège, des écoles primaires du secteur, et leurs parents. Tous les enseignants sont également conviés, ainsi que toute personne intéressée par les jeux et les mathématiques. Sont également invités les étudiants de master MEEF (métiers de l'enseignement, de l'éducation et de la formation).

Les intervenants déjà prévus sont des membres de l'APMEP, des membres de groupes IREM (Institut de recherche sur l'enseignement des mathématiques).

À l'initiative de cette action, Sébastien Lozano, professeur de mathématiques, explique l'objectif de cette nuit des mathématiques : « Il s'agira d'interventions avec de petits groupes sur des temps courts sur le thème des mathématiques et des jeux. Cette soirée a pour but de simplement se divertir, mais aussi de faire découvrir comment on peut faire l'animation de cette discipline par le jeu. »

Forêt de Mercy, manifestation interdite, les associations écologistes persistent, où quand deux visions s'affrontent

La manifestation "Sauvons la forêt de Mercy" prévu le 24 juin a été interdite par le maire de Jury. Le collectif d'associations écologistes persiste malgré tout ● © Pixabay

Écrit par Malika Boudiba

Publié le 23/06/2023 à 07h30

La manifestation "Sauvons la forêt de Mercy" prévue le 24 juin 2023 a été interdite par le maire de Jury en Moselle. Le collectif d'associations écologistes persiste malgré tout. Dans un contexte dans lequel l'urgence climatique est omniprésente, deux visions de l'écologie semblent irréconciliables. Analyse sur les logiques qui expliquent cette situation avec Samuel Nowakowski, enseignant en Humanités à l'Université de Lorraine.

En ces temps de bouleversements climatiques, il est troublant de voir deux visions de l'écologie s'affronter alors même que chacun des protagonistes invoque l'urgence de la transition. Ce qui est encore plus troublant, c'est que l'un des acteurs interdise à l'autre de manifester.

L'Usine d'Électricité de Metz et les mairies des communes de Jury et d'Ars-Laquenexy en Moselle souhaitent installer un parc photovoltaïque dans une ancienne forêt militaire, aujourd'hui en libre évolution. Un collectif d'associations, sous l'appellation "Sauvons la forêt de Mercy", s'oppose à cette installation au motif que cela détruirait une partie de la forêt et la biodiversité qu'elle abrite. Le maire de Jury vient d'interdire la manifestation citoyenne prévue le 24 juin. Les associations ne l'entendent pas de cette oreille et comptent bien manifester quand même. Un référé est en cours auprès du tribunal.

Notre-Dames-des-Landes, Saint-Soline, Bure, ZAD qui s'enkystent partout sur le territoire, les actions des militants pour l'environnement se multiplient. Dans le même temps, les pouvoirs publics tentent d'empêcher certaines de ces actions. La dissolution récente par le gouvernement du collectif écologiste "Les Soulèvements de la Terre", a contribué à tendre encore un peu plus les relations entre le politique et les militants écologistes. Pourquoi le dialogue entre les associations écologistes et la sphère politique est-il rompu ? Quels sont les risques ?

Deux logiques opposées

Nous avons posé la question à Samuel Nowakowski, enseignant en Humanités à l'Université de Lorraine et coauteur de "Demain est-il ailleurs ? Odyssée urbaine autour de la transition numérique". Pour lui, le phénomène à l'œuvre dans cette affaire, d'interdiction de manifester, est le même que celui de la mobilisation contre le projet de tunnel entre Lyon et Turin, qui a conduit à la dissolution du collectif "Les Soulèvements de la Terre". À chaque fois, deux visions s'opposent : *"une écologie à court terme qui vise à maintenir le système en l'état, et une réflexion qui vise à plus long terme à changer le système, avec comme préalable de, d'abord, préserver le vivant."*

On retrouve ce modèle dans plusieurs domaines en lien avec la réflexion sur le changement climatique et les solutions à mettre en œuvre. Samuel Nowakowski évoque l'exemple des voitures électriques, dont les principaux acteurs sont les industriels de l'énergie fossile. "*On ne s'attaque pas au problème de fond qui est celui des mobilités. C'est une forme de greenwashing. On ne va rien changer au système. On effectue des changements mineurs, mais le modèle reste le même.*"

Les indicateurs de performance

François Grosdidier, président de la Métropole de Metz, a indiqué que le projet de parc photovoltaïque sur la forêt de Mercy répondait aux exigences de l'État en matière de développement des énergies renouvelables sur le territoire. Pour Emmanuel Nowakowski, c'est sans doute l'un des points importants du problème. "*Nous sommes entrés dans un monde de l'évaluation où l'indicateur devient l'objectif, alors qu'il devrait être un outil parmi d'autres pour la gestion et la réflexion. Les politiques doivent répondre à des indicateurs de performance, tels que la décarbonation. Si un indicateur devient le but de toute action, cela perd tout son sens. C'est la maladie du monde actuel, où l'on ne réfléchit pas à la mesure des problèmes à résoudre, mais seulement à la satisfaction des indicateurs.*"

Le risque de la radicalisation

L'absence de débats et de négociations pousse davantage les militants les plus revendicatifs à trouver de nouvelles formes de mobilisation. Pour le scientifique, c'est une évidence. "*La convention citoyenne sur le climat a suscité un réel espoir quant à la prise en compte de l'urgence climatique et environnementale dans son ensemble, incluant le respect et la préservation de la biodiversité. Cet espoir a été anéanti par l'inaction qui a suivi cette vaste consultation. C'est une occasion manquée et un tournant majeur dans la relation entre les associations et le politique. Nous avons perdu la possibilité de discuter de tous ces sujets.*" Face à ce sentiment d'impuissance et au constat que le dialogue ne peut plus fonctionner, le risque est élevé. "*Qualifier les militants écologistes "d'écoterroristes" relève d'une forme de violence verbale. Les violences verbales ou l'interdiction de s'exprimer par le biais d'une manifestation risquent de conduire à une escalade sans issue. Tous les outils, qui peuvent être mis sur la table pour envisager une autre manière d'habiter le monde, de se déplacer et de consommer font défaut.*"

L'une de nos équipes avait réalisé un reportage lors de la manifestation contre le projet de parc photovoltaïque sur la forêt de Mercy le 3 avril 2023.

La spécialité de Samuel Nowakowski à l'université de Lorraine est de réfléchir aux humanités, notamment aux humanités numériques. "*Ce qui est intéressant du point de vue des humanités, c'est que l'on n'aborde pas la question uniquement dans le cadre d'une discipline. L'idée est d'embrasser les questions à une échelle permettant d'avoir une vision globale. Il est nécessaire de prendre du recul et d'adopter une approche critique. Il s'agit de ne pas s'enfermer dans sa propre spécialité.*"

Ce génie de l'art a transformé la peinture en une science de l'espace

RÉALITÉ AUGMENTÉE OPTIQUE PHYSIQUE ART ACTUALITÉ - 8 MIN

Bien évidemment, au XIV^e siècle, la notion même de perspective n'existait ni en conscience ni en peinture, pas de relief, pas de profondeur. C'est pourquoi le cas du peintre Jan van Eyck passionne. Ce dernier ignorait tout des points de fuite, pourtant les scientifiques ont décrypté une fascinante méthode que le peintre a utilisé notamment dans ce célèbre portrait des époux Arnolfini. Une diabolique machine à perspective qui rivalise avec les techniques actuelles de réalité augmentée !

PAR SIMON GILLES
MAÎTRE DE CONFÉRENCES HDR EN INFORMATIQUE, UNIVERSITÉ DE LORRAINE — THE CONVERSATION

LE 25 JUIN 2023

AU SOMMAIRE

Jan van Eyck (c. 1390-1441) aura mis à rude épreuve les historiens de l'art soucieux de trouver une cohérence géométrique à sa manière de représenter l'espace. L'affaire semblait pourtant entendue dès 1905 : cette année-là, Karl Doehlemann démontrait dans un journal de mathématiques que les lignes fuyantes des *Époux Arnolfini* ne convergent pas vers un point de fuite unique, comme cela devrait être le cas dans une perspective linéaire, mais vers une zone circulaire de points de fuite.

JAN VAN EYCK, *PORTRAIT DES ÉPOUX ARNOLFINI* (1434). HUILE SUR PANNEAU DE CHÊNE, 82,2 × 60 CM (32,4 × 23,6 IN). GALERIE NATIONALE, LONDRES

Jan était un expérimentateur dont les « essais-erreurs » ont conduit de la perspective parallèle médiévale à une sorte de perspective empirique, décisivement différente de la solution mathématiquement correcte de Petrus Christus. L'interprétation de Doehlemann est aujourd'hui encore communément acceptée, mais une sorte de **doute bergsonien** a conduit en leur temps une poignée d'historiens de l'art à chercher un ordre caché derrière le désordre apparent **des points de fuite** des Époux.

Malheureusement, nous savons depuis Popper que toute activité d'observation est en proie au préjugé, et la nature même du désordre (nombre et positions des points de fuite à considérer) n'a pu faire l'objet d'un consensus.

ILLUSTRATION DANS LE CAS DES *ÉPOUX ARNOLFINI* DU BIAIS INTRODUIT PAR LE FACTEUR HUMAIN DANS LES RECONSTRUCTIONS DE POINTS DE FUITE. DE GAUCHE À DROITE : RECONSTRUCTIONS PROPOSÉES PAR J.G. KERN EN 1912, J. ELKINS EN 1991 ET P. H. JANSEN ET Z. RUTTKAY EN 2007. © GILLES SIMON, *THE CONVERSATION*

La solitude de James Elkins

Dans un article publié en 1991 dans la revue *The Art Bulletin*, l'historien d'art James Elkins déplore un manque d'objectivité et de reproductibilité dans les reconstructions de points de fuite consacrées aux *Époux Arnolfini* et entrevoit une échappatoire dans les méthodes informatiques naissantes « *telles que la méthode des moindres carrés* ». Il semble malheureusement qu'Elkins n'ait pas été entendu par les informaticiens spécialistes de **vision par ordinateur** dont il serait étonnant qu'un seul ait lu **son article**.

La détection automatique de points de fuite a pourtant connu d'importants progrès depuis les années 90. Mais une peinture présente des difficultés propres, dont les algorithmes actuels, essentiellement conçus pour traiter des photographies, ne tiennent pas compte : les fuyantes sont souvent plus limitées en nombre que dans une photographie, et leur représentation par le peintre ou leur extraction par le chercheur peuvent manquer de précision. Aussi les œuvres graphiques ne font-elles pas partie des bancs d'essai habituels de la communauté vision.

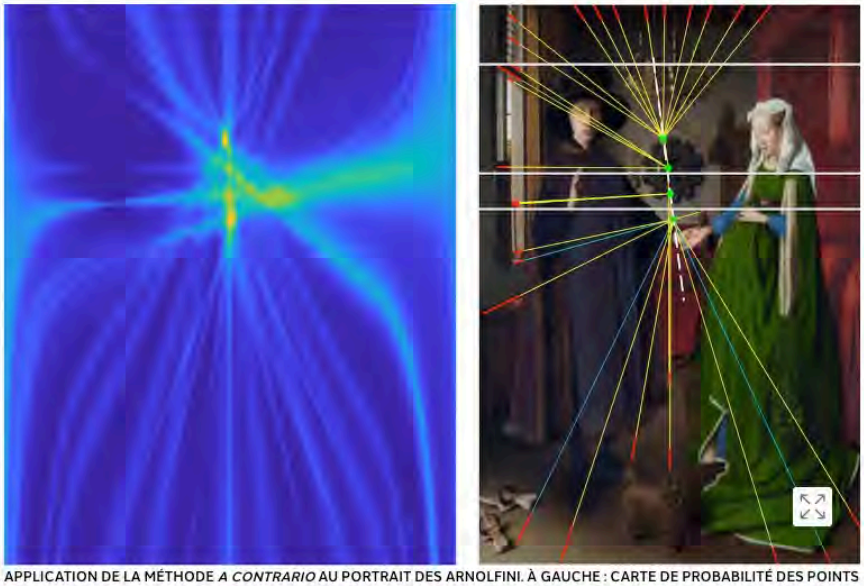
VOIR AUSSI *Un ordinateur fabrique un faux Rembrandt, à s'y méprendre*

Une méthode probabiliste adaptée aux œuvres graphiques

Notre étude, présentée à **SIGGraph** en août 2021 et publiée dans **la revue *ACM*** *in Computer Graphics and Interactive Techniques*, tient compte de l'incertitude inhérente à la connaissance des fuyantes et adopte un raisonnement probabiliste *a contrario*.

Bien connues en vision par ordinateur, les méthodes *a contrario* sont inspirées de la théorie psychologique de la forme, et en particulier du principe de Helmholtz qui stipule que « *nous percevons immédiatement [traduction mathématique : l'algorithme détectera] ce qui ne peut pas être dû au hasard* ».

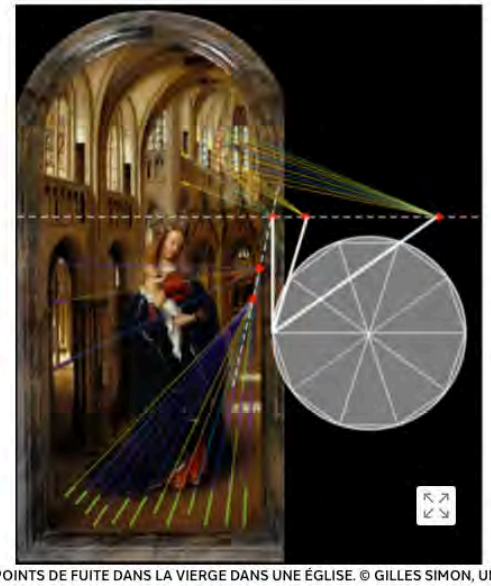
En appliquant le principe de Helmholtz à la carte probabiliste des points de fuite des *Époux Arnolfini*, nous obtenons une structure étonnamment ordonnée : quatre points principaux alignés périodiquement le long d'un axe vertical légèrement incliné. Et des structures similaires sont obtenues dans d'autres tableaux de Jan van Eyck : *Saint Jérôme dans son étude*, *La Vierge de Lucques*, *La Vierge de Dresde* et *La Vierge dans une église*. Chacun de ces tableaux peut être partitionné en autant de bandes horizontales qu'il y a de points de fuite, chaque bande regroupant l'ensemble des arêtes associées au même point : les perspectives de Jan sont rigoureusement exactes, par morceaux.



APPLICATION DE LA MÉTHODE *A CONTRARIO* AU PORTRAIT DES ARNOLFINI. À GAUCHE : CARTE DE PROBABILITÉ DES POINTS DE FUITE TENANT COMPTE D'UNE INCERTITUDE SUR LES EXTRÉMITÉS DES ARÊTES EXTRAITES (VISIBLES EN ROUGE DANS L'IMAGE DE DROITE). À DROITE : APPLICATION DE LA MÉTHODE A CONTRARIO À CETTE CARTE DE PROBABILITÉS. LES ARÊTES EXTRAITES SONT RELIÉES AU POINT DE FUITE CORRESPONDANT, LA COULEUR DU LIEN TRADUISANT SA CONSISTANCE : DU BLEU FONCÉ AU JAUNE CLAIR POUR UNE CONSISTANCE ALLANT RESPECTIVEMENT DE 0 À 1. LES ARÊTES SE REGROUPENT PAR BANDES HORIZONTALES, DÉLIMITÉES ICI PAR DES LIGNES BLANCHES. © GILLES SIMON, UNIVERSITÉ DE LORRAINE — THE CONVERSATION

Une précision diabolique

Le cas de la Vierge dans une église est particulièrement intéressant. Dans ce tableau presque aussi petit qu'une miniature (14 x 31 cm), la précision des traits au regard de leur convergence est extrême.



RECONSTRUCTION DES POINTS DE FUITE DANS LA VIERGE DANS UNE ÉGLISE. © GILLES SIMON, UNIVERSITÉ DE LORRAINE — THE CONVERSATION

Mais le plus étonnant est que les positions des points de fuite obtenus dans la bande supérieure du tableau sont parfaitement cohérentes avec la géométrie en demi-décagone du chœur de l'église. Cela est inattendu, car personne ne pouvait savoir à cette époque comment placer un point de fuite sur la ligne d'horizon en fonction de sa direction dans l'espace tridimensionnel. La seule explication possible est que Jan utilisait un dispositif optique à travers lequel il représentait l'espace, en superposant méticuleusement ses traits à la réalité.

Une « machine à perspective » des plus avant-gardistes

Près d'un demi-siècle après la mort de Jan, **Léonard de Vinci** dessinera une version simplifiée de cette « **machine à perspective** ».

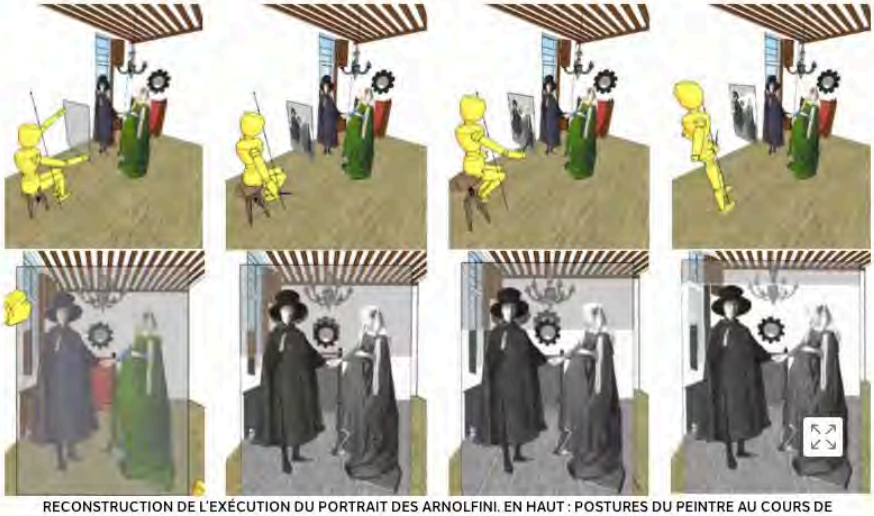
LÉONARD DE VINCI, VERS 1480. DÉTAIL DU CODEX ATLANTICUS F. 5 R, MILAN, BIBLIOTECA AMBROSIANA

Dans le dessin de Léonard, le peintre détoure les objets visibles à travers une vitre, le regard immobilisé derrière un œilleton. Plus élaboré, le dispositif de Jan comportait quatre œilletons répartis équitablement (à l'instar des points de fuite) le long d'un axe de visée incliné. Jan peignait son tableau bande après bande (œilleton après œilleton) de bas en haut ou de haut en bas. La vitre - probablement un miroir - pouvait elle-même être déplacée dans son plan, afin de raccorder au mieux, compte tenu de la parallaxe, le bord de la bande précédemment dessinée à la réalité perçue depuis l'œilleton suivant.

LA MACHINE À PERSPECTIVE DE JAN VAN EYCK : SIMULATION DE L'EXÉCUTION DU PORTRAIT D'ARNOLFINI. UNIVERSITÉ DE LORRAINE © SIMONMAGRIT, YOUTUBE

Cette étape cruciale permettait au peintre d'obtenir des transitions douces entre les

Cette étape cruciale permettait au peintre d'obtenir des transitions douces entre les bandes, difficilement décelables à l'œil nu. De surcroît, elle anticipait de plusieurs siècles le principe de la **réalité augmentée**.



RECONSTRUCTION DE L'EXÉCUTION DU PORTRAIT DES ARNOLFINI. EN HAUT : POSTURES DU PEINTRE AU COURS DE L'EXÉCUTION. EN BAS : VUES OBTENUES DEPUIS LES QUATRE ŒILLETONS. LE DESSIN SUR LA VITRE EST REPRÉSENTÉ EN NOIR ET BLANC, LA RÉALITÉ EN COULEUR. © GILLES SIMON, UNIVERSITÉ DE LORRAINE — THE CONVERSATION

Au plus près de la perception humaine

Notre reconstruction de l'exécution du portrait des Arnolfini permet de voir ce que Jan lui-même voyait à travers les œilletons, et d'observer par exemple la montée du plafond entre la vue du bas et celle du haut finalement retenue pour le plafond (et inversement pour le sol) : Jan semble avoir été soucieux d'éviter les « déformations latérales ».

VOIR AUSSI *Ce que nous racontent les craquelures de Mona Lisa*

L'amplification des déformations perspectives sur les bords du tableau n'est pas incorrecte du point de vue de l'optique, mais nous n'y sommes pas habitués parce que **le champ visuel** de l'œil humain est plus réduit que celui atteint dans une perspective artificielle à courte distance, ou à travers une vitre lorsque le peintre s'autorise à rouler des yeux et à se contorsionner pour élargir son champ visuel immédiat. Il est probable que Jan ne se satisfaisait pas de ces effets inhabituels, et qu'il ait préféré peindre à l'état naturel de repos les objets situés en face de lui, quitte à relever son **tabouret** en cours d'exécution et à terminer debout pour atteindre l'ensemble de l'espace visible.

Introduction de la vision binoculaire

L'inclinaison de l'axe de visée n'a sans doute pas été laissée au hasard, dans la mesure où elle était évidente à l'œil nu et compliquait le raccordement des bandes. Pour le portrait des Arnolfini, la distance horizontale entre les œilletons situés aux extrémités de l'axe de visée était égale à la distance interpupillaire d'un homme adulte (d'où cette impression de voir un anaglyphe dans **la réflectographie infrarouge des Époux**). Chacun décidera s'il s'agit d'une coïncidence, mais l'auteur de ces lignes parierait que non. Il imagine Jan fermant alternativement l'œil gauche et l'œil droit, observant les effets de cette action sur la perception de sa propre main et décidant de doter son dispositif des deux options.

Des chercheurs de la *National Gallery* ont souligné, à propos du portrait des Arnolfini, combien la représentation des mains et des pieds était importante à cette époque, à la fois sur le plan symbolique et esthétique. Si la plupart des objets présents dans le tableau n'ont été dessinés qu'une seule fois depuis l'œilleton le plus frontal, la main levée et les pieds de Giovanni Arnolfini ont été redessinés depuis d'autres œilletons. Les deux dessins de la main et les trois dessins des pieds sont décalés spatialement en raison de la parallaxe, mais les subtils raccords de Jan permettaient qu'ils ne le soient pas trop. Ce dernier pouvait donc

subtils raccords de Jan permettaient qu'ils ne le soient pas trop. Ce dernier pouvait donc retenir, au moment de peindre, l'une ou l'autre des déclinaisons.

Genèse du tableau

Les autres parties du corps de Giovanni ont également été dessinées plusieurs fois, et le partitionnement du tableau en bandes d'épaisseurs différentes suggère que Jan a focalisé son attention sur quatre régions d'intérêt : le plafond, la tête coiffée de Giovanni, sa main levée et le bas du corps. Un soin particulier semble donc avoir été apporté au portrait du commanditaire, plus encore qu'au cadre architectural. Et ainsi, le dispositif polyscopique de Jan pourrait bien être le fruit de l'évolution d'un dispositif monoscopique (équivalent à celui dessiné par Léonard) concomitante à la nécessité de réaliser un portrait en pied (**Adam dans Le retable de Gand** ?) après avoir réalisé des portraits en buste. Il ne s'agit là que d'une première hypothèse, qui mériterait d'être confrontée à d'autres. Encore faudrait-il que notre article ne connaisse pas le même sort que celui d'Elkins.

Nécrologie : Guy Perrier, combattant pour la Paix

29 juin 2023 - 15:43 par La rédaction Infodujour

C'est avec beaucoup d'émotion que l'Association France Palestine Solidarité de Lorraine Sud a appris le décès de son fondateur, Guy Perrier.

Guy Perrier, Association France-Palestine (DR)

Guy Perrier est né le 7 février 1950 à Saint-Claude dans le Haut-Jura. Après des études au collège de Saint-Claude, il poursuit au lycée et en prépa à Lyon. Il devient professeur de mathématique et obtient l'agrégation en 1990. Il s'intéresse ensuite à l'informatique, reprend des études et soutient une thèse de doctorat en 1995. Il est nommé enseignant-chercheur en informatique en 2005 au laboratoire Loria de l'Université de Lorraine. Il était un spécialiste reconnu du traitement automatique des langues. Depuis 2014, il continuait ses recherches en tant que Professeur Émérite de l'Université de Lorraine.

La cause d'une paix juste et durable

Parallèlement à son travail de professeur, Guy s'investit très tôt dans l'Association France Palestine Solidarité. Il y jouera un rôle très important tant au niveau national que local pour animer et développer l'association AFPS de Lorraine-Sud.
Il a été à l'origine de nombreuses actions de solidarité avec des ONG palestiniennes tant dans les camps de réfugiés du Liban, en Cisjordanie ou à Gaza. Il avait aussi de nombreux contacts avec les associations israéliennes militant pour la paix au Moyen-Orient. Il se rendait régulièrement sur place pour faire avancer les projets et soutenir inlassablement la cause d'une paix juste et durable.

Sa rigueur militante et sa combativité masquaient quelquefois sa grande sensibilité et un humanisme rare. Ses nombreux amis, tant en France qu'au Moyen-Orient, ne lui en tenaient pas rigueur, sachant son indéfectible attachement à la cause du peuple palestinien et aux Droits Humains.

Il ne verra pas la Palestine libre

Un combat qu'il a mené jusqu'à son dernier souffle puisqu'il est décédé dans un hôpital parisien quelques heures après sa participation au Conseil National de l'AFPS le 18 juin 2023.

Il ne verra pas la Palestine libre. Ici comme là-bas, ses amis pleurent un combattant fidèle et un homme dont la droiture et la pugnacité resteront un modèle d'engagement pour beaucoup de militants.

Ses obsèques auront lieu le mercredi 5 juillet à 13 h 30 au crématorium du Grand Nancy, cimetière du Sud, rue Paul Doumer à Vandœuvre. Il vivait depuis trente ans avec Mariola Ciesielska, sa compagne. Nous lui adressons toutes nos condoléances.

Nécrologie
Association France Palestine, Guy Perrier
France · Grand Est · Lorraine ·

L'Est républicain, 1er juillet 2023 (édition Nancy)

Vandœuvre-lès-Nancy ■ Nécrologie

Disparition de Guy Perrier

Nous avons appris le décès de Guy Perrier, survenu subitement, dans sa 73e année, alors qu'il avait été admis dans un hôpital parisien quelques heures après sa participation au Conseil National de l'Association France Palestine Solidarité (AFPS), le 18 juin dernier.

Guy Perrier est né en 1950 dans le Haut-Jura. Après ses études à Saint-Claude, il poursuit une prépa à Lyon, avant de devenir professeur de mathématique. Il obtient l'agrégation en 1990, s'intéresse ensuite à l'informatique, reprend des études et soutient une thèse de doctorat en 1995. Il est nommé enseignant-chercheur en informatique en 2005 au laboratoire Loria de l'Université de Lorraine. Il était un spécialiste reconnu du traitement automatique des langues. Depuis 2014, il continuait ses recherches en tant que Professeur Émérite de l'Université de Lorraine.

Parallèlement à son travail, Guy s'est investi très tôt dans l'Association France Palestine Solidarité. Il y jouera un rôle très important, tant au niveau national que local, pour animer et développer l'association AFPS de Lorraine-Sud.

Humanisme rare

Il a été à l'origine de nombreuses actions de solidarité avec des ONG palestiniennes, tant dans les camps de réfugiés du

Liban qu'en Cisjordanie et à Gaza. Il avait aussi de nombreux contacts avec les associations israéliennes, militant pour la paix au Moyen-Orient. Il se rendait régulièrement sur place pour faire avancer les projets et soutenir inlassablement la cause d'une paix juste et durable.

Sa rigueur militante et sa combativité masquaient quelquefois sa grande sensibilité et un humanisme rare. Ses nombreux amis, tant en France qu'au Moyen-Orient, admiraient son indéfectible attachement à la cause du peuple palestinien et aux droits humains. Guy partageait sa vie avec Mariola Ciesielska, son épouse, depuis une trentaine d'années, et résidait à Vandoeuvre.

Ses obsèques auront lieu le mercredi 5 juillet, à 13 h 30, au crématorium du Grand Nancy, 12 avenue Paul-Doumer à Vandoeuvre.

Nos condoléances.

L’Est républicain, Le Républicain lorrain, Vosges matin, 9 juillet 2023

Grande Région

Un outil franco-allemand de modération contre la haine en ligne

Les chercheurs en sciences humaines et informatiques se sont associés, trois années durant, en Lorraine et en Allemagne, pour mettre au point un modérateur de messages de haine sur les médias et autres réseaux en ligne. Il est, pour l'heure, le meilleur sur le marché !

C'est la règle. À l'intérieur de nos frontières européennes, les médias et plateformes internet ont l'obligation de supprimer les messages haineux dans les 24 heures suivant leur mise en ligne… Une injonction forcément difficile à faire appliquer au quotidien, alors que le déversoir a depuis longtemps pris des allures de puits sans fond. Une problématique à laquelle se sont attaquées deux disciplines de l'Université de Lorraine, de Mayence et Sarrebruck en Allemagne : les « sciences de l'information et de la communication » et les « sciences de l'informatique ». Côte à côte, durant trois ans, les chercheurs sont parvenus à mettre au point un outil, sorte de modérateur, permettant de nettoyer aussitôt la toile de ses commentaires illicites.

« Jusqu'ici, aucun corpus similaire n'a existé », explique Angeliki Monnier, directrice du Crem (Centre de recherche en économie et management), enseignante en information et communication, pour l'Université de Lorraine.

Un modérateur mis au point par le programme M-Phasis pour lutter contre la haine sur les réseaux sociaux. Photo Hugo Azmani

« C'est assez exceptionnel, un tel dispositif binational et interdisciplinaire. Avec une collecte de messages (près de 10 000 au total, N.D.L.R.) sur des sites français et allemands. Cela nous a permis de comprendre comment cette haine s'exprime sur les deux territoires. Nous avons travaillé surtout sur les sites des médias « mainstream » (grand public, N.D.L.R.), sur Twitter ainsi que sur des sites politiques. Sur ces trois années de travail, nous avons constaté que dans le couloir des médias, il devenait de plus en plus compliqué de trouver ces messages, effacés rapidement. »

Définir la haine

Dans un premier temps, c'est la définition même d'un écrit haineux qu'il a fallu établir. « Effectivement, car selon l'endroit où nous le trouvons, sa définition diffère. Il prend un nouveau visage. On remarque des stratégies pour contourner l'interdit : l'ironie, le sarcasme qui offrent plusieurs niveaux de lecture. Ceux sans équivoque appellent à des agressions pures et simples. »

De leur côté, les informaticiens, comme Irina Illina, ont apporté leur écot en mettant au point un système d'annotations face à chaque message considéré comme haineux. « Cela nous a permis d'obtenir des résultats d'une grande finesse, justement pour cibler les discours de haine implicite. Nous avons ainsi créé un programme permettant de les détecter, avec des algorithmes, évidemment. Notre travail a porté essentiellement sur les messages textuels et toutes les données provenant des journaux en ligne, les articles et commentaires. »

En libre accès

Le modérateur né de ce programme franco-allemand baptisé M-Phasis est aujourd'hui en libre accès, à la disposition des entreprises, de toutes les plateformes mais également des chercheurs qui pourront l'améliorer, en ligne. « On dit qu'il est aujourd'hui le plus performant mais cela ne durera pas longtemps s'il n'est pas travaillé. Comme tout ce qui touche aujourd'hui au numérique. »

● **Saada-Gisèle Sebaoui**

VIDÉO. La cryptographie, science qui code et déchiffre le quotidien

La cryptographie est la science des codes secrets, que l'on appelle aussi chiffrement.

Ouest-France
Nicolas BLANDIN

Publié le 31/08/2023 à 09h11

Le laboratoire Loria de l'Inria de Nancy est spécialisé dans la cryptographie.

Grand Est

Vulnérabilité du vote électronique à distance : des solutions made in Lorraine

Deux chercheurs lorrains ont découvert des failles et des vulnérabilités dans le vote électronique à distance des Français de l'étranger à l'occasion des législatives 2022. Ils ont proposé des solutions pour y remédier.

Lucca Hirschi et Alexandre Debant, chercheurs de l'Institut national de recherche en sciences et technologies du numérique au Laboratoire lorrain de recherche en informatique et ses applications. Photo Patrice Saucourt

Le vote électronique à distance lors d'élections politiques agite la société depuis des années. Les pour, les contre, les méfiants… En 2022, lors des élections législatives, les Français résidant à l'étranger ont eu la possibilité d'utiliser ce moyen pour choisir leur député. L'occasion pour Alexandre Debant et Lucca Hirschi, chercheurs de l'Institut national de recherche en sciences et technologies du numérique au Laboratoire lorrain de recherche en informatique et ses applications à l'Université de Lorraine de procéder à des tests pour savoir si le vote, par ce système, garantissait le secret et l'intégrité des résultats conformément à la loi.

Ce sont « nos collègues, Véronique Cortier, Pierrick Gaudry et Stéphane Glondu (NDLR : qui développe la plate-forme de vote Belenios) qui ont été mandatés pour la mise en place d'un outil « tiers de confiance » », confient-ils. Quelques semaines avant le début des votes, « une description partielle du protocole a été publiée. On est curieux, on est allé voir ! » Les deux chercheurs s'en sont donc saisis « pour comprendre comment ça fonctionnait ».

Attaque sans laisser de traces

Alexandre Debant et Lucca Hirschi ont travaillé pour tester leurs hypothèses. Là, ils ont constaté des failles et des vulnérabilités dans le système de vote.

D'abord, « personne ne doit savoir pour qui j'ai voté », c'est le secret du vote. En ce cas, le chiffrement se fait via une clef « donnée à plusieurs personnes qui ont des bouts de cette clef », soulignent-ils. « Il y a onze élections dans onze circonscriptions. Un attaquant pourrait mettre, par exemple, un bulletin prévu pour Sidney à Minsk ou dans une circonscription consulaire où il y a très peu de votants. Il va savoir, avec une bonne probabilité, pour qui j'ai voté ».

Bien sûr, ces attaques ne pourraient émaner de néophyte en la matière, « ce n'est pas donné à tout le monde, mais ça ne demande pas un très haut niveau de technicité ». De plus, « si un attaquant existe, il attaque sans laisser de traces ». D'ailleurs, ils ne peuvent pas dire, si ces élections de 2022 ont subi ou non des attaques qui auraient exploité ces failles de sécurité.

« Le gros du danger est inexistant en 2023 »

Quant à la vérifiabilité du vote, il s'agit de savoir s'il n'y a pas eu de « modification du bulletin car, une fois que j'ai cliqué sur « voter », je ne sais plus ce qui se passe ». Un reçu Pdf est envoyé au votant avec « un code associé à mon intention de vote. À la fin de l'élection, je peux me connecter sur le site » pour vérifier que le bon bulletin est dans la bonne urne. « On a analysé le pdf » et les chercheurs se sont aperçus que le vote pouvait être modifié mais que le reçu envoyé au votant portait bien les bonnes informations. Un problème dû « à un bug ».

En tout, deux failles majeures… qui ont été réparées. En effet, les chercheurs, qui ont signalé ces failles et ont participé à deux réunions « avec le ministère des Affaires Étrangères, l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et le prestataire » chargé de mettre en place le système de vote. En 2023, des législatives partielles ont été organisées pour les Français de l'étranger dans les circonscriptions où le scrutin avait été annulé par le Conseil constitutionnel. Différentes options avaient été proposées par Alexandre Debant et Lucca Hirschi qui sont retournés voir… Les failles avaient été réparées : « Ils ont choisi des options raisonnables. Le gros du danger était inexistant en 2023 ».

● **Frédéric Plancard**

« Il faut penser comme un attaquant ! »

Bien sûr, la sécurisation des votes électroniques « peut toujours être améliorée », expliquent Alexandre Debant et Lucca Hirschi. Par exemple, en faisant qu'un vote électronique soit conforme pour la confidentialité et l'intégrité du résultat, même si la machine du votant est corrompue. Il faut quand même que l'expérience utilisateur soit satisfaisante, que le « système soit utilisable par tous et qu'il ne soit pas trop long et trop compliqué ».

On le voit, « le problème du vote électronique est complexe et il n'y a pas de solutions satisfaisantes », poursuivent-ils. Pour le vote électronique, « détecter une fraude est plus difficile que pour une banque en ligne » et le risque « est souvent mal perçu ». Pour tester ces systèmes, « il faut penser comme un attaquant ! », poursuivent-ils.

Rappelons qu'en France, le vote électronique à distance est interdit pour les votes politiques quand le corps électoral inclut la métropole.

Et le vote pour les primaires ?

Concernant le vote sur des machines à vote, « le reçu est imprimé sur la machine et c'est la même problématique qui se pose ». Les machines à voter sont en outre, placées sous moratoire depuis 2008 ce qui altère d'autant plus la sécurisation.

Pour les chercheurs, le problème du vote électronique est complexe et il n'y a pas de solutions satisfaisantes. Photo d'archives Lionel Vadam

« Un autre enjeu, ce sont les primaires », confient les deux chercheurs. Ce vote est utilisé par les partis politiques pour désigner, par exemple, un candidat à la présidentielle. « C'est une zone grise », évoquent Alexandre Debant et Lucca Hirschi. Il a déjà été constaté qu'il y a eu « des systèmes qui étaient des passoires ».

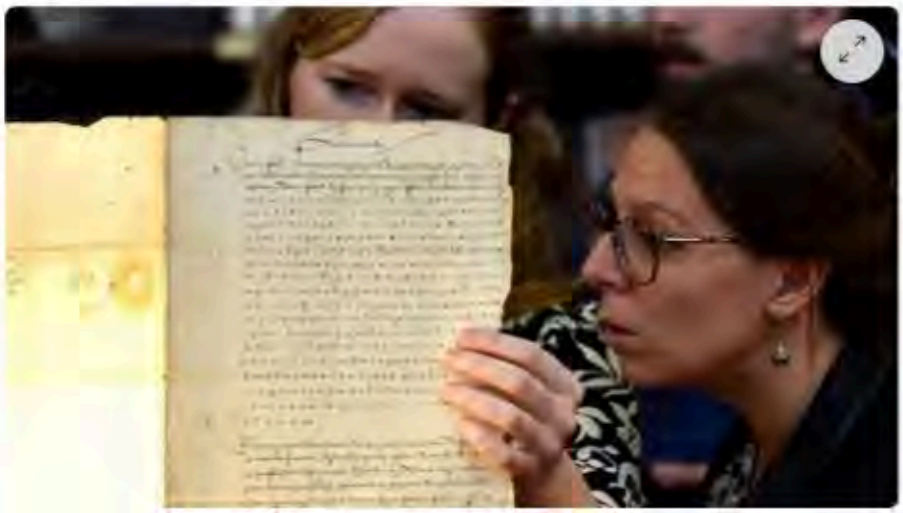
Les deux chercheurs qui travaillent sur la conception et la vérification de protocoles cryptographiques, le vote électronique en étant un, ont présenté leurs travaux dans ce domaine dans de prestigieuses manifestations. Cet été, c'est au colloque Usenix Security de Los Angeles que leurs résultats ont été évoqués. En mars, c'était au Real world crypto symposium de Tokyo.

● **F.P.**

La cryptographie, des algorithmes au cœur du quotidien... et des historiens

En apparence bien obscure, cette science fortement imprégnée de mathématiques présente de multiples applications concrètes. Dans la vie courante et pour les chercheurs en histoire.

Ouest-France
Nicolas BLANDIN.
Publié le 07/09/2023 à 10h30

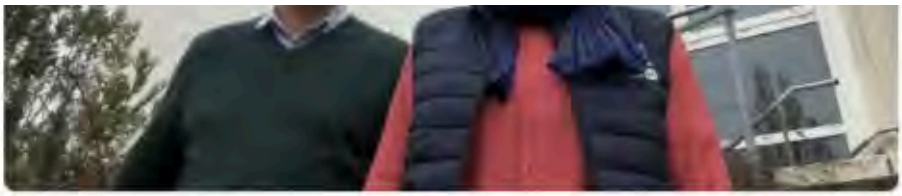


Cécile Pierrot, chargée de recherche à l'Inria de Nancy (Loria) et Camille Desenclos, maîtresse de conférences en histoire moderne, ont percé les secrets d'une lettre chiffrée de Charles Quint datant de 1547. | JEAN-CHRISTOPHE VERHAEGEN / AFP

La cryptographie est la science des codes secrets, que l'on appelle aussi chiffrement. Pour pouvoir comprendre un message ou une communication, il faut en connaître la clé. « **Un peu comme pour ouvrir un cadenas de vélo** », résume Aurore Guillevic, chargée de recherche Inria dans l'équipe Caramba de Nancy (Loria), spécialisée dans la cryptographie.

« La cryptographie a aidé à faire naître l'informatique »

Un algorithme permet de créer ces codes, c'est un peu le mécanisme qui se cache derrière l'antivol. « **C'est notre métier : on travaille à trouver les bons algorithmes.** » La cryptanalyse, c'est l'art du déchiffrement de ces codes sans avoir la clé.



Emmanuel Thomé, directeur de recherche, et Aurore Guillevic, chargée de recherche CNRS dans l'équipe Caramba de l'Inria de Nancy (Loria), spécialisée dans la cryptographie. | OUEST-FRANCE

« À Nancy, notre spécialité, c'est le vote électronique, sur lequel nous travaillons avec des start-up. C'est utile par exemple lors d'assemblées générales à distance pour remplacer le vote par correspondance », remarque Emmanuel Thomé, directeur de recherche au Loria. L'une des applications les plus concrètes est aujourd'hui, c'est la carte bancaire.

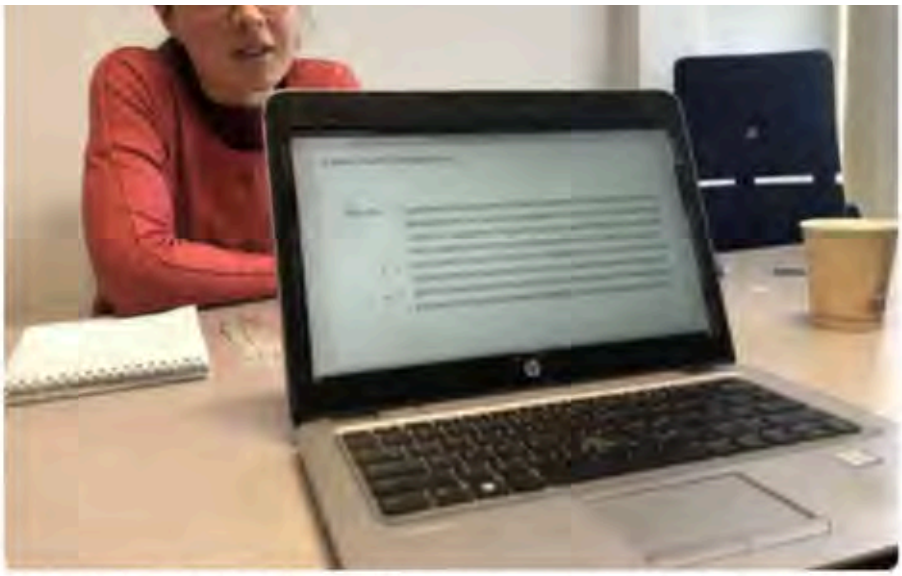
Car **« la cryptographie a aidé à faire naître l'informatique »**. Il n'y a pas de commerce électronique sans cryptographie, qui assure la sécurité de la transaction. Mais elle s'invite dès que l'on surfe sur Internet. **« Dès lors qu'il y a une identification pour accéder à sa boîte mail par exemple, il y a de la cryptographie. »**Autre application plus étonnante, **« en chimie, la crypto aide à trouver des polluants dans l'air »**, relève Aurore Guillevic.

