Assurons un monde plus ouvert

Recherche et prospective

Juillet 2024

Enjeux assurantiels du risque cyber d'ici à 2030 : menace, prévention et protection

Grâce à son dispositif de veille prospective, CNP Assurances réalise un suivi régulier des risques émergents ou en développement. Chaque année, ils sont classés suivant leur impact potentiel et leur survenance. En 2023, nos experts ont positionné le risque cyber en tête des dix principaux risques[1].

Le développement du numérique transforme notre société de manière profonde. Il constitue un des terreaux du cyber monde dans nos économies. Ce monde est en constante évolution entre opportunités et menaces. Il est source d'inquiétude pour les acteurs publics et privés à cause de l'augmentation constante des cyberattaques. Cette tendance engendre des risques spécifiques qui peuvent compromettre la sécurité des acteurs, personnes physiques ou morales. En 2023 par exemple, l'augmentation des attaques ciblant les petites entreprises a été significative. Presque 4 sur 10 ont été victimes d'une cyber-attaque, un chiffre en hausse de 50% au cours des trois dernières années.

Les Jeux Olympiques risquent d'être le motif d'une véritable cyberguerre : « *Le nombre de cyberattaques lors des Jeux Olympiques et Paralympiques (JOP) de Paris 2024 est estimé être huit à dix fois plus élevé que celui pour les JOP de Tokyo. En 2021, 450 millions de tentatives de cyberattaques avaient été repérées : plus de 4 milliards de cyberattaques sont attendues en juillet 2024. Les auteurs potentiels sont supposés être des cybercriminels animés par des motivations d'enrichissement financier et des Etats ennemis* ».[2]

Plusieurs signaux alertent sur les possibilités d'augmentation des cyberattaques :

- L'usage de l'informatique est incontournable.
- Les usages technologiques évoluent à un rythme effréné.
- Les investissements dans les innovations numériques augmentent sans cesse, notamment dans la recherche et le développement de systèmes d'intelligence artificielle (I.A.).
- Par rapport à 2023, les prévisions mondiales de croissance des dépenses en hautes technologies s'élèveront à 8% en 2024, selon le cabinet Gartner[3].
- Les personnes physiques et morales, publiques et privées sont plus enclines à essayer les solutions les plus disruptives qui leurs sont proposées (Chat GPT, I.A. entre autres). Par conséquent, elles s'exposent de plus en plus aux risques numériques, liées aux pertes de disponibilité, d'intégrité, de preuves et de possibilités de contrôle (DIPC). Ces pertes dégradent la confiance dans les systèmes d'informations et les informations elles-mêmes. Un comportement déviant, une erreur humaine non intentionnelle ou un accident technique peuvent être à l'origine de ces situations crisogènes.

[1] https://www.cnp.fr/le-groupe-cnp-assurances/newsroom/actualites/2024/risques-emergents-quelles-sont-les-perspectives-d-evolution-d-ici-a-10-ans
[2] https://www.portail-ie.fr/univers/risques-et-gouvernance-cyber/2024/cyberattaques-aux-jeux-olympiques-et-paralympiques-2024-enjeux-mythes-et-realite/
[3] https://www.gartner.com/en/newsroom/press-releases/2024-04-16-gartner-forecast-worldwide-it-spending-to-grow-8-percent-in-2024

Les volumes de données numériques (Big Data) augmentent de façon exponentielle :

- 500 millions de tweets, 294 milliards de courriels, 4 millions de giga-octets de données Facebook et 2,5 trillions d'octets de données sont produits chaque jour.
- Dans environ 150 ans, le nombre de bits numériques atteindrait une valeur gigantesque, dépassant le nombre de tous les atomes sur Terre.
- Les développements technologiques des 150 dernières années, sont quantitativement et qualitativement supérieurs à ceux des 2 millénaires précédents. Ils sont de plus en plus soutenus par une puissance de calcul remarquable.
- Le Big Data est un objet polymorphe et complexe qui permet de stocker un nombre incalculable d'informations numériques.
- Les entreprises connectées sont confrontées à des enjeux de développements commerciaux pour attirer et fidéliser la clientèle. Elles s'appuient sur le Big Data pour traiter leurs données, au profit du marketing prédictif[4].

