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

BULLETIN

2025 – N°2

SOMMAIRE

1. Editorial

Et voilà ! Vous avez entre vos mains le dernier bulletin IESF en Côte d'Azur ! Ce numéro vous donne un aperçu de nos dernières activités, notamment la Journée Nationale de l'Ingénieur (un grand merci à J.M. Morin) et notre AG, un moment toujours fort pour une association.

N'oubliez pas de visiter notre site, iesf-ca.fr, régulièrement mis à jour grâce à la diligence de P. Quirin.

N'oubliez pas votre cotisation, là c'est A. Giulieri qui vous remercie !

N'oubliez pas de participer à nos visites ; lors de la dernière en date, à la bastide Rouge, à Cannes, nous avons accueilli des membres des amicales X et CentraleMed. Merci à J.B.Titz.

N'oubliez pas de faire de la promotion pour les métiers de l'ingénieur, participez aux salons et forums ! Merci à J.L. Droulin et tous les membres qui l'accompagnent dans ces tâches chronophages.

N'oubliez pas nos amis IPF, actifs de Monaco à Marseille. Merci à B. Leiceaga et G. Valastro, qui répondent toujours à nos sollicitations.

Merci à tous les auteurs d'articles qui nourrissent nos bulletins. Merci à tous les membres du bureau, du Conseil d'administration, aux présidents des groupements d'alumni locaux, qui nous accompagnent, au directeur de Polytech Nice-Sophia qui nous héberge, ainsi qu'aux élus qui nous soutiennent, notamment ceux (ou celles) du Sénat, du Département, de la Métropole et des agglomérations qui nous aident.

N'oubliez pas de lire l'article de J.P. Damiano dans ce bulletin, en retour de sa conférence lors de l'AG, qui nous a brossé un tableau géopolitique/stratégique de la Méditerranée (et au-delà). Je rêve d'une association vivante des écoles d'ingénieurs du pourtour du bassin méditerranéen. Rendez-vous compte de ce que pourraient faire des jeunes ingénieurs issus d'écoles, parfois antennes des nôtres, du Maroc à l'Egypte, de l'Espagne au Liban, passant par la Grèce, la Turquie, et autres pays. Rendez-vous compte de ce que pourraient faire ces jeunes pour bâtir la paix dans ces régions qui partagent un passé historique commun ! Une association existe, il n'appartiendrait qu'à eux de la faire vivre !

N'oubliez pas de nous soutenir !

Nos activités sont nombreuses, rejoignez-nous pour partager ensemble des valeurs de l'ingénieur-humaniste que je défends.

Jean-Pierre ROZELOT

Président IESF-CA

2. Journée Nationale de l'Ingénieur (JNI) organisée par IESF en Côte d'Azur le 3 mars 2025

Chaque année, à l'occasion de la journée mondiale de l'Ingénieur, l'UNESCO appelle à une mobilisation accrue auprès du public et de la presse, pour promouvoir le rôle pivot de l'ingénieur dans le développement technique et économique, de nos sociétés, dans un souci de répondre à des objectifs non pas forcément de croissance, mais aussi de bien-être collectif.

Cette journée est célébrée depuis 2020 dans le monde entier le 4 mars (ou autour du 4 mars), chaque pays décidant de la formule la plus adaptée. En France, IESF prend part à cet événement en s'attachant à défendre le progrès, à mettre en relief l'innovation, l'industrie et plus généralement l'entreprise, et, à promouvoir les métiers de l'ingénieur.

Dans cet esprit, IESF-Côte d'Azur (IESF-CA) organise depuis de nombreuses années des conférences pour célébrer des réussites sur notre territoire (l'an passé l'IA au service du cancer du poumon au travers de programmes locaux universitaires et industriels) ou pour mettre en avant des actions d'avenir liées aux progrès de l'ingénierie (le programme Stratobus de Thalès par exemple).

Cette année, IESF-Côte d'Azur s'est associé pour cet évènement avec Telecom Valley, animateur azuréen du numérique au service des ingénieurs sophiapolitains, en proposant une conférence sur les jumeaux numériques donnée le 3 mars par **Jean-Michel Morin**, « Senior Director Executive Communication » de Dassault Systèmes, intitulée « *La Virtualisation Scientifique : L'Innovation au service d'un monde plus durable et plus humain* ».

Autour de ce sujet, deux autres conférences ont été données, par

- **Arnaud Mistre**, expert au sein de la direction « Technologies de l'information » du CSTB, sur les cas d'usage de numérisation du bâtiment (Voir enregistrement sur https://youtu.be/5Z6yeaVkicc)
- **Florian Pourcel**, ingénieur génie industriel INPG, Président chez sWartr (Make your warehouse smarter) qui a évoqué le "Digital Twin – Virtual Serving the Real!" (Voir enregistrement sur https://youtu.be/JAqbcig3pv0).

RESUME DE LA CONFERENCE DE J.M. MORIN.

« *Révéler l'invisible, explorer l'inconnu, le virtuel au service du réel* » examine comment les technologies virtuelles, comme celles développées par Dassault Systèmes, permettent de visualiser et de comprendre certains aspects du monde qui étaient auparavant inaccessibles, en rendant visible (i.e. concret) des phénomènes complexes.

Des UNIVERS VIRTUELS …
… pour construire un monde plus durable et plus humain

- Optimiser
- Produire à la demande des produits personnalisés
- Prendre les bonnes décisions à long terme
- Valider la réalité du besoin

L'un des outils le plus employé est le « *jumeau virtuel* », terme un tantinet plus noble que double d'un modèle numérique virtuel. Cet outil permet de créer des représentations numériques précises d'objets, de systèmes ou de processus physiques. Il facilite ainsi une simulation (en temps réel ou non) du comportement et de l'évolution d'un produit ou d'un système, le but étant d'optimiser les processus au-delà de ce qu'un (ou des) individu(s) seul(s) pourrai (en)t concevoir.

Les jumeaux numériques étaient jusqu'à présent surtout utilisés pour concevoir et fabriquer des produits de meilleure qualité ; dorénavant ils sont utilisés pour optimiser les processus de prise de décision. Un exemple, la Plateforme 3DEXPERIENCE, Développée par Dassault Systèmes, intègre des outils comme CATIA, SIMULIA et DELMIA pour la modélisation, la simulation et la gestion des données.

Quelques exemples dans divers secteurs :

Urbanisme : Les jumeaux numériques sont utilisés pour modéliser des infrastructures urbaines, optimiser la gestion des ressources et planifier des projets durables. Ils permettent de mieux faire dialoguer divers acteurs comme l'architecte, le maître d'œuvre et l'exploitant. Par exemple, la simulation de scénarios d'implantation de nouveaux bâtiments permet d'analyser en temps réel les facteurs bruit, pollution et écoulements du vent dominant en vue de réduire les impacts nuisibles au confort et à la santé des habitants, ou pour allonger la durée de vie des bâtiments.

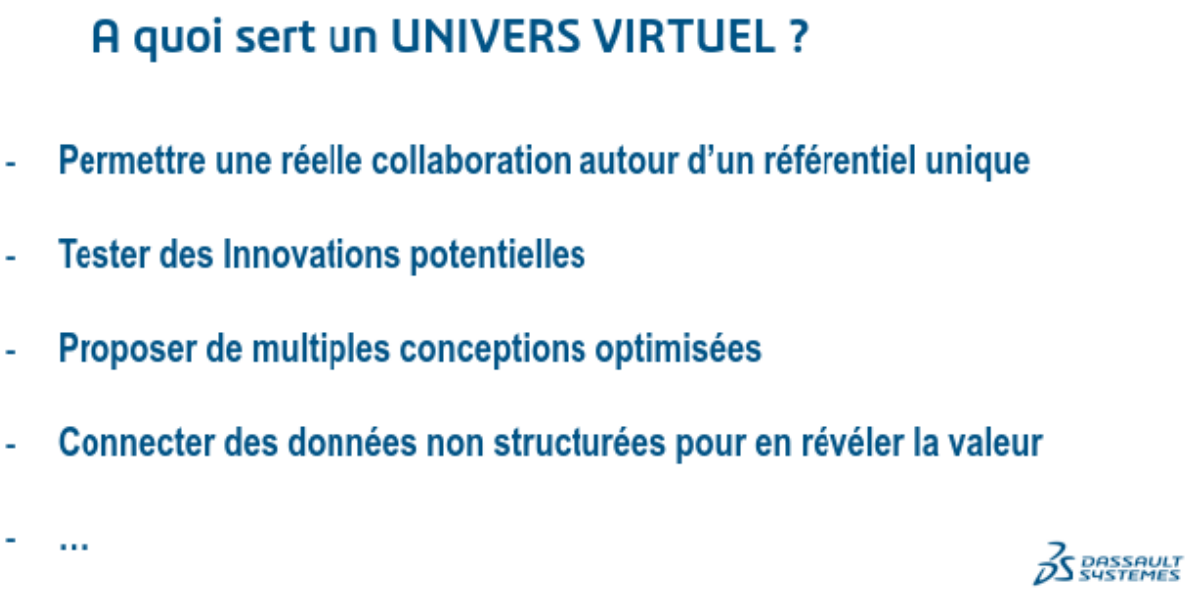
Impact d'un nouveau bâtiment sur l'environnement
bruit, pollution et écoulements du vent dominant

Industrie manufacturière : ils servent à prévoir les pannes, réduire et optimiser les coûts de développement de production et de maintenance, faire des tests (exemple crashs automobiles), le tout en simulant les chaînes de production et les équipements, etc. Il convient cependant de définir une stratégie claire pour une intégration fluide ultérieure des processus trouvés.

Innovation et matériaux génératifs : les jumeaux virtuels permettent, avec l'IA, de tester des milliers de combinaisons de molécules en vue de créer des matériaux plus résistants ou plus adaptés aux besoins, de tester des nouveaux médicaments, etc.

Logistique : Ils permettent de simuler et d'optimiser les chaînes d'approvisionnement, améliorant ainsi l'efficacité et réduisant les délais d'approvisionnement ou d'acheminement (cf. conférence de Florian Pourcel ci-dessus).

Ils révolutionnent le *secteur de la santé*, en créant des répliques numériques d'organes en les actualisant temporellement : les tests numériques permettent d'évaluer l'efficacité des interventions, de les écourter, et surtout, permet de personnaliser un traitement en fonction des caractéristiques de chaque patient (on peut faire un jumeau numérique d'un organe individualisé, d'où une médecine personnalisée). Une évaluation des risques est essentielle pour garantir ultérieurement une mise en œuvre efficace.



Les jumeaux numériques évoluent rapidement et plusieurs tendances prometteuses se dessinent pour l'avenir, que ce soit :

- pour fournir des analyses prédictives en temps réel, optimisant ainsi les processus et anticipant les défaillances ;
- pour modéliser des solutions durables, comme la gestion des infrastructures en amont d'un projet ou la réduction des déchets industriels en aval ;
- pour collecter des données en temps réel, permettant une surveillance et leur optimisation accrue.

Dans ce contexte, la responsabilité de l'ingénieur ne se limite plus à résoudre des problèmes techniques, mais inclut l'impact sociétal des décisions prises : des choix éthiques peuvent surgir. Dans le domaine législatif, la norme RTF 203 impose un certain nombre de critères environnementaux qu'il convient d'appréhender dès la première phase d'ingénierie. Il est crucial de déterminer comment les ingénieurs peuvent contribuer à répondre positivement à tous ces aspects.

Pour conclure, l'ingénieur acquiert au cours de sa vie une expérience, qui peut être définie comme la somme d'une expérimentation scientifique issue de son savoir et de l'usage qu'il en a fait. Elle lui permet de valider des hypothèses, d'apprendre de ses erreurs ou de celle des autres, pour, in fine, gérer au mieux la résistance

au changement et contribuer à garantir le bon fonctionnement ou le bon usage de produits nouveaux. Inventer un avenir « humain » en construisant un changement adapté au bien-être sociétal. Les univers virtuels peuvent, en révélant l'invisible, explorer l'inconnu, identifier les opportunités et maîtriser les risques.

Jean-Pierre Rozelot,

Président IESF-CA

Visuels @JM Morin, Dassault Systèmes

Jean-Michel Morin, ou la virtualisation scientifique d'hier à demain. Ingénieur de formation (Centrale Supelec 1977), il a largement contribué à l'aventure de DASSAULT SYSTEMES, depuis la startup de 35 personnes jusqu'au leader mondial de 25 000 personnes. Aujourd'hui Directeur de la Communication Executive au niveau Corporate, Jean-Michel a endossé au fil des années de très nombreux rôles dans des secteurs très variés. Il dirige aujourd'hui les Centres d'Excellence internationaux illustrant les transformations industrielles indispensables pour répondre aux grands défis écologiques et sociétaux de notre époque. Participant activement à la croissance et à la structuration de l'Entreprise, il a acquis une expérience exceptionnelle dans les partenariats technologiques et les solutions de réalité virtuelle immersive, les environnements web et internet, ainsi qu'en management international et en déploiement des systèmes complexes d'informations.

Il est par ailleurs membre du bureau exécutif d'un Think Tank géopolitique (Cercle des Nouveaux Monde), chargé tant de renforcer la capacité de réflexion que de dynamiser le dialogue en tant qu'intermédiaire entre les décideurs, les chercheurs et les PDG de grandes entreprises.

3. Visite CANNES La Bastide Rouge le 4 avril 2025

Les IESF-CA se sont rendus à Cannes Bastide Rouge le 4 avril dernier. Dans cette ville prestigieuse capitale du cinéma et du festival associé, ce site créé en 2021 a pour vocation d'être un vivier de créativité pour les métiers de l'art audio-visuel de la région et au-delà. Parmi les prestations proposées, ce site héberge des plateaux de tournage, des studios de post-production et des salles de projection permettant aux entreprises du secteur de maîtriser de bout en bout leur chaîne de production. Nous avons eu la chance de visiter l'auditorium, un espace high-tech haut de gamme permettant de projeter le rendu d'un montage cinéma en son haute-fidélité Dolby Atmos dans des conditions réelles, le tout étant piloté par une station de contrôle temps-réel. Infrastructures réellement impressionnantes !

Ce site se veut aussi et surtout être une pépinière d'entreprises capables d'héberger de nombreuses structures dans un cadre stimulant les échanges et l'innovation. Les infrastructures sont nombreuses et particulièrement appropriées pour ces types de métiers : 3 700 m2 d'espaces dédiés contenant 1 300 m2 de bureaux et plusieurs espaces de coworking incluant des salles de réunion et de créativité collaborative. Le tout situé sur le même site que les studios et salles de projection. Enfin, des studios de production sont à disposition pour créer des médias de communication en tous genres. Ce qui permet de diffuser rapidement et facilement les informations appropriées sur les plateformes et réseaux sociaux dans des conditions dignes des plus grands studios français, témoignages de célébrités à l'appui.

Cet espace montre la réelle volonté de l'Agglomération Cannes Pays de Lérins et de la Région Sud à développer et promouvoir l'art audio-visuel dans son intégralité, en se reposant sur ses acquis solides de ces dernières décennies et en pariant sur la qualité des contenus, court-métrages et films à venir. Un grand merci à Jean-Noël Ach, directeur adjoint et toute son équipe pour son accueil et sa convivialité pendant cette visite !

Visite fort intéressante du campus Georges Méliès de Cannes Bastide Rouge dédié aux industries créatives et aux métiers de l'image.

Nous avons pu visiter les studios, de son, d'images, de mixage et autres lieux à disposition des start-ups hébergées ou à des organismes de plus grande taille.

Ces découvertes ont été partagées avec nos amis alumni de Polytechnique et de Centrale Méditerranée avec qui nous avons conclu par un déjeuner convivial.

Guillaume BERTELLO

Alumni X01

4. Compte-rendu de l'AGO le 10 avril 2025

Activités

Comme l'an passé, la présentation des diverses activités de 2024 est faite sous forme d'une vidéo très vivante reflétant le fort dynamisme de l'année. Pour voir la vidéo cliquez sur le lien :

https://www.youtube.com/watch?v=awh_Rq_P12U

Le rapport moral est approuvé à l'unanimité.

Finances

Quelques précisions sont apportées par le Président sur le bilan financier qui est approuvé à l'unanimité.

Le trésorier adjoint confirme que les membres sont bien assurés dans leurs activités.

Les cotisations 2026 seront égales à celles de 2025.

Suite à une question, il est précisé que le Rectorat ne subventionne pas l'association.

Promotion des Métiers de l'Ingénieur et du Scientifique (PMIS)

Le nombre de contacts est stable mais le public est différent, pas de classes entières. L'équipe tâche de reprendre contact avec des établissements scolaires qui ne se sont pas manifestés cette année.

Les rencontres aux Salons sont en progression, très appréciés car ils permettent le contact avec les parents. Se reporter aux statistiques

Les moyens matériels de promotion sont satisfaisants mais l'objectif est de recruter des moyens humains.

Relation IESF national / IESF Régions

Comme suite à la démission du Président IESF en exercice, un Président intérimaire a été élu en attendant l'élection d'un nouveau président de l'IESF national.

Conseil d'Administration et Bureau

Quelques modifications sont approuvées :

- Un nouveau membre, François MANCHON rentre au CA et au bureau remplaçant Serge Chopard.
- Jean-Bernard Titz est nommé Vice-Président chargé de la communication et des partenariats.

Dominique Quéau

Secrétaire adjointe IESF CA

5. Nous y étions

5.1 Vœux de la Chambre de Commerce et d'industrie Nice Côte d'Azur le 16 janvier 2025

Vœux consulaires option XXL

Plus de 800 inscrits ce 16 janvier pour le traditionnel rendez-vous de début d'année de la Chambre de commerce et d'industrie Nice Côte d'Azur. Des patrons, des responsables de filières, des élus en pagaille... La saison entrepreneuriale 2025 est officiellement ouverte.

"Jean-Bernard Titz, CEO de Dev-Help et membre des IESF-CA était parmi les 800 personnes invitées aux vœux 2025 de la CCI Nice Côte d'Azur.

L'occasion de rencontrer de nombreux partenaires"

5.2 Concours de la Jeune Entreprise Innovante le 17 janvier 2025

Le concours de la Jeune Entreprise Innovante, porté par l'UPE 06, est ouvert aux étudiants, jeunes diplômés et néo-entrepreneurs des Alpes-Maritimes pour mettre en avant les projets ou structures de moins de deux ans axés sur l'innovation.

L'édition de cette année a eu lieu au Campus Georges Méliès (Cannes), ce 17 janvier 2025, en partenariat affiché et renforcé avec l'Université Côte d'Azur et le PUI Med'Innov, co-organisateur officiel de l'événement via sa commission *Innovation Valorisation en Formation Stratégique*, la CCI Nice Côte d'Azur, UCC Grand Sud, Rise Partners, Recherche & Avenir, l'incubateur Provence Côte d'Azur, Dev-Help, les Premières Sud et SoFab/Telecom Valley.

Les lauréats de cette édition sont :

- Prix Étudiant : ESIX, Karim BOUTIBA
- Prix du Jeune Créateur : PASS-MEMO, Pierre Getti, Pierre Canivet
- Prix de l'Entrepreneuriat Féminin : RAYONS DE SOLEIL, Lisa Unia

Félicitations aux vainqueurs et un grand bravo à tous les participants. Votre audace, vos idées et votre ambition incarnent l'avenir de notre territoire en matière d'innovation et de dynamisme économique.

Jean-Bernard TITZ

Vice-président IESF CA communication et partenariats

5.3 AG de TELCOM Valley le 1 avril 2025

Dans le cadre des relations initiées et approfondies depuis 2 ans avec l'association Telecom Valley, dont nous sommes adhérents croisés, nous avons assisté à leur assemblée générale du 1er avril chez Orange à Sophia-Antipolis.

Lors de cette AG électives, les co-présidents Teresa Colombi et Julien Holtzer ont été réélus par le nouveau Conseil d'Administration. Ils seront accompagnés par un bureau exécutif restreint à 6 personnes.

Lors du rapport d'activité les co-présidents ont insisté sur la nouvelle organisation mise en place dans les 2 ans passés dont un travail fort en mode projet et la mise en place de manifestations majeures que sont les "AzurTech Summer et Winter" et les "Nuits des Acteurs du Numérique" qui seront donc maintenues dans les 2 ans à venir.

Plus d'information sur https://www.telecom-valley.fr/

Jean-Bernard TITZ

Vice-président IESF CA communication et partenariats

6. Conférence enjeux et défis stratégiques en Méditerranée

Le 10 avril 2025 en ouverture de l'AGO IESF CA à Polytech Nice Sophia

Résumé :

De l'Antiquité à nos jours, la Méditerranée est le lieu d'échange et parfois de confrontation entre les grandes civilisations qui se sont développées sur son pourtour. Cette mer intérieure concentre les axes maritimes vitaux pour l'approvisionnement en matières premières stratégiques, comme le cuivre et l'étain nécessaires à la civilisation de l'âge du bronze au cours du premier millénaire avant notre ère. Que ce soit à l'époque hellénistique ou au temps de l'Empire romain, de nombreux échanges commerciaux existaient - produits agricoles (olives et huile d'olive, céréales, légumineuses, vins et produits de l'élevage), produits finis (des amphores, des œuvres d'art comme les guerriers de Riace, des œuvres technologiques tels la machine d'Anticythère, et bien d'autres), etc.