« Il est nécessaire d'actualiser l'exigence de sécurité »

« « »Si on prend l'analogie de la maison, nous sommes des spécialistes de la porte blindée. Et le piratage est plus souvent une question de fenêtre ouverte que de porte blindée forcée » », sourit Emmanuel Thomé. Autrement dit le danger est le plus souvent lié à une erreur humaine : quelqu'un qui laisse entrer le voleur. La sécurité a évolué au fur et à mesure des avancées technologiques.

Le chiffrement que l'on met parfois quand on est enfant – par exemple en utilisant une lettre de l'alphabet pour une autre – est assez simple à contourner. **« Aujourd'hui, à mesure que les moyens de calcul des attaquants monte, il est nécessaire d'actualiser l'exigence de sécurité. »** Des agences internationales, comme l'Agence nationale de sécurité des systèmes d'information (Anssi) en France, actualisent le degré de sécurité requis. C'est la raison pour laquelle vos mots de passe doivent être de plus en plus compliqués !

Lire aussi : Apple veut faire disparaître les mots de passe, voici comment



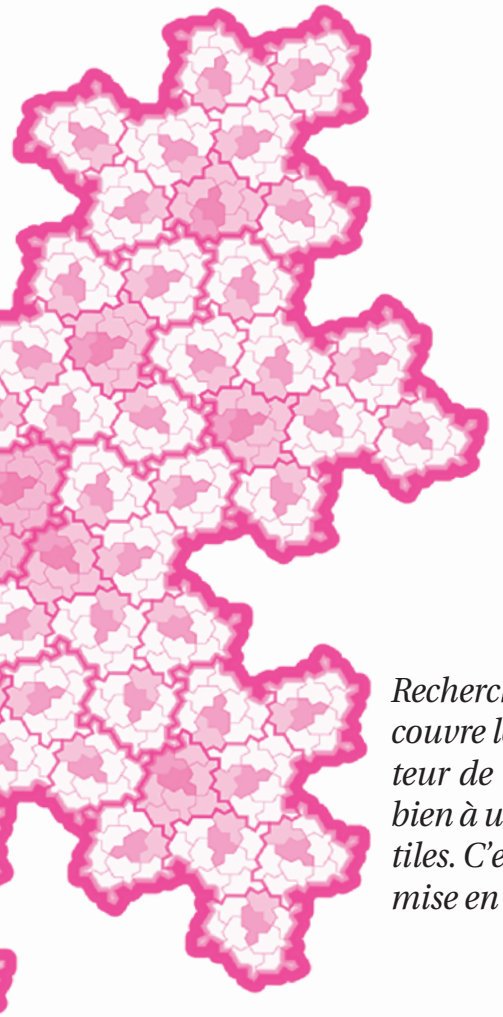
Aurore Guillevic, chargée de recherche Inria dans l'équipe Caramba de Nancy (Loria), spécialisée dans la cryptographie. | OUEST-FRANCE

Des applications pour l'histoire

La cryptographie est un étonnant allié des historiens. Nombre de documents nécessitant une certaine discrétion étaient rédigés en respectant un code dont la clé n'était connue que de ceux à qui ils s'adressaient. C'est par exemple le cas de correspondances diplomatiques comme la lettre de Charles Quint, empereur du Saint-Empire, envoyée en 1547 à son ambassadeur en France. Cette suite de quelque 120 symboles différents n'a été déchiffrée qu'en 2022, avec l'aide des puissants ordinateurs du laboratoire Loria de l'Inria de Nancy (Meurthe-et-Moselle). **« On apprend que quelqu'un essaie de tuer Charles Quint »**, indique Cécile Pierrot, chargée de recherche au Loria. Elle apporte un éclairage sur les relations tendues entre le roi François 1er et le puissant empereur.

En février, une équipe de trois cryptologues du projet international DECRYPT a déchiffré des lettres de Marie Stuart, reine d'Ecosse, décapitée en 1587. Une cinquantaine de lettres chiffrées, écrites entre 1578 et 1584 durant sa captivité en Angleterre, classées par erreur à la Bibliothèque nationale de France comme étant originaires de la première moitié du XVIe siècle en Italie. D'abord, les cryptologues ont compris que le texte n'était pas en italien mais en français. Des phrases comportant **« ma liberté »** et **« mon fils »** suggéraient une mère emprisonnée. Dans ces lettres, elle plaide sa cause avec diplomatie, se livre à quelques ragots, se plaint de ses conditions de captivité et exprime sa détresse après l'enlèvement de son fils.

Sciences Histoire Culture Actualité en continu



La tuile qu'on n'attendait plus

Recherchée depuis plus d'un demi-siècle, une pièce de puzzle unique, qui couvre le plan sans répétition, a été découverte récemment par un amateur de mathématiques britannique. La preuve que cette tuile aboutit bien à un pavage dit « apériodique » met en jeu des mathématiques subtiles. C'est en fait toute une famille de tuiles apériodiques qui a ainsi été mise en évidence. Les spécialistes du domaine saluent la performance.

Pour fabriquer un puzzle, on prend une surface que l'on découpe en morceaux, de sorte que le recouvrement ultérieur de la surface par les pièces est garanti. La question inverse est moins évidente : pour un jeu de pièces données, à quelles conditions couvrent-elles le plan ? C'est le problème général du pavage. Paver le plan de manière périodique est assez facile : des pièces carrées toutes identiques, par exemple, recouvrent complètement le plan. On connaît des collections de pavages périodiques avec des motifs variés, à l'aide de polygones ou d'autres formes dont les qualités décoratives se retrouvent partout, dans les pavages de l'Égypte ancienne, les mosaïques islamiques et jusque dans le carrelage de votre salle de bains. L'obtention d'un pavage apériodique – où il n'existe pas de symétrie par translation – nécessite à l'inverse des constructions assez techniques et avec plusieurs pièces. Et imaginer que l'on puisse le faire avec une seule pièce – une unique tuile – paraissait hors de portée. C'était devenu le graal du domaine. Les spécialistes avaient nommé cette pièce hypothétique « ein Stein » (une pierre en allemand, avec un calembour sur le nom du célèbre physicien allemand). Dans la communauté mathématique, même si elle était recherchée activement, nombre de spécialistes pensaient même qu'une telle pièce n'existait pas.

Coup de théâtre au printemps 2022 : un article exhibant une telle pièce apparaît sur le serveur de prépublication ArXiv ; elle est en forme de chapeau. Les spécialistes des pavages s'enflamment : tout le monde analyse le papier qui est vite jugé pertinent (1). Toutefois, si vous voulez carreler votre salle de bains de manière apériodique, dans l'absolu, deux tuiles différentes

◀ *Pavage partiel du plan avec la tuile en forme de spectre. Le regroupement de deux tuiles en une forme symétrique et des règles de substitution ont aidé à prouver que le pavage était apériodique.*

D. SMITH, J.S. MYERS, C.S. KAPLAN, C. GOODMAN-STRAUSS

Le Britannique David Smith, qui a découvert la fameuse tuile apériodique, est un technicien de l'imprimerie à la retraite, amateur de jeux mathématiques, de puzzles et de formes fractales

restent indispensables, puisque ce pavage nécessite non seulement des translations, mais aussi une symétrie. Autrement dit, c'est la pièce et la même pièce retournée qui pavent le plan, et formellement pas une pièce unique – même si les mathématiciens disent qu'il s'agit d'une pièce « à la symétrie près ». Deux mois plus tard, nouveau coup de théâtre, puisque la même équipe annonce avoir corrigé ce petit défaut : ils ont bien découvert une tuile unique couvrant le plan de façon apériodique (2).

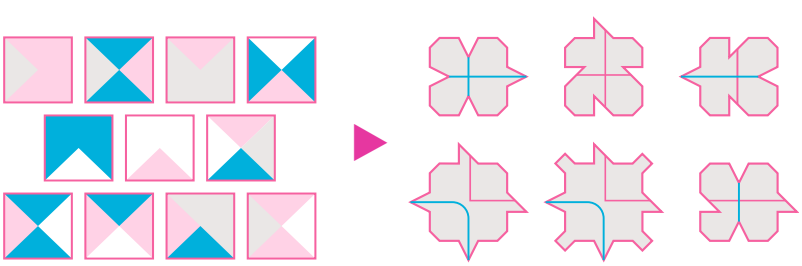
Ce qui surprend le plus, c'est que la pièce en question, que les auteurs ont baptisée « spectre », est assez simple. « *Cette simplicité et le fait que cette "tuile" n'ait pas été trouvée auparavant témoignent de notre compréhension encore très partielle de la naissance de l'apériodicité dans le plan* », confie Thomas Fernique, chercheur CNRS au Laboratoire d'informatique de Paris-Nord, à Villetaneuse. En d'autres termes, comment peut-on, à partir de règles locales, forcer un recouvrement apériodique du plan ?

Les pavages fascinent, car ils représentent un réservoir inépuisable de questions mathématiques. C'est par ailleurs l'un des rares domaines des mathématiques – sinon le seul – où, sans besoin d'un bagage théorique, amateurs et artistes se sont illustrés, en découvrant de nouveaux pavages avec des propriétés intéressantes. Cette percée l'illustre une nouvelle fois, puisque le Britannique David Smith, qui a découvert la fameuse tuile apériodique, est un technicien de l'imprimerie à la retraite, amateur de jeux mathématiques, de puzzles et de formes fractales.

Qu'est-ce qu'un pavage bidimensionnel ? C'est un recouvrement – sans trou – du plan euclidien avec une ou plusieurs pièces. Et c'est un recouvrement qui va jusqu'à l'infini, comme un puzzle que l'on imagine se poursuivre dans toutes les directions ! Si l'on essaye de paver le plan par translation d'une seule pièce utilisable autant de fois que l'on veut, alors de tels pavages sont possibles, à condition que la pièce soit un pseudo-hexagone (un hexagone qui peut être déformé) ; un tel pavage est périodique ou semi-périodique (invariant par certaines translations). En d'autres termes, on obtient un pavage dont le motif se répète à l'infini (les mathématiciens disent que le pavage admet une

RÉDUIRE LE NOMBRE DE PIÈCES

À partir des années 1960, on découvre des ensembles de tuiles qui pavent le plan euclidien de manière apériodique. De tels pavages sont composés d'une unité fondamentale qui se répète à l'infini sans symétrie de translation. Au fil des ans, le nombre de pièces nécessaires s'est réduit, jusqu'à une unique tuile, mais qui n'est pas d'un seul tenant. On a représenté ici quelques-uns de ces ensembles parmi les dizaines qui ont été mis en évidence au fil du temps.



1966-2015 TUILES DE WANG

Les tuiles de Wang s'assemblent comme des dominos. En 1966, il en fallait 20 426 différentes pour obtenir un pavage apériodique. En 2015, Emmanuel Jeandel et Michaël Rao trouvent cet ensemble minimal de onze tuiles.

1969 TUILES DE ROBINSON

Cet ensemble de six tuiles pave le plan de manière apériodique, en créant une hiérarchie infinie de réseaux carrés.

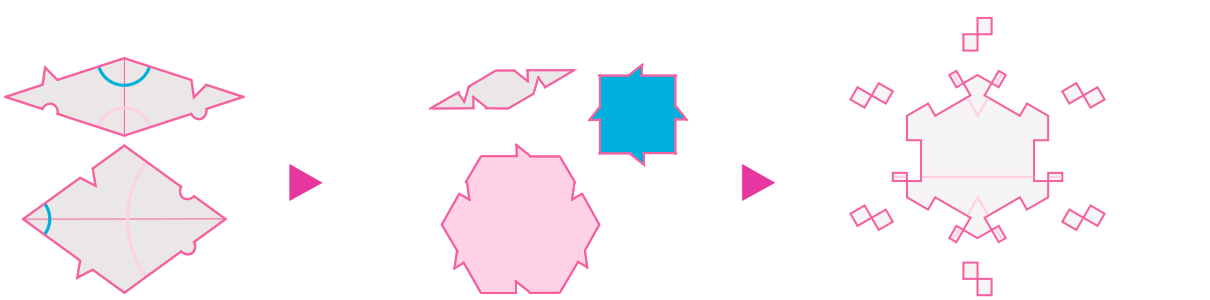
SOURCE : E. JEANDEL ET M. RAO, *ADV. COMB.*, DOI : 10.19086/AIC.18614, 2021

isométrie par translation). Ce résultat de 1990 est dû aux mathématiciens français Danièle Beauquier et Maurice Nivat (3). « *En autorisant seulement des translations, le pavage obtenu est forcément un pseudo-hexagone, et c'est très loin de faire quelque chose de compliqué* », explique Emmanuel Jeandel, professeur à l'université de Lorraine, à Vandœuvre-lès-Nancy. Ainsi, la plupart des pavages sont périodiques, et forcer l'apériodicité n'est pas chose aisée car, très vite, des structures complexes apparaissent. Dans la première partie du XX^{e} siècle, on ne connaissait d'ailleurs que des pavages périodiques.

TRANSLATION, ROTATION ET SYMÉTRIE

Un détour par un problème connexe permettra de mieux saisir la difficulté sous-jacente : le problème des dominos. En 1961, le logicien sino-américain Hao Wang (1921-1995) propose d'utiliser des carrés de taille identique avec des secteurs colorés pour paver le plan. La question qu'il se posait était : peut-on savoir si une collection donnée de tels carrés colorés – aujourd'hui nommés « tuiles de Wang » – peut paver le plan ? Travaillant sur ce problème des dominos, qui a des liens avec des questions de décidabilité algorithmique (problème de l'arrêt de Turing), l'Américain Robert Berger, étudiant de Wang, découvre en 1963 le premier pavage apériodique, qui nécessite 20 426 tuiles de Wang différentes… Ce pavage apériodique est un ingrédient clé de la preuve que le problème des dominos est indécidable : on ne peut pas construire un algorithme qui puisse y répondre. Au fil des ans, le nombre de tuiles nécessaire à la construction d'un pavage apériodique a été réduit. Tout d'abord à 104 tuiles, par Robert Berger lui-même, puis à 40 par le Suisse Hans Läuchli. En 1969, le mathématicien américain Raphaël M. Robinson s'inspire des tuiles de Wang pour créer un ensemble de six tuiles polygonales dont le recouvrement du plan est apériodique en utilisant la translation, la rotation et la symétrie (réflexion) (4).

Le Britannique Roger Penrose (prix Nobel de physique en 2020 pour sa contribution à la relativité générale et à la physique des trous noirs) commence à s'intéresser aux pavages dans les années 1970. En décomposant un pentagone en six pentagones plus petits et cinq demi-losanges fins, et en répétant le processus, il remarque qu'il peut combler la place restante avec d'autres formes : étoile, losange, pentagone et bateau. C'est ainsi qu'il obtient son premier pavage apériodique constitué de six pièces (trois pentagones, une étoile, un losange et un bateau). Par la suite, il met en évidence deux autres pavages apériodiques, mais toujours constitués de deux pièces différentes. En 1982, lorsqu'on découvre expérimentalement des matériaux qui n'ont pas



1978 PAVAGE DE PENROSE

Voici un des trois ensembles de tuiles apériodiques proposés par Roger Penrose, futur prix Nobel de physique (en 2020).

1989 TUILES DE SOCOLAR

En explorant les « quasi-cristaux », le physicien Joshua Socolar a découvert cet ensemble de trois tuiles dont l'assemblage forme un pavage apériodique avec une symétrie d'ordre 12 (symétrique par rotation d'un douzième de tour).

2010 TUILE DE SOCOLAR ET TAYLOR

Première monotuile apériodique, qui a toutefois le défaut de ne pas être d'un seul tenant.

Deux preuves valent mieux qu'une

Une fois démontré que votre tuile pave tout le plan, ce qui est la partie en général la plus facile, il faut aussi s'assurer que tous les pavages obtenus avec cette tuile sont apériodiques. Pour cela, les auteurs ont proposé deux démonstrations. La première consiste à essayer toutes les configurations possibles. C'est une preuve énumérative obtenue avec l'aide de l'ordinateur : on teste tous les cas et on aboutit à la conclusion que cela s'arrange toujours de manière apériodique. *« C'est une preuve classique de "force brute", mais qui n'est pas très satisfaisante en termes de compréhension,* confie Emmanuel Jeandel, professeur à l'université de Lorraine. *Les auteurs présentent toutefois une seconde preuve très élégante. »* Il s'agit d'un raisonnement par l'absurde en utilisant des déformations des tuiles. L'idée est de déformer continûment la tuile chapeau de deux façons pour aboutir à deux nouveaux pavages avec des tuiles plus simples. *« Leur argument est que s'il y avait une période pour la tuile chapeau, elle se répercuterait pour les deux nouveaux pavages plus simples. Or ils montrent que c'est incompatible »*, explique Nathalie Aubrun, chercheuse CNRS au Laboratoire d'informatique d'Orsay. Ph. P.

▲ *C'est en déformant la tuile chapeau que les auteurs sont parvenus à trouver la pièce en forme de spectre qui pave le plan de manière apériodique. Les déformations peuvent être différentes, de sorte que c'est toute une famille de pièces de type spectre qui a cette propriété.*

la régularité des cristaux, on s'aperçoit que ces « quasi-cristaux » ont des structures analogues aux pavages de Penrose. Les motifs résultants sont donc des pavages apériodiques qui présentent des symétries d'ordre 5 – on retrouve le même motif par une rotation d'un cinquième de tour, comme pour un pentagone régulier. Cela leur confère un aspect esthétique certain, de sorte qu'ils sont devenus très populaires : on les trouve aujourd'hui couramment en architecture et comme motif de décoration.

L'ÉTUDE DES QUASI-CRISTAUX

Dans les années 1980 et 1990, plusieurs ensembles de tuiles couvrant le plan euclidien de manière apériodique sont découverts. C'est le cas, en particulier, du pavage de Socolar, du nom du physicien américain Joshua Socolar, qui a mis en évidence ce pavage en 1989 en étudiant les quasi-cristaux. Il s'agit de trois tuiles – un losange allongé, un carré et un hexagone – avec des encoches qui contraignent les assemblages. En 2010, le même Socolar s'associe avec Joan Taylor pour proposer la première monotuile apériodique (5). C'est un grand pas, puisqu'on peut effectivement recouvrir ainsi le plan de manière apériodique, mais la pièce en question n'est pas connexe, c'est-à-dire qu'elle est constituée de plusieurs morceaux non connectés. Si l'on pense en termes de carreaux de carrelage, ce n'est pas très facile à fabriquer… Cette tuile de Socolar-Taylor est une nouvelle illustration du fait que des amateurs de mathématiques peuvent contribuer à la recherche dans ce domaine, puisque Joan Taylor, qui habite en Tasmanie (Australie), n'est pas mathématicienne, mais s'est prise de passion pour les pavages apériodiques après un seul regard sur un pavage de Penrose. Elle s'est alors mise à explorer le domaine, faisant quantité de dessins, avant de trouver une tuile hexagonale particulière qui lui montrait qu'elle s'approchait du but. *« Cette découverte a été partagée et étendue avec Joshua Socolar en 2009 et publiée par la suite »*, explique-t-elle sur son site, où elle a posté nombre de ses dessins – faits à la main –, qu'elle propose comme source d'inspiration pour toutes les personnes souhaitant explorer les pavages (6).

L'exploration des formes et des pavages était aussi l'une des activités préférées de David Smith. Mais, contrairement à Joan Taylor, il utilisait un logiciel nommé PolyForm Puzzle Solver. Lorsqu'en novembre 2022, il construit une tuile en forme de chapeau assez simple d'apparence, il s'amuse à tenter de remplir le plan à l'aide de l'ordinateur avec des copies de cette tuile.

D. SMITH, J.S. MYERS, C.S. KAPLAN, C. GOODMAN-STRAUSS

« C'est le problème de Heesch, explique Nathalie Aubrun, chercheuse CNRS au Laboratoire interdisciplinaire des sciences du numérique, à Orsay. *On part d'une tuile donnée et on cherche à paver autour d'elle avec des copies de la tuile : le nombre de Heesch est le nombre maximum de circonférences que l'on parvient à faire autour de la tuile de départ avant d'être bloqué. On sait qu'on arrive à atteindre une, deux, trois, quatre, cinq et six circonférences mais, au-delà, c'est un problème ouvert. »* Là, surprise : la tuile en forme de chapeau découverte par David Smith et son symétrique continuaient de paver le plan très loin, bien au-delà de six circonférences… Aussitôt, il fait part de sa découverte à Craig Kaplan, professeur d'informatique à l'université de Waterloo, au Canada, qui commence à étudier ce pavage. Le 20 mars 2023, la prépublication annonçant ce premier pavage apériodique à l'aide de cette pièce en forme de chapeau est mise en ligne, signée conjointement avec deux autres spécialistes reconnus des pavages, Chaim Goodman-Strauss, qui travaille au musée national des mathématiques de New York, et Joseph Samuel Meyer.

Là, surprise : la tuile en forme de chapeau et son symétrique continuaient de paver le plan bien au-delà de six circonférences

DÉMONTRER QUE TOUS LES PAVAGES OBTENUS SONT APÉRIODIQUES

Une fois la tuile exhibée, encore faut-il prouver qu'elle recouvre bien le plan de manière apériodique. En premier lieu, il faut démontrer que la tuile (et son symétrique) permet de paver tout le plan jusqu'à l'infini. Pour cela, les auteurs utilisent des techniques connues à base de substitution pour construire un pavage qui possède une invariance d'échelle (un peu comme une fractale), laquelle est incompatible avec une invariance par translation. *« La seconde partie de la preuve consiste à s'assurer que tous les pavages possibles (et pas seulement celui construit dans la première partie de la preuve) présentent cette invariance d'échelle, autrement dit que tous les pavages obtenus sont bien apériodiques,* explique Nathalie Aubrun. *Les auteurs proposent deux démonstrations : l'une aidée par ordinateur, qui explore de manière systématique toutes les possibilités, mais aussi une autre preuve originale, que je trouve très élégante, qui se fait par l'absurde, en déformant le chapeau, et via laquelle ils aboutissent à une incompatibilité qui permet de conclure »* (lire l'encadré p. 74).

Pour couronner le tout, le 28 mai 2023, un autre article est publié, par la même équipe, sur arXiv, présentant une déformation du chapeau pour aboutir au « spectre », cette fameuse tuile apériodique – en fait une famille de tuiles apériodiques –, qui ne nécessite pas de retournement. *« Ce n'est qu'après avoir publié le premier article sur la tuile en forme de chapeau que nous nous sommes rendu compte de l'existence possible d'une mono-tuile chirale »*, confie Dave Smith.

Finalement, si ces tuiles – le chapeau et le spectre – ont un aspect simple, de sorte qu'on peut s'étonner qu'elles n'aient pas été découvertes auparavant, elles font partie d'un « univers » d'une infinité de tuiles, ce qui explique la difficulté à trouver la bonne. *« Même lorsque vous avez ces tuiles sous les yeux, ce n'est pas si évident de voir qu'elles ont cette propriété d'apériodicité. Depuis que je m'intéresse aux pavages, je me suis souvent dit : "Le monde des pavages est plein de surprises et c'est pour cela que j'aime ce domaine" ; c'est aussi sans doute pour cela qu'il y a tant d'amateurs qui s'y plongent et trouvent des "trucs" »*, confie Michaël Rao, de l'ENS Lyon. Le monde des pavages n'a pas fini d'être exploré, mais même s'il reste quantité de problèmes ouverts, vous pouvez désormais carreler votre salle de bains ou votre cuisine de manière apériodique avec un seul carreau ! ■

Philippe Pajot

(1) D. Smith *et al.*, arXiv:2303.10798, 2023.
(2) D. Smith *et al.*, arXiv:2305.17743, 2023.
(3) D. Beauquier et M. Nivat, *Proc. Of the 6th Ann. Symp. On Com. Geometry,* 1990.
(4) R. M. Robinson, *Math. Ann., 179,* 296, 1969.
(5) J. E. S. Socolar et J. M. Taylor, *J. Comb. Theory A, 118,* 2207, 2011.
(6) http://taylortiling.com/

POUR EN SAVOIR PLUS

■ La découverte de cette tuile apériodique a déclenché un engouement sans précédent. Des pièces de Lego et des pièces de carrelage ont été créées, et un festival s'est tenu en juillet 2023 à l'université d'Oxford : https://sites.google.com/view/thegrimmnetwork/hatfest

■ Les auteurs ont aussi créé un site où ils proposent quantité de ressources, comme des logiciels pour faire ses propres pavages, des articles, des vidéos : https://cs.uwaterloo.ca/~csk/spectre/

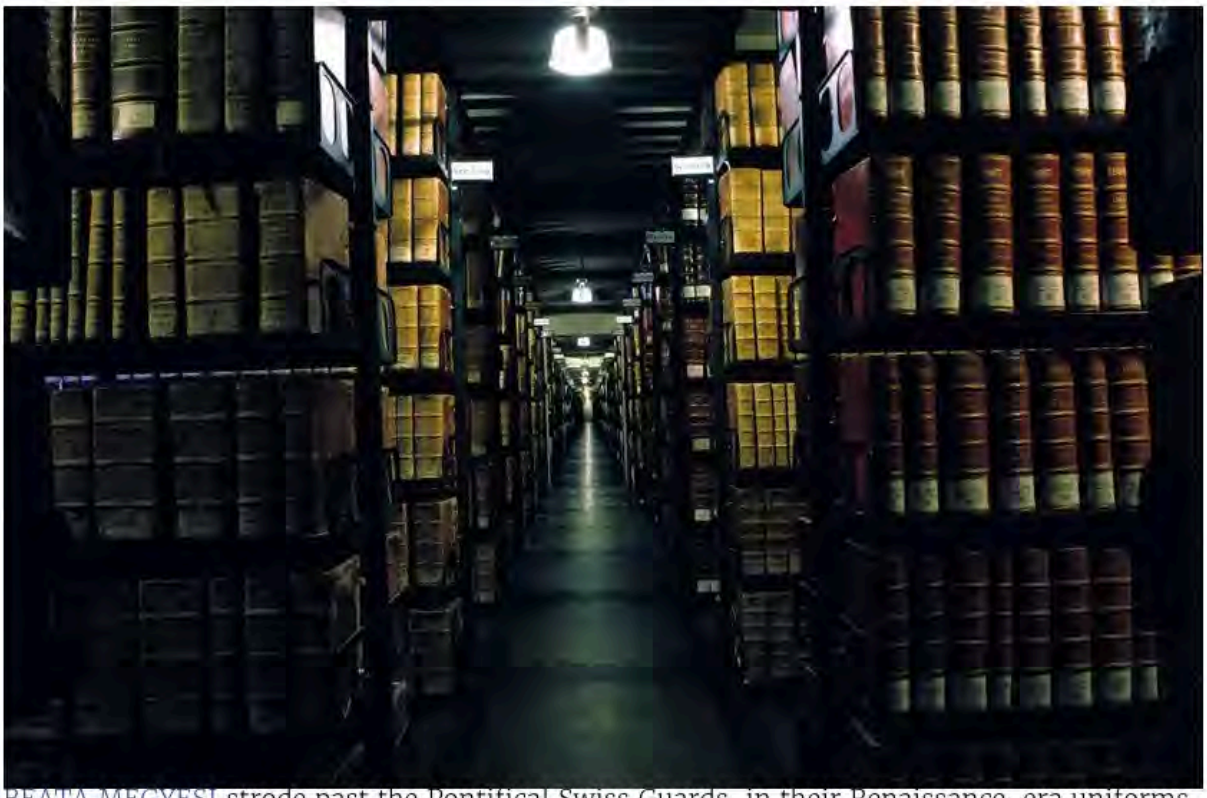
Technology

How scientists are cracking historical codes to reveal lost secrets

Deciphering encrypted messages from centuries past is a painstaking process. But linguists and computer scientists are starting to automate it, with some sensational results

By Joshua Howgego

18 September 2023



BEATA MEGYESI strode past the Pontifical Swiss Guards, in their Renaissance-era uniforms. She was headed not for the Sistine Chapel or St Peter's Basilica, but the Vatican's archives. Precious few people are allowed into this legendary collection of documents and letters spanning 12 centuries. Yet even in that context, Megyesi's 2012 visit was unusually intriguing. She was here to see texts so secret that no living person, not even the pope, could tell you what they contain.

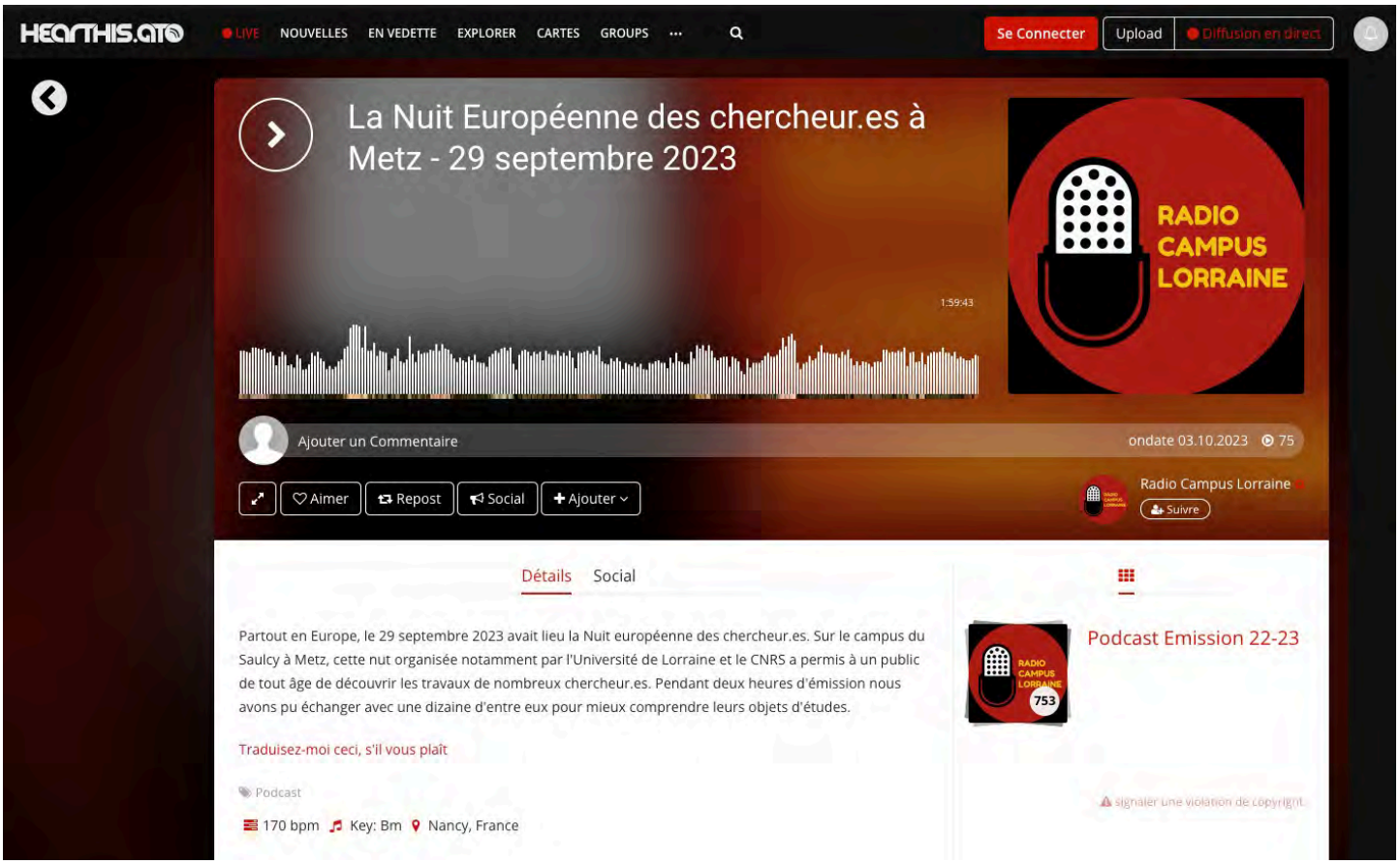
Megyesi, a linguist based at Uppsala University in Sweden at the time, had travelled to the Vatican to pore over a tranche of papers written in elaborate ciphers – the secret codes used by spymasters and others eager to send private messages. An expert in cracking historical codes, she had been invited after breaking the notorious Copiale cipher.

Megyesi had the opportunity to use the Vatican's encrypted papers for a project with an

audacious goal: to fully automate the process of decrypting historical ciphers so that many thousands of otherwise inaccessible letters could finally speak to us from down the centuries. "The dream is to be able to point your phone camera at a cipher and read it immediately," she says.

In the decade since, Megyesi and her colleagues have developed software that expedites their painstaking cryptanalysis – and researchers associated with the project have notched some remarkable successes. These include the recent decryption of a particularly fiendish code employed by a 17th-century French nobleman and, most sensationally, the cipher


HEARTHIS.AT
LIVE
NOUVELLES
EN VEDETTE
EXPLORER
CARTES
GROUPS
Se Connecter
Upload
Diffusion en direct
Boxe avec les mots - 26 septembre 2023
RADIO CAMPUS LORRAINE
2:01:07
Ajouter un Commentaire
ondate 27.09.2023
31
Aimer
Repost
Social
Ajouter
Radio Campus Lorraine
Suivre
Détails
Social
Un ring de boxe au milieu de l'Atrium de la fac de sciences. Mardi 26 septembre 2023, 16 étudiant.es se sont affronté.es dans des joutes de mauvaises fois. Nous étions en bord de terrain pour recueillir les impressions des perdants successifs du tournoi puis aux grands vainqueurs. L'évènement était organisé par Orion dans le cadre la semaine de la recherche.
Traduisez-moi ceci, s'il vous plaît
Podcast
93 bpm
Key: Em
Nancy, France
Podcast Emission 22-23
Signaler une violation de copyright


HEARTHIS.AT
LIVE
NOUVELLES
EN VEDETTE
EXPLORER
CARTES
GROUPS
Se Connecter
Upload
Diffusion en direct
La Nuit Européenne des chercheur.es à Metz - 29 septembre 2023
1:59:43
RADIO CAMPUS LORRAINE
Ajouter un Commentaire
ondate 03.10.2023
75
Aimer
Repost
Social
Ajouter
Radio Campus Lorraine
Suivre
Détails
Social
Partout en Europe, le 29 septembre 2023 avait lieu la Nuit européenne des chercheur.es. Sur le campus du Saulcy à Metz, cette nut organisée notamment par l'Université de Lorraine et le CNRS a permis à un public de tout âge de découvrir les travaux de nombreux chercheur.es. Pendant deux heures d'émission nous avons pu échanger avec une dizaine d'entre eux pour mieux comprendre leurs objets d'études.
Traduisez-moi ceci, s'il vous plaît
Podcast
170 bpm
Key: Bm
Nancy, France
Podcast Emission 22-23
signaler une violation de copyright

L'Est républicain, 1er octobre 2023 (édition Nancy)

Nancy

Consultation sur les relations police/population grâce à « Pol.is »

En utilisant l'outil numérique « Pol.is », l'association Terra Nova a proposé un large débat sur les actions et les missions de la police.

Association de loi 1901, Terra Nova a pour vocation de promouvoir des propositions innovantes et opérationnelles dans les domaines des politiques publiques. Le forum sur les « nouvelles pratiques démocratiques » qu'elle organise avec la ville de Nancy ce week-end offre différents débats et ateliers. Certains ont été l'occasion d'une consultation en amont avec un outil innovant.

Pol.is est un logiciel utilisé en Asie de l'Est qui permet d'organiser des débats dématérialisés à grande échelle. Terra Nova a choisi de l'expérimenter sur le sujet « Comment construire des relations de confiance entre la police et la population ? » Un panel de près d'un millier de personnes a participé à cette consultation qui a duré 3 semaines. Plus de 33 000 votes ont été recensés sur les propositions faites anonymement par les participants eux-mêmes.

Des antagonismes sont logiquement apparus entre des gens très conservateurs et d'autres très progressistes. La proportion est estimée à 25 % contre 75 %.

La relation de confiance entre la police et la population a été mise à mal par les actes de violence en marge des manifestations. Photo d'archives Ludovic Laude

Améliorer et d'allonger la durée de la formation des policiers

Si les premiers se sont déclarés hostiles au désarmement partiel de la police lors des interventions, les seconds se sont exprimés largement pour la minimisation de l'usage des armes, notamment des LBD. Terra Nova revendique « une indépendance politique » mais elle laisse apparaître une certaine « sensibilité » de gauche…

En revanche, des accords sont apparus sur certains thèmes. « Les points de consensus sont observés sur le rejet de la violence et sur la nécessité d'améliorer et d'allonger la durée de la formation des policiers dans plusieurs domaines », souligne Thierry Pech, directeur général de Terra Nova. « Notamment en ce qui concerne l'utilisation des armes et l'accueil des femmes victimes de violences. Ils sont également tombés d'accord pour le retour d'une police de proximité qui doit avoir une meilleure connaissance des lieux et de la population. »

Lors des débats menés à L'Autre Canal dans le cadre de ce forum « Place(s) de la Démocratie », la méthodologie a été abordée. « Pol.is est un bon outil pour que les gens s'expriment », a précisé Maxime Amblard, professeur et chercheur au Laboratoire lorrain de recherche en informatique et ses applications (LORIA). « Cependant, un algorithme se révèle être une opinion… » Les possibles failles du système ont été évoquées. Liée en particulier à l'anonymat ou au pseudonymat.

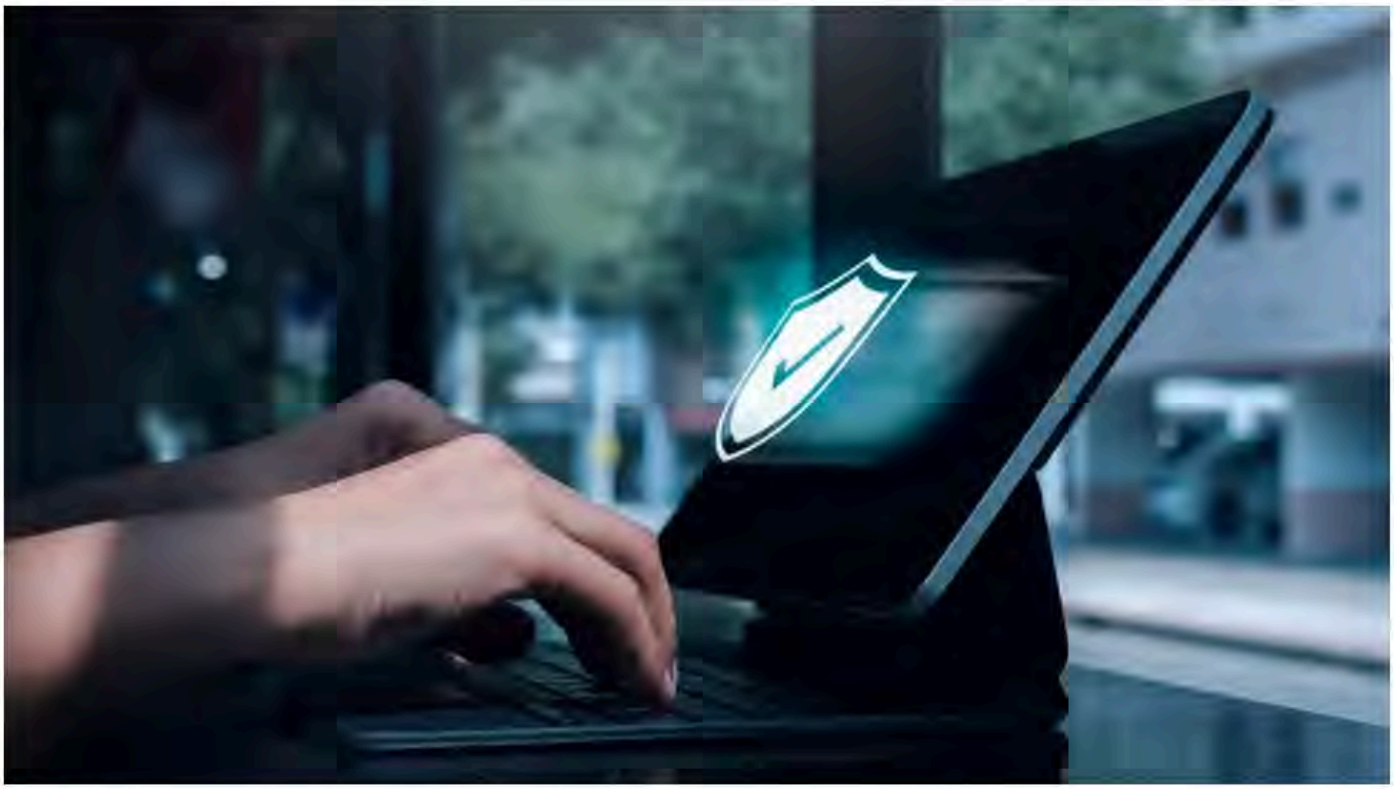
« La modération humaine apporte ses biais », a ajouté Samuel Nowakowski, maître de conférences à l'Université de Lorraine. Des questions très clivantes ont en effet été retirées par les modérateurs. Donc par une intervention humaine et pas par le logiciel… « L'intérêt de la plate-forme, c'est surtout de repérer des groupes d'opinion », a expliqué Foulques Renard, expert en démocratie participative.

Le fond et l'outil ont donné lieu à bien des discussions !

● **Jean-Charles Verguet**

La sécurité informatique, ce gisement de nouveaux services

IDEES ET OPPORTUNITES - Toutes les entreprises sont concernées par les attaques informatiques, notamment les PME et TPE qui sont, contrairement à une idée reçue, les plus souvent visées. La cybersécurité est un creuset d'innovations à long terme et un marché très attractif.



Les PME et TPE font souvent l'impasse sur la cybersécurité et constituent les « maillons faibles » de la chaîne de sécurité numérique. (Shutterstock)

Publié le 3 oct. 2023 à 14:00 Mis à jour le 3 oct. 2023 à 14:16

385.000. C'est le nombre de cyberattaques réussies sur des organisations en France, en 2022, dont 330.000 concernaient des PME*. Si le phénomène est en légère baisse par rapport en 2021, la menace reste élevée. Résultat ? « La sécurité

numérique devient une préoccupation croissante des entreprises », affirme Aurélie Clerc, aux manettes de Cyber Booster, branche d'Axeleo consacrée au financement de start-up de la cybersécurité. « C'est un secteur qui progresse de 10 % par an. Or, d'une part, les menaces sont de plus en plus nombreuses et protéiformes. D'autre part, le numérique est de plus en plus omniprésent dans nos vies. »

Sur un marché estimé à 5,6 milliards d'euros en France d'ici à 2027**, l'heure est à l'innovation. Avec plus de 164 start-up et 341 millions d'euros de fonds levés***, la France est sur le podium européen des pays les plus innovants en matière de cybersécurité. Et, chaque année, 25 jeunes pousses cyber voient le jour. Un segment déjà bien occupé donc, mais loin d'être saturé.

