Cybersécurité : des arnaques du quotidien aux menaces systémiques

Comment se protéger du point de vue personnel, familial et sociétal

2025 11 29 – Frederic VILANOVA, membre de l'AACLE

1. Cyberespace, nouveau champ d'opérations
2. Le risque numérique est protéiforme
3. Protéger notre quotidien
4. Conclusion et « call to action »

PER Package Enabled Reengineering
MIT Digital Transformation Platform
INSEAD Impactful Leadership for Sustainability
In progress (2025Q2- 2026Q1) :
INSEAD M&A Success Strategies
INSEAD 06 Supply Chain Strategies for Business

EDUCATION

INSEAD Chief Strategy Officer (in progress)
ESCP Master, IS Management
AMU Master, Industrial and Finance internation
Strategy
AMU DECF
POLYTECH Engineer, Information System

VOLUNTEERING

CLUSIF GT Data Protection & AI
IFACI GT Cyber Risk
ISACA Platinum member
CIP Méditerranée Vice President Cyber.
MEDINSOFT Exec. Board member
CAMPUS CYBER SUD Active Member

Cyber Governance, Board advisory, CISO
BIA Bank and various ETI/SMBs 2022-now,
Cybersecurity Risk Management, IT Internal Control (level 2), DORA compliance

CEO www.EffectiveYellow.com 2014-now
Cybersecurity and Privacy consulting services (10 partners). Serenity and lucidity for managers, for a strategic and effective alignment of your systems and your information.

CISO **Constructa Asset Management** 2019
Group Transitional CISO

CIO **Mercure International of Monaco** 2012
Group Transitional CISO in charge of CRM project

IS Advisory Dir. **Monaco Avangarde** 2006-2013
Various missions in Monaco and France, Delivery Direction

Org. & Audit Dir. **CAF83** 2003-2005
In charge of CRM activities (France South East area), 20 consultants

CRM Manager **Cap Gemini** 2001-2003
In charge of CRM activities (France South East area), 20 consultants

Director of Mission **EY** 1997-2001
French South East Area IT Audit Business Unit creation (multi-cultural), IS/IT audit and control, Business Process Reengineering, Package enabled reengineering, Financial Audit Manager

Supervisor **PWC** 1991-1996
IT audit processing and supervision, Financial audit processing and supervision, Data analysis

SITEC **French Navy** 1990-1991
CELENV Paris, Houilles, IT support

Invited Lecturer **Campus Cyber Région Sud**
Euromed 2025-now
Cybersecurity Governance , Secured AI, Crisis Management,

Invited Lecturer **IAE Aix, Bordeaux** 2015-2024
IS Governance, Information Security Compliance

Invited Lecturer **AMU University** 1999-2024
IS Audit and Governance, COBIT framework, ITIL certification

1. Cyberespace, nouveau champ d'opérations

1.1 Cybersécurité, sécurité informatique

1.2 Cyberespace : un terrain sans frontières ?

1.3 Évolution des menaces : individus, groupes, États

1.4 Objectifs : Comprendre, Prévenir, Réagir

1. Le cyberespace, nouveau champ d'opérations

1.1 Cybersécurité, sécurité informatique

La cybersécurité vise avant tout à protéger les logiciels, les matériels, les réseaux et les personnes contre les menaces numériques provenant d'Internet et des réseaux mobiles (4G, 5G, etc.). Ces menaces prennent par exemple la forme de cyberattaques, de courriels frauduleux (phishing), de virus avec demande de rançon (ransomwares) ou encore d'attaques massives qui saturent les systèmes (DDoS). Son objectif est de sécuriser les données, les utilisateurs, les réseaux et l'ensemble des systèmes dans l'espace numérique connecté. La cybersécurité se focalise sur la protection contre les attaques en ligne dans le cyberespace

La sécurité informatique (ou « sécurité de l'information et des systèmes », « sécurité des systèmes d'information ») a un périmètre plus large. Elle couvre non seulement les aspects numériques cités ci-dessus, mais aussi la protection physique des équipements (serveurs, postes de travail, câblage, etc.) ainsi que la sécurité des systèmes industriels informatisés, même lorsqu'ils ne sont pas raccordés à des réseaux externes.

La sécurité informatique et sa composante cybersécurité poursuivent le même but : garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, avec une spécialisation plus marquée de la cybersécurité sur les menaces issues du monde numérique.

1. Le cyberespace, nouveau champ d'opérations

1.2 Cyberespace : un terrain sans frontières ?

Le cyberespace est souvent perçu comme un terrain sans frontières, un espace où les informations circulent librement d'un continent à l'autre, indépendamment des limites géographiques physiques. Cette caractéristique est renforcée par l'interconnexion mondiale des réseaux informatiques, des appareils connectés et des ressources numériques, qui forment un univers dématérialisé et en perpétuel mouvement.

L'expression « village mondial » (ou « village planétaire ») a été popularisée par le philosophe et sociologue canadien Marshall McLuhan dans son ouvrage The Medium is the Message, publié en 1967 (https://web.mit.edu/allanmc/www/mcluhan.mediummessage.pdf), pour décrire l'effet des technologies de communication sur la globalisation des sociétés. Cette notion a été réactivée à la fin des années 1990, au moment de l'expansion d'Internet, pour décrire un monde devenu interconnecté grâce aux réseaux numériques, où les distances géographiques semblent s'effacer.

En 2025, le nombre d'utilisateurs atteint 5,64 milliards, soit 68,7 % de la population mondiale, selon une étude publiée en avril 2025 par We Are Social et Meltwater.
https://www.blogdumoderateur.com/chiffres-cles-internet-reseaux-sociaux-monde-avril-2025/

A noter un vecteur d'information, de loisir, de manipulation et de propagande majeur : les internautes de 16 ans et plus passent en moyenne près de 7 heures par semaine — soit 59 minutes par jour — à jouer aux jeux vidéo.
https://wearesocial.com/fr/blog/2025/04/digital-2025-rapport-davril-sur-les-data-mondiales-du-numerique/

1. Le cyberespace, nouveau champ d'opérations

1.2 Cyberespace : un terrain sans frontières ?

Document 1. Le réseau mondial des câbles sous-marins

Cependant, cette vision d'un espace sans frontières est nuancée par la réalité d'un ancrage physique. Le cyberespace repose sur une infrastructure tangible, incluant :

