IESF
SOCIÉTÉ DES INGÉNIEURS ET SCIENTIFIQUES DE FRANCE
CÔTE D'AZUR

BULLETIN

2023 – N°1

SOMMAIRE

1. Editorial : Vœux 2023

> *"… Nos concitoyens, à cet égard, étaient comme tout le monde, ils pensaient à eux-mêmes, autrement dit, ils étaient humanistes : ils ne croyaient pas aux fléaux. Le fléau n'est pas à la mesure de l'homme, on se dit que c'est le fléau qui est irréel, c'est un mauvais rêve qui va passer. Mais il ne passe pas toujours et, de mauvais rêve en mauvais rêve, ce sont les hommes qui passent, et les humanistes en premier lieu, parce qu'ils n'ont pas pris leurs précautions. Nos concitoyens n'étaient pas plus coupables que d'autres, ils oubliaient d'être modestes, voilà tout, et ils pensaient que tout était encore possible pour eux, ce qui supposait que les fléaux étaient impossibles…"*

Ce texte de Camus, dans La Peste, illustre bien ce que nous vivons de vivre au cours des deux années passées. Mais je le trouve pessimiste. Certes nous venons de vivre deux années difficiles. On croyait que c'était dernière nous ! Or cette période de vœux finit par s'annoncer morose. Les syndicalistes s'agitent avec le spectre du pouvoir d'achat en baisse ; les économistes dissertent sur l'ampleur des crises à venir, les aléas géopolitiques inquiètent notamment avec la guerre en Ukraine qui n'en finit pas, les risques climatiques s'aggravent (bien que la mer vînt à Nevers au Crétacé), la dette française demeure abyssale… Faut-il continuer ? Pas nécessairement car je demeure optimiste. Beaucoup de feux verts sont tout de même allumés (chômage en baisse par ex., deux prix Nobel en France dont un de physique, ce n'est quand même pas rien…) et surtout, j'ai foi en la science et la technologie qui sont de puissantes alliées. J'ai confiance en l'esprit de nos ingénieurs prêts à se mobiliser pour répondre aux défis actuels.

A notre niveau, cette dernière année a été plutôt bonne, avec une reprise forte de nos activités PMIS (lycées, forums, village des Sciences, réseau Masséna, Studyrama, UPSTI…), avec une journée nationale de l'ingénieur (JNI) réussie, sur le thème majeur de l'hydrogène dans le contexte de la transition environnementale, avec notre participation à des forums techniques locaux, comme la semaine de l'industrie à Grasse ou dans le secteur de l'énergie à Nice, avec la remise du livre blanc IESF aux autorités politiques locales, avec la publication de notre propre livre blanc, fruit d'une réflexion collaborative, avec la reprise de visites (ACRI, Salon de Provence, Ecole de l'aviation légère au Luc, Exposition ExodeS à Fréjus), avec notre participation aux instances locales (notamment au conseil d'administration de Nice-Sophia-Polytech, à la Journée portes ouvertes, à la cérémonie de remise des diplômes), sans oublier le Congrès des régions IESF tenu à Grasse, ni notre bulletin trimestriel qui a paru régulièrement et qui a été diffusé notamment à toutes les régions. Bref, nous sommes confrontés à l'impérieuse nécessité d'aller de l'avant !

Aussi pour 2023, je ne puis que souhaiter à notre Société des Scientifiques et Ingénieurs de France une excellente année, et pour nous en Côte d'azur, d'avoir suffisamment de forces pour continuer notre œuvre. Des projets, nous avons ! Par exemple celui lié à l'année Eiffel (2023), qui fut président des IESF, et qui a laissé sa trace dans notre région.

Aussi pour 2023, je souhaite à tous nos membres une excellente année, en particulier pour tous nos bénévoles qui ne ménagent pas leur peine.

Aussi pour 2023, je souhaite à chacun d'entre vous, à vos proches et tous ceux qui vous sont chers, une excellente année.

Jean-Pierre Rozelot

Président d'IESF-CA

2. IESF-CA et son déjeuner annuel convivial à la Guinguette Gaudoise

Enfin, après deux années d'interruption pour cause d'un virus "Mal intentionné", notre rassemblement convivial annuel de début d'année a eu lieu à la guinguette Gaudoise.

Nous y étions une trentaine, adhérents aux IESF-CA, conjointes, sympathisants dont une jeune fille "future ingénieure" ... Tout en regrettant que certains n'aient pu se joindre à nous pour raison familiale.

Notre président avec ses vœux, nous a fait part des principales actions de notre association tout en citant Albert Camus pour mieux cibler son propos.

Un gâteau d'anniversaire impressionnant a clôturé notre excellent déjeuner gargantuesque accompagnant des moments d'échange et de dialogue nous permettant de mieux nous connaître.

Un grand MERCI à toutes celles et ceux qui se sont réunis en toute amitié.

Une pensée particulière à Philippe qui a organisé ce déjeuner en ce lieu que certains ont fréquenté durant des années de labeur.

Henri Carsalade

Past Président

3. Salon Studyrama Palais Nikaïa Nice

Ce salon s'est déroulé les 6 et 7 janvier à Nice-Ouest (Palais Nikaïa) durant une demi-journée suivie d'une journée complète.

Notre objectif était, comme dans toute présentation PMIS, de présenter, avec les moyens mis en œuvre par l'association, les parcours et formations pour devenir ingénieur et accéder à l'offre multiple des métiers et carrières qui sont offerts.

Le vendredi après-midi a surtout été consacré à des élèves de collèges et lycées conduits par leurs établissements dans le cadre de leur parcours scolaire. Très peu de contacts et pas de conférence générale.

Le samedi a été très positif avec des rencontres efficaces avec des élèves et souvent leurs parents, durant lesquelles les différentes voies d'accès ont été décrites, incluant bien sûr les choix d'études à faire dès la seconde pour permettre l'orientation désirée. Une conférence a été tenue par Pierre et Germain, et qui a rassemblé un auditoire nombreux très attentif.

Il est suggéré qu'une connaissance approfondie de Parcousup par les contributeurs au programme PMIS des IESF permette d'aider de façon plus pertinente à l'orientation.

Il en résulte, aussi et une fois de plus, que les actions PMIS doivent être faites relativement tôt dans le cursus scolaire, dès les années de troisième et seconde, et si possible avec la présence des parents qui sont des contributifs d'orientation majeurs.

Nous étions trois sur le site, Pierre Quirin, Germain Sagols, Philippe Hernandez, sans oublier le support donné par une absente, Dominique Queau, pour raison personnelle.

Il vous est fait grâce du nombre de personnes rencontrées (étudiants et parents) lors de ces deux jours : il est éloquent et comptabilisé dans le programme PMIS 2002/2023 dirigé par Jean-Louis Droulin.

Le programme PMIS est excellent pour faciliter l'orientation des jeunes filles et garçons vers nos formations et ce qui en découle : il n'existe cependant pas d'outil d'évaluation de son efficacité : difficile certes mais souhaitable.

Philippe Hernandez

Ancien président

4. La cybersécurité : contexte, enjeux, constats et perspectives

Cybersecurity: context, issues, findings and outlook

Résumé

Le numérique a investi tous les secteurs - économie, santé, transport, énergie, télécommunications, éducation, aéronautique, spatial, défense, etc. Les défis industriels et technologiques sont nombreux. Les réseaux 5G, l'IA, l'IoT, etc. sont partie prenante de cette transformation. Cependant les innovations produites par des collaborations académiques et industrielles, nationales et internationales font souvent l'objet de convoitise, de tentative de captation technologique, de détournement de propriété industrielle, etc. de la part d'entreprises concurrentes ou d'organismes étatiques étrangers. De même, les infrastructures critiques (électricité, pétrole, gaz, agro-alimentaire, santé publique, etc.), largement interconnectées, sont susceptibles d'être vulnérables. Une cyberattaque réussie engendre des conséquences économiques et sociétales considérables. Il faut donc concevoir des stratégies de surveillance et de détection des menaces, de développer des solutions techniques de réaction adaptative pour protéger la confidentialité, l'intégrité et la disponibilité des informations, avec une prévention en amont : c'est le rôle de la cybersécurité, liée à la souveraineté numérique d'un pays, au cœur d'enjeux économiques, stratégiques et politiques. Elle a une approche globale incluant entre autres les risques juridiques sur le plan industriel ou politique. Cet article, non exhaustif, présente la cybersécurité, ses enjeux, un état des menaces, des solutions technologiques existantes et des perspectives. Les images présentées sont la propriété de leurs auteurs. Le texte est fondé sur l'ensemble des références citées.

Mots-clés

Cybersécurité, cyber intelligence, cyberattaque, cybercriminalité, cybermenace, cyberguerre, cyberdéfense, souveraineté, numérique, risques, vulnérabilités, menaces, sécurité économique, sécurité numérique, sécurité informatique

Abstract

Digital technology has taken over all sectors - economy, health, transport, energy, telecommunications, education, aeronautics, space, defense, etc. The industrial and technological challenges are numerous. 5G networks, AI, IoT, digital twins, etc. are part of this transformation. However, innovations produced by academic and industrial, national and international collaborations are often subject to covetousness, attempts to capture technology, misappropriation of industrial property, etc. by competing companies or foreign state agencies. Similarly, critical infrastructures (electricity, oil, gas, agri-food, public health, etc.), which are largely interconnected, are likely to be vulnerable. A successful cyber-attack has considerable economic and societal consequences. It is therefore necessary to design strategies for monitoring and detecting threats, to develop technical solutions for adaptive reaction to protect the confidentiality, integrity and availability of information, with upstream prevention: this is the role of cybersecurity, linked to the digital sovereignty of a country, at the heart of economic, strategic and political issues. It has a global approach including, among other things, legal risks on an industrial or political level. This article, which is not exhaustive, presents cybersecurity, its stakes, the state of the threats, the existing technological solutions and the perspectives. The images presented are the property of their authors. The text is based on all the references cited.

Keywords

Cybersecurity, cyber intelligence, cyber-attack, cybercrime, cyberthreat, cyber warfare, cyberdefense, sovereignty, digital, risks, vulnerabilities, threats, economic security, digital security, computer security

4.1 Contexte et enjeux

Compte-tenu du contexte européen et mondial, de la compétition scientifique, technologique et économique, dans les secteurs civil et militaire, il existe des défis que notre société doit relever. Tous les domaines sont concernés - transition énergétique, approvisionnement des matières premières, industrie numérique, mobilité électrique, télécommunications, sécurité, transports, santé, chimie, robotique, microbiologie, nucléaire, aéronautique, spatial, défense, etc.

D'importants investissements ont lieu dans des projets de recherche fondamentale ou d'innovation de rupture que ce soit dans la 5G, le quantique, l'IA, l'intelligence collective et collaborative, la *blockchain*, l'IoT, le biomimétisme, la médecine moléculaire, etc. L'exploitation des données et des connaissances se trouve au centre de toutes les attentes et inquiétudes. En effet nos sociétés sont de plus en plus numérisées car le besoin de communication mobile à très haut débit est devenu indispensable pour l'usage de nouveaux services et d'applications émergentes : la réalité étendue immersive, l'imagerie très haute résolution, etc.

N'oublions pas que le monde de la recherche est un espace d'échange d'idées, de présentation des problèmes à résoudre, de proposition de solutions parfois différentes mais souvent complémentaires. C'est un lieu de compétition entre laboratoires, instituts et pays et aussi un espace de conflits. Souvent pour de grands projets, les moyens financiers, humains, etc. d'un seul état ne suffisent pas. D'où le besoin de coopérations internationales dans de nombreux domaines : station orbitale, Iter, hydrogène, quantique, etc. la coopétition est l'idéal recherché mais bien souvent la concurrence reste de règle au détriment de l'intelligence collective.

La science et la technologie représentent une source de création de valeur économique vitale pour le maintien de la richesse nationale ainsi que pour la création d'emplois. Elles sont d'un intérêt majeur en termes de souveraineté (sécurisation des approvisionnements, maintien des bases industrielles, etc.). Enfin, le maintien d'un haut niveau de qualité est nécessaire afin que la France conserve son rayonnement et son influence et donc son attractivité pour les personnels qualifiés et les investissements directs.

Aujourd'hui, la dépendance vis-à-vis du numérique est donc devenue une arme *à double tranchant*, aussi bien du point de vue des données médicales, bancaires, professionnelles ou personnelles, par exemple que du point de vue industriel par les infrastructures, les réseaux, les architectures des moyens de conception, de production, de maintenance, etc. La presse quotidienne et spécialisée, les médias, etc. font de plus en plus état de cyberattaques ayant paralysé telle administration, tel hôpital ou tel industriel, de piratages d'infrastructures critiques et d'entreprises, etc. Toute faille de sécurité peut être exploitée de manière malveillante.

En effet, les secteurs stratégiques font souvent l'objet d'attaques ciblées par des contentieux juridiques, des ingérences économiques ou des tentatives de captation d'informations. Les atteintes peuvent tout aussi bien cibler les données scientifiques ou technologiques que les outils ou moyens qu'ils soient scientifiques, techniques ou humains. Les conséquences peuvent être la perte de maîtrise des technologies, la baisse de la compétitivité ou la perte de confiance auprès des partenaires, sans oublier la destruction d'emplois, etc. Ainsi au vu de ces enjeux, il s'agit d'assurer à la France et à l'Europe la maîtrise des technologies et des connaissances nécessaires pour faire face aux nombreux défis de la recherche scientifique, du développement économique et environnemental, etc.

La protection du potentiel scientifique et industriel est une nécessité. Au-delà du personnel qui le compose, ce potentiel comprend le plus souvent les équipements, les matériels d'expérience, les bases de données, les savoirs et savoir-faire, les travaux de recherche et d'expérience, les brevets en cours de dépôt, la réputation, l'image du laboratoire, etc. La production intellectuelle (PI) est devenue une source de convoitise de la part de diverses entités (laboratoires ou industriels) désirant exploiter au mieux des informations sur les études en cours, les nouveaux concepts et les brevets, etc. La protection de ce potentiel concerne tous les acteurs de la recherche qui est au carrefour des universités, des laboratoires et des industries. Des politiques publiques accompagnent cette mise en œuvre.

La gouvernance de la recherche académique et les directions industrielles incitent fortement leurs établissements à prendre en compte l'intelligence économique et stratégique : grands groupes, TPE/PME/ETI, start-ups, établissements d'enseignement supérieur et de recherche, écoles d'ingénieurs, etc. Ils sont confrontés régulièrement à des attaques ciblées par le biais de contentieux juridiques, de tentatives d'ingérence économique agressives ou de captation d'informations. L'innovation a besoin d'ouverture collaborative et d'échanges multiples, de type entreprises-entreprises ou entreprises-laboratoires, de protéger les travaux de recherche, les compétences et l'excellence de l'expertise.

La cybersécurité est un élément prépondérant constitutif de la sécurité économique. Elle est directement liée à la souveraineté numérique d'un pays. Elle est donc au cœur d'enjeux économiques, stratégiques et politiques. Elle a une approche globale dont les actions vont bien au-delà de la simple protection du potentiel immatériel. Elle concerne les réseaux informatiques, les liaisons satellites, les *clouds*, les données et leurs échanges, les objets connectés, la mobilité, l'élaboration de médicaments, le matériel militaire, etc. Elle inclut aussi les risques juridiques sur le plan industriel ou politique. Elle représente le rôle de l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion. Ses moyens peuvent être donc techniques, juridiques, méthodologiques ou humains. L'anglais « *digital security* » (sécurité numérique) traduit mieux ce concept. Les Etats, les entreprises, les infrastructures critiques, largement interconnectés, sont vulnérables. En cas de cyberattaque réussie, les conséquences économiques et sociétales peuvent être considérables.