La sophistication des cyberattaques conduit les internautes à s'adapter en permanence, en adoptant diverses solutions et gestes de prévention. L'assurance est l'un des moyens de se prémunir contre leurs conséquences.

Dans cet article, nous abordons la situation géopolitique mondiale dans un contexte d'accélération des cyberattaques à caractère politique. Nous analysons les impacts de ces risques émergents sur les populations et les conséquences pour les plus vulnérables. Nous revenons sur les effets du développement croissant de la numérisation et des systèmes d'intelligence artificielle pour la société. Enfin, l'exploration des avantages et des inconvénients de ce nouveau paradigme nous permet de dessiner les innovations assurantielles de demain.

1. Le contexte géopolitique

En France, l'ANSSI (Agence nationale de la sécurité des systèmes d'information) a constaté l'augmentation drastique des attaques destinées à :

- promouvoir des discours politiques,
- entraver l'accès à des contenus en ligne,
- ou à porter atteinte à l'image de marque des organisations institutionnelles et privées.

Les cyberattaques à caractère politique

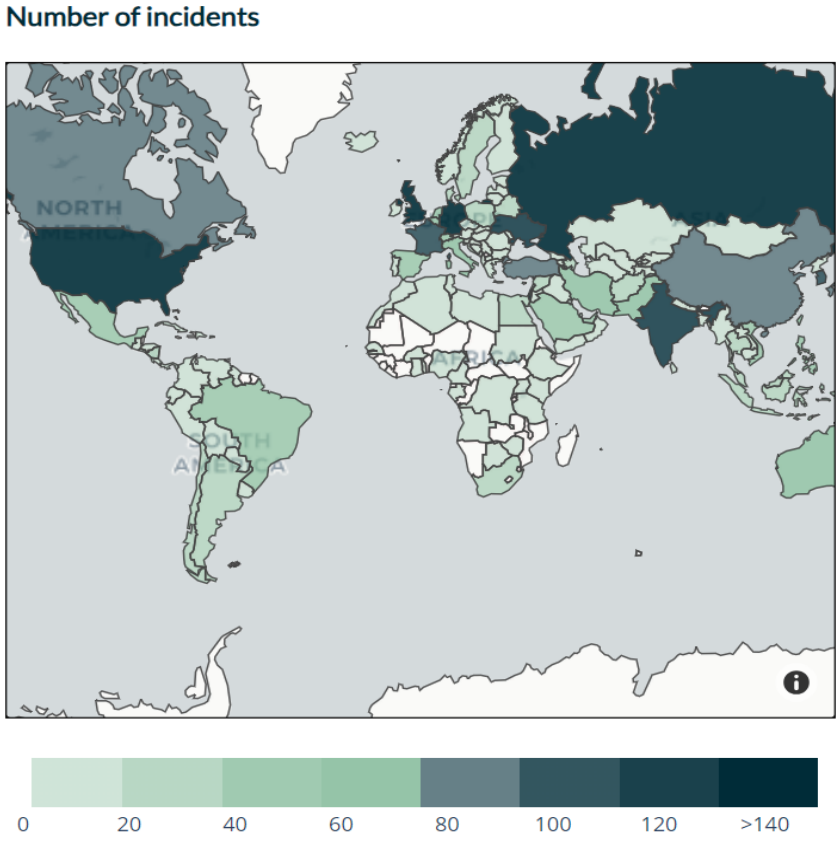
L'institut de recherche Eurepoc se focalise sur la dimension politique des attaques : cible et objectifs politiques, infrastructures critiques… Les données fournies ne couvrent que les cyberincidents politiques signalés publiquement. Un nombre potentiellement important de cas est laissé de côté en raison de leur non-détection ou de leur non-divulgation. Certains cyberincidents sont délibérément éliminés lorsqu'ils concernent des parties prenantes spécifiques, et ne sont pas traités par les acteurs politiques. C'est le cas, par exemple, de nombreuses attaques de ransomware à motivation criminelle contre des entités commerciales.

Comment fonctionne Eurepoc ? Les données sont collectées journalièrement. La base contient le nombre des attaques à caractère politique et l'intensité de ces attaques selon leur nature et leurs effets physiques. Un score d'intensité est affecté à chaque pays en fonction de l'importance politique de l'incident. Il varie entre 0 et 15 et est classé selon trois niveaux d'intensité :

- modérée pour un score de 1 à 5,
- élevée pour un score de 6 à 10,
- et très élevée pour un score de 11 à 15.