Tendances de fond : IA, cloud et vérification de l'âge

« Le marché de la sécurité numérique est en plein bouleversement », analyse Guillaume Tissier, directeur général du Forum international de la cybersécurité (FIC), grand-messe française annuelle des professionnels de la cyber. « De nombreuses innovations technologiques sont amenées à se développer, à l'instar du quantique et de l'intelligence artificielle. Il s'agit de tendances de long terme sur lesquelles les entrepreneurs peuvent s'appuyer pour lancer ou développer leur entreprise. »

C'est notamment le cas de Skyld, accompagné par l'Inria Startup studio à Rennes depuis 2022, pour sécuriser les algorithmes d'intelligence artificielle ; ou de Cybi - issu des travaux de l' équipe Resist et du Loria -, qui a développé un outil utilisant l'intelligence artificielle pour anticiper les cyberattaques.

LIRE AUSSI :

- **Se protéger des cyberattaques : huit réflexes à adopter d'urgence**

Autre tendance de fond : la sécurisation du cloud. En effet, le Covid-19 a accéléré la migration des entreprises vers cet environnement numérique. Dans une étude menée fin 2020, la société Palo Alto Networks avait détecté pas moins de 2.100 instances de cloud non sécurisées et facilement accessibles… en seulement quatre mois.

« Les entrepreneurs qui développent des solutions simples de sécurisation du

LES PLUS LUS

01 **Comment cette petite enseigne d'alimentation en circuit court a bâti un réseau de 12 magasins**

À LA UNE

PORTRAIT

cloud séduisent de plus en plus les investisseurs », souligne Aurélie Clerc. Certaines jeunes pousses se sont déjà lancées sur le créneau, à l'instar de Difenso ou de Dappwork. De son côté, la pépite française Astran a levé 5 millions de dollars, en juin 2023, pour sa solution de sécurisation des données sur le cloud.

Le marché de la vérification d'identité est également en pleine effervescence. « Depuis 2020, une loi oblige les sites pornographiques à empêcher les mineurs d'accéder aux contenus pour adultes. En juin, un texte a été adopté pour obliger les réseaux sociaux à vérifier l'âge des utilisateurs, etc. », égraine Jacky Lamraoui, CEO de Greenbadg (quatre salariés). « La liste des clients potentiels est longue et risque de grandir encore. » L'entrepreneur marseillais de 43 ans n'a donc pas hésité à saisir ces opportunités pour démarrer sa société en 2021 et proposer sa propre solution de double anonymat pour contrôler l'âge de l'internaute. Un succès ! Greenbadg est actuellement testé par le groupe Dorcel et par la Française des Jeux.

Un milliard d'euros pour la sécurité numérique

Si les grands groupes se sont équipés, les petites organisations, faute de moyens, font souvent l'impasse sur la cybersécurité. « Les TPE et PME sont les maillons faibles de la chaîne de sécurité numérique », constate Guillaume Tissier. « Il est donc urgent de développer des systèmes faciles d'utilisation et peu onéreux. » Comme Bastion, qui a développé une solution tout-en-un de cybersécurité, destinée aux entreprises de moins de 2.000 employés ; ou Stoik, qui propose une assurance incluant l'intervention immédiate de professionnels en cas de cyberattaque.

Pour stimuler la filière, la France multiplie les dispositifs d'aide. Le plan d'investissement France 2030 consacrera ainsi un milliard d'euros à la cybersécurité. Dans les territoires, plusieurs Campus Cyber sont en cours de création pour fédérer l'écosystème, à l'image de celui inauguré à La Défense à Paris en 2022.

Parallèlement, le gouvernement a mis en place le Grand Défi Cybersécurité, un appel à projet innovant autour de la sécurité numérique. « Nous avons été deux fois lauréats du dispositif », se félicite Thomas Kerjean, CEO de Mailinblack, créé en 2003. L'entreprise, qui compte 110 salariés et qui a réalisé 7,2 millions d'euros de chiffre d'affaires, a bénéficié d'une subvention de l'Etat de « 1,5 milliard d'euros pour financer une partie de [sa] R&D, et notamment des projets dans l'intelligence artificielle. »

LIRE AUSSI :

- Cybersécurité : DataDome armée pour son développement

Elle réinvente sa vie professionnelle après un grave accident de vélo

INTERVIEW

Cohésion d'équipe : « On n'est pas là pour s'aimer, on est là pour performer »

Ces séries et films cultes à voir absolument quand on est entrepreneur

Les entrepreneurs peuvent également compter sur des structures spécialisées dans la cyber, comme Cyber Booster à Lyon ; la division dédiée à la cyber d'EuraTechnologies à Lille ; ou encore la Cyberdéfense Factory, un incubateur à Rennes piloté par la Direction générale de l'armement (DGA). Certains grands groupes mettent également en place des programmes d'accélérateur de start-up, comme Thalès et son programme Cyber@StationF.

** Selon l'étude « Les cyberattaques réussies en France : un coût de 2 Mds€ en 2022 », du cabinet Asterès (2023). ** Source : Markess by Exaegis. *** Selon l'édition 2023 du radar de l'innovation cybersécurité français de Wavestone et Bpifrance.*

Salomé Ferraris

L'Est républicain, 3 octobre 2023 (édition Nancy)

Lorraine

La fac se modernise avec une chaire en droit du numérique

Depuis janvier dernier, les cours en droit du numérique se sont diversifiés pour les étudiants de la faculté de droit, à Nancy. C'est grâce à la création de la chaire « Régulation des Plateformes numériques et Souveraineté », qui demeure une rareté dans l'Université française, que les étudiants peuvent élargir leurs connaissances dans ce domaine.

Le professeur Maximilien Lanna a posé ses valises à Nancy en janvier dernier, et plus précisément à la fac de droit. Une aubaine pour les étudiants qui bénéficient de davantage de cours en droit du numérique grâce à la chaire « Régulation des Plateformes numériques et Souveraineté » (RPNS). C'est sous l'impulsion du professeur Olivier Cachard, et avec le soutien du doyen, Fabrice Gartner, et des laboratoires de droit public (IRENEE) et de droit privé (Institut François Gény) que cette nouveauté a été rendue possible. « Ils étaient convaincus de l'importance d'étudier le numérique par le prisme du droit. En l'occurrence, le droit des plateformes numériques interroge : que peut faire le droit pour réguler ces plateformes ? Au-delà de l'actualité du sujet, c'est un domaine très porteur qui ouvrira des voies à de nombreux étudiants », s'enthousiasme M. Lanna. « La chaire est une structure qui me permet de développer des projets, des colloques, des partenariats avec le Loria (un des plus grands laboratoires français dans le domaine de l'informatique, basé à Nancy) et avec des universités étrangères... C'est une vraie opportunité. »

Maximilien Lanna est le titulaire de la chaire "Régulation des plateformes numériques et souveraineté". Photo Laura Max

«Entre droit public et privé»

La particularité du droit du numérique ? Sa transversalité. En plus de son actualité, qui attire les étudiants. « Quelques élèves sont déjà venus me voir dans l'optique d'un mémoire sur le droit du numérique. Les retours sont très positifs. » Théo de Block et Alizée Thomas ont tous deux eu cours avec Maximilien Lanna au second semestre de leur M1, à partir de janvier dernier. Ils ne tarissent pas d'éloges, sur le cours comme sur le professeur : « Le numérique touche à tous les domaines du droit. Il franchit la frontière entre droit public et droit privé et se décline à toutes les échelles : l'État, les collectivités, l'individu... Je me serais peut-être spécialisé dans ce domaine si cela avait été possible plus tôt », explique Théo. Quant à Alizée, elle juge qu' « une introduction serait utile à chaque citoyen, parce qu'on est confronté au numérique tous les jours. »

Les colloques et entretiens consacrés à la matière feront l'objet de publications chez un éditeur juridique. De la souveraineté (« Comment nous, en tant qu'Européens, sommes censés retrouver une certaine souveraineté numérique face à des plateformes comme Google ou TikTok ? ») au rapport de l'individu au numérique, en passant par les usages du numérique dans les « Smart cities » que M. Lanna a étudiées (Comment le numérique influence-t-il les villes et peut-il les aider à s'approcher de la neutralité d'émissions carbone ?), le droit du numérique n'a certainement pas fini de créer des vocations.

● **Laura Max**

Vosges matin, octobre 2023 (édition Saint-Dié)

Saint-Dié-des-Vosges

Près de 250 élèves participent à la Fête de la Science organisée à l'IUT

La quinzième édition de la Fête de la Science se tenait ce vendredi 13 octobre à l'IUT de Saint-Dié. Une journée de découvertes pour les élèves de plusieurs établissements déodatiens. À l'image des élèves de 6e du collège Sainte-Marie, guidés par Delphine George, chargée de communication au sein de l'IUT.

Eric Ternisien a présenté la robotique aux élèves visiteurs. Ici, il a programmé le robot pour qu'il déplace des pièces de monnaie pour en faire deux tas distincts.

De 8 h 30 à 17 h, le personnel de l'IUT s'est relayé pour assurer les visites à pas moins de 250 collégiens et lycéens de Saint-Dié. Au programme : robotique, intelligence artificielle, motorisation électrique, audiovisuel et motion capture.

L'IUT de Saint-Dié, qui a fêté ses trente ans en 2022, compte actuellement 300 étudiants répartis sur trois formations de niveau BUT (brevet universitaire et technologique) et deux licences professionnelles. La Fête de la Science est l'occasion d'ouvrir les portes de l'établissement à des élèves qui en ignorent l'existence, pour bon nombre.

Six ateliers étaient proposés aux jeunes visiteurs. Les collégiens ont montré un attrait particulier pour les technologies présentées. Au travers d'utilisations concrètes de l'intelligence artificielle, de la robotique ou encore de la motion capture, ils ont pu avoir un aperçu des formations accessibles à l'IUT. Et il n'est jamais trop tôt pour y penser.

D'ailleurs, les jeunes élèves connaissent Scratch, le langage Python, Chat GPT, Dall-E... Des technologies qui en effraieraient plus d'un mais qui galvanisent ces collégiens.

Les élèves de sixième du collège Sainte-Marie ont fait preuve de beaucoup d'attention et n'étaient pas avares de questions. Des questions sur l'avenir notamment, en voyant travailler un des bras robotisés. Certains s'inquiètent : « C'est ça qui va travailler plus tard et nous, on n'aura pas de travail ». Quand d'autres y voient des avantages : « Lui, il n'est jamais fatigué, dommage qu'il n'en existe pas un pour ranger ma chambre ! ».

Les métiers de l'informatique en constante évolution

Comme Pierre-Frédérique Villard, professeur agrégé en informatique à l'IUT de Saint-Dié, le dit, les métiers de l'informatique ont de l'avenir devant eux. Il déplore que trop peu de jeunes filles se tournent vers cette voie.

11 photos :
https://c.vosgesmatin.fr/education/2023/10/14/saint-die-six-ateliers-proposes-aux-collegiens-et-lyceens-dans-le-cadre-de-la-fete-de-la-science-organisee-a-l-iut

Le DFKI, partenaire de confiance de l'IA européenne

L'institut allemand de l'intelligence artificielle DFKI basé à Sarrebruck a initié le *Centre for European Research in Trusted AI* (CERTAIN), qui doit renforcer la fiabilité de cette technologie à l'échelle européenne. Basé à l'université de Sarre, ce centre prolonge un engagement transfrontalier bien ancré.

Référence européenne en matière d'intelligence artificielle, l'institut allemand de l'intelligence artificielle (DFKI), basé à Sarrebruck, a inauguré sur le campus de l'université de la Sarre *Centre for European Research in Trusted AI* (CERTAIN), axé sur fiabilité et la protection des données des solutions d'IA.

Philipp Slusallek, directeur scientifique du DKFI. © DFKI.

"Le bon fonctionnement des logiciels d'IA est crucial. Ce n'est que sur la base de garanties que nous pourrons discuter utilement de son éthique", a estimé le professeur Philipp Slusallek, directeur scientifique du DKFI, qui compte parmi principaux responsables du projet CERTAIN, lors de l'inauguration du centre le 19 septembre dernier.

Le CERTAIN ambitionne de devenir un centre d'excellence européen en matière d'IA de confiance, étroitement lié à la recherche, à l'industrie et à la société. En tant que pendant allemand du programme de recherche technologique français confiance.ia, le CERTAIN s'est déjà associé à Triathlon, l'écosystème pour l'entrepreneuriat, l'innovation et le transfert de l'Université de la Sarre. L'objectif est d'aider les start-ups allemandes spécialisées dans l'IA à s'installer sur le marché français.

Une impulsion européenne dans la recherche commune

Cette coopération franco-allemande se trouve confortée par l'Union européenne. Confronté à l'essor récent de l'IA et à des barrières juridiques floues, surtout dans le cadre de son usage en entreprise, le Parlement européen a adopté en juin dernier le l'AI Act, un règlement destiné à rendre l'IA sûre, transparente, traçable, non discriminatoire et respectueuse de l'environnement.

« En ce qui concerne la protection des données, le RGPD offre une sécurité d'action à tous les pays de l'UE. Dans le AI Act, les objectifs, les priorités et les structures sont tout à fait différents » explique le DFKI dans une réponse commune aux questions de Voisins-Nachbarn.

Partenaire de l'Inria

A l'échelle régionale, le DKFI a conforté ses coopérations avec l'institut national de recherche en sciences et technologies du numérique (INRIA), basé à Nancy, à la faveur du Traité d'Aix-la-Chapelle. Depuis 2020, quatre projets franco-allemands portent sur des champs d'application. L'équipe de MePheSTO tente de développer une IA médicale capable d'affiner le diagnostic des patients atteints troubles psychiatriques et neurodégénératifs, tandis que le projet IMPRESS espère améliorer la compréhension des textes et du langage de leur IA, jugée insatisfaisante pour de nombreux logiciels actuels d'IA.

Début septembre, après deux éditions réussies en 2021 et 2022, le DFKI et l'INRIA ont coordonné leur troisième école d'été européenne, baptisée IDESSAI 2023. Une centaine de participants, principalement des étudiants en IA, ont pu suivre des cours et des conférences sur les thèmes « Simulation et IA » et « L'IA pour l'agriculture et l'environnement ».

L'IA en pratique dans la Grande Région

L'implantation du centre de recherche à Sarrebruck a permis à ses chercheurs de trouver non seulement des partenaires, mais aussi des applications dans l'espace transfrontalier. Au Luxembourg, le DFKI collabore avec le Luxembourg Institute of Health afin d'améliorer l'usage de l'IA à l'hôpital universitaire de la Sarre. La recherche s'étend de la médecine de précision au diagnostic assisté par l'IA.

Outre ses applications scientifiques, l'intelligence virtuelle peut également se révéler utile au quotidien pour les pour les habitants de l'espace frontalier :

« L'IA permet par exemple, de reproduire de manière transparente différents processus administratifs, tant de part et d'autre de la frontière. Elle peut ainsi aider les entreprises de construction ou les architectes à obtenir des autorisations dans le pays voisin. En outre, des chatbots et des assistants virtuels multilingues basés sur l'IA peuvent remplir des formulaires », explique le DFKI.

VOISINS NACHBARN
L'information libre et mitoyenne

LORRAINE – SARRE – RHÉNANIE-PALATINAT

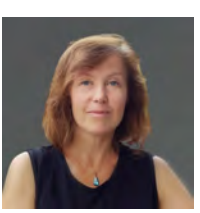
M-Phasis débusque la haine sur internet

Le projet franco-allemand M-Phasis, conduit par des chercheurs en sciences humaines et en informatique des universités de Lorraine, de Sarre et de Mayence, fourbit des armes innovantes pour juguler la haine en ligne.

DR

Romain Gascon *mercredi 18 octobre 2023*

Depuis les cours des écoles jusqu'aux soubresauts géopolitiques du moment, la haine en ligne semble pouvoir balayer en relative impunité toutes les parcelles de nos existences. Des chercheurs en sciences humaines et en informatique de plusieurs composantes des universités de Lorraine, de Sarre et de Mayence ont entrepris de disséquer des messages haineux pour nourrir la riposte avec le projet M-Phasis, lancé en 2018.



Irina Illina, maîtresse de conférences à l'IUT Nancy Charlemagne et chercheuse au Multispeech du Loria.

« Il n'y avait pas vraiment de définition unifiée de la haine. Cette notion n'avait pas été abordée dans la littérature scientifique », note Irina Illina, maîtresse de conférences à l'IUT Nancy Charlemagne et chercheuse au Multispeech du Loria, à l'origine du projet avec Angeliki Monnier, directrice du Centre de recherche sur les médiations et professeure en Sciences de l'information et de la communication à l'Université de Lorraine.

Après avoir défini scientifiquement le concept, les chercheurs ont collecté des commentaires en français et en allemand sur les sites internet de médias d'information des deux pays et sur le réseau social Twitter (devenu X, dans l'intervalle). Le corpus établi a été soigneusement étudié et annoté pour faire émerger un protocole solide et global de détection des discours de haine. Aux chercheurs en informatique est revenue la tâche de développer un outil pour l'automatiser, baptisé Human (Hierarchical universal modular annotator).

L'implicite n'a qu'à bien se tenir

« Notre logiciel évalue la probabilité de la présence de la haine dans un message textuel », résume Irina Illina. Il permet de gagner en efficacité dans l'analyse des flux de messages, à la fois en termes de volume et de rapidité, mais aussi dans le degré de finesse. A la détection de la haine explicite s'ajoute celle de la haine implicite. Parmi plusieurs travaux de thèse irrigués par le projet, celle qui sera soutenue en novembre prochain s'intéresse par exemple aux expressions dites « polylexicales », dont le sens global ne peut être déduit de la combinaison des sens des mots qui la composent.

Intelligence artificielle et citoyenne

Les résultats de M-Phasis présentent un intérêt manifeste pour les médias en ligne et les réseaux sociaux. La législation de l'Union européenne impose aux gestionnaires de plateformes de supprimer les messages à caractère haineux dans les 24 heures qui suivent leur publication. *« Cette détection est très coûteuse »*, note Irina Illina. Conduit et financé par des institutions publiques (Agence nationale de la recherche française et son homologue allemande Deutsche Forschungsgemeinschaft), M-Phasis s'inscrit dans le cadre du projet Olki (Open language and knowledge for citizens) développé par Lorraine Université d'excellence, qui promeut le développement d'une intelligence artificielle transparente. Scientifiques ou citoyens, tout le monde peut se saisir des résultats de M-Phasis, disponibles en open source.

Chat GPT générateur de haine

A ce stade, il est difficile de cerner l'impact que M-Phasis peut déjà avoir sur la haine en ligne. A tout le moins, il suscite l'intérêt. Il aura notamment les honneurs d'une conférence au Japon en novembre. Mais les enseignements sont d'ores et déjà nombreux. *« Nous nous sommes rendus compte que la haine est souvent propagée par quelques personnes seulement. Cela peut être utile pour la détecter. (…) Quant aux LLM* [Large language models, type Chat GPT, NDLR]*, ils sont efficaces pour mieux la tracer. Mais ils sont eux-mêmes capables de générer des messages haineux. Comment « débiaiser » ces modèles ? »*, interroge Irina Illina. A l'aune des résultats et enseignements de M-Phasis, clos à l'été 2022, les chercheurs espèrent obtenir de nouveaux financements pour pouvoir mieux étouffer la haine en ligne dans l'œuf et dans les textes, mais aussi dans les sons et les images.

Nancy

La start-up Marmelab veut réduire son empreinte carbone de 10 % par an

Nancy. Créée il y a dix ans à Nancy, la start-up Marmelab, atelier d'innovations numériques, s'est fixé pour principal objectif « de rendre le monde meilleur grâce à l'innovation numérique », en passant notamment par la réduction de l'empreinte carbone. La sienne, mais aussi celle des autres.

La start-up Marmelab emploie une vingtaine de personnes pour un chiffre d'affaires annuel d'1,5 million d'euros. Photo Mickaël Demeaux

> « Nous donnons chaque année 4 % de nos revenus à des associations caritatives »
> **François Zaninotto, fondateur et dirigeant de Marmelab**

On peut être innovant, travailler avec les plus grandes technologies du numérique et être engagé dans la lutte contre le réchauffement climatique. La preuve avec la start-up Marmelab, à Nancy.

Basée au cœur de la cité des ducs de Lorraine, place d'Alliance, à deux clics de la place Stanislas, Marmelab, atelier d'innovation numérique qui a vu le jour il y a dix ans, compte une vingtaine d'employés, principalement des développeurs, pour un chiffre d'affaires annuel d'1,5 million d'euros.

Améliorer l'impact social et environnemental

Son métier ? « On propose des services techniques digitaux très complexes à nos clients », explique François Zaninotto, 50 ans, fondateur et dirigeant de Marmelab. Ses clients ? Le groupe TF1, Canal Plus, le journal *L'Équipe*, Caritas, le CNRS et surtout le site arte.tv.

Marmelab est une entreprise « certifiée BCorp ». « Ce qui signifie, explique son responsable, que nos exigences en matière de responsabilité sociale et environnementale sont très élevées, et que nos actes reflètent nos valeurs. »

Il précise : « Nous effectuons des missions gratuitement pour des associations d'intérêt public comme Amnesty International, et nous donnons chaque année 4 % de nos revenus à des associations caritatives. Côté environnement, nous ne nous arrêtons pas au bilan carbone : chaque mois, un groupe de collaborateurs se réunit pour réfléchir à des actions concrètes à mettre en place pour améliorer notre impact social et environnemental. Surtout, notre objectif est de réduire notre empreinte carbone de 10 % par an, le double des accords de Paris. »

Un service gratuit et open source

François Zaninotto détaille : « Pour s'assurer que nos produits numériques eux-mêmes ne soient pas trop émetteurs, nous avons développé un outil de mesure de l'empreinte carbone des sites web, GreenFrame.io. Développé en collaboration avec un chercheur du Loria (laboratoire d'informatique de Nancy), ce service est gratuit et open source. Il est utilisé par des centaines de développeurs à travers le monde, dont ceux du site lemonde.fr qui ont réduit l'empreinte carbone d'une visite sur la page d'accueil du journal numérique de 21 % grâce à GreenFrame ».

La start-up nancéienne s'est récemment diversifiée et a pris une dimension internationale. Aujourd'hui, 25 % du chiffre d'affaires est réalisé hors de France.

« Cette activité permet de pérenniser un flux de revenus qui a permis le recrutement de quatre personnes supplémentaires en CDI en 2023 et probablement d'autres à venir en 2024 », se réjouit François Zaninotto.

● **Mickaël Demeaux**

Un dirigeant engagé formé à Nancy

Marmelab, c'est lui : François Zaninotto, 50 ans, visage souriant, allure jeune sympa, et des valeurs : discrétion, engagement.

François Zaninotto, c'est l'histoire d'un étudiant qui se retrouve au milieu des années 1990 aux Mines de Nancy. Après de brillantes études, le jeune ingénieur entre en 1988 chez Michelin, à Paris, pour travailler sur les célèbres cartes et guides. L'aventure dure trois ans.

Il part ensuite faire son service militaire chez Médecins sans frontières en Sierra Leone. À son retour, il multiplie les jobs. Avant d'être débauché par l'animateur Arthur en 2005 dans le cadre de la création d'une start-up consacrée aux seniors.

Mais en 2008, c'est la crise économique, le projet s'écroule. Arthur lui ouvre les portes du groupe TF1 dans lequel il devient directeur technique pour tous les aspects mobile, Internet, TV. Il y reste jusqu'au lancement de Marmelab en 2013 et il choisit Nancy comme camp de base, pour raison privée.

Francois Zaninotto, fondateur et dirigeant de Marmelab. Photo Mickaël Demeaux

Les Tablettes lorraines, 23 octobre 2023

Cybersécurité - Droit

Des Assises à Nancy

La loyauté civique à l'épreuve des outils numériques : comment ferons-nous société en 2100 ? La gestion de crise cyber : des OIV (opérateur d'importance vitale) aux PME en passant par la cybersécurité et la protection des données de santé. Ce 26 octobre, le centre de congrès Prouvé de Nancy accueille la deuxième édition des Assises universitaires Droit et Cybersécurité. Organisée par la Faculté de Droit de Nancy (Université de Lorraine) et le Loria (CNRS, Inria, Université de Lorraine), en partenariat avec la Région Grand Est, Grand E-nov, la Métropole du Grand Nancy et le laboratoire Irénée, cette rencontre interdisciplinaire à la croisée du droit et de l'informatique sera l'occasion de dresser un état des lieux de l'avancement de la recherche et du droit dans ce domaine.

Génération IA

Par Audrey Somnard
Publié le 28 oct. 2023

Écouter cet article 16:59

L'intelligence artificielle fascine et provoque des inquiétudes. Les spécialistes du secteur appellent à une réflexion globale sur son rôle dans notre société, à notre rapport aux médias et à la

démocratie.

Cet article est mis à ta disposition gratuitement. Si tu veux soutenir notre équipe et le journalisme de qualité, abonne-toi maintenant.

LIRE

75e Anniversaire du Lëtzebuerger Journal

17.10.2023

Le classement international des médias de Reporters sans frontières révèle bien souvent la bonne santé des démocraties et inversement. Des médias indépendants ne peuvent exister dans des régimes autoritaires, ces derniers ayant à cœur de museler la presse qui doit alors relayer la propagande du régime. Que viennent alors faire les outils technologiques comme l'IA dans ce fragile équilibre ? Créée comme un outil de calcul à la base, l'intelligence artificielle est utilisée aujourd'hui pour créer des voix, images et autres contenus qui ont de plus en plus l'air vrai, mais qui sont issus des machines. Une nouvelle façon de travailler pour les journalistes et les politiques, avec des sources d'information pas toujours fiables pour lesquelles le grand public doit faire le tri. La thématique est tellement complexe qu'elle fait l'objet d'attention de chercheur·euse·s de disciplines diverses, pour amorcer une conversation sur le rôle de l'IA dans notre société.

C'est le cas du laboratoire AI, media & democracy basé à Amsterdam, qui a vu le jour il y a deux ans. Si la technologie avance bien plus vite que nos législateur·rice·s, l'Europe veut être à la pointe concernant la régulation d'une espèce de Far-West qu'est devenue l'IA. "À quelles fins voulons-nous l'utiliser et quels sont les besoins, les points sur lesquels nous devons être prudents, par exemple, la factualité de ce contenu qui émerge de ChatGPT, etc. La loi, bien sûr, n'a pas encore rattrapé son retard. Je pense que l'essentiel est de reconnaître que tout n'est pas figé pour l'instant, que tout se développe à grande vitesse et que les gens adoptent déjà ces technologies", explique Sara Spaargaren, manager du lab que nous avons interviewée par visioconférence.

Pour cette dernière, il est impératif que la recherche apporte des réponses pour une société qui est perdue face aux applications de l'IA. Notamment pour les médias qui travaillent de plus en plus avec des outils de speech-to-text (reconnaissance vocale automatique qui permet de retranscrire des interviews audio), traduction ou encore ChatGPT pour générer des e-mails formels par exemple. Mais ce n'est pas sans conséquence : "Lorsque quelque chose ne va pas et que l'impact devient important, qui en prend la responsabilité ? C'est exactement le type de questions que les entreprises de médias tentent de résoudre en ce moment. Je pense que le monde universitaire et les institutions du savoir peuvent

être des interlocuteurs de choix pour prendre du recul et évaluer ce que nous voulons, comment nous voulons guider l'utilisation de ces outils. C'est ce que nous faisons avec le laboratoire." Deux de ses chercheur·euse·s vont être prochainement envoyé·e·s dans les locaux de la BBC, pour que ces dernier·ère·s travaillent en collaboration étroite avec les journalistes et comprennent les enjeux de la profession.

Sara Spaargaren

Car nous sommes passés en quelques années à des recommandations d'articles, des réseaux sociaux qui mettent en avant certains contenus d'après nos préférences, à des contenus générés par des machines. Une avancée qui pose certaines questions. Pour Dr Maxime Amblard, professeur d'informatique à l'Université de Lorraine à Nancy, il s'agit tout d'abord de bien poser la problématique avec une définition précise de ce qu'est l'IA. "Je pense qu'il y a un problème au départ, c'est qu'on appelle aujourd'hui IA un peu tout et n'importe quoi. L'informatique est une science qui est introduite autour des travaux d'Alan Turing (mathématicien et cryptologue britannique, auteur de travaux qui fondent scientifiquement l'informatique. Il est aussi un des pionniers de l'Intelligence artificielle. Ndlr), parce qu'il fait quelque chose qui est extrêmement difficile, mais qui est fondamental, le calcul mathématique en train de se faire. C'est ça qui donne les briques de base qui vont devenir l'informatique. À la fois théorique et puis concret avec la réalisation des langages de programmation. L'algorithmique est la partie qui est plus du côté de la conception, pour organiser le calcul qui est en train d'être réalisé. Ces différentes briques forment des algorithmes qu'on va ensuite implémenter avec un langage de programmation. Pour Turing, ce qui va être intéressant c'est de savoir si ce calcul permet de simuler une compétence humaine que l'Homme n'arrive pas à calculer ou à faire, ou encore parce qu'il y a trop de données à gérer. Et c'est ça qu'il appelle l'intelligence artificielle."

L'intelligence artificielle, selon la définition d'Alan Turing, est simplement de suppléer les incompétences des humains, poursuit Prof. Amblard : "Nous avons connu une révolution conceptuelle, plutôt au début des années 2000 où il y a eu à la fois les bons outils mathématiques théoriques qui sont apparus, et puis la capacité de calcul. Les données récoltées à partir de nos propres ordinateurs ont également été par la suite déterminantes. Aujourd'hui quand on parle d'intelligence artificielle, on fait un peu un mélange entre ces deux aspects. Théoriquement, on peut tout à fait faire de l'IA sans les apprentissages d'une part. Et puis surtout on fait plein d'informatique qui n'est pas du tout de l'IA."

L'outil le plus célèbre issu de l'intelligence artificielle, c'est ChatGPT qui a révolutionné tous les outils de prédiction du genre. Pour Prof. Amblard, "c'est un outil de génération de texte qui en fait n'est qu'un super modèle mathématique de probabilité. Il agrège plein de données de textes qui existent déjà. Il se nourrit donc au travers d'énormément de données qui sont volées ou qui sont utilisées sans le consentement de ses auteurs. Mais le modèle qui est construit, ça n'est qu'un modèle qui prédit le mot suivant, le plus probable. Et il génère tellement bien le mot suivant le plus probable que cela forme des phrases." Au contraire des humains qui eux "sont des machines à faire du sens parce que c'est une fois que l'outil numérique a produit une phrase, c'est nous, humains, qui regardons cette phrase et qui nous disons, 'ah qu'est-ce que ça veut dire ou qu'est-ce que la machine a voulu dire avec ça ?' Mais la machine, enfin le modèle ne veut rien dire du tout, il n'a rien voulu sous-entendre, il n'y a pas de message caché, il n'y a qu'un modèle de distribution des mots. C'est ça qui est vraiment important, c'est que cela n'a rien à voir avec la vérité. Parce que pour dire la vérité, il faut avoir une connaissance du monde."

"Il ne faut pas plus de données pour devenir plus intelligent, il faut en fait plus d'informations de qualité

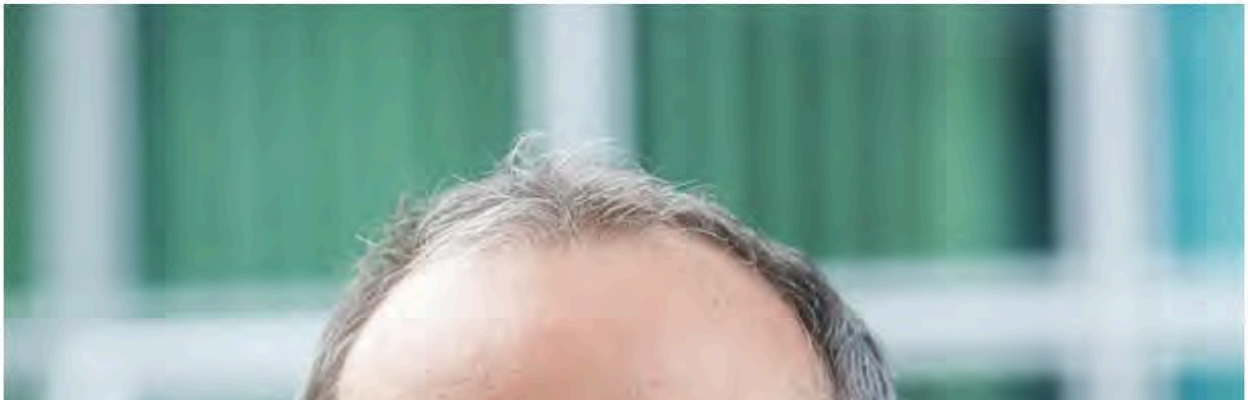
pour avoir un système qui génère de meilleurs contenus."

Maxime Amblard, professeur d'informatique à l'Université de Lorraine

Les outils actuels n'ont donc pour le chercheur pas de capacité à produire des contenus qui feront sens par eux-mêmes. Pour Sara Spaargaren, la réflexion est nécessaire notamment pour les médias qui seraient tentés d'utiliser ChatGPT par exemple. "Si vous regardez l'organisation des médias, où ils sont produits et comment ils sont diffusés, ainsi que les technologies qui les sous-tendent, il y a généralement une grande division au sein de l'organisation des médias. Et je pense que c'est également le cas dans la société en général. Les technologies ne s'adressent pas vraiment à l'utilisateur final ou à l'utilisateur de l'outil. Il est donc difficile de superviser les choix de conception technologique et leur impact à long terme."

Pour Maxime Amblard, le problème de ChatGPT du point de vue des médias, c'est "comment est-ce qu'on va donner du sens à ce qui a été produit ? Et c'est là où c'est un humain qui doit intervenir et éditorialiser ce qui a été produit. C'est tout le travail du journaliste typiquement, de prendre la suite des phrases et faire en sorte que ce qui a été généré construise une idée, un concept qui a du sens par rapport à la vérité et la déontologie. Ce qui est nouveau, c'est qu'on est capable de générer des fausses images, textes, vidéos, on est technologiquement capable de plein d'opérations. L'humain est obligé d'intervenir pour valider le discours, construire le discours de la réalité. Cela n'est pas la tâche de l'outil", insiste le chercheur.

Pour ce dernier, le métier de journaliste n'est donc pas près d'être remplacé par des machines. "Quand on regarde ChatGPT 3.5 par rapport à ChatGPT 4, il fait plus de choses. ChatGPT 4 a l'air d'être plus efficace, mais si on lui demande de résoudre des tâches de raisonnement simple, en fait ChatGPT 3.5 est meilleur que la dernière version." Le chercheur explique cela par une méconnaissance de l'IA. "Il ne faut pas plus de données pour devenir plus intelligent, il faut en fait plus d'informations de qualité pour avoir un système qui génère de meilleurs contenus. Mais nous avons atteint un niveau où nous avons tellement utilisé de données de mauvaise qualité ou générées synthétiquement qu'on finit par capter un peu toujours la même chose. La nature mathématique qui est utilisée dans ces outils ne fait que mécaniquement amplifier ce qui s'exprime dans les données." Si les avancées dans le domaine de L'IA sont assez spectaculaires, on est encore loin d'être dépassés par les machines, relativise le scientifique : "Je ne suis vraiment pas du tout inquiet au sens que je ne pense pas que l'IA va prendre le pouvoir sur les humains. Je pense que les humains doivent concevoir ce qu'est l'IA et que ce n'est pas plus que des outils."



Maxime Amblard

Le biais de l'IA, et par là des données dont elle se nourrit, est un problème dont le chercheur est bien conscient. Nous en avions parlé dans un article précédent avec la militante du réseau européen contre le racisme (European Network Against Racism – ENAR) Oyidiya Oji, venue à Luxembourg pour donner une conférence sur le sujet. Elle s'étonnait alors d'applications pour le grand public qui se basaient sur des données biaisées : "J'ai commencé à lire qu'aux États-Unis, par exemple, des voitures sans conducteur s'écrasaient ou avaient plus de chances de s'écraser contre des femmes, surtout s'il s'agissait de femmes de couleur ou de personnes souffrant d'un handicap quelconque, car la voiture ne voit pas les peaux plus foncées. Dans ce cas, comme les ingénieurs sont souvent des hommes, ils se disent que, bien sûr, ça marche. Mais ça marche pour eux." Le professeur se pose également la question du biais de l'IA. "En Europe, on s'est aussi posé la question de comment construire des modèles moins biaisés et en fait, c'est extrêmement difficile. Donc on n'a pas forcément réussi de manière ultra médiatique mais on est confronté à des questions qui sont vraiment difficiles."

Une prise de conscience pour les médias

Il faut donc une prise de conscience, pour le secteur, mais également pour les utilisateurs intermédiaires que sont les médias. "Que cela bouscule les organisations et des métiers, c'est évident, comme la question de la traduction assistée par ordinateur qui bouscule le métier de traducteur", indique Maxime Amblard, qui distingue par exemple des outils de traduction automatique pour des usages rapides du quotidien et des traductions de qualité qui doivent toujours être supervisées par des personnes compétentes. Le chercheur ne s'inquiète pas de la disparition de certaines professions. Si des tâches vont être automatisées, c'est une bonne chose selon lui : "Des tâches répétitives et sans plus-value, si on peut les automatiser et qu'on a des outils qui sont capables de les faire, tant mieux. Cela laisse beaucoup plus de temps pour faire le vrai travail que vous savez faire en tant que politique ou journaliste et qui est alors pour les journalistes l'éditorialisation et pour les politiques, la construction d'une pensée de l'organisation de la société."

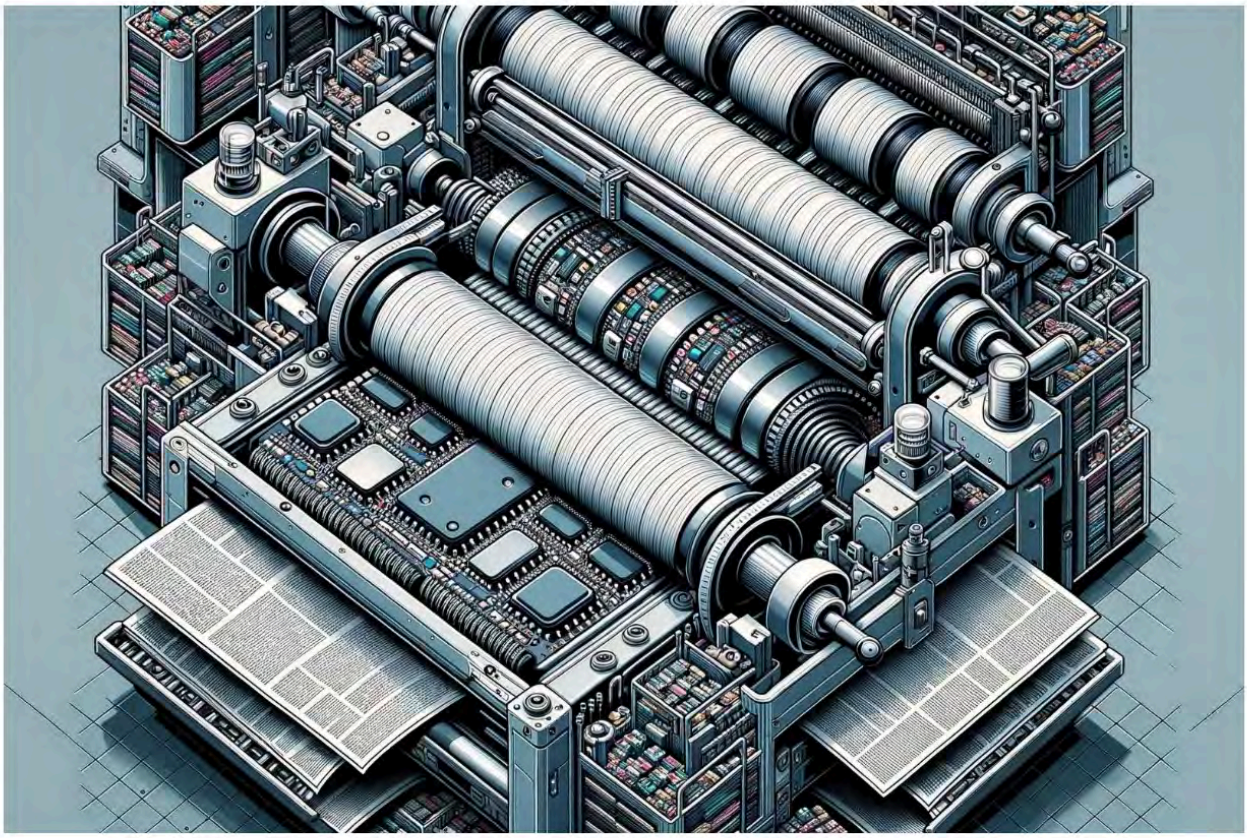
Et pour amorcer cette discussion, Sara Spaargaren estime que les différent·e·s acteur·rice·s de la société doivent se mettre autour de la table pour cibler les vrais enjeux : "Ce que nous essayons de faire ici, c'est d'organiser des groupes de discussion, des conversations avec les développeurs techniques d'une organisation, mais aussi avec les éditeurs qui gèrent la gestion, car ce sont eux qui décident quels outils peuvent être utilisés et ce que nous pouvons faire et ce que nous ne pouvons pas faire. Il s'agit donc de réunir différents groupes qui peuvent agir comme des îlots au sein d'une organisation." Pour Dr Amblard, "il y a un enjeu de souveraineté explicite et majeur autour de l'intelligence artificielle. Il faut des gens qui développent, comprennent et analysent ce qui se fait et ce qui est possible de faire avec l'intelligence artificielle et à la fois il faut, en termes d'organisation politique, sociale, sociétale, décider ce que l'on fait. Il y a un risque de polarisation majeure entre des acteurs qui maîtrisent l'intelligence artificielle et des acteurs qui seraient complètement dépendants des autres opérateurs."

> **"Je pense qu'il y aura des lois qui veilleront au moins à ce que les plateformes soient plus explicites sur la manière dont elles recommandent des informations aux gens."**
>
> Sara Spaargaren, manager du laboratoire AI, media & democracy

Les deux spécialistes sont d'accord sur le fait que le message clé résidera dans l'éducation du grand public à mieux appréhender ces outils. Si les rumeurs et autres fausses nouvelles ont toujours existé, la production facilitée et de masse nécessite une plus grande attention à tout ce que l'on voit et lit. "Je pense qu'il y aura des lois qui veilleront au moins à ce que les plateformes soient plus explicites sur la manière dont elles recommandent des informations aux gens. Un autre aspect est que cela doit être plus orienté vers l'humain. Nous acceptons toujours le cookie, nous disons tous oui. Et c'est très bien. Mais vous devez vraiment sentir que vous avez le choix et que vous êtes responsable de votre régime d'information, pour ainsi dire. Ce type de questions est vraiment important si nous voulons orienter la technologie dans une direction qui profite réellement à la diversité", explique Sara Spaargaren. "Le grand public n'a pas encore intégré qu'une image

n'est pas la réalité. C'est quelque chose qui va s'imposer. Raymond Depardon, Capra, c'est fini. On est en train de construire un autre rapport à l'information, enfin au sens de l'information visuelle, de l'information sonore, de l'information textuelle. On est en train de modifier ce rapport-là. On se rend compte qu'il y a 1% des comptes sur X (Twitter) qui produisent 34% de l'information qui circule. Cela veut dire que l'information qui circule sur Twitter n'est pas à l'image de ce que les gens peuvent exprimer. Le problème est qu'il n'y a personne pour déconstruire le discours, on les laisse croire que s'ils voient ça en grande quantité sur Twitter, c'est que c'est probablement vrai. Et quand ils essaieront de trouver quelque part l'expression de la vérité, cela redonnera un sens très grand au journalisme ou aux politiques", explique Dr Amblard.

