AUTOMOTIVE CYBERSECURITY (Ampere - Romain RIVIERE)

OEM : vehicle manufacturers

1. Contexte & Évolution

Ampere (Renault) : Créée en oct. 2023. Focus : **EV & Software**.

Historique :

- **1960-80s :** Mécanique → Électronique simple (Moteur, ABS).
- **1970-1980 :** Injection électronique de carburant, système de freinage antiblocage (ABS), affichages numériques du cockpit, boîte de vitesses.
- **1990-2000 :** Système d'infodivertissement, navigation GPS, technologies de conduite autonome (débuts).
- **2000 :** Multiplication des **ECU** (Electronic Control Unit). Introduction du bus **CAN** (réduction câblage) et **OBD-2** (diagnostic).
- **Auj. :** "Smartphone sur roues". Connectivité totale (Cellulaire, Wi-Fi, BT), ADAS, OTA (Over-The-Air). Surface d'attaque sans précédent.

2. Modèle de Menaces (Threat Model)

Target for Attackers

- **Safety :** harm road users (injuries, fatalities...)
- **Operational :** Disrupt functionality (partial or complete failure)
- **Privacy :** Access private and/or Personal Identifiable Information (PII)

Motivations

- **Safety :** Cause harm to others
- **Financial gain :** Extort money, install cryptographic miners
- **Operational :** disrupt operations by disabling vehicles
- **Recognition :** gain fame or credibility

Threat agents

- **Utilisateur légitime : Budget :** Presque aucun. **Expertise :** Profane. **Motivation :** Déblocager de fonctions ou modification de données.
- **Réparateur malhonnête : Budget :** Moyen (garage). **Expertise :** Bon savoir-faire véhicule. **Motivation :** Tuning, recul kilométrage ou pièces contrefaites.
- **Voleur (thief) : Budget :** Modeste. **Expertise :** Compétences pratiques (outils de vol). **Motivation :** Cible les véhicules ou leur contenu.
- **Initié (Insider) : Budget :** Aucun requis. **Expertise :** Accès privilégié. **Motivation :** Vol de données confidentielles ou utilisateur.
- **Hacktiviste : Budget :** Variable/limité. **Expertise :** Expert d'un domaine. **Motivation :** Dégradation politique ou interruption de service.
- **Chercheur : Budget :** Modéré. **Expertise :** Équipe de spécialistes. **Motivation :** Visibilité publique via divulgation de vulnérabilités.
- **Concurrent : Budget :** Très important. **Expertise :** Équipes d'experts ad hoc [1]. **Motivation :** Espionnage industriel ou sabotage.
- **Crime Organisé : Budget :** Réseau bien financé. **Expertise :** Multi-domaines. **Motivation :** Profit via vente d'outils ou vol de données.
- **Cyberterroriste : Budget :** Financement considérable. **Expertise :** Experts mixtes. **Motivation :** Dommages à grande échelle et peur.
- **État : Budget :** Quasi illimité. **Expertise :** Très étendue. **Motivation :** Espionnage ou cyber-guerre persistante.

1. ad hoc = Fait pour ça

ROI de l'attaquant : L'objectif est de rendre le coût/effort de l'attaque supérieur au gain potentiel. La sécurité est basé sur l'attaquant ! (on protege ce qui est probable de se faire attaquer - rentable/utile pour l'attaquant)

- **Zéro-Day :** Marché gris (ex : Zerodium). Prix en hausse (jusqu'à 5-7M$ pour Zero-click iOS/Android).
- **Acteurs :** Du profane (Layman) à l'État (ressources illimitées, espionnage, cyberguerre).
- **Supply Chain :** Menaces via tiers (Tier-1 à n), Open-source (ex : SolarWinds, xz), App-stores embarqués.

Crowdfence : **Zero Click** : Android (WhatsApp, RCS) (→ 5 M USD), iOS (iMessage) (→ 5 – 7 M USD)

Browsers : Chrome (RCE + LPE) (→ 2 – 3 M USD), Chrome (RCE w/o SBX) (→ 500k USD), Chrome (SBX) (→ 500k USD), Safari (RCE + LPE) (→ 2,5 – 3,5 M USD), Safari (RCE w/o SBX) (→ 500k USD), Safari (SBX) (→ 300 – 400k USD)

Supply-chain attack Aujourd'hui beaucoup d'open source(possible injection de code malicieu) et de sous traitant (injection code, attaque via le réseau partagé ave l'entreprise cible). Ex SolaWinds (2020), xz (2024).

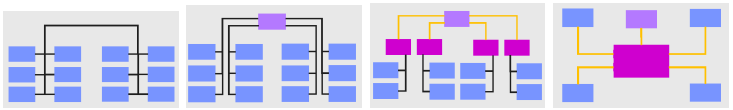
In-car app-stores L'accès aux boutiques d'applications (in car - genre le tableau de bord) expose les véhicules à des logiciels tiers et aux risques de développeurs non fiables(third-party developers).

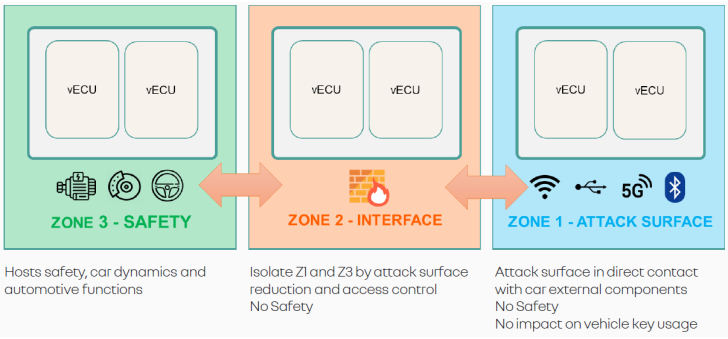
3. Architecture & Principes de Sécurité

ADAS : Driving assistance, **Powertrain :** Engine management, **Body :** Braking/Steering, **Cluster :** Driver information, **GW :** Gateway/Security (Routage & Isolation), **IVC :** Connectivity (5G), **IVI :** Infotainment (Wi-Fi/USB), **OBD :** Diagnostic port. **CAN :** Controller Area Network, **ECU :** Electronic Control Unit.

Évolution Architecture :

- **Before 2010 :** Distributed architecture where each function is implemented on a dedicated ECU connected to a single CAN bus.
- **After 2010 :** Distributed architecture with a Gateway to manage communication between multiple CAN buses for load balancing.
- **After 2015 :** Domain-driven architecture where ECUs are grouped by functional domains and managed by Domain Controllers.
- **After 2020 :** Central/SDV architecture using High Performance Computers (HPC) to centralize functions and Zonal ECUs for physical I/O.





Secure by design

Principes Clés :

- **Secured by Design :** ci-dessus
- **Detect & React :** Monitoring continu + réponse.
- **Preserve & Maintain :** Mise à jour continue contre les menaces évolutives.

4. Étude de Cas : Hack Jeep Cherokee (2015)

ACC : contrôle automatique de la vitesse par l'ECU selon le véhicule précédent. **FCW+** : détection d'obstacles et arrêt automatique pour éviter les collisions. **LDW+** : alerte de franchissement de ligne et correction de trajectoire. **PAM** : détection d'obstacles et guidage autonome pour le stationnement.

Vecteur : Système **UConnect** (Infotainment) exposé sur réseau cellulaire (Sprint).

Failles : **DBUS** en écoute sur port 6667 (accès root sans authentification) + Communication directe entre véhicules autorisée par l'opérateur + Firmware du contrôleur CAN non signé + Messages CAN en clair et non authentifiés.

Résultat : Contrôle à distance des freins, direction, moteur. Rappel de **1,4M** de véhicules. Impulsion pour régulation **UN-ECE R155**.