Les objectifs sont organisés selon des familles d'activités propres à la sécurité des systèmes d'information : la gouvernance, la maîtrise des risques et des systèmes, la protection des systèmes, la gestion des incidents, l'évaluation et la relation avec les autorités. La sensibilisation et la formation de l'ensemble des acteurs (monde académique, entreprises, industries) aux risques encourus et aux concepts de l'intelligence économique et stratégique, sont indispensables.

Comme l'État est responsable de la cyberdéfense et garant de la cybersécurité, ses agences et services aident les industriels, les entreprises et le monde de la recherche académique à mettre en œuvre les actions suivantes :

- protéger le potentiel scientifique, technique et industriel en incluant les partenariats académiques-industriels ;
- mettre en œuvre une politique adaptative (cartographie des environnements informatiques, identification des menaces, capacité d'anticiper, etc.) ;
- développer davantage les cursus supérieurs en intelligence économique et stratégique, en cybersécurité, aux nouvelles technologies innovantes, etc. ;
- élaborer un écosystème de confiance dans les écosystèmes de la recherche ;
- assurer la sensibilisation et la formation de tous les acteurs concernés.

Le papier présente un état des menaces actuelles et commente l'apport des nouvelles technologies. Il expose des éléments de la politique publique de la France et de l'Europe. Des éléments de perspective sont proposés. Le texte est basé sur les documents donnés en référence. Les images et figures sont la propriété des auteurs respectifs cités.

Les termes cybersécurité, cyberdéfense, cybernétique, etc. sont construits à partir du préfixe « cyber », d'origine grecque, signifiant « gouverner au sens du gouvernail », sans doute adapté pour la cybernétique, mais maintenant il est inadapté dans tous les autres cas ! Plus précisément, le mot cybernétique vient du grec *kubernêtikê*, de *kubernân* (gouverner). En 1948, Norbert Wiener, mathématicien au MIT (Etats-Unis) dans un programme de recherche consacré à de nouvelles formes d'armement (seconde guerre mondiale), baptisa « cybernétique », un nouveau domaine de la science, qui étudie la maîtrise des machines. Son livre « *Cybernetics or Control and Communication in the Animal and the Machine* » (1948, 2ème ed. 1961) comporte la première utilisation publique du terme « cybernétique » pour désigner les mécanismes d'autorégulation et de communication chez l'être vivant et la machine. Le sens actuel vient du mot anglais cyberspace, inventé en 1984 par l'auteur américano-canadien de science-fiction, William Gibson, dans son ouvrage Neuromancer.

Sources :

- Myriam Quéméner, Jean-Paul Pinte, Cybersécurité des acteurs économiques : Risques, réponses stratégiques et juridiques, Paris, Hermes Science Publications, coll. Cyberconflits et cybercriminalité, 13 décembre 2012, 239 p. ;
- Stéphane Taillat, Amaël Cattaruzza, Didier Danet (Dirs), La Cyberdéfense - Politique de l'espace numérique, Armand Colin, Coll. U, 4 juillet 2018, 256 p. ;
- Jean-Pierre Damiano, Les enjeux de la recherche et l'intelligence économique et stratégique, Techniques de l'Ingénieur, AG 1611, 10 octobre 2019 ;
- Arrête-moi si tu peux : histoire de la cybersécurité, Infographie complète "Histoire de la cybersécurité", Thalès Group, 5 décembre 2019 ;
- Jean-Pierre Damiano, De la 5G à la 6G : contexte et enjeux ! IESF Côte d'Azur, 2020, Bull. n°4, p.13-23 ;
- Rapport d'information déposé par la commission des affaires européennes sur l'avenir de la cybersécurité européenne, n° 2415, déposé le 14 novembre 2019 ;
- Le renseignement d'intérêt économique et la protection du patrimoine économique de la Nation, Alexis Deprau, Ecole de Pensée sur la Guerre Economique (EPGE), 6 janvier 2020 ;
- Yann Salamon, Cybersécurité et cyberdéfense : enjeux stratégiques, Éditions Ellipses, 6 octobre 2020, 336 p. ;
- Cloud Souverain : quels sont les enjeux pour la protection des données et l'écologie ? Les Echos, 8 mars 2022 ;
- Jean-Pierre Damiano, Stockage d'énergie électrique : un regard sur les enjeux et les défis technologiques, IESF Côte d'Azur, 2022, Bull. n°1, p.10-22 ;
- Jean-Pierre Damiano, Matières premières, métaux critiques, terres rares : contexte international et enjeux, IESF Côte d'Azur, 2022, Bull. n°2, p.12-30 ;
- Nicolas Arpagian, La Cybersécurité, Paris, PUF, coll. « Que sais-je ? », Mai 2022, 127 p. ;
- Axelle Degans, La sécurité économique en France et en Europe : du déni au changement de paradigme (1990-2022), *L'Espace Politique* [En ligne], (44) 2021-02, mis en ligne le 20 juillet 2022 ;
- La France face aux nouveaux enjeux de la souveraineté économique, Christian Harbulot, Ecole de Pensée sur la Guerre Economique (EPGE) par Claire Brobécher, 29 septembre 2022 ;
- Cinq plans pour reconstruire la souveraineté économique, Conclusions du rapport, Sénat, compte rendu analytique officiel du 5 octobre 2022 ;
- Histoire de la cybersécurité : Journée internationale de l'Internet, Le VPN, Vuk Mujović, 19 octobre 2022 ;
- Larousse.fr ;
- LaTribune.fr ;
- Wikipédia.

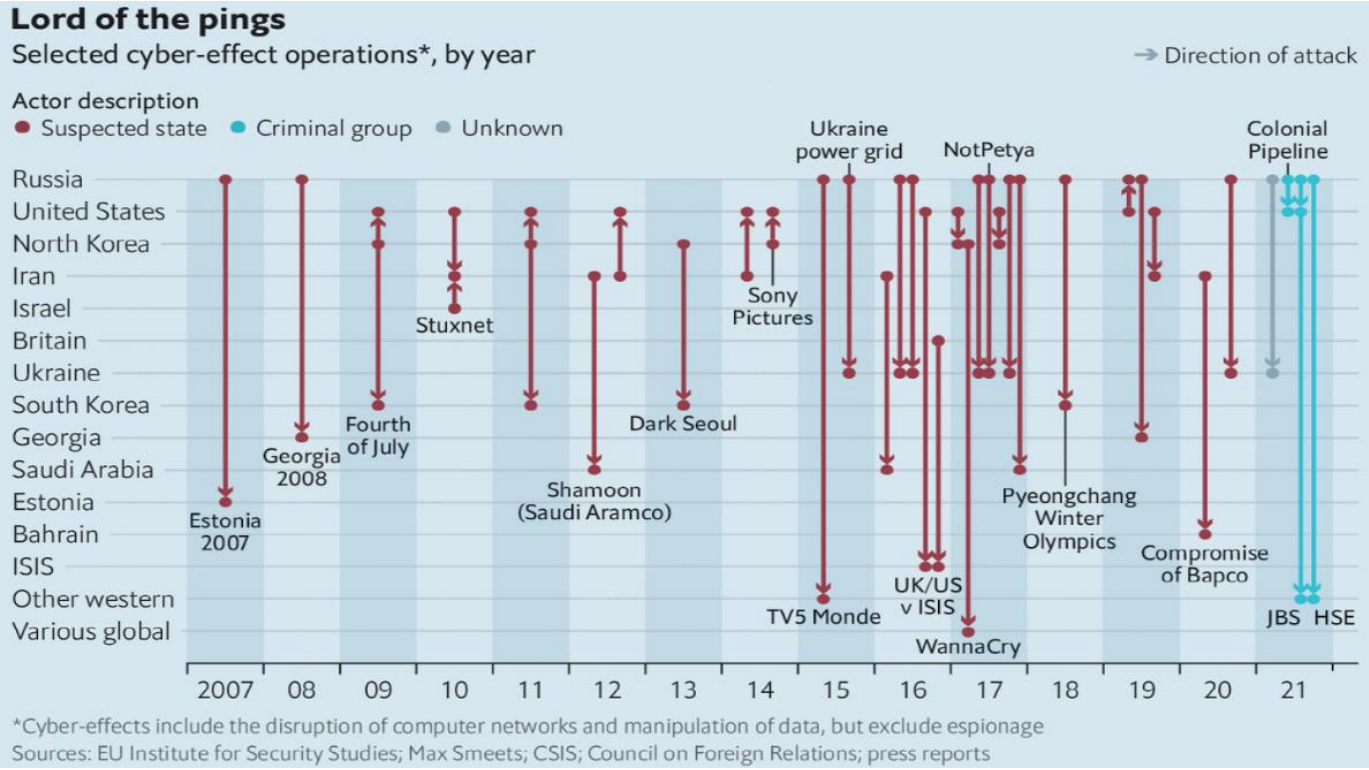
4.2 Quelques rappels sur les menaces

Les menaces peuvent être environnementales, intrinsèques, humaines, etc. Les menaces majeures identifiées peuvent être d'origine externe (compromission ou vol de données, physique, électronique, etc.) mais aussi internes (négligence du personnel, utilisation malveillante des matériels, présence de nombreux non permanents, etc.). Une menace est dite « passive » si elle ne modifie pas l'information et porte essentiellement sur la confidentialité, ou « active » si elle modifie le contenu de l'information ou le comportement des systèmes de traitement. Dans l'environnement économique, des concurrents peuvent devenir cyber-attaquants ou faire appel à des officines spécialisées. Il faut donc renforcer la cyber-résilience qui est la capacité de l'entreprise à résister à de nouvelles menaces.

Comme rapporté par InCyber, Cybercrime Magazine estime que le coût annuel de la cybercriminalité dans le monde dépassera 10 000 Mds $ (9 200 Mds €) d'ici 2025. Une enquête mondiale menée en 2022 révèle qu'environ 46 % des entreprises interrogées en Allemagne avaient été victimes d'une cyberattaque au moins une fois. En moyenne, environ 49 % des entreprises interrogées dans les différents pays ont déclaré avoir subi au moins une cyberattaque au cours des 12 derniers mois. Le volume des attaques par rançongiciel a doublé en 2021 et dépasse désormais les 600 M€.

Les attaques informatiques ne sont pas récentes. Déjà dans les années 70, les virus informatiques infectaient les ordinateurs et dans les années 80, les hackers sévissaient sur les réseaux informatiques alors peu sécurisés. La cybermenace se développe et se professionnalise au fil du temps : les acteurs sont de plus en plus souvent des groupes criminels privés, affiliés ou non à des états. [Quand Internet a-t-il commencé : histoire de la cybersécurité, Le VPN, septembre 2021].

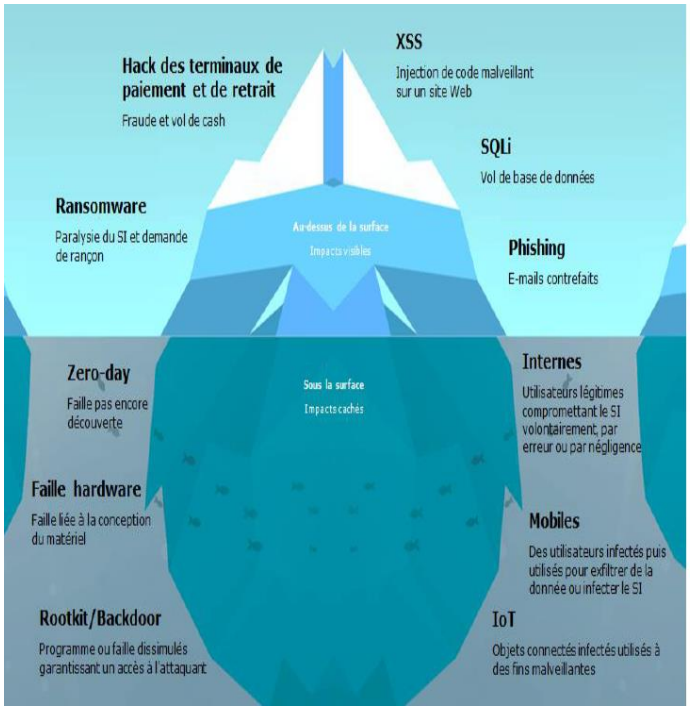
On constate qu'au cours des 15 ans passés, les états les plus souvent suspectés d'être à l'origine d'attaques informatiques sont la Russie et la Corée du Nord. Depuis 2015 et la guerre en Crimée, l'Ukraine est la cible de choix de la Russie. La cybercriminalité et les attaques informatiques sont des armes de plus en plus utilisées dans la guerre hybride (Audit & Systèmes d'Information).



Panorama de la cybersécurité 2022, Audit & Systèmes d'Information, Benoît Rivière, 19 déc. 2022 / conférence animée par Thierry Berthier, 16 nov. 2022 à l'IAE Limoges.

Le forum de Davos 2023 a eu lieu du 16 au 20 janvier 2023 dans les Alpes suisses. Dans le cadre de cet évènement, les experts du World Economic Forum alertent sur la prochaine crise mondiale qui serait une Cyber-Tempête à cause de l'instabilité économique et géopolitique. Une des craintes inquiétantes est que des gouvernements soutiennent les *hackers* ou s'impliquent directement dans les attaques (notamment la Russie ou la Corée du Nord). Le secrétaire général d'Interpol, Jürgen Stock, a résumé : « *c'est une menace mondiale, nécessitant une réponse mondiale et une action amplifiée et coordonnée* ». Il ajoute : « *La clé pour gagner la bataille contre la cybercriminalité est, bien sûr, de travailler ensemble pour en faire une priorité par-delà les lignes de fracture géopolitiques*. »

Une vulnérabilité est une faiblesse qui rend sensible à une menace. Par exemple, un accès au bâtiment mal réglementé et sans contrôle, l'absence de surveillance des entreprises lors de leurs interventions, des trous de sécurité dans les logiciels et applications, des défauts d'authenticité dans les accès réseaux, les coopérations internationales ou l'accueil de stagiaires, etc. nous imposent de rester vigilants, particulièrement lorsque les domaines de recherche sont sensibles ou stratégiques. *Ci-après une cartographie des vulnérabilités et de logiciels d'attaque*



Adware/Publiciel	Logiciel affichant des publicités
Backdoor/Porte dérobée	Logiciel permettant l'accès à distance d'un ordinateur de façon cachée.
Bot	Logiciel automatique qui interagit avec des serveurs.
Exploit	Logiciel permettant d'exploiter une faille de sécurité.
Keyloger/Enregistreur de frappe	Logiciel permettant d'enregistrer les touches frappées sur le clavier.
Ransomware/Rançongiciel	Logiciel qui crypte certaines données du PC, et demande une rançon pour permettre le décryptage.
Rogue	Logiciel se faisant passer pour un antivirus, et indiquant que le PC est gravement infecté. Il se propose de le désinfecter en échange de l'achat d'une licence.
Rootkit	Logiciel permettant de cacher (et de se cacher lui-même) une infection sur un PC.
Spammeur	Logiciel envoyant du spam/pourriel.
Spyware/espiologiciel	Logiciel collectant des informations sur l'utilisateur.
Trojan horse /Cheval de Troie	Logiciel permettant la prise de contrôle à distance d'un PC, il permet souvent l'installation d'une porte dérobée.
Ver/Virus réseau	Logiciel se propageant via un réseau informatique.
Virus	Logiciel conçu pour se propager de PC en PC et s'insérant dans des programmes hôtes.