En attendant à ce que le grand public et les autres se forment aux défis que représentent l'IA, les spécialistes sont tous et toutes unanimes pour dire que l'AI Act va poser un cadre bienvenu. "L'Europe est à l'avant-garde en matière de stratégie numérique. Et pas seulement une IA qui dictera comment les algorithmes peuvent et doivent être utilisés, mais aussi des lois sur les services numériques, qui réglementent les grandes plateformes telles que Facebook et Twitter. Il y a tout un ensemble de réglementations qui sont, dans l'ensemble, très innovantes et je ne pense pas qu'il y en ait ailleurs dans le monde", estime Sara Spaargaren.



Si certain·e·s chercheur·euse·s et autres spécialistes de la tech se plaignent des régulations, Maxime Amblard fait partie de ceux·celles qui voient en la régulation un bon moyen de prendre un peu de recul pour prendre les bonnes décisions sur l'utilisation de ces nouvelles technologies. "En Europe, nous sommes entravés dans le développement d'une partie de nos recherches pour des questions de droit. Mais cela nous force à faire porter une recherche éthique et déontologique. Cela peut apparaître comme un frein quand on regarde le niveau d'avancement de ce qui se fait aux États-Unis, mais nous avons un état de réflexion sur les questions éthiques et déontologiques qui est très bon. Je ne veux surtout pas dire qu'il n'y a rien aux États-Unis parce que j'ai plein de collègues qui travaillent là-dessus. Ils ont pu faire tout un tas de choses sans se poser de questions alors que nous en Europe, on s'est très rapidement retrouvé empêchés de collecter des données et de les utiliser. On a été forcé de s'interroger sur qu'est-ce que ça veut dire que de

prendre des données sans autorisation, qu'est-ce que ça veut dire que d'avoir des modèles qui amplifient des biais qui apparaissent dans les données ? On a l'impression que sur le web, tout le monde s'exprime, alors qu'en fait, c'est loin d'être le cas. Ça reste beaucoup d'Occidentaux, beaucoup d'hommes. Dès qu'on est racisé, qu'on est une femme, les modèles peinent énormément."

Du côté d'Amsterdam les choses avancent également. "Récemment, nous avons organisé un atelier de conception juridique avec des acteurs de la société civile dans l'espace numérique appelé Algorithm Watch. Nous avons réuni des experts du domaine et des milieux universitaires pour formuler des suggestions visant à réglementer l'IA à usage général et l'IA générative d'une manière qui permette à l'Europe de préserver l'approche responsable de l'IA qu'elle a annoncée comme devant être adoptée. Il existe donc une série de recommandations que les décideurs politiques peuvent suivre et nous sommes également prêts à dialoguer avec les organisations qui doivent mettre en œuvre la loi."

Si l'AI et ses applications peuvent faire peur, Maxime Amblard estime que ce n'est pas l'outil lui-même que l'on doit blâmer. Pour le scientifique, c'est à la société de décider de ce qu'elle veut en faire : "Ce que je trouve intéressant derrière toutes ces discussions et derrière toutes les présentations que je peux faire, c'est de porter le message que ça n'est que du travail de scientifique. Nous produisons des outils et c'est à la société de dire si ces outils sont acceptables ou pas, s'ils doivent être intégrés à son mode de fonctionnement ou pas. Je n'ai pas à juger en tant que scientifique, je peux les juger en tant que citoyen. Et c'est la difficulté. Actuellement, les citoyens prennent l'intelligence artificielle comme quelque chose d'extraordinairement supérieur, qui doit être utilisé parce que ça existe. Mais sans s'interroger une seule seconde, qu'est-ce que c'est ? Qu'est-ce que ça fait d'une part ? Et encore moins qu'est-ce que ça produit dans la société ? Et malheureusement pour nous, scientifiques, ce serait la bonne question et je serais ravi qu'elle soit traitée, mais ce n'est pas de mon ressort en tant que scientifique."

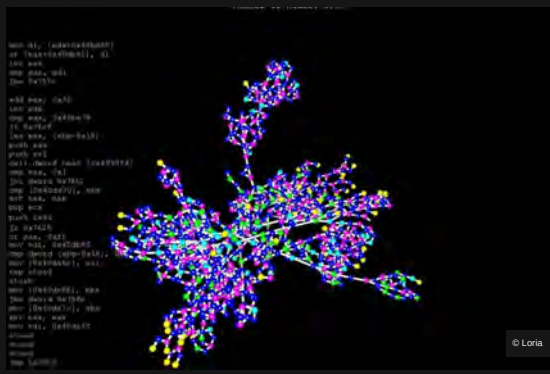
Cybersécurité : comment le Laboratoire de Haute Sécurité de Nancy analyse la morphologie des malwares pour mieux les détecter

Le Laboratoire lorrain de recherche en informatique et ses applications (Loria) abrite le Laboratoire de Haute Sécurité (LHS) à Nancy (Grand Est). Dans ce lieu sécurisé, les chercheurs étudient les logiciels malveillants (malwares) et analysent leur morphologie en vue de les détecter le plus tôt possible.

Abdessamad Attigui

27 octobre 2023 \ 10h00

3 min. de lecture



© Loria

Un malware étudié par le LHS.

Niché au cœur des locaux de l'INRIA et du Loria à Nancy, le Laboratoire de Haute Sécurité est le fer de lance de la recherche nationale en matière de cybersécurité. Depuis 2008, il s'est donné pour mission de lutter contre la prolifération de malwares, ces logiciels malveillants qui touchent les objets connectés (IoT) et les systèmes industriels (ICS/Scada). Le mercredi 25 octobre, Jean-Yves Marion, professeur à l'Université de Lorraine et chercheur au Loria, a présenté les avancées du laboratoire en la matière, notamment l'analyse morphologique, qualifiée de *« première mondiale »*.

Séparé des autres infrastructures du Loria, ce lieu clos traque, collecte et étudie des malwares de rançonnage (ransomwares) et leurs variants qui parviennent à échapper aux systèmes de protection existants en utilisant une technique d'obfuscation de code. *« Ils sont polymorphes et packés, c'est-à-dire que le fichier malveillant est caché, compressé jusqu'au moment de l'exécution »*, pointe Jean-Yves Marion.

Derrière la porte blindée, une petite pièce du LHS comporte deux éléments clés. Une salle de cluster équipée d'un « télescope virtuel » pour détecter les codes malveillants. Celui-ci surveille les vagues de cyberattaques en temps réel, permettant aux chercheurs d'observer des milliers d'attaques en direct. *« Par exemple, lors des élections américaines de 2016 ou pendant le conflit Ukraine-Russie, le télescope a enregistré des flots d'attaques sur les serveurs »*, commente le professeur.

Pour les intercepter et les collecter, le laboratoire dispose d'un « pot de miel virtuel », une ruse qui attire les cyberattaquants en leur faisant croire qu'ils ont trouvé la proie idéale. *« Ces deux infrastructures nous permettent d'analyser les malwares sans risquer de contaminer l'ensemble du réseau »*, souligne-t-il.

Caractériser les souches de virus existants

À ce jour, la base de données du LHS renferme 35 millions de malwares que les chercheurs ont minutieusement analysés pour développer une technique d'analyse dite morphologique, une avancée résultant de dix années de recherche fondamentale. Cette méthode repose sur un système d'intelligence artificielle, entraîné par apprentissage automatique, permettant d'identifier les fonctionnalités cachées dans les programmes tels que des applications et des mises à jour en se basant sur la forme du virus. Cela permet de détecter rapidement les intrusions qui échappent aux systèmes de détection existants.

Concrètement, l'approche implique de prendre en considération la structure globale d'un programme, de le désassembler, d'extraire des signatures - *« une sorte de souche de virus connu »* - et de le cartographier pour caractériser ses fonctionnalités. *« La recombinaison partielle de ces signatures permet de retrouver des similitudes entre le code analysé et un malware déjà identifié, ce qui facilite la détection des fonctionnalités indésirables dans un programme »*, souligne Jean-Yves Marion.

Le logiciel « Gorille » pour détecter des « variants »

La solution est commercialisée par la start-up Cyber-Detect, spin-off du Loria (CNRS, Inria, Université de Lorraine). Lancée en 2017, l'entreprise a transformé cet outil en une véritable arme contre les malwares à travers son logiciel « Gorille ». Avec l'analyse morphologique, il repère les dérivés des virus qui portent la même signature, avant qu'ils ne passent à l'attaque, selon la société. *« Comme en biologie, certains virus sont des mutants. Les cyberattaquants les font varier pour tromper les antivirus*, indique Régis Lhoste, son fondateur. *Nous pouvons ainsi repérer dans un virus des parts de LockBit, de DarkSide, de BlackMatter ou de ZLoader. »*

Selon les informations fournies par Cyber-Detect, ce logiciel affiche un taux de détection compris entre 95 % et 100 % pour les malwares connus, et de 90 % pour les variants. Cette solution est d'ores et déjà adoptée par des entreprises, dont Thales. Elle est utilisée pour des tâches variées, notamment l'analyse forensique visant à déterminer le mode opératoire et les conséquences post-attaque, la recherche de CVE (vulnérabilités et expositions courantes) ainsi que la vérification de l'intégrité des firmwares (mises à jour, nouvelles fonctionnalités d'un programme).

Par ailleurs, le LHS poursuit ses travaux avec en ligne de mire le développement de nouvelles approches d'analyse et de détection pour doter les *« industriels et les services étatiques de capacités d'anticipation et de réactions rapides face aux cyber-attaques »*, glisse Jean Yves Marion.

L’Est républicain, 28 octobre 2023 (édition Nancy)

Villers-lès-Nancy

La médaille scientifique du CNRS pour Math. en. JEANS du collège Chepfer

MATh. en. JEANS, c’est un slogan pour des mathématiques décontractées. C’est aussi, acronyme aidant, une méthode d’apprentissage des théories mathématiques. Le collège Chepfer est engagé dans cette démarche depuis 2008.

Une distinction qui constitue une reconnaissance pour tous les acteurs et actrices de Math.en. JEANS du collège Chepfer.

Ne pas subir les maths, mais plutôt les vivre », soulignent Ziya Findik, professeur, et Louisette Hiriart, enseignante de mathématiques retraitée, qui animent cet atelier d’apprentissage et d’ouverture où les thèmes étudiés sont sans rapport direct avec les programmes. Seuls comptent réellement rigueur, raisonnement, curiosité. Et plaisir. Ainsi, l’an dernier, à raison d’une heure hebdomadaire, dix-huit élèves volontaires de 4e et 3e s’étaient investis sur la base d’un sujet en forme de tour de magie proposé par Marie Duflot-Kremer, chercheuse de l’Inria. De la logique, de la réflexion, les élèves en situation de recherche avaient alors planché avec un évident plaisir sur ces problèmes.

« C’est l’envie de trouver sans jamais se décourager », ajoutent les enseignants, « ils en tirent une fierté, c’est très valorisant pour eux. » Cerise sur le gâteau, les activités Math. en. JEANS du collège Chepfer viennent de recevoir la médaille scientifique décernée par le CNRS.

Un dispositif innovant

« Cette récompense est une reconnaissance pour tous les acteurs et actrices de Math.en. JEANS qui, depuis des années, via un dispositif innovant, permet aux élèves du collège George-Chepfer de s’initier à la recherche mathématique et de découvrir les mathématiques comme science vivante et passionnante » indique Ziya Findik. « Elle constitue un vrai coup de chapeau pour le travail effectué, grâce notamment aux présentations réalisées dans le cadre d’un congrès national. Cette année, l’atelier Math. en. JEANS du collège Chepfer repart avec 13 élèves, dont 7 filles, avec le sujet de recherche proposé par Marie Duflot Kremer.

« Nos élèves se sont emparés des problèmes sur “Les tactiques de TIC-TAC”, avec la mise en place de stratégies basées sur des formes géométriques. Ils présenteront les résultats de leurs travaux lors du congrès qui se déroule au Luxembourg, du 15 au 17 avril 2024 ».

Lorraine

Cybercriminalité : partager le savoir pour traquer les intrusions

Face à la menace de logiciels malveillants dans nos usages quotidiens, le laboratoire Haute sécurité du Loria (Laboratoire lorrain de Recherche en Informatique et ses Applications) prône une vigilance scientifique mutualisée. Les dispositifs des hackers sont structurés de manière criminelle.

Régis Lhoste est le fondateur de la start-up Cyber-Detect, spécialisée dans la détection des malwares (logiciels malveillants). Photo Patrice Saucourt

Hôpital-ordinateur : même combat ? Avec un sas de filtrage préalable à toute entrée dans le LHS (Laboratoire Haute Sécurité) du Loria (Laboratoire lorrain de Recherche en Informatique et ses Applications), le parallèle entre la menace sanitaire du virus dans les couloirs des établissements hospitaliers et celle qui guette les systèmes numériques des sociétés contemporaines, vient à l'esprit assez naturellement.

La menace est bien réelle et plus personne ne l'ignore aujourd'hui. À la maison, sur son téléphone ou au travail, les malwares nous guettent. « Nous ne sommes plus à l'époque où le hacker s'assimilait à un adolescent boutonneux, désireux d'impressionner sa copine au fond du garage », illustre Jean-Yves Marion.

« Les objets aujourd'hui attaquables sont les objets connectés. Les attaquants disposent de moyens sophistiqués ».

« Nouvelles approches d'analyses »

Porteur du programme de cybersécurité DefMal, ce professeur à l'Université de Lorraine défend les vertus d'un partage de savoirs et de connaissances entre experts. « Cette dynamique répond aux grandes transitions de notre monde », a-t-il expliqué en milieu de semaine dans les entrailles du Loria, à des journalistes et experts de la cybercriminalité. Face à la profusion et l'intelligence des logiciels malveillants (malwares) aux aguets pour pénétrer nos codes secrets, DefMal vise à développer « de nouvelles approches d'analyse et de détection ».

Autour d'Hélène Boulanger, présidente de l'Université de Lorraine, les experts présents ont ciblé, en particulier, la nécessité d'une intervention de protection rapide dans les dispositifs de cybersécurité, pour limiter les risques. Car la course contre la montre est désormais engagée avec des univers criminels structurés et suffisamment habiles, au point de savoir eux-mêmes... protéger les malwares des dispositifs hostiles anti-malwares.

« Localiser les tentatives d'intrusion »

Le Loria s'est associé dans cette démarche avec la start-up Cyber-Détect, fruit de travaux en recherches en interne. « L'objectif est de comprendre les défis que rencontrent les entreprises, les collectivités, les institutions ou les États, et de renforcer le lien entre le monde académique et celui de l'innovation », insiste le Pr Jean-Yves Marion. Figurant parmi les dix premiers projets de recherche ciblés par le gouvernement, le programme DefMal sera ainsi porté et défendu lors de conférences internationales.

Président de Cyber-Détect, Régis Lhoste souligne au passage l'intérêt des solutions de détection du dispositif « Gorille », conscient toutefois de la nécessité de ne jamais baisser la garde. « Les collaborations de recherches nous permettent d'être au plus près des agresseurs du numérique », dit-il. « Il faut continuer de construire des outils bâtis sur la complémentarité des dispositifs pour déterminer en particulier les chemins d'attaques et localiser les tentatives d'intrusion. »

● **Antoine Pétry**

« Il faut apprendre à vivre avec l'intelligence artificielle »

« On est en train de changer de monde ». La phrase pourrait malheureusement s'appliquer à toute notre planète en crise(s). Elle concernait ce jeudi 26 octobre, au Centre de congrès Jean-Prouvé de Nancy, le numérique et nos vies désormais digitales. Pas un mois sans qu'une entreprise, un hôpital ou une collectivité ne soient attaqués et rançonnés par des hackers. Une menace invisible qui est pourtant partout, d'un mail à une clé USB, du Bluetooth au wifi de votre smartphone ou votre ordinateur.

Organisées par la Faculté de Droit de Nancy et le Loria (CNRS, Inria, Université de Lorraine), en partenariat avec la Région Grand Est, Grand E-nov, la Métropole du Grand Nancy et le laboratoire Irénée, les assises universitaires Droit et cybersécurité privilégient, comme lors de la première édition en 2022, « une approche transverse juridique, économique et organisationnelle ». « Cette rencontre interdisciplinaire est l'occasion de dresser l'état de l'art », revendiquent Jean-Yves Marion (professeur à l'Université de Lorraine, directeur du Loria) et Marc Burg (préfet chargé de mission au secrétariat général du Ministère de l'Intérieur et professeur associé à l'Université de Lorraine).

« La donnée au centre de tout »

Pour bien se rendre compte que notre rapport au temps est totalement bouleversé, prenons l'exemple de ChatGPT. Est-il encore besoin de présenter cette Intelligence artificielle (IA) conversationnelle disponible gratuitement en ligne ? En quelques mois à peine, elle s'est invitée, même imposée dans le débat. « La donnée est au centre de tout », insiste Marc Burg. « Et l'IA vient encore lui donner davantage de valeur. Rendez-vous compte : ChatGPT, lancé en 2017, intégrait 117 millions de paramètres, Un an plus tard, 1,5 milliard. Avec ChatGPT 4 sorti cette année, nous en sommes à 175 milliards de paramètres... »

ChatGPT a totalement pulvérisé sa puissance de calcul en quelques mois. Pour les professionnels réunis à Nancy, il ne faut pas interdire l'IA mais davantage apprendre à la dompter. Photo ER/Lionel Vadam

D'où cette question, soulevée en conclusion de la journée : comment canaliser cette puissance de calcul définitivement exponentielle ? » Dans les années 2000, au début d'internet, il y avait déjà des ayatollahs de la sécurité », se souvient Édouard Jeanson, Chief information security officer (Ciso) chez CapGemini France, un des experts présents en Lorraine. « Ils voulaient nous empêcher de connecter le moindre poste. Aujourd'hui, c'est pareil : il ne faut pas interdire l'IA mais apprendre à vivre avec. Se poser les bonnes questions en essayant de prendre un peu de recul. Le tout, avec beaucoup de bon sens paysan pour pouvoir se dire, si besoin : je m'arrête là. Mais en aucun cas, on peut se dire, je refuse l'IA ».

● **Paul-Marie Pernet**

AFP Infos Françaises
dimanche 29 octobre 2023

Informatique: un labo pour détecter les pirates avant intrusion

Villers-lès-Nancy (France), 29 oct 2023 (AFP) - - Détecter l'attaque informatique avant même qu'elle se concrétise : près de Nancy, dans l'est de la France, des chercheurs analysent le mode de fonctionnement des cybercriminels dans un programme de recherche unique en Europe.

Au sous-sol du Laboratoire lorrain de recherche en informatique et ses applications (Loria), à Villers-lès-Nancy, est située une salle de recherche "hautement sécurisée": ses fenêtres pourraient résister à sept coups de hache.

A l'intérieur du "laboratoire de haute sécurité" (LHS), des écrans d'ordinateur avec lesquels les chercheurs écoutent "les bruits de fond" des données, en partenariat avec le National Institute of Information and Communications Technology de Tokyo. Concrètement, des mouvements sont repérés sur des adresses IP "qui ne devraient pas être utilisées", ce qui peut présager d'une attaque à venir.

Et avec leur technique du "pot de miel", les universitaires attirent déjà au quotidien les attaquants dans des pièges, pour ensuite analyser leur mode de piratage.

La France compte deux laboratoires de haute sécurité, l'autre se trouve à Rennes, dans l'ouest du pays.

Fini le temps où les antivirus permettaient de protéger ses données face au pirate de base qui lançait ses attaques "au fond d'un garage", souligne Jean-Yves Marion, ancien directeur du Loria. Ils sont désormais plus organisés.

Ces dernières années, la menace s'est "démultipliée" selon lui, rendant "indispensable une mobilisation universitaire (...) en lien constant avec le monde de l'entreprise et des pouvoirs publics".

- Attaques sophistiquées -

Depuis la création du Loria en 2010, les chercheurs ont collecté plus de 35 millions de programmes malveillants. Si cela leur permet de les analyser et de les tester, "c'est insuffisant", insiste M. Marion.

Désormais, un nouveau programme de recherche lancé en juin, le "DefMal", pour "Défense contre les programmes malveillants", vient s'inscrire "dans une stratégie d'accélération annoncée par le président de la République", souligne Lorraine Université d'Excellence.

Présenté comme unique en Europe, un budget "inédit" de 5 millions d'euros sur six ans lui a été attribué. "Il permettra surtout d'embaucher des doctorants et des ingénieurs", selon Jean-Yves Marion.

L'enjeu, aujourd'hui, est "de détecter ces logiciels malveillants avant qu'ils ne passent à l'attaque".

Une attaque débute par l'exfiltration des données, qui sont ensuite chiffrées.

Certaines peuvent durer des mois, insistent les chercheurs: l'exfiltration se fait par petits morceaux, pour ne pas alerter.

Et signe de la professionnalisation des cybercriminels, les attaques sont de plus en plus sophistiquées, souligne Régis Lhoste, président de la société Cyber-Detect, qui a été créée dans la continuité des travaux du Loria: les programmes

malveillants sont "aujourd'hui conçus spécifiquement pour attaquer votre entreprise", sur mesure, tout en reprenant quelques structures déjà vues par le passé.

- Entreprises et institutions -

Sa jeune pousse travaille avec de nombreuses entreprises ou institutions, leur proposant son expertise pour anticiper les attaques ou les comprendre, via des analyses des virus informatiques semblables à celles utilisées dans la recherche médicale.

Abdelkader Lahmadi, enseignant-chercheur au Loria et co-fondateur, avec d'autres chercheurs, de la jeune pousse Cybi, explique que les grandes entreprises "sont submergées" par les rapports de failles de vulnérabilité qui se multiplient.

La solution mise au point par les chercheurs et désormais commercialisée, fondée sur l'intelligence artificielle, permet de "révéler les chemins d'attaque" qui pourraient être utilisés: cela peut, par exemple, débuter par le piratage d'une caméra de surveillance sur un parking, pour ensuite porter atteinte à toute l'unité de production d'un industriel.

Avec DefMal, les universitaires vont aller plus loin, en cherchant à déterminer le mode de fonctionnement des organisations cybercriminelles: comment recrutent-elles et communiquent-elles? Comment blanchissent-elles l'argent?

Cette analyse nécessite un travail "main dans la main" avec juristes et économistes, selon Jean-Yves Marion.

Les chercheurs du Loria travaillent aussi avec la police ou la gendarmerie sur certaines enquêtes.

mlx/bar/hj/pz

Informatique: un labo pour détecter les pirates avant intrusion

Source AFP
Publié le 29/10/2023 à 08h25

Informatique: un labo pour détecter les pirates avant intrusion © AFP

Détecter l'attaque informatique avant même qu'elle se concrétise : près de Nancy, des chercheurs analysent le mode de fonctionnement des cybercriminels dans un programme de recherche unique en Europe.

Au sous-sol du Laboratoire lorrain de recherche en informatique et ses applications (Loria), à Villers-lès-Nancy (Meurthe-et-Moselle), est située une salle de recherche "hautement sécurisée": ses fenêtres pourraient résister à sept coups de hache.

A l'intérieur du "laboratoire de haute sécurité" (LHS), des écrans d'ordinateur avec lesquels les chercheurs écoutent "les bruits de fond" des données, en partenariat avec le National Institute of Information and Communications Technology de Tokyo. Concrètement, des mouvements sont repérés sur des adresses IP "qui ne devraient pas être utilisées", ce qui peut présager d'une attaque à venir.

Et avec leur technique du "pot de miel", les universitaires attirent déjà au quotidien les attaquants dans des pièges, pour ensuite analyser leur mode de piratage.

La **France** compte deux laboratoires de haute sécurité, l'autre se trouve à Rennes.

Fini le temps où les antivirus permettaient de protéger ses données face au pirate de base qui lançait ses attaques "au fond d'un garage", souligne Jean-Yves Marion, ancien directeur du Loria. Ils sont désormais plus organisés.

Ces dernières années, la menace s'est "démultipliée" selon lui, rendant "indispensable une mobilisation universitaire (...) en lien constant avec le monde de l'entreprise et des pouvoirs publics".

Attaques sophistiquées

Depuis la création du Loria en 2010, les chercheurs ont collecté plus de 35 millions de programmes malveillants. Si cela leur permet de les analyser et de les tester, "c'est insuffisant", insiste M. Marion.

Désormais, un nouveau programme de recherche lancé en juin, le "DefMal", pour "Défense contre les programmes malveillants", vient s'inscrire "dans une stratégie d'accélération annoncée par le président de la République", souligne Lorraine Université d'Excellence.

Présenté comme unique en Europe, un budget "inédit" de 5 millions d'euros sur six ans lui a été attribué. "Il permettra surtout d'embaucher des doctorants et des ingénieurs", selon Jean-Yves Marion.

L'enjeu, aujourd'hui, est "de détecter ces logiciels malveillants avant qu'ils ne passent à l'attaque".

Une attaque débute par l'exfiltration des données, qui sont ensuite chiffrées.

Certaines peuvent durer des mois, insistent les chercheurs: l'exfiltration se fait par petits morceaux, pour ne pas alerter.

Et signe de la professionnalisation des cybercriminels, les attaques sont de plus en plus sophistiquées, souligne Régis Lhoste, président de la société Cyber-Detect, qui a été créée dans la continuité des travaux du Loria: les programmes malveillants sont "aujourd'hui conçus spécifiquement pour attaquer votre entreprise", sur mesure, tout en reprenant quelques structures déjà vues par le passé.

Entreprises et institutions

Sa jeune pousse travaille avec de nombreuses entreprises ou institutions, leur proposant son expertise pour anticiper les attaques ou les comprendre, via des analyses des virus informatiques semblables à celles utilisées dans la recherche médicale.

Abdelkader Lahmadi, enseignant-chercheur au Loria et co-fondateur, avec d'autres chercheurs, de la jeune pousse Cybi, explique que les grandes entreprises "sont submergées" par les rapports de failles de vulnérabilité qui se multiplient.

La solution mise au point par les chercheurs et désormais commercialisée, fondée sur l'intelligence artificielle, permet de "révéler les chemins d'attaque" qui pourraient être utilisés: cela peut, par exemple, débuter par le piratage d'une caméra de surveillance sur un parking, pour ensuite porter atteinte à toute l'unité de production d'un industriel.

Avec DefMal, les universitaires vont aller plus loin, en cherchant à déterminer le mode de fonctionnement des organisations cybercriminelles: comment recrutent-elles et communiquent-elles ? Comment blanchissent-elles l'argent ?

Cette analyse nécessite un travail "main dans la main" avec juristes et économistes, selon Jean-Yves Marion.

Les chercheurs du Loria travaillent aussi avec la police ou la gendarmerie sur certaines enquêtes.

29/10/2023 08:23:36 - Villers-lès-Nancy (France) (AFP) -

29 octobre 2023

Informatique: un labo pour détecter les pirates avant intrusion

Villers-lès-Nancy (France) (AFP) – Détecter l'attaque informatique avant même qu'elle se concrétise : près de Nancy, des chercheurs analysent le mode de fonctionnement des cybercriminels dans un programme de recherche unique en Europe.

Publié le : 29/10/2023 - 08:25 Modifié le : 29/10/2023 - 08:23 4 mn

Jean-Yves Marion, à la tête du Loria (Laboratoire lorrain de recherche en informatique et ses applications), à Villers-les-Nancy (Meurthe-et-Moselle), le 25 octobre 2023 © Jean-Christophe VERHAEGEN / AFP

Au sous-sol du Laboratoire lorrain de recherche en informatique et ses applications (Loria), à Villers-lès-Nancy (Meurthe-et-Moselle), est située une salle de recherche "hautement sécurisée": ses fenêtres pourraient résister à sept coups de hache.

A l'intérieur du "laboratoire de haute sécurité" (LHS), des écrans d'ordinateur avec lesquels les chercheurs écoutent "les bruits de fond" des données, en partenariat avec le National Institute of Information and Communications Technology de Tokyo. Concrètement, des mouvements sont repérés sur des adresses IP "qui ne devraient pas être utilisées", ce qui peut présager d'une attaque à venir.

Et avec leur technique du "pot de miel", les universitaires attirent déjà au quotidien les attaquants dans des pièges, pour ensuite analyser leur mode de piratage.

La France compte deux laboratoires de haute sécurité, l'autre se trouve à Rennes.

Fini le temps où les antivirus permettaient de protéger ses données face au pirate de base qui lançait ses attaques "au fond d'un garage", souligne Jean-Yves Marion, ancien directeur du Loria. Ils sont désormais plus organisés.

Ces dernières années, la menace s'est "démultipliée" selon lui, rendant "indispensable une mobilisation universitaire (...) en lien constant avec le monde de l'entreprise et des pouvoirs publics".

Attaques sophistiquées

Depuis la création du Loria en 2010, les chercheurs ont collecté plus de 35 millions de programmes malveillants. Si cela leur permet de les analyser et de les tester, "c'est insuffisant", insiste M. Marion.

Désormais, un nouveau programme de recherche lancé en juin, le "DefMal", pour "Défense contre les programmes malveillants", vient s'inscrire "dans une stratégie d'accélération annoncée par le président de la République", souligne Lorraine Université d'Excellence.

Un spécialiste en cybersécurité procède à une analyse morphologique d'un logiciel infecté par un virus, au Loria, à Villers-les-Nancy, le 25 octobre 2023 © Jean-Christophe VERHAEGEN / AFP

Présenté comme unique en Europe, un budget "inédit" de 5 millions d'euros sur six ans lui a été attribué. "Il permettra surtout d'embaucher des doctorants et des ingénieurs", selon Jean-Yves Marion.

L'enjeu, aujourd'hui, est "de détecter ces logiciels malveillants avant qu'ils ne passent à l'attaque".

Une attaque débute par l'exfiltration des données, qui sont ensuite chiffrées.

Certaines peuvent durer des mois, insistent les chercheurs: l'exfiltration se fait par petits morceaux, pour ne pas alerter.

Et signe de la professionnalisation des cybercriminels, les attaques sont de plus en plus sophistiquées, souligne Régis Lhoste, président de la société Cyber-Detect, qui a été créée dans la continuité des travaux du Loria: les programmes malveillants sont "aujourd'hui conçus spécifiquement pour attaquer votre entreprise", sur mesure, tout en reprenant quelques structures déjà vues par le passé.

Entreprises et institutions

Sa jeune pousse travaille avec de nombreuses entreprises ou institutions, leur proposant son expertise pour anticiper les attaques ou les comprendre, via des analyses des virus informatiques semblables à celles utilisées dans la recherche médicale.

Abdelkader Lahmadi, enseignant-chercheur au Loria et co-fondateur, avec d'autres chercheurs, de la jeune pousse Cybi, explique que les grandes entreprises "sont submergées" par les rapports de failles de vulnérabilité qui se multiplient.

Le professeur Jean-Yves Marion, dirigeant du Loria, devant un écran montrant l'analyse dynamique par le logiciel Gorille d'un programme infecté, à Villers-les-Nancy, le 25 octobre 2023 © Jean-Christophe VERHAEGEN / AFP

La solution mise au point par les chercheurs et désormais commercialisée, fondée sur l'intelligence artificielle, permet de "révéler les chemins d'attaque" qui pourraient être utilisés: cela peut, par exemple, débuter par le piratage d'une caméra de surveillance sur un parking, pour ensuite porter atteinte à toute l'unité de production d'un industriel.

Avec DefMal, les universitaires vont aller plus loin, en cherchant à déterminer le mode de fonctionnement des organisations cybercriminelles: comment recrutent-elles et communiquent-elles ? Comment blanchissent-elles l'argent ?

Cette analyse nécessite un travail "main dans la main" avec juristes et économistes, selon Jean-Yves Marion.

Les chercheurs du Loria travaillent aussi avec la police ou la gendarmerie sur certaines enquêtes.

Montpellier : à l'université Paul Valéry, un laboratoire de recherche consacré au bégaiement

À l'université Paul Valéry, Fabrice Hirsch dirige le laboratoire Praxiling, initiateur du projet BENEPHIDIRE visant à établir les origines du bégaiement.

Guillaume Herbet, neuropsychologue (à gauche) et Fabrice Hirsch, directeur du laboratoire Praxiling (à droite). (©Métropolitain / LP)

Par Léa Pippinato

Publié le 29 oct. 2023 à 14h36

« Les gens ont souvent cette idée préconçue selon laquelle le bégaiement serait d'ordre psychologique », souligne Fabrice Hirsch, directeur du **laboratoire Praxiling** de l'université Paul Valéry de Montpellier, regroupant chercheurs en analyse de discours, en phonétique et en sciences cognitives. Celui-ci travaille actuellement sur le **projet BENEPHIDIRE**, acronyme signifiant « Bégaiement : la neurologie, la phonétique et l'informatique pour son diagnostic et sa rééducation ». Son objectif est d'identifier **les réseaux neuronaux à l'origine du bégaiement** afin d'en améliorer le diagnostic et la prise en charge, mais aussi d'affiner le pronostic quant à son évolution. Pour mener de telles recherches, Fabrice Hirsch n'est pas seul. Praxiling est en effet accompagné de deux autres laboratoires, le Loria (Laboratoire Lorrain de Recherche en Informatique et ses Applications) à Nancy et le LiLPa (Linguistique, Langues, Parole) à Strasbourg.

Des recherches à la croisée des disciplines

En plus des laboratoires, le chercheur au CNRS bénéficie de l'appui du neuropsychologue Guillaume Herbet ainsi que du neurochirurgien Hugues Duffau. « Je m'occupe de toute la partie neuroscientifique. L'idée est de savoir si certains réseaux neuronaux dysfonctionnent chez les patients qui bégayent », détaille Guillaume Herbet. Afin de savoir si une région du cerveau est fonctionnelle, celui-ci a recours à la **chirurgie éveillée du cerveau**, généralement utilisée lors de l'extraction d'une tumeur. Dans ce cas, le patient est, réveillé, et peut interagir avec le chirurgien mais aussi les neuropsychologues et l'orthophoniste pendant la chirurgie. C'est ainsi qu'il a été découvert que certaines connexions stimulent le bégaiement. « Cela permet de dresser des hypothèses sur ce qui se passe dans le cerveau au moment du bégaiement. On voit donc quelles connexions sont anormales et comment le cerveau se déconnecte lorsqu'un patient bégaye », explique Guillaume Herbet.

À lire aussi

Montpellier. Santé : le CHU rénove son département de chirurgie pédiatrique

Au-delà de détecter les anomalies, ces travaux visent à améliorer la prise en charge du bégaiement. « Si on détecte des connexions anormales, cela peut stimuler une réflexion sur des stratégies thérapeutiques pour améliorer le bégaiement », pointe du doigt le neuropsychologue

améliorer le bégaiement », pointe du doigt le neuropsychologue.

Une étude clinique sur 60 sujets

Afin de compléter ces recherches, une étude clinique a été menée en partenariat avec les CHU de Montpellier et de Nancy pour évaluer **la disfluence verbale**, c'est-à-dire les anomalies dans le discours. Pour cela, **60 personnes**, 30 sujets bègues, plus ou moins impactés par le trouble, et 30 sujets « contrôle », ont été mobilisées. Dans un premier temps, celles-ci ont passé une **tractographie**, soit une cartographie des fibres cérébrales dans le but de les corréler au bégaiement. Moins elles sont développées et plus elles sont liées au bégaiement. Vient ensuite une partie consacrée à une **imagerie fonctionnelle**, durant laquelle les sujets effectuent une tâche. « On leur donne des mots et ils doivent générer une phrase avec. C'est un exercice très difficile pour le sujet bègue, mais cela permet de voir les activations dans le cerveau durant la tâche », concède Fabrice Hirsch.

À lire aussi

Montpellier. Santé, robots et sciences sociales : l'Université distingue 5 chercheurs

Un projet en plusieurs étapes

Pour ce qui est des résultats, les chercheurs ont commencé à acquérir des données il y un an et demi. Celles-ci sont actuellement en phase de traitement, les premiers résultats n'allant voir le jour que dans six mois. Cependant, le projet BENEPHIDIRE ne s'arrête pas là et comporte trois gros volets, dont un déjà abordé sur la neurologie du bégaiement. Les deux autres portent respectivement sur **la production de la parole chez les personnes bègues** et **le traitement informatique du bégaiement**. Des résultats ont déjà pu être mis en évidence pour le second. « Le bégaiement se manifeste par la prolongation, le blocage ou la répétition

des sons. Les recherches ont montré que ces trois formes de bégaiement ne sont basées que sur ce qu'entend l'orthophoniste. Par exemple, une répétition peut se manifester par des sons successifs, mais cela peut aussi être dû aux articulateurs du larynx qui s'arrêtent pendant un moment », explicite Fabrice Hirsch.

D'où vient le bégaiement ?

Cependant, les causes du bégaiement restent floues, même si certaines précisions ont pu être apportées. « Ce n'est pas une maladie, mais un trouble. Il s'agit du reflet du dysfonctionnement cérébral », insiste Fabrice Hirsch. **« On sait que c'est multifactoriel**, des études laissent penser que c'est lié à un trouble neurologique. Le bégaiement touche davantage les hommes que les femmes. Même si les chiffres varient, on est sur quatre hommes touchés pour seulement une femme », détaille le chercheur. Déterminer les causes du bégaiement est d'autant plus complexe qu'il en existe deux grandes familles : d'un côté **le bégaiement développemental** naissant lors de l'acquisition du langage, pouvant se régler ou non à l'aide d'un orthophoniste, et **le bégaiement acquis**, faisant suite à une lésion cérébrale. « Il y a même des cas de **bégaiement masqué**, où les personnes vont utiliser des synonymes pour remplacer les mots sur lesquels elles ont des difficultés », complète Fabrice Hirsch.

À lire aussi

Montpellier : Okba combat son bégaiement en échangeant avec les passants sur la Comédie

Bien qu'il ne s'agisse pas d'une maladie, le bégaiement **peut se révéler difficile à vivre**, surtout pour les enfants, bloqués à l'idée de prendre la parole en cours. « Les personnes bègues sont frustrées de ne pas réussir à exprimer ce qu'elles veulent et ont constamment le sentiment d'être jugées sur leur façon de parler plutôt que sur leur contenu », déplore le directeur de Praxiling, avant d'ajouter qu'il existe « autant de bégaiements que de personnes bègues », toutes n'allant pas rencontrer les mêmes obstacles selon la lourdeur de leur trouble.

El Watan-dz .com

Informatique : Un labo pour détecter les pirates avant intrusion

30/10/2023 mis à jour: 20:52 AFP 1178

Le Professeur Jean-Yves Marion, directeur du Loria prononce un discours devant un écran montrant l'analyse dynamique d'un logiciel contenant un malware dans le logiciel de cybersécurité Gorille le 25 octobre 2023 (Photo, AFP).

Au sous-sol du Laboratoire lorrain de recherche en informatique et ses applications (Loria), à Villers-lès-Nancy, est située une salle de recherche «hautement sécurisée» : ses fenêtres pourraient résister à sept coups de hache.

A l'intérieur du «laboratoire de haute sécurité» (LHS), des écrans d'ordinateur avec lesquels les chercheurs écoutent «les bruits de fond» des données, en partenariat avec le National Institute of Information and Communications Technology de Tokyo. Concrètement, des mouvements sont repérés sur des adresses IP «qui ne devraient pas être utilisées», ce qui peut présager d'une attaque à venir. Et avec leur technique du «pot de miel», les universitaires attirent déjà au quotidien les attaquants dans des pièges, pour ensuite analyser leur mode de piratage.

La France compte deux laboratoires de haute sécurité, l'autre se trouve à Rennes, dans l'ouest du pays. Fini le temps où les antivirus permettaient de protéger ses données face au pirate de base qui lançait ses attaques «au fond d'un garage», souligne Jean-Yves Marion, ancien directeur du Loria. Ils sont désormais plus organisés. Ces dernières années, la menace s'est «démultipliée» selon lui, rendant «indispensable une mobilisation universitaire (...) en lien constant avec le monde de l'entreprise et des pouvoirs publics».

Attaques sophistiquées

Depuis la création du Loria en 2010, les chercheurs ont collecté plus de 35 millions de programmes malveillants. Si cela leur permet de les analyser et de les tester, «c'est insuffisant», insiste M. Marion. Désormais, un nouveau programme de recherche lancé en juin, le DefMal, pour «Défense contre les programmes malveillants», vient s'inscrire «dans une stratégie d'accélération annoncée par le président de la République», souligne Lorraine Université d'Excellence.

Présenté comme unique en Europe, un budget «inédit» de 5 millions d'euros sur 6 ans lui a été attribué. «Il permettra surtout d'embaucher des doctorants et des ingénieurs», selon Jean-Yves Marion. L'enjeu, aujourd'hui, est «de détecter ces logiciels malveillants avant qu'ils ne passent à l'attaque».

Une attaque débute par l'exfiltration des données, qui sont ensuite chiffrées. Certaines peuvent durer des mois, insistent les chercheurs : l'exfiltration se fait par petits morceaux, pour ne pas alerter. Et signe de la professionnalisation des cybercriminels, les attaques sont de plus en plus sophistiquées, souligne Régis Lhoste, président de la société Cyber-Detect, qui a été créée dans la continuité des travaux du Loria : les programmes malveillants sont «aujourd'hui conçus spécifiquement pour attaquer votre entreprise», sur mesure, tout en reprenant quelques structures déjà vues par le passé.

Entreprises et institutions

Sa jeune pousse travaille avec de nombreuses entreprises ou institutions, leur proposant son expertise pour anticiper les attaques ou les comprendre, via des analyses des virus informatiques semblables à celles utilisées dans la recherche médicale. Abdelkader Lahmadi, enseignant-chercheur au Loria et co-fondateur, avec d'autres chercheurs, de la jeune pousse Cybi, explique que les grandes entreprises «sont submergées» par les rapports de failles de vulnérabilité qui se multiplient. La solution mise au point par les chercheurs et désormais commercialisée, fondée sur l'intelligence artificielle, permet de «révéler les chemins d'attaque» qui pourraient être utilisés : cela peut, par exemple, débuter par le piratage d'une caméra de surveillance sur un parking, pour ensuite porter atteinte à toute l'unité de production d'un industriel.

Avec DefMal, les universitaires vont aller plus loin, en cherchant à déterminer le mode de fonctionnement des organisations cybercriminelles : comment recrutent-elles et communiquent-elles ? Comment blanchissent-elles l'argent ? Cette analyse nécessite un travail «main dans la main» avec juristes et économistes, selon Jean-Yves Marion. Les chercheurs du Loria travaillent aussi avec la police ou la gendarmerie sur certaines enquêtes.

Tags: #Sécurité informatique #Elwatan #Magazine #labo #intrusion

Dépêche n° 701738
Sécurité globale - Sécurité publique
Par: Romain Haillard - Publiée le 30/10/2023 à 15h55
Lien dépêche

4 min de lecture

Avec DefMal, la recherche contre les logiciels malveillants veut "sortir du laboratoire" et aider les forces de l'ordre

"L'objectif de DefMal est de comprendre l'écosystème des cybercriminels et de lutter contre", résume Jean-Yves Marion, qui a été directeur du Loria (Laboratoire lorrain de recherche en informatique et ses applications) pendant dix ans. À l'occasion des assises universitaires du droit et de la cybersécurité à Nancy, le professeur a mis en avant ce projet financé par l'État à hauteur de 5 millions d'euros sur six ans. Le programme ne fera pas seulement de la recherche fondamentale mais aspire à créer des outils pour et avec ses partenaires, dont la SDLC, le Comcybergend, l'OCLCTIC, la BL2C.