5. Software Update & SDV

Objectifs OTA (Over-the-Air software update) : Réduction des coûts (facteur 10x vs garage), correctifs rapides, **Features on Demand**. $\Longrightarrow$ plusieurs interfaces et protocoles donc plusieurs ECU donc plusieurs bugs/failles et faut aimer les structures complexes.

Objectifs de Sécurité (Goals)

- **Authenticité :** Origine Renault/Fournisseurs de confiance ; absence d'altération du contenu.
- **Anti-downgrade :** Interdiction de retour à une version antérieure (protection contre les attaques par rejoue).
- **Confidentialité :** Empêcher le *reverse engineering* du contenu de l'update.
- **Sécurité (Safety) & Robustesse :** Exécution sous conditions de sécurité ; protection contre les bugs exploitables.
- **Conformité :** Respect de la norme **UN-ECE R155** (Intégrité, Authentification, Gestion des clés).

Réglementation : Focus UN-ECE R155

- **Intégrité & Authenticité :** Protection systématique du contenu des mises à jour.
- **Crypto & Clés :** Algorithmes à l'état de l'art et gestion des clés ultra-sécurisée.
- **Anti-Downgrade :** Défense contre les attaques par rejoue (*Replay attacks*).
- **Anti-Spoofing :** Sécurisation du canal de communication Serveur OTA $\leftrightarrow$ Véhicule.
- **Sécurité Back-end :** Protection contre les *insider attacks* et l'abus de privilèges staff.

Leviers Techniques (Enablers)

- **Cryptographie :** TLS pour com. sécurisée ; Authentification E2E (End-to-End) ; Ségrégation des clés Engineering vs Production.
- **Architecture :** Segmentation réseau (**VLANs**) ; Proxies/Protocol-breakers internes. **Privilèges :** Application du principe du moindre privilège ; ségrégation des responsabilités.
- **Développement :** Usage de **Rust** pour la sécurité mémoire (*memory safety*).

Architecture SDV (Software Defined Vehicle)

- **Orchestration (PCU) :** Le *Power Compute Unit* centralise : Téléchargement $\rightarrow$ Vérification (Authenticité/Cohérence) $\rightarrow$ Distribution aux ECUs $\rightarrow$ Commit final $\rightarrow$ Ack Serveur.
- **Manifeste de Mise à jour :** Fichier JSON contenant : Hashes des packages, Recette (*Recipe*) d'installation, **VIN** (liaison véhicule spécifique), Signatures et Chaînes de certificats.
- **Complexité :** Gestion de douzaines d'ECUs et environnements variés (RTOS, Linux, Android VMs/APEX, Firmwares, Sub-firmwares).
- **Cohérence :** Utilisation de *Baselines* logicielles pour garantir la compatibilité inter-ECU et éviter les comportements critiques.

6. Gestion des Clés (KMS & HSM)

- **KMS (Key Management System) :** Centralisé, standardisé et auditable. Utilisé par Renault et ses fournisseurs.
- **HSM (Hardware Security Module) :** Protection physique de la confidentialité des clés privées/symétriques.
- **Modèle :** *Crypto As A Service* via APIs ; support du **BYOK** (*Bring Your Own Key*) pour les fournisseurs.

7. Défis Futurs & Maintenance

- **Cycle de vie :** Maintenance requise sur **10, 15, voire 20 ans** (inédit dans le software classique).
- **Réactivité :** Nécessité de réduire la latence des correctifs (vulnérabilités) sur toute la supply-chain.
- **Post-Quantum (PQC) :** Anticipation du cassage de la crypto classique d'ici 2050.
- **Solutions PQC :** Implémentation hybride (PQC + Classique), Root-CA compatible PQC. **Obstacles :** Manque de maturité des IPs SoC, overhead massif (CPU/RAM/ROM) et standardisation incomplète.

Aspects légaux de l'informatique (Pierre-Yves Bonnetain-Nesterenko)

I. Socle Pénal : I&L et Godfrain

Loi I&L (Code Pénal 226-16+) : Sanctionne le traitement de données nominatives sans respecter les formalités, les collectes illégitimes ou les protections inadéquates.

Loi Godfrain (Code Pénal 323-1+) : Réprime les atteintes aux **STAD** (Systèmes de Traitement Automatisé de Données) :

- **Intrusion :** Accès ou maintien frauduleux.
- **Entrave :** Altération du fonctionnement ou déni de service (**DoS**).
- **Données :** Suppression, modification ou vol de données.

Application : Loi française applicable si le délit est **matérialisé en France**, même si les serveurs sont à l'étranger.

II. Données à Caractère Personnel (DCP)

Définition : Toute info permettant d'identifier directement ou indirectement une personne (physique ou numérique).

Méta-données identifiantes :

- **Réseau :** IP, MAC, résolutions DNS, logs de connexion.
- **Mobile :** Traces GPS, migration d'antennes (Cell ID).
- **Fichiers :** EXIF (photos), propriétés bureautiques.
- **Comms :** Listes d'appels, durée, fréquence des SMS.

Principe de Précaution : Une DCP est une "matière fissile" : si on ne sait pas la gérer (collecte, stockage, destruction), il ne faut pas y toucher.

III. RGPD : Obligations et Sanctions

Principes Clés :

- **Responsabilisation (Accountability) :** Plus de déclaration préalable CNIL, mais preuve de conformité permanente.
- **Minimisation :** Uniquement les données **nécessaires**, volume et durée limités.
- **Privacy by Design/Default :** Sécurité et confidentialité dès la conception.
- **Co-responsabilité :** Le donneur d'ordre et le sous-traitant sont solidairement responsables.

Licéité (Conditions de traitement) : Consentement explicite/univoque, exécution contrat, obligation légale, intérêts vitaux, service public ou intérêt légitime.

Sanctions Administratives :

- Jusqu'à **4% du CA mondial** ou **20 M€**.
- Exemples : Google (250 M€), TikTok (530 M€), Amazon (746 M€), Instagram (405 M€).
- Sanctions opérationnelles : **Arrêt du traitement** des données.

IV. Outils de Conformité RGPD

Registre des traitements : Obligatoire ($\geq$ 250 pers. ou traitements à risques). Contient :

- Identité DPO/Responsable, **Finalités**, Catégories de personnes/données.
- Destinataires, Transferts hors UE, Délais d'effacement, Mesures de sécurité.

Registre des incidents : Trace chaque violation (nature, victimes, volume).

Notification des violations : **72h maximum** à la CNIL après détection. Information des victimes si risque élevé.

EIVP (DPIA) : Analyse d'impact obligatoire pour traitements sensibles (santé, biométrie, profilage massif).

Portabilité : Fournir les données dans un format **structuré et lisible par machine**.

V. LCEN, LOPPSI et Lois Spéciales

LCEN (2004) :

- **Traçabilité :** Conservation IP/MAC par FAI/Hébergeurs (théoriquement 1 an).
- **Hébergeurs :** Responsabilité **a posteriori** après notification de contenu illicite.
- **Mentions Légales :** Obligatoires (Siret, Capital, Directeur publication, Hébergeur).

LOPPSI 2 (2011) : Blocage administratif de sites (listes noires IP/URL) sans juge.

LPM 2023 : Obligation pour les éditeurs de signaler les vulnérabilités à l'**ANSSI**.

eIDAS : Impose aux navigateurs des certificats racine d'États membres.

VI. Cyber Resilience Act (CRA)

Champ d'application : Fabricants/Importateurs de produits logiciels et matériels connectés en UE.

Exigences de Sécurité :

- **Zéro vulnérabilité connue** à la mise sur le marché.
- **Configuration sécurisée** par défaut.
- **Mises à jour :** Séparation MAJ sécurité / MAJ fonctionnelles. Distribution gratuite et auto.
- **SBOM :** Inventaire complet des composants (Software Bill of Materials).