Les données de l'Eurepoc confirment la croissance du nombre de cyberattaques à dimension politique dans le monde. L'année 2023 concentre à elle seule, plus de la moitié des incidents déclarés sur la période entre 2020 et 2023. Nous pouvons attribuer cela à l'intensification des guerres et à l'avènement des IA génératives.

[4] https://www.weforum.org/agenda/2021/05/world-data-produced-stored-global-gb-tb-zb/



A partir de ces informations, nous avons estimé la fréquence annuelle puis la sévérité des attaques cyber menées contre 40 pays, dont les pays de l'OCDE. La fréquence correspond au nombre annuel d'attaques divisé par le nombre de jours de l'année. Notre objectif est de comparer ces pays entre eux suivant leur niveau de richesse estimée en produit intérieur brut (PIB) par habitant.

Les pays les plus riches ne sont pas toujours les plus exposés

En 2023, ces pays ont subi une intensité d'attaques modérée car leur score est inférieur ou égal à 5. La Lituanie arrive en tête avec un score égal à 5 et l'Islande, avec un score égal à 0, n'a pas subi d'attaque déclarée. L'analyse suivant les axes d'intensité et de la fréquence annuelle, confirmée par le critère de la sévérité, montre que l'on peut distinguer 3 groupes dans ce panel.

Le premier groupe représente un peu moins de 2 pays sur 10 (17,5% du panel) ayant subi des attaques d'intensité supérieure ou égale à 3,5 en 2023. Parmi les Etats concernés, on distingue deux profils :

1. Les pays au niveau de PIB par habitant[5] assez différent et à la fréquence annuelle d'attaques très faible (proche de 0) comme : la Lituanie, le Portugal, l'Autriche, la Colombie, l'Irlande et le Luxembourg (pays au PIB par habitant le plus élevé du groupe).

2. Les Etats-Unis qui font cavalier seul avec une fréquence annuelle la plus élevée de l'ensemble du panel.

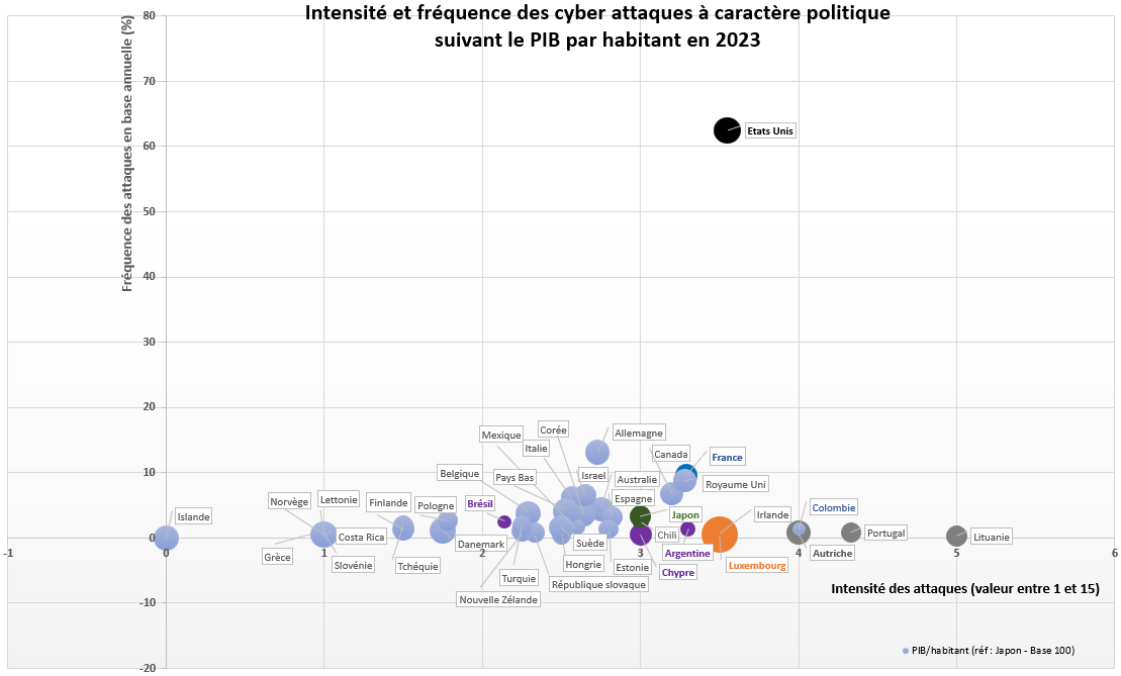
Le deuxième groupe concentre presque la moitié des pays (47,5% du panel) avec un score compris entre 2,5 et 3,5. Ce groupe est intéressant car on y trouve à la fois des pays de l'OCDE et hors OCDE comme le Brésil, Chypre et l'Argentine.