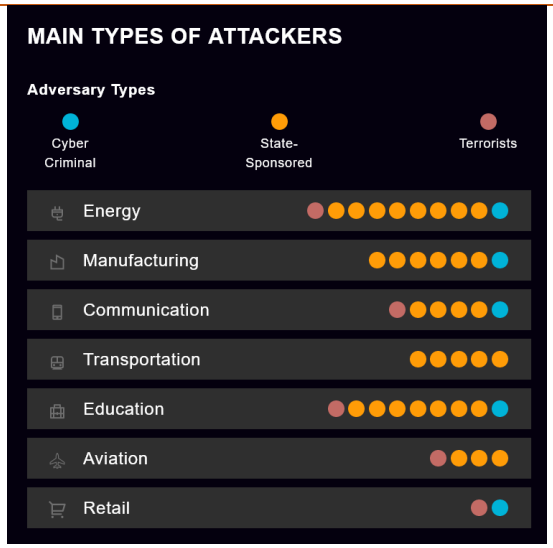
Audit & Systèmes d'Information

4.3 Typologie et cartographie des menaces

L'année 2022 a été une année particulièrement riche en cyberattaques de toute sorte. Les cibles ont été des hôpitaux, des administrations, des institutions, des écoles, des entreprises de toutes tailles, etc. De nombreuses tentatives de piratage d'infrastructures critiques (pétrole, gaz, nucléaire, etc.) ont été recensées (certaines ont réussi), parallèlement à des campagnes de cyber-espionnage, d'utilisation de programmes malveillants et de rançongiciels *(ransomwares),* sans oublier les manœuvres d'organisations cybercriminelles et les piratages de cryptomonnaies.

Exemple du pétrole et gaz offshore : dans un rapport publié fin octobre 2022, le *Government Accountability Office* (GAO), l'organisme d'audit, d'évaluation et d'investigation du Congrès des États-Unis, pointe l'obsolescence de nombreux logiciels de pilotage des 1 600 plateformes offshore de gaz et de pétrole du pays, et des infrastructures de transport associées. Il souligne aussi l'insuffisance des investissements cyber des opérateurs des infrastructures critiques. Les experts fédéraux alertent sur les éventuelles vulnérabilités des interconnexions récentes à des réseaux numériques (dont internet) en notant la faiblesse de leur cyberdéfense *by design, d'autant que des pays comme la* Chine, l'Iran, la Corée du Nord et la Russie tentent d'en tirer parti.

Selon le Thales Cyber Threat Intelligence Expertise, en ce qui concerne l'Europe, on constate que le top 3 des secteurs attaqués sont l'énergie, l'éducation et la fabrication.



Secteur de l'éducation - les écoles et les établissements d'enseignement supérieur sont parmi les cibles les plus populaires en 2021 :

Selon Checkpoint, les organisations ont été confrontées à 1605 attaques de sécurité par semaine. Ce chiffre représente une hausse de 75 % d'une année sur l'autre. À titre de comparaison, les cyberattaques, tous secteurs confondus, ont augmenté de 50 % sur la période. Les raisons de cette croissance apparaissent à la fois structurelles (données précieuses des utilisateurs, sous-appréciation chronique de la cybersécurité), mais aussi conjoncturelles avec l'adaptation complexe des méthodes pédagogiques à la pandémie du COVID 19. Cette combinaison de facteurs semble expliquer pourquoi, bien que le secteur soit confronté à des défis majeurs tels que le manque de personnel et le manque de financement et de ressources, la prévalence des cyberattaques semble augmenter d'année en année, les brèches dans les écoles et l'enseignement supérieur étant largement rapportées.

Secteur de l'énergie particulièrement vulnérable aux cybermenaces contemporaines à cause de :

- un nombre accru de menaces et d'acteurs ciblant les services publics (acteurs étatiques, cybercriminels et des hacktivistes).
- la surface d'attaque étendue et croissante des services publics, résultant de leur complexité géographique et organisationnelle, y compris la nature décentralisée de la direction de la cybersécurité de nombreuses organisations.
- les interdépendances uniques du secteur de l'électricité et du gaz entre les infrastructures physiques et cybernétiques rendent les entreprises vulnérables à l'exploitation.

Thales Cyber Threat Intelligence Expertise

Secteur de la fabrication

Le secteur manufacturier, de par la nature de ses activités, a longtemps été tenu à l'écart des prérogatives de protection des systèmes informatiques. La raison en est double : d'une part, les entreprises manufacturières ont longtemps pu fonctionner en étant déconnectées d'Internet et, d'autre part, la perception générale était que les hackers ne s'intéressaient pas aux informations et aux actifs détenus par les organisations manufacturières. L'émergence de l'industrie 4.0 et la nécessité pour les entreprises manufacturières de connecter leurs systèmes de contrôle industriel (ICS) à Internet ont remis en question ce paradigme. Ainsi, la nouveauté de l'émergence des problématiques de protection des réseaux pour ces entreprises s'accompagne d'un décalage par rapport aux autres secteurs. Cela multiplie les possibilités d'intrusion par des acteurs malveillants, qui peuvent exploiter les actifs de propriété intellectuelle (PI) afin de générer des revenus.

Dans son rapport *Threat Landscape* publié en 2022, l'*European Union Agency for Cybersecurity* (ENISA) a établi une liste des cyberattaques les plus fréquentes et des différentes causes de l'évolution de celles-ci. Il rappelle que l'impact du contexte géopolitique actuel a engendré des conséquences sur les cyber-opérations et les menaces de cybersécurité.

L'efficacité d'une cyberattaque réside dans sa capacité à être imprévisible, pouvant surgir à n'importe quel moment, et en n'importe quel lieu.

Panorama des principales cybermenaces identifiées - ENISA 2022

Pour la période de juillet 2021 à juillet 2022, voici les principales cybermenaces dans l'UE :

- Les attaques par rançongiciels (*ransomware*) permettent aux acteurs de la menace de prendre le contrôle des actifs (données, etc.) d'une cible et exigent une rançon en échange du retour de la disponibilité de cet actif. *60 % des organisations touchées pourraient avoir payé des demandes de rançon.*
- Les dénis de service distribué (DDoS) se concrétisent en ciblant la disponibilité des systèmes et des données. Les attaques se produisent lorsque les utilisateurs d'un système ou d'un service ne sont pas en mesure d'accéder aux données, services ou autres ressources pertinentes. Cela peut se faire en épuisant le service et ses ressources ou en surchargeant les composants de l'infrastructure du réseau. *Juillet 2022 a vu la plus grande attaque jamais enregistrée contre un client européen.*
- Les logiciels malveillants (*malware*) sont des logiciels ou microprogrammes destinés à exécuter un processus non autorisé qui aura un impact négatif sur la confidentialité, l'intégrité ou la disponibilité d'un système : les virus, les vers, les chevaux de Troie, logiciels espions, certaines formes de logiciels publicitaires, etc. *Rien qu'en juin 2022, des chevaux de Troie de type adware ont été téléchargés environ 10 millions de fois.*
- Les menaces d'ingénierie sociale génèrent des activités tentant d'exploiter une erreur humaine ou un comportement humain dans le but d'accéder à des informations ou à des services, à l'aide de diverses formes de manipulation pour inciter les victimes à commettre des erreurs ou à transmettre des informations sensibles ou secrètes. Exemples : *phishing, spear-phishing, whaling, smishing, vishing*, *business* e-mail compromise (BEC), fraude, usurpation d'identité et contrefaçon, etc. *82 % des violations de données impliquent un élément humain*.
- Les menaces contre les données ciblent les sources de données dans le but d'obtenir un accès et une divulgation non autorisés, ainsi que de manipuler les données pour interférer avec le comportement des systèmes (ransomware, RDoS, DDoS, etc .). La violation de données est une attaque intentionnelle menée par un cybercriminel pour obtenir un accès non autorisé et divulguer des données sensibles, confidentielles ou protégées. La fuite de données entraîne la divulgation involontaire de données sensibles, confidentielles ou protégées en raison, par exemple, d'une mauvaise configuration, de vulnérabilités, etc. *Les serveurs étaient les actifs les plus souvent visés par une attaque (près de 90%).*

- Les campagnes de désinformation sont toujours en hausse, stimulées par l'utilisation accrue des plateformes de médias sociaux et des médias en ligne. Les sites sociaux, les organes d'information et les médias, voire les moteurs de recherche, sont désormais des sources d'information pour de nombreuses personnes. La guerre entre la Russie et l'Ukraine a montré de nouvelles façons d'utiliser cette menace, en ciblant la perception qu'ont les gens de l'état de la guerre et des responsabilités des parties impliquées.
- Une attaque de la chaîne d'approvisionnement (*supply chain*) cible la relation entre les organisations et leurs fournisseurs. Elle consiste en une combinaison d'au moins deux attaques. Pour qu'une attaque soit classée comme une attaque de la chaîne d'approvisionnement, il faut que le fournisseur et le client soient tous deux des cibles. Les incidents liés à la chaîne d'approvisionnement ont représenté 17 % des intrusions en 2021, contre moins de 1% en 2020.

La menace, probablement la plus dangereuse, est d'origine étatique avec comme finalité l'espionnage et la déstabilisation. L'autre type de menace, d'origine criminelle, a pour objectif l'extorsion de fonds par une prise en otage des données des victimes, qui vont être chiffrées par un rançongiciel. Ces dernières années, on constate ainsi une augmentation exponentielle des cyberattaques avec le recours accru au télétravail (travail hybride) lié au Covid-19. Une augmentation de 250 % des attaques par rançongiciels a été constatée en 2020. [*Source* : CNRS Info, Janvier 2023].

De manière plus générale, comme le démontre son rapport annuel de prévision des menaces, *l'Advanced Research Center* de l'entreprise Trellix anticipe que le contexte géopolitique mondial (Asie, Europe, etc.) va continuer à façonner le paysage cyber, à développer des cyberattaques. Selon les analyses, une augmentation des cyberattaques commanditées par des États est observée avec une intensification de l'hacktivisme, d'où une augmentation des risques d'une guerre informationnelle à grande échelle.

Par exemple, une importante attaque par déni de service au Parlement européen, a eu lieu après que celui-ci ait voté une résolution déclarant que la Russie était un « État soutenant le terrorisme ». C'est le même type de réaction qui a eu lieu, contre Taïwan et ses alliés (Japon, Corée du Sud), à cause de la visite de la présidente de la Chambre des représentants des Etats-Unis, Nancy Pelosi.

Pour mémoire, l'hacktivisme est constitué d'individus ou de groupes d'individus s'alignant pour une cause commune, utilisant des cyber-outils pour exprimer leur colère et causer des perturbations et dommages de tout ordre.

De plus en plus compétents et professionnels, les cyberattaquants utilisent des codes malveillants sophistiqués pour infiltrer les réseaux industriels dont la protection est de plus en plus complexe à assurer compte-tenu de leurs architectures. C'est une des conclusions du rapport *OT/IoT Security Report: Cyber War Insights, Threats and Trends, Remediations* de Nozomi Networks, spécialiste de la protection des réseaux industriels, pour lequel il existe quatre tendances fortes :

- le nombre croissant d'appareils connectés de l'IoT ;
- la sophistication croissante des cyberattaques ;
- la dépendance accrue à l'égard des services dans le *cloud* et du partage des données ;
- la multiplication des attaques contre les infrastructures critiques et les systèmes de contrôle industriel.

De nombreux documents techniques et d'outils logiciels sont aujourd'hui disponibles sur internet. Le niveau de compétence des cyberattaquants est de plus en plus élevé. Ils sont donc en capacité de cibler des systèmes de plus en plus complexes. Cet outillage a souvent pour source des États. Il a été aussi constaté une prolifération de logiciels pour faire des tests de pénétration, détournés par des attaquants.

Parmi les menaces recensées :

La menace persistante avancée (*Advanced Persistent Threat - APT*)

C'est une cyberattaque prolongée et ciblée par l'attaquant non autorisé accédant au réseau et passant inaperçu pendant une certaine période. L'objectif de l'APT est d'obtenir un accès permanent au réseau, à en surveiller l'activité et à capter des données plutôt qu'à porter atteinte au réseau ou à l'organisation. Les secteurs visés sont plutôt la défense nationale, l'industrie et la finance - les informations sont d'une valeur capitale (propriété intellectuelle, programmes militaires et autres données issues des autorités et des entreprises). Pour éviter d'être détectés, les pirates (*hackers*) utilisent conjointement plusieurs techniques d'attaque comme l'exploitation des vulnérabilités *zero-day*, le hameçonnage ciblé (*spear phishing*) et autres techniques d'ingénierie sociale. Selon Nozomi Networks, les groupes APT s'appuient sur des codes malveillants en vue d'obtenir un accès complet à des systèmes de contrôle de supervision et d'acquisition des données - *Supervisory Control And Data Acquisition* (SCADA) et aux systèmes de contrôle industriel - Industrial Control System (ICS).

Les SCADA sont des systèmes de gestion et de contrôle, à grande échelle, surveillant, gérant et administrant des infrastructures complexes dans des activités aussi variées que le transport, le nucléaire, l'énergie, etc. Ces systèmes connectent des automates, des capteurs, des dispositifs de mesure ou d'analyse, des systèmes de commande et de contrôle, etc., sans oublier les interfaces homme-machine.

Les systèmes de contrôle industriel (ICS) surveillent les processus industriels (distribution, manutention et production de produits), les gèrent automatiquement et en permettent le contrôle humain. Ils se trouvent le plus souvent dans les projets d'extraction (mine, pétrole, gaz et charbon), ainsi que dans les usines, le traitement de l'eau et des déchets, les centrales électriques et le secteur des transports. Ils permettent d'accélérer les opérations, de réagir plus rapidement aux fluctuations et de renforcer la fiabilité.

De même la mise en œuvre des technologies RPA (*Robotic Automatisation Process*) et leur développement devront être réalisés selon des règles de sécurité fiables. Le RPA a de nombreux avantages - le déploiement de très nombreux automates dans le cadre d'un système de gestion intégré ERP (*Entreprise Resource Planning*), la prise de décision rapide, une réduction des erreurs humaines, une réponse immédiate aux incidents impactant des processus critiques, la création d'une réponse automatique à un courrier électronique, etc.

Concernant la sophistication des actions malveillantes, Nozomi Networks observe une forte augmentation des ***wipers*** déployés notamment lors d'attaques ciblées de type APT, des attaques furtives de longue durée, depuis le début de la guerre entre la Russie et l'Ukraine. Parfois utilisés conjointement avec des vers pour se propager sur tout le réseau, les ***wipers*** sont des codes malveillants qui effacent toutes les données enregistrées sur des disques durs ou les rendent inutilisables. L'objectif majeur, dans le cadre de la cyberguerre, est d'empêcher l'ennemi d'accéder à des données critiques ou essentielles à ses activités.