Catégories de produits :

- **Par défaut :** Majorité des produits.
- **Important Classe I :** VPN, Antivirus, Gestionnaires de mots de passe, OS, Navigateurs, Jouets connectés.
- **Important Classe II :** Firewalls, Hyperviseurs, Microprocesseurs tamper-resistant.
- **Critique :** Cartes à puce, HSM, Tachygraphes.

Sanctions : Jusqu'à 2,5% CA ou 15 M€ + **Rappel produit** et retrait du marché.

VII. Vie Privée et Travail

Poste de travail : Présumé professionnel. L'employeur peut y accéder librement.

Mention "Privé" : Seule mention protégeant le contenu (fichiers, dossiers, emails).

- L'employeur peut voir le **volume** mais pas lire le **contenu** sans le salarié (sauf impératif technique).
- Une clé USB perso sur poste pro est présumée pro sauf mention contraire.

Preuve Illicite : Recevable si l'atteinte à la vie privée est **proportionnée** et indispensable au droit à la preuve (Cass. 2021).

Chiffrement : L'employeur peut exiger le **déchiffrement** des données pro. Pour le privé, il peut exiger le déchiffrement (procédure) mais pas le mot de passe.

VIII. Surveillance et Logs

Contrôle : Information préalable obligatoire des salariés et des représentants (CSE). Pas de surveillance occulte ou individuelle ciblée sans preuve.

Journaux d'activité :

- **Finalité :** Ne peuvent être détournés (ex : utiliser les logs accès pour flicage horaire est illicite).
- **Conservation :** Préconisation CNIL de **1 an**.
- **Protection :** Les bases de logs doivent être hautement sécurisées.

1. **La portabilité des données correspond :**
   - ☐ à l'utilisation de formats standards de stockage des données pour faciliter l'échange avec des tiers
   - ☒ à l'obligation pour tout détenteur de données à caractère personnel de les fournir à leur propriétaire légitime
   - ☐ aux travaux de vérification et regroupement des données administratives...
   - ☐ à l'obligation pour tout détenteur de données à caractère personnel de les fournir aux autorités...
2. **Des données personnelles stockées par un utilisateur professionnel :**
   - ☐ Peuvent être mises à disposition de la CNIL pour garantir la sécurité et la qualité.
   - ☐ Sont fournies uniquement à l'entreprise après que le salarié en ait fait la demande.
   - ☐ Doivent avoir été modifiées pour permettre à la CNIL de consulter le contenu.
   - ☒ Peuvent être anonymisées pour garantir une meilleure sécurité des informations du collaborateur.
3. **La notification d'une atteinte aux données personnelles :**
   - ☐ Est obligatoire à l'entreprise au-delà de 251 personnes.
   - ☐ Est déposée auprès de la préfecture.
   - ☒ Se fait à la CNIL dans un délai de 72 heures après la découverte de l'incident.
   - ☒ Aux personnes concernées si l'incident a un impact sur la vie privée (risque élevé).
4. **En cas d'atteinte à la sécurité des données à caractère personnel :**
   - ☐ Seul le fondateur d'entreprise est responsable.
   - ☐ Seule l'entité ayant collecté les données en question est responsable.
   - ☒ Tous les maillons de la chaîne de traitement peuvent être responsables.
   - ☐ Les sous-traitants ne sont jamais responsables.
5. **Une entreprise conforme au RGPD fait (entre autres) :**
   - ☒ Tient à jour un registre des traitements de DCP qu'elle é
   - ☒ Tient à jour un registre des traitements qu'elle fait traite par des sous-traitants.
   - ☒ Tient à jour un registre des incidents sur les DCP dont el est responsable.
   - ☐ Tient à jour la déclaration de traitements auprès de la CNIL (N'existe plus !).
6. **La notification à la CNIL d'un incident sur des DCP :**
   - ☒ Doit être faite dans les 72 heures après l'incident (ou sa détection).
   - ☐ Doit être faite dans les 6 heures après la détection.
   - ☐ Ne doit pas être faite de façon progressive.
   - ☐ Entraîne automatiquement une amende.

PwC

1. Écosystème Industriel : IT, OT, IoT & IIoT

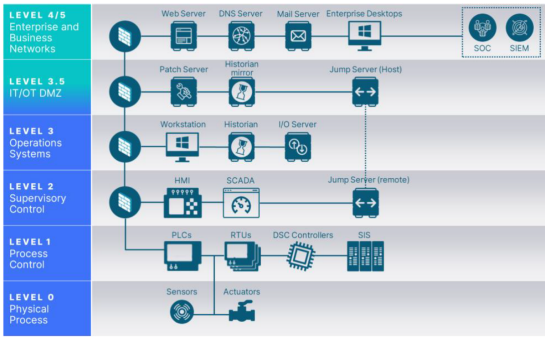
Définitions & Convergence

- **IT (Information Technology)** : Gestion de l'information, SI entreprise (ERP, Mail, RH). Priorité : **C** (Confidentialité) > I(Integrité) > A (Disponibilité).
- **OT (Operational Technology)** : Pilotage process physiques (vannes, moteurs, automates). Priorité : **A** > I > C.
- **IoT (Internet of Things)** : Objets connectés via Internet (tablettes, caméras, montres).
- **IIoT (Industrial IoT)** : Capteurs maintenance prédictive, robots autonomes en usine.
- **Convergence IT/OT** : Analyse de performance (conso thermique/élec), croisement données terrain (batch de fab) avec gestion (stocks).

2. Architecture de Référence : Le Modèle PURDUE

Division structurée des réseaux industriels en couches :

- **Layer 4/5 (Enterprise)** : Web, DNS, Mail, Desktops.
- **Layer 3.5 (DMZ IT/OT)** : Zone tampon de sécurité.
- **Layer 3 (Operations Systems)** : SOC, SIEM, Patch Server, Historian.
- **Layer 2 (Supervisory Control)** : SCADA(Système d'acquisition et de supervision globale), HMI (Human Machine Interface), Workstations.
- **Layer 1 (Process Control)** : PLC (Automates), RTU, SIS (Sécurité), Contrôleurs DCS.
- **Layer 0 (Physical Process)** : Capteurs (température, pression), Actionneurs (vannes, moteurs).



3. Analyse de Risques : Concepts & Statistiques

Définitions ISO 27005

- **Danger** : Propriété intrinsèque risquée (ex : acide sulfurique, défaut isolation).
- **Risque** : Éventualité de rencontre avec le danger (*Probabilite* × *Consequence*).
- **Dommage** : Préjudice subi (fracture, décès, pollution).
- **Menace** : Acteur (intentionnel ou non) cherchant à compromettre le bien.
- **Vulnérabilité** : Faiblesse de conception/usage (ex : absence de MFA).
- **Risque cyber** : evenement qui pourrait impacter la CIA(conf, int, dispo). **RISQUE = VULNÉRABILITÉ × MENACE**.

Panorama de la Menace

- **Secteur le plus touché** : manufacturing (25.7%), finance and insurance (18.2%), profesional and business consumer service (15.4%), energy (10.7%), healthcare (6.3%), goverment (4.3%), transport (4.3%), education (2.8%), media/telecom (1.2%)
- **Statistique critique** : 70% des organisations industrielles victimes de cyberattaques en 2023.

4. Études de Cas Réels & Retours d'Expérience

- **Colonial Pipeline (2021)** : Attaque **IT** via mot de passe VPN compromis (sans MFA) sur le dark web. Conséquence : Arrêt de 45% du carburant Côte Est USA, rançon de 4,4M$.
- **Oldsmar Floride (2021)** : Attaque directe **OT** via TeamViewer. Tentative d'empoisonnement (Hydroxyde de sodium passé de 100 à 11 100 ppm). Stoppé manuellement par un technicien.
- **Pierre Fabre (2021)** : Ransomware REvil. Secteur Pharma. Impact : Arrêt production 4 semaines, fermeture entrepôts 2 semaines.
- **Hôpital Corbeil-Essonnes (2022)** : Ransomware paralysant les urgences et dossiers. Conséquence : Décès d'une patiente lors d'un transfert.