L'analyse de la fréquence annuelle des attaques positionne l'Allemagne avec un niveau de 13% avec le 3e PIB par habitant du groupe. Tandis que les fréquences annuelles du Pays Bas et de la Suède, respectivement 1er et 2e PIB par habitant du groupe, sont plus faibles : moins de 2% pour le premier et un peu plus de 4% pour le second.

[5] https://www.imf.org/external/datamapper/PPPPC@WEO/OEMDC/ADVEC/WEOWORLD/URY

D'autres pays au PIB par habitant comparable, comme la France (9,59%) et le Royaume Uni (8,77%), ont une fréquence annuelle d'attaques proche de 10%.

Dans le troisième groupe, plus de 3 pays sur 10 (32,5% du panel) ont une intensité d'attaques modérée comprise entre 1 et 2,5 et une fréquence annuelle d'attaques proche de 0.



DE : Allemagne ; AR : Argentine ; AUS : Australie ; AT :Autriche ; BE : Belgique ; BR :Brésil ; CA : Canada ; CL : Chili ; CY : Chypre ; CO : Colombie ; KR : Corée ; DK : Danemark ; ES : Espagne ; EE : Estonie ; US : Etats Unis ; FI : Finlande ; GR : Grèce ; HU : Hongrie ; IE : Irlande ; IS : Islande ; IL : Israël ; IT : Italie ; JP : Japon ; LV : Lettonie ; LT : Lituanie ; LU : Luxembourg ; MX : Mexique ; NO : Norvège ; NZ : Nouvelle Zélande ; NL : Pays Bas ; PL : Pologne ; PT : Portugal ; SK : République Slovaque ; GB : Royaume Uni ; SI : Slovénie ; SE : Suède ; CZ : Tchéquie ; TR : Turquie

2. La numérisation croissante d'un monde à l'épreuve de cyber risques

La prolifération technologique est à l'origine d'une hausse des vulnérabilités pour les systèmes économiques, politiques et sociaux. L'engouement pour le numérique augmente concomitamment à la hausse mondiale des cyberattaques.

Le taux de croissance des coûts de la cybercriminalité est estimé à 50% d'ici à 2028[6]. Ce chiffre est aligné avec les statistiques des revenus mondiaux de l'*Internet of things* (IoT) : ils augmenteront de 55% entre 2024 et 2028. Cette tendance devrait se poursuivre.

Selon le baromètre de la Transformation digitale des petites et moyennes entreprises en France[7], 77% des PME développent leurs stratégies digitales et ne comptent pas s'arrêter en si bon chemin. L'émergence de l'I.A. va accélérer l'adoption du *cloud*. Gartner prévoit une utilisation de cette solution par 70% des entreprises d'ici 2027, contre 15% en 2023. L'informatique quantique va se développer.