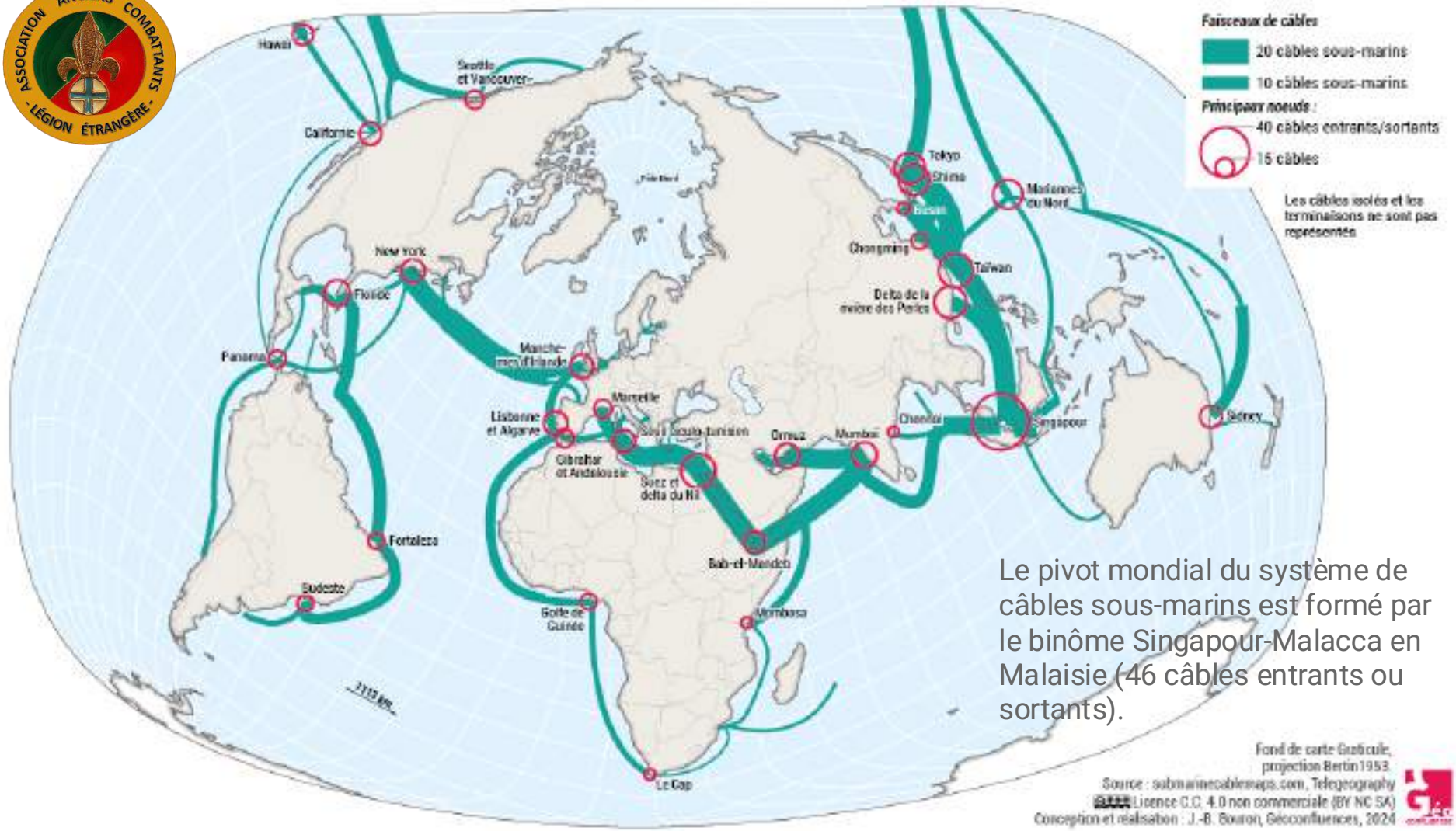
- des câbles sous-marins
- des réseaux terrestres de fibre optique / de câbles en cuivre
- des réseaux spatiaux
- des serveurs informatiques
- des datacenters
- des dispositifs connectés ou non connectés au réseau Internet…

Tous ces éléments physiques sont localisables et soumis à des juridictions spécifiques. Cette infrastructure physique rend les frontières géographiques et juridiques pertinentes, même si elles sont souvent contournées dans la pratique. En 2025, le nombre d'utilisateurs atteint 5,64 milliards, soit 68,7 % de la population mondiale, selon une étude publiée en avril 2025 par We Are Social et Meltwater.

1. Le cyberespace, nouveau champ d'opérations

1.2 Cyberespace : un terrain sans frontières ?

Document 1. Le réseau mondial des câbles sous-marins



Le pivot mondial du système de câbles sous-marins est formé par le binôme Singapour-Malacca en Malaisie (46 câbles entrants ou sortants).

Source: https://geoconfluences.ens-lyon.fr/glossaire/cables-sous-marins

Source: https://geoconfluences.ens-lyon.fr/glossaire/cables-sous-marins

1. Le cyberespace, nouveau champ d'opérations

1.2 Cyberespace : un terrain sans frontières ?

Des tentatives croissantes de réinstaller une certaine souveraineté nationale se manifestent, notamment par des politiques de contrôle des données, des lois nationales sur la cybersécurité, ou des initiatives comme le Patriot Act aux États-Unis, qui permettent à un État de surveiller des serveurs situés à l'étranger si ceux-ci sont exploités par des entreprises américaines.

Des pays comme la Chine ont également évoqué la possibilité de créer des « Internets parallèles », ce qui reflète un processus de balkanisation du cyberespace, où les frontières numériques se redéfinissent.

Ainsi, bien que le cyberespace soit fondamentalement sans frontières dans sa conception, il est de plus en plus soumis à des formes de gouvernance territoriale et de contrôle national, ce qui montre que les frontières existent, mais sous une forme différente de celle du monde physique.