5. Méthodologie EBIOS RM (ANSSI)

Méthode en 5 ateliers pour l'appréciation et le traitement des risques :

Atelier 1 : Cadrage & Événements Redoutés

- Définition du périmètre, interconnexions et biens critiques.
- Identification des événements et des impacts (Financier, Image, Juridique, **Sécurité des personnes**), définir le socle de sécurité.
- Gravité notée de **1 (Peu grave)** à **4 (Très grave)**.

Atelier 2 : Sources de Risques (SR) & Objectifs Visés (OV)

- **Typologies** : États (espionnage), Concurrents (perte d'activité), Crime organisé (profit), Insiders (vengeance), Hacktivistes (idéologie), Amateurs (challenge).
- **Matrice de pertinence** : Croisement entre **Motivation** et **Ressources** (Faible, Moyen, Élevé).

Atelier 3 : Scénarios Stratégiques/haut niveau

- Cartographie des parties prenantes (Écosystème).
- Évaluation de la dangerosité : Dépendance, Pénétration, Maturité, Confiance.

— Zones de surveillance : Danger, Control, Watch, Out of Scope.

Atelier 4 : Scénarios Opérationnels

— Graphes d'attaque en 4 étapes : **CONNAÎTRE** (dark-web) → **RENTRER** (Rogue Access Point) → **TROUVER** (Scan réseau) → **EXPLOITER** (Malware).

— Probabilité globale notée de **P1 (Peu probable)** à **P4 (Quasi certain)**.

Atelier 5 : Stratégie de Traitement

— Synthèse Gravité (A1) vs Vraisemblance (A4).

— **Décisions** : Faible (Acceptable), Moyen (Tolerable sous contrôle), Élevé (**Inacceptable**, mesures immédiates).

6. Mythes vs Réalités en Cyber Industrie

— **Mythe 1** : "Isolation d'Internet suffit". **Réalité** : Maintenance VPN et liens IT sont omniprésents.

— **Mythe 2** : "Un firewall par couche protège tout". **Réalité** : Inefficace contre compromission interne ou USB.

— **Mythe 3** : "Système trop complexe pour être attaqué". **Réalité** : Simulateurs OT et outils open-source disponibles pour les attaquants.

— **Mythe 4** : "Une attaque n'a jamais tué personne". **Réalité** : les attaques sur les hopitaux.

7. Hygiène & Bonnes Pratiques (ANSSI/PwC)

Mesures de Mitigation

— **Inventaire** : Maintenir une liste exhaustive des appareils connectés.

— **Segmentation** : Isoler logiquement/physiquement IT, OT et Internet (VLAN, Zones & Conduits).

— **Sécurité Physique** : Badges, barrières, blocage ports USB, restriction supports amovibles.

— **Accès Stricts** : Moindre privilège, **MFA** (Authentification forte), gestion rigoureuse des comptes admin.

— **Défense en Profondeur** : sécu physique > Politiques et procédures > zone et conduits > malware prevention > access controls > monitoring/détection patching.

— **Sensibilisation** : Former sur les spécificités OT (cycles de vie longs, contraintes de sûreté physique).

Règles d'Hygiène ANSSI Clés

— **Règle n°4** : Identifier serveurs sensibles et schéma réseau.

— **Règle n°5** : Inventaire exhaustif des comptes privilégiés.

— **Règle n°13** : Systématiser l'authentification forte.

— **Règle n°15** : Protection contre les supports amovibles.

— **Règle n°16** : Tests de sécurité réguliers.

quizz :

1. Vous travaillez dans un laboratoire de chimie. Il y a une bouteille d'acide sulfurique concentré sur une étagère. **Danger**
2. Un employé renverse accidentellement la bouteille d'acide sulfurique et se brûle la main. **Dommage**
3. Vous remarquez que l'étagère où est posée la bouteille d'acide sulfurique est instable et pourrait tomber à tout moment. **Risque**

Loi de programmation militaire

1. Contexte : Ecosystème Spatial & CNES

Le CNES (Centre National d'Études Spatiales)

- **Missions :** Proposer et mettre en œuvre la politique spatiale (Civile & Militaire).
- **4 Centres :** Siège (Paris), Daumesnil (Paris), CST (Toulouse - 1740 pers), CSG (Guyane - Port spatial).
- **Priorités Stratégiques :**
  1. Renforcer l'autonomie stratégique (Accès espace, Défense).
  2. Soutenir la compétitivité (Innovation, NewSpace).
  3. Monde durable (Climat, Débris).
  4. Excellence scientifique.

Poids du Spatial Français

- **Budget :** 3 Mds € (2ème puissance mondiale par habitant après USA).
- **Emploi :** +17 000 pers. (Industrie + Académique).
- **Industrie :** 90% PME/ETI. Leader européen.

2. Cadre Législatif : Loi de Programmation Militaire (LPM)

Organisation Institutionnelle

- **Premier Ministre (PM) :** Autorité suprême en matière de défense/sécurité.
- **SGDSN :** Secrétariat Général de la Défense et de la Sécurité Nationale.
- **ANSSI :** Agence Nationale de la Sécurité des Systèmes d'Information (Bras armé opérationnel).

Évolution de la LPM

- **LPM 2014-2019 (Loi 2013-1168, Art. 22) :**
  - Introduction du statut **OIV** (Opérateur d'Importance Vitale).
  - Obligation de protection des SI critiques.
  - Approche "Conformité" (Disponibilité/Intégrité > Confidentialité).
- **LPM 2019-2025 (Loi 2018-607, Art. 34) :**
  - Renforcement de la détection.
  - Implication des **OCE** (Opérateurs de Com. Électroniques) et hébergeurs.
  - Sondes de détection ANSSI chez les prestataires critiques.

3. Dispositif SAIV (Secteurs d'Activités d'Importance Vitale)

Définitions Clés

- **SAIV :** 12 secteurs vitaux (arrêtés sectoriels).
  - *Régalien :* État, Justice, Armées.
  - *Humain :* Santé, Eau, Alimentation.
  - *Économique :* Énergie, Finance, Transport.
  - *Technologique :* Com. élec, Industrie, **Espace**.
- **OIV (Opérateur d'Importance Vitale) :**
  - Désigné par le Ministre coordonnateur.
  - Critère : Le dysfonctionnement menace le potentiel de guerre, l'économie ou la survie de la Nation.
  - Notification confidentielle (Secret Défense).
- **SIIV (SI d'Importance Vitale) :** Systèmes critiques de l'OIV.

4. Obligations des OIV (LPM)

Le dispositif repose sur 4 piliers majeurs pour les OIV :

1. Identification & Déclaration

- L'OIV doit identifier ses SIIV (avec les métiers).
- Déclaration obligatoire à l'ANSSI.

2. Protection (Règles de Sécurité)

- Application des règles fixées par **Arrêté Sectoriel**.
- 20 règles types (Physique, Logique, Organisationnel).
- Objectif final : **Homologation** du SIIV (souvent max 3 ans).

3. Notification d'Incidents

- Obligation de signaler **sans délai** à l'ANSSI tout incident grave impactant un SIIV.
- Permet la corrélation nationale des attaques.

4. Contrôle (Audit)

- Vérification par l'ANSSI ou des prestataires qualifiés (**PASSI**).
- Sanctions pénales : 150 k€ (Dirigeant), 750 k€ (Personne morale) si non-respect.

5. Cadre Européen : Directive NIS

NIS 1 (2016 → 2018)

- Objectif : Niveau de sécurité commun dans l'UE.
- Création du statut **OSE** (Opérateurs de Services Essentiels).
- Différence OIV/OSE : OIV = Survie de la Nation / OSE = Fonctionnement Économie & Société.
- Coopération européenne (CSIRT Network).