La sécurité des infrastructures industrielles encore trop vulnérable aux attaques

L'European Union Agency for Cybersecurity (ENISA) rapporte qu'il y a un risque accru pour les réseaux de technologie opérationnelle (OT) qui concernent les composants matériels et logiciels pour la détection et le contrôle des équipements industriels (machines-outils, chaînes de production, etc.). Les industries, intégrant de plus en plus de composants informatiques, sont confrontées aux mêmes menaces que les entreprises, mais avec une plus grande complexité pour la gestion de leur sécurité.

Fortinet®, l'un des leaders mondiaux de solutions globales, intégrées et automatisées de cybersécurité, a publié, en juin 2022, son rapport sur l'état des lieux des technologies OT et de la cybersécurité. Si les environnements industriels restent la cible des attaques cybercriminelles (93% des acteurs de l'OT ont subi une intrusion sur les 12 derniers mois et 78 % en avaient enregistré plus de 3), le rapport identifie aussi des vulnérabilités majeures en matière de sécurité industrielle et propose des axes d'amélioration. Tous les secteurs sont concernés : industries pétrolière et gazière, production et distribution d'électricité, aviation, marine, ferroviaire, agro-alimentaire, etc.

La situation est inquiétante car les industriels ne sont pas prêts à affronter ces différentes menaces. 35 % des entreprises interrogées ne savaient pas si leur organisation avait été victime d'un piratage selon le rapport « *The State of OT/ICS Cybersecurity in 2022 and Beyond* » (SANS Institute).

Parmi les vulnérabilités identifiées sur les systèmes d'information industriels, on compte :

- l'absence de gestion des correctifs de sécurité, de l'obsolescence matérielle ;
- l'absence de politique de veille sur les vulnérabilités et menaces ;
- l'insuffisance de politiques réelles d'accès aux systèmes ;
- les mots de passe de configuration figés (constructeur, maintenance, etc.) sur les automates ;
- l'absence de gestion de comptes et de l'authentification ;
- l'absence de politique de gestion des interfaces de connexion, des accès distants ;
- l'utilisation de terminaux nomades non maîtrisés ;
- le défaut ou le manque de maîtrise de la configuration ou l'absence de configurations sécurisées ;
- l'utilisation d'équipements et/ou de protocoles vulnérables et/ou une maintenance non maîtrisée ;
- le défaut de contrôle d'accès physique, de cloisonnement, de télémaintenance ;
- le suivi insuffisant des évènements de cybersécurité ;
- *etc*.

En ce qui concerne les entreprises, selon une étude de Kaspersky, près de 52 % d'entreprises de moins de 2 000 personnes accordent beaucoup d'importance à la cybersécurité. À côté, seuls 35 % des entreprises comptant plus de 5 000 employés avouent en faire autant. Au-delà des problèmes d'implication des dirigeants, le budget fait aussi partie des principaux aléas des entreprises en matière de cybersécurité. Il en est de même pour le manque de formation.

Convergence des univers IT et OT

Aujourd'hui il y a une convergence des réseaux informatiques (IT - *Information Technology*) et industriels (OT - *Operational Technology*) autrefois séparés. Cela a permis de gagner en efficacité, mais cela a augmenté la surface d'attaque. Les industriels ont un défi majeur : assurer la continuité de service, de la chaîne de production ou des automates surveillant un réseau de transport, etc.

Pour les industriels, la situation est très difficile à gérer car les réseaux deviennent de plus en plus complexes. Ces interconnexions deviennent un potentiel maillon faible de la sécurité, par manque d'homogénéité et de manque d'historique précis de maintenance et des modifications apportées tout au long de la période d'activité des systèmes. Cela entraîne une suractivité des *botnets* IoT avec perte de contrôle des machines, des capteurs industriels. Les attaques de DDoS (*Distributed Denial of Service* - déni de service distribué) ont pu entraver l'activité d'un serveur ou d'une ressource web en le submergeant de requêtes.

> *Les botnets sont des réseaux d'ordinateurs ou d'objets connectés contenant un même logiciel malveillant. Une machine infectée reste sous contrôle de l'attaquant qui peut décider de l'utiliser à tout moment pour viser une nouvelle cible à l'insu de l'utilisateur dans l'objectif d'envoyer des pourriels, de diffuser des codes malveillants, de miner de la cryptomonnaie, de lancer des attaques par déni de service distribuées, etc. Ces botnets exploitent toute défaillance du SI ou failles rencontrées.*

La sécurité des technologies opérationnelles (OT) et des systèmes de contrôle industriels (ICS) est un domaine en constante évolution qui nécessite d'adapter continuellement les stratégies de défense pour relever les nouveaux défis

et les nouvelles menaces - tout en maintenant la sécurité et la fiabilité des opérations des installations. En février 2022, l'agence *Cybersecurity and Infrastructure Security Agency* des Etats-Unis (CISA) avait alerté sur la multiplication de ces programmes malveillants (HermeticWiper, CaddyWiper, WhisperGate, etc.) visant des infrastructures ukrainiennes. Ces codes malveillants (utilisés conjointement avec des vers pour se propager sur tout le réseau) effacent toutes les données enregistrées sur des disques durs ou les rendent inutilisables pour empêcher l'ennemi d'accéder à des données critiques ou essentielles à ses activités.

Les vulnérabilités logicielles

Elles permettent la prise de contrôle à distance, sans condition préalable, et avec des procédures automatisées. Les attaquants déposent, sur des millions de machines, des rançongiciels (*ransonware*) capables de chiffrer le contenu d'un disque, mais aussi de se répliquer sur d'autres machines via les réseaux. En cas de non-paiement de la rançon, les données sont publiées. Ce type de manœuvre peut servir des états qui cherchent à discréditer un autre état en divulguant des données confidentielles ou mieux encore de disséminer de fausses informations.

Afin de centraliser l'ensemble des outils nécessaires à la gestion d'une entreprise, un ERP (*Entreprise Resource Planning*) est connecté à la chaîne de production. Une faille de sécurité au niveau de cette application, peut être exploitée par un cybercriminel. En infiltrant tout le réseau informatique, il peut récupérer des données sensibles ou les chiffrer pour exiger une rançon, par exemple, ou pour nuire aux activités de l'entreprise.

Dans ce contexte, des sociétés spécialisées, comme Tenable, craignent une compromission majeure d'un fournisseur SaaS. Une solution SaaS (*Software as a Service* - logiciel en tant que service) est une solution logicielle applicative hébergée dans le *cloud* et exploitée en dehors de l'organisation ou de l'entreprise par un tiers, aussi appelé fournisseur de service qui gère toute l'infrastructure et assure la disponibilité et la sécurité des données et de l'application choisie.

Une pratique qu'il faut proscrire car elle est une source de risques majeurs, c'est la **Shadow IT** : utilisation de systèmes, d'appareils, de logiciels, d'applications et de services informatiques qui n'ont pas reçu l'approbation explicite du service informatique. Elle a connu une croissance exponentielle ces dernières années avec l'adoption d'applications et de services basés dans le *cloud*. Cependant, les risques d'atteinte à la sécurité du système d'information sont certains à cause des biais de fuites de données, de violations potentielles de la conformité, etc.

Une intensification du *phishing*

L'hameçonnage (*phishing* en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe, etc.) et/ou bancaires en se faisant passer pour un tiers de confiance. Des attaques de type *callback phishing* (hameçonnage par rappel) devraient connaître un essor particulier. En effet les pirates en lancent un grand nombre pour tenter de pénétrer dans les réseaux d'entreprise. Une fois dans le réseau, les pirates ont tendance à déployer des rançongiciels. L'hameçonnage par rappel implique généralement un courriel, un appel téléphonique et un faux avis d'abonnement ou de facture. En 2022, en 3 mois, les attaques de *callback phishing* ont augmenté de 625% : usurpation d'identité pour de nombreuses entreprises.

L'internet des objets (IoT)

Dans un environnement général où la cybersécurité est une composante essentielle des réseaux et services, les objets de l'IoT (*Internet of Things*) présentent des vulnérabilités :

- une assez faible sécurité : mot de passe unique et trivial pour toute une série d'objets ; ports série restés ouverts, interfaces radio sans protection, clés secrètes en clair, etc. ;
- un point d'entrée aux systèmes d'information personnels et professionnels ; la multitude de ces objets et leur accessibilité aisée, augmentent la surface d'attaque des réseaux et systèmes ;
- un déploiement d'un grand nombre d'objets élaborés sur une même base avec les mêmes vulnérabilités, les transforment en menace de grande envergure ;
- un grand volume de données personnelles à protéger dans le cadre des règlements ;
- une porte ouverte sur de l'espionnage de domicile par caméra ou assistant vocal, sur des systèmes industriels utilisés pour entraver le fonctionnement d'une usine de production, etc.

Les acteurs publics et privés, industriels et civils, perçoivent de plus en plus l'enjeu de la sécurité de l'IoT aussi bien pour son développement économique qu'au regard de son impact sociétal. Imaginer ce qu'il pourrait se passer dans un hôpital dont des tâches seraient impactées directement par un dysfonctionnement de ces objets connectés, capteurs, etc. : erreur de géolocalisation des lits disponibles, perturbations dans le suivi de patients à distance grâce à des dispositifs connectés mesurant différents indicateurs (taux de glycémie pour les personnes diabétiques, par exemple) ou encore une gestion erronée des stocks de produits médicaux, etc.

Aussi faut-il repenser la sécurité de ces objets depuis leur conception (*security by design/ privacy by design*) jusqu'à leur production certifiée en veillant au respect des législations et de la protection des données en vigueur. Pour répondre à ces enjeux, l'élaboration de technologies fiables et reconnues établiront une base de confiance en vue de garantir l'identité numérique indispensable. Le principe de protection de la vie privée (*security by default*) impose aux entreprises de paramétrer par défaut leurs produits avec les valeurs optimales des paramètres pour assurer la meilleure protection. Tout est préconfiguré de telle sorte que les données ne puissent être pas utilisées dans des buts autres que la collecte annoncée.

Une autre menace pas souvent évoquée est celle relative aux *satellites IoT* (*Internet of Things* ou internet des objets). En effet ils offrent une bien meilleure connectivité pour l'ensemble des objets connectés sur Terre, mais ils sont aussi

très exposés. Ils sont en orbite basse (environ 600 Km à 2 000 Km d'altitude) et leur nombre s'accroît rapidement. Les dizaines de milliards d'objets connectés y ont recours pour se localiser, s'orienter, à travers de multiples applications mobiles. Les systèmes de localisation et de navigation - GPS, Galileo, Beidou, Glonass, etc. - sont ainsi utilisés quotidiennement par les applications mobiles. Ces satellites peuvent aussi servir de solutions de sauvegarde pour les applications nécessitant une résilience efficace. Ces satellites risquent d'être détournés à des fins d'espionnage ou de vol de données de grand volume. Il est donc indispensable que les sociétés les construisant et les entreprises les exploitant s'assurent que le contrôle à chaque phase de réalisation soit effectif et bien dimensionné.

L'externalisation (hébergement, traitement de données, etc.)

L'hébergement de données dans les nuages (*clouds*) est devenu très courant. Les entreprises, les institutions publiques et les particuliers utilisent beaucoup cette technologie. Parfois les données stockées sont délocalisées et relocalisables par l'hébergeur dans un souci d'optimisation et de rationalisation, avec les compétences nécessaires pour mettre à niveau les infrastructures et les sécuriser dans les meilleures conditions annoncées (confidentialité, continuité, suivi de qualité, etc.). Cependant les risques existent comme la captation par des entités hostiles à cause de législations différentes des nôtres et de l'exigence de certains gouvernements d'obtenir un accès total aux données. Les conséquences juridiques sont susceptibles d'être dramatiques : suivant les conditions contractuelles, l'utilisateur peut se trouver, par exemple, empêché d'effectuer la migration désirée de ses données vers un autre prestataire. Les enjeux sont très importants.

Sécurisation de l'Active Directory

L'ANSSI a présenté ses mesures en matière de cybersécurité, dont une importante pour les acteurs critiques comme les opérateurs d'importance vitale (OIV), les opérateurs de services essentiels (OSE), les administrations : la sécurisation de l'Active Directory (AD) dont l'objectif principal est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs. L'AD est défini comme un annuaire répertoriant des éléments de réseaux tels les comptes utilisateurs, les serveurs, les postes de travail, les dossiers partagés, etc. C'est donc un élément critique assurant la gestion centralisée de l'ensemble des permissions sur l'ensemble du système information. L'ANSSI a aussi développé un service ADS (*Active Directory Security*) côté clients pour fournir une aide dans le renforcement de la sécurité. Ainsi il est essentiel de maîtriser les vulnérabilités d'AD et de mettre en œuvre des contrôles d'accès de sécurité et de moindre privilège pour protéger les comptes de domaine et assurer la sécurité de l'écosystème informatique.

4.4 Apport des nouvelles technologies

La *blockchain* (chaîne de blocs)

De nombreux experts prévoient qu'en 2023, la *blockchain* sera de plus en plus souvent utilisée en cybersécurité. Cette technologie de stockage et de transmission d'informations est sans autorité centrale. Elle est constituée d'une base de données contenant l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. L'identification de chaque partie s'effectue par procédé cryptographique ; la transaction est envoyée à un réseau (ou nœud de stockage) d'ordinateurs situés dans le monde entier ; chaque nœud héberge une copie de la base de données dans lequel est inscrit l'historique des transactions effectuées. Toutes les parties prenantes peuvent y accéder simultanément ; le système de sécurisation repose sur un mécanisme de consensus de tous les nœuds à chaque ajout d'informations. Les données sont déchiffrées et authentifiées par des centres de données (ou mineurs). La transaction ainsi validée est ajoutée dans la base sous forme d'un bloc de données chiffrées ; la décentralisation de la gestion de la sécurité empêche la falsification des transactions. Chaque nouveau bloc ajouté à la chaîne est lié au précédent et une copie est transmise à tous les nœuds du réseau. L'intégration est chronologique, indélébile et réputée infalsifiable.

L'automatisation de la cybersécurité

L'automatisation est une des grandes tendances dans les prévisions des acteurs du marché de la cybersécurité. Cependant, une majorité affirme utiliser des systèmes automatisés de détection des intrusions (IDS), mais ces organisations éprouvent des difficultés à adopter un système de prévention des intrusions (IPS) par crainte que des faux positifs provoquent inutilement la mise à l'arrêt de leurs activités. L'utilisation actuelle de l'automatisation est telle que si un moteur automatisé est tout à fait capable de détecter un problème, il n'est pas en mesure de l'identifier.

« Si une plateforme enregistre, mensuellement, des milliards de points de données, parmi eux, mille doivent être analysés manuellement, dont deux seulement constituent probablement des menaces réelles, mais quelqu'un doit tout de même être chargé de l'analyse de ces mille alertes. Le facteur humain existe toujours, malgré les processus automatisés de détection des intrusions ».

Le rôle de l'intelligence artificielle (IA)

En reconnaissant les modèles et les comportements suspects, l'IA est capable de bloquer les activités potentiellement dommageables avant que le mal ne se produise. En outre, la technologie de l'IA crée des environnements sûrs appelés *sandbox* (bacs à sable) où les nouveaux fichiers sont testés pour détecter les dangers potentiels avant d'être ouverts sur les réseaux de votre système. Ainsi, les établissements peuvent détecter rapidement les failles de sécurité et agir en conséquence. L'automatisation des tâches répétitives permet alors d'utiliser le personnel pour des problèmes plus complexes, en fournissant une analyse instantanée des ensembles de données à grande échelle.