Au début du XXI^{e} siècle, la Méditerranée demeure un espace mondial privilégié pour le commerce, les échanges de biens et de personnes, les transferts d'information et de connaissance. Elle a une spécificité particulière car elle permet un accès aux océans Atlantique et Indien par le canal de Suez et la mer Rouge. Elle est en effet le point de contact naturel entre l'espace européen (447 millions d'habitants + 125 millions en ajoutant la Russie), le monde africain (1 milliard 549 millions) et le Moyen-Orient (371 millions), donc un ensemble démographique de près de 2,5 milliards d'habitants dont les activités s'articulent autour de l'axe méditerranéen.

Autant dire que se concentrent naturellement dans cette zone maritime, les enjeux économiques, diplomatiques, de maintien des écosystèmes et les affrontements de souveraineté. Cela se traduit par des tensions plus ou moins vives pour le contrôle des voies maritimes commerciales, des infrastructures de transport de l'énergie ou des matières premières, la mise en valeur des aires touristiques, le développement des principaux secteurs industriels et technologiques de la future « économie bleue ».

Le développement de ces activités ainsi que les débuts de l'exploration des grands fonds marins en vue de l'exploitation des ressources naturelles, contribuent à la croissance économique certaine de l'aire géographique méditerranéenne. Ils participent aussi à ce que cette mer intérieure devienne un lieu de rivalités et de confrontations présentant des risques et des menaces spécifiques : l'expansion des réseaux d'influence , les stratégies russe et chinoise dans les domaines militaire, économique et politique, le développement de réseaux criminels transnationaux, la hausse des trafics illicites, l'augmentation des cyberattaques notamment sur les sites industriels, les infrastructures portuaires, la logistique des armateurs, etc. A cet égard, l'exemple des câbles sous-marins est le plus caractéristique et fait l'objet d'un développement particulier.

En définitive, ce bref aperçu historique et géopolitique, montre que la sécurité, la sûreté et la sauvegarde des espaces marins relèvent de la puissance publique et de l'exercice de la pleine souveraineté des États.

De ce point de vue, il importe de bien connaître les règles de droit international qui régissent les espaces marins et le rôle singulier que la France a joué au cours des cinquante dernières années dans leur élaboration, du fait de l'étendue de sa zone économique exclusive maritime (laquelle est la deuxième au monde en termes de surface).

La mise en place de règles de droit était indispensable, pour régir les espaces marins afin d'assurer la coexistence pacifique des États. C'est le rôle qui est dévolu à la Convention des Nations Unies sur le droit de la mer (CNUDM) signée, à l'instigation de la France, en 1982, à Montego Bay (Jamaïque), par de nombreux pays à l'exception des États-Unis d'Amérique, de pays de l'Amérique du Sud, etc. La Turquie et Israël n'ont pas ratifié l'accord.

Pour assurer l'effectivité opérationnelle de cette norme juridique, la France s'est dotée d'une structure originale unique pour gérer le deuxième espace marin au monde et assurer le maintien de sa souveraineté maritime : « l'action de l'État en Mer ».

L'importance de la mer au cœur du mouvement scientifique et technologique, depuis près de deux siècles, est expliquée. Les acteurs et les réalisations concrètes dans les domaines de la biodiversité et des ressources naturelles offrent des perspectives réelles de développement de l'économie bleue.

Les territoires de la Côte d'Azur font l'objet d'une attention particulière, avec la mise en exergue de la spécificité de l'espace azuréen dans la recherche marine. Cette particularité est illustrée notamment par Villefranche-sur-Mer et la Principauté de Monaco avec les travaux du Prince Albert I^{er} de Monaco et de la Fondation Albert II de Monaco qui contribuent à l'émergence de pôles d'excellence préfigurant un nouvel écosystème centré sur la mer et les fonds marins.

Dans l'aire géographique de la Côte d'Azur, de nombreuses compétences scientifiques, technologiques et industrielles couvrent tous les domaines de la recherche marine. L'Université Côte d'Azur (UniCA) et son Institut Fédératif de Recherche (IFR) « Ressources Marines », le Pôle Mer Méditerranée, et bien d'autres établissements français et monégasques comme le Centre scientifique de Monaco, stimulent l'économie maritime et littorale dans la région méditerranéenne en encourageant la recherche et l'innovation.

Aujourd'hui, les espaces marins constituent un défi en termes de connaissance, de préservation et de valorisation : il s'agit d'un enjeu économique majeur dans un contexte géopolitique complexe où le changement climatique, les problématiques énergétiques, la pression migratoire, etc. sont autant de facteurs d'affrontement que de coopération. Les États devront faire preuve d'un comportement responsable au vu des risques et des menaces.

La troisième Conférence des Nations Unies sur l'Océan, qui se tiendra à Nice en juin 2025, a pour but d'accélérer la mise en œuvre des engagements pris lors des éditions précédentes et de définir de nouvelles stratégies pour valoriser et protéger les océans, fournisseurs de ressources vitales pour le développement de l'humanité et espaces régulateurs cruciaux de l'écosystème mondial.

La préservation et la valorisation des espaces maritimes dépendront de la capacité stratégique, économique, technologique, militaire et scientifique des États, d'où l'importance de cette conférence internationale.

Si le support de la conférence vous intéresse cliquez sur le lien suivant pour télécharger le document : https://drive.google.com/file/d/1QqHx07RM73j9N88OLenOTjZIPRia_Ait/view?usp=drive_link

Jean-Pierre DAMIANO

Ancien Ingénieur de Recherche (UniCA CNRS) Administrateur et conseiller IESF Côte d'Azur

Le contenu de la conférence est issu de recherches à partir de diverses sources et références publiques authentifiées provenant de diverses origines. Les informations exposées (vignettes et commentaires) le sont à titre de référence uniquement. Les auditeurs sont entièrement responsables de l'utilisation qu'ils feront du support. Le rédacteur n'assume aucune responsabilité quant à l'exactitude ou à l'omission de certains éléments ainsi qu'aux conséquences possibles.

Support de la conférence

7. Enjeux et défis majeurs du cyberespace : cybermenaces, cyberattaques, cybersécurité, cyberdéfense, …

Résumé

Cette publication fait suite à la conférence « Cybermenaces vs Cyberdéfense : la France est une cible privilégiée en Europe » organisée par l'Association des Auditeurs de l'Institut des Hautes Etudes de Défense Nationale (IHEDN) le 17 décembre 2024 à Nice.

Elle a pour objectif de sensibiliser au contexte des cybermenaces visant la France jusque dans ses infrastructures critiques, en exposant des stratégies de cyberdéfense et en prenant connaissance des raisons géopolitiques et technologiques exposant notre pays à de tels risques. Des références et des sources authentifiées sont présentées pour la compréhension de la complexité du cyberespace devenu un enjeu géopolitique majeur du 21ème siècle.

Après quelques rappels de terminologie, du contexte des cyberattaques et des ingérences, en détaillant les modes opératoires des attaquants, en France et à l'étranger, il est expliqué comment les cybermenaces engendrent des attaques de plus en plus sophistiquées dont les conséquences économiques et sociétales sont considérables - cas des infrastructures critiques (électricité, pétrole, gaz, agro-alimentaire, santé publique, etc.) ou bien des Jeux Olympiques et Paralympiques de Paris 2024, largement interconnectées et donc susceptibles d'être vulnérables. Dans l'Union européenne (UE) et plus particulièrement en France, les innovations issues des collaborations académiques et industrielles, nationales et internationales font l'objet de convoitise, de tentative de captation technologique, de détournement de propriété industrielle, d'influences de toutes sortes, etc., de la part d'entreprises concurrentes, de groupes d'intérêt ou d'organismes étatiques étrangers.

Le rôle respectif des divers organisations et agences d'état spécialisées, françaises et européennes, est détaillé quant à leurs actions de cyberdéfense - stratégies de surveillance et de détection des menaces, solutions techniques pour protéger la confidentialité, l'intégrité et la disponibilité des informations, prévention en amont, etc. (rôle de la cybersécurité).

La vigilance accrue est indispensable sur les moyens de télécommunication - câbles sous-marins, réseaux satellitaires, etc. - ainsi que sur les solutions aux problèmes de brouillage en vue de désorienter les véhicules, les navires, les avions, les navettes, etc. à l'aide de divers exemples.

La multiplication des cyberattaques basées sur l'intelligence artificielle (IA) permet des attaques automatisées, plus ciblées et difficiles à détecter. La cybersécurité utilise évidemment les algorithmes de l'IA pour répondre et anticiper de telles attaques avec des outils de plus en plus sophistiqués. Cependant, la situation est préoccupante car l'IA est intégrée dans la préparation des missions jusqu'aux théâtres d'opération, en passant par les processus décisionnels, d'engagement et de maintenance, sans oublier les équipements militaires.

…/…

…/…

Les enjeux technologiques et les défis dans la défense numérique sont primordiaux. Ils doivent être traités avec suffisamment d'anticipation avec l'aide des écosystèmes civil et militaire, notamment le monde académique, les industries et entreprises, etc. Les coopérations nationales et internationales permettent le renforcement de la protection du cyberespace, en contexte de guerre cognitive. La recherche de talents et de profils compétents est devenue plus que nécessaire. La sensibilisation, la formation et les simulations de crise dans les entreprises et les services publics sont vitales.

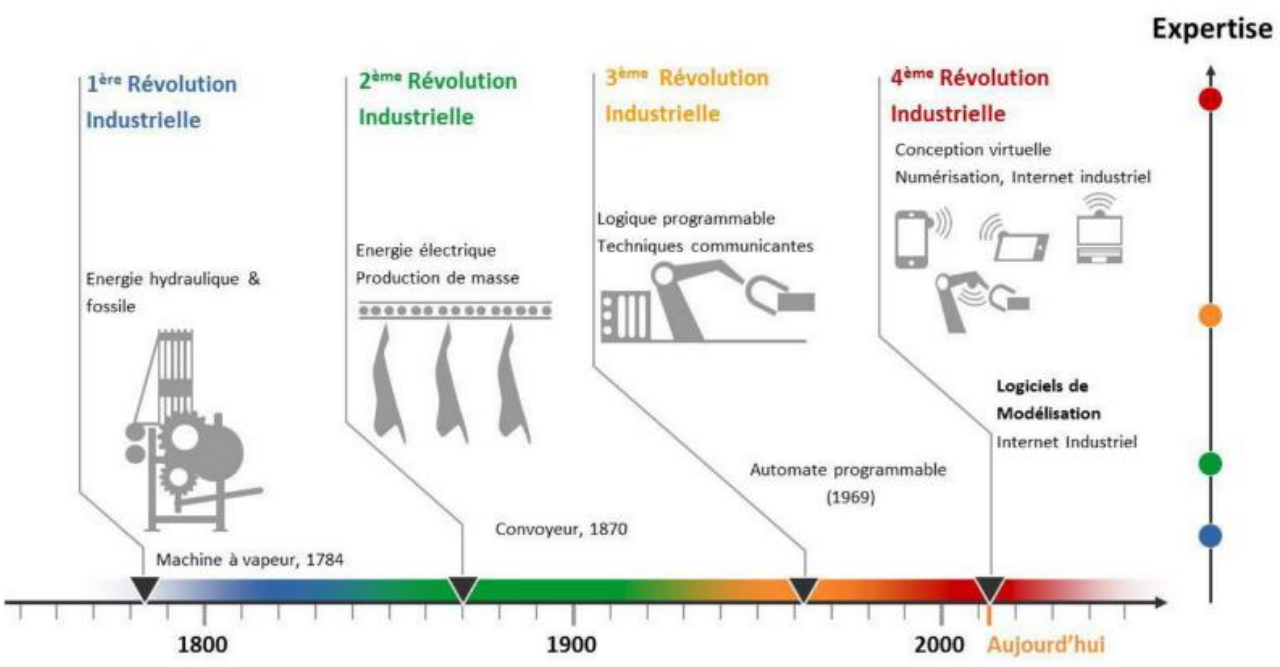
Le texte est fondé sur des références vérifiées, d'organismes publics et privés, d'institutions, de sites spécialisés, etc. dont une liste non exhaustive est présentée. Il est rappelé que les figures, les images, les logos et les tableaux présentés sont la propriété de leurs auteurs.

Le texte est constitué de deux parties 1 et 2 publiées séparément.

PARTIE 1 *LES CYBERMENACES ET LES CYBERATTAQUES*

7.1 LE CONTEXTE

La numérisation de la société est la quatrième révolution industrielle après les deux premières relatives aux énergies mécanique et électrique, la troisième concernant les techniques de communication, les automates programmables, l'informatique, etc.



Source FIM . Guide pratique de l'usine du futur

https://www.ifm40.fr/industrie-4-0-cest-quoi/

La sécurité numérique est essentielle pour que la confiance numérique soit réelle et résiliente dans les réseaux de télécommunication, la cybersécurité des systèmes industriels, les systèmes digitaux, les algorithmes et les systèmes de l'intelligence artificielle générative, les applications logicielles, les assistants numériques, les composantes de l'internet des objets (IoT), etc.

La France fait partie des démocraties du monde occidental. Elle est attaquée à cause de sa position diplomatique dans le monde en devenant la cible de groupes terroristes contestant les intérêts français sur le continent africain, par exemple. Elle est aussi attaquée pour sa maîtrise des hautes technologies (nucléaire, quantique, etc.) et de l'énergie en général, pour son expertise, etc. Cela s'est traduit par de nombreuses tentatives de déstabilisation lors de la Coupe du Monde de Rugby en 2023, d'élections diverses, des Jeux Olympiques de Paris 2024 qui ont dû supporter de nombreuses cyberattaques de grande ampleur, sans dégât majeur, alors que cette guerre cyber a commencé, il y a plusieurs années.

Pour mémoire, à l'époque des attentats de Paris en 2015, le nombre de cyberattaques était passé de 3 000 à plus de 20 000 dans l'objectif de bloquer les échanges ministériels avec les unités de commandement entre autres. Tous les types d'infrastructure publique ou privée, d'importance stratégique ou non, sont concernés. Par exemple, des grands groupes ou organismes tels France Travail, Viamedis, Almerys ou encore SFR : les données des adhérents ou clients ont fuité et mis en vente sur le *dark web*.

Deux exemples :

- En milieu hospitalier, une paralysie des réseaux de communication ou des pannes électriques ont pour conséquence d'empêcher très rapidement la réalisation de radiographies, d'examens au scanner ou IRM, d'analyses biologiques, etc. mais aussi de bloquer l'accès aux dossiers des patients, à leur transport, etc. Il est indispensable d'assurer la protection des infrastructures hospitalières et d'avoir les moyens d'anticiper de telles attaques (plans de crise adaptés, des exercices de simulation, etc.) ;
- En milieu maritime, l'enjeu de la cybersécurité est tout aussi évident et crucial pour les écosystèmes portuaires, car ils jouent un rôle vital dans le commerce international et toute perturbation des activités peut avoir des conséquences importantes pour l'économie. Les places portuaires doivent être en capacité d'offrir toutes les garanties nécessaires pour la sécurité de leurs partenariats et des opérations.

Il est nécessaire d'expliquer quelques notions de base en faisant des rappels de terminologie.

7.2 Quelques rappels de terminologie

Le préfixe « ***cyber*** » est d'origine grecque, signifiant « gouverner au sens du gouvernail ». Il sert à former de nombreux mots : cyberdéfense, cyberguerre, cyberespace, cybersécurité, cybermenace, cyberespionnage, cybernétique, etc.

Le **cyberespace** (initié par William Gibson, ouvrage Neuromancer, 1984) est un néologisme créé avec les termes cybernétique et espace. C'est un espace à la propriété immatérielle et particulièrement technique compte tenu de sa complexité : il élimine tout concept de distance, car ce milieu est intangible. Il est constitué du maillage des réseaux de télécommunication, des réseaux informatiques, de tous les systèmes informatiques, avec les processeurs, les mécanismes de sécurité, les opérateurs, etc. sans oublier les utilisateurs. Olivier Kempf, stratégiste et géopolitologue (2012), proposait un schéma à trois couches physique (infrastructure matérielle), logique et applicative (services traitant les informations) et cognitive et sémantique (les internautes).

Le cyberespace concerne les domaines privés et professionnels, dans les secteurs économiques, financiers, administratifs, étatiques, etc. avec des échanges de toutes sortes de données ou d'informations au niveau mondial de manière quasi instantanée. Devenant un espace de tensions et d'oppositions où les impacts politiques, stratégiques et économiques des menaces peuvent déstabiliser les États et les structures économiques, il est considéré comme le 5ème milieu de conflictualité, après la terre, les mers et océans, les airs et l'espace. Il s'agit donc de maintenir et d'adapter une vigilance extrême dans le cyberespace.

Les risques d'attaque de systèmes informatiques sur les infrastructures d'une compagnie, d'un État, d'une organisation privée ou publique, de ses systèmes d'information, constituent des **cybermenaces.** Elles peuvent provenir de l'intérieur d'une organisation par des utilisateurs de confiance ou de sites distants par des parties inconnues. Les acteurs de la menace étatique mènent des opérations en faisant appel à des cybercriminels et à des moyens malveillants pour recueillir des renseignements ou voler des données. Les cybermenaces font partie intégrante de la vie numérique : pour s'en protéger, il est essentiel de bien comprendre la nature des attaques.

Une **cyberattaque** est un acte malveillant de piratage informatique mais pas uniquement : elle a un champ d'application plus large visant aussi les internautes pour les escroquer, fausser leur jugement ou les influencer pour telle ou telle action. Elle peut se définir comme le fait de subir un acte malveillant envers un dispositif informatique portant atteinte de manière significative à la confidentialité et/ou à l'intégrité de l'information de l'entreprise ou encore à la disponibilité du système d'information, entraînant des pertes financières significatives et/ou une atteinte à l'image de l'entreprise et/ou des efforts significatifs de défense pour contenir et traiter l'attaque. Une cyberattaque peut être le fait d'une personne isolée, d'un groupe, d'un Etat, etc.

Face aux risques numériques, deux types d'approches complémentaires existent :

La **cybersécurité** concerne tous les responsables de systèmes et de réseaux, assure la prévention des menaces, la minimisation des vulnérabilités par une protection renforcée des systèmes et des données ainsi que la résilience de tous les systèmes numériques de manière globale. Elle est un élément prépondérant constitutif de la sécurité économique qui en traite tous les aspects économiques et sociaux, permettant ainsi d'établir et de maintenir la confiance dans les économies de plus en plus dépendantes du numérique et d'accroître la résilience dans le contexte actuel de conflits à l'échelle de la planète et de l'essor de la cybercriminalité.

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 : c'est un levier stratégique, où l'anticipation et la capacité de réponse rapide participent à la résilience des entreprises mais aussi des États. Ses moyens sont techniques, juridiques, méthodologiques ou humains.

La **cyberdéfense**, menée par différents services de l'État, ou sous leur responsabilité selon les lois en vigueur, traite les aspects techniques (matériels, logiciels, etc.) en organisant la réaction face aux intrusions et incidents, en assurant une surveillance active et une gestion rapide des crises, pour la sécurité et la résilience des systèmes vitaux dont la défaillance pourrait nuire gravement à la nation.

Enjeu et priorité stratégique, la cyberdéfense est garante de la souveraineté nationale. Avec de nombreux acteurs, le ministère des Armées participe activement à la protection et à la défense des systèmes d'information dans le cyberespace. L'évolution des menaces informatiques oblige à étendre cette définition au domaine civil. La question n'est plus de savoir si une attaque se produira, mais quand elle aura lieu. Cela impose une approche plus proactive, intégrant des stratégies de réponse et de résilience. C'est dans ce contexte que l'on peut véritablement parler de cyberdéfense.

La cyberdéfense se distingue de la cybersécurité du quotidien au même titre que la sécurité nationale n'a pas la charge des missions classiques de sécurité publique.

La **cybernétique** (initiée par Norbert Wiener, mathématicien, 1948) désignait un nouveau domaine de la science étudiant la maîtrise des machines. Elle est un moyen d'expliquer et de comprendre tous les mécanismes rencontrés avec quelques éléments comme la boîte noire dont le fonctionnement est déduit des informations entrantes (par un émetteur) et sortantes (à travers un récepteur). Ce flux d'informations est l'information efficace. Le système compte un élément de rétroaction (*le feedback*) avec les entrées d'information permettant de corriger ou d'autoréguler le modèle élaboré. D'une autre manière, la cybernétique est une modélisation de l'échange entre les humains, les machines et l'ensemble de la société, élaborée par l'étude de l'information et des principes d'interaction.

La menace cyber est permanente et en évolution continue. Profitant des opportunités offertes par le cyberespace, le nombre et l'intensité des attaques menées dans ce milieu ne cessent de croître, visant le profit financier, la captation de données, la déstabilisation des institutions par la manipulation des opinions ou la paralysie de systèmes étatiques et privés.

7.3 La typologie générale des menaces

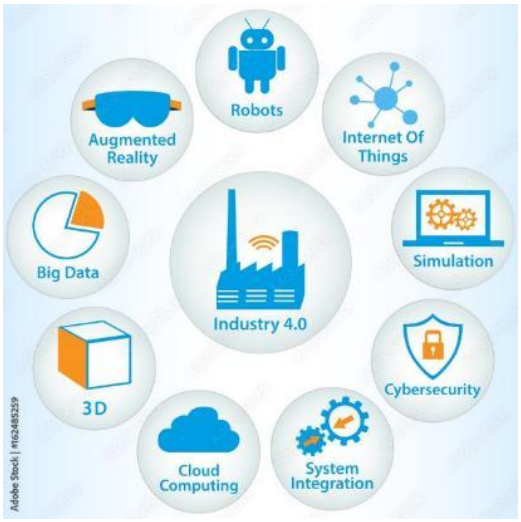
Les menaces peuvent être environnementales, intrinsèques, humaines, etc. Les menaces majeures peuvent être d'origine externe (compromission ou vol de données, physique, électronique, etc.) mais aussi internes (négligence du personnel, utilisation malveillante des matériels, etc.).