NIS 2 (2024)

- **Changement d'échelle :** Passage de 300 à ∼15 000 entités en France.
- **Périmètre :** 18 secteurs (Ajout : Gestion déchets, Eaux usées, Espace, Admin publique...).
- **Typologie Entités :**
  - **Essentielles (EE) :** Grandes entreprises secteurs critiques. Contrôle *ex-ante* (régulier).
  - **Importantes (EI) :** PME/ETI ou secteurs périphériques. Contrôle *ex-post* (sur incident).
- **Nouveautés :** Sécurité de la Supply Chain, Cyber-hygiène, Responsabilité du Top Management.
- **Sanctions :** Indexées sur le CA mondial (jusqu'à 2% ou 10M€).

6. Mise en Œuvre Opérationnelle

Processus de Conformité SIIV

1. **Cadrage :** Définition périmètre (Métier + SSI).
2. **Gap Analysis :** Écart entre existant et Règles (Arrêté).
3. **Plan de transformation :** Budget (CAPEX/OPEX), Roadmap.
4. **Homologation :** Validation des risques résiduels par une commission.

Gouvernance SSI (4 axes)

- **Gouvernance :** Stratégie, Analyse de risques (EBIOS), Politiques.
- **Protection :** Durcissement, Chiffrement, IAM, Cloisonnement.
- **Défense :** Détection (SOC, PDIS), Réaction (CSIRT).
- **Résilience :** PCA/PRA (Continuité/Reprise), Gestion de crise.

Labels et Qualifications ANSSI

- **PASSI :** Audit.
- **PDIS :** Détection (Sondes).
- **PRIS :** Réponse à incident.
- **SecNumCloud :** Cloud de confiance.

LPM : Synthèse OIV & Cybersécurité (Loi de Programmation Militaire)

1. Calendrier de Mise en Conformité

Délais déclenchés à partir de la publication de l'arrêté sectoriel (T0) :

- **T0** : Notification OIV et publication de l'arrêté.
- **T0 + 3 mois** : Déclaration des Systèmes d'Information d'Importance Vitale (SIIV).
- **T0 + 12 mois** : Application des premières règles (les plus critiques).
- **T0 + 24 à 36 mois** : Conformité totale (dernières règles complexes).

2. Gouvernance (R1)

PSSI (Politique de Sécurité des SI) :

- Obligatoire, doit couvrir les spécificités OIV.
- Contenu : Stratégie, organisation, rôles/responsabilités, plan de sensibilisation/formation.
- **Cycle de vie** : Approuvée, communiquée, reporting annuel.

Homologation de Sécurité :

- **Définition** : Décision formelle de l'autorité qualifiée acceptant les risques résiduels.
- **Durée** : Maximum **5 ans** (ou révision si évolution majeure).
- **Pré-requis** : Analyse de risques (EBIOS), audit (PASSI), conformité réglementaire.
- **Formes** : Simplifiée (déclaration), Intermédiaire, ou Complète (audit approfondi) selon la criticité.

3. Maîtrise des Risques & Cartographie (R3)

Analyse de risques :

- Couverture du cycle de vie complet (Conception → Opérations → Fin de vie).
- Prise en compte de la *Supply Chain* et des tiers.

Cartographie (R3) :

- **Objectif** : Indispensable pour la réaction aux incidents et l'attribution des signalements.
- **Niveaux requis** :
  - *Métier* : Écosystème, acteurs, flux fonctionnels.
  - *Applicatif* : Applications, protocoles, flux d'admin.
  - *Infrastructure* : Physique (bâtiments, câbles) et Logique (réseaux, VLANs).
- Doit être maintenue à jour et communicable à l'ANSSI.

4. Maintien en Condition de Sécurité (MCS - R4 & R20)

Gestion des vulnérabilités :

- Veille active (CERT, éditeurs).
- Application des correctifs de sécurité obligatoire.
- Si impossibilité technique → Justification + mesures compensatoires.

Indicateurs (R20) :

- Communication annuelle à l'ANSSI.
- Ex : % de systèmes obsolètes, % de comptes sans rotation de mot de passe, usage de comptes génériques.

5. Détection & Gestion des Incidents

Journalisation (R5) :

- **Rétention** : Au moins **6 mois**.
- Périmètre : Serveurs, équipements sécurité, postes admin.
- Exigences : Centralisation, intégrité, horodatage synchronisé.

Corrélation & Analyse (R6) :

- Usage d'un SIEM pour détecter les scénarios d'attaque.
- Référence : **PDIS** (Prestataires de Détection d'Incidents de Sécurité).
- Distinction : Événement (neutre) vs Alerte (suspect) vs Incident (avéré).

Détection (R7) :

- Sondes qualifiées (analyse fichiers/protocoles).
- Positionnement stratégique (interconnexions SIIV/Tiers).

Traitement des Incidents (R8) :

- Procédure formelle requise.
- Référence : **PRIS** (Prestataires de Réponse aux Incidents de Sécurité).
- Infrastructure dédiée et cloisonnée pour l'analyse (stockage preuves 6 mois).

Alertes & Crise (R9 & R10) :

- **R9** : Point de contact H24/7J (ou astreinte) pour recevoir les alertes ANSSI.
- **R10** : Gestion de crise. Capacité à appliquer des mesures d'urgence (isolement réseau, blocage USB, arrêt production).

6. Architecture du SOC (Security Operations Center)

- **Missions** : Prévenir, Détecter, Réagir, Administrer.
- **Organisation** : N1 (Tri/Alertes), N2 (Analyse), N3 (Expertise/-Crise).
- **Outils** : SIEM, Sondes, Threat Intel, Ticketing.
- **Défis** : Minimiser les Faux Positifs et Faux Négatifs.

7. Défense en Profondeur (Mesures Techniques)

Approche globale : Organisation + Technique + Physique.

Gestion des Accès (R11, R12, R13) :

- **Identification** : Comptes nominatifs obligatoires. Comptes partagés interdits (sauf exception justifiée).
- **Authentification** : Mots de passe robustes, changement périodique, pas de défaut constructeur.
- **Droits** : Principe du moindre privilège (Juste besoin). Revue régulière.

Administration (R14, R15) :

- **Comptes dédiés** : Interdiction d'administrer avec un compte utilisateur standard.
- **Postes dédiés** : Pas d'usage bureautique, **pas d'accès Internet direct**.
- **Flux** : Réseau d'administration cloisonné (physique ou chiffré).

Réseau & Cloisonnement (R16, R17) :

- **Cloisonnement** : Séparation des zones de confiance. VLAN insuffisant → Chiffrement requis si logique.
- **Filtrage** : Strict (flux entrants et sortants), granularité fine.

Accès Distants (R18) :

- **Moyens** : VPN IPsec (certifié) ou TLS.
- **Sécurité** : Authentification forte (MFA) obligatoire.
- **Poste** : Maîtrisé par l'entité (Pas de BYOD), disque chiffré.

Durcissement (R19) :

- Principe de minimisation : Seuls les services indispensables sont installés.
- Supports amovibles (USB) : Interdits par défaut ou liste blanche + station de décontamination (blanchiment).

Récapitulatif des Acronymes Clés

- **ANSSI** : Agence Nationale de la Sécurité des Systèmes d'Information.
- **OIV** : Opérateur d'Importance Vitale.
- **SIIV** : Système d'Information d'Importance Vitale.
- **PASSI** : Prestataire d'Audit de la Sécurité des SI (Qualifié).
- **PDIS** : Prestataire de Détection d'Incidents de Sécurité.
- **PRIS** : Prestataire de Réponse aux Incidents de Sécurité.