Sur l'une des vitres du LHS (laboratoire de haute sécurité) du Loria, des post-it forment un rond jaune fendu d'une grande bouche poursuivant un fantôme, une référence à Pac Man, célèbre jeu d'arcade. Le DefMal, pour Defence against Malware (défense contre les logiciels malveillants), tout jeune programme de recherche de cette unité mixte (CNRS, Inria, et université de Lorraine), a le même objectif : poursuivre les logiciels malveillants. La dizaine de chercheurs affiliée au programme, un nombre appelé à doubler d'ici 12 à 18 mois, va orienter ses recherches vers une meilleure compréhension de l'écosystème de la cybercriminalité.

5 millions d'euros

Les recherches ne mobiliseront pas seulement des informaticiens, mais également des juristes, des sociologues et des économistes. "Il faut étudier le recrutement au sein des groupes d'affiliés cybercriminels, le suivi des cryptoactifs et des circuits de blanchiment", explique Jean-Yves Marion, professeur à l'université de Lorraine et responsable du programme. "L'idée, c'est ensuite de pouvoir anticiper leurs prochains mouvements à partir de signaux faibles."

Le programme de recherche commence ses travaux après avoir obtenu en 2022 un financement de 5 millions d'euros étalés sur six ans avec le plan d'investissement de l'État France 2030. "C'est beaucoup pour de la recherche en informatique", souligne celui qui a dirigé le laboratoire de 2013 à 2023. Il souligne le caractère exceptionnel de ce financement : "Il y a dix ans, peu d'universitaires et de chercheurs français travaillaient sur la cybersécurité et ils étaient très peu visibles." Le programme DefMal va également candidater pour un financement européen du fonds Horizon Europe Framework Programme, dont une partie soutient les projets pour lutter contre les cybermenaces.

De nombreuses institutions policières partenaires

Parmi les partenaires de DefMal figurent la SDLC (sous-direction de la lutte contre la cybercriminalité de la DNPJ), le Comcybergend, l'OCLCTIC, la BL2C (brigade de lutte contre la cybercriminalité de la Préfecture de police), la SDAEF (sous-direction des affaires économiques et financières de la Préfecture de olice) et la DRPJ. "Nous avons discuté avec les forces de l'ordre et la justice pour orienter les bonnes questions de recherche", rapporte l'expert en informatique, désireux d'avoir des débouchés opérationnels pour son programme. De ces discussions ont découlé de grandes orientations du programme : "Nous voulons travailler sur le Forensic, c'est-à-dire l'analyse post-mortem d'une cyberattaque. L'idée est de savoir ce qu'il s'est passé, quelles données ont été altérées ou exfiltrées, reconnaître le mode opératoire d'attaque de groupes déjà existants pour éventuellement faire de l'attribution."

Les gendarmes seraient particulièrement intéressés par l'étude des objets connectés, sur laquelle elle travaille déjà (lire sur AEF info). "À partir d'un produit, étudier ses fonctionnalités, connaître s'il existe aussi des fonctionnalités cachées et d'éventuelles portes dérobées", développe l'universitaire. L'une des parties du programme pourrait basculer vers un volet plus offensif, "avec beaucoup de réserves", précise Jean-Yves Marion. "Faire de la recherche du côté du hacking éthique, pour envisager des ripostes après attaque ou pour des applications en infiltration dans le cadre d'enquête : cette question scientifique est plus excitante, parce qu'il y a un réel changement de posture par rapport à une culture très défensive."

Une analyse morphologique des logiciels

Le programme ne va pas se limiter à des publications scientifiques. "Développer des outils fait partie de notre feuille de route. Nous ferons aussi des prototypes pour les mettre à disposition de nos partenaires", précise Jean-Yves Marion. L'expression revient souvent, les scientifiques du Loria veulent "sortir du laboratoire". À ce titre, Cyber-detect fait figure d'exemple. Cette start-up et son outil Gorille sortent tout droit des travaux du laboratoire lorrain. Régis Lhoste, passé lui aussi par le LHS, a fondé cette entreprise en 2017 après dix années de recherche. Il exploite ses travaux sur l'analyse morphologique des logiciels malveillants et va aussi les mettre au service du programme DefMal.

Cette analyse issue du Loria permet de reconnaître les logiciels malveillants par leur composition. "De plus en plus, les attaques deviennent sophistiquées et les logiciels malveillants sont fabriqués spécialement pour une attaque", explique le cofondateur de Cyber-detect. Parce que ces logiciels sont confectionnés et donc considérés comme nouveaux, ils passent plus facilement sous les radars des antivirus ou EDR (Endpoint Detection and Response), les outils classiques de détection de menaces.

"Contrairement aux EDR, nous ne nous intéressons pas à la forme complète d'un exécutable, mais aux morceaux de codes potentiellement malveillants." Régis Lhoste explique : "Un hacker va réécrire d'une nouvelle manière des lignes de code déjà écrites et déjà utilisées. S'il y a un petit bout de BlackMatter ou de HermerticWiper - deux malwares connus - alors je le détecte, je sais ce qu'il va faire et comment réagir, faire de l'identification de menace et de l'attribution. L'objectif, c'est de les détecter avant qu'ils fassent des dégâts." Selon une étude menée par l'Enisa entre 2021 et 2022, les rançongiciels auraient provoqué 18 milliards d'euros de dommages, soit 57 fois plus qu'en 2015.

Habitat & urbanisme, Sécurité Globale) à leurs abonnés un service d'information continue par courrier électronique et via l'application mobile. Être abonné à ces services, c'est avoir l'assurance d'être informé rapidement, précisément et objectivement des faits essentiels.

Cliquez ici pour tester gratuitement les services d'information AEF info

---

Cybercriminalité

Ce labo lorrain est à la pointe de la lutte contre les pirates

RTL avec AFP | Actualisé: 31.10.2023 06:10

Jean-Yves Marion, à la tête du Loria (Laboratoire lorrain de recherche en informatique et ses applications), à Villers-les-Nancy (Meurthe-et-Moselle), le 25 octobre 2023 / © AFP

Détecter l'attaque informatique avant même qu'elle se concrétise : près de Nancy, des chercheurs analysent le mode de fonctionnement des cybercriminels dans un programme de recherche unique en Europe.

Au sous-sol du Laboratoire lorrain de recherche en informatique et ses applications (Loria), à Villers-lès-Nancy, Meurthe-et-Moselle, est située une salle de recherche *"hautement sécurisée"*: ses fenêtres pourraient résister à sept coups de hache.

À l'intérieur du *"laboratoire de haute sécurité"* (LHS), des écrans d'ordinateur avec lesquels les chercheurs écoutent *"les bruits de fond"* des données, en partenariat avec le National Institute of Information and Communications Technology de Tokyo. Concrètement, des mouvements sont repérés sur des adresses IP *"qui ne devraient pas être utilisées"*, ce qui peut présager d'une attaque à venir.

Et avec leur technique du *"pot de miel"*, **les universitaires attirent déjà au quotidien les attaquants dans des pièges**, pour ensuite analyser leur mode de piratage.

La France compte deux laboratoires de haute sécurité, l'autre se trouve à Rennes.

Fini le temps où les antivirus permettaient de protéger ses données face au pirate de base qui lançait ses attaques *"au fond d'un garage"*, souligne Jean-Yves Marion, ancien directeur du Loria. Ils sont désormais plus organisés. Ces dernières années, la menace s'est *"démultipliée"* selon lui, rendant *"indispensable une mobilisation universitaire (...) en lien constant avec le monde de l'entreprise et des pouvoirs publics"*.

Les plus lus

1 Mortellement fauchée hier soir
Le jeune conducteur sans permis se rend aux gendarmes

2 Célibataires, familles, parents isolés...
Voici les baisses d'impôt dont vous allez profiter en 2025 au Luxembourg

3 Incendie à Esch
Cinq personnes évacuées aux urgences

4 Drame à Paris
Un automobiliste fonce sur la terrasse d'un café, faisant un mort et six blessés

5 Les frontaliers privés de trains
"Ça va être compliqué de tenir un mois comme ça"

Un spécialiste en cybersécurité procède à une analyse morphologique d'un logiciel infecté par un virus, au Loria, à Villers-les-Nancy, le 25 octobre 2023 / © AFP

Depuis la création du Loria en 2010, **les chercheurs ont collecté plus de 35 millions de programmes malveillants**. Si cela leur permet de les analyser et de les tester, *"c'est insuffisant"*, insiste M. Marion.

Désormais, un nouveau programme de recherche lancé en juin, le "DefMal", pour *"Défense contre les programmes malveillants"*, vient s'inscrire **"dans une stratégie d'accélération annoncée par le président de la République"**, souligne Lorraine Université d'Excellence.

Présenté comme unique en Europe, **un budget *"inédit"* de 5 millions d'euros sur six ans lui a été attribué**. *"Il permettra surtout d'embaucher des doctorants et des ingénieurs"*, selon Jean-Yves Marion.

L'enjeu, aujourd'hui, est *"de détecter ces logiciels malveillants avant qu'ils ne passent à l'attaque"*. Une attaque débute par l'exfiltration des données, qui sont ensuite chiffrées. Certaines peuvent durer des mois, insistent les chercheurs: l'exfiltration se fait par petits morceaux, pour ne pas alerter.

Et signe de la professionnalisation des cybercriminels, les attaques sont de plus en plus sophistiquées, souligne Régis Lhoste, président de la société Cyber-Detect, qui a été créée dans la continuité des travaux du Loria: les programmes malveillants sont *"aujourd'hui conçus spécifiquement pour attaquer votre entreprise"*, sur mesure, tout en reprenant quelques structures déjà vues par le passé.

Sa jeune pousse travaille avec de nombreuses entreprises ou institutions, leur proposant son expertise pour anticiper les attaques ou les comprendre, via des analyses des virus informatiques semblables à celles utilisées dans la recherche médicale.

Le professeur Jean-Yves Marion, dirigeant du Loria, devant un écran montrant l'analyse dynamique par le logiciel Gorille d'un programme infecté, à Villers-les-Nancy, le 25 octobre 2023 / © AFP

Abdelkader Lahmadi, enseignant-chercheur au Loria et co-fondateur, avec d'autres chercheurs, de la jeune pousse Cybi, explique que **les grandes entreprises *"sont submergées"* par les rapports de failles de vulnérabilité** qui se multiplient.

La solution mise au point par les chercheurs et désormais commercialisée, fondée sur l'intelligence artificielle, permet de *"révéler les chemins d'attaque"* qui pourraient être utilisés: **cela peut, par exemple, débuter par le piratage d'une caméra de surveillance sur un parking**, pour ensuite porter atteinte à toute l'unité de production d'un industriel.

Avec DefMal, les universitaires vont aller plus loin, en cherchant à déterminer le mode de fonctionnement des organisations cybercriminelles: comment recrutent-elles et communiquent-elles ? Comment blanchissent-elles l'argent ?

Cette analyse nécessite un travail *"main dans la main"* avec juristes et économistes, selon Jean-Yves Marion. Les chercheurs du Loria travaillent aussi avec la police ou la gendarmerie sur certaines enquêtes.

Informatique: un labo pour détecter les pirates avant intrusion

Par ETX Studio

Publié le 01/11/23 à 20:15

Au sous-sol du Laboratoire lorrain de recherche en informatique et ses applications (Loria), à Villers-lès-Nancy, est située une salle de recherche "hautement sécurisée": ses fenêtres pourraient résister à sept coups de hache.
JEAN-CHRISTOPHE VERHAEGEN / AFP

Détecter l'attaque informatique avant même qu'elle se concrétise : près de Nancy, dans l'est de la France, des chercheurs analysent le mode de fonctionnement des cybercriminels dans un programme de recherche unique en Europe....

Détecter l'attaque informatique avant même qu'elle se concrétise : près de Nancy, dans l'est de la France, des chercheurs analysent le mode de fonctionnement des cybercriminels dans un programme de recherche unique en Europe.

Au sous-sol du Laboratoire lorrain de recherche en informatique et ses applications (Loria), à Villers-lès-Nancy, est située une salle de recherche "hautement sécurisée": ses fenêtres pourraient résister à sept coups de hache.

A l'intérieur du "laboratoire de haute sécurité" (LHS), des écrans d'ordinateur avec

En continu

13:00 Marseille : il voulait se suicider et passe la nuit en garde à vue, son chien abattu par les policiers

12:54 Terrasse percutée par une voiture à Paris : "l'acte pourrait être intentionnel"

12:21 Festival d'Avignon Off : "Michelle doit-on t'en vouloir d'avoir fait un selfie à Auschwitz ?", une interrogation sur notre rapport avec les réseaux sociaux. On a adoré

12:12 Festival d'Avignon OFF : "Close Up", art de la fugue ou du combat ?

12:11 P Festival d'Avignon OFF : la beauté glacée du théâtre de Warlikowski jette un froid au Palais des papes

12:11 INFO LA PROVENCE. Baptiste Lecaplain va tourner un film sur le Festival d'Avignon

12:01 Logement social attribué à la mère de Nora Preziosi : le

lesquels les chercheurs écoutent "les bruits de fond" des données, en partenariat avec le National Institute of Information and Communications Technology de Tokyo. Concrètement, des mouvements sont repérés sur des adresses IP "qui ne devraient pas être utilisées", ce qui peut présager d'une attaque à venir.

Et avec leur technique du "pot de miel", les universitaires attirent déjà au quotidien les attaquants dans des pièges, pour ensuite analyser leur mode de piratage.

La France compte deux laboratoires de haute sécurité, l'autre se trouve à Rennes, dans l'ouest du pays.

Fini le temps où les antivirus permettaient de protéger ses données face au pirate de base qui lançait ses attaques "au fond d'un garage", souligne Jean-Yves Marion, ancien directeur du Loria. Ils sont désormais plus organisés.

Ces dernières années, la menace s'est "démultipliée" selon lui, rendant "indispensable une mobilisation universitaire (...) en lien constant avec le monde de l'entreprise et des pouvoirs publics".

- Attaques sophistiquées -

Depuis la création du Loria en 2010, les chercheurs ont collecté plus de 35 millions de programmes malveillants. Si cela leur permet de les analyser et de les tester, "c'est insuffisant", insiste M. Marion.

Désormais, un nouveau programme de recherche lancé en juin, le "DefMal", pour "Défense contre les programmes malveillants", vient s'inscrire "dans une stratégie d'accélération annoncée par le président de la République", souligne Lorraine Université d'Excellence.

Présenté comme unique en Europe, un budget "inédit" de 5 millions d'euros sur six ans lui a été attribué. "Il permettra surtout d'embaucher des doctorants et des ingénieurs", selon Jean-Yves Marion.

L'enjeu, aujourd'hui, est "de détecter ces logiciels malveillants avant qu'ils ne passent à l'attaque".

Une attaque débute par l'exfiltration des données, qui sont ensuite chiffrées.

Certaines peuvent durer des mois, insistent les chercheurs: l'exfiltration se fait par petits morceaux, pour ne pas alerter.

Et signe de la professionnalisation des cybercriminels, les attaques sont de plus en plus sophistiquées, souligne Régis Lhoste, président de la société Cyber-Detect, qui a été créée dans la continuité des travaux du Loria: les programmes malveillants sont "aujourd'hui conçus spécifiquement pour attaquer votre entreprise", sur mesure, tout en reprenant quelques structures déjà vues par le passé.

- Entreprises et institutions -

Sa jeune pousse travaille avec de nombreuses entreprises ou institutions, leur proposant son expertise pour anticiper les attaques ou les comprendre, via des analyses des virus informatiques semblables à celles utilisées dans la recherche médicale.

Abdelkader Lahmadi, enseignant-chercheur au Loria et co-fondateur, avec d'autres chercheurs, de la jeune pousse Cybi, explique que les grandes entreprises "sont submergées" par les rapports de failles de vulnérabilité qui se multiplient.

La solution mise au point par les chercheurs et désormais commercialisée, fondée sur l'intelligence artificielle, permet de "révéler les chemins d'attaque" qui pourraient être utilisés: cela peut, par exemple, débuter par le piratage d'une caméra de surveillance sur un parking, pour ensuite porter atteinte à toute l'unité de production d'un industriel.

Avec DefMal, les universitaires vont aller plus loin, en cherchant à déterminer le mode de fonctionnement des organisations cybercriminelles: comment recrutent-elles et communiquent-elles? Comment blanchissent-elles l'argent?

Cette analyse nécessite un travail "main dans la main" avec juristes et économistes

parquet de Marseille ouvre une enquête

11:57 Guerre à Gaza : le ministère de la Santé du Hamas annonce un nouveau bilan de 38.848 morts

Plus d'infos →

Les plus lus

1 L'A55 à la sortie de Marseille a dû fermer en raison de la panne d'un poids lourd

RÉGION

2 L'Abbé Pierre accusé, dans un rapport, d'agressions sexuelles par plusieurs femmes

selon Jean-Yves Marion.

Les chercheurs du Loria travaillent aussi avec la police ou la gendarmerie sur certaines enquêtes.

FAITS DIVERS - JUSTICE

3 "Maman est tombée, elle ne peut plus se réveiller" : à 4 ans, Shannon alerte les

TECHNOS CYBERSÉCURITÉ L'USINE 4.0 FACE AU RISQUE CYBER

« Avec DefMal, nous voulons développer des outils de prédiction des cyberattaques », dévoile Jean-Yves Marion, du Loria

Implanté à Nancy, le laboratoire de haute sécurité (LHS) du laboratoire lorrain de recherche en informatique et ses applications (Loria) a fait de l'analyse des logiciels malveillants (malwares), sa spécialité. Jean-Yves Marion, professeur à l'Université de Lorraine et chercheur au Loria, nous éclaire sur l'importance de la recherche fondamentale sur les cyberattaques pour garantir la sécurité des industriels.

Réservé aux abonnés

Propos recueillis par Abdessamad Attigui

02 novembre 2023
10h00

3 min. de lecture

Jean-Yves Marion, professeur à l'Université de Lorraine et chercheur au Loria.

Quelle est la tendance en matière de cyberattaques, en particulier dans le monde industriel ?

Actuellement, nous observons deux principaux types d'attaques. Le premier concerne principalement l'espionnage et le vol d'informations, tandis que le second est lié aux attaques par rançongiciel (ransonware, ndlr). Ces deux types d'attaque ne sont pas totalement indépendants, car les rançongiciels peuvent également exfiltrer des informations avant de bloquer le système.

En ce qui concerne ces attaques, on applique une grille de lecture simple : la CIA, pour Confidentialité, Intégrité et Accessibilité. La confidentialité concerne les risques liés à l'espionnage, l'intégrité des systèmes est impactée par les rançongiciels, et

IA, chiffrement homomorphe et télé-assistance : zoom sur le futur équipement intelligent de laminage et de planage de Redex et Siemens IT

Cybersécurité : comment le Laboratoire de Haute Sécurité de Nancy analyse la morphologie des malwares pour mieux les détecter IT

l'accessibilité concerne les attaques de type déni de service visant à bloquer les serveurs de l'entreprise pour pousser la proie à payer.

Quels sont les secteurs industriels les plus vulnérables ?

Selon les rapports, les secteurs industriels les plus touchés par les cyberattaques incluent généralement ceux qui gèrent des infrastructures critiques et des données

Dans le bunker anti-cyberattaques de Nancy où les chercheurs piègent les pirates du web

INFORMATIQUE CYBERSÉCURITÉ INTELLIGENCE ARTIFICIELLE SÉCURITÉ

ACTUALITÉ - 3 MIN

PAR FUTURA AVEC ETX DAILY UP

LE 4 NOVEMBRE 2023

La cybercriminalité touche désormais de nombreuses entreprises ou institutions avec des attaques virales de plus en plus sophistiquées. Dans ce laboratoire hautement sécurisé du Loria, les chercheurs examinent tous les mouvements suspects signalant l'activité de programmes malveillants. Grâce au programme de recherche « Défense contre les programmes malveillants », ils ont pour mission de détecter les attaques informatiques avant qu'elles ne se déclenchent.

AU SOMMAIRE

CELA VOUS INTÉRESSERA AUSSI

[EN VIDÉO] Qu'est-ce qu'une cyberattaque ? Avec le développement d'Internet et du cloud, les cyberattaques sont de plus en plus fréquentes...

Détecter l'**attaque informatique** avant même qu'elle se concrétise : près de Nancy, dans l'est de la France, des chercheurs analysent le mode de fonctionnement des cybercriminels dans un programme de recherche unique en Europe. Au sous-sol du Laboratoire lorrain de recherche en informatique et ses applications (Loria), à Villers-

lès-Nancy, est située une salle de recherche « hautement sécurisée » : ses fenêtres pourraient résister à sept coups de hache.

À l'intérieur du « laboratoire de haute sécurité » (LHS), des **écrans d'ordinateur** avec lesquels les chercheurs écoutent « les bruits de fond » des données, en partenariat avec le *National Institute of Information and Communications Technology* de Tokyo. Concrètement, des mouvements sont repérés sur des **adresses IP** « *qui ne devraient pas être utilisées* », ce qui peut présager d'une attaque à venir. Et avec leur technique du « pot de miel », les universitaires attirent déjà au quotidien les attaquants dans des pièges, pour ensuite analyser leur mode de piratage.

VOIR AUSSI *Intelligence artificielle : les risques d'une utilisation malveillante*

La France compte deux laboratoires de haute sécurité, l'autre se trouve à Rennes, dans l'ouest du pays. Fini le temps où les antivirus permettaient de protéger ses données face au pirate de base qui lançait ses attaques « ***au fond d'un garage*** », souligne Jean-Yves Marion, ancien directeur du Loria. Ils sont désormais plus organisés. Ces dernières années, **la menace s'est démultipliée** selon lui, rendant « *indispensable une mobilisation universitaire (...) en lien constant avec le monde de l'entreprise et des pouvoirs publics* ».

LE PROFESSEUR JEAN-YVES MARION, DIRECTEUR DU LORIA, ICI, AU SOUS-SOL DU LABORATOIRE LORRAIN DE RECHERCHE EN INFORMATIQUE ET SES APPLICATIONS, À VILLERS-LÈS-NANCY, DANS UNE SALLE DE RECHERCHE HAUTEMENT SÉCURISÉE DONT LES FENÊTRES POURRAIENT RÉSISTER À SEPT COUPS DE HACHE. © JEAN-CHRISTOPHE VERHAEGEN, AFP

Des attaques de plus en plus sophistiquées visant les entreprises

Depuis la création du Loria en 2010, les chercheurs ont collecté plus de 35 millions de **programmes malveillants**. Si cela leur permet de les analyser et de les tester, « *c'est insuffisant* », insiste M. Marion. Désormais, un nouveau programme de recherche lancé en juin, le « *DefMal* » -- pour Défense contre les programmes malveillants -- vient s'inscrire « *dans une stratégie d'accélération annoncée par le président de la République* », souligne Lorraine Université d'Excellence.

Présenté comme unique en Europe, un budget « inédit » de 5 millions d'euros sur six ans lui a été attribué. « *Il permettra surtout d'embaucher des doctorants et des ingénieurs* », selon Jean-Yves Marion. L'enjeu, aujourd'hui, est « *de détecter ces logiciels malveillants avant qu'ils ne passent à l'attaque* ».

Une attaque débute par l'exfiltration des données qui sont ensuite chiffrées. Certaines peuvent durer des mois, insistent les chercheurs : l'exfiltration se fait par petits morceaux, pour ne pas alerter. Et signe de la professionnalisation des **cybercriminels**, les attaques sont de plus en plus sophistiquées, souligne Régis Lhoste, président de la société Cyber-Detect, qui a été créée dans la continuité des travaux du Loria : les programmes malveillants sont « *aujourd'hui conçus spécifiquement pour attaquer votre* ***entreprise*** », sur mesure, tout en reprenant quelques structures déjà vues par le passé.

Des entreprises et des institutions submergées par les attaques

Sa jeune pousse travaille avec de **nombreuses entreprises ou institutions**, leur proposant son expertise pour anticiper les attaques ou les comprendre, *via* des analyses des virus informatiques semblables à celles utilisées dans la recherche médicale. Abdelkader Lahmadi, enseignant-chercheur au Loria et cofondateur avec d'autres chercheurs de la jeune pousse Cybi, explique que les **grandes entreprises** « *sont submergées* » par les rapports de failles de vulnérabilité qui se multiplient.

VOIR AUSSI *FIC 2021 : les cybergendarmes 2.0 mènent l'enquête*

La solution mise au point par les chercheurs et désormais commercialisée, fondée sur l'intelligence artificielle, permet de « *révéler les chemins d'attaque* » qui pourraient être utilisés : cela peut, par exemple, débuter par le piratage d'une **caméra de surveillance** sur un parking, pour ensuite porter atteinte à toute l'unité de production d'un industriel.

Avec DefMal, les universitaires vont aller plus loin, en cherchant à déterminer le mode de fonctionnement des organisations cybercriminelles : comment recrutent-elles et communiquent-elles ? Comment blanchissent-elles l'argent ? Cette analyse nécessite un travail « *main dans la main* » avec juristes et économistes, selon Jean-Yves

Marion. Les chercheurs du Loria travaillent aussi avec la police ou la gendarmerie sur certaines enquêtes.

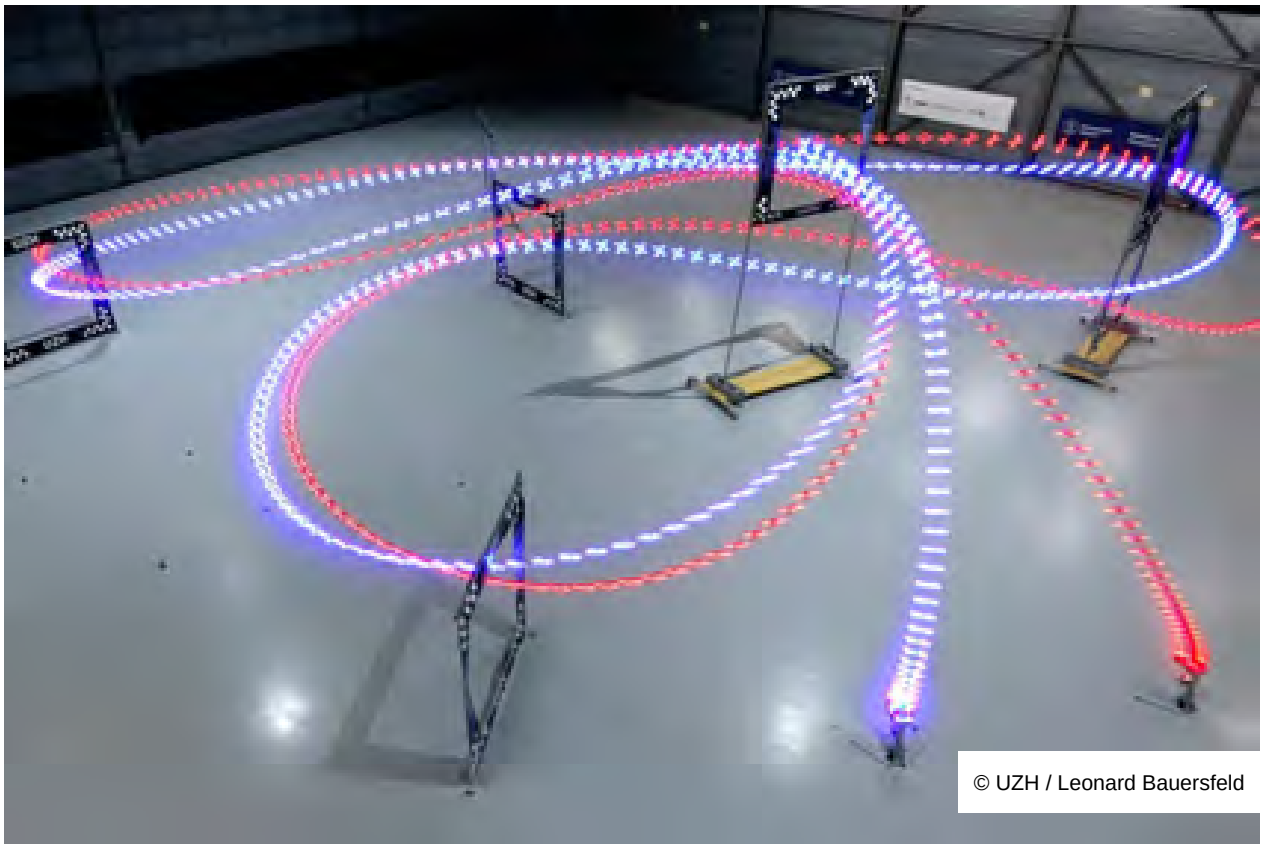
L'USINENOUVELLE

L'IA passe championne en course de drones

Marion Garreau

05 novembre 2023 \
15h30

1 min. de lecture



Grâce à son IA super-entraînée, le drone évite les obstacles en toute autonomie.

L'intelligence artificielle a déjà battu l'humain aux échecs, au jeu de go, puis au jeu-vidéo Starcraft II. Mais dans le monde réel, l'humain restait le seul gagnant. Jusqu'à ce que le système de pilotage Swift, conçu par des chercheurs de l'université de Zurich (Suisse), dépasse trois champions du monde lors de véritables courses de drones.

Embarqué dans l'engin, Swift est 100 % autonome : il n'a bénéficié que de ses calculateurs et des données fournies par les capteurs du drone, précise l'article paru dans Nature. Pour savoir quels ordres envoyer à l'appareil afin de contourner les obstacles et trouver la meilleure trajectoire (le circuit de 75 mètres avait sept portes), Swift s'appuie sur des algorithmes d'apprentissage par renforcement profond, fondé sur la méthode des récompenses, et a été entraîné en simulation.

Une victoire non sans limite

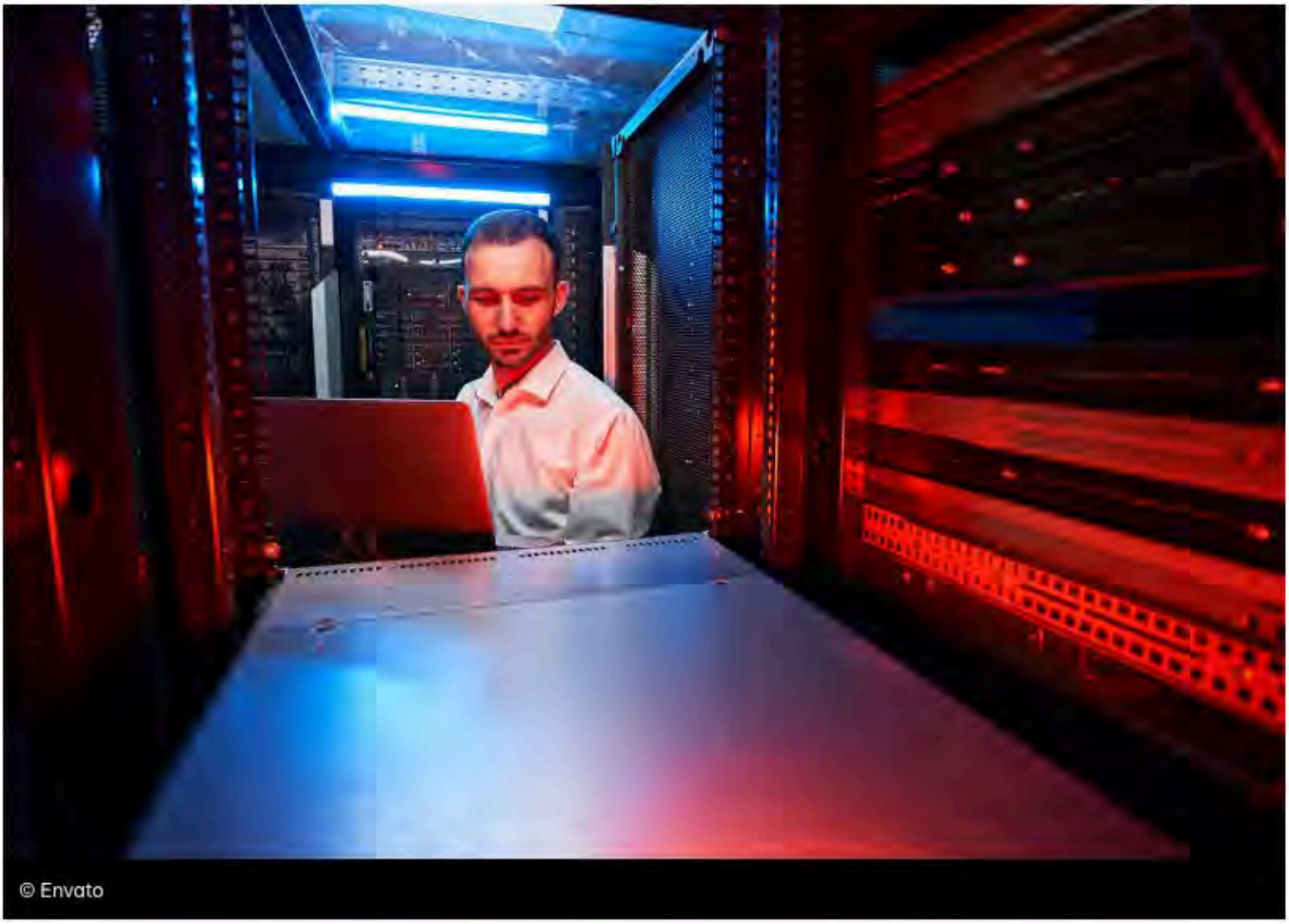
Restait à confirmer ses performances dans la réalité. *«L'enjeu a été d'obtenir une modélisation physique parfaite du drone dans le circuit, ce qui a été fait en collectant des données dans le réel*, décrypte Franck Ruffier, directeur de recherche au CNRS. *L'IA réussit à repousser en permanence les limites de la machine parce qu'elle a parcouru le circuit une multitude de fois dans le virtuel, en crashant un nombre incalculable de drones. Mais sa performance ne vaut que sur ce circuit.»*

C'est là toute la limite de l'expérience. *«Ici, tout a été appris par avance*, abonde Laurent Ciarletta, chercheur au laboratoire Loria et enseignant à Mines Nancy. *Le système est autonome, mais changez la forme des obstacles ou la lumière et il sera perdu. Il faut donc désormais l'entraîner davantage.»* Swift devra apprendre à reconnaître différents obstacles et à s'adapter à l'imprévu (pluie, vent, nouvel obstacle...). Des améliorations nécessaires pour trouver des applications, qu'elles soient dans la défense ou les véhicules autonomes.

En Lorraine

Un labo hautement sécurisé pour traquer les hackers

RTL | Actualisé: 05.11.2023 12:01



© Envato

Détecter l'attaque informatique avant même qu'elle se concrétise: près de Nancy des chercheurs analysent le mode de fonctionnement des cybercriminels dans un programme de recherche unique en Europe.

Au sous-sol du Laboratoire lorrain de recherche en informatique et ses applications (Loria), à Villers-lès-Nancy, est située **une salle de recherche "hautement sécurisée"**: ses fenêtres pourraient résister à sept coups de hache.

A l'intérieur du "laboratoire de haute sécurité" (LHS), des écrans d'ordinateur avec lesquels **les chercheurs écoutent "les bruits de fond" des données,** en partenariat avec le National Institute of Information and Communications Technology de Tokyo. Concrètement, des mouvements sont repérés sur des adresses IP

Communications Technology de Tokyo. Concrètement, des mouvements sont repérés sur des adresses IP "*qui ne devraient pas être utilisées*", ce qui peut présager d'une attaque à venir.

Et avec leur technique du "pot de miel", **les universitaires attirent déjà au quotidien les attaquants dans des pièges, pour ensuite analyser leur mode de piratage.**

La France compte deux laboratoires de haute sécurité, l'autre se trouve à Rennes, dans l'ouest du pays.

Fini le temps où les antivirus permettaient de protéger ses données face au pirate de base qui lançait ses attaques "*au fond d'un garage*", souligne Jean-Yves Marion, ancien directeur du Loria. Ils sont désormais plus organisés.

Ces dernières années, **la menace s'est "*démultipliée*"** selon lui, rendant "*indispensable une mobilisation universitaire* (...) en lien constant avec le monde de l'entreprise et des pouvoirs publics".

Attaques sophistiquées

Depuis la création du Loria en 2010, les chercheurs ont collecté **plus de 35 millions de programmes malveillants.** Si cela leur permet de les analyser et de les tester, "c'est insuffisant", insiste M. Marion.

Désormais, un nouveau programme de recherche lancé en juin, le "DefMal", pour "*Défense contre les programmes malveillants*", vient s'inscrire "dans une stratégie d'accélération annoncée par le président de la République", souligne Lorraine Université d'Excellence.

Présenté comme unique en Europe, un budget "inédit" de 5 millions d'euros sur six ans lui a été attribué. "Il permettra surtout d'embaucher des doctorants et des ingénieurs", selon Jean-Yves Marion.

L'enjeu, aujourd'hui, est "de détecter ces logiciels malveillants avant qu'ils ne passent à l'attaque".

Une attaque débute par l'exfiltration des données, qui sont ensuite chiffrées.

Certaines peuvent durer des mois, insistent les chercheurs: l'exfiltration se fait par petits morceaux, pour ne pas alerter.

Et **signe de la professionnalisation des cybercriminels, les attaques sont de plus en plus sophistiquées,** souligne Régis Lhoste, président de la société Cyber-Detect, qui a été créée dans la continuité des travaux du Loria: les programmes malveillants sont "*aujourd'hui conçus spécifiquement pour attaquer votre entreprise*", sur mesure, tout en reprenant quelques structures déjà vues par le passé.

Entreprises et institutions

Sa jeune pousse travaille avec de nombreuses entreprises ou institutions, leur proposant son expertise pour anticiper les attaques ou les comprendre, via des analyses des virus informatiques semblables à celles utilisées dans la recherche médicale.

Abdelkader Lahmadi, enseignant-chercheur au Loria et co-fondateur, avec d'autres chercheurs, de la jeune pousse Cybi, explique que les grandes entreprises "*sont submergées*" par les rapports de failles de vulnérabilité qui se multiplient.

© Photographie JEAN-CHRISTOPHE VERHAEGEN / AFP©

La solution mise au point par les chercheurs et désormais commercialisée, fondée sur l'intelligence artificielle, permet de "*révéler les chemins d'attaque*" qui pourraient être utilisés: cela peut, par exemple, débuter par le piratage d'une caméra de surveillance sur un parking, pour ensuite porter atteinte à toute l'unité de production d'un industriel.

Avec DefMal, les universitaires vont aller plus loin, en cherchant à déterminer le mode de fonctionnement des organisations cybercriminelles: comment recrutent-elles et communiquent-elles? Comment blanchissent-elles l'argent?

Cette analyse nécessite un travail "main dans la main" avec juristes et économistes, selon Jean-Yves Marion.

Les chercheurs du Loria travaillent aussi avec la police ou la gendarmerie sur certaines enquêtes.

Vosges matin, 6 novembre 2023 (édition Saint-Dié)

Ramonchamp

Un stage de mathématiques et d'informatique réservé aux filles

Plus de 20 lycéennes ont suivi un stage afin qu'elles s'orientent vers des études de mathématiques ou d'informatique.

La Maison familiale de Ramonchamp « Les 4 Vents » organisait un stage d'une semaine, réservé exclusivement à des filles. Il avait pour but de lutter contre le fait que peu de femmes s'orientent vers des études scientifiques.

La Maison familiale de Ramonchamp « Les 4 Vents » vient d'accueillir, pour une semaine, une vingtaine de lycéennes, venues du Grand Est et leurs encadrants, pour un stage de mathématiques et d'informatique.

Nommé « Les Cigognes », le stage a pour objectif de participer à la diffusion de la culture et de l'esprit scientifique, tout en luttant contre la désaffection des femmes pour les mathématiques et l'informatique. Les intervenants pour accompagner ces activités de recherche sont les organisateurs ainsi que des collègues des laboratoires de mathématiques et informatique des universités de Strasbourg et de Lorraine. Une sociologue étudie l'impact de ce stage sur les lycéennes.

Déroulement du stage

Toutes les matinées de la semaine étaient consacrées à des projets de recherche en mathématiques et informatique, encadrés par un groupe d'enseignants-chercheurs avec des actions de type « informatique débranché ».

Lors de ces ateliers, les lycéennes, réparties en petits groupes, travaillaient en parallèle sur différents sujets. Au programme, il y avait de la recherche sur les nombres premiers, une étude sur la vulgarisation de l'informatique et sur l'intelligence artificielle, les probabilités, la logique en 3D et des exercices de géométrie en relief.

En fin de semaine, chaque groupe a présenté les résultats de ses travaux aux autres groupes, ainsi qu'aux parents qui récupéraient les lycéennes le vendredi après-midi.

Les lundis et mardis après-midi étaient réservés à des activités ludiques de plein air, encadrées par des étudiantes en fac de sport de Strasbourg ou de Nancy.

En fin d'après-midi, avaient lieu des rencontres et des moments d'échange entre des lycéennes et des enseignantes-chercheuses ou doctorantes.

Le jeudi après-midi, quelques femmes scientifiques issues du monde de l'entreprise sont venues présenter leurs métiers et leurs parcours.

La semaine fut ponctuée par des conférences sur les mathématiques et l'informatique.

LE GRAND ENTRETIEN · RCF ALSACE · LORRAINE NANCY · JERICO MOSELLE

Emission présentée par Bénédicte Bossard, Nicolas Dufour (54), Thierry Georges

Rencontrez le Grand entretien de la rédaction. Celles et ceux qui font l'actualité politique, économique, culturelle, religieuse et associative de l'Alsace-Lorraine-Moselle.

SUIVRE PARTAGER S'ABONNER

Episodes

Trier

Intelligence artificielle : puiser dans les sciences humaines face au débat

6 novembre 2023

22 min

PARTAGER </> INTÉGRER

Chaque jour apporte son lot de nouvelles dans le domaine de l'intelligence artificielle. À tel point que les voix s'élèvent, de plus en plus nombreuses, pour questionner les limites (le plus souvent éthiques et technologiques) de ce qui s'impose déjà dans nos quotidiens : car l'intelligence artificielle est déjà partout autour de nous et s'impose comme une fatalité.

L'USINENOUVELLE
L'Usine Nouvelle (site web)
mercredi 8 novembre 2023 - 11:00 GMT+1 1172 mots

Au Loria, l'innovation au service de la détection précoce des cyberattaques

[L'instant tech] Situé à Villers-lès-Nancy (Meurthe-et-Moselle), le Laboratoire de Haute Sécurité (LHS) de l'Université de Lorraine est un lieu quasi-unique en France. A travers un programme de recherche inédit en Europe et deux start-up innovantes, ses chercheurs travaillent sur l'analyse et la détection précoce des attaques.

Dans les sous-sols du laboratoire Lorrain de Recherche en Informatique et ses Applications (Loria), situé à Villers-lès-Nancy (Meurthe-et-Moselle), un imposant sas protège le Laboratoire de Haute sécurité (LHS). Cette plateforme dédiée à la recherche en cybersécurité, fruit d'un partenariat de l'Université de Lorraine avec l'INRIA et le CNRS, est l'une des deux seules de ce type en France avec celle de l'IRISA à Rennes. Visant la détection des intrusions et la protection contre les logiciels malveillants, elle abrite dans sa salle de serveurs « 35 millions de malwares », mais aussi de nombreuses données sensibles.