On assiste à une sophistication croissante des attaques

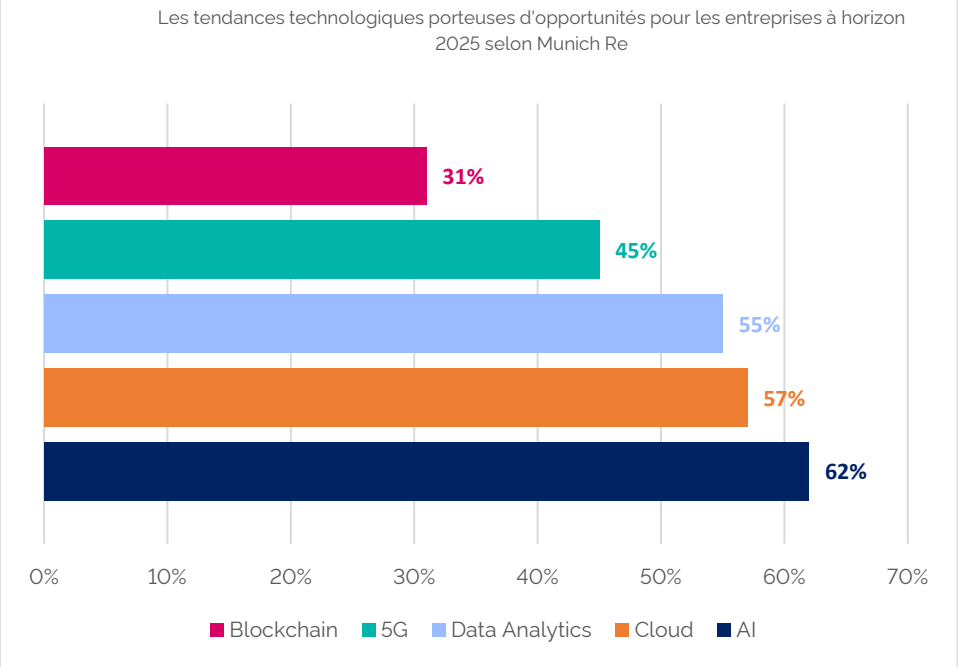
Les particuliers multiplient leurs connexions. 87% des Français possèdent un smartphone, 27% ont une enceinte connectée. La plupart des usages de la vie courante s'appuie sur les technologies numériques[8].

[6] https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/
[7] https://www.imt.fr/wp-content/uploads/2021/07/2021_barometre-transformation-digitale-entreprises.pdf
[8] https://www.arcep.fr/uploads/tx_gspublication/rapport-barometre-numerique-edition-2022-Rapport.pdf

Informations principales à retenir d'après l'étude réalisée en avril 2023 par le Blog du Modérateur[9] :

- Le nombre d'utilisateurs d'internet a augmenté de 1,1 % depuis janvier 2023 dans le monde.
- Le nombre d'internautes mondial est de 5,181 milliards.
- 93,9 % de la population mondiale utilise un smartphone pour surfer sur le web.
- 92,6 % de la population française utilise Internet.
- Le temps moyen passé sur Internet en France est de 5 heures et 19 minutes par jour.

Le développement technologique favorise la sophistication croissante[10] des attaques depuis l'avènement de Chat GPT entre fin 2022 et début 2023[11]. Au cours de cette période, les attaques par phishing (ou hameçonnage) ont augmenté de 135% grâce, également, à l'amélioration des messages frauduleux et l'assistance de l'I.A.[12] pour lancer des attaques[13].



Inspiré de la publication "Technology trends with significance relevance for companies until 2025"[14] In Cyber Risks

Cyber Insurance Risks and Trends 2024 de Munich Re

Eduquer et former pour prévenir les risques numériques

Dans une société ultra dépendante du numérique, il est nécessaire d'éviter les menaces tout en saisissant les opportunités, car les utilisateurs ne peuvent pas se soustraire à la révolution technologique.

C'est grâce à l'éducation, la sensibilisation et la formation de tous les publics, que l'on peut maitriser les usages technologiques, en intégrant les précautions nécessaires à la sécurité des systèmes et des informations. Dans les entreprises, une parfaite compréhension des dispositifs de cybersécurité, des politiques de sécurité des systèmes et des informations améliore la prévention des risques numériques.

[9] https://www.blogdumoderateur.com/chiffres-cles-internet-reseaux-sociaux-monde-avril-2023/
[10] https://numeum.fr/system/files/2024-03/livre%20blanc%20IA%20cyber%20VF.pdf
[11] https://www.stationx.net/phishing-statistics/
[12] https://www.verspieren.com/fr/entreprise/article/iard/risques-cyber-ia
[13] https://arxiv.org/abs/2403.02817
[14] https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html

Les technologies comme l'IA porteuse de risques et d'atouts

Certaines technologies duales sont à la fois porteuses de risques et d'atouts contre les menaces. Par exemple, l'I.A. peut servir[15] à sécuriser les systèmes d'information en permettant de :

- détecter de nouveaux risques de sécurité,
- limiter les erreurs dans la gestion des menaces et des incidents,
- automatiser des tâches dans les processus de réponses et détecter des *deepfakes*.