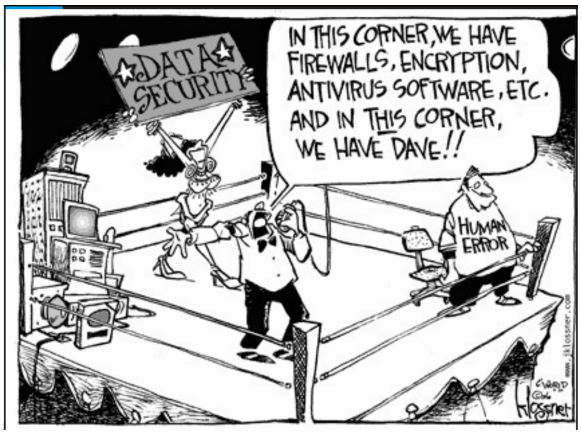
Ingéniererie sociale - Ladislas Hajnal

1. Ingénierie Sociale (IS) : Définitions & Enjeux

Contextes disciplinaires

- **Science Po.** : Pratique de modification comportementale de groupes sociaux à grande échelle.
- **Sécurité Info. (SSI)** :obtenir par manipulation mentale une information confidentielle.
- **Psychologie** : techniques de manipulation psychologique afin d'aider ou nuire à autrui
- **Synthèse** : Modification **planifiée** du comportement humain.
- **def SSI** Ensemble des techniques de manipulation psychologique visant à amoindrir, contourner ou supp les mesures de sécurité. A l'insu de la personne ciblée

Importance en Cyber Historiquement focus sur machines, mais l'humain reste le maillon faible. *"Seuls les amateurs s'attaquent aux machines, les professionnels prennent les hommes pour cible"* (B. Schneier). L'IS exploite les **failles cognitives** là où les outils techniques échouent.



2. Fondements Psychologiques & Nature Humaine

Attribution causale (Heider) L'humain agit en **scientifique naïf** :

- **Besoin de maîtrise** : Recherche systématique de cohérence entre les éléments cognitifs (attribution causale).
- **Inférences subjectives** : Causes **internes** (motivation/capacité) vs **externes** (environnement). Le choix des causes dépend su sujet cible (**hétéro-attribution**=recherche des causes dans le comportement d'autrui / **auto-attribution**=son propre comportement) + statut social du sujet-cible + relations entre les groupes de cible/sujet
- **Biais d'auto-attribution** : Succès = interne ; Échec = externe.

Psychologie Évolutionniste Comportements hérités de la séléction naturelle :

- **Coopération** : Besoin vital de contacts sociaux et soutien du groupe.(Dunbar 1998)
- **Compétition** : Stratégies de survie favorisant les meilleurs stratèges(Hauser 1996).
- **Filtre Cognitif** : Tri info pour éviter la paralysie cognitive. Critères : **Contexte** et **Contenu transmis**

3. Systèmes Cognitifs : Dual Process (Kahneman/Tversky)

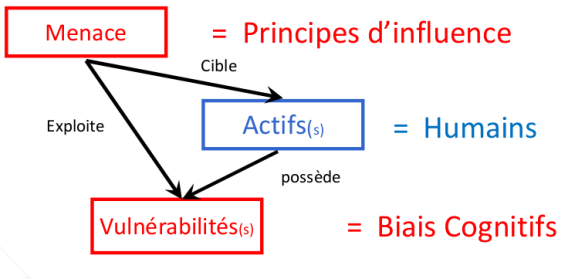
L'humain ne peux pas traiter consciemment toutes les informations qu'il reçoit : 2 proc mentaux (si mention du jeu monty hall, faut changer de porte jsp pq y'a ça dans le cours)

- **Système 1 (Auto)** : Rapide, intuitif, émotionnel, inconscient, peu d'effort. **Pilote par défaut**.
- **Système 2 (Réfléchi)** : Lent, logique, conscient, gourmand en énergie, calculatoire.
- **Mécanisme IS** : Maintenir la victime en **Système 1** via le stress, l'urgence ou l'émotion pour court-circuiter l'analyse critique du Système 2.

4. Failles Humaines & Biais Cognitifs (Catalogue)

- **Nous sommes des êtres de comparaison plutôt que de raison** : Influence démesurée de la 1ère info reçue (ex : prix initial barré).
- **Cadrage/Saillance/encrage** : Une info attirante (clickbait) occulte le reste. (1x2x...x7x8 vs 8x7x...x2x1)
- **Familiarité** : Préférence pour ce qu'on connaît (usage de jargon/argot cible).
- **Aversion à la perte** : On craint plus de perdre 10€ qu'on ne désire en gagner 20.
- **Effet IKEA** : Sur-affection pour ce qu'on a fabriqué/-possède.
- **Biais de confirmation** : Tendance à ne valider que les infos confortant nos opinions.
- **Attentes/Perception** : Nos préjugés modifient nos sens (ex : dégustation vin truquée).
- **Biais du présent** : Préférence pour un gain immédiat faible vs futur élevé.
- **Effet de causalité** : La simple justification (utiliser "parce que") augmente l'acceptation.
- **Effet Barnum (Forer)** : Accepter des descriptions vagues comme spécifiques à soi (horoscope, profils psy).
- **Effet FREE** : Une offre gratuite est irrésistible, même si elle impose des contraintes cachées.
- **Victime Identifiable** : L'émotion pour un individu l'emporte sur les statistiques de masse.

Influences psychologiques : influences explicites et acceptées / influences décelables



5. Engagement & Dissonance Cognitive

Besoin de Cohérence L'humain déteste la contradiction interne.

- **Dissonance (Festinger)** : Tension entre croyance et acte. On modifie l'opinion pour justifier l'acte (ex : justifier une tâche ennuyeuse pour 1$ vs 20$).
- **Pied dans la porte** : Obtenir un petit "OUI" insignifiant pour amorcer un engagement forçant des "OUI" plus coûteux ensuite.

6. Les 8 Leviers d'Influence Majeurs (Cialdini)

- **1. Réciprocité** : Obligation sociale de rendre un service (cadeaux "gratuits"). L'humain valorise l'égalité
- **2. Autorité** : Soumission naturelle aux symboles de pouvoir/personnes influentes (Milgram : 65% d'obéissance aux chocs électriques).
- **3. Rareté** : Ce qui est limité a plus de valeur (urgence artificielle, stocks limités).
- **4. Engagement/Cohérence** : Une fois positionné, on s'y tient par pression sociale.
- **5. Sympathie** : On dit "OUI" à ceux qu'on apprécie (similitude, compliments).
- **6. Preuve Sociale** : Imiter le comportement d'autrui en cas d'incertitude (effet témoin).
- **7. Unité/Familiarité** : Sentiment d'appartenance (famille, groupe, nation).
- **8. Contraste** : Comparaison entre deux options pour faire paraître la 2nde dérisoire.

Pour éviter la mort de 5 personnes sur une voie : les gens acceptent de dévier le train par un levier, mais refusent de pousser physiquement un homme vers la mort.

Par respect de l'autorité, l'humain peut commettre des atrocités.

HORS DES COURS - GEMINI QUI RAJOUTE SA PETITE TOUCHE MAIS RESTE UTILE SI IL FAUT

7. Mécanisme de l'Attaque en IS

Cycle de l'exploitation **Source de menace** exploite des **Vulnérabilités** (Biais/Failles) possédées par la **Cible** pour atteindre ses **Actifs**.

Techniques courantes

- **Phishing/Spear-phishing** : Hameçonnage (générique vs ciblé).
- **Vishing/Smishing** : Via téléphone ou SMS.
- **Pretexting** : Création d'un scénario élaboré (faux technicien, audit).
- **OSINT** : Collecte info publique (réseaux sociaux) pour crédibiliser l'attaque.