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 cyberattaquants 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.

Les cibles peuvent être des hôpitaux, des administrations, des établissements publics, des institutions, des écoles, des universités, des instituts de recherche, des entreprises de toutes tailles, des collectivités, etc. De nombreuses tentatives de piratage d'infrastructures critiques (pétrole, gaz, nucléaire, etc.) ont déjà eu lieu, parallèlement à des campagnes de cyber-espionnage, d'utilisation de programmes malveillants et de rançongiciels, sans oublier les manœuvres d'organisations cybercriminelles et les piratages de cryptomonnaies.

Lors d'un conflit (intérêts divergents, rivalités géopolitiques, etc.) opposant deux puissances, afin d'éviter un affrontement direct sur un champ de bataille et de rester ainsi en retrait, les deux antagonistes utilisent des tiers qui peuvent être des États, des groupes rebelles, des organisations terroristes ou d'autres entités : c'est une guerre par procuration (*proxy war*) pour laquelle les puissances leur fournissent un soutien matériel, logistique, financier, ou militaire.

Enjeux et les défis pour l'industrie



Chiffres clés

73% des entreprises industrielles

Au moins une cyberattaque en 2022

4,6 M€

Coût moyen d'une cyberattaque

10%

Croissance annuelle attendue du marché de la cybersécurité en France

Menaces et vulnérabilités : les défis

Espionnage industriel

Secrets de fabrication, de production, …

Technologies innovantes

Sabotage industriel

Perturber, ralentir, endommager les processus de production

Cyberattaques

Déstabiliser les infrastructures critiques

Avantages stratégiques

Ils sont nombreux et liés à la transformation numérique essentielle pour maintenir la compétitivité - la continuité de service, de la chaîne de production ou des automates, le réseau de transport, etc. L'ère de l'industrie 4.0 est caractérisée par la mise en réseau de ses activités, l'automation, le recours aux nouvelles technologies (IA, IoT, *cloud computing*, etc.) pour assurer des opérations diverses de la conception à la production de biens et de services assurant la robustesse de l'organisation.

Il y a convergence des réseaux informatiques (IT - *Information Technology*) et industriels (OT - *Operational Technology*) autrefois séparés. Les opportunités sont considérables, mais exposent aussi les entreprises industrielles à des cybermenaces croissantes dues à l'augmentation de la surface d'attaque. Elles doivent privilégier une approche proactive et intégrée, combinant solutions techniques, organisationnelles et humaines. Le facteur clef de succès est la gestion des flux de données numériques et le traitement de l'information. Cela influence les stratégies de gestion des risques cybernétiques au cours des deux prochaines années (World Economic Forum).

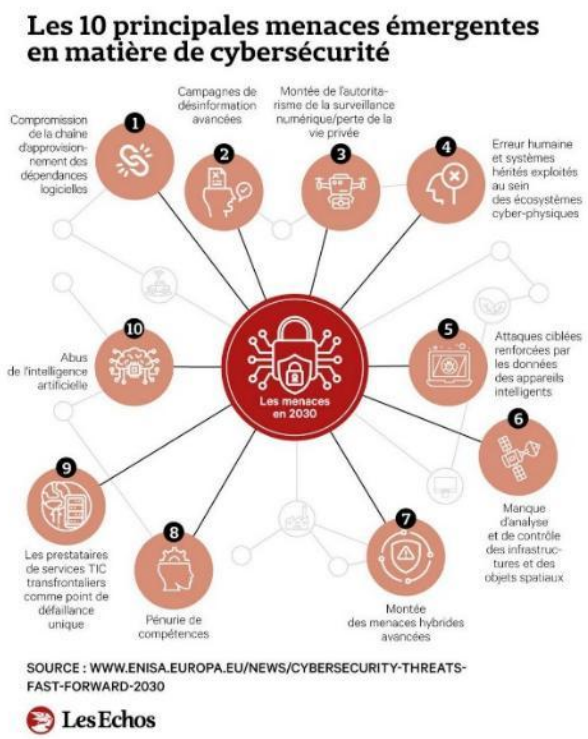
Le déterminant de la mutation industrielle et sociétale est la capacité à gérer l'information en permanence et à tous les niveaux avec toutes les règles de cybersécurité en vigueur, en vue de consolider sa résilience face à la menace cyber.

Les risques pèsent sur les infrastructures cybernétiques et physiques du pays (secteurs de l'énergie, des communications, etc.). Cependant, le plus grand risque de cybersécurité pour la plupart des entreprises est représenté par les personnes, et non par la technologie.

@CESIN

De manière générale, les menaces sont classées selon trois directions, à savoir :

- La voie informatique : vers, virus, chevaux de Troie, *keyloggers*, portes dérobées, bombes logicielles, saturation des réseaux, etc. ;
- La voie cognitive : manipulations à distance ciblée ou de masse, manipulations au contact ;
- La voie physique : effraction (salle serveurs, etc.), destruction (câbles, etc.), piégeage (réseaux informatiques, etc.), et autres faits.



En analysant les objectifs des attaques, six thématiques apparaissent :

Lucrative

- Cybergangs
- Cybermercenaires
- Officines

Politique

- Hacktivistes
- Cyber patriotes
- Cyber terroristes

Militaire

- Unités spécialisées

Ludique

- Adolescents désœuvrés

Technique

- Hackers

Pathos

- Employé(e) mécontent(e)

A mesure que les acteurs de la menace deviennent plus pertinents et que les surfaces d'attaque des organisations continuent de s'étendre, la gestion des risques cybernétiques pose donc un défi croissant pour les organisations.

7.4 Les cybermenaces et les cyberattaques

7.4.1 Introduction

Selon le rapport de l'Agence de l'Union européenne (UE) pour la cybersécurité (ENISA), les deux grands types d'attaques sont les rançongiciels (+10 téraoctets de données volés chaque mois) et les attaques par déni de service distribué qui, combinées, représentent 62% des menaces identifiées en Europe, en 2023.

Selon les estimations, le coût annuel de la cybercriminalité pour l'économie mondiale a atteint 7 800 Mds € en 2023. Ce chiffre était 5 500 Mds € à la fin de 2020 et 2 750 Mds € en 2015.

Selon le rapport annuel sur la cybercriminalité en 2024, émis par le ministère de l'Intérieur, il apparaît que le secteur des technologies de l'information est le plus ciblé avec 24 % par les cyberattaques, suivi par l'éducation et la recherche avec 21 %, le gouvernement avec 12 %, la santé, etc.

Du côté des entreprises, le rapport de PwC CEO Survey de 2025, montre que, sur le plan international, les craintes de volatilité macroéconomique (29 %) sont en tête des préoccupations suivies par celles de l'inflation (27 %) et des risques cyber (24 %). En France, la culture cyber et les attaques récentes mettent les risques cyber en première place (39 %), devant la raréfaction des compétences clés (34 %) et la volatilité macroéconomique (31 %).

Le cabinet PwC France et Maghreb explique la minoration des perceptions des menaces à court terme par la nature même des risques considérés : ceux ayant un impact direct sur l'entreprise - économiques, cyber, etc. - et ceux plus indirects et diffus, liés au contexte mondial - aspects climatiques et géopolitique, etc. - dont les impacts sur la performance immédiate ne se mesurent que sur une échelle de temps plus longue.

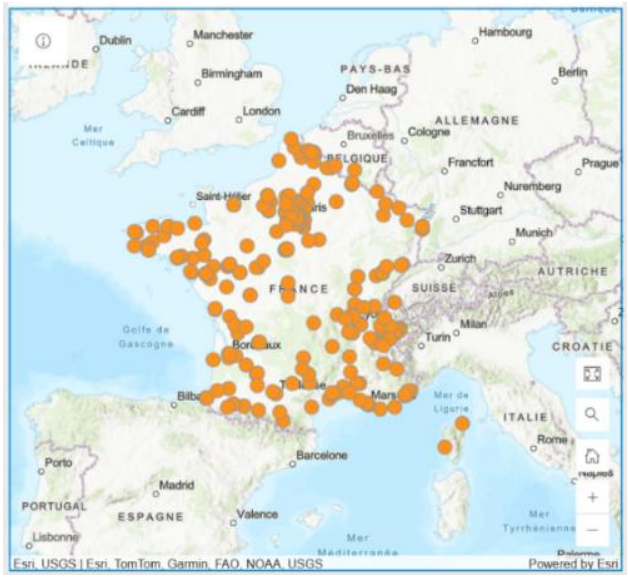
Les conflits actuels mobilisent de nombreux hacktivistes, des cybercriminels et des groupes instrumentalisés par des États. Les cybermenaces font partie intégrante de la vie numérique : pour s'en protéger, il est essentiel de bien comprendre la nature des attaques.

Selon une étude récente réalisée par CheckPoint, le nombre total d'attaques contre les organisations a considérablement augmenté au cours de 2024 : en moyenne 1 673 attaques par semaine et par organisation, soit 44 % de plus qu'en 2023 !

Selon le rapport de l'entreprise de cybersécurité Crowstrike, en 2024, l'ingénierie sociale, les intrusions dans le *cloud* et les techniques sans logiciel malveillant se sont très largement développées. Les groupes à la solde d'États ont intensifié le cyberespionnage et ajouté les techniques IA à leurs outils. Pour garder une longueur d'avance sur ces cyberadversaires, les entreprises doivent s'adapter à des temps de propagation de cyberattaques très courts (de l'ordre de la minute à une cinquantaine selon les configurations) et à des techniques plus furtives en continuant d'innover.

En ce qui concerne **les collectivités**, la plateforme gouvernementale Cybermalveillance.gouv.fr a publié, en novembre 2024, sa 3ème étude sur la maturité cyber des collectivités et montre une prise en compte des risques insuffisante (enquête avec OpinionWay). La frontière s'accentue entre les petites collectivités et celles de plus de 1 000 habitants. Les administrations françaises font aussi face à diverses cybermenaces : l'hameçonnage, les rançongiciels, le piratage de comptes en ligne, etc. Ces menaces évoluent constamment, obligeant les autorités à renforcer leurs mesures de cybersécurité.

Carte des cyberattaques sur les services publics jusqu'à la fin de l'année 2024.



Chaque point **orange** est cliquable à partir du site web : https://actu-cartes-de-france.fr/2025/02/carte-des-attaques-de-cybersecurite-dans-les-services-publics-en-france.html

Accès à des informations : type d'attaque, date, etc.

Source des données : Association pour le développement et l'innovation numérique des collectivités (ADICO)

7.4.2 Les catégories d'attaquants :

- Les amateurs : des acteurs imprévisibles, autodidactes, de niveau technique variable avec des motivations financières, idéologiques, des atteintes aux personnes ;
- Le terme hackeur prend, en sécurité informatique, le sens de « pirate informatique » sans nécessairement avoir d'aspect cybercriminel : le terme cracker est parfois utilisé pour désigner les pirates mal intentionnés, les démarquant ainsi de la culture académique des hackers ;
- Les hacktivistes : des acteurs nombreux et engagés avec des motivations de désinformation, d'influence, de haine en ligne, etc., de niveau technique très variable, s'alliant entre eux pour augmenter leur cercle d'influence, leur force de frappe ainsi que leurs connaissances techniques ;
- Les cybercriminels : des professionnels motivés par le gain financier, organisés, indépendants et experts spécialisés, avec un niveau technique plutôt élevé. De nombreux groupements sont soutenus par des États ou se livrent à des actes d'espionnage industriel.

7.4.3 Les menaces persistantes avancées (APT)

Une APT (*Advanced Persistent Threat*) est une cyberattaque prolongée et ciblée par l'attaquant non autorisé accédant au réseau et passant inaperçu pendant une certaine période, avec l'objectif d'obtenir un accès permanent au réseau, d'en surveiller l'activité et d'en capter des données, sans atteinte a priori au réseau ou à l'organisation. Les secteurs visés sont plutôt la défense nationale, l'industrie et la finance auxquels il convient d'ajouter les *think tanks* et les organismes de recherche spécialisés sur les questions de défense, de relations internationales, de diplomatie, de politiques publiques…

Il existe plusieurs étapes progressives d'une attaque APT résumées ainsi :

1	2	3	4	5
! Pour accéder au S.I., **utilisation** de fichiers infectés, de courriels malveillants, ou bien d'applications vulnérables, etc. *S.I. Système d'information*	**Installation** de logiciels malveillants et **configuration** de réseau de tunnels et de portes dérobées pour naviguer, sans être détectés, tout en effaçant les traces.	Tentatives de **compromission** de mots de passe pour accéder à des droits administrateurs en vue d'une intrusion plus étendue.	Avec une meilleure connaissance du réseau convoité, **exploration** de nouvelles zones encore non visitées.	La cartographie du S.I. et de ses vulnérabilités permet l'**observation** des transactions, en restant indétectable jusqu'au moment de la **cyberattaque**.

Les termes « attaque » ou « compromission » sont relatifs à une action offensive avec un impact direct immédiat sur la disponibilité, l'intégrité, la confidentialité ou la traçabilité des données présentes sur le système d'information.

Les pirates utilisent diverses techniques d'attaque comme l'exploitation des vulnérabilités *zero-day* (l'attaque se produit avant que la cible n'ait détecté la vulnérabilité en cause), l'hameçonnage ciblé (*spear phishing*) - usage de courriels ciblant une personne ou une entreprise spécifique, avec des données très précises augmentant ainsi leur crédibilité) - et autres techniques d'ingénierie sociale. Les groupes APT s'appuient sur des codes malveillants pour obtenir un accès complet à des systèmes de contrôle de supervision et d'acquisition des données SCADA (S*upervisory Control And Data Acquisition*) et à des systèmes de contrôle industriel ICS (*Industrial Control System*). Ils peuvent aussi utiliser la technique BYOVD (*Bring Your Own Vulnerable Driver*) permettant d'exploiter les vulnérabilités de bas niveau, en attaquant les pilotes (imprimantes, caméra, microphone, écran, etc.) obsolètes, non-mis à jour, non détectés dans une recherche de vulnérabilité classique, …

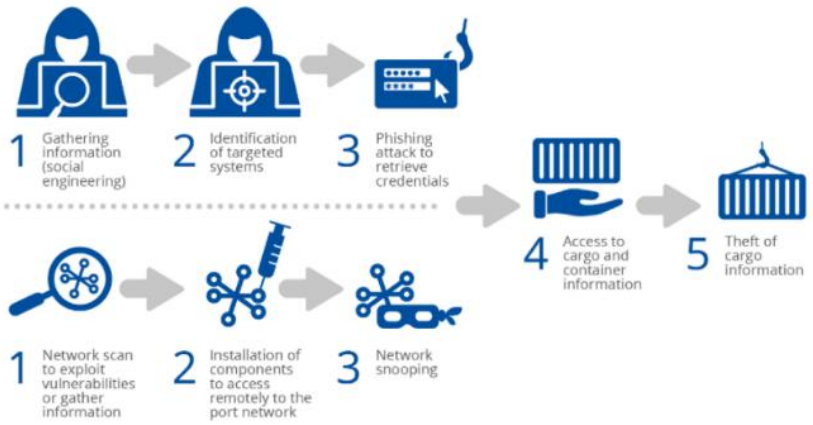
Les SCADA sont des systèmes de gestion et de contrôle, à grande échelle, surveillant, gérant et administrant des infrastructures complexes dans des activités variées : le transport, le nucléaire, l'énergie, etc. Ils connectent des automates, des capteurs, des dispositifs de mesure ou d'analyse, des systèmes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

Les ICS surveillent les processus industriels (distribution, manutention et production de produits), les gèrent automatiquement et en permettent le contrôle humain. Ils se trouvent 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 accélèrent les opérations, permettent de réagir plus rapidement aux fluctuations et de renforcer la fiabilité.

La mise en œuvre des technologies RPA (*Robotic Automatisation Process*) et leur développement doivent être réalisés selon des règles de sécurité fiables pour assurer le bon fonctionnement des 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, etc.

Concernant la sophistication des actions malveillantes, il a été constaté une forte augmentation des *wipers* (codes malveillants effaçant toutes les données enregistrées sur des disques durs ou les rendant inutilisables) déployés conjointement avec des vers pour se propager sur tout le réseau, notamment lors d'attaques ciblées de type APT (attaques furtives de longue durée), depuis le début de la guerre entre la Fédération de Russie et l'Ukraine. 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.

Exemple de compromission de données critiques destinée à dérober des cargaisons de grande valeur ou permettre un trafic illégal par le biais d'une attaque sophistiquée ciblée contre des systèmes portuaires : cas de l'attaque contre ceux d'Anvers, en Belgique, en 2011. Un cartel de la drogue avait pris le contrôle du mouvement des conteneurs, par l'envoi de *malwares* (logiciels malveillants) à des employés des agences maritimes. Une fois l'intrusion a été détectée, le pare-feu a été remis à niveau mais les cyberpirates avaient réussi à le surmonter pour installer des outils malveillants sophistiqués dans les ordinateurs de ces agents. Ainsi ils ont pu identifier les mots de passe utilisés pour récupérer leurs containers sur les quais.



Impacts :

Vol de marchandises et de biens ; Trafic illégal ; Réputation ternie

Actifs concernés :

Cargo Community Systems (CCS) ; Réseaux ; Courriel ; Personnes

Acteurs concernés :

Opérateurs de terminaux ; Police ; Compagnies de navigation et de fret maritime ; Expéditeurs et destinataires

Source : Port cybersecurity, Good practices for cybersecurity in the maritime sector, ENISA, Novembre 2019

Informations sur les affiliations et les actions des groupes APT

Des communautés de hackers ont marqué la période récente, en raison de l'ampleur de leurs modes opératoires d'attaque (MOA), de leurs affiliations, de la nature ou du volume des données volées. Leurs actions ont évidemment engendré une vigilance renforcée pour les cibles choisies : États, entreprises stratégiques, infrastructures critiques, opérateurs et points d'importance vitale (OIV, PIV), opérateurs de services essentiels (OSE), secteurs public et privé (santé, gestion de l'eau, transports, communications électroniques, industrie, recherche, etc.) : par exemple, le brouillage des signaux GPS des systèmes de navigation maritime modifiant ainsi la location réelle du navire avec tous les risques que cela engendre.

Ces groupes sont classés parmi les menaces persistantes avancées (APT). Ils comptent généralement des acteurs hautement qualifiés, souvent soutenus par des États ou des organisations criminelles organisées. Ils peuvent prendre des formes clandestines, intégrées à des États, indépendantes ou supposées telles mais avec des liens forts avec des Etats, etc.

Leur objectif est de cibler principalement les infrastructures critiques, les secteurs financiers, les organisations technologiques et les institutions gouvernementales. Ils peuvent aussi attaquer des sous-traitants ou des entreprises partenaires, moins protégés, leur permettant d'accéder plus facilement aux systèmes d'information visés.

Les informations données sur les différentes APT, en pages suivantes, proviennent de sources authentifiées dûment référencées. Cependant, l'auteur les expose avec réserve, en effet :

Il est difficile de déterminer l'origine exacte et les commanditaires des cyberattaques qui peuvent avoir lieu sous une fausse bannière (*false flag*) afin de masquer l'identité et diriger les soupçons vers d'autres acteurs.

C'est la surveillance incessante du trafic sur les réseaux, l'analyse des informations collectées qui conduisent souvent à des groupes d'attaquants agissant pour le compte d'États, d'officines, etc.

La situation est asymétrique car, d'un côté, avec quelques centaines d'euros, il est possible d'acheter, sur le *dark web*, un kit complet pour préparer de telles attaques et d'un autre côté, il est nécessaire de disposer de gros moyens matériels, technologiques et financiers pour s'en prémunir.

Ceux affiliés à la République populaire de Chine (RPC)

Les groupes de pirates informatiques chinois sont connus pour leur focus sur les industries stratégiques (défense, finance, technologies, télécommunications et santé) et leurs actions sont le vol de propriété intellectuelle, des perturbations à caractère politique, des attaques d'infrastructures critiques, etc. Ils exploitent les capacités de l'IA pour faire des reconnaissances sur les organisations militaires et gouvernementales américaines, entre autres, en cherchant des failles de sécurité, pour acquérir des accès privilégiés au sein des réseaux compromis.

Selon un rapport de Check Point Research, une campagne *HTML Smuggling (technique* consistant à intégrer du code Javascript malveillant dans un fichier HTML légitime) menée depuis la RPC, a ciblé des entités gouvernementales européennes dont l'activité porte sur les politiques étrangères et nationales. Ainsi, le Canada, l'Union européenne (Suède, France, etc.) et d'autres pays subissent des cyber-opérations chinoises explicites à visée d'espionnage, des vols de propriété intellectuelle, d'influence malveillante, de répression transnationale, etc. afin d'éliminer des menaces, à savoir ceux qui servent les "cinq poisons" - les militants pour l'indépendance de Taïwan, les minorités nationales (Ouïghours et Tibétains), le Falun Gong et les partisans de la démocratie et des Droits de l'Homme.

Le régime chinois vise d'une part tous les citoyens chinois vivant à l'étranger (étudiants, chercheurs, hommes d'affaires, etc.), d'autre part les Chinois d'outre-mer, les étrangers d'origine chinoise, et enfin les opinions publiques nationales des pays qui comptent pour Pékin.