CLOUDFLARE

Sous certains angles (Cascade des fournisseurs informatiques = IT Supply Chain), le cyberespace est centralisé :

- La panne du logiciel en ligne Cloudflare du 18 novembre 2025 en témoigne. Cette société US spécialisée en protection cybersécurité a stoppé ses services quelques heures et a affecté 20% des acteurs internet mondiaux dont Facebook, X, Marmiton, le site internet de l'Elysée, La Société Générale, Doctissimo, bet365, Canva, Spotify, BrightHR, Decathlon ou encore le jeu League of Legends… Panne informatique = effet en chaine d'un changement des permissions sur un système de base de données; il ne s'agit pas d'une cyberattaque mais d'une erreur opérationnelle technique.

https://www.bfmtv.com/tech/panne-monstre-sur-internet-un-incident-chez-cloudflare-met-a-l-arret-une-partie-du-web-mondial_AN-202511180555.html https://blog.cloudflare.com/18-november-2025-outage/

1. Le cyberespace, nouveau champ d'opérations

1.2 Cyberespace : un terrain sans frontières ?

En outre, le cyberespace ne constitue pas un simple univers virtuel détaché du monde physique : il est devenu un véritable champ de rivalités géopolitiques, où États, grandes entreprises et acteurs individuels se disputent le contrôle des infrastructures, des données et des flux d'information.

Des épisodes comme la demande adressée par le Département d'État américain à Twitter de reporter une opération de maintenance en Iran illustrent clairement que le cyberespace peut servir d'outil d'influence politique, prolongeant de fait le périmètre de la souveraineté nationale, notamment en préservant un canal de communication crucial pour les manifestants iraniens. Fin 2018, l'Iran est par ailleurs soupçonné d'avoir mobilisé des milliers de faux comptes privés sur des plateformes comme Facebook et Twitter afin de mener une campagne de manipulation de l'information à l'échelle mondiale (Pierre Pahlavi, « La stratégie de cyber-influence de la République islamique d'Iran », Le Rubicon, 7 avril 2022).

Parallèlement, des acteurs comme l'ICANN, organisation de droit privé, jouent un rôle central dans la gouvernance d'Internet, ce qui montre que le cyberespace, tout en étant ouvert, reste encadré par des règles et des autorités qui en fixent les limites. D'abord liée au gouvernement américain par contrat, l'ICANN a progressivement acquis son autonomie. Basée à Playa Vista, en Californie, elle est notamment chargée de la gestion de l'adressage IP, des noms de domaine de premier niveau (TLD) et du système des serveurs racines du DNS.Ainsi, le cyberespace apparaît à la fois comme un espace sans frontières et comme un lieu de confrontation où les frontières sont sans cesse réinventées, redéfinies, voire renforcées.

1. Le cyberespace, nouveau champ d'opérations

1.2 Cyberespace : un terrain sans frontières ?

Dans cette logique, la guerre économique trouve dans le cyberespace un prolongement privilégié. Les États comme les entreprises s'y affrontent pour capter des informations stratégiques (données industrielles, brevets, savoir-faire) ou pour fragiliser la compétitivité d'un concurrent en perturbant ses chaînes de production et de valeur.

Les rançongiciels, les attaques contre les systèmes industriels (OT) ou encore l'espionnage numérique deviennent ainsi des instruments de puissance économique autant que des outils criminels.

La France a déjà fait l'expérience de ces logiques de confrontation.

En 2017, le constructeur automobile Renault a dû interrompre temporairement la production sur plusieurs sites à la suite de l'attaque mondiale au rançongiciel WannaCry, illustrant la capacité d'un malware à paralyser des chaînes industrielles entières et à générer des pertes économiques significatives.

La même année, l'onde de choc du malware NotPetya a fortement touché le groupe Saint-Gobain, dont le coût de l'incident a été estimé à plusieurs centaines de millions de dollars, alors que l'attaque visait à l'origine l'Ukraine dans un contexte de tensions géopolitiques.

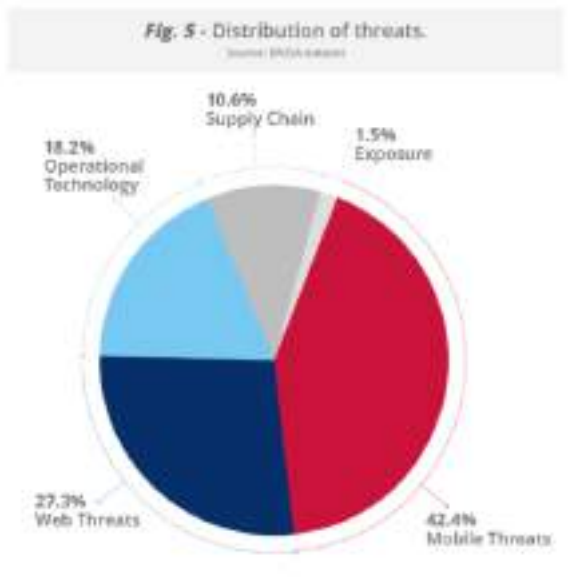
Ces cas montrent comment des entreprises françaises peuvent devenir des « dommages collatéraux » de confrontations étatiques dans le cyberespace, avec des effets très concrets sur l'économie réelle.

Au-delà du sabotage, la guerre économique en ligne passe aussi par l'espionnage industriel. Airbus a ainsi été la cible de plusieurs campagnes visant ses propres systèmes puis ceux de ses sous-traitants, les assaillants cherchant à s'emparer de secrets commerciaux et technologiques sensibles.

Face à ces menaces, l'ANSSI – autorité nationale en matière de cybersécurité – insiste sur la vulnérabilité des PME et sur la nécessité de renforcer la sécurité numérique de l'ensemble du tissu productif français, en diffusant guides pratiques, formations (SecNumacadémie) et dispositifs d'alerte.

La cybersécurité devient ainsi un enjeu central de souveraineté économique : elle ne relève plus seulement de la protection technique des systèmes d'information, mais de la défense des intérêts stratégiques de la Nation dans un contexte de compétition mondiale accrue.

1. Le cyberespace, nouveau champ d'opérations
1.3 Évolution des menaces : individus, groupes, États

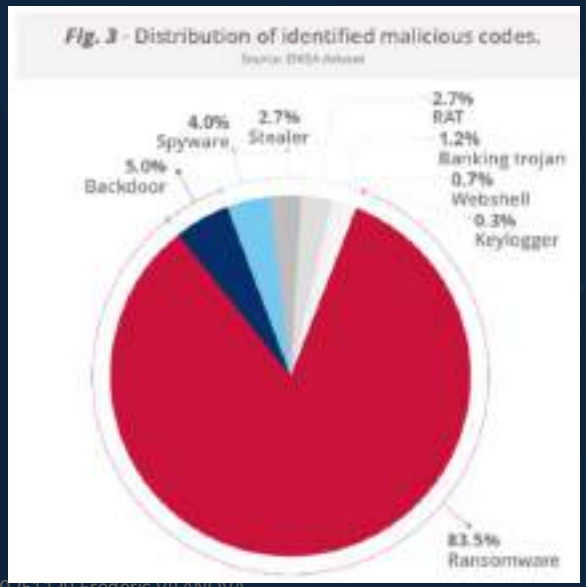


La cybersécurité fait face à une évolution rapide des menaces, avec une multiplication des acteurs malveillants, allant des individus isolés aux États, chacun ayant des motivations et des méthodes distinctes.