8. Protections & Recommandations

- **Sensibilisation** : Comprendre que "l'erreur est humaine" mais évitable par la connaissance des biais.
- **Verification** : Sortir du Système 1. Toujours vérifier l'identité via un canal alternatif.
- **Hygiène SI** : Ne pas utiliser de supports inconnus, rapporter les mails suspects, gérer sa trace numérique.

autre

Milgram : L'expérience de Milgram démontre que des individus ordinaires peuvent infliger des souffrances à autrui par simple obéissance à une autorité jugée légitime. **Photocopieuse :** Si quelqu'un te passe devant à la photocopieuse et qu'il se justifie genre "je suis prof".

SSI RGPD - Gillou (Trouessin)

Timeline Légale et Évolutions

- **6 janv. 1978 :** Loi Informatique et Libertés (I&L) + création de la **CNIL**.
- **24 oct. 1995 :** Directive européenne de protection des données.
- **21 juin 2004 :** Loi **LCEN** (Confiance dans l'Économie Numérique).
- **6 août 2004 :** Transposition de la directive 1995 en droit français.
- **14 mars 2011 :** Loi **LOPPSI 2** (Sécurité intérieure).
- **27 avril 2016 :** Adoption officielle du **RGPD**.
- **25 mai 2018 :** Entrée en application du RGPD (responsabilisation).
- **20 juin 2018 :** Mise à jour de la loi I&L française.
- **2023 :** Loi de Programmation Militaire (**LPM**) : signalement vulnérabilités.
- **11 sept. 2026 :** Début obligation signalement vulnérabilités (**CRA**).
- **11 déc. 2027 :** Entrée en vigueur totale du **Cyber Resilience Act**.

1. Concepts Fondamentaux : SSI & Patrimoine Informationnel

Données, Information & Valeur

- **Donnée** : Élément brut (caractère, bit). **Information** : Donnée interprétée avec un sens. **Connaissance** : Information intégrée pour l'action.
- **Patrimoine immatériel** : Capital intellectuel, savoir-faire, données clients. C'est l'actif le plus critique de l'organisation.
- **Objectifs de la SSI (DICP)** :
  - **Disponibilité** : Accessibilité au moment voulu.
  - **Intégrité** : Non-modification accidentelle ou malveillante.
  - **Confidentialité** : Accès restreint aux seules personnes autorisées.
  - **Preuve / Non-répudiation** : Impossibilité de nier une transaction ou une action.
- **Vulnérabilité vs Menace** : Une faiblesse (vulnérabilité) exploitée par un événement redouté (menace) génère un **Impact**.

2. RGPD : Cadre Juridique & Champ d'Application

Définitions Clés

- **Donnée à Caractère Personnel (DCP)** : Toute info identifiant directement (nom) ou indirectement (n° sécu, IP, empreinte, ID) une personne physique.
- **Traitement** : Opération sur DCP (collecte, enregistrement, stockage, modification, suppression).
- **RGPD** : Règlement (UE) 2016/679 entré en application le **25 mai 2018**.
- **Champ territorial** : S'applique si le RT/ST est en UE, OU si le traitement concerne des résidents UE (offre de biens/services ou profilage).

Acteurs du Traitement

- **Responsable de Traitement (RT)** : Détermine les finalités et les moyens du traitement.
- **Sous-traitant (ST)** : Traite les données pour le compte du RT (ex : hébergeur cloud).
- **Délégué à la Protection des Données (DPO)** : Pilote la conformité, conseille le RT et fait l'interface avec la CNIL.
- **CNIL** : Autorité de contrôle française (contrôle, sanctionne, conseille).

3. Les 6 Principes Fondamentaux du RGPD

- **1. Licéité, Loyauté, Transparence** : Base légale obligatoire (consentement, contrat, intérêt légitime, etc.) et info claire des personnes.
- **2. Limitation des finalités** : Données collectées pour un but déterminé, explicite et légitime. Interdiction de réutilisation incompatible.
- **3. Minimisation des données** : Collecter uniquement ce qui est adéquat et strictement nécessaire (*"Need to know"*).
- **4. Exactitude** : Tenir les données à jour. Effacer ou rectifier les données inexactes sans délai.
- **5. Limitation de la conservation** : Durée proportionnée à la finalité. Archivage ou suppression après usage (sauf obligations légales).
- **6. Intégrité et Confidentialité** : Garantir la sécurité technique et organisationnelle contre le traitement non autorisé, la perte ou la destruction.

4. Droits des Personnes Concernées

L'organisation doit répondre aux demandes sous **1 mois** (prolongation possible de 2 mois) :

- **Droit d'accès** : Savoir si des données sont traitées et en obtenir copie.
- **Droit de rectification** : Corriger des données erronées.
- **Droit à l'effacement (Oubli)** : Supprimer les données (si non nécessaires/illégales).
- **Droit à la portabilité** : Récupérer ses données dans un format structuré/lisible par machine.
- **Droit d'opposition** : Refuser un traitement (ex : prospection commerciale).
- **Droit à la limitation** : Geler l'usage des données pendant une vérification.

5. Gouvernance & Accountability (Responsabilisation)

Le passage d'un régime de déclaration préalable à un régime de **preuve permanente** :

- **Registre des traitements** : Document obligatoire listant tous les processus utilisant des DCP (finalités, acteurs, catégories de données, transferts).
- **Privacy by Design** : Intégrer la protection des données dès la conception d'un projet.
- **Privacy by Default** : Garantir par défaut le plus haut niveau de protection (ex : options de profilage décochées).
- **AIPD / PIA** : Analyse d'Impact relative à la Protection des Données. Obligatoire pour les traitements à **haut risque** (santé, surveillance masse, profilage).
- **Gestion des Sous-traitants** : Contrats spécifiques imposant les obligations de sécurité du RT au ST.

6. Sécurité, Incidents & Sanctions

Obligations de Sécurité (Art. 32)

- **Mesures techniques** : Chiffrement, pseudonymisation, authentification forte (MFA), sauvegardes, tests d'intrusion réguliers.
- **Mesures organisationnelles** : Politiques (PSSI), sensibilisation, gestion des habilitations, clauses de confidentialité.

Gestion des Violations de Données

- **Notification CNIL** : Obligatoire sous **72 heures** si la violation présente un risque pour les droits et libertés.
- **Information des personnes** : Obligatoire sans délai si le risque est **élevé** (ex : vol de coordonnées bancaires en clair).

Sanctions Administratives (CNIL)

- **Niveau 1** : Jusqu'à 10 M€ ou 2% du CA mondial annuel.
- **Niveau 2** : Jusqu'à **20 M€ ou 4% du CA mondial annuel** (la valeur la plus élevée est retenue).
- **Critères** : Gravité, durée, intentionnalité, coopération, mesures prises pour atténuer le dommage.

7. Synthèse pour l'Examen (QCM)

- **DCP vs Anonyme** : Si on peut réidentifier (même par recoupement), c'est une DCP.
- **Consentement** : Doit être libre, spécifique, éclairé et univoque (pas de case pré-cochée).
- **Transferts Hors UE** : Interdits sauf si pays "adéquat" ou garanties (BCR, clauses contractuelles types).
- **Données Sensibles (Art. 9)** : Origine raciale/ethnique, opinions po/religieuses, santé, vie sexuelle, biométrie. Traitement interdit par défaut (sauf exceptions : consentement explicite, intérêt public).

EUROCONTROL CERT - Patrick MANA

1. Contexte : Cybersécurité de l'Aviation et de l'ATM

Enjeux et Spécificités

- **ATM (Air Traffic Management)** : Infrastructure critique où la **Sûreté (Safety)** prime sur tout.
- **Évolution** : Passage de systèmes propriétaires isolés à des systèmes connectés, numériques et interopérables (IP, Cloud).
- **Complexité** : Écosystème vaste incluant compagnies, aéroports, constructeurs et fournisseurs de services de navigation aérienne (ANSP).
- **Impacts potentiels** : Perturbation du trafic, pertes économiques massives, atteintes à l'intégrité des données de vol.