L'I.A. peut également optimiser la mise en place de couvertures d'assurance cyber afin de déterminer des montants de primes plus justes et rendre les produits plus attractifs[16].

3. Jeunes et seniors : des personnes plus vulnérables du fait de leurs rapports extrêmes aux technologies

Ces populations ont, au cours des dernières années, accru leur usage des objets numériques. D'une part, le taux d'équipement des personnes âgées de 60 à 69 ans a augmenté de 24% entre 2019 et 2022[17]. D'autre part, en 2023, selon une étude de CNP Assurances réalisée avec l'IFOP[18], 83% des jeunes de 15 à 24 ans fréquentaient quotidiennement les réseaux sociaux. Ils sont de ce fait particulièrement exposés aux risques cyber. En effet, la même étude indique que les proportions des Français de 18-24 ans et de plus de 65 ans, ayant vécu au moins une situation de cyber risque, sont respectivement de 86% et 71%.

Deux types de risques concernent les personnes le plus vulnérables

Les personnes âgées sont particulièrement vulnérables aux arnaques par phishing. Ce phénomène est dû à leur technophobie, leur illectronisme ou encore à leur moindre maîtrise des objets connectés. Les risques cybers restent insuffisamment connus de ces publics, ce qui limite l'adoption de comportements préventifs.

Concernant les jeunes, l'étude révèle que deux Français sur trois, dont 85% des 18-24 ans, ont été confrontés à des situations de cyberharcèlement[19].

Par ailleurs, l'IFOP a mené une analyse[20] sur une autre source d'inquiétude pour les jeunes : le *deepfake*. Cette technique de synthèse multimédia basée sur l'IA, permet de disséminer de fausses informations : slogans, textes, images, vidéos. Bien que 83% des jeunes internautes en soient informés, 46% d'entre eux tombent dans le piège et continuent de partager des contenus à risques avec leurs proches sur les réseaux sociaux.

Cela fait d'eux de potentielles victimes d'usurpation d'identité et de vol de données. Notons également que les plateformes qu'ils fréquentent peuvent contribuer à alimenter leur défiance envers les institutions[21].

90% des Français jugent utile de souscrire une assurance contre les cybers risques

En réponse à ces situations, 90% des Français interrogés jugent utile de souscrire une assurance contre les cybers risques. Dans certains cas, des garanties contre les cybers risques, sont incluses dans des packages d'assurances auxquelles ils ont souscrit. Mais 29% des clients ne savent pas s'ils disposent ou non de ce type de couverture.

---

[15] https://www.groupeonepoint.com/fr/nos-publications/intelligence-artificielle-et-cybersecurite-risques-ou-opportunites/
[16] https://www.tcs.com/what-we-do/industries/insurance/white-paper/ai-overcoming-cyber-insurance-industry-challenges
[17] https://fr.statista.com/statistiques/505110/taux-de-penetration-du-smartphone-par-age-france/
[18] IFOP-CNP Assurances, 2024, publication interne au Groupe CNP Assurances
[19] IFOP-CNP Assurances, 2024, publication interne au Groupe CNP Assurances
[20] https://www.ifop.com/publication/les-francais-et-les-jeunes-face-aux-deepfakes/
[21] En 2022, une enquête de l'OCDE montre que 63 % des 18-29 ans au sein des pays de l'OCDE n'ont pas confiance en les pouvoirs publics. https://www.oecd.org/governance/reinforcing-democracy/public-governance-ministerial-meeting-issues-paper-2022-fr.pdf

Solutions assurantielles

Les garanties d'assurance disponibles sur le marché couvrent la protection en ligne et les e-achats. Elles peuvent faire bénéficier les moins de 30 ans d'une réduction[22]. Il existe des offres de couverture contre les nouveaux risques, dont une assurance pour aider les jeunes victimes de cyber harcèlement ou d'intimidation. Ces offres peuvent contenir des conseils, des mesures de sécurité pour y mettre fin, ainsi qu'une protection pour les parents.