Les attaques par rançongiciels restent la menace principale pour les entreprises et institutions françaises, tandis que les groupes cybercriminels, souvent soutenus par des États, exploitent des vulnérabilités croissantes pour des fins financières ou d'espionnage. Les menaces d'origine étatique, notamment de la Chine, de la Russie, de l'Iran et de la Corée du Nord, se seraient intensifiées, avec semble-t-il une multiplication par quatre des intrusions financières soutenues par ces pays en 2024.

CYBERSECURITY NIS2 ENISA THREAT LANDSCAPE 202510 :
https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025_0.pdf

Synthèse de la menace informatique spécifique aux Collectivités Territoriales:
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-002.pdf



Individus et groupes cybercriminels :

La cybercriminalité s'est démocratisée, permettant à des individus peu expérimentés d'exploiter des outils disponibles sur le Dark Web, souvent accompagnés de tutoriels clairs, pour compromettre des systèmes.

Les rançongiciels sont la menace la plus courante, affectant désormais les petites entreprises et les particuliers, avec des attaques de type "pêche au chalut" ou des tentatives d'ingénierie sociale comme les faux messages de colis non livrés.

Des groupes comme APT 44 (supposé Russie) ou APT41 (supposé Chine) utilisent des ransomwares à la fois pour extorquer de l'argent et collecter des renseignements.

1. Le cyberespace, nouveau champ d'opérations
1.3 Évolution des menaces : individus, groupes, États

Acteurs étatiques et para-étatiques :

Les États étrangers, dont la Chine, la Russie, l'Iran et la Corée du Nord, utiliseraient le cyberespace pour des opérations d'espionnage, de sabotage ou de déstabilisation.

Ces opérations, souvent menées par des groupes spécialisés comme APT 41 ou APT 44, combinent trivialité et sophistication, rendant leur attribution difficile grâce au principe de "plausible deniability". La France est ciblée par des acteurs aux intérêts hétérogènes, et la DGSI assure une mission proactive de détection et d'imputation des ingérences cyber.

https://www.dgsi.interieur.gouv.fr/dgsi-a-vos-cotes/cyberdefense/letat-de-menace-cyber-en-france

Les conseils de la DGSI aux entreprises et aux institutions pour se préserver de l'ingérence : https://www.dgsi.interieur.gouv.fr/dgsi-a-vos-cotes/contre-espionnage/conseils-aux-entreprises-flash-ingerence

https://www.dgsi.interieur.gouv.fr/incidents-impliquant-des-chercheurs-etrangers-accueillis-dans-cadre-de-programmes-academiques

https://www.dgsi.interieur.gouv.fr/risques-associes-a-lutilisation-doutils-numeriques-personnels-a-des-fins-professionnelles

https://www.dgsi.interieur.gouv.fr/facteur-humain-principal-vecteur-de-compromission-des-systemes-dinformation

https://www.dgsi.interieur.gouv.fr/incidents-survenus-a-loccasion-de-visites-publiques-de-sites-industriels-de-societes-ou-de

https://www.dgsi.interieur.gouv.fr/risque-datteinte-a-reputation-dentreprises-ou-de-laboratoires-francais-evoluant-a-linternational

https://www.dgsi.interieur.gouv.fr/vols-de-donnees-par-des-collaborateurs-internes-a-societe

Autres acteurs :

- Les hacktivistes, comme le groupe Anonymous, cherchent à défendre des causes politiques ou environnementales en exposant des informations sensibles.
- Les cyberterroristes, bien que moins fréquents, peuvent frapper à tout moment, notamment en période d'actualité sensible.
- Les employés d'entreprise, par méconnaissance ou mauvais usage, peuvent également devenir des acteurs de menace, notamment par le biais de phishing.

1. Le cyberespace, nouveau champ d'opérations

1.3 Objectifs : Comprendre, Prévenir, Réagir

- Comprendre la cybersécurité

La cybersécurité vise à protéger les systèmes informatiques, les réseaux et les données contre les accès, utilisations, divulgations, perturbations, modifications ou destructions non autorisés. Elle englobe un ensemble de pratiques, technologies, politiques et processus conçus pour assurer la confidentialité, l'intégrité et la disponibilité des informations.

Les cyberattaques peuvent prendre diverses formes, comme le phishing (email pour voler vos identifiants et mots de passe), le ransomware (chiffre vos données et demnde une rançon), les attaques par déni de service (DDoS, sature les serveurs et bloque les flux) ou l'exploitation de maliciels (malware, s'immisce chez vous et exploite les données à des fins malveillantes). Comprendre ces menaces permet d'identifier les vulnérabilités et de renforcer les défenses numériques.

- Prévenir les cybermenaces

La prévention repose sur des mesures proactives pour réduire le risque d'incidents.

Parmi les meilleures pratiques :

- Mettre à jour régulièrement systèmes et logiciels.
- Utiliser des antivirus et pare-feu efficaces.
- Appliquer l'authentification à deux facteurs au moins (2FA, comme avec les applications bancaires…).
- Chiffrer les données sensibles.
- Effectuer des sauvegardes fréquentes et sur des supports différents (en line et hors ligne).
- Mettre en place une politique de sécurité claire au sein des organisations et la faire respecter.
- Effectuer une veille informationnelle cyber (vulnérabilités nouvelles, techniques d'attaque émergentes) permet d'anticiper les nouvelles menaces

1. Le cyberespace, nouveau champ d'opérations

1.3 Objectifs : Comprendre, Prévenir, Réagir

- Réagir à une cyber-attaque

En cas d'attaque, une réponse rapide et structurée est essentielle.