Le *machine learning* (apprentissage automatique) est une technique d'intelligence artificielle : apprendre à des machines à prendre des décisions efficaces dans un cadre prédéfini, via des algorithmes nourris par des exemples

(les données de l'apprentissage) sélectionnés par un analyste humain. Pour aller plus loin, le *deep learning* (apprentissage profond) propose des algorithmes permettant à partir d'un jeu de données d'extraire des corrélations et des motifs qu'un humain ne saurait voir. Les algorithmes se perfectionnent au fur et à mesure des nombreux tests effectués.

En situation de défense, les apprentissages sont indispensables aux algorithmes de l'IA, pour des problématiques de détection comportementale (*threat intelligence).* Il s'agit d'apprendre les modes de propagation de virus ou de logiciels malveillants ou ceux de l'exploitation d'une vulnérabilité de corruption mémoire par exemple. Chiffrer un grand nombre de fichiers ou tenter d'accéder à des fichiers systèmes pourrait être considéré comme un comportement anormal et deviendrait donc suspect. Il serait possible de détecter un usage de vulnérabilités *zero-day* (impossible par des solutions de sécurité historiques par signature). L'approche inverse peut aussi être considérée. Cependant la détection est complexe car il faut savoir qu'un algorithme peut être biaisé alors qu'il y aura validation de son comportement au vu des résultats émis : l'attaquant a pu augmenter le bruit de fond, faire ressortir de faux positifs et donc réduire l'efficacité des mécanismes d'apprentissage. L'analyse des preuves est donc primordiale pour être sûr de la pertinence.

En situation d'attaque, le *machine learning* peut être utilisé pour faire du *phishing* efficace (hameçonnage dont le but est de faire cliquer un utilisateur sur un lien malveillant) ou pour faire de la détection et de l'exploitation de vulnérabilités connues. Des outils de recherche IA sont capables de détecter des failles de sécurité et de proposer et décider les solutions pour remédier à l'exploitation frauduleuse de ces failles. Par exemple, concernant l'analyse morphologique, la suite logicielle Gorille© propose une approche de rupture dans la recherche des virus car les techniques actuelles ne sont pas toujours à même, par exemple, de contrer des attaques basées sur l'offuscation plus élaborée (action pour rendre illisible et donc non réplicable le code source d'un programme).

IA on the edge

Parmi les tendances en IA, il y en a au moins une, appelée IA *on the edge*, qui consiste à faire exécuter les traitements par le terminal (smartphone, drone, robot, etc.) muni d'une architecture informatique *ad hoc* et non plus par le *cloud*. En effet l'augmentation de la puissance de calcul des processeurs graphiques est utilisée pour effectuer des calculs de modélisation tensorielle sur divers types de données. Grâce aux nouveaux processeurs équipés d'un grand nombre de cœurs et à leur fonctionnement en parallèle, les applications de traduction en temps réel, de reconnaissance visuelle, d'identification automatique des défauts d'une structure etc. offrent des résultats de plus en plus précis. Cette puissance de calcul permet d'exécuter des modèles d'apprentissage profond pré-entraînés avec une capacité de 1 TFlops (mille milliards d'opérations par seconde) avec une consommation d'énergie minimale et une connexion via un port USB (exemple de la *Neural Compute Stick* sous forme d'une clé USB au profil adapté pour faciliter son refroidissement).

Les technologies quantiques

Des réseaux de communication performants et sécurisés sont essentiels pour les échanges nationaux et internationaux, le développement des Etats, dans tous les secteurs civils et militaires. L'arrivée des technologies quantiques faisant redouter des atteintes à l'intégrité des données, entre autres, aux conséquences dramatiques en période de crise (énergie, approvisionnement, etc.), il est impératif de repenser les systèmes de sécurité et d'anticiper les solutions possibles pour les infrastructures et les systèmes associés, au vu des progrès théoriques et technologiques.

De nombreux projets européens existent, comme par exemple The Quantum Internet Alliance ou l'Alliance pour l'Internet quantique (QIA) lancé en octobre 2018 et achevé en septembre 2021. Il était l'un des 20 projets retenus dans le cadre du Quantum Flagship de l'UE (troisième initiative de recherche et d'innovation à grande échelle de ce type financée par la Commission européenne). Le projet QIA a pour objectif de développer un plan directeur pour un Internet quantique en Europe basé sur l'intrication, en développant, intégrant et démontrant tous les sous-systèmes matériels et logiciels fonctionnels, aboutissant à la première démonstration expérimentale d'une pile réseau entièrement intégrée fonctionnant sur un réseau quantique multi-nœuds. Neuf pays ont participé à ce projet - Allemagne, Autriche, Danemark, Espagne, France, Pays-Bas, Portugal, Suisse, Royaume-Uni. Pour la France, on compte le CNRS, le CEA, VeriQloud, Muquans, My Cryo Firm et Sorbonne Université.

En juillet 2021, les 27 pays membres de la commission européenne (CE) et l'agence spatiale européenne (ESA) ont officialisé la création d'une infrastructure de communication quantique sécurisée de l'UE, l'EuroQCI, initiée en 2019. Son rôle est de protéger les données sensibles et les infrastructures critiques en intégrant des systèmes quantiques dans les dispositifs existants, fournissant ainsi une couche de sécurité supplémentaire basée sur la physique quantique. Il renforce les capacités scientifiques et technologiques de l'Europe en matière de cybersécurité et de technologies quantiques. L'EuroQCI comprendra un segment terrestre reposant sur des réseaux de communication en fibre optique reliant des sites stratégiques au niveau national et transfrontalier, et un segment spatial basé sur des satellites. Il reliera les réseaux nationaux de communication quantique à travers l'UE et assurera une couverture mondiale. La communication par satellite commence à devenir concrète avec l'annonce par l'agence spatiale européenne (ESA), la Commission européenne et la SES (Société Européenne des Satellites, connue pour ses satellites dédiés à la TV, Astra) du développement d'un système de distribution de clés cryptographiques par satellite. Eagle-1 sera le premier système spatial de distribution de clés quantiques en Europe. Il devra démontrer la faisabilité du système de distribution quantique développé dans le cadre du programme Scylight (*Secure and Laser communication technology*) de l'ESA.

La Commission européenne a sélectionné Airbus Defence and Space pour piloter un consortium d'entreprises et d'instituts de recherche. Il est chargé de concevoir un réseau sécurisé de communication quantique couvrant l'ensemble de l'UE dans le cadre d'un projet de EuroQCI (Quantum Communication Infrastructure).

Un premier démonstrateur devra être disponible en 2024, puis un service opérationnel en 2027. Ce consortium, dirigé par Airbus, est composé de Leonardo (second groupe industriel italien - secteur aéronautique et spatial, constructeur d'hélicoptères civils), Orange, PwC France et Maghreb, Telespazio (coentreprise détenue par Leonardo à 67% et par Thales 33%), le *Consiglio Nazionale delle Ricerche* (CNR) et *l'Istituto Nazionale di Ricerca Metrologica* (INRiM).

Afin d'assurer la sécurité des transactions de la vie quotidienne que ce soit dans le domaine de la vie privée ou publique, les données sont cryptées à l'aide de systèmes cryptographiques de type asymétrique ou symétrique.

Cependant, pour faire face aux enjeux stratégiques, deux tendances de cryptographie prennent forme et se développent. Elles concernent les secteurs civil et militaire, les entreprises, les grands groupes industriels ou l'État :

- *la première est la cryptographie quantique* utilisant les propriétés de la physique quantique, particulièrement le principe de l'intrication, pour sécuriser le transport de l'information. Elle permet le partage de clés sur de longues distances avec les futurs répéteurs quantiques. La distribution de clés quantique, *Quantum Key Distribution* (QKD), assure la confidentialité absolue des clés transmises car le niveau de sécurité est garanti par le principe physique. Elle est étudiée depuis de nombreuses années : ses performances et sa fiabilité sont croissantes. Elle est ainsi devenue une technologie à très haut niveau de maturité. C'est l'emploi de photons uniques qui garantit que leur détection et leur copie par un tiers malveillant, soient impossibles, au vu des lois de la physique quantique, sans que le destinataire ait connaissance de cette interception. Mais pour que les industriels puissent intégrer cette technologie, il est nécessaire qu'elle soit rentable avec de véritables garanties de sécurité à long terme.
- *la deuxième tendance est la cryptographie post-quantique*, basée sur les nouveaux concepts mathématiques pour chiffrer les protocoles de communication. Ces nouveaux algorithmes ne font pas appel à des phénomènes quantiques mais ils sont fondés sur des problèmes mathématiques parmi les plus difficiles à résoudre, même pour un ordinateur quantique. Ils sont développés pour contrer les attaques des ordinateurs quantiques et assurer la protection des données stockées civiles ou militaires. Par exemple, le protocole d'échange de clefs, *Supersingular Isogeny Diffie-Hellman* (SIDH) repose sur la difficulté de trouver des chemins dans de très grands graphes d'isogénies entre courbes elliptiques super singulières.

Sources :

- Yannick Fourastier, Ludovic Pietre-Cambacedes, Cybersecurite des installations industrielles : défendre ses systèmes numériques, Toulouse, Éditions Cépaduès, 24 juin 2015, 528 p. ;
- Cybersecurity. Current challenges and Inria's research directions. Ouvrage collectif, INRIA Janvier 2019 ;
- Eunika Mercier-Laurent. Intelligence artificielle 4.0 pour l'Industrie 4.0. 1024 : Bulletin de la Société Informatique de France, Société Informatique de France, 15 avril 2020, pp.127-137 ;
- Jean-Pierre Damiano, Biomimétisme, intelligence artificielle, robotique et applications de l'intelligence en essaim. Cybersécurité et questions d'éthique et de droit. Part.2, IESF Côte d'Azur, 2020, Bull. n°2, p.7-25 ;
- Daniel Ventre, Intelligence artificielle, cybersécurité et cyberdéfense, ISTE, Londres, Septembre 2020, 246 p. ;
- Hugo Loiseau, Daniel Ventre, Hartmut Aden (Eds.), Cybersecurity in Humanities and Social Sciences: A Research Methods Approach, Wiley-ISTE, novembre 2020, 234 p. ;
- Jean-Pierre Damiano, Aperçu des apports des technologies quantiques à la sécurité et à la défense. IESF Côte d'Azur, 2021, Bull. n°4, p.5-25 ;
- Colonel Florian Manet, Industrie 4.0, cheval de Troie de la cybersécurité intégrée au sein de l'aéronautique ? Une opportunité historique à saisir. *in* Sécurité numérique et aéronautique, Regards croisés, Coll. Cyber Cercle, sous la direction de Bénédicte Pilliet. juin 2022, p.79-92 ;
- Anticipation, innovation, collaboration : les trois piliers de la cybersécurité pour Pierre Barnabé (Atos), InCyber, 5 juin 2022 ;
- Cybersécurité : wipers et botnet IoT s'attaquent de plus en plus aux systèmes industriels, selon Nozomi Networks, Usine Nouvelle, Philippe Richard, 13 sept. 2022 ;
- La cybersécurité est au cœur du budget 2023 du gouvernement : quel est le projet ? Bercy Numérique, 6 oct. 2022 ;
- The State of OT/ICS Cybersecurity in 2022 and Beyond, SANS Institute, 28 octobre 2022 ;
- Faker Skandrani, « Comment utiliser l'IA dans la cybersécurité ? » , iotindustriel.com, 22 nov. 2022 ;
- Cybersécurité : les 6 grandes menaces qui pourraient faire de 2023 un enfer, 01net, Eric Le Bourlout, 26 nov. 2022 ;
- Cybersécurité : l'automatisation, au bonheur des attaquants ? Silicon, Clément Bohic, 1er déc. 2022 ;
- Cybersécurité 2023 : nos 7 tendances et prédictions, GlobalSign Blog, Michelle Davidson, 1er déc. 2022 ;
- La sécurité des infrastructures industrielles reste trop vulnérable aux attaques, Techniques de l'ingénieur - Informatique et Numérique, Philippe Richard, 1er déc. 2022 ;
- Cybersécurité : quelles menaces devons-nous craindre en 2023 ? MIT Technology Review, Capital, 3 déc. 2022 ;
- 2023 : Une année sous le signe de la cybersécurité, Journal du Net, Marijus Briedis (NordVPN), 6 déc. 2022 ;
- Les réseaux industriels sont confrontés à de multiples attaques et contraintes, Techniques de l'ingénieur - Entreprises et marchés, Philippe Richard, 6 déc. 2022 ;
- Cybersécurité : les prévisions pour 2023 ne sont pas réjouissantes, L'Usine digitale, Mathieu Pollet, 7 déc. 2022.
- Panorama de la cybermenace 2022, ANSI, janvier 2023.

4.5 Eléments de politique et réglementations

Aux Etats-Unis

Les Etats-Unis ont promulgué le Cloud Act (*Clarifying Lawful Overseas Use of Data Act*) qui, outre *le Patriot Act,* est un ensemble de lois donnant droit aux autorités américaines d'accéder aux données électroniques, stockées en dehors de leur territoire, par les entreprises américaines, dans le cadre de procédures judiciaires. Seuls le président et deux de ses ministres (Procureur général et Secrétaire d'État) peuvent connaître les détails d'une enquête, qui par essence, avec cette disposition, sera parfaitement opaque.

En Chine

Elle a adopté de telles lois sur la protection des données, pour le secteur privé, en les faisant évoluer avec des règles inspirées du RGPD européen. Il est ainsi interdit aux fournisseurs de services en ligne de collecter et de vendre les informations personnelles des utilisateurs. Les entreprises doivent surveiller et sauvegarder leurs données localement et toute publication d'information via des applications de messagerie ou sur les réseaux sociaux, devrait, au préalable, faire l'objet d'une demande d'autorisation du gouvernement. En 2021, la Chine adopte la loi *Personal Information Protection Law* (PIPL) qui vise à réguler la collecte, le traitement et la protection des données. Elle oblige les entreprises à mieux sécuriser le stockage des données personnelles. Elle consacre également le principe de minimisation des données, déjà au cœur du RGPD : *« le traitement des informations personnelles doit avoir un objectif clair et raisonnable et doit être limité à la portée minimale permettant d'atteindre les objectifs du traitement des données ».* Le transfert de données vers des pays tiers est abordé. Contrairement au RGPD, qui s'applique à toute entreprise traitant des données de citoyens européens, le PIPL ne semble concerner en premier lieu que les sociétés domiciliées en Chine. Cette loi impose aux entreprises un cadre bien défini pour gérer les données en fonction de leur valeur économique et leur pertinence pour la sécurité nationale.

Depuis mars 2022, les entreprises chinoises sont obligées de s'assurer auprès des autorités de régulation de la conformité de leurs algorithmes et d'en fournir les détails techniques. Cet été, une publication de l'autorité du cyberespace fait état des dispositions d'usage de ces algorithmes par les grands groupes (Alibaba, Tencent, ByteDance, etc.). *Récemment, Didi, leader du VTC a dû payer une amende d'environ 1,2 Mds € pour diverses infractions en matière de données personnelles.*

En Europe

De nombreux projets, programmes et initiatives existent. L'exposé ci-après n'est pas exhaustif. Pour plus de détails, consulter le site de la Commission européenne.