A l'intérieur de la salle de travail, les chercheurs observent sur des ordinateurs les « bruits de fonds » des données pour repérer d'éventuelles attaques. Dans le cadre d'une collaboration avec le National Institute of Information and Communications Technology (NICT) de Tokyo, les chercheurs lorrains et tokyoïtes s'échangent des sondes ou des « pots de miel » c'est-à-dire des faux serveurs remplis de vulnérabilités afin d'attirer les cybercriminels. L'objectif: « Analyser les modes opératoires, les détecter et les comprendre pour pouvoir mieux y réagir », précise, à l'occasion d'une visite, Jean-Yves Marion, professeur à l'Université de Lorraine et ancien directeur du Loria. Un projet de recherche unique en Europe

En effet souligne Jean-Yves Marion, les attaques, de plus en plus sophistiquées, sont également plus complexes à détecter, à l'image de celle menée en 2021 contre le système de santé irlandais et qui a mis trois mois à être repérée. « Tous les objets connectés sont attaquables et forment une chaîne qui permet aux cybercriminels de progresser discrètement dans le système », rappelle le chercheur du Loria. Des cyberattaques qui font aussi des dégâts toujours plus importants, à l'image de celle menée contre le port de Nagoya, paralysé pendant plus de trois jours en juillet 2023. « Les modes opératoires des rançongiciels ont évolué, avec l'exfiltration systématique des données de la victime. Les groupes sont structurés, avec un modèle économique, et sont capables d'attaques ciblées », rappelle Jean-Yves Marion.

Pour répondre à cette nouvelle réalité, le Loria a obtenu le financement d'un projet de recherche unique en Europe, le programme et équipement prioritaire de recherche (PEPR) en cybersécurité DefMal (Défense contre les programmes Malveillants). Lancé en 2022 pour une durée de six ans et financé à hauteur de cinq millions d'euros, il vise une avancée décisive dans l'analyse et la défense face aux rançongiciels où à l'espionnage : « DefMal illustre la volonté étatique d'accélérer les choses. Ce programme va nous permettre de faire avancer la recherche fondamentale qui est un facteur important d'innovation » estime Jean-Yves Marion. Autre source d'avancées, le partage de données avec des institutions partenaires comme le NICT japonais, le CISPA allemand et d'autres institutions partenaires dans la Sarre, au Luxembourg et en Belgique. Pour que sa recherche reste en lien avec les besoins des entreprises, le Loria a également créé un laboratoire commun avec l'éditeur de logiciels Wallix, et deux start-up issues de ses travaux de recherche ont été fondées. Cybi : l'IA pour détecter les chemins d'attaques

Cofondée en mai 2022 par Abdelkader Lahmadi, enseignant chercheur à l'Université de Lorraine, Cybi est le résultat de 10 ans de recherche au sein des laboratoires lorrains Loria et Inria Nancy. Son ambition ? Utiliser l'intelligence artificielle pour prédire les chemins d'attaques et générer automatiquement un audit de cybersécurité et un plan de remédiation priorisé des vulnérabilités. L'IA développée par le chercheur du Loria et ses collègues a été entraînée à partir de « milliards de documents de sécurité » précise Abdelkader Lahmadi. Ce dernier, qui a notamment travaillé sur la sécurité des objets connectés, rappelle que pour chaque dispositif, plus de 160 vulnérabilités sont détectées en moyenne chaque jour, et jusqu'à 5000 par mois. Des chiffres qui font que les analystes de cybersécurité se retrouvent vite submergés et incapables de prioriser les interventions.

S'il existe déjà sur le marché des solution de détection de vulnérabilités, « aucune n'utilise l'intelligence artificielle ni n'est en mesure de trouver le chemin d'attaque associé à ces vulnérabilités » selon Abdelkader Lahmadi. En termes de commercialisation, si Cybi en est encore aux prémisses, l'idée est de proposer un accès à la solution par abonnement ou via la vente de jetons d'analyse. « Au travers de nos revendeurs et distributeurs, nous avons déjà effectué des démonstrations auprès d'industriels travaillant dans différents secteurs d'activité, dont la fabrication

d'équipements, l'aéronautique ou l'énergie », précise le chercheur. Cyber-Detect, l'analyse morphologique des malwares

Créée en 2017 à l'issue de 10 années de recherche au sein du Laboratoire de Haute Sécurité du Loria, la start-up Cyber-Detect est spécialisée dans la détection et la caractérisation de malwares (logiciels malveillants) grâce à l'analyse morphologique. « Aujourd'hui, les malwares se transforment spécifiquement pour attaquer les entreprises... Pour protéger les infrastructures, il faut pouvoir détecter ces variants avant qu'ils ne passent à l'attaque. L'enjeu est aussi de distinguer ceux qui présentent un réel danger et les faux positifs, afin d'alerter uniquement lorsque cela est nécessaire » introduit le président de Cyber-Detect, Régis Lhoste.

La méthode, baptisée « Gorille », est « plus performante qu'un antivirus classique », puisqu'elle permet de « cartographier chaque fonctionnalité d'un fichier afin de voir si l'une d'elles correspond à un caractère malveillant », explique Régis Lhoste. En d'autres termes, l'enjeu est de décomposer le contenu de l'attaque, afin de mieux la comprendre. La start-up a déjà établi des partenariats avec les pépites françaises Tehtris et Quarklab afin de proposer une méthode complète. « Notre objectif est de travailler avec des intégrateurs et des éditeurs comme une brique complémentaire des EDR (Détection et réponse aux points finaux), qui ne sont pas actuellement en mesure de prendre des décisions sur un certain nombre de fichiers » détaille le président de Cyber-Detect. Savoir attaquer pour mieux se défendre

En parallèle, les chercheurs du Loria collaborent avec la police et la gendarmerie afin de les aider à mieux appréhender le mode opératoire des cybercriminels. Mais aussi pour élaborer des scénarios d'attaque. Car, pointe Jean-Yves Marion, « une des meilleures façons de se défendre est parfois d'attaquer ». Un domaine de recherche dans lequel la France est plutôt en retard, selon lui. Pour remédier à cette situation, Gabriel Sauger, l'un des deux doctorants intégré au programme DefMal, collabore notamment avec la section informatique de l'Université d'Arizona à Tucson.

La recherche collaborative porte sur la construction d'une attaque contre des systèmes de défense basés sur l'intelligence artificielle, afin de repérer d'éventuels défauts dans le système de protection. Enfin, le Loria collabore de manière étroite avec des économistes et des juristes, afin d'approcher la cybercriminalité dans toutes ses dimensions. « Nous cherchons à comprendre l'écosystème et le mode organisationnel des cybercriminels et des cyberattaquants. La manière dont ils communiquent, recrutent, comment ils blanchissent l'argent » détaille Jean-Yves Marion, qui espère à l'avenir intégrer également la psychologie et la sociologie. Dans le but, toujours, de mieux anticiper les futurs mouvements des cybercriminels.

Au cœur de la Lorraine, la dure lutte de l'IA contre les malwares

publié le 9 novembre 2023 par *Jean-Baptiste Lautier*

Sur le site de l'Université de Lorraine à Nancy, le Loria (Laboratoire lorrain de recherche en informatique et ses applications), héberge des chercheurs de pointe en cybersécurité. En partenariat avec des start-up, certains se concentrent sur la collecte de données relatives aux malwares, dans le but de mieux les chasser grâce à l'intelligence artificielle. Un combat difficile.

« DefMal ». Derrière ce nom de code, se cache un projet lancé il y a un an par le centre de recherche lorrain Loria, qui réunit le CNRS, l'Inria et l'Université de Lorraine. Son objet ? Passer un cap en matière d'analyse de programmes malveillants à l'aide de l'intelligence artificielle, pour anticiper les

malveillants à l'aide de l'intelligence artificielle, pour anticiper les mouvements des cyberattaquants. "L'un des principaux objectifs est de développer une nouvelle approche d'analyse et de détection grâce à une approche interdisciplinaire. Il s'agit d'analyser l'écosystème des virus et de mieux prédire les attaques grâce à une plateforme d'échanges d'informations ", explique Jean-Yves Marion, professeur à l'Université de Lorraine, qui a dirigé le Loria pendant une décennie.

Le projet DefMal est doté de 5 millions d'euros et repose en grande partie sur les compétences réunies au sein d'un laboratoire de haute sécurité (LHS) situé à Nancy. Dans ce bureau ultra-sécurisé, protégé par une vitre qui résiste "à cinq coups de hache", des chercheurs rivalisent d'ingéniosité pour connaître leurs ennemis, grâce à des « pots de miel ». "Ce sont des serveurs que nous créons et qui ont volontairement des vulnérabilités pour attirer les attaquants. Une fois l'attaque passée, on récupère les informations et on ferme le serveur", raconte Jean-Yves Marion. Au fil des mois, les chercheurs disposent d'une importante masse de données disponible pour entraîner des intelligences artificielles capables ensuite de reconnaître des attaques. Le moteur d'intelligence artificielle peut en effet reconnaître la structure d'un code, mais également la manière dont celui-ci se comporte au sein d'un système d'information.

Lutter contre les « variants »

"Dès les années 90, le jeu a été d'identifier les codes malveillants. Mais aujourd'hui, l'IA ouvre de nouvelles opportunités. » commente Gérome Billois, associé au sein du département cybersécurité et confiance numérique de Wavestone, une entreprise de conseil. « Cette idée n'est pas neuve mais on gagne clairement en efficacité aujourd'hui et plusieurs centres de recherches et startup se sont positionnés sur ce sujet porteur" décrit-il.

Au Loria, les chercheurs s'appuient sur la dynamique entrepreneuriale pour avancer plus vite : le projet DefMal se fait avec la participation de start-up comme Cyber-Detect. Née à Nancy, au sein même du centre de recherche, cette entreprise s'est spécialisée dans l'analyse morphologique des logiciels malveillants. "De plus en plus les malwares sont construits spécifiquement pour attaquer une entreprise en particulier", estime Régis Lhoste, président de l'entreprise et ancien chercheur du Loria. "Chaque malware est donc potentiellement nouveau et il peut même se transformer au fur et à mesure des exécutions".

Le rapprochement avec l'image du virus n'a donc jamais été aussi pertinente et le dirigeant emploie d'ailleurs volontairement un lexique sanitaire pour expliquer comment l'IA permet de mieux détecter des fonctionnalités malveillantes au sein d'un programme. "Notre logiciel Gorille analyse et caractérise les malwares et leurs comportements malicieux. Le but est d'avoir une approche relativement résistante aux « variants » d'une souche, mais également de détecter quand un hacker a réécrit une fonctionnalité connue dans un autre langage de programmation par exemple".

Le long chemin vers la détection automatique

Selon l'un des hackers éthiques travaillant au sein du LHS, il ne faut que trois jours pour créer un nouveau malware. L'IA doit donc fournir une aide précieuse pour s'adapter à ces changements incessants, même si elle ne peut aujourd'hui pas détecter un programme malveillant complètement nouveau. "Il faut entraîner et réentraîner régulièrement l'IA pour qu'elle soit toujours à jour dans son niveau de défense", reconnaît Gérôme Billois. "Tant qu'il y a des similitudes avec un code existant, cela peut bien fonctionner mais quand le code est tout nouveau, on atteint la limite de la reconnaissance de l'IA", précise-t-il.

L'intelligence artificielle pourrait-elle demain prendre complètement la main sur la détection et la luttre contre les malwares ? "Son efficacité ultime sera atteinte quand une IA pourra lancer d'elle-même une défense automatisée. Mais l'IA en cybersécurité n'est pas encore 100 % fiable. Aujourd'hui, si l'une d'elles lance des corrections de systèmes de manière automatisée, cela pourrait créer des dégâts encore plus importants", nuance Gérôme Billois. Cet usage des technologies d'intelligence artificielle n'est d'ailleurs pas testé au sein du Loria. Si la fiabilité des détections augmente, il reste encore bien du chemin à l'IA en cybersécurité.

Informatique: un labo pour détecter les pirates avant intrusion

AFP | MIS À JOUR LE 16 AVRIL 2024

À l'intérieur du «laboratoire de haute sécurité» (LHS), des écrans d'ordinateur avec lesquels les chercheurs écoutent «les bruits de fond» des données, en partenariat avec le National Institute of Information and Communications Technology de Tokyo. (Photo: 123RF)

Détecter l'attaque informatique avant même qu'elle se concrétise: près de Nancy en France, des chercheurs analysent le mode de fonctionnement des cybercriminels dans un programme de recherche unique en Europe.

Au sous-sol du Laboratoire lorrain de recherche en informatique et ses applications (Loria), à Villers-lès-Nancy (Meurthe-et-Moselle), est située une salle de recherche «hautement sécurisée» : ses fenêtres pourraient résister à sept coups de hache.

À l'intérieur du «laboratoire de haute sécurité» (LHS), des écrans d'ordinateur avec lesquels les chercheurs écoutent «les bruits de fond» des données, en partenariat avec le National Institute of Information and Communications Technology de Tokyo. Concrètement, des mouvements sont repérés sur des adresses IP «qui ne devraient pas être utilisées», ce qui peut présager d'une attaque à venir.

Et avec leur technique du «pot de miel», les universitaires attirent déjà au quotidien les attaquants dans des pièges, pour ensuite analyser leur mode de piratage.

La France compte deux laboratoires de haute sécurité, l'autre se trouve à Rennes.

Fini le temps où les antivirus permettaient de protéger ses données face au pirate de base qui lançait ses attaques «au fond d'un garage», souligne Jean-Yves Marion, ancien directeur du Loria. Ils sont désormais plus organisés.

Ces dernières années, la menace s'est «démultipliée» selon lui, rendant «indispensable une mobilisation universitaire (...) en lien constant avec le monde de l'entreprise et des pouvoirs publics».

Attaques sophistiquées

Depuis la création du Loria en 2010, les chercheurs ont collecté plus de 35 millions de programmes malveillants. Si cela leur permet de les analyser et de les tester, «c'est insuffisant», insiste M. Marion.

Désormais, un nouveau programme de recherche lancé en juin, le «DefMal», pour «Défense contre les programmes malveillants», vient s'inscrire «dans une stratégie d'accélération annoncée par le président de la République», souligne Lorraine Université d'Excellence.

Présenté comme unique en Europe, un budget «inédit» de 5 millions d'euros sur six ans lui a été attribué. «Il permettra surtout d'embaucher des doctorants et des ingénieurs», selon Jean-Yves Marion.

L'enjeu, aujourd'hui, est «de détecter ces logiciels malveillants avant qu'ils ne passent à l'attaque».

Une attaque débute par l'exfiltration des données, qui sont ensuite chiffrées.

Certaines peuvent durer des mois, insistent les chercheurs : l'exfiltration se fait par petits morceaux, pour ne pas alerter.

Et signe de la professionnalisation des cybercriminels, les attaques sont de plus en plus sophistiquées, souligne Régis Lhoste, président de la société Cyber-Detect, qui a été créée dans la continuité des travaux du Loria : les programmes malveillants sont «aujourd'hui conçus spécifiquement pour attaquer votre entreprise», sur mesure, tout en reprenant quelques structures déjà vues par le passé.

Entreprises et institutions

Sa jeune pousse travaille avec de nombreuses entreprises ou institutions, leur proposant son expertise pour anticiper les attaques ou les comprendre, via des analyses des virus informatiques semblables à celles utilisées dans la recherche médicale.

Abdelkader Lahmadi, enseignant-chercheur au Loria et co-fondateur, avec d'autres chercheurs, de la jeune pousse Cybi, explique que les grandes entreprises «sont submergées» par les rapports de failles de vulnérabilité qui se multiplient.

La solution mise au point par les chercheurs et désormais commercialisée, fondée sur l'intelligence artificielle, permet de «révéler les chemins d'attaque» qui pourraient être utilisés : cela peut, par exemple, débuter par le piratage d'une caméra de surveillance sur un stationnement, pour ensuite porter atteinte à toute l'unité de production d'un industriel.

toute l'unité de production d'un industriel.

Avec DefMal, les universitaires vont aller plus loin, en cherchant à déterminer le mode de fonctionnement des organisations cybercriminelles : comment recrutent-elles et communiquent-elles? Comment blanchissent-elles l'argent?

Cette analyse nécessite un travail «main dans la main» avec juristes et économistes, selon Jean-Yves Marion.

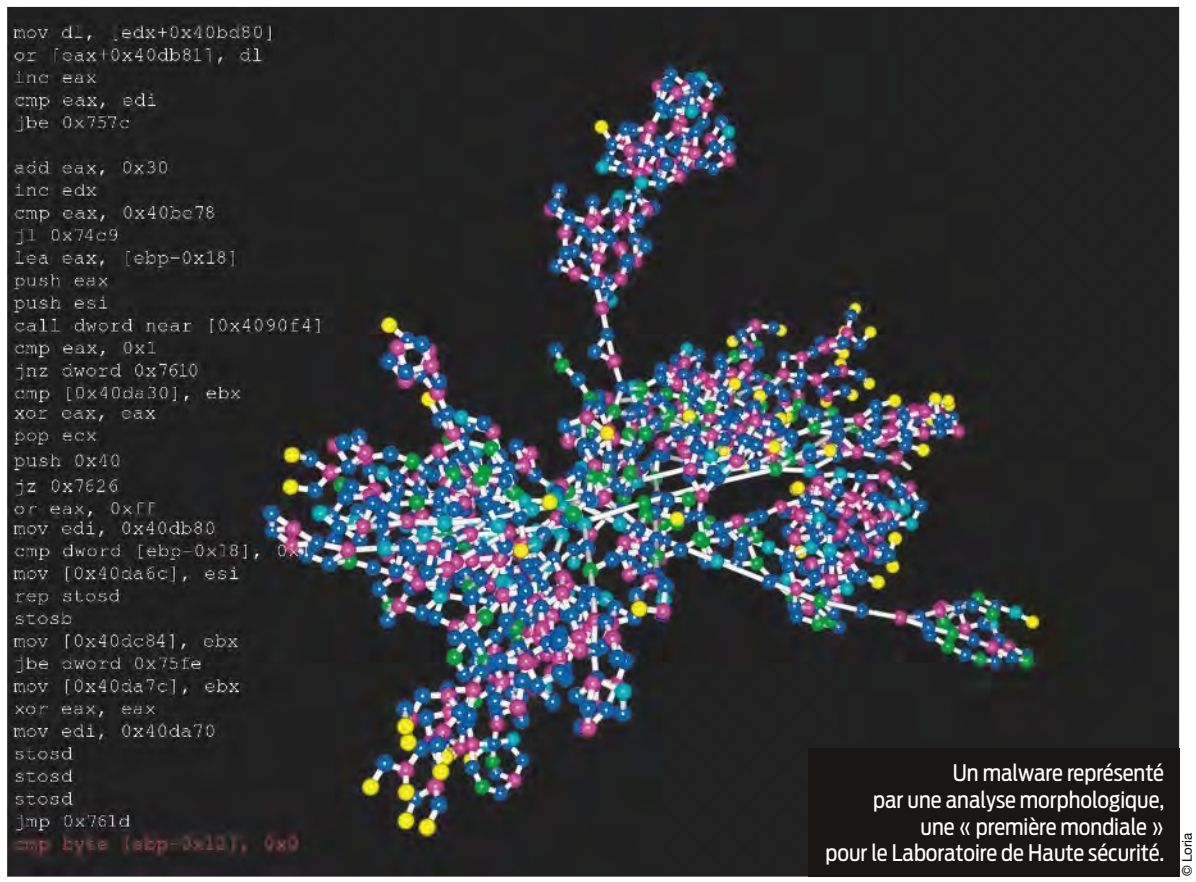
Les chercheurs du Loria travaillent aussi avec la police ou la gendarmerie sur certaines enquêtes.

Une Semaine à…

Lorraine / TECHNOLOGIE

Cybersécurité : les virus du monde entier analysés depuis Nancy

Quelques jours après les **ASSISES UNIVERSITAIRES DROIT ET CYBERSÉCURITÉ** organisées à Nancy, « La Semaine » plonge au cœur du référent mondial en matière de cybersécurité qui constitue la première force de recherche nationale dans ce domaine : le laboratoire de Haute sécurité (LHS) installé au sein du Loria et de l'Inria.



Un malware représenté par une analyse morphologique, une « première mondiale » pour le Laboratoire de Haute sécurité.

© Loria

C'est un lieu pas comme les autres. Dans les méandres du Laboratoire lorrain de recherche en informatique et ses applications (Loria) et de l'Institut national de recherche en sciences et technologies du numérique (Inria), au détour d'un couloir, après un sas surprotégé, des vitres blindées, deux pièces hautement sécurisées sont enfin accessibles. **C'est dans cet antre totalement clos et retiré du reste de l'agitation universitaire et scientifique que les chercheurs s'affairent.** Depuis 2010, toute une équipe est mobilisée autour des questions de cybersécurité. Avec un objectif : lutter contre la prolifération de malwares, ces logiciels malveillants qui touchent les objets connectés et les systèmes industriels. Ils étudient les logiciels malveillants (malwares), de rançonnage bien souvent, leurs variants et analysent leur morphologie en vue de les détecter le plus tôt possible. Car bien souvent, ils parviennent à échapper aux systèmes de protection existants des entités privées comme publiques en utilisant une technique d'offuscation de code. **Encore récemment en Meurthe-et-Moselle, l'entreprise Baccarat en a été victime.** À quelques kilomètres des frontières départementales, deux hôpitaux de la plaine vosgienne ont aussi été touchés ces derniers jours. Les attaquants vont bloquer les systèmes en cryptant les données. Ils récupèrent ces données et demandent une rançon pour les libérer ou les revendre.

Afin de détecter ces codes malveillants, les chercheurs *« écoutent les bruits »* par le biais d'un *« télescope virtuel »*. Ce super outil scrute, observe et recense les vagues de cyberattaques en temps réel, permettant aux chercheurs d'observer des milliers d'attaques en direct. Si elles sont généralement constantes, des grands moments qui vont faire l'actualité peuvent être détectés avec un flux d'attaques ou de bruits bien plus conséquent. **« Ce fut le cas lors des élections américaines de 2016, pendant le conflit Ukraine-Russie aussi par exemple**. *Mais sur le conflit au Proche-Orient, c'est plus compliqué. Il y a eu une activité. Mais il est très difficile de l'attribuer à quelqu'un. Et encore moins de déterminer une source géographique. On ne peut rien en déduire comme type d'information. On écoute de manière très large. De temps en temps, quand on a de la chance, on peut relier l'activité à un événement. Mais le plus souvent, c'est lié à une vulnérabilité qui a été découverte ou à un tas d'autres raisons »*, explique Jean-Yves Marion, professeur à l'Université de Lorraine, chercheur au Loria et membre de l'Institut universitaire de France.

« Comme en biologie, certains virus sont des mutants »

Pour intercepter et collecter tous ces logiciels malveillants, le laboratoire dispose d'un **« pot de miel virtuel »**. Une ruse qui attire les cyberattaquants en leur faisant croire qu'ils ont trouvé la proie idéale. Mais pas question de contaminer l'ensemble du réseau du Laboratoire de Haute sécurité, l'analyse des malwares est alors permise sans risques. À ce jour, le laboratoire dispose d'une base de données de près de 35 millions de malwares que les chercheurs ont minutieusement analysés. Et après ? **Toute cette collecte leur a permis de développer une technique d'analyse morphologique.** Cette méthode, *« première mondiale »*, repose sur un système d'intelligence artificielle, entraîné par apprentissage automatique, permettant d'identifier les fonctionnalités cachées dans les programmes tels que des applications et des mises à jour en se basant sur la forme du virus. Cela permet de détecter rapidement les intrusions qui échappent aux systèmes de détection existants. Les chercheurs dissèquent le virus pour déterminer si des souches sont déjà connues ou non. Ils les répertorient et déterminent leurs fonctionnalités au cas où un même comportement serait revu quelques semaines plus tard dans une autre attaque. Mais pas question de garder toute cette prouesse dans les deux pièces sécurisées. **Depuis 2017, cette solution est commercialisée par la start-up** *Cyber-Detect* à travers le logiciel « Gorille ». Un dispositif utilisé par des entreprises privées comme des entités gouvernementales avec une mise à jour constante. *« Comme en biologie, certains virus sont des mutants. Les cyberattaquants les font varier pour tromper les antivirus »*, précise Régis Lhoste, fondateur de Cyber-Detect.

Autre entreprise issue du LHS : Cybi. Encore hébergée dans les locaux, cette entité développe, **Skuba, basé sur l'intelligence artificielle.** Alors que de plus en plus d'attaques utilisent les objets connectés peu sécurisés pour rebondir et s'introduire dans les systèmes, Skuba va analyser et prédire tous les chemins d'attaques, toutes les vulnérabilités de l'entreprise et proposer des solutions pour éviter que ces objets connectés ne permettent aux pirates de pénétrer le système.

La recherche lorraine à la pointe

Si des solutions existent, pas question d'arrêter la recherche. **Le Loria reste à la pointe et représente l'une des premières forces de recherche académique en France dans la cybersécurité.** Ses travaux, menés en étroite collaboration avec d'autres structures de recherche universitaire en France et en Europe, sont à l'origine d'avancées significatives dans la détection précoce des menaces cyber pour mieux les combattre.

Dans ce sens, le programme de recherche en cybersécurité, *DefMal*, portant sur l'étude des logiciels et programmes malveillants, s'intensifie après son évaluation à un an. Lancé en 2022 dans le cadre du plan France Relance et porté par l'Université de Lorraine, mobilisant les mondes de la recherche et de l'entreprise, bénéficiant de collaborations à l'échelle européenne et internationale, ce projet vise à renforcer la détection des malwares et rançongiciels tout en appréhendant les aspects économiques, juridiques, criminels et sociologiques qui sous-tendent cet écosystème. **Avec un budget de cinq millions d'euros échelonné sur six ans,** il s'agit de l'un des dix premiers projets de recherche ciblés qui s'inscrivent dans une stratégie nationale d'accélération annoncée par le président de la République. *« L'évaluation du projet, un an après son lancement, va nous permettre de répondre à l'objectif fondamental de se doter de capacités d'anticipation et de réactions rapides face aux cyber-attaques par programme malveillant et de permettre aux entreprises, administrations et institutions d'en profiter. Il faut saluer l'engagement du gouvernement à renforcer la cybersécurité et à soutenir la recherche dans ce domaine »* conclut Jean-Yves Marion.

Les résultats du programme *DefMal* seront présentés lors de conférences internationales. Le projet s'impliquera également dans la formation de jeunes chercheurs et établira des échanges avec les services de l'État et les entreprises. Un élément supplémentaire d'excellence pour l'Université de Lorraine.

Baptiste Zamaron

CYBER-SÉCURITÉ

Il était une science

Transition numérique de l'industrie et de la société

COMPRENDRE L'ÉCOSYSTÈME DES CYBERCRIMINELS POUR MIEUX LES COMBATTRE

Les cybercriminels ne sont plus de jeunes geeks qui agissent dans leur coin mais des organisations criminelles qui s'accaparent des données pour les monnayer en exigeant des rançons. Dans le cadre du projet DefMal (Défense contre les programmes malveillants), Lorraine Université d'Excellence mène des recherches en matière de cybersécurité. Les explications de Jean-Yves Marion, professeur à l'Université de Lorraine, à l'École Nationale Supérieure des Mines de Nancy (ENSMN) ainsi qu'au LORIA (Laboratoire Lorrain de Recherche en Informatique et ses Applications – CNRS, Inria, Université de Lorraine).

Nul n'est à l'abri. La cybercriminalité concerne les particuliers comme les organisations, les entreprises comme les états. Comprendre que la cybersécurité est un enjeu majeur. Différents partenaires de Lorraine Université d'Excellence (LUE) mènent des travaux de recherche en matière de cybersécurité. Ils portent sur la cryptographie, la vérification des protocoles (communication entre deux ordinateurs) notamment en lien avec le vote électronique, ou bien encore sur les programmes malveillants. Dans la continuité d'un premier projet appelé Impact DigiTrust destiné à redonner « confiance dans le numérique », LUE a permis de lancer DefMal (Défense contre les programmes malveillants) qui est un projet du programme France Relance.

Des groupes organisés comme des entreprises

Les recherches se concentrent sur la compréhension des écosystèmes cybercriminels pour être en mesure de détecter les signaux faibles et d'anticiper les attaques. « *Certains de ces groupes sont organisés comme de véritables petites entreprises avec un service en charge de développer des logiciels d'attaque, des services de négociation, d'aide aux victimes pour qu'ils puissent payer en bitcoin, d'exfiltration des données, de blanchiment de l'argent… Et au bas de l'échelle, il y a les affiliés qui vont perpétrer l'attaque. C'est une sorte d'ubérisation de la cybercriminalité, ce qui fait que l'arrestation de l'ensemble d'un groupe de cybercriminels est très compliquée* », a expliqué Jean-Yves Marion, professeur à l'Université de Lorraine, à l'ENSMN et au LORIA, lors d'un webinaire auquel participait aussi Bertrand Pailhes, directeur des technologies et de l'innovation à la CNIL qui est revenu sur les missions et priorités de la Commission nationale de l'informatique et des libertés. La cybercriminalité est donc portée par des organisations et des procédures au service d'un modèle économique. « *Et la concurrence entre les groupes est vive car il est important de séduire et de fidéliser les affiliés car ce sont eux qui sont à la manœuvre, en sachant que l'on n'est pas chez les bisounours* », précise l'expert qui a dirigé le LORIA (Laboratoire Lorrain de Recherche en Informatique et ses Applications – CNRS, Inria, Université de Lorraine) durant 10 ans.

Programmes malveillants : détecter et anticiper

Mieux comprendre ces écosystèmes cybercriminels dans leurs multiples dimensions (organisationnelle, technologique, juridique…), c'est le premier volet de DefMal qui mobilise des experts en informatique ainsi que des économistes ou des juristes. Et demain, peut-être, des sociologues, des psychologues ou des anthropologues. Jean-Yves Marion plaide en tout cas pour qu'il en soit ainsi. À ce volet s'en ajoute un second qui porte plus spécifiquement sur la détection et l'analyse des programmes malveillants à l'heure de l'Intelligence Artificielle qui « industrialise le phishing et le hacking humain ». Là encore l'ambition est d'anticiper sur les programmes, variants et menaces à venir, alors que la multiplication des objets connectés s'accompagne de nouvelles vulnérabilités. « *La surface d'attaque ne fait qu'augmenter : caméras, capteurs, voitures, avions, drones… L'informatique est partout* », souligne le chercheur non sans évoquer toute l'importance de ce que l'on appelle la « *Security by design* », autrement dit la nécessité d'intégrer la sécurité dans le développement même des objets (connectés) avec pour priorité de réduire leur vulnérabilité.

À noter que ces travaux qui relèvent de la recherche fondamentale ont déjà des applications très concrètes comme le confirme, par exemple, la création de la start-up Cyber-Detect qui commercialise une solution innovante d'analyse de logiciels malveillants.

LE JOURNAL DES ENTREPRISES

Avec Defmal, la recherche lorraine se place en première ligne sur la cybersécurité

Par Jean-François Michel, le 13 novembre 2023

Lancé dans le cadre du plan France relance et porté par l'Université de Lorraine, le programme de recherche en cybersécurité Defmal va mobiliser 5 millions d'euros sur six ans. Aux avant-postes, à Nancy, le Loria, le laboratoire lorrain de recherche en informatique et ses applications, et son Laboratoire de haute sécurité.

▲ L'accès à la salle "serveur" du Laboratoire haute sécurité du Loria, à Nancy, est rigoureusement contrôlé. — Photo : Inria - Kaksonen

Changer de regard pour mieux comprendre. C'est en substance le point de vue adopté par Jean-Yves Marion, professeur à l'Université de Lorraine, chercheur au Loria et responsable du programme DefMal. Lancé en 2022 dans le cadre du plan France Relance et porté par l'Université de Lorraine, le programme de recherche en cybersécurité DefMal, portant sur l'étude des logiciels et programmes malveillants, entame une phase d'accélération. Doté d'un budget de 5 millions d'euros sur 6 ans, DefMal va notamment s'attacher à comprendre le modèle économique de la cybercriminalité : "D'après les derniers chiffres dont nous disposons, les cybercriminels ont amassé plus de 10 milliards d'euros en 2019", rappelle Jean-Yves Marion.

Au fur et à mesure que les outils numériques s'imposent dans les entreprises et les administrations, les logiciels malveillants représentent une menace exponentielle, s'infiltrant dans l'ensemble de l'environnement numérique : les objets connectés, les véhicules autonomes, les systèmes industriels et l'ensemble de l'infrastructure informatique, y compris le cloud, les smartphones et, de manière générale, les logiciels internes de l'ensemble des produits électroniques. L'enjeu est de parvenir à développer de nouvelles méthodes d'analyse et de défense face aux malwares, d'appréhender les aspects économiques, juridiques, criminels et sociologiques qui sous-tendent cet écosystème.

Écouter le trafic et collecter les logiciels malveillants

"La démultiplication des menaces ces dernières années rend indispensable une mobilisation universitaire interdisciplinaire, en lien constant avec le monde de l'entreprise et les pouvoirs publics", estime Jean-Yves Marion, qui a structuré le projet autour de collaborations européennes, avec le Centre de cybersécurité CISPA, à Sarrebruck en Allemagne ou internationales, comme avec le Japan Advanced Institute of Science and Technology basé à Kanazawa au Japon et le National Institute of Information and Communications Technology de Tokyo.

En Lorraine, le Loria, le Laboratoire lorrain de recherche en informatique avec ses applications, dispose d'une pièce maîtresse avec le LHS, le Laboratoire de haute sécurité. Sas d'accès contrôlé, vitres blindées, les

chercheurs travaillent ici dans une ambiance particulière visant à protéger deux salles contenant des serveurs. Dans ces machines, les chercheurs du Loria ont développé des outils capables d'écouter le trafic internet, à la recherche des mouvements suspects. "C'est ce que nous appelons le brouillard de la guerre. Sur les plages d'adresses IP que nous écoutons, normalement, il ne devrait pas y avoir de trafic. Nous observons donc de potentiels attaquants à la recherche de cibles", détaille Jean-Yves Marion.

Autre mission du LHS, la collecte des logiciels malveillants. Pour attirer les attaquants, les chercheurs du Loria ont déployé un "honey poot", soit un pot de miel : une machine faussement vulnérable, permettant à un attaquant de passer à l'attaque. En déployant son logiciel malveillant dans cette machine, le hacker va finalement enrichir la collection du LHS, qui n'en compte déjà pas loin de 35 millions. C'est pour prévenir les risques de fuite que les serveurs du LHS sont aussi sécurisés.

Ce travail de recherche a déjà permis à deux start-up, Cybi et Cyber-Detect, de mettre sur le marché des outils très avancés permettant de prévenir les cyberattaques. Autant d'efforts qui vont désormais encore s'accentuer : "L'évaluation du projet DefMal va nous permettre de répondre à l'objectif fondamental de se doter de capacités d'anticipation et de réactions rapides face aux cyberattaques par programme malveillant et de donner l'opportunité aux entreprises, administrations et institutions d'en profiter", précise Jean-Yves Marion.


HEARTHIS.AT
LIVE
Se Connecter
Upload
Diffusion en direct
RADIO CAMPUS LORRAINE
Quoi de Neuf du 14 novembre: Para Handball et Cybersécurité
Radio Campus Lorraine
Suivre
56:41
Ajouter un Commentaire
ondate 14.11.2023
16
Aimer
Repost
Social
Ajouter
Détails
Social
Au programme de cette émission nous reçevont Eve DHALMANN chargé de développement du Para Handball de la Ligue Grand Est FFHandball. Elle vient nous parler de la deuxième édition de la coupe régionale de Handfauteil. Nous acceuillons également Jean Yves Marion, professeur à l'université de lorraine et membre de l'institut universitaire de France. Il vient nous parler des recherches en matière de cybersécurité
Traduisez-moi ceci, s'il vous plaît
RADIO CAMPUS LORRAINE
753
Podcast Emissio...

TAGS : ANSSI - CIBY - CYBER-DETECT - DEFMAL - E.D.I 132 - LORIA - VINCENT VERHAEGHE - WALLIX

La recherche fondamentale au service de la cyber

> **Installé à Nancy, le Loria et son Laboratoire de haute sécurité nous ont ouvert leurs portes en marge des assises universitaires Droit et Cybersécurité. La cyber est un sujet phare de la recherche en France.**

Nov 2023

PAR VINCENT VERHAEGHE À NANCY

Nancy accueille plus de 50 000 étudiants. Autant dire que la recherche est un des secteurs d'activité les plus dynamiques de la ville, et on y trouve de nombreuses initiatives et projets scientifiques au sens large. Regroupé sous l'appellation Lorraine Université d'Excellence (LUE), le pôle comprend en effet 68 laboratoires, et près de 4 500 chercheurs et 2 000 doctorants en liaison ou au cœur des grands instituts que sont le CNRS, l'Inserm ou l'Inrae, pour ne citer que les plus connus.

« C'est une politique de mise en commun de tout ce qui fait la recherche en France avec une approche pluridisciplinaire, toujours dans le but d'en faire profiter la société », résume Hélène Boulanger, présidente de l'université de Lorraine.

Parmi ces labos se trouve le Loria, « laboratoire lorrain de recherche en informatique et ses applications », issu en 1997 de la réunion du Crin et de l'Inria Lorraine. C'est avant tout un centre de recherche, mais son objectif est aussi que les fruits de ses recherches puissent être exploités concrètement par des entreprises, en général par le biais d'éditeurs dont certains incubés directement au sein du pôle LUE.

À la racine du mal

En France, dans le cadre du programme et équipements prioritaires de recherche (Prep), une dizaine de projets sont liés de près ou de loin à la cybersécurité (certains touchent la cryptographie et la vérification des protocoles) sur lesquels le Loria collabore. Parmi ces projets, il en porte un directement : le DefMal (Défense contre les programmes malveillants), qui a pour objectif de s'attaquer à l'analyse et à la défense contre les malwares. « Nous sommes avec les malwares dans des cas de cybermalveillance qui touchent non seulement les entreprises, mais aussi les collectivités locales ou les OIV. La plupart sont combinés à des attaques par rançongiciels, souvent avec des systèmes de double extorsion, mais ils servent également à l'espionnage ou dans les conflits tels que ceux que nous connaissons actuellement, en Ukraine ou au Proche-Orient », explique Jean-Yves Marion, professeur à l'université de Lorraine et directeur du Loria.

*Lancé il y a un an pour succéder au projet DigiTrust**, DefMal bénéficie d'un budget de 5 millions d'euros réparti sur six ans et se pare de collaborations à grande échelle en France comme à l'international, avec le Cispa en Allemagne ou le Nict au Japon. Il dispose, au sein du campus de l'université de Lorraine, du Laboratoire de haute sécurité (LHS) où les chercheurs axent leur travail sur trois pans.

> *« L'analyse polymorphe arrive en complément d'autres outils développés par les éditeurs, comme l'EDR ou le XDR »*
>
> *Régis Lhoste, président de Cyber-Detect*

Le premier, et le plus important, concerne le développement de nouvelles méthodes algorithmiques pour détecter et se défendre contre les malwares. « On parle ici de ceux qui attaquent les PC, mais cela concerne également d'autres cibles potentielles, comme les drones, les voitures autonomes et, plus globalement, tous les objets connectés », explique Jean-Yves Marion.

L'équipe du LHS exploite pour ses recherches une base d'environ 35 000 malwares, ce qui représente au final une petite partie de tous ceux qui pullulent sur les réseaux et dans les infrastructures, mais beaucoup sont de simples variations d'une souche commune. C'est d'ailleurs une des caractéristiques qui a déjà permis au DefMal de produire des résultats en développant des outils dits d'analyse polymorphe. Son principe : repérer dans un code des signatures typiques de malwares connus et ainsi prévenir les attaques.

Chaque signature correspond à des centaines de déclinaisons d'un même malware souche, ce qui rend l'outil d'autant plus efficace. Il y a déjà des applications concrètes, la start-up Cyber-Detect l'exploitant dans son outil de protection Gorille (voir encadré). « Personne ne peut assurer une protection à 100 % et l'analyse polymorphe arrive en complément d'autres outils développés par les éditeurs, comme l'EDR ou le XDR », explique Régis Lhoste, président de Cyber-Detect, qui précise que sa solution à base d'analyse polymorphe atteint un taux de détection de 95 à 100 % sur les malwares connus avec moins de 5 % de faux positifs.

Le deuxième axe de travail du projet DefMal est plus empirique puisqu'il consiste à utiliser

l'analyse pour mieux comprendre l'aspect comportemental des malwares et des cybercriminels. « On peut, par exemple, identifier un groupe d'attaques en fonction de caractéristiques typiques, mais nous analysons aussi les conséquences des attaques, le tout dans une approche pluridisciplinaire », explique Jean-Yves Marion.

Ce qui rejoint le troisième axe, la mise à disposition d'une plate-forme d'échange pour faire profiter tout l'écosystème des avancées du LHS, qui ne s'arrête pas aux échanges entre chercheurs. Des connexions sont établies entre le laboratoire et les institutions publiques, comme le ministère de la Justice, ComCyberGend (la branche de la gendarmerie spécifiquement dévolue aux cybermenaces) ou l'Anssi.

Des organismes qui eux-mêmes remontent des informations vers le LHS, même si elles sont sélectionnées
et filtrées. Le lien avec le secteur privé est permanent, ce qui change des habitudes qu'on retrouve souvent dans la recherche universitaire. « Il est vrai que la recherche fondamentale se fait généralement sur des temps longs, alors que, dans le cadre de la cybermalveillance, il est indispensable de travailler sur des temps courts car la typologie des attaques évolue rapidement. Avec le Loria et le LHS, nous sommes dans une posture réactive et nous nous adaptons à ces évolutions pour pouvoir produire des résultats rapides quand c'est nécessaire. »

Chercheur et enseignant à l'université de Lorraine, Jean-Yves Marion est à la tête du projet DefMal, initié par le Loria.

Ainsi, outre les start-up incubées au sein de l'université, le Loria travaille avec des éditeurs qui ont déjà pignon sur rue, comme c'est le cas avec le français Wallix. Ce dernier dispose de chercheurs qui travaillent en collaboration étroite avec le LHS. « Ce qui manque en revanche, c'est un véritable outil qui permettrait de tester les solutions de cybersécurité de façon indépendante car beaucoup d'éditeurs font leurs propres tests et les orientent de façon que leurs solutions produisent les meilleurs résultats », regrette Jean-Yves Marion.

C'est d'ailleurs une des pistes qu'il évoque pour la mise en route de futurs projets au sein du LHS, parmi d'autres, comme la possibilité de plus agir en mode défense vis-à-vis des hackers, mais en mode contre-attaquant de façon à entrer dans leurs systèmes et, par exemple, débloquer des données encryptées par ransomware ou récupérer des rançons payées en cryptomonnaie.

L'analyse des flux financiers et le blanchiment d'argent, souvent corolaires de la cybermalveillance, sont également dans les projets, à condition toutefois de pouvoir les financer, car cela reste le nerf de la guerre, qu'elle soit cyber ou pas.

* Le mandat de dix ans de Jean-Yves Marion à la tête du Loria s'est terminé le 1er octobre 2025. Mais il reste à la tête du Laboratoire de façon transitoire. Il a été remplacé à la direction du Loria par Samira Tounsi.

** DigiTrust avait pour objectif de renforcer la confiance des citoyens dans le monde numérique.

Des start-up en quête de distribution

Au sein du site Lorraine Université d'Excellence, une demi-douzaine d'entreprises sont créées chaque année pour donner un écho commercial aux recherches effectuées dans les laboratoires du pôle. Deux d'entre elles sont directement liées à la cybersécurité, Ciby et Cyber-Detect.