Les étapes clés incluent :

- Identifier et isoler les systèmes compromis.
- Évaluer l'ampleur de l'incident.
- Communiquer de manière adaptée avec les parties prenantes.
- Collaborer avec des experts pour contenir et éradiquer la menace.
- Mettre en œuvre un plan de reprise informatique / activités (PRI,PRA) pour restaurer les services et le travail en mode normal.
- Analyser l'incident pour en tirer des enseignements.

Les cadres comme le NIST Cybersecurity Framework américain ou le modèle MITRE ATT&CK® aident à structurer la réponse aux incidents de manière efficace.

Les guides français de l'ANSSI sont forts utiles également.

L'adhésion à une norme internationale telle que l'ISO 27001 (système de mangement de la sécurité de l'information) permet de piloter clairement pour se doter d'un socle informatique sécurisé. L'utilisation d'une méthodologie d'analyse de risque comme l'ISO 27005 et/ou l'EBIOS RM français, permet d'orienter sa démarche sur les processus et données critiques.

2. Le risque numérique est protéiforme

2.1 Le risque numérique, une réalité stratégique économique

2.2 Maîtriser les cyber risques en entreprise et en collectivités

2.3 Maîtriser une cyberattaque

2. Le risque numérique est protéiforme

2.1 Le risque numérique, une réalité stratégique économique

- Transformation numérique et dépendance accrue aux technologies

La transformation numérique, accélérée par la pandémie et la généralisation du télétravail, a profondément transformé les modes de fonctionnement des entreprises, entraînant une dépendance accrue aux technologies numériques, au cloud, aux objets connectés (IoT) et à l'intelligence artificielle.

Cette évolution, bien que porteuse de bénéfices comme une meilleure communication interne et externe, élargit considérablement la surface d'exposition aux cybermenaces. En effet, la montée en complexité des infrastructures numériques, combinée à l'expansion des dispositifs IoT souvent peu sécurisés, crée de nouvelles vulnérabilités et des points d'entrée potentiels pour les attaquants.

La domotique personnelle (télévision connectée, caméra connectées, réfrigérateur connecté, IoTs Internet des Objets…) et les véhicules connectés élargissent également considérablement la surface d'exposition aux cybermenaces

Les cyberattaques se multiplient et gagnent en sophistication, notamment grâce à l'usage croissant de l'intelligence artificielle générative par exemple pour automatiser les campagnes de fraude.

Cette menace s'accentue dans les secteurs critiques comme l'énergie, les transports et la santé, où les attaques peuvent avoir des conséquences graves.

2. Le risque numérique est protéiforme

2.1 Le risque numérique, une réalité stratégique économique

- Les organisations restent largement insuffisamment préparées.

Selon l'étude Global Digital Trust Insights de PwC du 06/11/2025, seulement 6 % des entreprises se sentent pleinement prêtes à faire face à une cyberattaque, un chiffre alarmant face à l'intensification des menaces

Cette insuffisance s'explique par une dépendance à des solutions de sécurité traditionnelles, comme les pares-feux ou les systèmes de contrôle d'accès, qui ne suffisent plus face à la complexité actuelle. Ce chiffre alarmant révèle un décalage criant entre les ambitions stratégiques et la maturité opérationnelle des organisations, même si 78 % d'entre elles prévoient d'augmenter (de combien?) leur budget cybersécurité en 2026 (en pratique on voit diminuer les budgets de maîtrise pour acheter vite fait des outils de protection, pour compenser la dette technique).

De plus, les entreprises peinent à intégrer la cybersécurité dans leur transformation numérique, la considérant souvent comme une problématique distincte plutôt que comme une pierre angulaire de cette transformation.

La formation effective des employés, facteur humain essentiel, reste un enjeu majeur, car l'erreur humaine est une des principales causes de failles de sécurité (erreur d'usage, erreur de paramétrage technique, erreur de management, erreur d'audit…).

2. Le risque numérique est protéiforme

2.2 Maîtriser les cyber risques en entreprise et en collectivités

Pour faire face à ces défis, les organisations doivent adopter une approche intégrée, incluant des politiques de sécurité robustes, des solutions automatisées, des architectures Zero Trust, et une gestion proactive des vulnérabilités. La cybersécurité doit être vue comme un pilier fondamental, non pas un obstacle, pour garantir la continuité des opérations, la protection des données sensibles et la résilience des infrastructures numériques critiques.

- Le risque cyber est désormais un risque d'entreprise
- Les critères fondamentaux de la sécurité de l'information:

  Confidentialité Intégrité Disponibilité

  auxquels on ajoute souvent :

  Traçabilité Authenticité (pas de « fake ») Privacité (données personnelles)

- Gouvernance et 3 lignes de maîtrise (AMRAE/ANSSI)

Audit interne – IFACI Guide des risques cyber 3.0 auquel j'ai participé :
https://www.ifaci.com/guide-des-risques-cyber-3-0/#dlguide

Guides ANSSI / gouvernement

https://cyber.gouv.fr/construire-la-gouvernance-de-securite-numerique-adaptee-son-organisation

https://cyber.gouv.fr/parcours-de-cybersecurite

2. Le risque numérique est protéiforme
2.3 Maîtriser une cyberattaque

A. Se préparer à une crise d'origine cyber nécessite :

- De connaître son Système d'information,
- D'analyser régulièrement les risques associés et leurs impacts,
- De mobiliser son organisation,
- De formaliser un processus de gestion de crise,
- De se former
- Et de s'entrainer régulièrement à la gestion de crise.

En cybersécurité comme en santé, mieux vaut prévenir que guérir ! Des mesures préventives (organisationnelles, humaines, physiques, technologiques) sont nécessaires, avec la mise en place d'un véritable management de la sécurité de l'information et des données.

2. Le risque numérique est protéiforme

2.3 Maîtriser une cyberattaque

B. Détecter une cyberattaque

- Détecter une attaque est difficile, surtout si elle n'est pas "bruyante".
- La base repose sur une bonne formation et une pratique régulière de la surveillance du trafic réseau, de l'analyse des journaux de sécurité.
- La surveillance des points de terminaison (PC, Mac, Tablettes, Smartphones, Photocopieurs, etc.) et des serveurs informatiques permet également de récolter des indicateurs de compromission (IOC).
- Certains outils de technologies avancés sont pertinents selon la taille de votre organisation.