Concernant la Fédération de Russie, plusieurs modes opératoires d'attaque réputés chinois auraient été employés pour cibler des entités russes du secteur de la défense depuis les années 2010, à des fins d'espionnage industriel et militaire dans les secteurs spécialisés dans le développement d'équipements de communications satellitaires et de systèmes radio à finalité militaire.

- APT1 (Comment Crew, PLA Unit 61398) a été identifié très tôt. Il est connu pour avoir ciblé des organisations du secteur privé des États-Unis à des fins de cyberespionnage ;
- APT10 (Stone Panda), connu depuis 2009, a été associé à des campagnes visant des opérations gouvernementales, des opérations militaires et des entreprises dans plusieurs secteurs. Selon l'éditeur de sécurité Checkpoint, il serait à l'origine du ciblage d'au moins deux organismes de recherche russes (et potentiellement un à la Biélorussie) œuvrant dans le développement de technologies avancées de défense ;
- APT27 (LuckyMouse ou Emissary Panda) est un groupe de cyberespionnage sophistiqué actif depuis au moins 2010. Il est axé sur des secteurs tels que le gouvernement, l'aérospatiale, l'industrie manufacturière, les télécommunications, la défense, l'éducation, etc. Il exploite les vulnérabilités des accès à distance. Parmi les entités impactées il y a des organismes de recherche publics français ;
- APT41 (Wicked Panda, Winnti, Barium, Double Dragon, …) est un groupe actif, depuis 2012, combinant l'espionnage parrainé par l'État chinois et la cybercriminalité à motivation financière. Ses membres figurent sur la liste des personnes les plus recherchées par le FBI. Ils sont soupçonnés d'être responsables du piratage des chaînes d'approvisionnement dans le secteur de la santé, du vol de données sensibles auprès de sociétés de biotechnologie et du vol de paiements de soutien liés au COVID-19 aux États-Unis ;
- Le groupe d'activistes chinois Mustang Panda cible des organisations non gouvernementales en utilisant des leurres sur le thème de la Mongolie à des fins d'espionnage. Selon CrowdStrike Falcon Intelligence, une nouvelle activité de ce groupe utilise une chaîne d'infection unique pour cibler des victimes probablement basées en Mongolie. Cette nouvelle activité utilise une série de redirections et d'implémentations malveillantes sans fichier d'outils légitimes pour accéder aux systèmes ciblés ;
- Salt Typhoon : il est connu pour avoir prétendument violé les réseaux des fournisseurs d'accès à Internet américains et les systèmes d'écoute électronique, notamment Lumen Technologies, Verizon et AT&T ;
- Le groupe BlackTech (Palmerworm, Temp.Overboard, Circuit Panda et Radio Panda), apparu en 2010, mêle espionnage et cybercrime. Il cible des organisations publiques et des entreprises privées des États-Unis et de l'Asie de l'Est. Il utilise des techniques « *Living-off-the-Land* » basées sur des outils natifs pour mener ses attaques, très difficile à détecter car il n'y a pas de code malveillant ajouté ;
- Un autre groupe, PlushDaemon, spécialisé en cyberespionnage, identifié par ESET Research, opère principalement en détournant les mises à jour d'applications chinoises et a notamment compromis l'installeur d'un VPN sud-coréen. Il cible des individus et des organisations dans six pays : République Populaire de Chine, Taiwan, Hong Kong, Corée du Sud, États-Unis et Nouvelle-Zélande. Sa technique de prédilection consiste à substituer des installeurs légitimes par des versions compromises intégrant son logiciel malveillant SlowStepper, une porte dérobée sophistiquée avec plus de 30 modules.

En décembre 2024, Proofpoint alerte sur de nouvelles activités du groupe TA397 (Bitter) de cyberespionnage, originaire d'Asie du Sud, ciblant les organisations gouvernementales, énergétiques, de télécommunications, de défense et d'ingénierie dans les régions EMEA (Europe, Moyen-Orient et Afrique) et APAC (Asie-Pacifique). Ils utilisent des techniques de spear phishing avec des pièces jointes malveillantes. Ils ont ciblé une organisation turque avec une campagne utilisant pour leurre un projet de financement de la Banque mondiale à Madagascar pour le développement d'infrastructures, thème récurrent du groupe qui cible régulièrement des entités publiques.

Ceux affiliés à la Fédération de Russie

Les groupes russes visent, en particulier, l'Ukraine, les pays de l'Union européenne et les États-Unis. Ces groupes utilisent, entre autres moyens, le *spear phishing* comme accès initial. Peu de groupes russes ont pu être identifiés avec une utilisation de Gemini (IA de Google, générative et multimodale, de type *transformer* présentée en décembre 2023) car ils auraient peut-être une préférence pour des grands modèles de langage (*Large Language Model* - LLM) russes plutôt que ceux offerts par Google.

Leurs utilisations incluent principalement l'assistance à la rédaction de scripts, à la traduction, etc. Par ailleurs, il semble qu'ils se focalisent davantage sur la reconfiguration de logiciels malveillants disponibles publiquement en différents langages de programmation.

Le Canada et ses alliés sont fort probablement une cible intéressante pour l'espionnage de la part de ces groupes notamment par la compromission de la chaîne d'approvisionnement, compte tenu de son statut de pays membre de l'Organisation du Traité de l'Atlantique Nord (OTAN), de son soutien à l'Ukraine et de sa présence dans l'Arctique, dans le but d'influencer sa politique étrangère.

- APT28 (Fancy Bear) en 2022 et le groupe Sandworm (APT44) sont soupçonnés de tentatives d'ingérence dans les processus électoraux en Occident (Allemagne, France, etc.), d'être à l'origine du piratage du gouvernement géorgien en 2008, afin d'obtenir des informations clés juste avant l'invasion du pays par les troupes russes, et d'avoir piraté les échanges électroniques des membres de la Convention nationale démocrate américaine (tentatives de court-circuitage de la campagne présidentielle de Joe Biden, etc.) ;
- APT29 (The Dukes ou Cozy Bear) serait une organisation de cyber-espionnage massivement financée et efficacement coordonnée, travaillant dans l'intérêt de la Fédération de Russie depuis au moins 2008. Son objectif principal de collecter des renseignements permettant d'influencer les décisions en matière de politique étrangère et de sécurité ;
- Selon Microsoft Threat Intelligence, BadPilot, entité du groupe de pirates APT44 (Sandworm, Seashell Blizzard) est connu pour ses attaques destructrices, cherchant à s'infiltrer dans de nombreuses organisations critiques (énergie, commerce de détail, éducation, etc.) de nombreux pays (Amérique du Nord, plusieurs pays d'Europe et d'Afrique, Inde, Pakistan, Chine, Australie, etc.).
  Les analystes de Mandiant (filiale cybersécurité de Google) considèrent que ce groupe APT est soutenu par la Fédération de Russie, affilié à l'unité 74455, le centre principal des technologies spéciales (GTsST) au sein de la direction principale du renseignement militaire russe (GRU).
  Ce groupe a été accusé d'avoir piraté les systèmes d'information des Jeux Olympiques de 2018. Les compromissions d'infrastructures Internet ont permis à Seashell Blizzard de persister sur des cibles de grande valeur et de soutenir des opérations réseau sur mesure (rapporté par The Hacker News).
- Turla (affilié au FSB ?) est actif depuis une vingtaine d'années. Il cible des entités gouvernementales et des agences de renseignement de nombreux pays occidentaux (Pentagone, le Bundestag, etc.) ;
- Callisto (Star Blizzard) est un groupe d'officiers du renseignement russe (FSB) menant des cyber-opérations contre l'UE et des pays tiers par le biais de campagnes d'hameçonnage permanentes visant à voler des données sensibles concernant des fonctions critiques de l'État (États-Unis, UE, etc.) comme des identifiants et des mots de passe valides. Une analyse des *Five Eyes* (coopération menée par les services de renseignement des États-Unis d'Amérique, du Canada, du Royaume-Uni, de l'Australie et de la Nouvelle-Zélande), montrait que Callisto aurait ciblé, en 2022 et 2023, des *think tanks*, des ONG et des entités du secteur de la défense aux États-Unis et en Europe (notamment en Belgique, aux Pays-Bas et en Grande-Bretagne), afin de collecter des identifiants, des mots de passe valides ;
- NoName057(16) est un groupe activiste, actif depuis trois ans, ciblant tout pays qui agit contre les intérêts russes (pays membres de l'OTAN et de l'UE, etc.). Il mènerait exclusivement des attaques DDoS en identifiant les noms de domaine, les adresses IP et cartographiant l'exposition globale de leurs cibles sur Internet. Leur efficacité et leur organisation suggèrent une menace significative pérenne.

- **A propos du scénario des attaques cybernétiques russes vers le système électrique ukrainien**

Afin d'assurer la transmission d'énergie sur des milliers de kilomètres de ligne à haute tension, la synchronisation temporelle est vitale. Le réseau électrique est donc très sensible à une infime variation d'autant plus que le nombre de sous-traitants est élevé. Pour une cybersécurité efficiente, il est indispensable de séparer les systèmes d'information administratifs des environnements industriels.

Lors de la cyberattaque de novembre 2023, les cyberattaquants n'ont pas utilisé, comme en 2022, des *industroyers* (logiciels malveillants publiquement connus ciblant les protocoles industriels pouvant créer des dommages physiques bien réels) de même type que Stuxnet ou Triton, mais ont exploité une vulnérabilité du système de supervision industrielle pour en prendre le contrôle, ce qui leur a permis d'être discrets et non détectables. En même temps, des missiles et des drones survolaient le territoire et attaquaient les bâtiments physiques ukrainiens : c'est la guerre hybride. En mars 2024, ciblant une vingtaine d'entreprises ukrainiennes des secteurs énergétiques, le groupe Sandworm (APT44) avait pour objectif d'amplifier les effets des bombardements de certaines infrastructures énergétiques : convergence entre cyberattaques et opérations militaires conventionnelles.

Ceux affiliés à l'Iran

Ces groupes sont connus pour leurs logiciels malveillants (wiper, etc.) et leurs stratégies de représailles. Ils sont spécialisés dans le *spear phishing*, l'ingénierie sociale, les détériorations de sites Web, les dénis de service distribué, le vol d'informations personnelles identifiables, diverses opérations sur les médias sociaux, etc. Ils ciblent surtout les États-Unis et l'UE. Certains utiliseraient *Generalized Multimodal Intelligence Network* ou Gemini (IA de Google) pour créer des contenus de *phishing* ciblés. Ils exploreront l'IA de Microsoft (Microsoft Azure Copilot) pour recueillir des informations sensibles sur des cibles militaires et les technologies nucléaires.

- Des pirates iraniens avaient exploité une appliance de sécurité Fortigate pour accéder aux réseaux de contrôle de l'environnement d'un hôpital pour enfants basé aux États-Unis. Ils avaient accédé à des comptes d'utilisateurs repérés de l'hôpital à partir d'une adresse IP : *attaque déjouée* ;
- Le groupe Tortoiseshell (Imperial Kitten), apparu en 2018, a mené une campagne d'attaque sur Facebook, en se faisant passer pour des recruteurs et attirer des cibles américaines avant de leur envoyer des fichiers corrompus ou de les inciter à saisir des informations sensibles sur des sites d'hameçonnage ;
- APT34 (Helix Kitten, Cobalt Gypsy, Irn2) vise les gouvernements, les secteurs de la finance, de l'aérospatiale, de l'énergie, des télécommunications, de la chimie, du pétrole et du gaz. Le groupe cible principalement les entreprises du Moyen-Orient ;
- APT35 (Charming Kitten, TA453, Cobalt Illusion, Magic Hound, ITG18, Phosphorus, Newscaster) pratique des attaques de type « *watering hole* » (trou d'eau) utilisant des sites web légitimes compromis mais pertinents pour les victimes ciblées.
  Il usurpe l'identité de sites en ligne populaires (Google, Microsoft, Yahoo) pour recueillir les informations d'identification des utilisateurs. Des liens existeraient entre ce groupe et Memento, une souche de ransomware déployée dans des attaques à l'automne 2021 ;
- APT42, actif depuis 2015, est un groupe de cyberespionnage, chargé de mener des opérations de collecte d'informations et de surveillance contre des personnes et des organisations présentant un intérêt stratégique pour le gouvernement iranien. Il cible diverses organisations de nombreux pays (Australie, UE, Moyen-Orient et aux États-Unis) ;
- Le groupe MuddyWater (Earth Vetala, Static Kitten, Seedworm, …) effectuent des attaques mondiales contre des infrastructures vulnérables : avis conjoint du 24 avril 2022 par la *National Security Agency* (NSA), le *Federal Bureau of Investigation* (FBI), la *Cybersecurity and Infrastructure Security Agency* (CISA), le Centre national de cybersécurité du Royaume-Uni, la *Cyber National Mission Force* des États-Unis et des organismes chargés de l'application de la loi. Il mène des activités de cyberespionnage et des campagnes malveillantes dans divers secteurs - défense, télécommunications, pétrole et gaz naturel, administrations locales - en Europe, en Afrique, en Asie et en Amérique du Nord ;
- Récemment, le groupe Emennet Pasargad (Cotton Sandstorm, Marnanbridge ou encore Haywire Kitten) étend ses activités à de nouvelles cibles en dehors des États-Unis et d'Israël. Il intègre l'utilisation de caméras IP et d'autres actifs informatiques dans ses offensives, posant un défi particulier pour les mesures de sécurité traditionnelles. Il offre ses services à d'autres groupes menaçant de bouleverser l'équilibre du cyberespace au Moyen-Orient, en Europe (France, Suède, etc.) et même au-delà.

Ce groupe œuvre sous le nom d'Aria Sepehr Ayandehsazan (ASA). Il serait parvenu à compromettre un fournisseur français d'affichage dynamique commercial durant les Jeux olympiques afin de détourner des bornes d'affichage publicitaire en y incrustant des photomontages dénonçant la participation d'athlètes israéliens. L'opération a été contrée avant qu'elle ne se réalise.

Par exemple, le FBI estime que cette entité s'est, pendant deux ans, fait passer pour un groupe de hacktivistes propalestiniens (Hackers of Savior), afin d'attaquer plusieurs cibles israéliennes, en dérobant puis en faisant fuiter des données ainsi qu'en modifiant la page d'accueil de plusieurs sites…

Ceux affiliés à la Corée du Nord

La Corée du Nord a de grandes ambitions dans des domaines scientifiques et techniques, comme le nucléaire, l'armement, l'aérospatial, les crypto-monnaies, les chaînes d'approvisionnement, etc. Cependant, le pays est tenu sous embargo et n'a pas accès, de manière légale, aux équipements technologiques dont elle aurait besoin pour se développer en raison du double usage, civil et militaire, qui peut en être fait. ESET Research signale qu'une des tactiques utilisées consiste à œuvrer sans que l'attaque soit signalée, afin d'accroître son efficacité. L'attaquant se fait alors passer comme recruteur pour le compte de ces entreprises : les victimes sont invitées à faire part de leur identité et de leurs compétences techniques sous forme de test en ligne et le piège se referme. L'objectif est d'avoir des renseignements sur la technologie militaire et nucléaire sud-coréenne.

- APT37 (Vedalia, ScarCruft, Reaper) est un groupe ayant déployé une porte dérobée et un cheval de Troie d'accès à distance non documentés auparavant, appelés VeilShell (logiciel malveillant de type *backdoor* basé sur PowerShell), dans le cadre d'une campagne ciblant les pays d'Asie du Sud-Est, afin de recueillir et d'exfiltrer des informations sur le système ;
- APT38 (Lazarus Group) est certainement à l'origine du vol du logiciel Wanacry développé par la NSA. Ce collectif s'est illustré par de multiples actions dans le domaine de l'intrusion numérique depuis 2014 (incursion chez Sony Pictures en 2014, se traduisant par une fuite massive de données sensibles), etc. Sa stratégie vise à décrédibiliser la cybersécurité mondiale et à générer des revenus pour le gouvernement. Il est soupçonné d'avoir détourné des dizaines de millions de dollars de crypto-monnaies ;
- En 2021, l'Institut coréen de recherche sur l'énergie atomique (KAERI) a fait savoir qu'il avait été compromis par l'exploitation d'une vulnérabilité dans une passerelle VPN. Selon les autorités, cette compromission serait due au groupe nord-coréen, Velvet Chollima ou Kimsuky, référencé APT43 par Mandiant : résultat d'une campagne de cyber-espionnage contre des groupes de réflexion sud-coréens.

Ceux affiliés à l'Inde

- Le groupe SideWinder (RattleSnake et T-APT-04), actif depuis 2012, de haut niveau de connaissances, est soupçonné d'origine indienne. Il cible les forces armées et les forces de l'ordre au Pakistan, au Bangladesh et dans d'autres pays d'Asie du Sud. Ses secteurs d'activités sont essentiellement liés aux forces policières, militaires, maritimes et navales, aux affaires étrangères, aux organisations scientifiques, au secteur de la défense, de l'aéronautique, de l'industrie informatique et les cabinets juridiques.

Ceux affiliés au Pakistan

- APT-36 (Transparent Tribe) est un groupe, qui serait lié au Pakistan, ciblant surtout les employés d'organisations gouvernementales indiennes. Par exemple, les cyberattaquants ont créé des sites web images des sites officiels du gouvernement indien. Ainsi des utilisateurs peu méfiants sont amenés à saisir leurs informations d'identification.

Ceux affiliés au Kazakhstan

- Par exemple, le groupe SturgeonPhisher, signalé par ESET, mène une campagne au Moyen-Orient. Il est à l'origine d'une attaque contre un site d'information (région Gilgit-Baltique), de type *watering-hole*.

Ceux affiliés à la Biélorussie

- Par exemple, le groupe Winter Vivern qu'ESET considère comme une équipe de pirates, est aligné sur les intérêts biélorusses et exploite une vulnérabilité *zero-day* dans la messagerie Roundcube ;
- Le groupe Ghostwriter (UNC1151, Storm-0257) serait originaire de Biélorussie. Selon la société de cybersécurité Mandiant, il a diffusé de la désinformation critique à l'égard de l'OTAN depuis 2016 ;
- Selon l'ANSSI, les données auraient été divulguées par deux groupes prorusses, Beregini et Zarya, qui dénoncent la lutte contre le dopage comme un chantage à l'encontre des pays qui mènent une politique opposée à celle des États-Unis.

Ceux affiliés aux États-Unis d'Amérique

- L'Équation Group, spécialisé en cyberespionnage de haut niveau, lié à la (NSA), est connu pour avoir diffusé les malwares Wanacry (ransomware) et NotPetya* (type *wiper* destruction des données) en 2017, dans plus de 150 pays et des entreprises comme Telefonica, FedEx, Saint Gobain, Renault, certains aéroports, les services de santé britanniques, etc. gravement impactées ;
- Il aurait travaillé avec le groupe israélien Unit 8200 concevant le virus Stuxnet ayant mis à mal le programme nucléaire iranien entre 2005 et 2015, en ciblant les systèmes de contrôle industriel et d'acquisition de données (SCADA) ;
  **NotPetya est un malware initié en Fédération de Russie, œuvrant en Ukraine, puis dans le monde entier ;*
- Le groupe Shadow Brokers s'est fait connaître par l'ambiguïté autour de son identité et de ses motivations, et par la nature des informations qu'il prétendait détenir. Leur cible était le groupe Equation. Il a réussi à publier et à vendre aux enchères des outils utilisés par la NSA. Avec la volonté de générer du profit et de transmettre des messages de nature politique et idéologique, il est devenu le symbole d'un nouveau type de guerre cybernétique, ses actions ont permis de montrer les limites des actions défensives et la capacité de manipulation offerte par le cyberespace : l'anonymat et l'impossible attribution des attaques.

Ceux affiliés à Israël

- Unit 8200 est un groupe illustrant les cellules de hackers à la fois clandestines et dépendantes d'un pouvoir étatique : entité approuvée par le gouvernement israélien. Intervenu pour défendre les institutions du pays et mener des actions de contre-terrorisme, il s'est fait connaître par ses campagnes d'espionnage de masse, auprès de gouvernements étrangers et de civils.
  Il a participé au développement de Stuxnet, ver informatique conçu avec la NSA pour perturber les infrastructures nucléaires iraniennes et du logiciel espion Duqu 2.0 qui a permis d'infiltrer Kaspersky Labs (géant russe des services de cybersécurité), d'infecter les hôtels suisses et autrichiens ayant accueilli les grandes négociations internationales avec l'Iran au cours de l'année 2015.