Au niveau de la gouvernance de l'Union européenne (UE), la cybersécurité n'est pas limitée à la sécurité des réseaux et de l'information, mais elle concerne aussi toutes les activités illicites impliquant l'utilisation de technologies numériques, les actes cybercriminels (attaques par logiciel malveillant, fraude aux paiements, désinformation, etc.) et d'autres secteurs relevant du terrorisme. La Commission européenne a créé des agences spécialisées comme l'ENISA (Agence de l'Union européenne pour la cybersécurité) qui a un rôle d'expertise et de coopération entre les états membres, le *European Cybercrime Centre* - Centre européen de lutte contre la cybercriminalité (EC3) et d'autres.

L'Agence de l'Union européenne pour la cybersécurité, (ENISA), créée en 2004, renforcée par l'adoption du "Cybersecurity Act" européen, le 11 juin 2019, se consacre à la réalisation d'un niveau commun élevé de cybersécurité en Europe. Elle contribue à la cyber politique de l'UE, renforce la fiabilité des produits, services et processus TIC grâce à des systèmes de certification de la cybersécurité, coopère avec les États membres et les organes de l'UE et aide l'Europe à se préparer aux défis de demain.

Le Forum international de la cybersécurité s'inscrit dans une démarche de réflexions et d'échanges visant à promouvoir une vision européenne de la cybersécurité et à renforcer la lutte contre la cybercriminalité.

L'Organisation européenne de cybersécurité (ECSO) est une organisation européenne intersectorielle qui contribue au développement des communautés de cybersécurité et à la construction de l'écosystème européen de la cybersécurité. Elle fédère les secteurs public et privé de la cybersécurité européenne, notamment les grandes entreprises, les PME et les start-ups, les centres de recherche, les universités, les utilisateurs finaux et les opérateurs de services essentiels, les clusters, etc.

En 2016, le Parlement européen et le Conseil de l'Union européenne ont adopté la directive sur la sécurité des réseaux et des systèmes d'information connue sous l'appellation Directive NIS dont le règlement d'exécution a été publié au Journal officiel de l'Union européenne le 30 janvier 2018. Elle présente :

- le renforcement des capacités nationales de cybersécurité ;
- l'établissement d'un cadre de coopération volontaire entre États ;
- le renforcement par chaque État de la cybersécurité d'opérateurs dits de services essentiels (OSE) au fonctionnement de l'économie et de la société (élargissement de la notion d'opérateur d'importance vitale OIV) ;
- l'instauration de règles européennes communes en matière de cybersécurité des prestataires de services numériques dans les domaines de l'informatique en nuage (*cloud*), des moteurs de recherche et places de marché en ligne.

C'est le 25 mai 2018 que l'UE a adopté le règlement général sur la protection des données (RGPD) avec de fortes implications pour les entreprises hors d'Europe, qui traitent des données sur les européens ou qui exploitent des

établissements et des centres de données européens. Chaque personne a le droit d'accéder aux données détenues par une organisation, de les rectifier, de demander leur suppression et de les transférer à une structure concurrente. Il est prévu, évidemment, le droit à l'oubli et le droit d'être informé en cas de piratage des données. Le règlement ePrivacy, associé au RGPD, est relatif à la protection de la vie privée en ligne des citoyens dans laquelle il amène un changement important au niveau de l'utilisation des *cookies*. Les opérateurs de sites *web* ne seraient autorisés à placer des cookies que si les utilisateurs les acceptent expressément.

Dans la réponse de l'UE aux défis en matière de cybersécurité, compte-tenu des tensions géopolitiques croissantes résultant de l'agression russe en Ukraine, entre autres conflits, la politique de cyberdéfense joue un rôle essentiel. Présentée le 10 novembre 2022, elle vise à renforcer les capacités européennes, à stimuler la coopération militaire et civile, à combler les lacunes potentielles en matière de sécurité, à réduire les dépendances stratégiques et à développer les cyber-compétences. Parallèlement, davantage d'investissements sont nécessaires. Plusieurs programmes européens existent : la coopération structurée permanente, le Fonds européen de défense (7,9 Mds €) pour la période 2021-2027, Horizon Europe, l'Europe numérique (programme finançant l'adoption de compétences numériques avancées, de projets d'éducation et de formation, de programmes d'enseignement spécialisé conçus et fournis par des établissements universitaires, des centres de recherche et des entreprises), etc.

La politique de cyberdéfense a donc établi une feuille de route pour les cyber-technologies, fondée sur une évaluation stratégique des points vulnérables les plus critiques, afin de soutenir les investissements stratégiques à long terme des États membres, éventuellement avec le soutien du futur Fonds européen de souveraineté.

L'implémentation de l'authentification forte des consommateurs (SCA - *Strong Customer Authentication*) prévue dans le cadre de la deuxième directive européenne sur les services de paiement (DSP2) a pris un peu de temps. Elle instaure notamment des normes de sécurité plus strictes pour les paiements en ligne pour renforcer la confiance des consommateurs dans les achats en ligne. Cependant la nouvelle directive DSP3 intégrera des technologies de pointe pour l'authentification des clients et la prévention de la fraude faisant suite à DSP2 : les données comportementales et biométriques sont privées - et ne peuvent pas être modifiées en cas de fuite.

Les pays, où les législations sur la protection des données sont obsolètes, devraient commencer à réviser et actualiser leurs législations, avec un effet d'entrainement sur les législations des autres pays. Le nécessaire devrait être fait pour se conformer, du moins au niveau conceptuel, au Règlement général sur la protection des données (RGPD) qui fixe la barre haute.

Pour le cas des signatures numériques, le règlement eIDAS (eIDAS 2.0) concerne principalement les organismes du secteur public et les prestataires de services de confiance établis sur le territoire de l'Union européenne. Il instaure un cadre européen en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence du marché unique numérique. Il établit un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques.

Parallèlement à cela, l'arrivée du portefeuille européen d'identité numérique (*EU digital ID Wallet*) devrait faire évoluer les contours de l'authentification des identités : production des documents d'identité et autres titres sécurisés depuis un smartphone. Il se présente comme un coffre-fort électronique réputé ultrasécurisé permettant aux citoyens de l'UE de stocker leurs documents d'identité et autres titres sécurisés (carte d'identité, diplôme, certificat médical, etc.).

En France

Le Premier ministre, déclarait le 21 février 2014 : la cybersécurité « *est une question d'intérêt majeur et d'intérêt national qui concerne tous les citoyens, tous les Français, et c'est pourquoi il est important que le gouvernement s'engage totalement* ». L'année suivante, une stratégie nationale pour la sécurité du numérique voit le jour. Elle s'appuie sur la formation et la coopération internationale, avec négociations multilatérales au sein de l'ONU et de l'Organisation pour la sécurité et la coopération en Europe (OSCE).

Adoptée en 2016, la directive NIS fut le premier texte législatif européen sur la cybersécurité, imposant notamment des niveaux de cyberdéfense pour de nombreux secteurs critiques. Le décret d'application de la loi de transposition de la directive européenne NIS est publié au *Journal officiel* le 25 mai 2018. Une nouvelle étape d'application de cette directive est franchie avec l'identification d'une première vague d'OSE le 9 novembre 2018. La nouvelle version, NIS2, a été adoptée le 13 mai 2022 par le Parlement et le Conseil européen. Elle concerne les fournisseurs de services publics de communications électroniques, les gestionnaires d'eaux usées et de déchets, les fournisseurs de services numériques, les fabricants de *« produits critiques »*, les services postaux et de messageries ou les administrations publiques. Elle couvre plus largement le secteur de la santé (fabricants de dispositifs médicaux, etc.). Elle promeut le partage d'informations et la coopération dans la gestion des cyber-crises, au niveau national et européen. Elle renforce mettre en place des normes sur les chaînes d'approvisionnement, etc.

La plateforme Cybermalveillance.gouv.fr a été confirmée, début 2017, par l'ANSSI pour venir en aide aux victimes d'actes de cybermalveillance. Elle réunit les acteurs publics et privés de la cybersécurité : représentants de l'État, utilisateurs, prestataires et sociétés de services. D'autres initiatives amènent aussi leurs compétences comme l'Alliance pour la Confiance Numérique (ACN), Tech in France (éditeurs de logiciels), Hexatrust, association regroupant des PME d'édition et d'intégration informatiques, membres de la Fédération des industries électriques, électroniques et de communication (FIEEC).

Le CNRS est copilote, au côté de l'Inria et du CEA, du Programme et équipements prioritaires de recherche (PEPR) en cybersécurité, lancé en juin 2022. Ce PEPR vise à accélérer la recherche fondamentale sur 10 projets portant sur deux grands axes qui font consensus dans la communauté scientifique - la sécurité de l'information et la sécurité des

systèmes. La stratégie nationale d'accélération Cybersécurité décline également plusieurs mesures à destination des entreprises pour favoriser le développement d'innovations de rupture souveraines dans le domaine.

Cette stratégie incite au développement d'approches collaboratives et coopératives entre acteurs de la filière, dynamique dans laquelle le CNRS s'inscrit pleinement. C'est dans ce cadre que le Campus Cyber, inauguré le 15 février 2022, a pour vocation d'être un lieu privilégié de la cybersécurité rassemblant les principaux acteurs nationaux et internationaux du domaine. Ainsi il accueille des entreprises (grands groupes, PME), des services de l'État, des organismes de formation, des acteurs de la recherche et des associations. Le Campus Cyber met en place des actions visant à fédérer la communauté de la cybersécurité et à développer des synergies entre ces différents acteurs. Des Campus territoriaux de cybersécurité sont en cours de développement. À ce jour, plus de 160 acteurs, issus d'une pluralité de secteurs d'activité, ont confirmé leur engagement. Le Groupement de recherche en Sécurité Informatique (GDR SI) regroupe 1300 chercheuses et chercheurs de l'ESR français en Cybersécurité, a pour objectif de partager les connaissances en cyber, de faire dialoguer l'ensemble de l'écosystème et se pose en outil complémentaire du Campus Cyber.

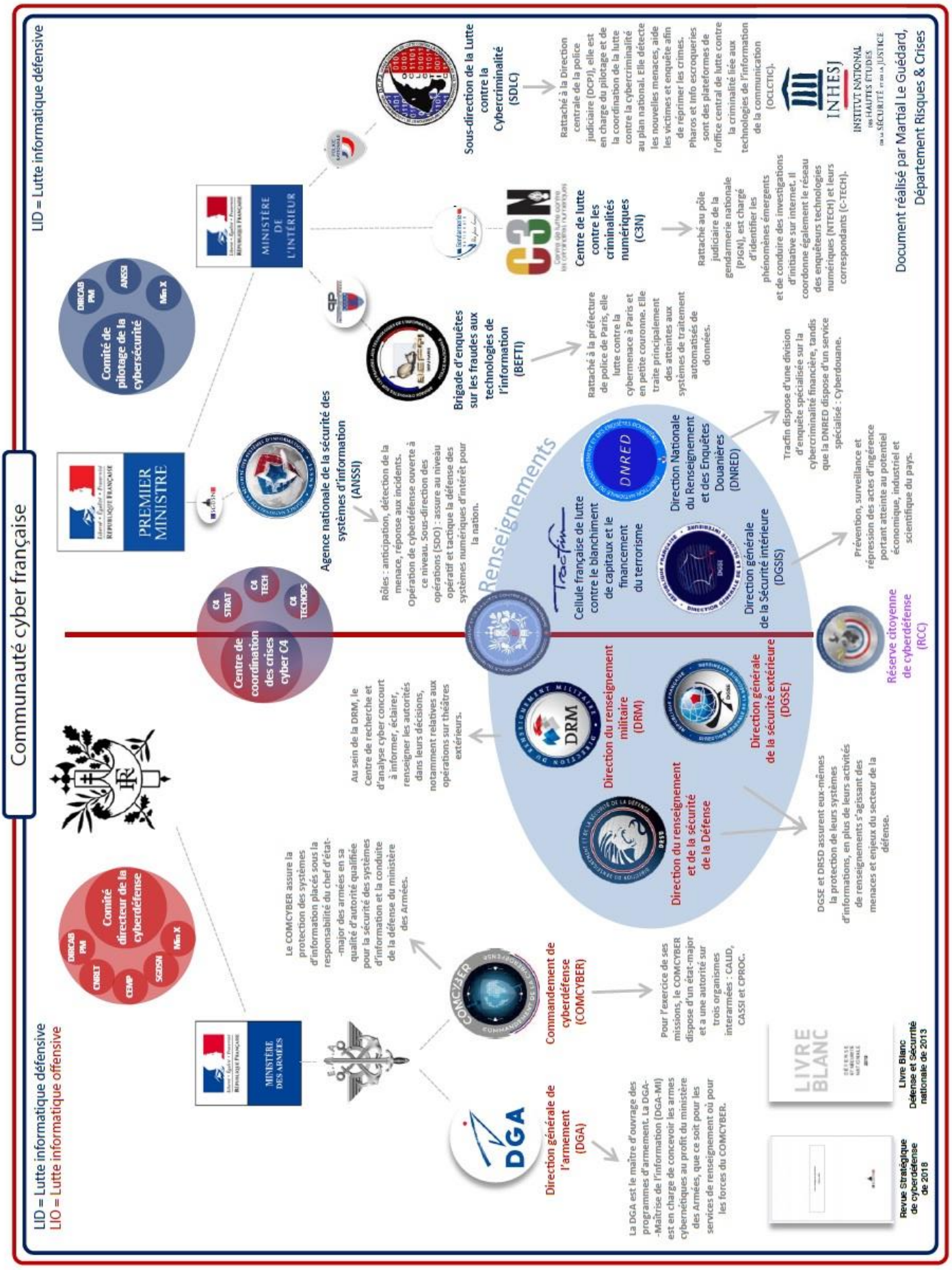
SecNumCloud est une qualification de sécurité proposée par l'ANSSI à destination des opérateurs du *cloud*, qui proposent des services en PaaS (*Platform as a Service*), IaaS (*Infrastructure as a Service*) ou Saas (*Software as a service*). L'objectif est de proposer une approche centralisée plutôt que de laisser les entreprises clientes négocier leurs exigences de sécurité avec chaque prestataire. Un prestataire qualifié SecNumCloud peut donc prouver que son système respecte les bonnes pratiques listées dans le référentiel et que la conformité de son système a été vérifiée par des prestataires d'audit également approuvés par l'ANSSI (les PASSI). Cette offre concerne les entités publiques, les OIV et les OSE. Ces organismes peuvent ainsi externaliser l'hébergement de leurs données, applications et systèmes d'information auprès de partenaires de confiance.

Les enjeux essentiels de la sécurité des systèmes d'information (SSI) d'un laboratoire, par exemple, consistent à protéger et à assurer la disponibilité de ses éléments. Il convient d'identifier ce qui doit être protégé, de quantifier les enjeux, de définir les objectifs de sécurité et d'élaborer une politique de sécurité des systèmes d'information (PSSI). Cependant un tel plan d'actions conduit à des règles qui ne doivent pas entraver la recherche, la compétitivité, les échanges et les coopérations nationales et internationales, le dépôt de brevets, les publications, les congrès, etc. La sensibilisation et la formation des membres du laboratoire aux enjeux de la sécurité sont indispensables.