Ralentissements inexpliqués

Des ralentissements soudains des systèmes peuvent indiquer une attaque en cours

Messages et activités suspectes

Surveillez les emails suspects, les modifications non autorisées de fichiers, et les comportements inhabituels des comptes utilisateurs

Signalements des utilisateurs ou des tiers

Anomalie de fonctionnement, réception de mail douteux, problématique d'accès des métiers...

2. Le risque numérique est protéiforme

2.3 Maîtriser une cyberattaque

C. Gérer et clôturer une cyberattaque

- Activer le mode de crise (critères, équipe)
- Etablir /actualiser un plan de gestion de crise
- Gérer le confinement
- Analyser en détail et éradiquer les éléments malveillants ou compromis
- Gérer le fonctionnement en mode dégradé : le système D
- Récupérer : rétablir le système en mode normal (restaurer, reconstruire, renforcer, reconfigurer, durcir, réinitialiser…)
- Capitaliser l'expérience post-mortem : leçons apprises, mises à jour des politiques, procédures, modes opératoires, exercices de simultaion de crise, formations…

Ralentissements inexpliqués

Des ralentissements soudains des systèmes peuvent indiquer une attaque en cours

Messages et activités suspectes

Surveillez les emails suspects, les modifications non autorisées de fichiers, et les comportements inhabituels des comptes utilisateurs

Signalements des utilisateurs ou des tiers

Anomalie de fonctionnement, réception de mail douteux, problématique d'accès des métiers...

3. Protéger notre quotidien

3.1 Les arnaques informatisées du quotidien, comment s'en protéger ?

3.2 Du quotidien au systémique

3. Protéger notre quotidien
3.1 Les arnaques informatisées du quotidien, comment s'en protéger ?

L'objectif des attaquants « bruyants » est toujours la désorganisation, la mise en stress et la perte de confiance (les attaquants « discrets » restent planqués et non détectables pendant des mois)

=> Réflexes utiles au quotidien :

- Mises à jour et antivirus : Activer les mises à jour automatiques (PC, téléphone, tablette, box, objets connectés). Garder un antivirus/antimalware activé et à jour.
- Sauvegardes régulières: Sauvegarder les photos/documents importants sur un disque externe déconnecté la plupart du temps et/ou un cloud de confiance. En cas de malware ou rançongiciel qui chiffre toutes les données, on évite la catastrophe.
- Mots de passe & double authentification : Un mot de passe fort (> 15 chiffres et caractères dont spéciaux) et différent pour chaque service important (mail, banque, réseaux sociaux). Utiliser un gestionnaire de mots de passe et active la double authentification (2FA), idéalement via une application (Google Authenticator, etc.), pas seulement par SMS (interceptable).
- Vérifier avant de cliquer : Ne jamais cliquer spontanément sur un lien ou une pièce jointe reçus par mail/SMS/messagerie si c'est non attendu. Passer la souris sur le lien (sur ordinateur) ou regarder bien l'adresse qui s'affiche : si elle est bizarre, raccourcie ou mal orthographiée → poubelle.
- Toujours passer par le site officiel: Pour la banque, les impôts, l'URSSAF, les colis…, taper soi-même l'adresse dans le navigateur ou utiliser un « favori », ou mieux un lien de son « coffre-fort de mots de passe ». Jamais un lien reçu par message.
- Ne jamais donner de codes ou mots de passe: Ni par téléphone, ni par mail, ni par SMS, ni via un soi-disant « support technique » à distance. La banque, l'URSSAF, etc., ne demanderont jamais ton mot de passe ou un code de validation complet.
- Limiter ce que l'on expose: Sur les réseaux sociaux, éviter d'afficher publiquement son adresse, sa date de naissance complète, son numéro de téléphone, etc. Moins il y a d'infos, plus c'est difficile d'usurper l'identité.
- Doute = pause : Si un message crée un sentiment d'urgence (« tout de suite », « sinon compte bloqué », « papa répond vite »), arrêtez-vous, respirez, vérifiez par un autre canal (appeler directement au téléphone la personne ou l'organisme à partir d'un numéro connu).
- Utiliser un logiciel d'entretien de son PC/Mac (tel que https://www.ccleaner.com/fr-fr par exemple)
- Utiliser un coffre-fort chiffré pour ses mots de passe (tel que KeypassXC, Strongox…)
- Utiliser un filtre à email vérolés, un anti-spam (tel que https://www.mailinblack.com/) si on a son propre nom de domaine (celui de son entreprise, de son association, de sa famille).
- Chiffrer son surf internet = Utiliser des outils « VPN » sur réseaux publics : hôtel, aéroports, gare, TGV, etc. https://protonvpn.com/fr/free-vpn ; https://freevpnplanet.com/fr/
- Ne pas brancher un cable USB sur une prise USB publique (gare, aéroport, hôtel…)
- Utilisez un routeur de sécurité équipé d'un pare-feu intégré (BBOX, FREEBOX, SFRBOX8…)

3. Protéger notre quotidien
3.1 Les arnaques informatisées du quotidien, comment s'en protéger ?

Hameçonnage email, SMS, vocal, IA Intelligence Artificielle
(Phishing, smishing, vishing, faux « Bonjour papa », faux support technique, faux conseiller bancaire…)

1. Ne pas cliquer pas sur les liens ni les pièces jointes.
2. Vérifier l'adresse email / le numéro de téléphone (souvent approximatif, étranger, ou très générique).
3. Pour un faux « Bonjour papa / maman » ou un appel paniqué :
   - Rappeller son enfant / son proche sur son vrai numéro ou via un autre canal.
   - Si la personne refuse que l'on raccroche pour vérifier → quasi sûr que c'est une arnaque.
4. Un support technique ou conseiller bancaire qui demande :
   - d'installer un logiciel de prise en main à distance,
   - de valider des transactions que tu n'as pas initiées,
   - de donner des codes reçus par SMS

   ⇒ raccrocher immédiatement et appeler la banque / l'éditeur du logiciel sur le numéro officiel.

   En France, on peut signaler les SMS frauduleux en les transférant au 33700, plateforme officielle contre les spams SMS et appels malveillants.

3. Protéger notre quotidien
3.1 Les arnaques informatisées du quotidien, comment s'en protéger ?

QR codes piégés

1. Considérer un QR code comme un lien cliquable :
   - Ne pas scanner ceux qui traînent sur des affiches collées à la va-vite, sur des mails douteux, etc.
   - Après scan, regarder attentivement l'URL avant de valider l'ouverture.
   - Si le QR code demande un paiement ou des identifiants, redoubler de prudence : taper plutôt l'adresse du site soi-même.