Eléments de tendances des APT en 2025

Les analyses détaillées du rapport High-Tech Crime Trends Report 2025 de Group-IB, l'un des leaders mondiaux de la cybersécurité, exposent que la prolifération des APT a intensifié les cyber risques mondiaux, avec une augmentation de 58% des attaques attribuées aux APT enregistrées en 2024 :

- En Europe, les groupes de menace APT28 (présumés russe) et Gamaredon (groupe de cyberespionnage présumé russe) ciblent des organisations militaires, des ONG, des autorités judiciaires, des forces de l'ordre et des organisations à but non lucratif en Ukraine depuis au moins 2013). Ils se sont concentrés sur les secteurs gouvernementaux, énergétiques et militaires dans un contexte de tensions géopolitiques ;
- Le Moyen-Orient et l'Afrique connaissent une activité accrue de la part d'organisations telles que OilRig (Iran) et MuddyWater (Iran), ciblant les services financiers et l'énergie ;
- L'Asie-Pacifique a été confrontée aux menaces d'APT10 (RPC) qui s'est attaqué aux technologies de l'information et à l'industrie manufacturière, tandis que le célèbre Lazarus Group (Corée du Nord) a intensifié le vol de crypto-monnaies et DarkPink (nouveau groupe APT) a ciblé les organisations gouvernementales et militaires de la zone Asie-Pacifique (APAC) tels le Cambodge, l'Indonésie, la Malaisie, les Philippines, le Vietnam, ainsi que des organisations religieuses à but non lucratif, et l'Europe. Utilisation de courriels de *spear-phishing* ciblés ;
- Quant à l'Amérique du Nord, elle a été la cible de Dark Halo (UNC2452, SolarStrom), qui a lancé des campagnes de cyberespionnage contre les secteurs de l'informatique, des services financiers et de la défense. Il est actif depuis 2019, a priori. Le groupe a lancé plusieurs opérations de reconnaissance contre les principaux fournisseurs des États-Unis et les organisations gouvernementales ;
- En Amérique latine, APT10 (RPC) a étendu ses opérations au Brésil, s'attaquant aux télécommunications et aux institutions financières.

7.4.4 Quelques modes opératoires

- Au-delà des actions purement criminelles, il existe des serveurs proxys souvent utilisés par des états non-amis. *Rappels* : *En entreprise, par exemple, l'usage d'un serveur proxy permet d'anonymiser les adresses IP internes et de mettre en cache le contenu afin d'améliorer la vitesse de transfert des données et donc de réduire l'utilisation de la bande passante. Il peut aussi filtrer le contenu qui ne doit pas être téléchargé sur le réseau de l'entreprise : c'est un intermédiaire entre le web et les machines clients.*

  Cependant, lorsque des personnes se connectent à un tel serveur qui serait contrôlé par un attaquant, l'adresse IP sortante est enregistrée sur le serveur. Les attaquants sont alors en capacité d'initier une attaque par déni de service (DDoS). Cette IP peut aussi leur indiquer que les salariés naviguent sur le site, ce qui donne la possibilité de créer des attaques plus ciblées comme le *phishing.*

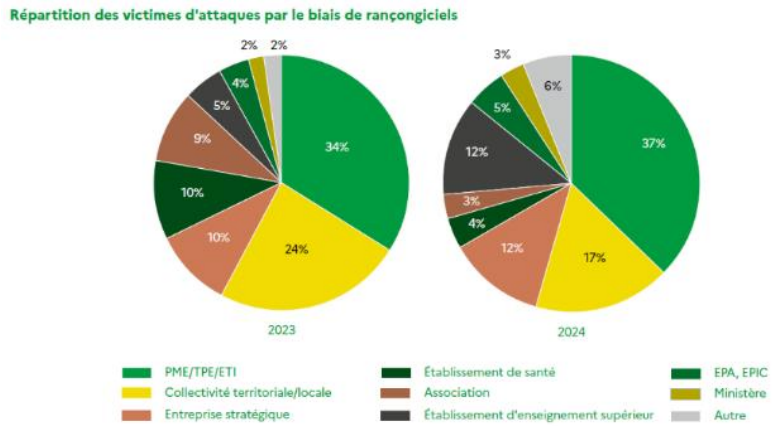
  Les serveurs proxy gratuits représentent le plus grand risque : les cyberattaquants hébergent des serveurs proxys pour inciter les utilisateurs à s'y connecter et à divulguer des données sensibles. Tout le trafic qui passe par un proxy est accessible à l'administrateur du serveur. Dans le cas où il n'y a pas de chiffrement des flux de données, cela conduirait à une usurpation d'identité ou à une prise de contrôle du compte ;
- Les *Distributed Denial of Service* ou 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. Cela entraîne une suractivité des *botnets* IoT avec une perte de contrôle des machines, des capteurs industriels, etc. La 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. Ces botnets exploitent toute défaillance du SI ou failles rencontrées ;
- Les logiciels malveillants (*malware*) sont des logiciels 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.
  Aujourd'hui, un logiciel malveillant en tant que service (*Malware-as-a-Service* - MaaS) est un modèle commercial utilisé par les cybercriminels connus sous le nom d'opérateurs MaaS. Ces derniers distribuent leurs logiciels sur le *dark web* et fournissent même parfois une assistance à la clientèle malveillante.
  Des modèles opérationnels de cybercriminalité comme service (*cybercrime-as-a-service* - CaaS), permettent des attaques cybercriminelles ;

- 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.
  - Le *phishing* et le *smishing* consistent à envoyer un e-mail ou un SMS en se faisant passer pour un organisme reconnu (banque, fournisseur d'accès Internet ou site de commerce en ligne, etc.) ou un établissement public (Trésor public, La Poste, etc.). Le but est d'inciter à cliquer sur des pièces jointes ou des liens malveillants pour ensuite récupérer des informations personnelles, etc.
  - Le *vishing* ou hameçonnage par téléphone est une arnaque téléphonique utilisant le plus souvent des techniques d'ingénierie sociale (usurpation d'identité) dont le but est de faire réaliser des opérations frauduleuses ou de soutirer des informations personnelles et/ou bancaires. La finalité est identique à celle du *phishing* qui repose quant à elle sur l'envoi d'e-mails frauduleux alors que le *vishing* s'appuie sur des appels téléphoniques frauduleux.
  - Le *spoofing* est une technique de cybercriminalité qui vise à vous mettre en confiance en usurpant l'adresse du courriel de l'expéditeur ou d'un organisme reconnu (France Travail, le Trésor public, etc.). Les fraudeurs vont tenter de gagner votre confiance en déguisant leur véritable numéro d'appel et en le remplaçant par le numéro de téléphone de l'organisme ou de la personne usurpée ;
- 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 d'une mauvaise configuration, de vulnérabilités, etc. ;
- 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 Fédération de 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 ;
- 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 ;

> Selon le rapport de l'Observatoire de la sécurité des flux et des matières énergétiques, l'électricité est une composante vitale du mode d'organisation de nos sociétés dont dépendent l'approvisionnement en eau, la conservation de la nourriture, l'ensemble de l'économie mondialisée et des modes de communication. L'approvisionnement en électricité reposent sur des réseaux d'infrastructures assurant la production et la distribution de la ressource. Ce sont évidemment des éléments stratégiques de la défense et de la sécurité nationale. Ils sont devenus des cibles physiques. Les mutations techniques et la dynamique de transition énergétique augmentent de fait leur vulnérabilité. *Source* : Architecture électrique européenne, Observatoire de la sécurité des flux et des matières énergétiques, IRIS, octobre 2024 : Rapport - Synthèse.

- Mise en œuvre de l'exploitation du système de publicité en ligne pour surveiller, traquer et infiltrer - l'*Advertising Intelligence* (ADINT) qui utilise les données publicitaires et les mécanismes de ciblage, détournés à des fins de renseignement. Les cyberattaquants visent des utilisateurs via des publicités malveillantes sans rechercher des vulnérabilités du système d'information, car ces publicités contiennent des *scripts* ou des liens vers des sites compromis : *au premier clic sur la page web de publicité, le navigateur est exploité pour récupérer et exécuter un code malveillant, en toute discrétion sans que l'utilisateur en ait conscience*. Ils ont alors tout loisir de récupérer des données de géolocalisation de l'utilisateur, à des fins de surveillance ou d'espionnage, par exemple. Ces techniques d'attaque impactent directement la vie privée de militaires, de diplomates, du personnel politique français, de dirigeants d'entreprises stratégiques mais aussi des convoyeurs de fonds, du personnel pénitentiaire, etc.

- Le cybersquatting est une pratique malveillante qui consiste à enregistrer un nom de domaine similaire ou identique à celui d'une entreprise (quand celle-ci n'a pas enregistré son nom de domaine, par exemple), d'une marque ou d'une personnalité publique, dans le but de collecter des données personnelles et de s'enrichir en tirant profit de la notoriété de celle-ci ;
- Le typosquatting exploite les erreurs de frappe ou typographiques que les internautes peuvent faire en tapant les adresses de site ;
- 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 TPE, PME et ETI sont les entités françaises les plus touchées (37% des cas).

La proportion de collectivités territoriales à être affectées par un rançongiciel a diminué (17% pour 24% en 2023), tout comme celle des établissements de santé (4% pour 10% en 2023).

Les attaques contre les établissements d'enseignement supérieur représentent 12% du nombre total de compromissions de ce type, contre 5% en 2023.

@ itforbusiness.fr

Le rançongiciel RansomHub (2024), variante de Cyclops et Knight, s'est imposé en ayant pris la place de LockBit 3.0 et d'Alphv. Selon la *Cybersecurity and Infrastructure Security Agency (CISA),* RansomHub a déjà chiffré et exfiltré des données d'au moins 210 victimes dans divers secteurs (l'eau, les eaux usées, les technologies de l'information, les services et installations gouvernementaux, la santé publique, etc.).

En novembre 2024, la police néerlandaise, le FBI, l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) et d'autres organisations ont démantelé le célèbre « infostealer » RedLine Stealer, lors de l'Opération Magnus.

7.4.5 La guerre cognitive, une nouvelle menace ?

La guerre cognitive (*cognitive warfare*) désigne l'ensemble des offensives intentionnelles visant à manipuler la cognition d'individus, de groupes ou de populations afin d'altérer ou d'infléchir leur manière de penser (raisonnement, prise de conscience, prise de décision, etc.) à des fins hostiles, par une approche scientifique et en utilisant des moyens technologiques inédits, en particulier numériques. Elle s'appuie aussi sur l'usage des réseaux sociaux et d'opinions radicales, une méfiance croissante envers les institutions, une connaissance incomplète ou biaisée des relations internationales et des sujets sociétaux, des ingérences de toute sorte, etc. Elle concerne les secteurs civil et militaire.

- Elle met en lumière les possibilités de manipulation offertes par les sciences de la cognition à des acteurs hostiles (propagande, désinformation, etc.) ;
- Elle englobe les opérations visant à corrompre les mécanismes de pensée de l'adversaire et à altérer sa capacité de décision grâce à une approche scientifique ;
- Elle affecte les capacités cognitives des individus par le biais des technologies, pouvant influencer à court terme leur attention et leurs réactions, et à long terme leur structure cognitive ;
- Pour y faire face, il s'agit notamment de protéger physiquement les individus en situation stratégique et de promouvoir un usage raisonné du numérique, malgré les défis ;
- Le projet Gecko vise à développer des dispositifs d'exploration de la guerre cognitive dans le cadre de crises fictives, pour préparer les acteurs d'opérations liées à la sécurité nationale. Il est porté par l'Institut National des Langues et Civilisations Orientales (INALCO), en collaboration avec l'Ecole nationale supérieur de cognitique de l'Institut Polytechnique de Bordeaux (ENSC - Bordeaux INP) et l'Institut de Recherche Stratégique de l'Ecole Militaire (IRSEM) et mené dans le cadre du dispositif d'Accompagnement Spécifique des Travaux de Recherches d'intérêt Défense (ASTRID) financé par l'Agence de l'innovation de défense (AID) et hébergé par l'Agence nationale de la recherche (ANR).
  Source : Bernard Claverie, La guerre cognitive : le nouveau champ de bataille qui exploite nos cerveaux, Polytechnique Insights, 5 février 2025.

7.4.6 Eléments de bilan cyber des Jeux Olympiques et Paralympiques de Paris 2024

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été cheffe de file du volet cybersécurité dans la préparation et la conduite des Jeux Olympiques et Paralympiques (JOP) de Paris 2024. Le dispositif mis en place, en étroite collaboration avec les différentes structures impliquées dans l'organisation des Jeux - dont en particulier la Délégation interministérielle aux Jeux Olympiques et Paralympiques (DIJOP), le ministère de l'Intérieur et des Outre-Mer (MIOM) et le Comité d'Organisation des Jeux Olympiques et Paralympiques (Paris 2024) - s'articulait autour de cinq axes principaux :

- Parfaire la connaissance des menaces cyber pesant sur les Jeux ;
- Sécuriser les systèmes d'information critiques ;
- Protéger les données sensibles ;
- Sensibiliser l'écosystème des Jeux ;
- Se préparer à intervenir en cas d'attaque cyber affectant les Jeux.

Avec le soutien de la Coordination nationale pour la sécurité des Jeux (CNSJ) du ministère de l'Intérieur et des Outre-mer et de Paris 2024, l'ANSSI a identifié un écosystème JOP d'environ 500 entités, réparties en 3 catégories selon leur criticité, en vue d'une stratégie de sécurisation préventive.

Plusieurs exercices de crise ont par ailleurs été organisés en 2023 pour se préparer collectivement à réagir à toute cyberattaque affectant les JOP. Cela a permis de déterminer les actions à réaliser prioritairement (mises à niveau de milliers de serveurs pour bénéficier de tous les correctifs de sécurité, homologation de systèmes d'information critiques, etc.).

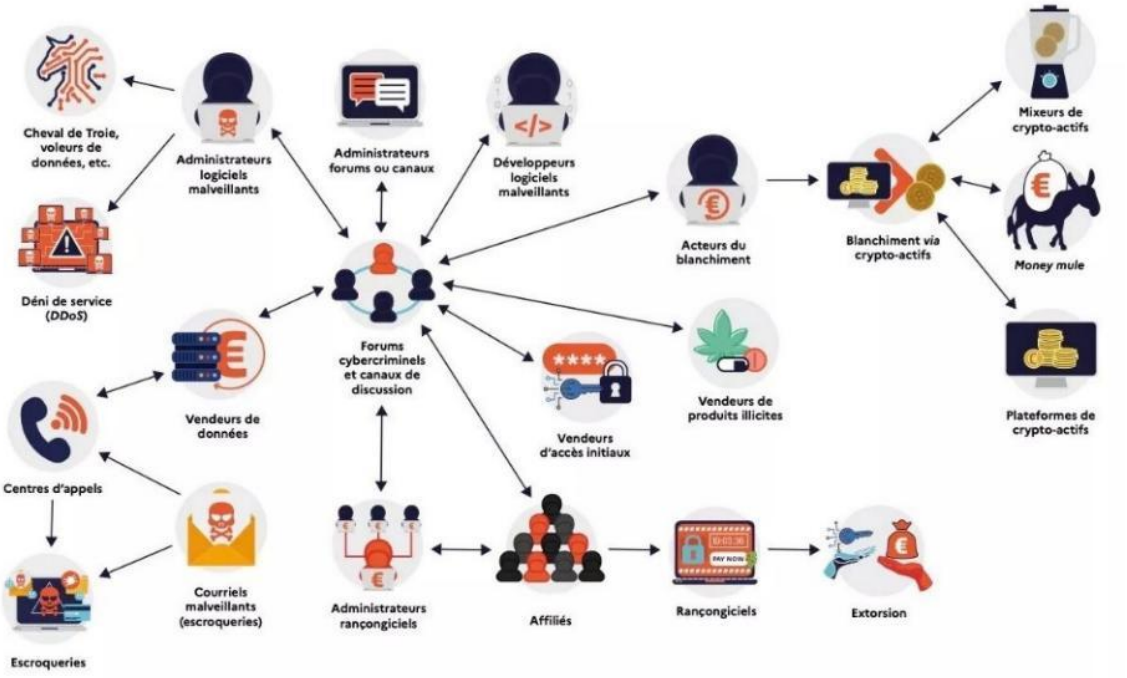
De plus, les partenaires nationaux et internationaux de l'ANSSI ont été sollicités et mobilisés de manière régulière en amont des JOP afin de garantir la coopération dans le cadre de cet événement international. Durant l'événement, l'information cyber liée aux Jeux a par ailleurs fait l'objet d'un partage régulier avec les partenaires internationaux, tant de manière bilatérale que dans le cadre de dispositifs dédiés, en particulier le Centre de coopération internationale (CCI) et le réseau européen de gestion de crise EU-CyCLONe.

Un total de 548 événements de cybersécurité affectant des entités en lien avec l'organisation des JOP entre le 8 mai et le 8 septembre 2024, ont été recensés et ont donné lieu à un traitement par les équipes opérationnelles. Près de la moitié d'entre eux correspondaient à des indisponibilités dont un quart sont dues à des attaques par déni de service (DDoS). Le reste des événements concernent des tentatives de compromission ou des compromissions, des divulgations de données ou bien encore des signalements de vulnérabilités. Les secteurs d'activité ciblés sont les entités gouvernementales, le sport, le divertissement (sites de compétition et Paris 2024) et les télécommunications.

En conclusion, l'ANSSI et ses partenaires nationaux ont accompagné plusieurs victimes dans la résolution d'incidents. Malgré une intensité élevée, les événements de cybersécurité n'ont pas affecté ou ont eu que de faibles impacts sur les cérémonies d'ouverture, de clôture et le bon déroulement des épreuves. Comme attendu, des tentatives de déstabilisation, de l'espionnage et des attaques à but lucratif ont été observées.

7.4.7 Modélisation d'un écosystème cybercriminel

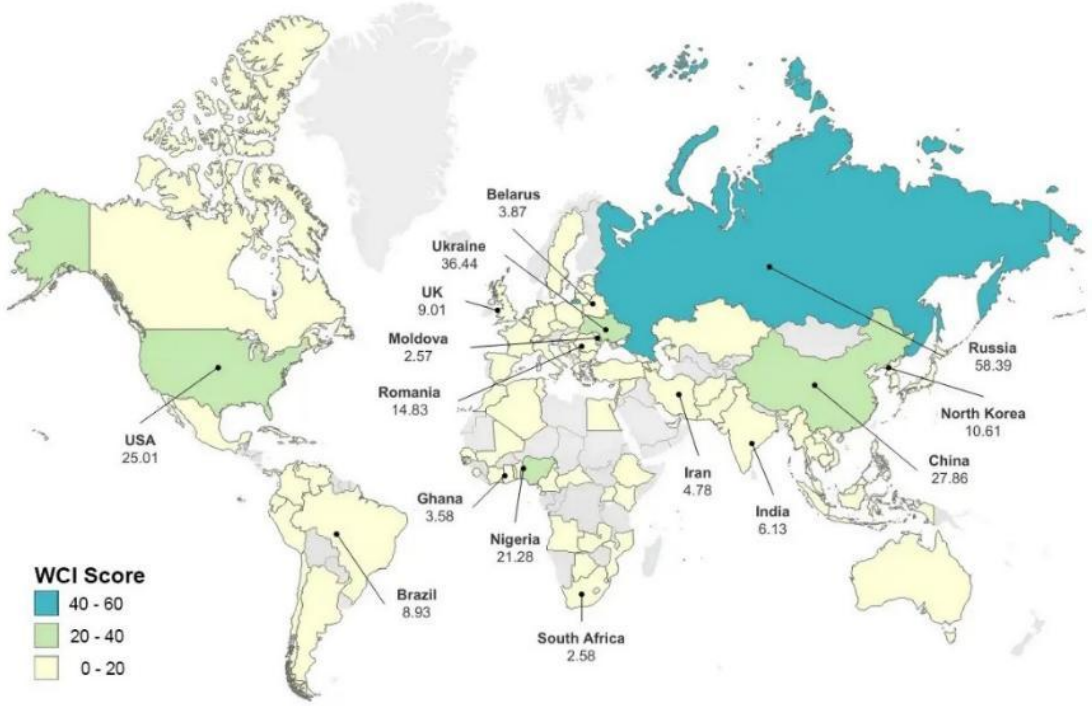
La criminalité numérique s'est professionnalisée de manière significative en matière d'appropriation des outils techniques et d'industrialisation des processus cybercriminels. Pour mettre en oeuvre leurs activités illicites, les acteurs malveillants s'appuient sur de nombreux vecteurs (serveurs, logiciels malveillants, etc.) et canaux de communication (forums, messageries chiffrées, réseaux sociaux, etc.) leur permettant d'interagir et d'optimiser leurs actions.



Exemple de modélisation d'un écosystème cybercriminel

La cybercriminalité recouvre l'ensemble des délits et crimes commis à l'encontre ou par le biais des systèmes d'information. Chaque année, des milliers de dépôts de plainte sont enregistrés par les unités de la gendarmerie nationale et les services de la police nationale concernant des escroqueries, des services illicites, des atteintes aux personnes, aux institutions, aux systèmes d'information, etc.

Le coût annuel de la cybercriminalité en France est évalué à 100 milliards d'euros (Technology Market Insights Statista) avec une progression moyenne de 30% par année, due à diversification et au perfectionnement ainsi qu'au haut niveau des attaquants.



Représentation cartographique du World Cybercrime Index

Les 15 premiers pays identifiés, © 2024 Bruce et al. & OpenStreetMap)

En avril 2024 a été publié le premier classement mondial de la cybercriminalité (*World Cybercrime Index* - WCI) donnant une évaluation du niveau d'impact, de professionnalisation et de technicité des activités criminelles produites dans ces États. C'est le résultat de travaux de recherche et d'analyse de chercheurs universitaires ayant interrogé 92 grands experts de la cybercriminalité et traité les résultats selon une méthodologie scientifique. Cinq catégories de cybercriminalité ont été étudiées (produits ou services techniques, attaques et extorsion, vol de données ou d'identité, escroqueries en ligne, et décaissement ou blanchiment d'argent).

Quatre ans ont été nécessaires pour mener l'étude au sein du projet d'envergure ERC CRIMGOV (2021-2026), afin de mieux comprendre le crime organisé, de la cybercriminalité en Europe au commerce international de drogues de la Colombie vers l'Europe, en passant par l'émergence d'une gouvernance criminelle à l'intérieur et à l'extérieur des prisons. Ainsi, le classement proposé montre la spécialisation de certains pays : le Nigéria se classe au premier rang pour les escroqueries en ligne, la Corée du Nord juste derrière la Fédération de Russie et l'Ukraine pour les attaques et extorsions, les encaissements frauduleux et le blanchiment sont la première catégorie au Royaume-Uni, etc.