Pour mémoire, les mesures mises en œuvre tiennent compte de critères déterminants comme :

- La disponibilité : l'information est accessible et utilisable sans faille. L'accès aux services et ressources installés est garanti avec le temps de réponse prévu ;
- L'intégrité : l'information est exacte et exhaustive. Elle ne peut être altérée ou détruite de manière non autorisée, volontairement ou non ;
- La confidentialité : l'information n'est accessible qu'aux personnes ou processus autorisés. Tout accès indésirable doit être bloqué ;
- L'authentification : c'est l'exactitude de l'identité d'une personne, ou d'une machine par exemple, pour maintenir la confiance dans les relations d'échange et de partage (action d'identification) ;
- La non-répudiation : l'information ne peut faire l'objet d'un déni de la part de son auteur ;
- Le contrôle d'accès : seules les personnes autorisées peuvent accéder à l'information ;
- La traçabilité : c'est la garantie que les accès ou les tentatives d'accès sont recensés et que ces traces sont conservées et demeurent exploitables ;
- L'imputation : un tiers ne peut pas s'attribuer les actions d'un autre.

Face à la menace cyber croissante et à un nombre d'attaques toujours plus important, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), le Campus Cyber et le Club de la continuité d'activité (CCA) se sont unis pour organiser REMPAR22, un exercice de simulation de crise cyber de grande ampleur, le jeudi 8 décembre 2022, autour d'un scénario unique créé. Elle a réuni plus de 200 participants, issus de 100 organisations sur tout le territoire national.



Cartographie des acteurs étatiques du cyber en France, Space & Security, Martial Le Guédard (Institut National des Hautes Etudes de la Sécurité et de la Justice - INHESJ), juin 2020

La Direction générale de la sécurité intérieure (DGSI) publie des Flashs « Ingérence économique » à destination des sociétés françaises, des centres de recherche, des entreprises et des industries. Divers sujets sont exposés (risques liés aux audits externes, sécurité des biens immatériels, sécurité informatique, faux profils sur les réseaux sociaux professionnels, etc.). Ils sont argumentés et documentés avec des exemples et des préconisations.

Le dernier Flash#89 publié (Décembre 2022) traite des risques d'accès aux appareils électroniques lors de contrôles aéroportuaires :

En effet, cadres d'entreprise, experts ou encore chercheurs sont amenés à se rendre régulièrement à l'étranger pour rencontrer des partenaires commerciaux, prospecter de nouveaux marchés ou assister à des salons professionnels, des colloques, etc. Dans la majorité des cas, ces déplacements impliquent le transport de supports numériques (ordinateurs portables, tablettes, téléphones portables, etc.). Ces appareils peuvent contenir des données sensibles ou confidentielles comme des informations financières, commerciales ou encore les résultats de travaux de recherche.

La DGSI a constaté une recrudescence tendancielle de démarches intrusives menées à l'égard de dirigeants ou de salariés d'entités stratégiques françaises lors de leurs voyages, plus particulièrement à l'occasion des contrôles aéroportuaires. Justifiés par des motifs d'ordre sécuritaire, ces contrôles peuvent être détournés et exploités à de fins de captation de données ou de piégeage informatique.

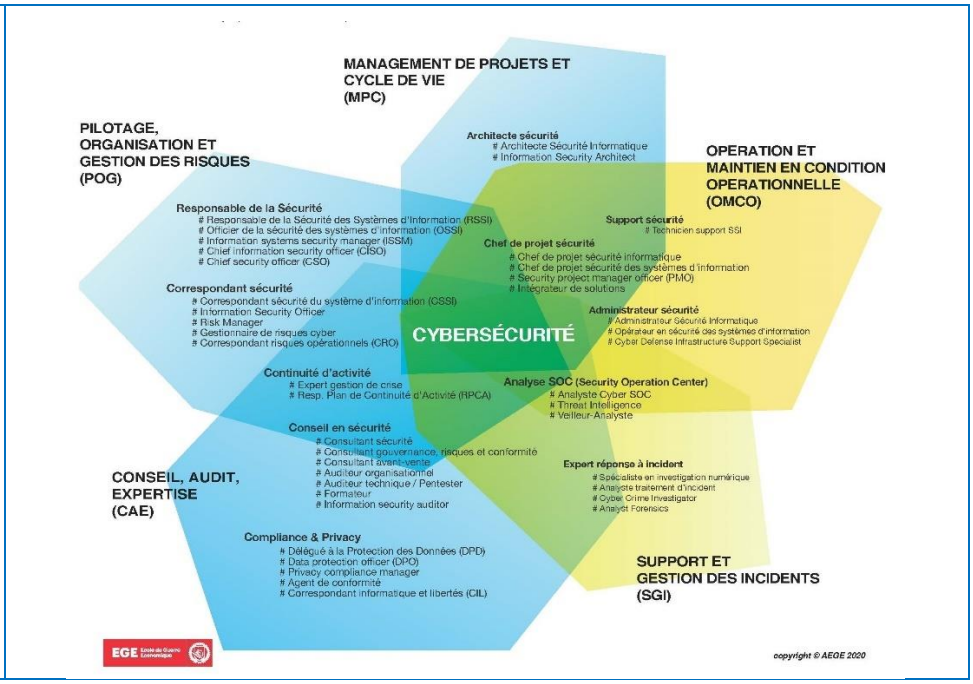
4.6 Les métiers de la cybersécurité

Le marché de la cybersécurité est porteur et connaît une forte dynamique. Selon le rapport 2022 d'études *Security Architect Skill Gap* de Fortinet (expert mondial en solutions de cybersécurité), la sécurité du cloud (57%) et les opérations de sécurité (50%) sont les domaines les plus difficiles à recruter, suivis par les rôles techniques dans le développement des réseaux et des logiciels.

Compte tenu des coûts croissants et tangibles des violations, la cybersécurité devient une priorité pour toutes les organisations à travers leurs conseils d'administration. Par exemple, 90 % des organisations des Etats-Unis discutent de la cybersécurité avec leur conseil d'administration et 77 % de ces conseils recommandent une augmentation des effectifs dans l'informatique et la sécurité. Il en est de de même en Inde et en Chine où, compte tenu du nombre élevé de violations, 92 % des conseils d'administration indiens et 100 % des conseils d'administration chinois votent les mêmes recommandations.

Les entreprises et les institutions publiques cherchent des équipes de sécurité aux compétences techniques et relationnelles pertinentes. Cependant elles devront s'engager dans une approche architecturale à la sécurité, au vu des menaces de plus en plus sophistiquées et la transformation numérique en cours.

Le Club Cybersécurité de l'AEGE et l'Ecole de Guerre Economique publient la « Cartographie des métiers de la Cybersécurité » (2020). Il apparaît deux groupes de famille : l'un orienté management (en bleu) et l'autre orienté ingénierie et technique (en jaune).



4.7 Perspectives

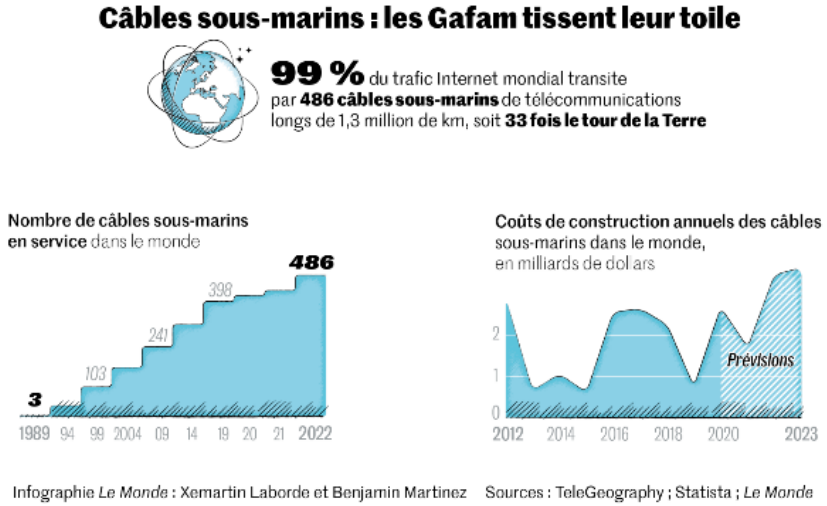
Dans les conclusions du rapport du Global Risks Perception Survey (GRPS 2022), il est indiqué, entre autres constats sur l'inaction climatique, que c'est l'inégalité numérique qui est une menace imminente pour le monde, alors que 3 milliards de personnes ne sont pas connectées.

Le continent européen est un territoire privilégié pour le développement des cybermenaces : la taille de la surface d'attaque (structures gouvernementales, entreprises) offre des opportunités aux cybercriminels. L'Europe est à la fois le berceau d'entreprises prêtes à payer des rançons et un puissant symbole du monde occidental - justifiant des attaques basées sur l'idéologie. Elle est le lieu d'aspirations politiques qui peuvent provoquer des crises sociétales, économiques, politiques et territoriales, lesquelles peuvent être utilisées comme leviers de déstabilisation par des groupes de cyberattaquants. Elle compte des pôles d'excellence scientifiques, techniques, financiers, etc. (académiques et industriels). Ses PME et startups sont de tout premier plan à l'international : elles sont donc cibles permanentes de la cybercriminalité organisée voire de l'espionnage industriel.

Selon un récent rapport de commission du Sénat à propos de la souveraineté économique, compte-tenu de la perte d'autonomie de la France, certains faits sont mis en exergue :

- en Europe, près de 99% des câbles sous-marins de communication sont contrôlés par les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) ;

  Selon un article du Monde, en moins de dix ans, Alphabet (Google, YouTube, etc.), Meta (Facebook, Instagram, WhatsApp, etc.), Amazon et Microsoft ont réussi à construire de très nombreux câbles de communication et se retrouvent donc propriétaires de ces supports, à la place des grands opérateurs internationaux de télécoms classiques. Le groupe français Alcatel Submarine Networks (ASN), premier fabricant européen de câbles sous-marins de fibre optique, estime que 70 % des projets mondiaux actuels, notamment transpacifiques et transatlantiques, sont supportés par ces géants du web



  TeleGeography offre la cartographie des câbles sous-marins de fibre optique - certains offrent un débit de 1,92 Pbps (petabits/s). On en compte 486 faisant transiter 99% des données numériques mondiales.

- notre dépendance aux matières premières et terres rares est trop forte vis-à-vis des pays asiatiques entre autres ;
- nos compétences industrielles, scientifiques, etc. ne sont pas renouvelées suffisamment. Près d'un tiers des employés de l'industrie partiront à la retraite d'ici à 2030 et 50% des emplois sont en tension - dans la mécanique ou ingénierie, par exemple.

Pour faire face aux divers types de menace (tentatives de déstabilisation, cyber-intrusions, vols ou détournements d'informations stratégiques, etc.), à des déficits en matière d'ingérence et de vigilance, à la diminution des moyens défensifs, il faut se doter de réels moyens, pas seulement financiers : le manque dramatique de main-d'œuvre qualifiée pose un réel problème.

Selon l'ANSSI, la crise cyber devient systémique. Les analyses montrent clairement une exploitation massive de vulnérabilités dites *zero-day*, une augmentation réelle de divulgation des données, de récupération de données d'authentification permettant aux cyberattaquants d'augmenter leurs capacités offensives, de même que les chaînes d'approvisionnement de la *supply chain* sont de nouvelles cibles au même titre que les entreprises de services numériques (ESN), etc. Durant la crise sanitaire, 60 % des organisations ont adopté un mode de travail hybride en 2022. Les *clouds* ont permis une flexibilité accrue pour les utilisateurs. Cependant, les enjeux de garantie de la sécurité des informations, du maintien de la confiance, sont bien présents.

Que ce soit dans le milieu industriel ou académique, le risque zéro n'existe pas et il faut se préparer à être la cible d'une cyberattaque réussie. Il s'agit donc de bien connaître les enjeux. Les directives de sécurité numérique doivent être pragmatiques, opérationnelles et réalistes pour mener à bien la mise en place de dispositifs adaptés. Face à une cyberattaque, la résilience des dispositifs doit être effective : les retours d'expérience techniques et opérationnels ont toute leur importance. C'est durant les phases de formation, de simulation, de situation, etc. que les réponses possibles sont étudiées, élaborées : ce n'est pas en temps de catastrophe que l'on va pouvoir rapidement inventer des réponses.

Une cybersécurité opérationnelle doit générer une réflexion stratégique globale, tester en permanence l'ensemble de ses infrastructures face à tout type d'attaques, anticiper toutes les situations, même les plus improbables, pour assurer la robustesse des cyberdéfenses. Le caractère de confiance doit être établi avec les partenaires et sans cesse analysé pour éviter des crises d'ampleur avec des effets domino en cas d'attaque. Il faut anticiper et être prêt à gérer sa communication de crise cyber.

Selon les propos de Pierre Barnabé, chef du *big data* et de la cybersécurité chez Atos (leader international de la transformation digitale), rapportés par InCyber, trois enseignements sont essentiels pour assurer la cybersécurité d'un grand événement, valables aussi pour une entreprise ou un particulier : anticipation, innovation, collaboration. Pour faire face à des cyberattaques toujours plus complexes, il faut investir dans l'innovation, en particulier l'IA et la robotisation : les cybercriminels investissent massivement en R&D, en recrutant les meilleurs experts dans les meilleures universités.

L'acquisition de nouvelles compétences, toutes technologies confondues, en consolidant nos acquis scientifiques et techniques est indispensable afin de se maintenir dans le peloton de tête des nations et d'obtenir des avantages concurrentiels dans les domaines applicatifs civils et militaires. La France doit poursuivre sa stratégie de cyberdéfense et de cybersécurité, continuer à soutenir l'innovation en y associant fortement les secteurs public et privé.

Quelques pistes à suivre :

- investir à bon escient ;
- anticiper les menaces futures ;
- rehausser le niveau de défense ;
- réévaluer la sûreté et la sécurité ;
- maîtriser la sécurité des systèmes d'information ;
- mener des réflexions d'ordre stratégique et technologique ;
- réexaminer la liste des technologies-clefs et leur potentiel ;
- intégrer l'intelligence économique à tous les niveaux ;
- renforcer considérablement sa cyber-résilience ;
- collaborer, échanger ;
- sensibiliser, former, simuler, analyser les retours d'expérience.

Sources :

- Global Risks Report 2022, 11 janvier 2022 ;
- Anticipation, innovation, collaboration : les trois piliers de la cybersécurité pour Pierre Barnabé (Atos), InCyber, 5 juin 2022 ;
- Cinq plans pour reconstruire la souveraineté économique, Rapport d'information de Mmes Sophie Primas, Amel Gacquerre et M. Franck Montaugé, fait au nom de la commission des affaires économiques n° 755 (2021-2022) - 6 juillet 2022 ;
- De la crise cyber à la crise systémique - conclusion par l'ANSSI, Publications du Clusif, 24 octobre 2022.

4.8 Un petit quiz !

1. La cybersécurité

L'État est responsable de la cyberdéfense et garant de la cybersécurité. Quelles sont les actions recommandées pour la recherche ?

A.- Protéger le potentiel scientifique et technique des entités y compris les partenariats
B.- Conserver la politique actuelle de sécurité sans anticipation
C.- Élaborer un écosystème de confiance
D.- Mettre en œuvre une politique adaptative
E.- Assurer la sensibilisation, la formation et développer les cursus supérieurs en IES, en cybersécurité, etc.

3. La sécurité économique et numérique

Quelle menace a une origine interne dans le cas d'une entreprise ou d'un laboratoire ?

A.- Exportations de biens à double usage
B.- Exploitation via les réseaux sociaux
C.- Visites mal encadrées
D.- Contrats de sous-traitance sous évalués

2. Les conséquences de vulnérabilités non détectées au sein de systèmes d'information peuvent être très graves : quelles sont-elles ?