Ciby se positionne sur le marché de la détection des vulnérabilités des systèmes d'information. Son produit Scuba scanne les différents points d'entrée possible pour révéler les chemins d'attaque potentiels et propose aussi bien des plans d'urgence que des correctifs. « Nous permettons ainsi aux DSI de gagner énormément de temps en limitant à la source le nombre d'attaques », explique Abdelkader Lahmadi, cofondateur de Ciby et enseignant-chercheur au Loria.

Cyber-Detect exploite de son côté directement les avancées du LHS avec une solution de détection de malwares appelée Gorille, exploitant l'analyse polymorphe. « Notre solution, comme celle de Ciby, a pour vocation à être distribuée par des intégrateurs, des MSP et des MSSP auprès des entreprises. Nous en avons déjà quelques-uns avec qui nous travaillons mais c'est un réseau que l'on veut étendre », explique Régis Lhoste, président de Cyber-Detect.

Yannick Toussaint est le nouveau directeur du Loria, le Laboratoire lorrain de recherche en informatique et ses applications, compo-sante du CNRS, de l'Inria, et de l'Université de Lorraine. Le nouveau directeur, qui était auparavant directeur adjoint au Loria, succède à Jean-Yves Marion, qui a passé onze ans à la tête de ce laboratoire.

Le Journal des entreprises, 16 novembre 2023

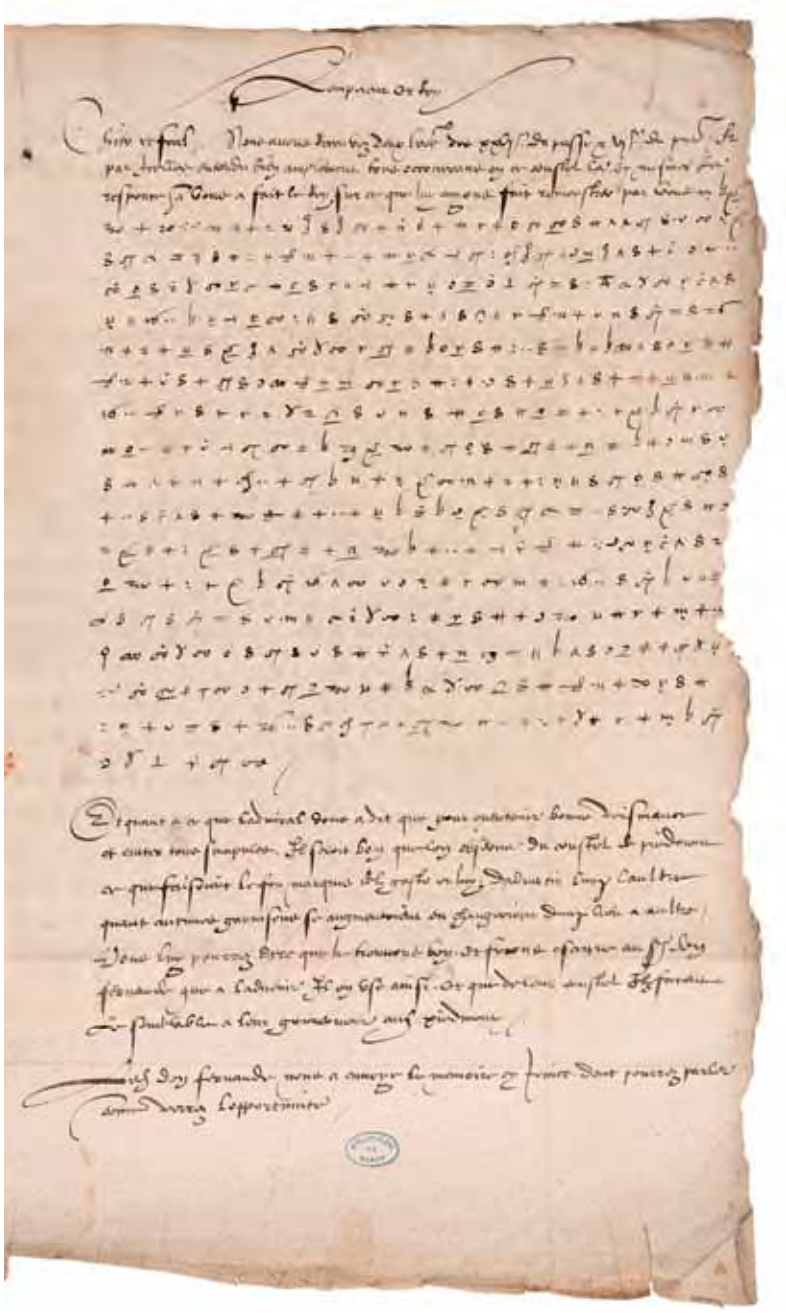
Deux start-up lorraines issues du PeeL deviennent des Pépites

Le prix Pépite France vient de distinguer deux start-up lorraines issues du PeeL, le Pôle entrepreneuriat étudiant de Lorraine, basé à Nancy. Dans la catégorie "Grande Pépite France", c'est Louis Abel qui a été récompensé pour son projet Dynalips. La start-up développe une solution pour transformer l'animation grâce à une technologie issue de l'intelligence artificielle qui permet d'animer automatiquement les lèvres d'un personnage virtuel. Dans la catégorie "Prix spécial du jury" dédié à la transition écologique, les professionnels ont choisi Jean-Christian Hartemann et son projet Kardes. Encore en phase de préincubation, le projet Kardes développe ses liens avec les acteurs universitaires de la recherche pour mettre au point une technologie innovante pour l'hygiène et la santé.

Histoire d'un manuscrit

La lettre chiffrée de Charles Quint

En novembre 2022, la bibliothèque Stanislas de Nancy annonçait le déchiffrement d'une lettre secrète envoyée par Charles Quint à l'un de ses ambassadeurs dans le royaume de France. Une équipe de chercheurs s'est penchée sur l'histoire du chiffrement au XVIe siècle.



Lettre chiffrée de Charles Quint datée du 22 février 1546 (selon le style de Pâques), ce qui correspond à l'année 1547 selon notre calendrier contemporain. © Bibliothèque Stanislas, Nancy, Collection des autographes Charles Quint, 2.

Quand Cécile Pierrot, chargée de recherche en cryptographie à l'INRIA (Institut national de recherche en sciences et technologies du numérique) apprend par hasard l'existence d'une correspondance chiffrée écrite par l'empereur Charles Quint, sa curiosité est piquée au vif. Grâce au bouche à oreille, elle découvre en 2021 qu'une lettre rédigée sur papier est conservée à la bibliothèque municipale Stanislas de Nancy. Ce document n'apparaît dans aucun catalogue et n'a pas été numérisé. Cécile L'Huillier, bibliothécaire, retrouve le manuscrit dans la collection des autographes. Il est adressé à Jean de Saint-Mauris, ambassadeur de Charles Quint dans le royaume de France.

Cryptographie et informatique

La chercheuse constate qu'une partie du texte est en effet chiffrée, tandis que le reste est rédigé en clair dans le français du XVIe siècle qu'on appelle le « moyen français ». Cette langue, utilisée par Montaigne, Rabelais ou encore les poètes de la Pléiade, est un intermédiaire entre l'ancien français et le français classique. Cécile Pierrot utilise les méthodes habituelles de déchiffrement fondées sur l'informatique sans parvenir à comprendre tout le texte. Elle demande alors à deux collègues cryptographes, Pierrick Gaudry et Paul Zimmermann, directeurs de recherche au CNRS et à l'INRIA, d'étudier la lettre avec elle. Ensemble, ils créent un algorithme permettant de tester de nombreuses hypothèses de correspondance entre chacun des 120 symboles utilisés et son sens possible : lettre, lettre double, ensemble de lettres, personnalité ayant vécu dans la première moitié du XVIe siècle… Ils savent également qu'à cette époque les documents de cette nature comportaient souvent des symboles nuls, c'est-à-dire des caractères ne donnant aucune information, mais dont le but était de brouiller la lecture éventuellement effectuée par des yeux indésirables. À ce stade, la solution n'a pas encore été trouvée, la lettre conserve une part de mystère.

L'histoire à la rescousse

C'est alors que l'équipe d'informaticiens entre en contact avec Camille Desenclos, spécialiste d'histoire diplomatique, experte en cryptographie des XVI[e] et XVII[e] siècles et maîtresse de conférences à l'université de Picardie-Jules Verne. En effet, pour pouvoir déchiffrer le texte, il faut une connaissance fine du contexte historique dans lequel il a été écrit et des sources de cette époque. L'historienne confirme que la partie chiffrée est probablement en moyen français, tout comme le texte en clair, car les documents diplomatiques étaient généralement rédigés dans une seule langue. De plus, Charles Quint parlait le français, notamment avec ses interlocuteurs habituels, comme l'atteste sa correspondance avec sa sœur Marie de Hongrie. Jean de Saint-Mauris, destinataire de la fameuse lettre, est le beau-frère de l'un de ses plus proches conseillers, le cardinal Antoine Perrenot de Granvelle. Par chance, certains des papiers du cardinal sont conservés à la bibliothèque de Besançon car ils ont été rassemblés par l'abbé Boisot (1639-1694), grand collectionneur, dont les fonds sont répertoriés et numérisés par la bibliothèque municipale. Dans cette collection se trouvent plusieurs lettres de Jean de Saint-Mauris.

Camille Desenclos apporte des informations précieuses : la taille de l'empire qui s'étend des Pays-Bas espagnols au nord à la péninsule Ibérique au sud et de la Franche-Comté à l'ouest jusqu'à l'Autriche à l'est nécessite un système performant de communication entre Charles Quint et ses différents relais de pouvoir sur ces vastes territoires. Les courriers circulent selon un modèle en étoile dont l'empereur forme le centre. Sont parvenus jusqu'à nous bon nombre de documents écrits dont beaucoup devaient être chiffrés car ils contenaient des informations confidentielles sur la politique à mener. Ceux adressés aux ambassadeurs ont souvent été conservés par les familles, puis vendus ultérieurement à titre de documents historiques. Quant aux lettres qui étaient adressées aux souverains, elles sont généralement restées dans les archives de l'État. Elles pouvaient être envoyées soit par une organisation rudimentaire de poste régulière, soit par courrier spécial ou encore transportées par des marchands. Dans le premier cas, le risque était grand que les paquets de lettres soient ouverts et les documents recopiés lors d'un des nombreux arrêts du véhicule. Si certaines lettres refermées pouvaient ensuite reprendre leur itinéraire, il était impossible de savoir

De haut en bas :
Portrait de Charles Quint, gravure au burin [XVII[e] siècle], bibliothèque Stanislas, Nancy, cote FG3. © Bibliothèque Stanislas, Nancy.

Portrait de Charles Quint, gravure sur cuivre signée Harrewÿn [Jacques Harrewyn (1660-1727)] en frontispice de l'ouvrage *Les Actions heroiques et plaisantes de l'Empereur Charles V.*…, Brusselle, Antoine Lemmens, 1715, in-12, reliure plein veau, bibliothèque Stanislas, Nancy, cote 258 543. © Bibliothèque Stanislas, Nancy.

Histoire d'un livre

La lettre est étudiée par Cécile Pierrot, chargée de recherche à l'Inria de Nancy (à gauche au premier plan) et Camille Désenclos, maîtresse de conférences en histoire moderne (à droite au premier plan). © Ville de Nancy.

qu'on les avait lues. Le système du courrier chevauchant seul comportait moins de risques puisqu'une éventuelle interception était forcément connue, à moins que le chevaucheur ne se laisse acheter. Mais c'était un système plus coûteux, qu'on ne pouvait utiliser que pour les dépêches à très haut risque ou présentant un caractère d'urgence. Et, sur les longues distances, le changement de monture comportait toujours la possibilité d'une lecture pendant les temps de repos, sans que le cavalier s'en aperçoive.

La clé de l'énigme

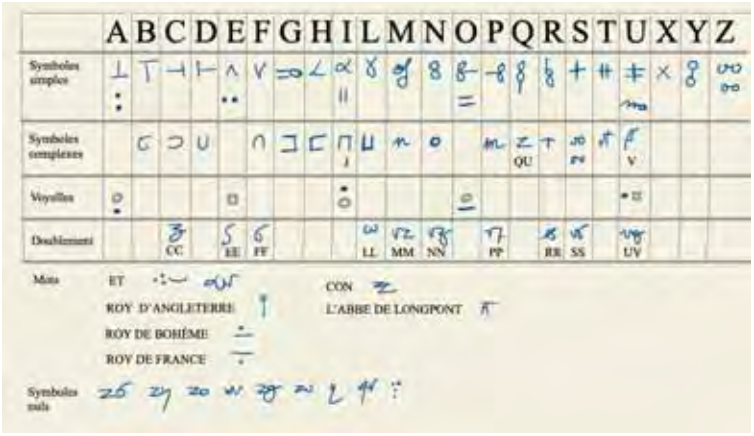
Finalement, c'est en cherchant dans les papiers Granvelle à Besançon qu'on découvrit une partie de la correspondance de Jean de Saint-Mauris. En utilisant la même clé que la lettre de Charles Quint, des passages avaient pu être déchiffrés et notés en clair dans la marge. Cette découverte permit de confirmer ou d'infirmer les hypothèses des chercheurs. Première surprise, le procédé avait contourné un des moyens les plus évidents de déchiffrage. Il est en effet de tradition, lorsqu'on cherche à comprendre un document, de commencer par repérer le signe qui apparaît le plus souvent. En français, il s'agit de la lettre « e ». Or, dans les dépêches de Charles Quint, toutes les lettres « e » sont systématiquement éliminées lorsqu'elles suivent une consonne, ce qui complique largement le travail des cryptanalystes. Une autre question restait sans réponse : les chercheurs avaient compris que certains symboles renvoyaient à des personnalités de haut rang : le roi de Bohême Ferdinand de Habsbourg, frère de Charles Quint, et le roi de France François Ier avaient été clairement identifiés, d'autant plus que ce dernier était justement la personne à laquelle on devait cacher les informations contenues dans le message. Un autre personnage de premier plan restait mystérieux, désigné par un symbole en forme d'épingle. La lettre, datée en clair de 1546, le désignait comme mort. Pourtant, à cette date, aucun souverain ne venait de trépasser en Europe. Mais Camille Desenclos savait qu'au XVIe siècle l'habitude était encore de changer d'année à Pâques et non le 1er janvier. Or, le 28 janvier 1547 de notre calendrier actuel, le roi d'Angleterre Henri VIII était décédé. C'est donc bien lui que désigne l'épingle. Grâce à cette information, la lettre a pu être précisément datée du 22 février 1547.

Rumeurs et consignes

Malgré le mystère qui a plané sur son contenu pendant plusieurs mois et les espoirs qu'elle a suscités, la lettre une fois déchiffrée n'a pas révélé de secrets remettant en cause une page de notre histoire. On y apprend surtout que Charles Quint a eu vent d'une rumeur : Pierre Strozzi, chef de guerre au service de François Ier, aurait cherché à le faire assassiner. La suite prouvera que ce projet n'a pas été suivi d'effet, puisque l'empereur mourut de fièvre typhoïde en 1558 au monastère de Yuste après avoir abdiqué en faveur de son fils Philippe II, devenu roi d'Espagne, et de son frère Ferdinand Ier, recueillant la couronne impériale. Par ailleurs, Charles Quint se montre soucieux de cacher au roi de France les difficultés auxquelles il se heurte avec les princes allemands protestants qui, regroupés dans la ligue de Smalkalde, remettent en cause l'autorité catholique trente ans après l'apparition des thèses de Luther. Deux mois après la rédaction de la lettre, Charles Quint va remporter une victoire décisive sur la ligue de Smalkalde à Mühlberg, le 24 avril 1547. Finalement, le document ne fait que confirmer des faits historiques, sans apporter d'éclairage nouveau sur la longue concurrence entre François Ier et Charles Quint. Ce qui en fait la saveur est peut-être le fait qu'elle a été écrite un mois avant la disparition de François Ier, une mort inespérée pour son rival de toujours.

Claire L'Hoër

Institutions et particuliers sont invités à proposer leurs documents anciens à déchiffrer à l'équipe interdisciplinaire qui a mené à bien ce travail. Contact : Cécile Pierrot, cecile.pierrot@inria.fr



« Malgré le mystère qui a plané sur son contenu pendant plusieurs mois et les espoirs qu'elle a suscités, la lettre une fois déchiffrée n'a pas révélé de secrets remettant en cause une page de notre histoire. »

De haut en bas :
Clef de chiffrement des correspondances entre Charles V et son ambassadeur Jean de Saint-Mauris, établie par Cécile Pierrot et son équipe. © Cécile Pierrot.

Déchiffrement final de la première page. © Cécile Pierrot.

Savoir(s)

(/fileadmin/upload/Savoirs/Societe/stage_maths_irma.jpg)

17 | 11 | 23

Par **Elsa Collobert**

Temps de lecture : 4 min

Un stage de mathématiques et informatique pour susciter des vocations chez les jeunes filles

Résoudre des problèmes le matin, se détendre l'après-midi, pendant les vacances de la Toussaint, le tout dans un village de vacances des Vosges : 25 lycéennes issues de tout le Grand Est et même d'Allemagne ont relevé le défi ! A la clé pour les organisateurs, issus de trois laboratoires de recherche des universités de Strasbourg et de Lorraine* : désamorcer les appréhensions liées à ces enseignements et faire tomber les barrières à l'orientation liée au genre.

« Personnellement, ce stage m'a enrichie énormément car on se dit qu'on peut avoir confiance, qu'il y a des femmes qui ont réussi dans ces domaines, que ce n'est pas qu'un truc de gars », témoigne Ozanne. Eryne, de son côté, a *« pris conscience qu'il y avait aussi des femmes brillantes en mathématiques et informatique, pas seulement Pythagore et Thalès »*.

Si l'on en juge d'après les témoignages de ces deux lycéennes, les objectifs affichés par les organisateurs du stage qui s'est tenu du 22 au 27 octobre derniers, à Ramonchamp (Vosges) ont été pleinement atteints. *« Et même au-delà de nos espérances »*, se félicite Clémentine Courtès, enseignante-chercheuse en mathématiques au sein de l'Irma (Université de Strasbourg), qui fait partie de l'équipe organisatrice du stage, baptisé « Les Cigognes » *(lire encadré)*.

Parmi leurs objectifs : *« Participer à la diffusion de la culture et de l'esprit scientifique, tout en luttant contre la désaffection des femmes pour les mathématiques et l'informatique »* – en 2016, sur quatre ingénieurs de moins de 30 ans, seule une est une femme. Une désaffection qui commence tôt, seules 19 % de filles parmi les élèves de classe de 1ère choisissant la spécialité Numérique et sciences informatiques (NSI), et semble même s'accentuer depuis la dernière réforme du lycée. Clémentine Courtès (Irma, Université de Strasbourg), Marie Duflot-Kremer (Loria, Université de Lorraine), Anne de Roton (IECL, Université de Lorraine), Pierre Py (CNRS, Université de Strasbourg jusqu'au 31/08/2023 puis Université de Grenoble) et Samuel Tapie (IECL, Université de Lorraine) ont donc décidé de prendre le problème à la racine.

Lutter contre l'autocensure

« Nous avons pris soin de sélectionner des profils variés, et de nous baser sur les lettres de motivation plutôt que sur les notes. » Une quarantaine de candidatures ont été reçues, pour 25 places. Au final, dix élèves de 2nde, quatorze de 1ère et une de Tle ont participé au stage, issues de lycées de secteurs très variés (Metz, Nancy, Colmar, Strasbourg, Bouxwiller, Lunéville, Remiremont, Thann, Guebwiller, Saint-Dié-Des-Vosges, Vésoul, Fribourg-en-Brisgau) : *« Ce large recrutement nous permet de toucher des élèves issues de milieux ruraux, plus éloignées des études scientifiques. »*

(/fileadmin/upload/Savoirs/Societe/stage_cicognes2.jpg)

« L'idée du stage est de montrer aux jeunes filles que les métiers des mathématiques et de l'informatique leur sont ouverts. » © DR

« L'idée du stage n'était pas de trouver à tout prix les Marie Curie de demain, mais de montrer aux jeunes filles que les métiers des mathématiques et de l'informatique, que ce soit dans la recherche académique ou dans le secteur privé, leur sont aussi ouverts. Nous voulions lutter contre l'autocensure qu'elles ont trop tendance à s'imposer dans les matières scientifiques et leur montrer que les options mathématiques et NSI en classe de 1ère leur sont tout à fait accessibles. »

Les mathématiques dans la vraie vie ?

Le programme de la semaine avait été particulièrement soigné pour ne pas être indigeste. Les matinées étaient consacrées au travail de réflexion sur des problèmes, pour certains encore ouverts (géométrie, parallélisme en parallélisme, arithmétique, probabilités…), en groupe, loin du programme scolaire. Une restitution a eu lieu en fin de stage, devant les familles. D'autres activités scientifiques étaient organisées : des temps d'échanges et de témoignages de femmes scientifiques, des conférences généralistes (« A quoi servent les mathématiques dans la vraie vie ? », « Détecter les nouvelles pollutions de l'air au moyen de l'informatique »), des ateliers interactifs (« Comprendre l'intelligence artificielle », « Comprendre l'importance des nombres premiers », « Comment paver un rectangle au moyen de carrés ? »). Une après-midi était consacrée à un atelier sur les stéréotypes garçon-fille, *« avec des échanges très intenses et des témoignages très personnels »*. Un questionnaire créé par une sociologue a permis d'aborder les motivations à participer au stage et l'éventuel impact futur sur leur choix d'études.

La semaine a aussi été ponctuée d'activités ludiques et récréatives : yoga, pilates, atelier d'expression corporelle, soirée escape game (basée sur l'informatique), soirée « informagie » (avec des tours de magie dont les astuces reposent sur de l'informatique et des mathématiques), une projection d'un film (*Secret of the surfaces*, sur la vie de Maryam Mirzakhani, première lauréate de la médaille Fields, en 2014), et une soirée festive.

Cadre verdoyant

Le choix du lieu n'a pas non plus été laissé au hasard : *« Pas dans un amphithéâtre universitaire, ce qui aurait pu être intimidant, mais à l'inverse un cadre verdoyant, pour faire passer ce message : "L'université vient à votre rencontre". Ainsi que celui de l'accessibilité : "Nous ne sommes pas obligés d'être particulièrement brillantes pour nous amuser en faisant des mathématiques et de l'informatique". Nous voulions que cette expérience reste avant tout sympathique, ludique et amusante »*. Reçu 5/5 !

L'initiative a été financée par les partenaires des universités de Lorraine et de Strasbourg, les organismes de recherche et les laboratoires dont l'Institut de recherche mathématique avancée (Irma) et l'Institut de recherche sur l'enseignement des mathématiques (Irem), la région Grand Est, la fondation Blaise-Pascal, le programme national MathC2+. Forte d'un bilan très positif, l'initiative devrait être reconduite à l'avenir.

→ (file:///Users/ecollobert/Downloads/cp_ul_les_cigognes_octobre_2023.pdf)**Plus d'informations (/fileadmin/upload/Savoirs/Societe/cp_ul_les_cigognes_octobre_2023.pdf)**

** Institut Elie-Cartan de Lorraine (IECL), Laboratoire lorrain de recherche en informatique et ses applications (Loria) et l'Institut de recherche mathématique avancée (Irma)*

Les « Cigognes » succèdent aux « Cigales »

« Le choix du nom du stage, "les Cigognes", est un clin d'œil au stage "Les Cigales" (https://www.fr-cirm-math.fr/les-cigales-automne-2023.html#:~:text=DU%2023%20au%2027%20octobre%202023&text=L%27%C3%A9cole%20de%20m organisé par nos collègues de Marseille, dont il s'inspire », explique Clémentine Courtès. En 2019, des collègues enseignants-chercheurs de l'Université d'Aix-Marseille ont décidé d'organiser une semaine de stage de mathématiques pour lycéennes. Quatre ans plus tard, le concept a tellement bien pris qu'ils organisent deux stages par an et qu'ils sont obligés de refuser des candidates. *« Nous avons souhaité exporter le concept dans le Grand Est, avec la spécificité de rajouter de l'informatique dans notre stage. »*

« Pas de notion de supériorité »

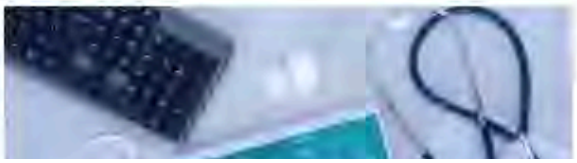
« J'ai pris connaissance de ce stage par mon professeur de physique-chimie, qui a envoyé un mail à des élèves de mon lycée. Je suis allée sur le site internet et j'ai vu que l'emploi du temps avait l'air pas mal. A la base, l'informatique n'est pas quelque chose qui me passionne vraiment, même si je pense qu'on n'a pas encore vraiment vu [ce qu'est] l'informatique au collège et lycée. Ce qui me plait dans le stage, c'est qu'il y a vraiment une bonne ambiance, c'est un stage décomplexé. Personne ne juge les autres. Il y a vraiment un bel ensemble et pas de notion de supériorité des uns par rapport aux autres. Même avec les encadrants, on ne se sent pas inférieures comme dans les cours, personne ne nous prend de haut. Je reviendrais bien l'année prochaine.

***Témoignage de Céline** »*

Cet article fait partie de la série : [Dossier] Numérique en Santé : de la défiance à l'inspiration

À Corbeil-Essonnes, les données de santé tiraillées entre innovation et cybersécurité

publié le 23 novembre 2023 par *Jean-Baptiste Lautier*



L'an passé, l'Hôpital de Corbeil-Essonnes a subi une attaque d'ampleur de son système

informatique. Cet électrochoc a conduit la DSI à placer la sécurité au centre de tous les projets, tentant malgré tout de continuer à exploiter ses données pour faire avancer la recherche.

"Avant, on construisait l'intérieur de la maison et ensuite seulement on posait les murs". Cette métaphore de Patrice Garcia, directeur des systèmes d'information du Centre hospitalier sud francilien, à Corbeil-Essonnes, résume la prise de conscience que l'établissement en matière de cybersécurité. « Avant » fait en effet référence aux évènements d'août 2022 : le Centre hospitalier est alors la proie d'une attaque d'ampleur de son système informatique. Celle-ci a eu un impact sur l'établissement pendant plusieurs mois. "Maintenant, dès la première pierre d'un projet, la sécurité est présente", assure le DSI. Ce qui peut paraître du bon sens, alors que les cybercriminels lorgnent toujours plus sur les données de santé, ne va pourtant pas toujours de soi. En effet, le secteur dans son ensemble est pris dans un étau, entre la nécessité d'exploiter les données à sa disposition avec l'aide de tiers pour faire avancer la médecine, et le risque qu'un tel partage implique.

Des gisements de données convoités

"La numérisation de l'hôpital a créé un énorme gisement de données", assure Patrice Garcia. L'analyse de ce patrimoine grâce à des outils numériques prévus pour gérer des « big data », plutôt que manuellement, est un accélérateur important pour la recherche. Pour Jean-Yves Marion, ancien président du Loria (Laboratoire lorrain de recherche en informatique et ses applications) à Nancy et professeur à l'Université de Lorraine, les établissements de santé ont besoin de valoriser leurs données : "Ils ouvrent leurs données [à d'autres acteurs] pour des raisons légitimes". C'est l'un des moyens clés pour innover.

À lire aussi : Quelles leçons tirer de la cyberattaque du Centre hospitalier de Corbeil-Essonnes ?

En effet, l'arrivée de l'intelligence artificielle apporte des perspectives immenses dans l'analyse de la masse de données que détient un hôpital. "On fait du deep learning pour permettre à l'intelligence artificielle d'apprendre afin d'aider les médecins", explique Patrice Garcia, DSI du Centre Hospitalier Sud-Francilien. Il prend un exemple concret : "Aux urgences, une IA aide à interpréter des radios. Cela permet aux jeunes radiologues en traumatologie de ne pas laisser passer de graves blessures".

Si l'apprentissage automatique donne de la valeur aux données de santé, les

Si l'apprentissage automatique donne de la valeur aux données de santé, les hôpitaux comme celui de Corbeil-Essonnes peuvent difficilement mener les projets seuls. Jean-Yves Marion souligne que dans l'écosystème, nombre d'acteurs regardent d'ailleurs avec appétit ces gisements. "Les données de santé ont de la valeur pour des entreprises qui font de la médecine personnalisée, de la pharmacovigilance, du repositionnement de molécule…", illustre l'ancien directeur du Loria. "L'IA promet aussi beaucoup dans les nouvelles thérapies, mais pour faire la différence, il faut énormément de données". Pour faire avancer la médecine, il est donc nécessaire de partager les données et ce, sans compromettre leur sécurité ou la vie privée des patients.

Trouver un cadre de confiance avec les tiers

"Avec l'attaque que nous avons subie, la démarche a totalement changé. Tout est dorénavant analysé sous l'angle de la sécurité. Elle est intégrée à tous les projets. Cette démarche nous rassure", souligne le DSI de l'Hôpital de Corbeil-Essonnes. Le sérieux de la démarche vient également du choc subi par le personnel. : "Ce qu'on a vécu a eu un effet pédagogique monstrueux. Ça vaut toutes les communications du monde", assure Patrice Garcia. "Je dis souvent qu'avec cette attaque, j'ai gagné trois ans de communication interne". Il salue le niveau de vigilance très fort du personnel : "On effectue régulièrement des tests de phishing. Nous sommes à un taux de clic de deux à trois pour cent". Des niveaux qui feraient pâlir nombre de grandes entreprises y compris celles spécialistes du numérique.

Afin de permettre une exploitation des données à sa disposition en toute confiance, le Centre hospitalier sud francilien applique donc une politique stricte. "Ce qui est important, c'est de travailler avec des entreprises qui ont pignon sur rue et qui sont capables de prouver qu'elles ont un niveau de sécurité au moins équivalent au nôtre", indique le DSI. "La société doit respecter les standards du marché et nous devons pouvoir mener des audits". De plus, lorsque le centre hospitalier collabore avec l'extérieur, les données sont totalement anonymisées.

À lire aussi : Grâce au bruitage, le CEA-List crée un écosystème de confiance pour entraîner des IA

Au-delà de la question de la cybersécurité, l'aspect éthique est également pris en considération. Patrice Garcia souligne à ce titre une différence entre les partenariats avec les acteurs privés et ceux du secteur public : "Avec le privé, nous n'avons pas la même philosophie, contrairement à la recherche publique où le côté éthique nous rassure", affirme Patrice Garcia. "On ne veut pas offrir à une entreprise un monopole en leur transmettant trop d'informations. On cherche avant tout le bénéfice pour le patient". Une préoccupation importante d'après Jean-Yves Marion, qui donne un avantage

aux travaux menés en commun avec des acteurs publics : "Dans la recherche publique, on est extrêmement clair sur l'utilisation qui est faites des données".

A l'avenir, le partage de données en confiance pourrait être facilité par la technologie elle-même.

L'apprentissage fédéré, méthode qui permet à différentes entités de contribuer à un modèle d'IA sans centraliser les données, fait partie de ces pratiques qui peuvent rassurer les détenteurs de données sensibles à valoriser. "C'est une des solutions possibles. On attend également beaucoup du chiffrement homomorphique qui permettra au machine learning de se faire directement sur des données chiffrées." laisse entrevoir le professeur Jean-Yves Marion. Un moyen peut-être de réconcilier définitivement cybersécurité et recherche médicale.

Les dirigeants, cible préférée des hackers

● Il suffit d'un « like » d'un ami sur une photo ou d'un centre d'intérêt rendu public pour les exposer.
● Souvent inconscients du danger de leur activité en ligne, les dirigeants et cadres supérieurs sont douze fois plus ciblés par les cybercriminels.

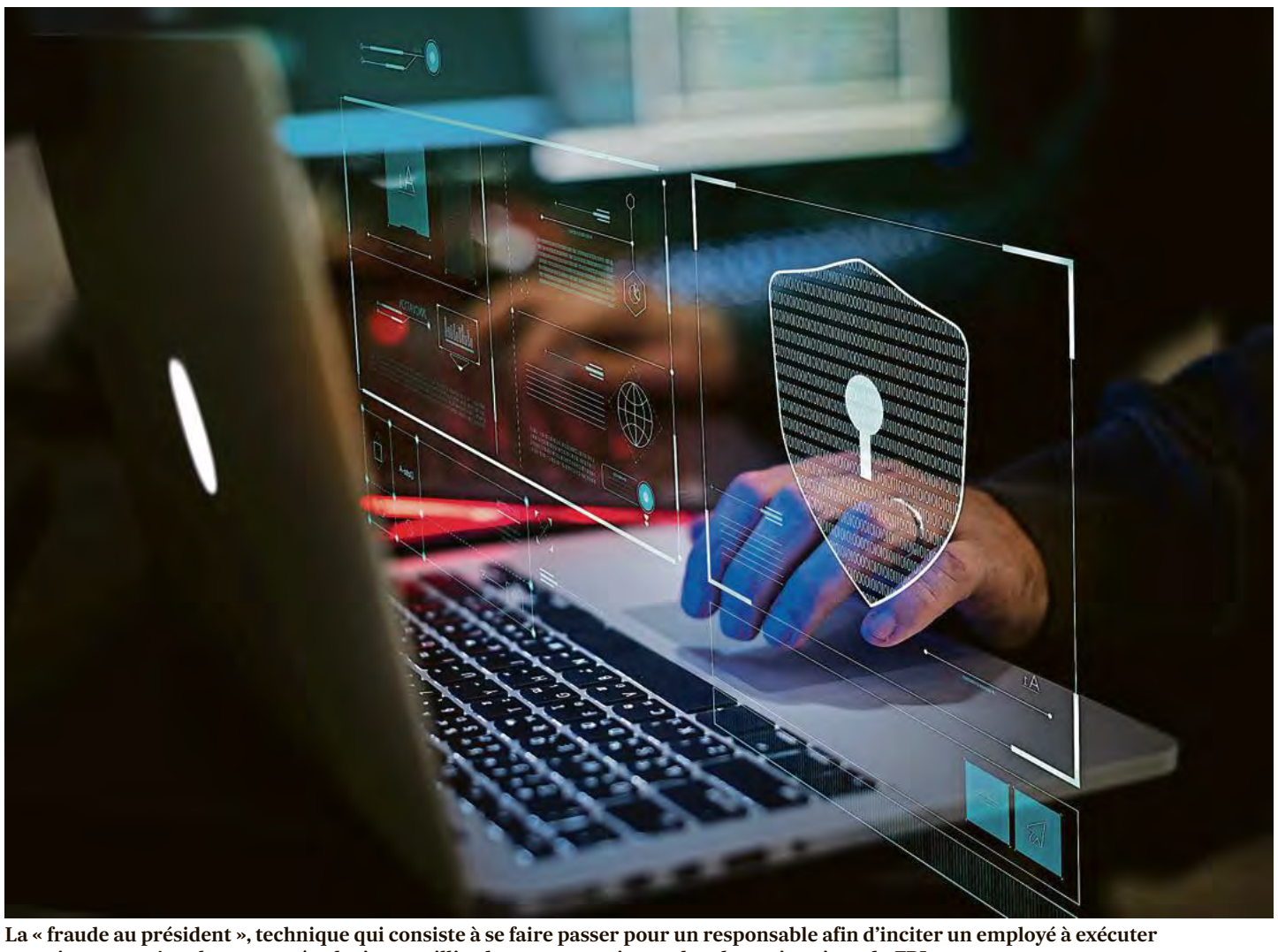
CYBERSÉCURITÉ

Leïla Marchand

Il est un secret encore bien gardé des entreprises : celui du nombre de fois où elles ont été ciblées par des cyberattaques. Mais il est un secret encore mieux gardé que celui-là : celui du nombre de fois où leurs dirigeants étaient directement dans le viseur des pirates. Et pourtant, le phénomène est aussi important que silencieux, rapporte la société Anozr Way.

« Les dirigeants et les membres de comex ou de codir sont douze fois plus ciblés que les autres par les attaques de toutes sortes », alerte Philippe Luc, cofondateur et CEO de cette start-up installée à Rennes, haut lieu de la cybersécurité en France, où se tenait justement cette semaine l'European Cyber Week (ECW 2023), un des grands événements du secteur.

Alors que le nombre de cyberattaques contre les organisations publiques et privées explose – au point de leur avoir coûté environ 2 milliards d'euros en 2022 en France, selon une évaluation récente du cabinet Asterès –, ces dommages viennent plus souvent qu'on ne le croit de fuites au plus haut niveau hiérarchique.



La « fraude au président », technique qui consiste à se faire passer pour un responsable afin d'inciter un employé à exécuter un paiement, coûte chaque année plusieurs milliards aux entreprises, selon des estimations du FBI. *Photo Shutterstock*

Des dirigeants pas assez méfiants

D'après une étude menée par Anozr Way, sept dirigeants sur dix présentent une exposition cyber à haut risque. *« Généralement, ils ne sont pas assez méfiants. Ils pensent qu'ils sont protégés car pas très actifs sur les réseaux sociaux ou, au contraire, ils considèrent qu'en tant que personnalités publiques, leur exposition est normale »*, pointe Philippe Luc, dont l'entreprise travaille surtout pour des grands comptes, dans la finance, l'industrie, l'énergie ou l'assurance. *« Les dirigeants – surtout les plus anciens – peuvent être peu sensibilisés aux bonnes pratiques. Et les patrons de PME pensent représenter une entreprise lambda parmi d'autres et ne pas être des cibles intéressantes »*, confirme Jonathan Gosselin, responsable Europe du Sud de SailPoint, entreprise américaine de solutions de gestion des identités.

Mais un simple commentaire sur une photo ou un centre d'intérêt rendu public les rend vulnérables, les pirates ayant vite fait d'exploiter ces informations personnelles, généralement accessibles facilement : d'après Anozr Way (qui s'appuie sur des cas réels anonymisés de 100 membres de comex ou codir d'entreprises de tous secteurs), environ 66 % des dirigeants affichent des réseaux sociaux personnels ouverts publiquement.

« On a eu par exemple le cas d'un haut cadre qui postait des publications en lien avec sa passion du tennis. En retour, il a été visé par des mails de phishing sur le thème du tennis », raconte l'entrepreneur Philippe Luc. Il n'est pas rare que les pirates usurpent l'identité d'un proche pour faire passer ces messages piégés : 70 % des décideurs font face à ce risque de phishing ciblé. *« Le nerf de la guerre aujourd'hui est de trouver des techniques pour crédibiliser l'attaque le plus possible, et affiner les scénarios d'hameçonnage »*, explique Jonathan Gosselin. Le mail ou le SMS reçus seront ainsi très difficiles à différencier d'un message authentique.

Un pseudonyme ne suffit pas

Autre cas d'école : celui d'un directeur financier avec une seule photo publiée sur Facebook et « likée » par sa conjointe. Il n'en fallait pas plus pour identifier les noms de tout son cercle proche, dont ses enfants, leurs photos et leur adresse personnelle. *« Ce sont des informations hautement sensibles, qui peuvent permettre de faire pression sur le dirigeant ou l'entreprise »*, relève Adèle Hayel, responsable marketing d'Anozr Way.

Très poreuse avec la sphère professionnelle et moins bien protégée, la sphère personnelle représente l'angle mort idéal. *« Certaines personnes pensent être bien cachées, par exemple en menant une vie privée sous pseudonyme. Mais ce n'est pas le cas ! »* prévient Adèle Hayel. Les pirates parviennent quand même à remonter la piste, notamment grâce aux données qui fuitent régulièrement sur le dark web : environ un dirigeant sur deux a un numéro de téléphone, ou au moins un mot de passe exposé en ligne.

Problématique, lorsque l'on sait que 80 % d'entre eux utilisent un seul et même mot de passe pour au moins 4 à 5 comptes différents, professionnels ou personnels. *« Aujourd'hui, acheter des bases de données, pour savoir si une entreprise a déjà payé pour un ransomware ou obtenir des mots de passe de dirigeants, est possible pour quelques centaines d'euros sur le dark web »*, a constaté Thomas Kerjean, CEO de l'entreprise française de cybersécurité Mailinblack.

Droits d'accès

Une fois ces données entre leurs mains, une des pratiques favorites des cybercriminels est celle de la « fraude au président ». La technique – qui coûte chaque année plusieurs milliards aux entreprises, selon des estimations du FBI – consiste à se faire passer pour le dirigeant et à profiter de son statut élevé pour convaincre des employés de lui transférer des fonds. *« En France, le ton d'autorité d'un message affiche un taux de succès deux fois supérieur que d'autres registres, quel que soit le profil de la personne visée »*, a pu vérifier Thomas Kerjean.

Changer régulièrement de mot de passe, bien vérifier l'expéditeur avant de cliquer… Outre ces pratiques élémentaires, les experts conseillent aux personnes haut placées de réduire le plus possible leur empreinte numérique – en limitant leurs infos publiques sur les réseaux sociaux – mais aussi en révisant leurs droits d'accès, comme le pointe Jonathan Gosselin : *« Ce n'est pas parce que vous êtes le PDG que vous avez besoin d'avoir accès à tout le système informatique de l'entreprise depuis votre session ! »* ■

« Les antivirus sont tous défaillants » : les chercheurs contre-attaquent face aux malwares

Grâce à leur collection de 35 millions de malwares, les chercheurs du Loria, à Nancy, ont mis au point un outil capable de détecter n'importe quel « variant » de programme malveillant. Prometteur, leur projet va se muscler grâce à un budget de cinq millions d'euros.

REPORTAGE

« Quand on a commencé, en 2010, l'université n'y croyait absolument pas. Alors on nous a mis au sous-sol… » raille malicieusement le chercheur Jean-Yves Marion en faisant visiter sa « cyberforteresse » dans les dédales de l'université de Lorraine. Ce lieu fermé par un sas sécurisé, dont les fenêtres *« ont été conçues pour résister à sept coups de hache »* et qui abrite *« des morceaux de code pouvant être considérés comme des armes de guerre »*, c'est le Laboratoire de haute sécurité (LHS) du Loria (Laboratoire lorrain de recherche en informatique et ses applications), situé à Nancy.

« Il s'agit d'un des plus importants lieux de recherche dédiés à la cybersécurité en France – avec Rennes et Paris – et le premier labo de haute sécurité ouvert sur le territoire », précise le professeur. Il y a près de quinze ans, aux prémices du LHS, *« on parlait encore de virus et de vers »* et *« d'ados boutonneux à capuche qui préparaient des cyberattaques gentillettes depuis leur garage »*, se souvient Jean-Yves Marion, presque nostalgique.

La technique du pot de miel

Ce temps est bien révolu ! Ce que l'on appelle désormais des programmes malveillants, malwares ou ransomwares, sont téléguidés par des organisations cybercriminelles qui sont parfois proches d'Etat, comme la Russie ou la Chine. *« Ce sont quasiment des entreprises, qui passent des annonces sur le web, revendent des données sur le marché noir, organisent des concours de recherche de vulnérabilités… »* décrit le chercheur.

Face à cette menace mouvante et grandissante – *« plus les appareils sont connectés, plus les possibilités d'attaques augmentent ! »* –, une foultitude de solutions de cybersécurité a été lancée sur le marché, que ce soit par les grands noms du secteur, comme Trellix, Microsoft ou Symantec, ou par des start-up mettant à profit les dernières avancées de l'intelligence artificielle.