Tous types de menaces confondues, la Fédération de Russie arrive en tête, suivie par l'Ukraine, la Chine, les États-Unis, le Nigéria et la Roumanie. Chacun de ces pays se classe aussi dans le top 10 pour chacune des catégories de menaces. Toutefois, 97 pays ont été désignés par au moins un expert comme étant un point chaud pour une catégorie particulière. La France arrive ainsi en 30ème position de l'indice global de cybercriminalité.

Cet indice pourrait donc permettre aux acteurs publics et privés de cibler les efforts de prévention en les concentrant là où ils sont les plus utiles, notamment en différenciant les types de cybercriminalité.

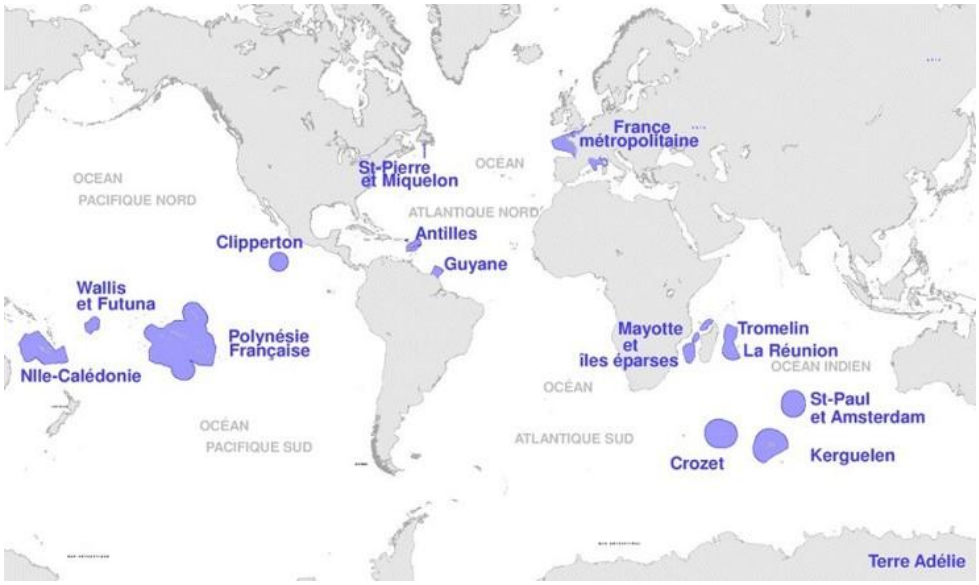
Les résultats révèlent qu'un petit nombre de pays représente la menace cybercriminelle la plus importante. Le *WCI* donne des indications précieuses sur la dimension locale de la cybercriminalité en aidant à lever le voile de l'anonymat qui protège les cybercriminels et renforcer les efforts déployés au niveau mondial.

7.4.8 Le secteur maritime

Pour mémoire, après les deux conflits mondiaux, la Communauté internationale par la voix de l'ONU a eu pour objectif d'établir la souveraineté des États sur leurs espaces maritimes proches afin de prévenir les conflits, de définir les différents espaces maritimes susceptibles d'être revendiqués par les États côtiers ainsi que les droits et obligations des États sur l'ensemble de ceux-ci. Ainsi, le 10 décembre 1982, la Convention des Nations Unies sur le droit de la mer (CNUDM), à Montego Bay en Jamaïque, a été signée. Elle est entrée en vigueur le 16 novembre 1994 (adhésion de 160 états) et a été ratifiée par la France le 11 avril 1996. Plusieurs États n'ont pas signé (États-Unis d'Amérique, Turquie et Israël, des pays d'Amérique Latine et quelques États enclavés).

La création des Zones Économiques Exclusives **(**ZEE) relève de cette Convention de Montego Bay. Ainsi, la ZEE est une bande de mer ou d'océan située entre les eaux territoriales et les eaux internationales, sur laquelle un État riverain (parfois plusieurs États dans le cas d'accords de gestion partagée) dispose de l'exclusivité d'exploitation des ressources. La ZEE est donc constituée d'une bande limitée par la ligne des 200 milles marins internationaux (370 km) à partir de la ligne de base en l'absence d'autre rivage. Si le rivage le plus proche est à moins de 200 milles nautiques, on trace, en principe, la frontière à mi-distance des lignes de base des deux pays riverains. Il est prévu l'extension des droits d'exploitations sur le sous-sol et le sol du plateau continental, à l'exception de la colonne d'eau et des eaux de surface, et au-delà des 200 milles marins jusqu'à 350 milles marins, dans la limite du rebord externe de la marge continentale (1 mille marin, 1 nautique, 1 M =1,852 km).

La ZEE de la France est, conformément au droit de la mer, l'espace maritime sur lequel elle exerce des droits souverains en matière d'exploration et d'usage des ressources. C'est crucial : elle dispose, en raison de son passé historique, de la deuxième ZEE (10 186 624 km^2) après celle des États-Unis d'Amérique (11 351 000 km^2), devant celles de l'Australie (9 025 053 km^2), de la Fédération de Russie (7,6 millions de km^2) et du Royaume-Uni (6,8 millions de km^2). La maîtrise de sa ZEE en pleine souveraineté est un atout considérable pour la France qui est présente sous toutes les latitudes et dispose donc d'un patrimoine unique à explorer, valoriser et préserver. Les territoires ultramarins concentrent 95 % de la faune vertébrée et de la flore terrestre française, 10 % des récifs mondiaux et 55 000 km^2 de récifs et de lagons, 20 % des atolls coralliens mondiaux (principalement en Polynésie française) et le plus grand champ d'algues d'Europe en mer d'Iroise.



© Wikipédia - La représentation en planisphère ne permet pas de rendre compte de la taille réelle des surfaces indiquées.

La ZEE française :

- Intérêts économiques puissants
- Enjeux stratégiques majeurs
- Questions géopolitiques
- Problématiques environnementales cruciales
- Défis scientifiques et énergétiques fondamentaux

L'économie mondiale repose largement sur les échanges maritimes, organisés selon des routes qui relient les bassins de production aux foyers de consommation. Mais ces routes ne compte qu'un nombre limité de lieux de passage - caps, détroits, grands canaux, etc. - dont plusieurs sont aujourd'hui en crise.

Face à l'importance grandissante des océans dans la géopolitique mondiale, le texte de cette Convention est confronté à des interprétations divergentes, ce qui est source de conflits. Plusieurs états riverains de la Méditerranée occidentale, n'ont pas voulu signer la Convention de Montego Bay, ce qui a pour conséquence des tensions et des litiges maritimes accentués par la découverte de gisements d'hydrocarbure et gaziers au cours des dernières années (principalement au large de la Syrie, du Liban et de la bande de Gaza).

La France renforce le dispositif de protection et de mise en valeur des espaces marins qu'elle contrôle. Cette stratégie nationale à laquelle concourent plusieurs administrations et services est connue sous l'appellation générale d'Action de l'Etat en Mer : c'est une organisation française spécifique en une unité de mission, de décision et d'action sous contrôle direct du chef du gouvernement, réalisée par différentes composantes administratives avec le rôle central dévolu à la Marine nationale. Le Secrétaire Général de la Mer (SGMer), poste assuré généralement par un haut-fonctionnaire auquel est associé un Secrétaire Général Adjoint issu de la marine avec le grade d'Amiral, exerce une mission de contrôle, d'évaluation et de prospective, assure la coordination du suivi des textes relatifs à la mer et en propose les adaptations nécessaires, compte tenu de l'évolution du droit international et communautaire. A ce niveau décisionnel ne se trouvent que deux autres organismes, le Secrétariat Général de la Défense Nationale (SGDN) et le Secrétariat Général du Gouvernement (SGN).

Le Préfet maritime dirige les opérations en France métropolitaine alors que ce sont le Préfet de région et le commandant de région maritime qui décident conjointement dans l'espace ultra marin.

Les câbles sous-marins

Les câbles sous-marins constituent un enjeu cyber majeur en milieu maritime. En effet, ils assurent la quasi-totalité des échanges de données entre continents. Depuis les premiers câbles télégraphiques du XIX^{e} siècle jusqu'aux fibres optiques actuelles, sur des distances de plusieurs milliers, voire dizaines de milliers de kilomètres, ils permettent de faire transiter de gigantesques flux internationaux de données (courriels, vidéos, transactions bancaires, données de géolocalisation, etc.).

Aujourd'hui, 98 à 99% de l'internet mondial transite par les câbles sous-marins. La France est le leader mondial dans la pose des câbles et les moyens de haute technologie déployés.

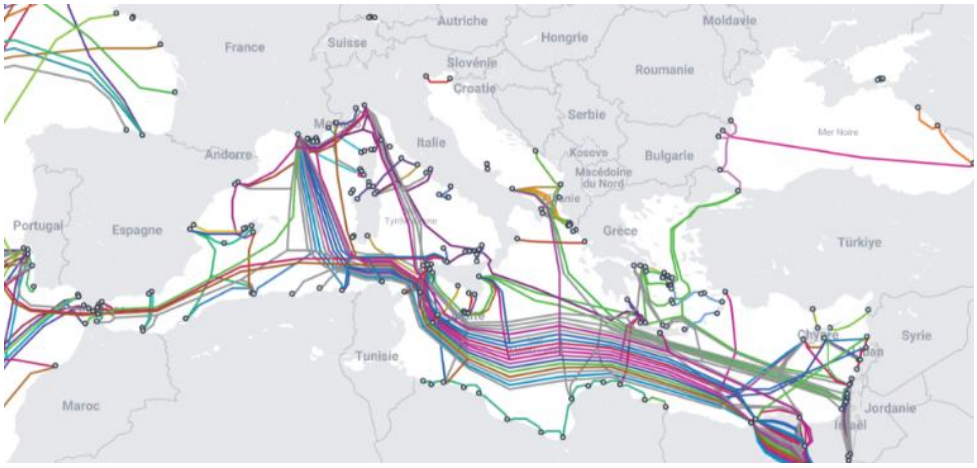
Pour mémoire, en Europe, plus de 90 % des câbles sous-marins de communication sont contrôlés par les GAMAM (Google, Apple, Meta, Amazon et Microsoft) à la place des grands opérateurs internationaux. Le groupe français Alcatel Submarine Networks (ASN), premier fabricant européen de câbles sous-marins de fibre optique, estime que 70 % des projets mondiaux actuels, notamment transpacifiques et transatlantiques, sont supportés par ces géants du web.

Sur la planète, 597 systèmes de câbles et 1 712 atterrissements sont actuellement en service ou en cours de construction. Ce sont près de 1,5 millions de km qui sont posés sur le fond des mers. Dans ce maillage mondial, la Méditerranée est une artère majeure reliant l'Asie à l'Europe.

La ville de Marseille, avec la connexion de 18 câbles sous-marins, occupe la 7ème place mondiale, bientôt la 5ème ? pour la capacité de données sachant que de nombreux *data-centers* y sont installés ou en cours de réalisation. Le futur câble, le Sea-Me-We-6, long de 21 700 km, reliera la France à Singapour.

Les câbles sous-marins sont devenus un vrai sujet de préoccupation pour les États. D'abord au titre de la sécurité, les câbles pouvant faire l'objet de menaces criminelles, terroristes ou militaires. Mais aussi au titre de l'environnement, la pose de câbles dans des aires marines protégées est devenu l'objet d'une véritable attention de la part des pouvoirs publics. Face à ce défi des télécommunications, la France renforce actuellement ses moyens de surveillance et de protection du réseau de câbles numériques en Méditerranée.

Dans la ZEE française, le contrôle du passage des câbles sous-marins dans le secteur méditerranéen est un enjeu stratégique. En effet, dès les années 1850, la Méditerranée est un des berceaux historiques de la pose de câbles sous-marins reliant les îles et les archipels au continent ainsi que les pays riverains, l'Afrique du Nord, l'Afrique Noire et le Moyen-Orient vers le Sud-est Asiatique.



La mer Méditerranée a vu, grâce au Canal de Suez, le renforcement de son positionnement parmi les principales voies mondiales de navigation commerciale.

Jouant un rôle de carrefour, les flux de cargos, de porte-containers et de pétroliers alimentent non seulement ses ports mais aussi ceux de l'océan Atlantique, de la Manche et de la Mer du Nord.

Ce qui est vrai pour les câbles numériques l'est aussi pour les gazoducs, les réseaux énergétiques au fur et à mesure du développement de champs éoliens en mer. De même, les enjeux de l'accès aux fonds marins en Méditerranée couvrent un large spectre de sujets, et ont conduit à la nécessité de définir une véritable stratégie nationale avec l'octroi de moyens consacrés à sa mise en œuvre. Cette stratégie nationale, qui inclut l'exploration des ressources minérales dans les grands fonds marins, a fait l'objet d'une première approche avec la circulaire du Premier ministre en date du 5 mai 2021. D'importants enjeux environnementaux existent, particulièrement dans les aires marines protégées.

Les câbles sous-marins sont exposés à diverses menaces, allant des sabotages aux cyberattaques, sans oublier les accidents dûs à des ancres raclant les fonds marins et heurtant un câble, volontaires ou non, ou bien un séisme ou une éruption volcanique. Le contrôle permet non seulement d'assurer la sécurité des infrastructures, mais aussi le renforcement de la résilience numérique de la France et de l'Europe. Les ruptures éventuelles peuvent entraîner des dysfonctionnements d'Internet et potentiellement des conséquences économiques graves dans les espaces les moins bien reliés.

Le N/C René Descartes (Photo Ross Hendry)

Parmi les navires les plus rapides au monde en termes de délais d'intervention, il a été construit pour Orange marine, entreprise française dont sa flotte câblière (15% de la flotte mondiale) est l'une des plus expérimentées au monde : plus de 30 000 km de câbles sous-marins posés, dont 8 200 ensouillés.

Le N/C René Descartes, conçu en 2002, dispose des technologies de toute dernière génération, répondant aux plus hautes exigences du marché en termes de qualité et fiabilité des prestations offertes.

Il possède une importante autonomie de navigation (deux mois) ainsi qu'une grande capacité de stockage permettant de transporter en une seule fois jusqu'à 6 000 kilomètres de câble, soit l'équivalent d'un système sous-marin transatlantique.

https://www.cluster-maritime.fr/wp-content/uploads/2024/06/08-l-economie-bleue-en-france-2022-cables-sous-marins_compressed.pdf

Le Système d'identification automatique (SIA) ou *Automatic Identification System* (AIS)

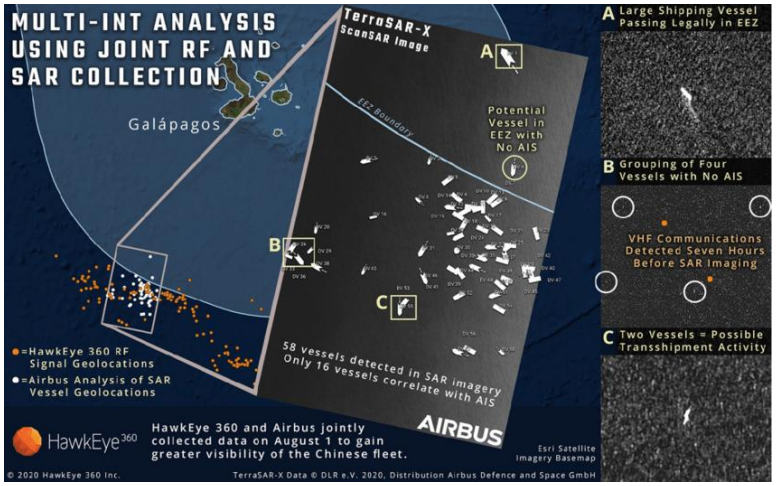
De nos jours, le développement des systèmes de navigation et de positionnement a considérablement amélioré la fiabilité et la rapidité de la navigation maritime. Les vulnérabilités de ces systèmes aux cybermenaces représentent un problème majeur pour la sécurité de la navigation : diffusions ouvertes, absence ou existence limitée du cryptage et de l'authentification des données.

Les questions de cybersécurité concernent le système mondial de navigation par satellite (GNSS), le système électronique de visualisation des cartes marines (ECDIS) et le système d'identification automatique (AIS). Une interférence sur le GPS augmente la vulnérabilité de l'ECDIS et de l'AIS.

Pour mémoire, l'*Automatic Identification System* (AIS) est un système d'échanges automatisés de messages entre navires par radio VHF qui permet aux navires et aux systèmes de surveillance de trafic (CROSS France) de connaître l'identité, le statut, la position et la route des navires se situant dans la zone de navigation. Il joue un rôle important dans la surveillance et la sécurité en incluant les procédures d'anticollision si le dispositif n'est pas désactivé. Souvent couplé à un radar côtier, il permet d'obtenir de l'information sur les navires et leurs cargaisons : c'est un outil VTS (*Vessel Traffic System*) indispensable pour la gestion du trafic maritime en temps réel. Leur objectif est d'améliorer la sécurité maritime, la fluidité du trafic et de protéger l'environnement marin.

Des menaces existent comme l'usurpation d'identité pouvant nuire à la prise de décision concernant une collision ou un trafic intense. Cela peut déclencher de fausses alertes afin d'inciter les victimes à naviguer vers des zones maritimes hostiles et contrôlées par les attaquants.

Un exemple d'usurpation (*spoofing*) a été observé en juillet 2020 lorsqu'une des plus grandes flottes de pêche du monde a été accusée d'avoir mal indiqué sa position pour dissimuler des activités de pêche illégales dans la ZEE autour des îles Galápagos (Equateur).



Disparition de navires du suivi AIS, îles Galápagos

Les navires ont signalé via l'AIS une position en Nouvelle-Zélande qui se trouvait à environ 10 000 km de leur position observée.

En fait, ils ont pu pénétrer profondément dans la ZEE des Galápagos où la pêche illégale était pratiquée.

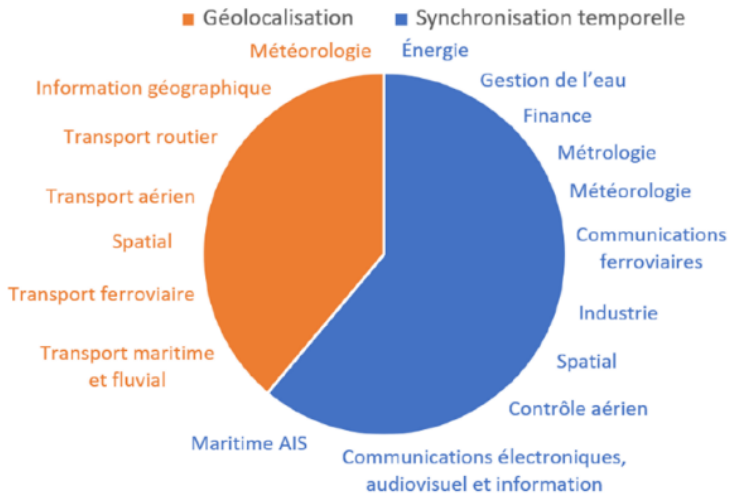
Cette disparition est une des nombreuses méthodes des criminels utilisant l'usurpation de la localisation d'un système dépendant du GNSS pour soutenir leurs activités malveillantes.

Andrej Androjna, Marko Perkovic, Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. Transactions on Maritime Science, vol.2, p.361-373, 2021

7.4.9 Le secteur de la navigation par satellite

Quelques rappels

Les systèmes mondiaux de navigation par satellite - *Global Navigation Satellite System* (GNSS) - comprennent des constellations de satellites en orbite autour de la Terre qui diffusent leur position dans l'espace et dans le temps, des réseaux de stations de contrôle au sol et des récepteurs qui calculent les positions au sol par trilatération. Les GNSS proposent une solution de navigation complète (position, vitesse et temps ou PVT). La précision de position est de l'ordre de 1 à 10 m selon les situations et les versions publiques. Ces données fournies sont indispensables aux besoins de synchronisation et de référence de temps, dans de nombreuses applications : les télécommunications, les transports, la sécurité, les services de secours, la santé, l'application de la loi, les interventions d'urgence, l'agriculture de précision, l'exploitation minière, la finance, la recherche scientifique, etc.