4. Phishing (ou hameçonnage) utilisé comme principal mode d'attaque

Les cyberattaquants privilégient la manipulation de leurs cibles pour les amener à commettre des erreurs : divulgation de données confidentielles, compromission des systèmes d'information…. La forme la plus courante d'attaque est le phishing dans 51% des cas recensés[23]. Le phishing est une technique destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (compte d'accès, mots de passe…) et ou bancaires en se faisant passer pour un tiers de confiance[24].

Selon le baromètre annuel 2023 du Club des Experts de la Sécurité de l'Information et du Numérique (CESIN), 60%[25] des entreprises estiment que ce type d'attaque est le mode privilégié des cybercriminels.[26]Et dans 74% des cas, ce type d'attaque est celui qui a le plus d'impacts dans les organisations[27].

Pour réduire ce risque, des campagnes de prévention et d'informations sont réalisées par les acteurs publics et privés. CNP Assurances met à disposition du grand public une page de conseils[28], afin de les aider à adopter les meilleures pratiques contre les risques numériques.

5. Environnements professionnels et économiques de plus en plus confrontés aux cyberattaques

Les entreprises (grands groupes, petites et moyennes entreprises) les plus exposées sont celles qui n'ont pas mis en place de dispositif de prévention approprié. C'est souvent le cas des PME dont les ressources humaines et financières sont insuffisantes pour investir, se protéger ou se relever des offensives informatiques.

Typologie de cyberattaques

- Ingénierie sociale
- Phishing (ou hameçonnage)
- Programmes malveillants
- Attaque par déni de service distribué (DDoS)
- Attaque par injection de code SQL
- Scripting inter-site (XSS)
- Attaque par Botnet
- Rançongiciels

En 2022 une enquête d'Asteres évaluait à 52% la proportion des PME ayant subi une attaque cyber réussie[29]. A la suite d'une attaque de ce type, 60% des PME déposent le bilan[30].

[22] https://www.allianz.ch/fr/clients-prives/offres/habitation-droits/cyberprotection.html#/formrunner, https://www.allianz-partners.com/fr_FR/services/allyz/allyz-cybercare.html
[23] https://assets.barracuda.com/assets/docs/dms/Spear-phishing-vol7.pdf
[24] Ministère Français de l'économie et des finances, de la souveraineté industrielle et numérique - https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage
[25] https://systematic-paris-region.org/barometre-annuel-du-cesin/
[26] https://systematic-paris-region.org/barometre-annuel-du-cesin/
[27] https://asteres.fr/site/wp-content/uploads/2023/06/ASTERES-CRIP-Cout-des-cyberattaques-reussies-16062023.pdf
[28] https://www.cnp.fr/nos-conseils-pour-renforcer-votre-securite-numerique
[29] https://asteres.fr/site/wp-content/uploads/2023/06/ASTERES-CRIP-Cout-des-cyberattaques-reussies-16062023.pdf
[30] https://themas.lemondeinformatique.fr/les-chiffres-cles-signifiants-de-la-cyber-resilience/

Les PME sont fragiles et démunies face aux attaques cyber

Les offensives contre ces acteurs peuvent provoquer l'interruption de leurs activités et des pertes majeures : vol de données, usurpation d'identité, déni de service... Le cabinet d'étude Asteres chiffre le coût moyen d'un incident informatique à 59 000 euros minimum, selon le type d'attaque et d'organisation[31].

CNP Assurances et La Banque Postale, en partenariat avec MARSH France, accompagnent les PME dans la compréhension et la maîtrise des risques cyber. Leur offre « Protection Cyber » les protège contre ces risques en combinant garanties d'assurance et services de qualité. Cette démarche est très utile en amont des projets de sécurisation des entreprises. Elles bénéficient ainsi d'une étude préalable à l'installation de leurs dispositifs de cyber protection.

Enfin, l'Etat français s'est mobilisé en créant ACYMA[32], dans le cadre de la stratégie numérique du Gouvernement, présentée le 18 juin 2015. Il s'agit d'un groupement d'intérêt public d'action contre la cyber-malveillance. Son site web propose un kit de sensibilisation de neuf thématiques, déclinées en six formats : fiches pratiques, réflexes, mémos, affiche A2, BD, vidéos, quiz et infographies. Il est destiné à tous les internautes.