Réseaux sociaux, usurpations, faux profils & rencontres en ligne

1. Activer la double authentification sur vos comptes et vérifier régulièrement les connexions actives.
2. Si vous voyez un compte qui utilise votre photo ou votre nom : signalez-le à la plateforme et prévenez vos contacts.
3. Arnaques sentimentales / faux profils (sites de rencontre ou réseaux sociaux) :
   - la relation évolue très vite, la personne déclare son amour, mais ne peut jamais te voir « pour de vrai »
   - au bout d'un moment, demande d'argent (billet d'avion, frais médicaux, douane, dette urgente…).

   ⇒ Ne jamais envoyer d'argent, de photos intimes ou de copies de pièce d'identité à quelqu'un que l'on n'a jamais rencontré physiquement.

3. Protéger notre quotidien
3.1 Les arnaques informatisées du quotidien, comment s'en protéger ?

Faux sites (banques, e-commerce, URSSAF, etc.), fausses factures & faux présidents

1. Faux sites de commerce / enchères / banques / URSSAF :
   - Vérifier le nom de domaine exact (orthographe, .fr / .com, pas d'ajout suspect).
   - Un site sérieux a des mentions légales complètes, une vraie adresse postale et un SIRET vérifiable sur les sites haituel : https://www.pappers.fr/ https://www.sirene.fr/sirene/public/static/recherche
   - Cherche le nom du site + « arnaque » dans un moteur de recherche avant de payer.Privilégie les moyens de paiement qui offrent une protection (carte bancaire, PayPal…) et évite les virements instantanés vers des inconnus.
2. Fausses factures, faux présidents / faux conseillers :
   - Très répandu dans les entreprises, mais ça peut toucher les indépendants/auto-entrepreneurs.
   - Vérifier systématiquement un RIB ou une demande de paiement « urgente » via un autre canal (appeler le vrai client, ton vrai comptable, etc.).
   - Pour les nouveaux destinataires d'un virement bancaire (nouveau fournisseur) : virer 1 € et appeler le destinataire au téléphone pour savoir si il a ien reçu sur le bon compte bancire.

3. Protéger notre quotidien
3.1 Les arnaques informatisées du quotidien, comment s'en protéger ?

Offres d'emploi, prix gagnés, dons, prêts, fausses associations

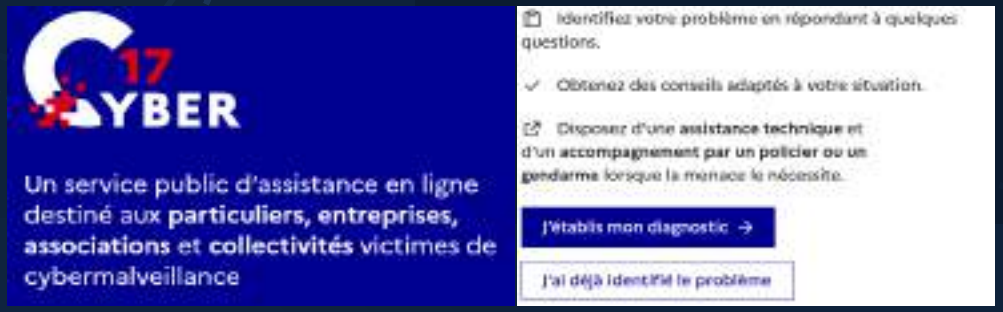
1. Offres d'emploi fictives :
   - Poste très bien payé pour très peu de travail, recrutement ultra rapide, demande de copies de papiers d'identité, RIB, achats de matériel à vos frais → drapeau rouge.
   - Ne jamais envoyer d'argent pour « frais de dossier », « matériel à rembourser », etc.
2. Prix gagnés / loteries / héritages :Si tu n'as pas participé, c'est une arnaque. On ne paie pas pour recevoir un gain.
3. Fausses organisations caritatives, faux crowdfundings :
   - Passer par des plateformes connues, ou par le site officiel de grandes associations.
   - Vérifier sur un moteur de recherche « le nom de l'association + arnaque » avant de donner.
4. Prêts avec frais à payer d'avance :
   - C'est presque toujours frauduleux. Un organisme de crédit sérieux ne te demande pas de payer des « frais » avant de verser l'argent.
5. Messages / vidéos de détresse depuis l'étranger :
   - Scénario classique : un proche en voyage, bloqué, demande un virement urgent.
   - Vérifier toujours par un autre moyen (appel vidéo sur un canal connu, appel à un autre proche, etc.) avant d'envoyer quoi que ce soit.

3. Protéger notre quotidien
3.1 Les arnaques informatisées du quotidien, comment s'en protéger ?

Que faire en cas de doute ou si l'on est victime (France)

1. Pour s'informer / avoir des tutoriels simples :
   - https://www.cybermalveillance.gouv.fr/ : fiches pratiques « Hameçonnage, que faire ? », « Faux support technique », « Fraude au faux conseiller bancaire », etc.
   - L'ANSSI propose aussi des guides de bonnes pratiques pour le grand public. https://cyber.gouv.fr/publications

2. Pour signaler une escroquerie / un site frauduleux :
   - https://internet-signalement.gouv.fr/ (plateforme THESEE & PHAROS) pour les escroqueries en ligne, faux sites de vente, contenus illicites, etc.
   - https://www.masecurite.interieur.gouv.fr/fr Ma Sécurité (Police) pour les harcèlements etc.
   - +33700 : numéro téléphonique du service national français de plainte des SMS ou appels vocaux frauduleux
   - https://www.cybermalveillance.gouv.fr/17cyber Pour être aidé en cas de cyberattaque. La nouvelle plateforme 17Cyber oriente les victimes vers les bons interlocuteurs (Pharos, Perceval, forces de l'ordre, etc.) et donne des conseils immédiats.



3. Protéger notre quotidien
3.2 Du quotidien au systémique

On peut expliquer l'effet papillon de façon très simple :

- L'hygiène numérique quotidienne réduit la probabilité qu'une machine serve de "première marche" à une attaque de grande ampleur. Les mesures de base que promeut l'ANSSI – mises à jour, mots de passe robustes, sauvegardes, limitation des droits, sensibilisation des utilisateurs – visent justement à empêcher les attaquants de prendre pied sur un poste, un téléphone ou un petit serveur « anodin ».