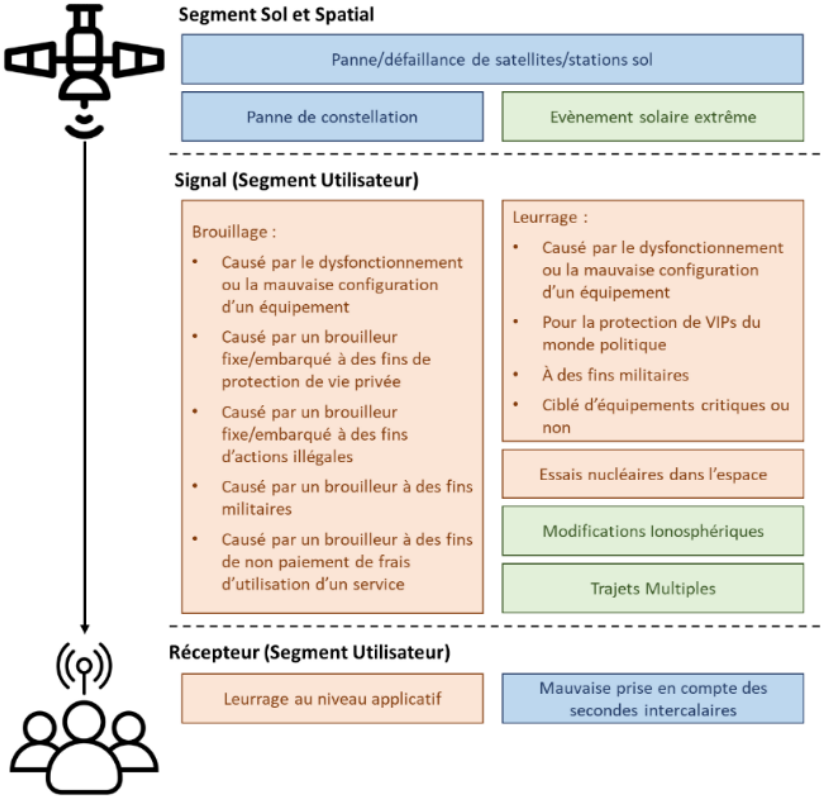
Exemple du secteur aérien :

- *La gestion du trafic aérien et sa surveillance, y compris pour les mouvements au sol ;*
- *Le suivi en temps réel des opérations ;*
- *L'intégration des données GNSS dans les systèmes de bord ;*
- *Les moyens et méthodes de suivi de la navigation et des approches ;*
- *Les systèmes de surveillance et de prévention des collisions, principalement avec le sol.*

©ANFR

À l'heure actuelle, les systèmes GNSS comprennent :

- Deux systèmes mondiaux pleinement opérationnels :
  - Le système de positionnement mondial - *Global Positioning System* (GPS) - des États-Unis, lancé en 1978 en tant que système de navigation militaire indépendant, puis ouvert au public en 1983. C'est le plus utilisé dans le monde et aussi le plus précis aujourd'hui (?). Le GPS fonctionne dans une partie du spectre radio entre 1 et 2 GHz, appelée bande L, choisie pour des raisons physiques liées à l'ionosphère, à la minimisation de l'impact des conditions météorologiques, etc. *Rappelons qu'il faut faire la différence entre le système GPS et les GPS qui sont des assistants de navigation* ;
  - Le système mondial de navigation par satellite, *Globalnaya Navigatsionnay Sputnikovaya Sistema* (GLONASS) de la Fédération de Russie, développé par les forces de défense aérospatiales débuta en 1976, fut opérationnel en 1996 et restauré en service complet au début des années 2010. Il fournit des données de positionnement et de vitesse en temps réel pour les objets de surface, marins et aéroportés avec une précision comparable aux autres systèmes.
- Des systèmes mondiaux et régionaux en cours de développement :
  - Le système européen de navigation par satellite (GALILEO), conçu pour être compatible avec le GPS et le GLONASS, a commencé à fournir des services en décembre 2016 ; Galileo est composé de 24 satellites en orbite autour de la Terre à une altitude de 23 000 km. Les signaux de Galileo sont transmis gratuitement à toute personne disposant d'un appareil capable de les recevoir (par exemple, un smartphone). Galileo est trois fois plus précis que le GPS, avec une précision d'un mètre et une large gamme de services. Il propose aussi une fonction d'authentification du message de navigation (OS-NMA) et un signal de navigation crypté mis en œuvre dans un service d'authentification commercial (CAS) : premières protections contre le leurrage pour tous les utilisateurs civils du GNSS ;
  - Le système chinois (COMPASS/Bei-Dou) a été initié en 2000, avec la constellation Beidou-1.
    La troisième génération, lancée en 2015, avait pour objectif une couverture mondiale. Le déploiement s'est achevé en 2020 et a permis de doter le système de capacités de transpondeur de recherche et de sauvetage ;
  - Le système indien régional de navigation par satellite *Indian Regional Navigation Satellite System* (IRNSS) fournira deux types de services (le positionnement standard et un service restreint). Il devrait proposer une précision de position de l'ordre de 20 m dans la zone de service primaire. Le nom opérationnel est *Navigation with Indian Constellation* (NavIC) qui est prévu pour offrir des services précis de positionnement et de chronométrage en temps réel ;
  - Le système satellitaire quasi-zénithal (QZSS) du Japon, lancé en 2018 et basé sur des horloges au rubidium, comporte un prototype de base d'un système expérimental de synchronisation d'horloges à cristaux, donc sans horloge atomique comme cela est déjà le cas dans le cas de systèmes GPS, GLONASS et Galileo ;
  - Le système coréen *Korean Satellite System* (KPS) est un système de positionnement par satellite régional complémentaire du système GPS en cours de développement par l'agence spatiale coréenne KARI. Son développement qui a débuté en 2022 devrait s'achever en 2035 ;
  - Le système turc régional de positionnement et de synchronisation, *Bölgesel Konumlama ve Zamanlama Sistemi* (BKZS), est un projet spatial des forces armées sur le positionnement global et le transfert de temps par système de navigation par satellite, indépendant des autres systèmes existants.



Menaces sur le GNSS

Les systèmes GNSS actuels sont composés de trois segments :

- le segment spatial désignant les constellations de satellites ;
- le segment sol se composant de stations réparties à travers le monde pour suivre les satellites et leur transférer régulièrement des informations, en particulier sur leurs positionnements ;
- le segment utilisateur désignant les récepteurs utilisant les signaux envoyés par les satellites afin de calculer les données de position, vitesse et de temps (PVT).

Légende : Causes des menaces identifiées
: Altération naturelle
: Défaillance système
: Attaque (intentionnelle ou non)

© FDC

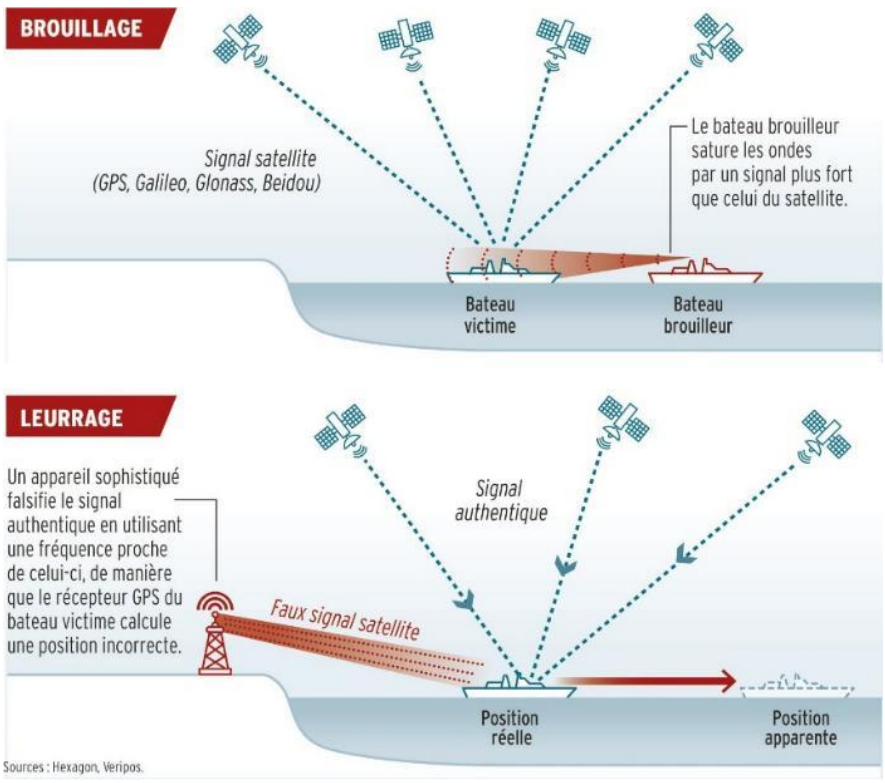
La dépendance toujours plus grande aux signaux GNSS présente un risque pour l'ensemble des acteurs : l'Organisation de l'Aviation Civile Internationale (OACI), l'*European Union Aviation Safety Agency* (EASA) et d'autres autorités nationales s'organisent pour en réduire les effets.

Sachant que les signaux GNSS sont de faible puissance et sans protection cryptographique, ils sont donc vulnérables aux interférences intentionnelles ou non (par exemple, le couvert végétal dense d'une forêt, un très fort orage, signaux malveillants leurrant les récepteurs civils, etc.). Avec la généralisation des systèmes autonomes et leur intégration croissante dans les systèmes opérationnels civils et militaires, les attaques contre les signaux de navigation par satellite se sont largement multipliées particulièrement dans les secteurs maritimes, terrestres, aériens et spatiaux, de transport, etc. en induisant des doutes préjudiciables à une bonne prise de décision. D'autre part, selon la phase de vol, les conséquences de tels évènements peuvent s'avérer critiques lors d'un départ, d'une approche ou d'une remise de gaz, etc.

Une dégradation ou une indisponibilité de la synchronisation et du positionnement est susceptible d'affecter grandement le fonctionnement des dispositifs visés d'autant plus que les systèmes GNSS ne sont pas utilisés de la même manière par les acteurs : certains ont mis en œuvre des contre-mesures spécifiques pour contrôler l'impact des menaces sur le GNSS et alerter les entités compétentes (ANFR, etc.) alors que d'autres n'ont pas mis en œuvre des solutions optimales.

Voici quelques sources potentielles d'interférence :

- Les conditions atmosphériques telles les perturbations ionosphériques et l'activité solaire ;
- Des dispositifs de protection de la vie privée, achetés illégalement, permettant de ne pas être repérés ;
- Le brouillage intentionnel d'équipements de groupes criminels (pour voler des biens, détourner des navires ou des avions, etc.) ;
- Des dispositifs plus puissants utilisés pour protéger des sites sensibles et des lieux de visite ou de résidence d'autorités ou de personnes influentes ;
- Des dispositifs militaires utilisés lors de conflits ou de manœuvres de grande ampleur ;
- Des installations présentant un dysfonctionnement ou non conformes, provoquant des brouillages involontaires - relais de télévision ou de radio, répéteurs GPS utilisés dans des centres de maintenance ;
- Des équipements radioélectriques, électriques et électroniques en défaut ou non conforme, émettant des parasites électromagnétiques en excès (problème de compatibilité électromagnétique) ;
- Etc.



Le brouillage d'un signal génère des interférences perturbant la réception des signaux satellitaires, les rendant ainsi inexploitables par les systèmes embarqués des utilisateurs (dégradation de précision, perte du positionnement, etc.).

Le leurrage consiste à diffuser des signaux satellitaires contrefaits pouvant tromper les récepteurs GNSS, les amenant à calculer des données de position, de navigation et de temps incorrectes.

C'est une technique de piratage où des informations d'identification sont donc falsifiées pour usurper une identité. En aviation, cette pratique dangereuse peut détourner les GPS d'avions, posant un risque sévère pour la sûreté aérienne, surtout dans les zones de tension géopolitique ou de conflit (Scandinavie, mer Baltique, Europe centrale, mer Noire, Proche et Moyen-Orient, Afrique, etc.).

Contrairement à l'attaque par brouillage, dans celle par leurrage, la plupart du temps les récepteurs GNSS ne savent pas s'ils sont usurpés : le récepteur continue à traiter les signaux reçus et fournit donc des valeurs de position, de vitesse et de temps erronées.

Des comptes rendus des évènements notifiés à l'autorité française de l'aviation civile, sont issus de la base de données *European Co-ordination Center for Accident and Incident Reporting Systems* (ECCAIRS), plateforme numérique intégrant les autorités - l'Agence de l'Union européenne pour la sécurité aérienne (AESA) - *National Aviation Authority* (NAA) - et les autorités responsables des enquêtes de sécurité (SIA). Leurs analyses montrent que la menace d'interférences est réelle.

Les fédérations aéronautiques et la direction de la sécurité de l'aviation civile (DSAC), au sein de l'Instance de Sécurité de l'Aviation légère (ISAL), travaillent à concevoir des campagnes de promotion de la sécurité. Chaque année, la Mission Évaluation et Amélioration de la Sécurité (DSAC/MEAS) fait le bilan de l'accidentologie.

L'Agence nationale des fréquences (ANFR) prépare, coordonne et défend les positions françaises dans les enceintes internationales traitant de politique et d'harmonisation des fréquences, sur l'ensemble du spectre. L'ANFR est responsable de l'élaboration et de la mise à jour du tableau national de répartition des bandes de fréquences (TNRBF). C'est un texte réglementaire de référence auxquels les administrations de l'État et autorités administratives indépendantes, les affectataires, ont accès en vue de l'accomplissement de leurs missions.

Quelques exemples de brouillage traités par l'ANFR :

Brouillage en zone portuaire

Le 3 mars 2023, l'opérateur mobile Orange Caraïbe signale un brouillage important (téléphonie et internet mobile), dans la bande 1 920-1 930 MHz, autour du terminal de croisière de la pointe Simon, à Fort de France, en Martinique. Les appels d'urgence risquent de ne pas fonctionner …

La cause est le réseau interne sans fil, de type DECT, servant aux membres de l'équipage. La bande de fréquences utilisée est valide en Amérique du Nord. La Martinique, département français, utilise un plan de fréquences européen, Le réseau du navire doit utiliser la bande européenne 1 880 - 1 900 MHz.

Avions et hélicoptères du SAMU perturbés

Le 22 mars 2023, la Direction générale de l'aviation civile (DGAC) saisit l'ANFR pour un brouillage de la fréquence 1 575 MHz du GPS : les hélicoptères du SAMU et les avions étaient perturbés à une trentaine de kilomètres de Lille, à proximité de l'aérodrome de Merville (59). Depuis quelques jours, des pertes de positionnement étaient constatées.

Plusieurs brouilleurs de signaux GPS sont découverts dans un véhicule et dans une habitation. La gendarmerie aide l'ANFR dans les investigations afin de résoudre ces problèmes créés par des dispositifs interdits.

Saturation par des émetteurs en bandes voisines

En juillet 2024, à quelques heures du début du défilé des JOP 2024, les drones ne décollaient pas : un brouillage était suspecté.

Après enquête, des caméras sans fil pour filmer et rediffuser la cérémonie d'ouverture étaient installées sur des barges, sur la Seine, sur lesquelles étaient aussi disposés les drones. Les fréquences utilisées par ces caméras étaient le 1530, le 1540 et le 1550 MHz, mais avec une remontée forte de bruit dans les bandes adjacentes. Cela aveuglait les récepteurs GPS des drones. La pose de filtres a permis le fonctionnement de l'ensemble.

7.5 Conclusion de la Partie 1

« *Les cybermenaces sont le nouveau baromètre des tensions géopolitiques mondiales. Les rapports de nos experts offrent une perspective solide et nouvelle sur les perturbations internationales et leurs impacts opérationnels sur la société* », déclare Hugues Foulon, CEO d'Orange Cyberdefense dans l'étude Security Navigator 2025.

Les opérations des groupes APT continueront de refléter le contexte conflictuel mondial. Les campagnes de cyberespionnage s'étendront dans des conflits régionaux cherchant à profiter de l'avantage asymétrique procuré par les nouvelles technologies. Avec l'IA qui devient un outil central dans les stratégies des cybercriminels, une explosion des attaques automatisées, plus ciblées et plus difficiles à détecter, sera constatée. La capacité de contrôler les données sur soi-même (individu, entreprise ou État) devient de plus en plus souhaitable et de plus en plus difficile sur le plan technique.

"*Les cyberadversaires à la solde d'État utiliseront des opérations cyber pour appuyer d'autres objectifs nationaux, tels que la diffusion de propagande ou la génération de revenus*", ajoute Joshua Miller, Staff Threat Researcher, dans les prévisions 2025 de Proofpoint.

La tendance dans les années à venir devrait être l'accroissement du pouvoir politique des acteurs non étatiques dont les actions pourraient dépasser la capacité de régulation des États-nations à contrôler et à réglementer de telles interactions. La riposte serait alors des stratégies diplomatiques et réglementaires pour relever les défis posés par ce type d'influence.

La Partie 2 traitera du rôle respectif des divers organisations et agences d'état spécialisées, françaises et européennes, dans leurs actions de cyberdéfense. Des exemples avec l'apport de l'IA, entre autres technologies, dans les secteurs civils et militaires seront présentés et discutés. La recherche de talents et de profils compétents est devenue plus que nécessaire. La sensibilisation, la formation et les simulations de crise dans les entreprises et les services publics sont vitales…

Jean-Pierre DAMIANO
Ancien ingénieur de recherches (Univ. Côte d'Azur CNRS)
Docteur ès sciences, docteur en électronique
Conseiller IESF-Côte d'Azur et membre URSI-France

https://cv.archives-ouvertes.fr/jean-pierre-damiano
https://www.researchgate.net/profile/Jean-Pierre_Damiano
Contact : jean-pierre.damiano@univ-cotedazur.fr

7.6 Références et sources

- La cyberdéfense : un enjeu mondial, une priorité nationale, Sénat, Rapport d'information n° 681 (2011-2012), déposé le 18 juillet 2012 ;
- Stéphane Taillat, Amaël Cattaruzza, Didier Danet (Dirs), La Cyberdéfense - Politique de l'espace numérique, Armand Colin, Coll. U, 4 juillet 2018 ;
- Yann Salamon, Cybersécurité et cyberdéfense : enjeux stratégiques, Éditions Ellipses, 6 octobre 2020 ;
- Guide cybersécurité des systèmes industriels, Clusif, Février 2021 ;
- J.-P. Damiano, Les technologies quantiques. Contexte et enjeux, applications et perspectives, IESF Côte d'Azur, Bull. n°2, p.8-29 - Aperçu des apports des technologies quantiques à la sécurité et à la défense, Bull. n°4, p.5-25, 2021 ;
- Bertrand Warusfel. La cyberdéfense, dimension numérique de la sécurité nationale. Sébastien-Yves Laurent. Conflits, crimes et régulations dans le cyberespace, ISTE, 2021 ;
- Andrej Androjna, Marko Perkovic, Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. Transactions on Maritime Science, vol.2, p.361-373, 2021 ;
- Réseaux d'influence de la Chine, Institut de recherche stratégique de l'École militaire (Irsem), septembre 2021 ;
- Lutter contre les brouillages des systèmes de navigation par satellite (GNSS), ANFR, rapport final, Catherine Gabay, 15 octobre 2021 ;
- Ports cybersécurisés. Guide de bonnes pratiques pour la cybersécurité dans le secteur portuaire, Direction générale des infrastructures, des transports et des mobilités (DGITM), Janvier 2022 ;
- Étude d'impact de perte de signaux GNSS, Presentation of the Final Report L04 - Final Version, Formation, Innovation, Recherche, Services et Transfert en Temps-Fréquence (FIRST-TF), Réseau d'excellence du Programme Investissements d'Avenir, 15 février 2022 ;
- Nicolas Arpagian, La Cybersécurité, Paris, PUF, coll. « Que sais-je ? », Mai 2022 ;
- Lianxiao Meng, Lin Yang, Wu Yang, Long Zhang, A Survey of GNSS Spoofing and Anti-Spoofing Technology, Remote Sensing, vol.14, n°19, 4826, 2022 ;
- J.-P. Damiano, La cybersécurité : contexte, enjeux, constats et perspectives, IESF CA, Bull. n°1, p.5-24, 2023 ;
- J.-P. Damiano, Intelligence artificielle et souveraineté numérique. Enjeux et défis du XXIème siècle pour la protection du citoyen. Compte-rendu (avec de nombreux compléments explicatifs) de la conférence du général Patrick Perrot (coordonnateur Intelligence Artificielle et Administrateur des données, codes sources et algorithmes pour la Gendarmerie Nationale) et de la table ronde *Souveraineté numérique et protection des citoyens* réunissant Marina Teller (professeure de droit privé UniCA, CNRS-GREDEG), le général Patrick Perrot et l'ancien député Jean-Michel Mis (Via Publica). Evènement #IADATES organisé avec le concours de la Maison de l'Intelligence Artificielle, le Département des Alpes-Maritimes et Smart Deal 06, avec l'Institut EuropIA. 26 avril 2023, Nice ;
- Camille Morel, Les câbles sous-marins : enjeux et perspectives au XXIe siècle, CNRS Editions, Biblis, mars 2023 ;
- Pour une coordination de la cyberdéfense plus offensive dans la loi de programmation militaire 2024-2030. Sénat, Rapport d'information n°638 (2022-2023), déposé le 24 mai 2023 ;
- J.-P. Damiano, ChatGPT-4 - Comprendre, démystifier, s'approprier. Compte-rendu (avec de nombreux compléments explicatifs) du colloque-débat à l'initiative de l'Espace Ethique Azuréen (EEA) du Centre Hospitalier Universitaire de Nice (CHU) & Département Ethique et Sciences Humaines de la Faculté de Médecine (DESH) - Prof. Gilles Bernardin, avec Geraldine Geoffroy (Responsable d'ingénierie documentaire, SCD UniCA), Isabelle Galy (Dir. Maison de l'Intelligence Artificielle) pour le cadre législatif et la régulation et Anthony Fornes (Philosophe) sur le thème de la prudence - 2 juin 2023, Faculté de Médecine de Nice ;
- Francis Bruckmann, Ecosystème de la cybersécurité, Association des Réservistes du Chiffre et de la Sécurité de l'Information - mise à jour du 29 juin 2023 ;
- Cyber guide des places industrialo-portuaires de l'axe Seine, Haropa Port, Juillet 2023 ;
- Les défis de la cyberdéfense, rapport rédigé par la Commission de la Défense nationale et des Forces armées en conclusion des travaux d'une mission flash, constituée le 15 mars 2023, présenté par Mme Anne Le Henanff et M. Frédéric Mathieu, Députés. Rapport d'information n°2068 dé,posé le 17 janvier 2024 ;
- Cybersécurité des systèmes industriels – Partie 1, Revue 3EI, n°111, janvier 2024 - Partie 2 Revue 3EI, n°112, février 2024 ;
- Tara Mina, Ashwin Kanhere, Akshay Shetty, Grace Gao, GPS Spoofing-Resilient Filtering Using Self-Contained Sensors and Chimera Signal Enhancement, Navigation, J. of the Institute of Navigation June vol.71, n°2, 2024 ;
- Guy-Philippe Goldstein, Quel état de la menace cyber en France en 2024 ? Usine Nouvelle, 29 mars 2024 ;
- D'où proviennent les menaces cyber ? SciencesPo, Paris, 18 avril 2024 ;
- L'UE face au défi de l'intelligence artificielle - Pas de progrès possibles sans une gouvernance renforcée et sans investissements plus importants et mieux ciblés, Rapport spécial - Cour des Comptes européenne, 29 mai 2024 ;
- Biaggi Catherine et Carroué Laurent, « Les grands détroits et canaux internationaux dans la géopolitique des mers et océans, un système très hiérarchisé sous tensions multiformes », Géoconfluences, 10 juin 2024 ;
- J.-P. Damiano, Villes et territoires intelligent(e)s, durables et résilient(e)s : éléments historiques, enjeux et défis, stratégies, modèles, gouvernances, réalités et futurs, IESF Côte d'Azur, Bull. n°2, 2024 ;
- Grandes Constellations de Satellites : Enjeux et Impacts, Rapport de l'Académie des sciences - 30 mars 2024 ;
- Katarina Radoš, Marta Brkić, Dinko Begušić, Recent Advances on Jamming and Spoofing Detection in GNSS, Sensors, vol.24, n°13, 4210, 28 juin 2024 ;