A.- Gain de productivité
B.- Perte de maîtrise des technologies
C.- La baisse de la compétitivité
D.- Perte d'image et de confiance
E.- Destruction d'emplois

4. Quelles sont les causes les plus fréquentes des vulnérabilités observées ?

A.- Absence de séparation des usages entre utilisateur et administrateur des réseaux
B.- Ouverture excessive d'accès externes incontrôlés au S.I. d'information (nomadisme, télétravail, etc.)
C.- Absence de surveillance des systèmes d'information
D.- Politique de chiffrement avec des procédés fiables
E.- Sensibilisation et formation insuffisantes face aux menaces

Réponses :
1. A,C,D,E / 2. B,C,D,E / 3. C / 4. A,B,C,E

Autres sources à consulter

- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
- Alliance pour la confiance numérique (ACN)
- Centre National de la Recherche Scientifique (CNRS)
- Cercle européen de la sécurité et des systèmes d'informations (CESSI)
- Chambre de commerce et d'industrie (CCI)
- Cité des Sciences et de l'Industrie
- Club des Experts de la Sécurité de l'Information et du Numérique (CESIN)
- Club Informatique des Grandes Entreprises Françaises (CIGREF)
- Club de la Sécurité de l'Information Français (CLUSIF)
- Commission Européenne
- Commission Nationale de l'Informatique et des Libertés (CNIL)
- Compagnie nationale des conseils en propriété industrielle (CNCPI)

- *Computer Emergency Response Team* du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR)
- Confédération générale des petites et moyennes entreprises (CGPME)
- CyberEdu
- Cybermalveillance.gouv.fr
- Délégation générale des entreprises (DGE)
- Direction générale de la sécurité intérieure (DGSI)
- La Direction interministérielle du numérique (DINUM)
- Directions régionales de l'économie, de l'emploi, du travail et des solidarités (DREETS)
- Ecole de guerre économique (EGE)
- École européenne de l'intelligence économique (EEIE)
- Emergency Response Team (CERT-FR)
- Agence européenne pour la cybersécurité (ENISA)
- ENtreprises DEfense & Relations Internationales (ENDERI)
- Europa (statistiques européennes)
- Fédération Française de la Cybersécurité
- Flash DGSI
- France Cybersecurity (Label lié aux produits et services de cybersécurité)
- Gendarmerie nationale
- Groupement français de l'industrie et de l'information (GIFI)
- Hexatrust (Club de PME et ETI françaises innovantes, sécurité des systèmes d'information et de la cybersécurité)
- inCyber, média de la communauté cyber / Forum International de la Cybersécurité (FIC)
- Institut national de recherche en sciences et technologies du numérique (INRIA)
- Institut des hautes études de défense nationale (IHEDN)
- Institut européen des sciences avancées de la sécurité (IESAS)
- Institut national de la propriété industrielle (INPI)
- Mouvement des entreprises de France (MEDEF)
- Nouvelle France industrielle
- Observatoire des métiers du numérique, de l'ingénierie, du conseil et de l'évènement (OPIIEC)
- Observatoire de la sécurité de l'internet des objets (OSIDO)
- Observatoire de la sécurité des systèmes d'information et des réseaux (OSSIR)
- Observatoire de l'intelligence économique français (OIEF)
- Observatoire des sciences et des techniques (OST)
- Organisation de coopération et de développement économiques (OCDE)
- Portail IE
- Règlement général de protection des données (RGPD)
- Sécurité informatique
- Service de l'information stratégique et de la sécurité économiques (SISSE)
- Guide cybersécurité des systèmes industriels, Clusif, février 2021
- Sécurité de l'Internet des Objets - Introduction aux principaux risques et approches de sécurisation, Clusif, 2022
- La cybersécurité pour les TPE/PME en 13 questions, Guide édité par l'ANSSI, v2.0, octobre 2022
- ENISA Threat Landscape 2022, ENISA, novembre 2022

- 01net.com
- Archimag
- Industrie et Technologies
- Journal du Net
- lebigdata.fr
- Numerama
- Pour la Science
- Universalis
- Usine Digitale
- Usine Nouvelle
- Veille Mag
- Wikipédia
- *etc.*

Publications IESF CA (du même auteur) à consulter :

- Matières premières, métaux critiques, terres rares : contexte international et enjeux. Bull. n°2, p.12-30 (2022) ;
- Stockage d'énergie électrique : un regard sur les enjeux et les défis technologiques. Bull. n°1, p.10-22 (2022) ;
- Aperçu des apports des technologies quantiques à la sécurité et à la défense. Bull. n°4, p.5-25 (2021) ;
- Les technologies quantiques. Contexte et enjeux, applications et perspectives. Bull. n°2, p.8-29 (2021) ;
- De la 5G à la 6G : contexte et enjeux ! Bull. n°4, p.13-23 (2020) ;
- Biomimétisme, intelligence artificielle, robotique et applications de l'intelligence en essaim. Cybersécurité et questions d'éthique et de droit. Part.2, n°2, p.7-25 (2020) ;
- Réflexions sur les enjeux de l'IA et les questions d'éthique. Bull. n°3, p.2-7 (2019) ;
- Les laboratoires de recherche et la sécurité numérique. Part.1&2, Bull. n°2, p. 3-5 / Bull. n°3, p. 5-7 (2018).

Jean-Pierre DAMIANO
Ancien ingénieur de recherches (Université Côte d'Azur CNRS)
Membre IESF-Côte d'Azur et URSI-France
jean-pierre.damiano@univ-cotedazur.fr

5. Jeu mathématique et distraction astronomique

Par J.P. Rozelot

Cette excellente photographie, extraite d'une séquence vidéo, a été prise à Antibes, par D. Huber, membre du Groupement Astronomique Populaire de la Région d'Antibes (GAPRA) le 11 septembre 2022. C'est le passage d'un avion devant la lune en direction de l'aéroport de Nice. Photographie prise avec un Canon 90D équipé d'un tamron 400 mm et doubleur de focale ; mode vidéo 4k 25fps, pour les spécialistes. Voir : https://youtu.be/GdJm6wqYUGs (passer l'annonce).

En supposant qu'il s'agit d'un AirBus A320 dont la longueur est 38 m, à quelle distance est-il par rapport au point de prise de vue de la photo ? Que peut-on en déduire ?

Réponse par Pierre Chessac, membre du GAPRA :

Le diamètre angulaire moyen de la Lune est 31' d'arc pour une distance moyenne de 384 400 km. D'après la photo, le diamètre angulaire de l'avion est 19' d'arc (mesuré). On en déduit donc sa distance par rapport au point de prise de photo : de l'ordre de 6,9 km. Cela le placerait à mi-chemin entre le phare d'Antibes et l'emprise de l'aéroport. C'est ce qu'a confirmé le photographe.

L'avion va se poser face au vent venant d'Italie, sur la piste orientée à 043°, qui devrait grosso modo correspondre à l'azimut de la Lune à ce moment-là. Il a donc contourné le cap d'Antibes et est quasi perpendiculaire à la piste lors de la prise de vue : on voit que les deux winglets en bout d'aile ne sont pas à la même hauteur, avant de virer pour s'aligner. Bizarrement, on ne voit pas ses phares et il n'a pas le nez en l'air.

6. Jeu mathématique

L'hirondelle et l'escargot

Quelle sera la distance parcourue par l'hirondelle de Bêtaville en direction d'Alphaville ?

Un escargot part d'Alphaville à la vitesse de 1 km/h pour se rendre à Bêtaville, distante de 21 kilomètres. Dans le même temps, une hirondelle part de Bêtaville en direction d'Alphaville, à la vitesse de 30 km/h. Dès que l'hirondelle atteint la position de l'escargot, elle fait demi-tour. Arrivée à Bêtaville, l'hirondelle fait à nouveau demi-tour en direction de l'escargot et ainsi de suite. Sachant que le chemin emprunté par les deux animaux est la ligne droite entre les deux villes, quelle distance aura parcouru l'hirondelle quand l'escargot atteindra Bêtaville ?

© Pitsch, Pixabay, DP

Quelle sera la distance parcourue par l'escargot ?

Hervé Lehning Normalien et agrégé de mathématiques, il a enseigné sa discipline une bonne quarantaine d'années.

7. Jeu mathématique : Solutions du bulletin N°4 de 2022

Si Perrette n'avait pas cassé son pot au lait...

Jean de La Fontaine était poète mais guère mathématicien si bien que, dans sa fable sur la laitière et le pot au lait, il a omis quelques détails.

Perrette a un pot rempli de huit litres de lait et deux pots vides de cinq litres et de trois litres respectivement. Un quidam lui demande de lui fournir un litre de lait. Comment peut-elle faire en n'utilisant que ces trois pots ?

La laitière et le pot au lait

Perrette, sur sa tête ayant un pot au lait,
Bien posé sur un coussinet,
Prétendait arriver sans encombre à la ville.
Légère et court vêtue, elle allait à grands pas,
Ayant mis ce jour-là, pour être plus agile,
Cotillon simple et souliers plats.

Notre laitière, ainsi troussée,
Comptait déjà dans sa pensée
Tout le prix de son lait; en employait l'argent;
Achetait un cent d'œufs; faisait triple couvée;
La chose allait à bien par son soin diligent.

— « Il m'est », disait-elle, « facile
D'élever des poulets autour de ma maison;
Le renard sera bien habile
S'il ne m'en laisse assez pour avoir un cochon.
Le porc, à s'engraisser, coûtera peu de son;
Il était, quand je l'eus, de grosseur raisonnable;
J'aurai, le revendant, de l'argent bel et bon.
Et qui m'empêchera de mettre en notre étable,
Vu le prix dont il est, une vache et son veau
Que je verrai sauter au milieu du troupeau? »

Perrette, là-dessus, saute aussi, transportée :
Le lait tombe; adieu veau, vache, cochon, couvée.
La dame de ces biens, quittant d'un œil marri
Sa fortune ainsi répandue,
Va s'excuser à son mari,
En grand danger d'être battue.

Le récit en farce en fut fait;
On l'appela *le Pot au lait*.

LA FONTAINE.

Réponse :

Appelons les trois pots A, B et C. Au départ, ils contiennent 8, 0, 0 litres. Partant de cet état initial, nous transvasons d'abord le pot A dans le B pour obtenir 3, 5, 0 et ainsi de suite selon le tableau :

Action / Etat	A (8 litres)	B (5 litres)	C (3 litres)
Etat initial	8	0	0
A => B	3	5	0
B => C	3	2	3
C => A	6	2	0
B => C	6	0	2
A => B	1	5	2

À la fin, nous obtenons un litre dans le pot A.

La solution proposée demande 5 transvasements, il existe des solutions n'exigeant que 4 transvasements comme plusieurs l'ont remarqué. En voici une où on obtient 1 litre en C :

A -> C, C -> B, A -> C et C -> B.

La question qui se pose alors est : existe-t-il des solutions en moins de transvasements ? Il est assez clair qu'on ne peut la réaliser en 1 ou 2 transvasements, la question ne se pose que pour 3 transvasements. Pour montrer que c'est impossible, il suffit de construire l'arbre de toutes les possibilités, ce qui est fastidieux.

Hervé Lehning Normalien et agrégé de mathématiques, il a enseigné sa discipline une bonne quarantaine d'années.

8. Sudoku

Complétez la grille avec les chiffres manquants, sachant que chaque colonne, chaque ligne et chacun des neuf carrés doit contenir **une seule fois tous les chiffres de 1 à 9**

La solution sera donnée dans le prochain bulletin

				6	9			
	2	7				4		
					8			7
9		2					3	
7			4	5				
4		3					6	
					1			5
	1	5				2		
				3	2			

Solution du Sudoku du dernier bulletin

2	6	4	3	1	8	9	7	5
9	8	7	5	4	6	1	2	3
1	3	5	9	7	2	4	8	6
3	2	6	7	9	4	8	5	1
8	5	9	1	6	3	2	4	7
4	7	1	8	2	5	6	3	9
5	4	3	6	8	9	7	1	2
6	1	2	4	3	7	5	9	8
7	9	8	2	5	1	3	6	4

9. Sur votre Agenda

Dates	*Sujets / événements*	*Lieux*	*Organisation*
2 mars 2023	Conseil d'administration IESF CA	Hôtel Omega Sophia	IESF CA
6 Avril 2023	Assemblé Générale Ordinaire IESF CA	Hôtel Omega Sophia	IESF CA

10. Cotisations 2023

ADHÉSION – COTISATIONS 2023 AUX IESF COTE D'AZUR

Cette cotisation vous permet de participer à la formation de notre jeunesse avec le projet « Promotion des Métiers de l'Ingénieur et du Scientifique » PMIS dans les collèges et les lycées, de recevoir notre bulletin trimestriel, d'accéder aux informations sur les activités, conférences et visites organisées par l'IESF Côte d'Azur.

Nous ne pouvons faire fonctionner notre association sans votre aide.

- Pour les membres individuels (actifs et retraités), elle s'élève à 65 €, avec une réduction d'impôt de 66%.
- Pour les groupes régionaux, elle s'élève à 5,40 € par membre cotisant.
- Payer par carte bancaire en cliquant sur le lien suivant : Payer sa cotisation 2023 sur HelloAsso
- Payer par carte bancaire votre cotisation sur HelloAsso en scannant ce Qrcode
- Ou établir un chèque à l'ordre d'IESF Côte d'Azur
- Ou par virement interbancaire : IBAN FR76 1460 7003 3434 0190 9537 082

Merci.

Si vous ne l'avez déjà fait, il n'est pas trop tard pour devenir membre adhérent des Ingénieurs et Scientifiques de France de la Côte d'Azur (IESF-CA). Il vous suffit de retourner le bulletin ci-dessous accompagné de votre cotisation pour cette année, à l'adresse :

IESF-CA - Polytech'Nice-Sophia Site Templiers 930 route des Colles - BP 145

06903 - Sophia Antipolis Cedex

NOM : ……..…….. Prénom :……..

Ecole / Université : ……..... Adresse : ……..

Code Postal ……Ville: …… Courriel : ……..

Tous nos Bulletins sont disponibles sur le site d'IESF-CA : coteazur.iesf.fr

Conformément à la loi informatique et liberté du 06/01/1978 (art.27), vous disposez d'un droit d'accès et de rectification des données vous concernant. Si vous souhaitez modifier vos coordonnées ou si vous ne désirez plus recevoir de messages électroniques de cet annonceur, envoyez un mail aux IESF-CA :

contact-coteazur@iesf.fr

Responsables des groupes régionaux, faites-nous part des manifestations que vous organisez. Nous les publierons sur le site IESF Côte d'Azur (IESF-CA) pour en informer tous nos adhérents et sympathisants.

Article 18 du Règlement Intérieur : L'Association n'est pas responsable des opinions de ses membres, même dans ses publications.

Siège : Espace Associations Nice Garibaldi - SIRET 810 124 982 000 10

Adresse Postale : IESF-CA Polytech'Nice-Sophia - Site Templiers

930 route des Colles BP 145 -- 06903 – Sophia Antipolis Cedex

Site : **coteazur.iesf.fr** (**www.iesf-ca.fr**) Compte Twitter **: @IESF_CA** - Email : **contact-coteazur@iesf.fr**

Page Facebook : **facebook.com/iesfca/**