Un écosystème très dynamique, mais où le monde académique a son rôle à jouer. *« Les entreprises ont un calendrier court terme, au mieux moyen terme quand elles en ont les moyens. Tandis que la recherche peut se consacrer à du long terme »*, rappelle Jean-Yves Marion, en donnant l'exemple du phénomène mondial ChatGPT, issu de plusieurs décennies de recherche en laboratoire.

Alors, quel serait le « ChatGPT » du Loria ? Dans sa « cyberforteresse », le laboratoire a confiné 35 millions de programmes malveillants, collectés sur Internet. *« On utilise la technique du pot de miel, qui consiste à se faire passer pour un ordinateur vulnérable, pour les attirer »*, glisse le chercheur. Cette base de virus est soigneusement disséquée par la petite équipe de chercheurs, pour améliorer leurs connaissances sur l'état de la cybermenace, mais pas seulement. Ils sont aussi parvenus à concevoir un système capable d'identifier n'importe lequel de ces virus, ainsi que n'importe quelle *« souche »* issue de ces virus, même sous forme de *« variants »*, légèrement modifiés.

Une start-up, Cyber-Detect, a été lancée en 2017 pour commercialiser l'outil. *« Tous les antivirus que l'on a aujourd'hui sur nos ordinateurs sont défaillants, car ils sont conçus pour identifier les virus déjà connus. Dès qu'un programme sort de ce périmètre, par exemple s'il a été construit spécifiquement pour vous attaquer, ils ne le repèrent plus »*, pointe Régis Lhoste, à la tête de la start-up, qui emploie une dizaine de personnes. *« De notre côté, on ne s'intéresse pas à la forme complète d'un virus mais uniquement aux petits morceaux de code, aux variants, qui correspondent à des morceaux malveillants »*, explique l'entrepreneur, dont l'outil a déjà été adopté par une quinzaine de clients, dont la moitié dans le secteur public.

Une discipline devenue « plus attirante »

Si la cyber souffrait encore d'un problème de popularité auprès des chercheurs il y a quelques années, car considérée *« trop technique »*, cette voie universitaire *« est devenue plus attirante »* et *« d'énormes moyens ont été mis sur la table au fur et à mesure »*, a pu constater Jean-Yves Marion.

A l'image du quantique qui a bénéficié d'un plan de financement de 1,8 milliard d'euros en 2021, la filière cybersécurité a été dotée l'an dernier d'une enveloppe de 65 millions d'euros dans le cadre du programme national PEPR Cybersécurité, piloté par le CNRS, Inria et le CEA. Sur cette somme, le projet Defmal de l'université de Lorraine – consacré aux programmes malveillants – a décroché un budget inédit de 5 millions d'euros, échelonné sur six ans.

De quoi mobiliser une douzaine de chercheurs, et surtout développer une approche pluridisciplinaire dans le domaine. *« Une plateforme d'échange doit être mise en place pour partager nos données avec les services de l'Etat et des partenaires industriels »*, précise l'expert. In fine, le but est de multiplier les ponts entre public et privé pour couvrir les multiples facettes de l'écosystème cybercriminel, par exemple, explique-t-il, en entretenant des relations avec les forces de l'ordre, des juristes ou des sociologues. — ***Le. M.***

Il a dit

DR

« Les entreprises ont un calendrier court terme, au mieux moyen terme quand elles en ont les moyens. Tandis que la recherche peut se consacrer à du long terme. »

JEAN-YVES MARION
Professeur à l'université de Lorraine

Cet outil français promet de détecter tous les malwares, variantes incluses

PAR THOMAS POVÉDA
LE 27/11/2023

1 COM

Développé dans un laboratoire de haute sécurité français, un nouvel outil est plus efficace que les anti-virus actuels en repérant également les variantes des malwares. Il est déjà utilisé par plusieurs entreprises.

Crédits : 123RF

Les **malwares**, c'est un peu comme les **spams** dans notre boîte mail. On aura beau lutter contre, il y en aura toujours. Ça n'empêche pas de développer des outils pour s'en prémunir, **anti-virus** en tête, ou d'ajouter des fonctions à un système existant comme sur le Play Store. Le problème, c'est que "tous les antivirus que l'on a aujourd'hui sur nos ordinateurs sont défaillants, car ils sont conçus pour identifier les virus déjà connus. Dès qu'un programme sort de ce périmètre, par exemple s'il a été construit spécifiquement pour vous attaquer, ils ne le repèrent plus", constate Régis Lhoste, dirigeant de la start-up **Cyber-Dectect**.

Son entreprise a été créée pour vendre un produit bien spécifique : un anti-virus capable de détecter les malwares bien sûr, mais surtout leurs **variantes**. Moins faciles à repérer, elles peuvent devenir un vrai danger pour nos

informations personnelles. C'est dans le **Laboratoire de haute sécurité** (LHS) du **Loria** (Laboratoire lorrain de recherche en informatique et ses applications) à Nancy que l'outil a vu le jour. Il a été conçu grâce à l'**analyse de 35 millions de malwares**.

CE DÉTECTEUR DE MALWARE FONCTIONNE MÊME POUR REPÉRER LEURS VARIANTES

Afin de récolter un maximum de programmes malveillants, Jean-Yves Marion, chercheur et professeur à l'université de Lorraine, précise que lui et ses équipes utilisent "la technique du pot de miel, qui consiste à se faire passer pour un ordinateur vulnérable, pour les attirer". Le nouveau détecteur, lui, "ne s'intéresse pas à la forme complète d'un virus mais uniquement aux petits morceaux de code, aux variants, qui correspondent à des morceaux malveillants", explique Régis Lhoste.

Lire aussi – Google : une fausse pub pour ce logiciel connu cachait un malware

C'est comme ça que cet anti-virus d'un nouveau genre parvient à obtenir de meilleurs résultats que les systèmes actuels. Il a dépassé les phases de test puisqu'**il est utilisé par une quinzaine d'entreprises** déjà, dont la moitié dans le secteur public. Jean-Yves Marion indique qu'une "plateforme d'échange doit être mise en place pour partager [ses] données avec les services de l'État et des partenaires industriels" dans un avenir proche.

Source : Les Échos

Des chercheurs français ont mis au point un outil permettant de détecter n'importe quel malware

Par Stéphane Ficca
Spécialiste hardware & gaming
Publié le 27 novembre 2023 à 11h02

14

Le Loria de Nancy abrite pas moins de 35 millions de malwares © KS JAY / Shutterstock

À Nancy, au sein de l'Université de Lorraine, on dispose d'un laboratoire dédié à la culture de virus... informatiques.

Ce lieu de recherche intégralement dédié à la cybersécurité se charge de stocker les programmes malveillants qui sévissent sur le Web. Une équipe, composée d'une douzaine de chercheurs, s'évertue alors à analyser ces derniers, afin de comprendre leur fonctionnement, mais aussi d'identifier plus rapidement et plus efficacement les éventuels variants à venir.

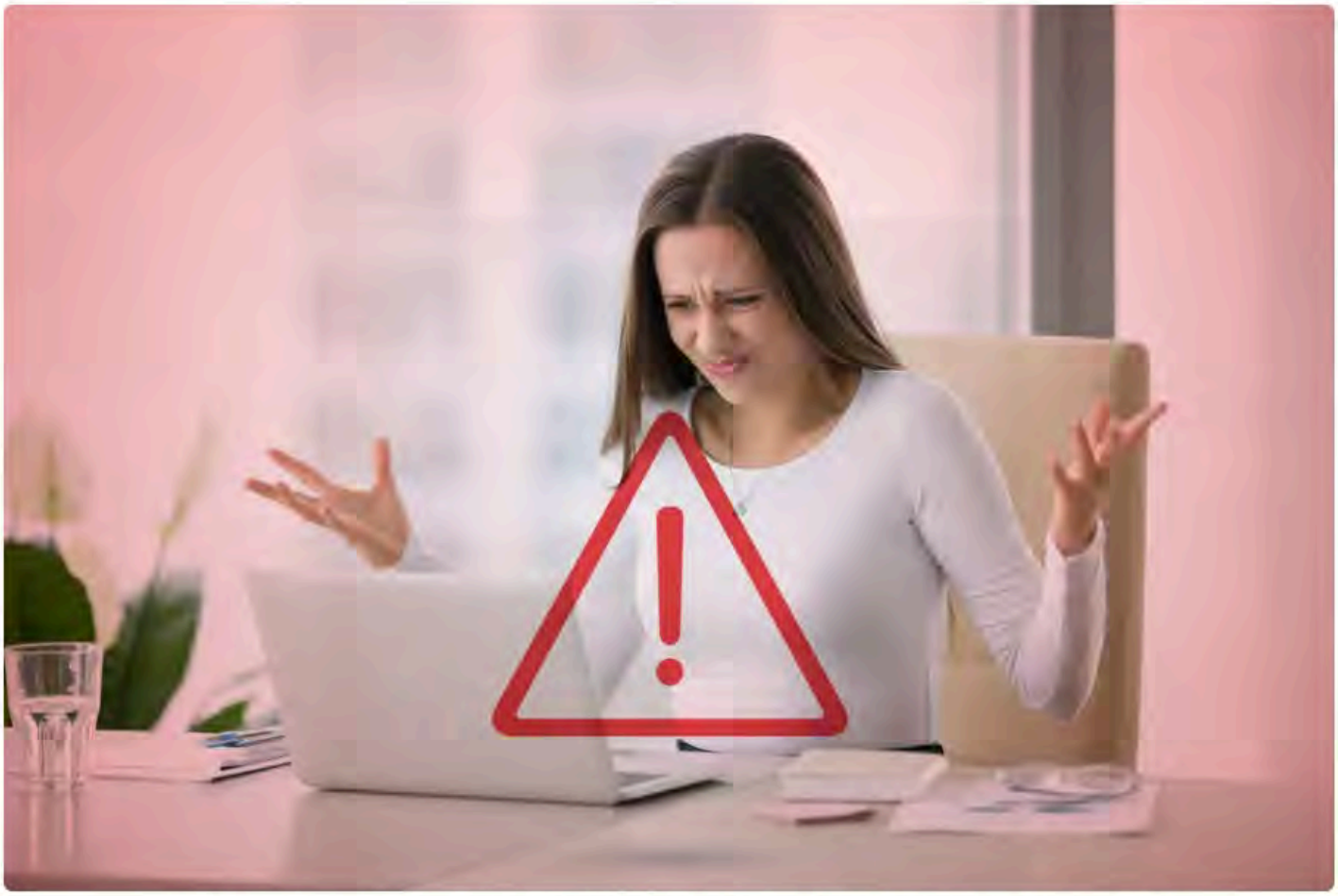
Une culture de virus informatiques à Nancy

Le Laboratoire de haute sécurité (LHS) du Loria (pour Laboratoire Lorrain de Recherche en Informatique et ses Applications), situé à Nancy, constitue l'un des plus importants lieux de recherche dédiés à la cybersécurité en France. Depuis 2010, une équipe a isolé pas moins de 35 millions de programmes malveillants, ayant sévi sur le Web.

De quoi permettre à l'équipe de chercheurs de concevoir un système en mesure d'identifier n'importe lequel de ces virus, mais aussi (et surtout) n'importe quelle « souche » issue de ces mêmes virus. Les fameux « variants », dont la structure peut être légèrement modifiée afin de se rendre indétectable auprès des antivirus classiques.

Des moyens pour lutter contre la cybercriminalité

Selon Régis Lhoste, à la tête de l'outil Cyber-Detect : « *Tous les antivirus que l'on a aujourd'hui sur nos ordinateurs sont défaillants, car ils sont conçus pour identifier les virus déjà connus* ». Soucieux de poursuivre la recherche sur le long terme, le projet de l'université de Lorraine a récemment décroché un budget de 5 millions d'euros, qui s'étalera sur un total de six années.



L'outil mis au point promet de détecter efficacement tous les virus, y compris les variants © Shutterstock x Clubic.com

Rappelons que la filière cybersécurité a bénéficié en 2022 d'une enveloppe totale de 65 millions d'euros, dans le cadre du programme national PEPR Cybersécurité, piloté conjointement par le CNRS, Inria et le CEA.

Depuis quelques années déjà, les malwares et autres ransomwares sont parfois employés par des organisations cybercriminelles rattachées à certains États. Récemment, c'est un malware russe, mis au point par Gamaredon, qui s'est échappé du champ de bataille ukrainien pour se répandre dans le monde entier.

Source : Les Échos

THE CONVERSATION

L'expertise universitaire, l'exigence journalistique

Rançongiciel, une plongée dans le monde de la cybercriminalité

Publié: 28 novembre 2023, 18:18 CET

Jean-Yves Marion

Professeur d'informatique et directeur du Loria, CNRS, Inria, Université de Lorraine

Les cybercriminels agissent en bandes très organisées, et surtout très modulables.
Dan Asaki, Unsplash, CC BY

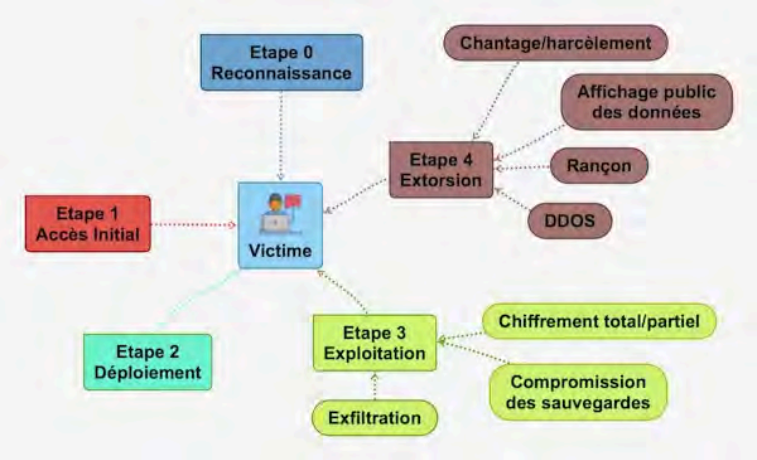
Europol vient d'annoncer le démantèlement d'un groupe de rançongiciels en Ukraine. Dans leur forme la plus basique, ces cyberattaques bloquent les systèmes informatiques et exfiltrent les données de la victime, promettant de les restituer contre rançon.

Ainsi, en août 2022, une cyberattaque attribuée au rançongiciel LockBit a paralysé le centre hospitalier sud-francilien en exfiltrant 11 Gigaoctets de données de patients et d'employés. L'hôpital a dû fonctionner en « mode dégradé » pendant plusieurs mois, avec les dossiers médicaux inaccessibles et des appareils de soin inutilisables. En juillet 2023, c'est le port de Nagoya, l'un des plus importants du Japon, qui a été obligé de s'arrêter pendant deux jours à cause d'un rançongiciel.

De l'exfiltration des données à leur revente sur des marchés illicites et aux menaces de rendre publiques les informations volées, jusqu'au fonctionnement très altéré des organisations victimes des attaques, la réalité du terrain est brutale, purement criminelle et vise sans discernement les particuliers, les hôpitaux, les écoles et toutes les organisations et entreprises vulnérables.

Les organisations cybercriminelles sont aujourd'hui bien organisées et leurs façons de procéder évoluent pour plus d'efficacité : l'économie et l'écosystème souterrains à l'origine de ces cyberattaques sont très modulables et se sont même « uberisé », ce qui les rend résilients aux démantèlements et actions en justice.

C'est une plongée dans ce monde de la cyberextorsion que nous vous proposons ici.



Le mode opératoire des cybercriminels utilisant des rançongiciels est en constante évolution. Jean-Yves Marion, Fourni par l'auteur

L'extorsion cyber en constante évolution

Quand on parle de rançongiciel, on pense à un programme malveillant qui va chiffrer (crypter) les données d'un ordinateur et demander une rançon pour rendre ces données. Par exemple, le rançongiciel Wannacry, qualifié de « sans précédent » par Europol, avait compromis environ 5 millions d'appareils en 2017, après avoir exploité une vulnérabilité pour se propager automatiquement.

Aujourd'hui, cette notion a évolué : les rançongiciels sont opérés par des humains qui explorent l'ensemble du système informatique compromis. Les attaques peuvent se déployer sur plusieurs mois, tenir compte des systèmes attaqués et « avancer » à l'intérieur du réseau informatique. Les données sensibles et d'autres informations peuvent être exfiltrées et stockées sur des serveurs contrôlés par les cybercriminels.

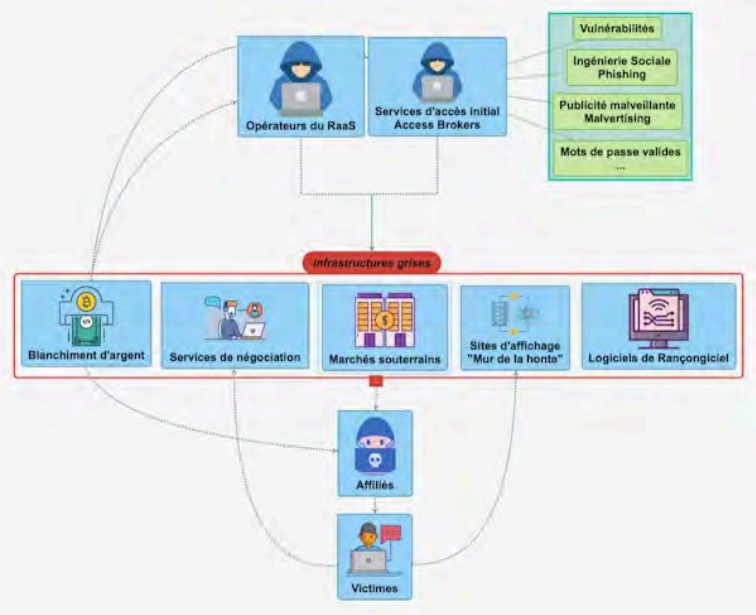
Le groupe cybercriminel Royal a par exemple publié en mai 2023 des informations de la ville de Dallas, y compris des informations confidentielles sur la police et sur des affaires pénales.

De fait, des données partiellement rendues publiques permettent déjà de faire pression sur la victime, et l'exfiltration suffit à demander une rançon. Les données peuvent aussi être revendues à un tiers.

Les attaquants peuvent aussi procéder au chiffrement des données sur les serveurs de leur propriétaire. Ce mécanisme est dit de « double extorsion » : exfiltration et chiffrement.

Enfin, le harcèlement sur la victime peut aller jusqu'à une attaque par « déni de service (DDOS) », qui rendent les services web de la victime inaccessibles. On parle alors de « triple extorsion ».

Le gain financier est le principal moteur des campagnes de rançongiciels, et en fait il faudrait plutôt parler aujourd'hui d'« extortion-wares », qui mobilisent toute une économie souterraine.



L'écosystème des rançongiciels s'est ubérisé, avec des services disponibles, dont des fournisseurs de logiciels d'attaques ainsi « facilitées », qui permettent à de la main-d'œuvre relativement peu qualifiée en informatique, les « affiliés », de sous-traiter les attaques des commanditaires. Jean-Yves Marion, Fourni par l'auteur

Un écosystème souterrain

Les organisations souterraines responsables de ces cyberextorsions ont gagné en maturité. Le modèle *Ransomware as a Service* (RaaS) s'est imposé comme à la fois la structure principale d'organisation et comme modèle économique.

Le RaaS est un ensemble d'acteurs qui monnayent des infrastructures, des services et des savoir-faire à leurs « affiliés » : c'est ainsi que ceux-ci disposent des moyens technologiques et humains pour réaliser concrètement les cyberattaques par rançongiciel.

Nos connaissances sur ce système cybercriminel proviennent d'interviews et des fuites d'information. Les « ContiLeaks » en particulier furent le fait de disputes entre les acteurs. Pour certaines des fuites documentées sur ContiLeaks, les fuites émanent plus précisément de désaccords subséquents à l'invasion de l'Ukraine.

Le monde de la cybercriminalité s'est ubérisé

Dans ce modèle économique du *Ransomware as a Service*, le recrutement d'« affiliés » est essentiel : ce sont eux qui réalisent les cyberattaques grâce à un certain nombre d'outils et de panneaux de contrôle fournis par l'organisation cybercriminelle à l'initiative de l'attaque. Ces organisations sont assez disparates : il existe à la fois des groupes d'acteurs et des acteurs isolés. Dans tous les cas, ces organisations sont fragmentées – ce qui, on le verra par la suite, leur permet de se reconfigurer, en cas de démantèlement notamment.

Ce soutien « technique » permet de recruter des exécutants dont le niveau technique n'est pas forcément élevé, car ils bénéficient d'outils relativement faciles à mettre en œuvre. Ironiquement d'ailleurs, un groupe se nomme « Read the Manual ».

Autrement dit, le monde de la cybercriminalité s'est, lui aussi, ubérisé. Les profits sont partagés entre les commanditaires et les affiliés (environ 70 % du paiement de la victime est reversé à l'affilié).

Ventes d'« accès » : comment pénétrer chez la victime

Un des services les plus importants est celui des fournisseurs d'accès (*Internet Access Brokers*) qui vendent notamment des mots de passe et des cookies provenant de campagnes précédentes, soit de phishing qui cherche à manipuler une victime pour obtenir un mot de passe, soit d'infostealers qui sont des logiciels spécialisés dans le vol d'information, ou enfin à la suite d'une exfiltration de données par une précédente attaque d'un rançongiciel.

En 2021, l'attaque de Colonial Pipeline a forcé l'arrêt de toutes les opérations d'un pipeline qui transporte environ 400 millions de litres d'essence par jour, ce qui a amené le ministère américain de la Justice à élever les attaques par rançongiciel au niveau du terrorisme. En effet, selon l'audition de la commission de la sécurité intérieure de la Chambre des représentants des États-Unis, l'accès initial au réseau s'est fait à partir d'un mot de passe réutilisé.

Ce type de « vente d'accès » se fait dans des marchés souterrains et des forums, comme RaidForums.

Blanchiment des rançons : démêler les flux de cryptomonnaies

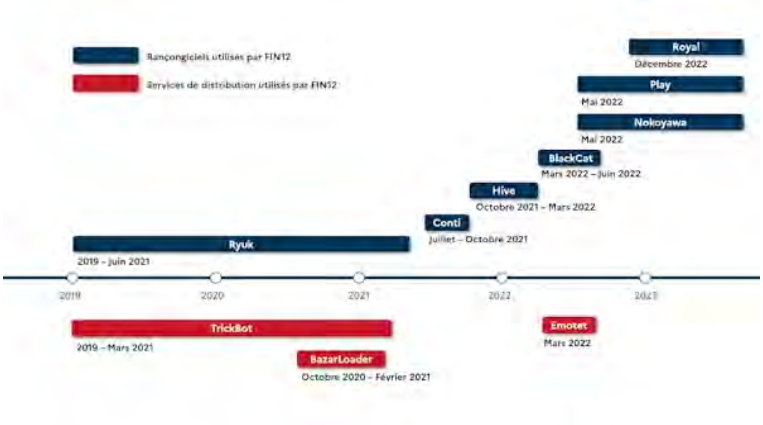
Pour faire fonctionner l'écosystème, un autre service important est celui du blanchiment des rançons (en cryptomonnaies, souvent en Bitcoin). Pour cela, des outils informatiques sont utilisés : des « mixeurs » pour rendre les transactions financières intraçables, et des « échangeurs » pour échanger les cryptoactifs.

Afin de démanteler les services de blanchiment et d'arrêter les cybercriminels, les forces de l'ordre essaient de surveiller ces échanges de cryptomonnaies. C'est ainsi qu'une action internationale a permis de démanteler la plate-forme d'échange de cryptoactifs Bitzlato.

Une des limitations à ces actions internationales est que les organisations RaaS s'appuient le plus souvent sur des infrastructures hébergées dans des pays qui ne collaborent pas, ou peu, avec les forces de l'ordre européennes et américaines.

Une économie souterraine résiliente

Le modèle RaaS permet de réduire les risques pour les cybercriminels, comme l'observe le rapport 2022 de l'agence européenne pour la cybersécurité (Enisa). En effet, l'arrestation d'un seul cybercriminel n'est pas suffisante pour stopper les méfaits d'un rançongiciel : les groupes comme Conti se fragmentent et se recomposent en différents autres groupes.



Synthèse chronologique des activités connues du groupe cybercriminel FIN12, illustrant le fait que ce type de gang se désagrège et se reconstitue, ce qui démontre leur adaptabilité et leur résilience. Agence nationale de la sécurité des systèmes d'information (ANSSI) -- septembre 2023. Licence ouverte (Étalab -- v2.0)

Aussi efficaces soient-elles, les actions de justice internationale n'ont parfois qu'un effet limité. Par exemple, le « world's most dangerous malware », appelé Emotet, a été démantelé en janvier 2021… pour reprendre du service un an plus tard.

Ce constat peut sembler pessimiste mais ne doit pas masquer que les actions de justice secouent de fait le monde cybercriminel, comme l'ont montré l'opération offensive contre le rançongiciel Hive ou le démantèlement de Ragnar Locker (suite notamment à une arrestation à Paris).

D'un point de vue économique, le modèle RaaS optimise le retour sur investissement (ROI). L'économie souterraine RaaS prospère. Elle est basée sur des marchés illicites dans le dark web. En moyenne, un ransomware est vendu pour 56 dollars américains selon l'étude menée entre novembre 2022 et février 2023.

Les marchés souterrains sont très volatils et fragmentés. Cette fragmentation permet aux cybercriminels de poursuivre leurs activités commerciales, même après une saisie par les forces de l'ordre comme celles de DarkMarket et de HydraMarket.

Cyberattaques et conflits armés : la naissance des « cyber-mercenaires » ?

Des organisations clandestines prennent forme, disparaissent et renaissent, parfois instrumentalisées par les États, comme l'a montré le conflit ukrainien. Rien d'étonnant à cela, puisque les moyens d'une cyberattaque sont quasiment les mêmes, que l'objectif soit financier, d'espionnage ou de destruction.

Déjà en 2017, et malgré sa ressemblance avec le rançongiciel WannaCry déjà bien connu, les actions du malware NoPetya ont été destructrices, causant environ 10 milliards de dollars de dommages totaux, et préfigurant les cyberattaques menées pendant le conflit ukrainien à l'aide d'armes avec les « wipers », qui effacent les informations de systèmes compromis.

Les tensions géopolitiques pourraient encourager les acteurs à l'origine des rançongiciels à poursuivre les cyberconflits en cours : en adaptant légèrement leurs comportements, ils peuvent facilement devenir des sources d'espionnage, comme des « cyber-mercenaires ».

Le PEPR Cybersécurité et le projet ANR-22-PECY-0007 sont opérés par l'Agence nationale de la recherche (ANR), qui finance en France la recherche sur projets. Elle a pour mission de soutenir et de promouvoir le développement de recherches fondamentales et finalisées dans toutes les disciplines, et de renforcer le dialogue entre science et société. Pour en savoir plus, consultez le site de l'ANR.

franceinfo junior du 29 novembre. À quoi ressembleront les robots du futur ?

écouter (7min)

franceinfo junior
Estelle Faure et Marie Bernardeau
Du lundi au jeudi à 14h21 et 16h23

s'abonner

L'exposition internationale de robots, iRex, se tient à Tokyo jusqu'au 2 décembre. Jean-Baptiste Mouret, ingénieur et chercheur en robotique et intelligence artificielle à l'INRIA, répond aux questions des enfants de franceinfo junior.

Estelle Faure - Benjamin Fontaine
Radio France

Publié le 29/11/2023 20:09

Temps de lecture : 7 min

Des visiteurs de l'IRex, à Tokyo observe un robot. (NICOLAS DATICHE / LIGHTROCKET)

Plusieurs centaines de robots sont réunies jusqu'au 2 décembre à Tokyo, à l'occasion de l'IRex et les collégiens, du collège Jean-Mariotti à Nouméa en Nouvelle-Calédonie s'interrogent sur l'avenir des robots. Pour leur répondre, l'émission tend son micro à Jean-Baptiste Mouret, ingénieur et chercheur en robotique et intelligence artificielle à l'INRIA.

La première question revient à Marin : *"Quand avons-nous commencé à exploiter les robots ?"* À son tour, Édouard veut savoir si *"nous pouvons vivre sans robots"*.

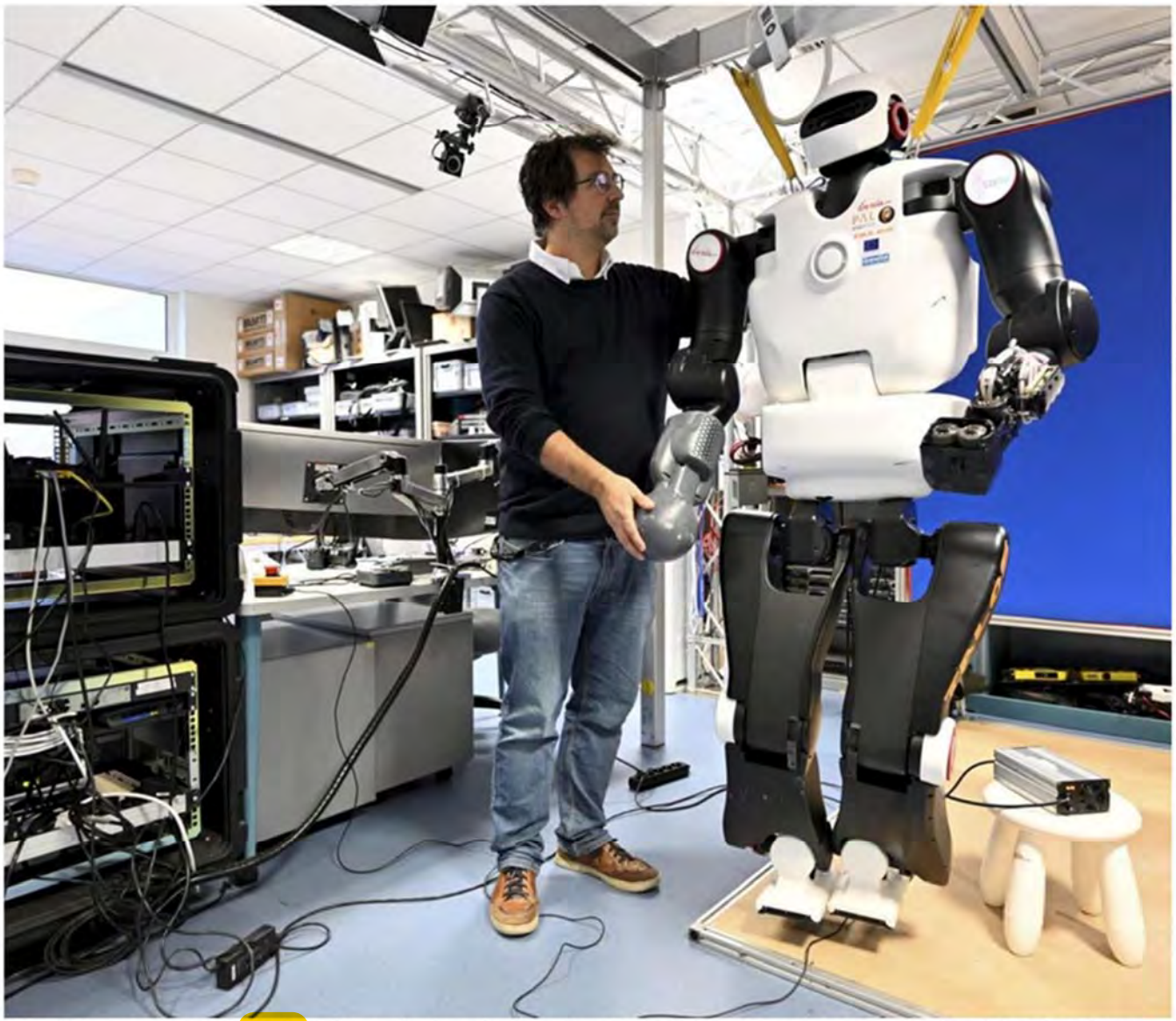
Adrien veut connaître le prix et Marin se demandent si *"les robots vont remplacer l'être humain dans le travail"*. Édouard s'interroge ensuite sur le remplacement des soldats par des robots, alors qu'Adrien demande si *"les robots peuvent effectuer des travaux de maintenance sous l'eau ?"* La dernière question revient à Naïm : *"Est-ce que les robots peuvent avoir une conscience ?"*

Sur cette page, réécoutez en entier cette émission franceinfo junior.

L’Est républicain, 4 décembre 2023 (édition Nancy) (1/3)

Nancy

Un laboratoire qui humanise les robots



Dans les laboratoires du Loria (Laboratoire lorrain de recherche en informatique et ses applications), les chercheurs font avancer les robots et la science. Photo Alexandre Marchi *Pages 2-3*

Nancy

L'Inria Nancy, un labo pilote pour donner des réflexes aux robots

Dans les laboratoires du Loria (Laboratoire lorrain de recherche en informatique et ses applications) les chercheurs font avancer les robots et la science. Le directeur de recherche Jean-Baptiste Mouret et ses équipes parviennent déjà à doter des humanoïdes de réflexes et d'anticipation via des algorithmes de « machine learning ». Un gain d'autonomie pour des robots téléopérés, au service des humains.

Entre ses deux écrans géants d'ordinateur ce jeudi 30 novembre, Jean-Baptiste Mouret commence par nous rappeler les bases : « Les robots sont des outils. Ils font des choses soit trop dangereuses soit trop difficiles pour les humains. » Balayées les craintes d'apocalypses technologiques, ici les chercheurs sont au service des humains et travaillent d'abord sur la partie software.

« Notre spécialité, c'est la partie algorithmique », explique Serena Ivaldi, directrice de recherche Inria au Loria (CNRS, Inria, Université de Lorraine). La chercheuse a elle-même mis au point des exosquelettes qui ont servi aux soignants pendant la pandémie.

« Un humanoïde coûte le prix d'un appartement parisien ! »

Le Loria possède des imprimantes 3D, compte deux humanoïdes, des drones et plusieurs exosquelettes. Mais concevoir des robots, c'est d'abord concevoir les algorithmes qui vont les contrôler. « Les structures des robots doivent être contrôlées à chaque milliseconde. Dans ce laps de temps les calculs doivent être terminés et la commande envoyée », précise Jean-Baptiste Mouret

Heureusement pour le labo un même algorithme peut être utilisé sur plusieurs machines. Le chercheur le reconnaît : « Un humanoïde coûte le prix d'un appartement parisien ! »

Réflexes et anticipation

Au Loria, les chercheurs planchent sur des algorithmes qui pourront être appliqués à des robots téléopérés dans l'espace ou des centrales nucléaires. » Une extension de l'humain à distance »

Tola est un humanoïde téléopéré mesurant 1m80. Pour bouger, un humain doit se tenir à quelques mètres de lui en combinaison spéciale. Le robot est capable d'imiter ses mouvements tout en effectuant des tâches comme porter des charges lourdes.

Mais une innovation du labo a vu le jour cette année. Lors des dernières expériences, Tola a été capable de se rattraper : « On lui coupe le courant dans le genou et il sait trouver où s'appuyer avec sa main pour ne pas tomber. »

Même opéré par un humain, le robot doit avoir un peu d'autonomie. « Si le genou ne répond plus, l'opérateur ne va pas décider comment bouger à sa place. Il faut qu'il ait des réflexes ! » résume le chercheur.

Chose moins aisée, les chercheurs aimeraient pouvoir téléopérer des robots sur la Lune ou dans l'ISS. Mais un décalage de 1 seconde entre le mouvement du robot et le retour visuel de l'opérateur rend l'action impossible telle quelle : « C'est extrêmement perturbant, on n'arrive à rien faire ! »

Pour y remédier, l'humanoïde du Loria utilise l'IA pour prédire les mouvements de l'humain : « Si le robot fait tout 1 seconde avant de recevoir l'information, l'opérateur aura l'impression de le piloter en tant réel. »

Le robot doit donc deviner ce que va faire l'opérateur : « C'est du machine learning : le robot va faire des prédictions en continu, en s'appuyant sur son environnement et les gestes humains des 3 dernières secondes. » Au Loria, il est déjà capable d'anticiper des gestes simples.

Là encore, la solution se cache côté logiciel : « Pour nous, le gros du travail, c'est l'algorithme qui fera de bonnes prédictions. »

• **Thomas Baudoin**

1

Une seconde, c'est le temps entre le mouvement d'un robot dans l'ISS et le retour visuel d'un opérateur humain sur terre.

Jean-Baptiste Mouret, directeur de recherche au Loria (CNRS, Inria, Université de Lorraine) et le robot humanoïde Talos. Photo Alexandre Marchi

Nancy a sa place sur la carte du développement des humanoïdes

Dans un an, Nancy vibrera pendant 8 jours au rythme des robots. La ville accueillera la Conférence internationale des robots humanoïdes (IEEE) du 22 au 24 novembre 2024 au Centre Prouvé et verra des exposants et des compétitions entre robots du monde entier.

La conférence sera suivie du 25 au 29 novembre 2024 par le hackathon de euROBIN, le réseau européen de recherche en robotique. Ce concours d'innovation aura également lieu à Prouvé. Il verra s'affronter des humanoïdes et des robots de différentes formes dans des épreuves d'adresse et de précision.

La robotique, à quoi ça sert ?

Ce qu'il se trame dans les labos de l'Inria n'a rien d'effrayant : « On ne fait pas des gros bras industriels ! On essaie plutôt de faire des robots un peu plus intelligents et autonomes, de les doter robots de capacités d'adaptation. »

Francis Colas est chercheur à l'Inria et fait partie de l'équipe du LARSEN, spécialisée dans la robotique. Une discipline « assez vaste, à l'intersection de la mécanique et de l'électronique », selon le chercheur, qui attire facilement les profils et les financements publics français et européens.

En France, seule une poignée de labos se penchent sur la recherche en robotique comme à Montpellier, Paris (l'ISIR de Paris Sorbonne) ou le LAAS à Toulouse : « On n'est pas les plus gros en France, mais on fait partie des rares à être actifs dans la robotique humanoïde »

Francis Colas et son équipe travaillent jusqu'à quatre projets en simultané. Pour autant, ses travaux ne sont pas destinés à atterrir sur les chaînes de fabrique des usines : « Je ne pense pas que ce qu'on développe va être appliqué demain dans l'industrie. Notre travail à nous, chercheurs, c'est d'établir une compréhension. » Aux ingénieurs ensuite, de développer des solutions pour les problèmes spécifiques des industriels.

L'IA jamais bien loin

La robotique permet aussi d'appliquer concrètement ce que permet l'intelligence artificielle. Pour le chercheur : « Notre travail au Larsen est une sous-discipline de l'IA. »

Ainsi, l'IA connaît un regain d'intérêt récent dans la recherche : « Nous avons toujours fait de l'IA mais après les années 80-90 il y a eu une période de disette. Depuis 5-10 ans la quantité de publications scientifiques a explosé et on utilise à nouveau l'IA et des réseaux de neurones profonds. »

Ce tournant se répercute dans la robotique et dans l'apprentissage des robots. Ceux de Jean Baptiste Mouret, sont désormais capables de s'adapter à des obstacles (un bras cassé, un déséquilibre) sans avoir besoin de les comprendre totalement. C'est grâce notamment l'apprentissage par renforcement ou méthode essai-erreur rendu possible par ces réseaux de neurones profonds.

Au Loria, la recherche permet de mettre au point des robots plus intelligents. Photo Alexandre Marchi

Inria, Loria, Larsen... Dans la robotique, qui fait quoi ?

L'Inria tout d'abord, est un institut national qui compte neuf centres de recherches en France, dont un se situe à Villers-lès-Nancy sur le campus Sciences (ex-Nancy 1) depuis 1986.

Dans ce centre, le Loria est le laboratoire dédié à la recherche informatique appliquée, en association avec le CNRS et l'Université de Lorraine. Il est né en 1997 et emploie près de 450 personnes. Il en existe seulement quatre de ce type en France.

Au sein de ce labo se trouvent 30 équipes dont le Larsen de Francis Colas qui compte 25 à 30 personnes spécialisées dans la robotique, qui se trouve être une sous-discipline de l'informatique et de l'IA.

Le logo de l'Inria Nancy. Photo Alexandre Marchi.

La start-up nancéienne Alerion développe un robot cueilleur de mirabelles

Pour pallier le manque de main-d'œuvre, Alerion développe un bras robot capable de cueillir des mirabelles. Photo Alexandre Marchi

Des robots dans les mirabelliers dès cet été ? La start-up nancéienne Alerion y travaille et y croit sérieusement. Baptisé Syracus, le projet doit voir naître une solution robotique d'aide à la récolte de mirabelles. Il occupe l'entreprise et sa présidente, Anne-Sophie Didelot, depuis début 2023. Le client, la coopérative Végafruits, fait face à une grosse problématique de main-d'œuvre.

« C'est un secteur d'activité complètement nouveau pour Alerion », selon la dirigeante. Et pour cause, la récolte des fruits est un secteur encore peu robotisé.

Mission exigeante

Louis Viard, ingénieur chef de projet sur Syracus résume les contraintes : « Le système doit être capable de cueillir les fruits assez délicatement. Il faut aussi développer l'intelligence nécessaire pour identifier les bons fruits et pas des feuilles par exemple. »

Le travail de ce dernier consiste à décomposer les gestes de la cueillette pour pouvoir écrire les algorithmes qui contrôleront le robot : « Sur le terrain, on observe les personnes pour pouvoir caractériser leur travail et le traduire ensuite en robotique. »

Alerion planche sur un robot autonome : « On part d'un robot téléopéré et à mesure qu'on rajoute des capteurs on arrive à une autonomie complète. »

Un premier prototype doit arriver courant 2024.

● T.B.

« Sur le terrain, on observe les personnes pour pouvoir caractériser leur travail et le traduire ensuite en robotique. »
Anne-Sophie Didelot, présidente d'Alerion

3 QUESTIONS À • SMART TECH • mar. 19/12/23

Cybersécurité : mieux analyser les malwares

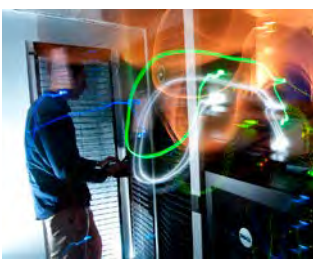
Parmi les menaces qui pèsent sur les systèmes informatiques, les malwares sont sûrement les plus redoutables. Ces logiciels malveillants peuvent, en effet, rapidement compromettre la sécurité des données qui s'y trouvent. Afin de les détecter le plus tôt possible, Cyber-detect a mis au point une solution innovante. Cette dernière est capable de modéliser et de caractériser le comportement d'un fichier suspect pour l'éliminer. Explications avec Régis Lhoste, son président.

Partager

NANCY **CYBERSÉCURITÉ**

Le projet DefMal mobilise 5 millions d'euros contre les logiciels malveillants

Lancé dans le cadre du plan France relance et porté par l'Université de Lorraine, le programme de recherche en cybersécurité DefMal va mobiliser 5 millions d'euros sur six ans. Le projet porte sur la lutte contre les logiciels malveillants, touchant les objets connectés, les systèmes embarqués, les véhicules autonomes, les systèmes industriels ou encore l'infrastructure informatique. L'enjeu est de parvenir à développer de nouvelles méthodes d'analyse et de défense face aux malwares, d'appréhender les aspects économiques, juridiques, criminels et sociologiques qui sous-tendent cet écosystème. « La démultiplication des menaces rend indispensable une mobilisation universitaire interdisciplinaire, en lien constant avec le monde de l'entreprise et les pouvoirs publics », analyse Jean-Yves Marion, professeur à l'Université de Lorraine, chercheur au Loria et responsable du programme DefMal.



© INRIA - PHOTO KAKSONEN