2. Protocoles Aéronautiques et Vulnérabilités

Les protocoles historiques manquent de mécanismes de sécurité modernes (chiffrement, authentification) :

- **ADS-B (Automatic Dependent Surveillance-Broadcast)** : Transmission de position GPS en clair. Vulnérabilités : **Jamming** (brouillage) et **Spoofing** (injection de fausses cibles).
- **ACARS (Aircraft Communications Addressing and Reporting System)** : Messagerie texte sol-bord. Pas de chiffrement natif, risque d'interception et de manipulation.
- **CPDLC (Controller-Pilot Data Link Communications)** : Dialogue contrôleur/pilote via texte. Risque d'usurpation d'identité ou d'instructions malveillantes.
- **PENS (Pan-European Network Service)** : Réseau IP critique reliant les centres de contrôle européens, nécessitant une protection accrue.

3. Cadre Réglementaire : EASA Part-IS

Le nouveau standard de l'Agence Européenne de la Sécurité Aérienne (EASA) :

- **Objectif** : Imposer un **ISMS (Information Security Management System)** cohérent pour toute l'aviation.
- **Obligations** : Identification des actifs critiques, analyse de risques, détection d'incidents et notification obligatoire.
- **Homologation** : Les SI critiques doivent être certifiés conformes pour garantir la résilience opérationnelle.
- **Échéance** : Mise en œuvre progressive pour assurer la conformité d'ici 2025-2026.

4. EATM-CERT : Rôle et Missions

Le **European Air Traffic Management Computer Emergency Response Team** est le pivot de la défense sectorielle :

- **Gouvernance** : Opéré par Eurocontrol pour le compte de ses États membres.
- **Rôle** : Hub central de partage d'informations sur les menaces et de coordination de la réponse aux incidents.
- **Bénéficiaires** : ANSP, aéroports, compagnies aériennes et autorités de régulation.

5. Catalogue de Services du CERT

Divisé en trois piliers stratégiques (selon le standard FIRST) :

Services Réactifs (Réponse)

- **Gestion des incidents** : Triage, analyse technique et coordination du rétablissement.
- **Analyse Forensique** : Investigation post-mortem pour comprendre le mode opératoire de l'attaquant.
- **Gestion des vulnérabilités** : Aide au déploiement des correctifs critiques sur les systèmes ATM.

Services Proactifs (Anticipation)

- **Alertes et Bulletins** : Diffusion d'informations sur les nouvelles menaces ou failles.
- **Veille Technologique** : Surveillance du dark web et des groupes d'attaquants ciblant l'aviation.
- **Audits de sécurité** : Tests d'intrusion et scans de vulnérabilités sur les SIIV.

Sécurité & Qualité (Support)

- **Analyse de Risques** : Support méthodologique via EBIOS RM.
- **Sensibilisation** : Formations spécifiques pour les contrôleurs et techniciens OT.

6. Partage d'Information et Protocole TLP

Pour garantir la confiance lors des échanges, le **Traffic Light Protocol (TLP)** est utilisé :

- **TLP :RED** : Diffusion restreinte aux seules personnes présentes lors de la réunion.
- **TLP :AMBER** : Diffusion limitée à l'organisation et ses clients directs sur une base *need-to-know*.
- **TLP :GREEN** : Partage possible avec toute la communauté aéronautique/CERT.
- **TLP :CLEAR (ex-WHITE)** : Information publique, aucune restriction de partage.

7. Cycle de Vie d'un Incident au CERT

Processus structuré pour une gestion efficace :

- **Détection/Notification** : Réception de l'alerte par un partenaire ou via monitoring.
- **Triage** : Évaluation de la gravité (Impact opérationnel vs étendue de la brèche).
- **Analyse** : Caractérisation de la menace (Malware, intrusion, déni de service).
- **Endiguement** : Mesures d'urgence pour limiter la propagation (isolation réseau).

— **Éradication/Rétablissement** : Nettoyage des systèmes et retour à la normale.

— **Leçons apprises** : Rapport final pour améliorer les défenses futures.

8. GNSS RFIs

— **Bases du signal :** Calcul du PVT (Position, Vitesse, Temps) via mesures temporelles. Frequences civiles : 1575.42 MHz (L1) et 1176.45 MHz (L5).

— **Jamming (Brouillage) :** Déni de service par saturation de la bande avec du bruit RF. Une puissance de 0.1 à 1 W suffit à perturber la réception sur plusieurs kilomètres, forçant un repli sur les aides au sol.

— **Spoofing (Leurrage) :** Déception par transmission de signaux contrefaits (meaconing ou synthèse en temps réel). Permet de manipuler la position/le temps perçus sans nécessairement déclencher d'alertes.

9. Bonnes Pratiques pour la Résilience ATM

— **Défense en profondeur** : Multiplication des couches de sécurité (physique, réseau, applicatif).

— **Zonage (ISA 62443)** : Séparation stricte entre les réseaux entreprise (IT) et critiques (OT/ATM).

— **Authentification forte** : Utilisation du MFA pour tout accès distant ou privilégié.

— **Continuité d'activité** : Plans de secours dégradés pour maintenir le trafic sans radar ou sans CPDLC.

sur 3700 domains relatifs à l'aviation : DNSSEC presence 9%, **TLS presence** 88%, **Secure TLS version presence** 52%, **Secure TLS ciphers presence** 44%, **SPF strict policy presence** 87%, **DMARC strict policy presence** 24%, **DANE presence** 2%, **MTA-STS presence** 1%.

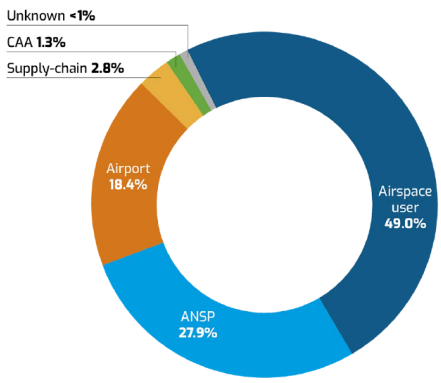


FIGURE 1 – Victim

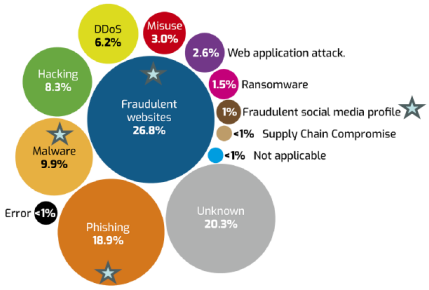


FIGURE 2 – comment ?

pourquoi ? principalement financier puis pour voler de la data

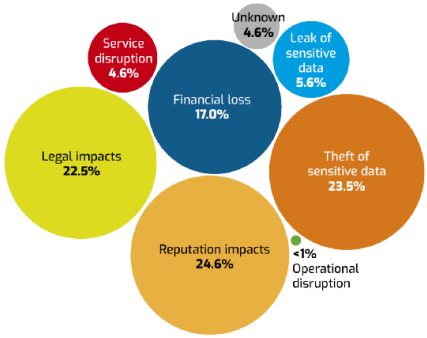


FIGURE 3 – Impact

les acteurs de ces attaques ? cybercriminels (52.3%) puis unknown (38.2%) puis hacktivist (6.2%)

— CERT (Computer Emergency Response Team) : Une unité d'experts chargée de centraliser, traiter et répondre aux incidents critiques de sécurité au niveau national ou sectoriel.

— CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information) : Un laboratoire agréé par l'ANSSI pour réaliser des audits techniques et évaluer la robustesse des produits de sécurité (en vue d'une certification).

— SOC (Security Operations Center) : Une plateforme opérationnelle qui assure la surveillance continue (24/7) des systèmes d'information pour détecter et analyser les menaces en temps réel.