- Rapport annuel sur la cybercriminalité, ministère de l'Intérieur, Juillet 2024 ;
- Alerte sur le brouillage GPS des avions civils, L'Usine Nouvelle, Juillet-Août 2024 ;
- Global Research and Analysis Team (GReAT), Kaspersky, Août 2024 ;
- Bruce M, Lusthaus J, Kashyap R, Phair N, Varese F Miranda Bruce, Jonathan Lusthaus, Ridhi Kashyap, Nigel Phair, Federico Varese, Mapping the global geography of cybercrime with the World Cybercrime Index. PLoS ONE, vol.19, n°4, 2024 ;
- Organismes de recherche et Think tanks. Etat de la menace informatique, ANSSI, CERT-FR, Licence ouverte (Etalab - v2.0), 10 septembre 2024 ;
- ENISA Threat Landscape 2024, ENISA, Novembre 2024 ;
- Les nouveaux développements de l'intelligence artificielle, Rapport au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST), M. Alexandre Sabatou, député, M. Patrick Chaize, sénateur, et Mme Corinne Narassiguin, sénatrice, Rapport n°642 déposé le 29 novembre 2024 ;
- Rapport sur les cybermenaces, ESET Research, Décembre 2024 ;
- Comprendre le Spoofing : Une Menace Invisible pour la Sécurité Aérienne, FlyWest, Marc Leonelli, 27 déc. 2024 ;
- Cyberespace, cyberdéfense : enjeux et conflits, Sélection d'émissions, Radio France, 2025 ;
- Baromètre de la cybersécurité des entreprises, vague 10, CESIN, janvier 2025 ;
- Song Li, Xiaomei Tang, Honglei Lin, Feixue Wang, GNSS spoofing detection based on frequency domain processing, Measurement, vol.242, Part B, article 115872, January 2025 ;
- Bernard Claverie, La guerre cognitive : le nouveau champ de bataille qui exploite nos cerveaux, Polytechnique Insights, La Revue de l'institut Polytechnique de Paris, Février 2025.

Agences, directions, organismes, entreprises, etc.

- Agence ministérielle pour l'intelligence artificielle de défense (AMIAD)
- Agence nationale de la sécurité des systèmes d'information (ANSSI)
- Agence nationale des fréquences (ANFR)
- Alcatel Submarine Networks (ASN)
- Autorité de régulation des communications électroniques et des Postes (ARCEP)
- Base industrielle et technologique de défense (BITD)
- Carte des câbles sous-marins Submarine Cable Map
- Centre cyber de préparation opérationnelle (C2PO)
- Centre de coordination des crises cyber (C4)
- Centre d'analyse en lutte informatique défensive (CALID)
- Cercle européen de la sécurité et des systèmes d'informations (CESSI)
- 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)
- Commandement de la cyberdéfense (COMCYBER)
- Commission Européenne
- Commission nationale de l'informatique et des libertés (CNIL)
- Computer Emergency Response Team (CERT-FR)
- Cooperative Cyber Defence Centre of Excellence (CCDCOE)
- CybelAngel
- Cyber-Defence Campus: Strengthening Switzerland's Cyber Defence
- CyberEdu
- Cybermalveillance.gouv.fr
- Délégation générale des entreprises (DGE)
- Délégation à l'information et à la communication de la défense (DICOD)
- Direction générale de l'armement (DGA)
- Direction générale de l'armement - maîtrise de l'information (DGA-MI)
- Direction générale du numérique (DGNUM)
- Direction générale de la sécurité extérieure (DGSE)
- Direction générale de la sécurité intérieure (DGSI)
- Direction interministérielle du numérique (DINUM)
- Direction de la protection des installations, moyens et activités de la Défense (DPID)
- Direction du renseignement militaire (DRM)
- Direction du renseignement et de la sécurité de la Défense (DRSD)
- Diplomatie.gouv.fr
- Eurocontrol
- European Union Agency for Cybersecurity - Agence européenne pour la cybersécurité (ENISA)
- European Union Aviation Safety Agency (EASA)
- Entreprises défense & relations internationales (ENDERI)
- Europa (statistiques européennes)
- Federal Aviation Administration - All Safety Alerts for Operators (SAFOs)
- Fédération Française de la Cybersécurité (FFCyber)

- Fortinet Cybersécurité
- Forum international de la cybersécurité (FIC)
- Label France Cybersecurity
- Gendarmerie nationale
- Groupement français de l'industrie et de l'information (GIFI)
- Guardia School
- Helsing.ia, IA Défense (Suède, Allemagne, France)
- Hexatrust Cloud confidence & Cybersecurity
- International Maritime Organization (IMO) – ONU
- The JRC Publications Repository, Commission européenne
- Média de la communauté cyber (inCyber)
- Institut des hautes études de la défense nationale (IHEDN)
- Institut européen des sciences avancées de la sécurité (IESAS)
- Institut français des relations internationales (Ifri)
- Institut national de recherche en sciences et technologies du numérique (INRIA)
- International Air Transport Association (IATA)
- International Telecommunication Union (ITU)
- Ministère des Armées
- Naval Group
- Nouvelle France industrielle
- 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)
- Orange Cyberdefense
- Organisation de l'Aviation Civile Internationale (OACI)
- Potentiel scientifique et technique de la Nation (PSTN)
- Proofpoint
- PwC CEO Survey
- PwC France et Maghreb
- Règlement général de protection des données (RGPD)
- Safran
- Secrétariat général de la Défense et de la sécurité nationale (SGDSN)
- Service de l'information stratégique et de la sécurité économiques (SISSE)
- Service hydrographique de la Marine (SHOM)
- Statista, plateforme mondiale de données et d'intelligence économique
- Submarine Cable Map
- Telegeography
- Thales Group

Médias, Presse, etc.

- L'avionnaire
- Cybercercle.com
- Diploweb.com
- Epsiloon
- Global Security Mag
- Industries & Technologies
- Journal du Net
- La Recherche
- Lebigdata.fr
- Le Mag IT
- Les Echos
- Le Monde Informatique
- Micronora Informations
- The MITRE Corporation
- Numerama
- Pixees
- SiecleDigital
- Techniques de l'ingénieur
- Toute l'Europe
- TrustMyScience
- Usine Digitale
- Usine Nouvelle
- Vie publique
- Wikipédia
- Zataz.com
- ZDNet
- *etc.*

8. Une évaluation de l'attractivité de l'enseignement supérieur français pour les étudiants internationaux

Cour des comptes - 10.03.2025

Le nombre d'étudiants en mobilité diplômante dans le monde est passé de 600 000 en 1975 à 3,5 millions en 2005 et à 6,4 millions en 2021, après l'arrêt notable de l'année 2020-2021 marquée par la crise sanitaire. Les étudiants en déplacement international représentent aujourd'hui 2,7 % des 256 millions estimés dans le monde, contre 2 % seulement en 2008. L'accueil de ces derniers fait l'objet d'une compétition de plus en plus intense entre les établissements d'enseignement supérieur pour attirer les talents, mais aussi entre les États qui associent leurs stratégies d'attractivité à des objectifs plus ou moins précis. Sur la base des données de l'Unesco qui recense le nombre des étudiants internationaux en mobilité dite diplômante, la France était le deuxième pays d'accueil en 1980 derrière les États-Unis et le quatrième en 2017. Elle est en 2022 septième derrière le Canada, l'Allemagne et la Russie. L'évaluation de la politique publique d'attractivité de l'enseignement supérieur prolonge plusieurs travaux récents de la Cour des comptes sur les droits d'inscription dans l'enseignement supérieur, les programmes d'études internationaux ainsi que sur l'entrée et le séjour des personnes étrangères en France.

Pour lire la suite de l'article : https://www.ccomptes.fr/fr/publications/une-evaluation-de-lattractivite-de-lenseignement-superieur-francais-pour-les-etudiants

9. Les billets de la Société des Sciences de Cherbourg :
La France au premier rang mondial

Ces billets sont extraits des mémoires LXII et LXIII de la Société Nationale des Sciences Naturelles et Mathématiques de Cherbourg.

9.1 René Laennec, inventeur du stéthoscope, créateur du diagnostic médical par auscultation

Alors qu'il est âgé de 6 ans, René Laennec (1781-1826) perd sa mère qui meurt de tuberculose ; son père le confie alors à son frère Guillaume, médecin-chef de l'Hôtel Dieu de Nantes qui se charge de son initiation médicale qui va décider de sa vocation. En 1801, il étudie à l'Hôpital de la Charité à Paris. Quelques mois plus tard, il écrit dans le « Journal de la Médecine », un premier article sur les inflammations du péritoine et, presque chaque mois, il fera paraître, sous sa signature, des mémoires concernant surtout les affections thoraciques qui le font connaître. L'année suivante, à 21 ans, il reçoit les deux grands prix de médecine et de chirurgie.

Pendant dix ans (1804-1814), Laennec enseigne principalement l'anatomo-pathologie (spécialité médicale qui consiste à examiner les organes pour repérer et analyser des anomalies liées à une maladie). Il se consacre aussi à sa clientèle qu'il reçoit chez lui. Il a pour patients, entre autres, Chateaubriand et son épouse, plusieurs cardinaux, Mme de Staël mais il se consacre également aux plus pauvres au dispensaire de la Société philanthropique de la rue Lacépede.

Laennec est nommé médecin-chef à l'hôpital Necker en juin 1816 et c'est cette année-là qu'il va révolutionner l'auscultation qui consistait, jusque-là, à appliquer la main et utiliser la percussion pour confirmer le diagnostic.

Alors qu'il est consulté par une jeune fille qui présente des symptômes d'une maladie de cœur, il s'aperçoit que l'embonpoint de la patiente empêche cette auscultation classique. Or, peu de temps auparavant, en passant sous les guichets du Louvre, son attention a été attirée par des enfants qui jouent là. L'un d'entre eux gratte l'extrémité d'une longue poutre avec la pointe d'une épingle. À l'autre extrémité, l'oreille collée à la poutre, les autres enfants recueillent les sons et se bousculent en riant pour entendre. Il se demande alors s'il est possible d'utiliser ce phénomène acoustique pour ausculter cette malade. Il prit un cahier de papier qu'il mit en rouleau. Il en appliqua une extrémité sur la poitrine de la patiente et posa son oreille à l'autre bout. Il écrit lui-même plus tard : *« je fus aussi surpris que satisfait d'entendre les battements du cœur d'une manière beaucoup plus nette et plus distincte que je ne l'avais jamais fait par application directe de l'oreille ainsi que le bruit de la respiration ».*

Laennec vient d'inventer un appareil qui amplifie les bruits de l'auscultation et qu'il nomme « stéthoscope » (de deux mots grecs, *stethos*, poitrine, et *skopein,* examiner).

Avec Laennec, les médecins allaient apprendre pour la première fois à se servir de leur oreille. Celui-ci note avec soin tout ce qu'il entend, analyse les bruits et établit une coïncidence entre les symptômes et les constatations faites par autopsies. Il va consigner toutes ses observations dans son « *Traité du diagnostic des maladies des poumons et du cœur fondé principalement sur ce nouveau moyen d'exploration* » paru en août 1818. Cet ouvrage fait encore autorité aujourd'hui. Sa classification des bruits d'auscultation est toujours utilisée par les médecins.

Il est également connu pour sa description de la péritonite et de la cirrhose, maladie à laquelle il a donné son nom (de *kirrhos*, en grec qui signifie « roux » en référence aux nodules jaunes caractéristiques de la maladie). Il a apporté de nombreuses contributions à la connaissance de la tuberculose, maladie qui va l'emporter précocement. C'est son neveu qui, en l'auscultant justement avec le propre stéthoscope de l'inventeur, va déceler sur lui les symptômes de la tuberculose. Retiré en son manoir proche de Douarnenez, il s'éteint le 13 août 1826 à l'âge de 45 ans. Dans son testament, Laennec lègue à son neveu ce stéthoscope qu'il considérait comme « le plus grand héritage de sa vie ».

Cette invention et la nouvelle méthode d'auscultation qui en découle et qu'il a décrite dans son traité de 1818 ont fait sa renommée dans le monde entier.

L'un des plus grands médecins anglais, le Professeur Benjamin Ward Richardson écrivit dans son livre *Les disciples d'Esculape* : « *le véritable étudiant en médecine se doit de lire le traité de Laennec sur l'auscultation et l'utilisation du stéthoscope au moins une fois tous les deux ans tant qu'il pratique son art. Cette œuvre originale situe Laennec parmi les grands pionniers de la médecine aux côtés d'Hippocrate* ».

En 1879, l'hospice des incurables prend le nom d'hôpital Laennec ; c'était la première fois en France qu'un hôpital recevait le nom d'un médecin. ***Jacques FOOS***

9.2 Amédée Bollée « Plus vite, Chauffeur ! »

1873 : « L'Obéissante », ancêtre de l'autocar

1878 : « La Mancelle » première voiture en série

1879 : « La Marie-Anne » ancêtre du semi-remorque

L'Obéissante est le nom que son inventeur, ***Amédée Bollée (1844-1917***) a donné au premier véhicule « automobile » pour particuliers (en opposition avec le fardier du Cugnot, plus ancien mais pour une application militaire) ; premier véhicule à avoir circulé sur plusieurs centaines de kilomètres (1873).

Il a été conçu pour transporter 12 personnes à la fois. On peut donc dire que c'est l'ancêtre de l'autocar. «La Mancelle », véhicule qui suivra cette première invention sera la première voiture fabriquée en série pour particuliers et « La Marie-Anne », locomotive sur route comme l'a définie son inventeur, est l'ancêtre du semi-remorque.

Un seul inventeur donc pour ces 3 véhicules : Amédée Bollée. Né dans une famille de fondeurs de cloches, c'est dans l'entreprise paternelle qu'il fait ses premiers pas d'inventeur en embellissant la qualité des sons grâce à de nouveaux procédés de coulée des métaux. Mais en visitant l'Exposition Universelle de Paris en 1867 naît une nouvelle vocation : la construction de véhicules à vapeur mais qui circuleront sur route et non pas sur rail comme on connaît jusque-là.

Après la fabrication d'armes pendant la guerre franco-prussienne de 1870, Amédée Bollée peut enfin se consacrer, dans l'atelier de mécanique de la fonderie familiale, à l'assemblage de son premier véhicule, l'Obéissante, suivi d'autres modèles qui sont construits sur le même principe. Le châssis repose sur une suspension indépendante chaque roue. Les roues avant sont directrices, avec braquage différentiel pour les virages. La propulsion se fait sur les roues arrière indépendantes par deux moteurs bicylindres en V à vapeur avec la chaudière située elle aussi à l'arrière. Les commandes sont centralisées autour du volant avec un changement de vitesse à engrenages (boîtes dites « à pignons coulissants »). Comme on le voit, tout ou presque était en place par rapport aux voitures modernes.

Le véhicule est prévu pour le transport de 12 personnes dont un pilote à l'avant et un chauffeur à l'arrière qui charge le foyer de la chaudière comme dans les locomotives (*photos : Musée des Arts et Métiers - Paris*) ! En 1873, l'Obéissante sort des ateliers. Pesant 4 800 kg, elle pouvait atteindre 40 km/h en palier et grâce à son changement de vitesse, gravir une côte de 12 %.

Le 26 mars 1873, A. Bollée obtient du Préfet de la Sarthe l'autorisation de circuler dans le département. Ce qui frappe le plus les spectateurs lors de son passage, c'est le silence de fonctionnement et la maniabilité de la voiture. Amédée Bollée veut toutefois la présenter à Paris, après avoir fait le trajet avec sa voiture. Cette fois, il faut l'accord du Ministre des Travaux Publics, qui le donne en Août 1875.

Avec cet accord, A. Bollée obtint également le premier permis de conduire de l'histoire de l'Humanité ! Le 9 octobre 1875, il fit les 230 km en 18 heures après avoir écopé de 75 amendes pour excès de vitesse. A. Bollée aura l'intelligence d'inviter le lendemain le Préfet de Paris pour une démonstration de son « engin » devant un public nombreux et médusé et les contraventions ont toutes été levées !

À partir de 1878, il fabriqua des voitures plus petites et en série (une cinquantaine) : « La Mancelle » suivie de « La Nouvelle » la première conduite intérieure et quelques « trains routiers », ancêtres de nos semi-remorques modernes. Ainsi, « La Marie-Anne » avec son moteur de 100 chevaux, pouvait transporter 100 tonnes sur terrain plat mais était limité à 35 tonnes en côte de 6 %. En 1881, il construit « La Rapide » première voiture capable d'atteindre la vitesse de 62 km/h soit plus d'un kilomètre par minute !

Son fils aîné Amédée va expérimenter les moteurs à combustion interne dont le premier est dû aux frères Niepce (*voir un précédent billet de cette série*). Avec leur développement, il en sera fini des véhicules à vapeur et de leur chauffeur.

Ce dernier, sans le savoir, est à l'origine de l'expression qu'emploient toujours les enfants en autocar : «*plus vite, chauffeur !*» sans toujours en connaître l'origine !

Jacques FOOS

Directeur de la Société des Sciences de Cherbourg

Professeur Honoraire au Conservatoire National des Arts et Métiers (Sciences et Technologies Nucléaires)

10. Jeu mathématique : La multiplication dans l'Égypte antique

L'addition de deux nombres dans le système égyptien est relativement facile puisqu'il suffit de rassembler les différents symboles de chaque nombre pour en obtenir la somme. Ainsi :

© d'après Hervé Lehning

Éventuellement, il peut se produire des retenues mais cela ne pose guère de problème. La question est autrement plus compliquée pour multiplier !

Question : comment les anciens Égyptiens faisaient-ils pour multiplier ?

Réponse : Les anciens Égyptiens ont inventé une méthode ne demandant qu'à multiplier par deux, ce qui se fait comme une addition. Des traces de cette formule se retrouvent en Abyssinie… et en Russie !

Prenons l'exemple de la multiplication : 253 x 13. Et écrivons le plus petit de ces nombres comme une somme de puissances de deux : 8 + 4 + 1. L'opération devient : 253 x (8 + 4 + 1). Si nous calculons les multiples de 253 par 2, 4 et 8, nous sommes amenés à effectuer une simple addition. Il suffit donc de savoir multiplier par deux !

2	5	3	x		1								2	5	3	
2	5	3	x		2	=		5	0	6						
2	5	3	x		4	=		5	0	6	x	2	=	1	0	1	2
2	5	3	x		8	=	1	0	1	2	x	2	=	2	0	2	4
2	5	3	x	1	3								=	3	2	8	9

Multiplication selon la méthode égyptienne. © D'après Hervé Lehning

Nous n'avons pas utilisé l'écriture égyptienne des nombres pour montrer que l'algorithme en lui-même est simple, d'ailleurs cette façon de multiplier est toujours applicable !

Remarque

Ceux qui connaissent la base deux remarqueront que l'écriture de 13 comme une somme de puissance de 2, revient à l'écrire en base deux.

Hervé LEHNING

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

11. 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

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

Solution du Sudoku du dernier bulletin

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

12. Sur votre Agenda

Date	*Sujet / événement*	*Lieu*	*Organisation*
Fin juin Date à confirmer	Visite de la Maison de l'IA	Sophia Antipolis	IESF CA

13. Cotisations 2025

ADHÉSION – COTISATIONS 2025 AUX IESF CÔTE 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 2025 sur HelloAsso
- Payer par carte bancaire votre cotisation sur HelloAsso en scannant ce QR code
- 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 LinkedIn : linkedin.com/company/iesf-côtedazur**
- **Compte Facebook** : facebook.com/iesfca/
- **Email** : contact-coteazur@iesf.fr