6. Conclusion : la prospective au service de l'innovation assurantielle

La digitalisation des activités humaines est irréversible. Les revenus générés à l'échelle mondiale par l'intelligence artificielle devraient augmenter de 141,5% entre 2024 et 2030[33]. Et l'Europe œuvre pour devenir le leader mondial du numérique d'ici 2030[34]. La numérisation croissante de l'économie alimente et accélère le développement de l'intelligence artificielle. Aujourd'hui, les organisations sont très attentives aux avantages et aux inconvénients de l'IA.

Elle permet d'améliorer les performances des entreprises car c'est un outil d'organisation, de renforcement des connaissances et d'amélioration de l'expérience client. Elle offre la capacité d'accélérer la prise de décision, la gestion de protocoles réglementaires et les réponses aux réclamations des clients. Depuis quelques années, certains acteurs du secteur de l'assurance l'utilisent pour mieux prédire, comprendre et suivre les risques.

L'IA, source d'une meilleure rentabilité pour les assureurs ?

Selon une étude publiée par McKinsey en 2023, l'I.A. pourrait être aussi « *source d'une meilleure efficacité de rentabilité pour les assureurs : en utilisant l'I.A., les assureurs obtiendront des gains importants en matière de services et d'opérations. Elle ajouterait jusqu'à 1,1 billion de dollars en valeur annuelle pour le secteur mondial de l'assurance, dont environ 400 milliards de dollars pourraient provenir des mises à niveau technologiques en matière de souscription et 300 milliards de dollars dédiés au service client et aux offres personnalisées* »[35].

L'IA est aussi source de menace pour la société, notamment par l'augmentation de l'exposition de la population et des acteurs aux risques cyber. Pour encadrer le déploiement et l'usage éthique des technologies de l'IA, l'UE a adopté en 2023 l'IA Act. Cette règlementation est considérée comme une avancée majeure en Europe et dans le monde.

Vers de nouvelles garanties contre les risques de défaillance de l'IA d'ici à 5 ans ?

Malgré le développement de la réglementation et des bonnes pratiques, les progrès très rapides de ces outils technologiques gardent un temps d'avance. Il existe des inquiétudes spécifiques à l'usage des systèmes d'intelligence artificielle principalement liées au « risque algorithmique ». La machine pourrait prendre des décisions incontrôlables par l'humain avec des conséquences financières et réputationnelles dommageables.

Les stratèges manquent actuellement de données scientifiques, sur les événements cybers, y compris dans le domaine de l'Open-Data. Or, l'accès aux données de qualité est un facteur majeur d'accélération ou de limitation des innovations pour tous les secteurs économiques. C'est un appui considérable pour la recherche scientifique transdisciplinaire et la

[31] https://asteres.fr/site/wp-content/uploads/2023/06/ASTERES-CRIP-Cout-des-cyberattaques-reussies-16062023.pdf
[32] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybersecurite-les-cybermalveillances-les-plus-frequentes
[33] https://www.statista.com/statistics/941835/artificial-intelligence-market-size-revenue-comparisons/
[34] https://www.aboutamazon.fr/actualites/aws/une-nouvelle-etude-daws-et-strand-partners-revele-que-leconomie-francaise-pourrait-croitre-de-99-milliards-deuros-grace-a-ladoption-de-lintelligence-artificielle
[35] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#introduction

prospective stratégique. Ses objectifs sont de suivre l'état de l'art des évolutions des cybermenaces associées aux technologies de pointe, afin d'en déduire des pistes de progrès pour les assureurs et protéger le plus grand nombre.

Dans ce contexte, le secteur de l'assurance est-il prêt à repousser les limites de l'assurabilité face à ces risques émergents et au caractère systémique pour proposer des protections aux clients particuliers et entreprises ? Les réflexions sont en cours. Sous certaines conditions, les conséquences financières et réputationnelles des cyber-attaques pourraient être assurées. Une opportunité pour certains acteurs du secteur qui sont déjà sur les rangs. Ils innovent en proposant des couvertures contre les risques de défaillance des modèles d'intelligence artificielle[36].

[36] *https://www.munichre.com/en/solutions/for-industry-clients/insure-ai.html*