- Or ce sont souvent ces points d'entrée banals (PC perso d'un télétravailleur, compte mail réutilisé partout, box mal configurée, objet connecté vulnérable…) qui servent ensuite de tremplin vers une entreprise, une collectivité, un hôpital, voire un opérateur d'importance vitale.

- Autrement dit : en empêchant une petite compromission locale, on casse une marche de l'escalier qui mène à un incident majeur.

- Les exercices comme REMPAR25, organisés par l'ANSSI, simulent justement ce type de crise «systémique», où de nombreuses organisations sont touchées en même temps et doivent assurer la continuité d'activité, coordonner leurs réponses et communiquer sous pression.
    - Dans ces scénarios, la gravité de la crise dépend directement de la facilité avec laquelle les attaquants peuvent enchaîner les rebonds : exploiter des mots de passe faibles, contaminer des postes non mis à jour, transformer des milliers d'objets peu sécurisés en botnet pour saturer des services essentiels, etc.
    - Plus il y a de maillons faibles dans la population (particuliers, PME, associations, collectivités), plus le risque de propagation et d'emballement est élevé.
    - J'ai été animateur au CyberCampus Région Sud dans le dernier exercice REMPAR25, c'était très intéressant. https://cyber.gouv.fr/actualites/rempar25-un-exercice-de-crise-cyber-dune-ampleur-inedite

3. Protéger notre quotidien
3.2 Du quotidien au systémique

L'effet papillon, c'est donc l'idée suivante :

- Quand un individu applique l'hygiène numérique (ne clique pas sur un lien piégé, met à jour son téléphone, active la double authentification), il protège ses propres données ;
- Quand des millions de personnes font la même chose, on réduit massivement le nombre de machines et de comptes faciles à compromettre ;
- Ce faisant, on réduit la taille potentielle des botnets, la vitesse de propagation des malwares et le nombre de portes d'entrée vers les organisations critiques : on diminue donc le risque de crise systémique telle que simulée dans REMPAR25.

4. Conclusion et « Call to Action »

4. Conclusion et « Call to Action »

Le cyberespace conçu sans frontières est de plus en plus soumis à des formes de gouvernance territoriale et de contrôle national, ce qui montre que les frontières existent, mais sous une forme différente de celle du monde physique.
Les menaces cyber se sont développées très rapidement ces 10 dernières années, le hacking non éthique s'est démocratisé. La guerre économique utilise les armes cyer également.
Il faut donc :

- Comprendre ce dont il s'agit,
- Changer sa façon de faire en informatique au plan personnel comme professionnel
- Apprendre à réagir à une cyber-attaque de manière préparée et structurée.

Ce n'est pas simple mais le monde numérique est ainsi, il facilite beaucoup de choses mais nous expose et nous contraint également. En cyber comme sur le terrain, la vigilance sauve.

CALL TO ACTION

En prenant deux minutes pour mettre à jour votre téléphone ou vérifier un mail suspect, vous ne protégez pas seulement vos photos et vos comptes : vous évitez aussi, à votre échelle, que votre appareil devienne une arme dans une attaque qui pourrait perturber un hôpital, une ville ou un service public. Vos petits gestes d'hygiène numérique, multipliés par des millions d'utilisateurs, rendent les grandes crises beaucoup plus difficiles à déclencher.

Merci à chacun de vous pour votre attention et un grand merci à notre organisateur et animateur de la dynamique de l'association!

Contact : Frederic Vilanova https://fr.linkedin.com/in/fredericvilanova

Questions


ASSOCIATION ANCIENS COMBATTANTS
- LÉGION ÉTRANGÈRE -
MONSIEUR
Légionnaire


ASSOCIATION ANCIENS COMBATTANTS
- LÉGION ÉTRANGÈRE -
MONSIEUR
Légionnaire

Remerciements de l'organisateur à:

-Lcl Christian et Marie-Dominique SABATIER,
- M. Frédéric VILANOVA, pour brillance intervention,
- Les Cch BIANCHI et ROMANO,
- Les Dames qui ont apporté des agapes,
- M. Christian MICHEL, ancien Cre aux comptes,
- Lég. de 1re Cl Christian LALOUX, clairon.
- Mme Patricia GOMEZ-BASQUEZ,
- Mme Jeanne LIANOS,
- à tous les participants à cette conférence et à sa préparation,
- Merci d'avance à tous ceux qui nous aideront pour le démontage.

Prochaines activités de l'AACLE et Confrérie de SALG

- 30 novembre à 9h30 à l'Arc de Triomphe : Cérémonie du Souvenir Napoléonien
- 12 décembre : Assemblée générale pour l'année 2025 au Lycée-Hôtelier d'Aix-Marseille.
- 14 décembre : Visite à nos Séniors de 9 à 18 h 00.
- Du 14 décembre 2025 au 6 janvier 2026 le siège de l'AACLE sera fermé
- 17 janvier 2026 après-midi :
  - 14 à 17h 00 : préparation de la crypte à confirmer si éclairage est réparé.
  - 17 h 30 : bénédictions des écharpes et écussons de la Confrérie de SALG
  - 21h à 23h : veillée à confirmer suivant l'état de la crypte sinon pas de veillée.

18 janvier 2026 :

- à 8h00 : ouverture de la crypte et MEP pot par l'équipe de X. LAQUIEZE
  de 8 à 9h45 : préparation et récupération des écussons et écharpes.
- 10 h 00 : installation dans la basilique Sacré-Cœur, (lumignons statue SALG)
- 10 h 15 : formation de la procession sur parvis de Sacré-Cœur
- 10 h 29 : entrée en procession après les porte-drapeau.
- 11 h 30 : sortie en procession photo sur le parvis puis à la crypte.

Pot de l'amitié : (inscription payante 10€ par personne)

Chapitre de la Confrérie de SALG du 29 11 2025

Remise des écussons aux membres dont les noms suivent:

Madame **Marceline THU THON,**

Madame **Christiane THU THON,**

Madame **Marie-Louise PHILIPPON,**

Madame **Marie-Denise GARRENNE-THIEU,**

Madame **Madette JAMOND,**

Madame **Mariamo SUAREZ,**

Monsieur **Fréderic VILANOVA,**

Leg. de Classe **Christian LALOUX,**