

DOCUMENT DE RÉFÉRENCE

AUDIT COMPARATIF DES BUDGETS CYBERSÉCURITÉ

France vs Europe vs États-Unis vs Italie vs Japon

« 200 Millions d'Euros : Le Pansement sur l'Artère Coupée »

CONFIDENTIEL — USAGE INTERNE

Alexandre Kerbaol | alexk29@live.fr | 07 67 58 94 12
Quai Nicolas Fouquet, BP63, 56360 Le Palais, France
<https://architecture-du-reel.fr>

Édité par AkDevSystem — Mai 2026

AUDIT COMPARATIF DES BUDGETS CYBERSÉCURITÉ

France vs Europe vs États-Unis vs Italie vs Japon — 2022-2026

« 200 Millions d'Euros : Le Pansement sur l'Artère Coupée »

Pensée d'Alexandre Kerbaol

« Des milliards de pertes et on met le budget d'un Yacht de luxe pour faire du placo pour réparer un sous-marin nucléaire lanceur d'engins pour le remettre en service. »

— **Alexandre Kerbaol**

Document de réflexion stratégique Auteur : Alexandre Kerbaol | AkDevSystem **Date :** Mai 2026

Classification : CONFIDENTIEL — Usage interne strict

En quelques mots

En mai 2026, la France annonce le déblocage de **200 millions d'euros** pour la cybersécurité de l'État. Un chiffre qui fait les titres. Mais que représente-t-il vraiment face à la menace ? Cette étude compare notre effort avec celui de nos voisins : les États-Unis investissent **~25 milliards de dollars** par an, le Royaume-Uni **~2,1 milliards d'euros**, l'Allemagne **~750 millions d'euros**. La France, avec 200 millions (soit **~0,07 %** de son budget), est en queue de peloton. Au-delà des chiffres, nous avons analysé **les incidents majeurs** qui ont frappé la France entre 2024 et 2026 : 43 millions de profils France Travail exfiltrés, 33 millions de données santé compromises, le fichier national des comptes bancaires (FICOBA) piraté... Et nous avons examiné si le citoyen français dispose d'un recours. Ce document propose une **feuille de route concrète** : de l'authentification multifactorielle généralisée à la création d'une National Cyber Force, en passant par la transposition urgente de la directive NIS2 et la professionnalisation des équipes de l'ANSSI. **Pour qui ?** Les décideurs publics, les dirigeants d'entreprises, les citoyens concernés — et tous ceux qui se demandent si 200 millions suffisent à sécuriser un pays.

TABLE DES MATIÈRES

1. Introduction — Le constat d'un praticien
2. Le constat factuel — L'asymétrie budgétaire
3. La comparaison internationale
4. Les dépenses des entreprises
5. La structure institutionnelle
6. Les attaques sur sites stratégiques français
7. Le citoyen français peut-il porter plainte ?
8. Analyse critique — Pourquoi la France est en retard
9. Feuille de route recommandée
10. Recommandations stratégiques
11. L'espace et l'OTAN — Le domaine oublié
12. La cyberguerre énergétique en Europe
13. Les géants de la sécurité face à l'IA — Le cas Cloudflare
14. Conclusion — Le réalisme nécessaire Annexes — Sources, Méthodologie, Glossaire

1. INTRODUCTION — Le constat d'un praticien

Le 1er mai 2026, le Premier ministre français annonce le déblocage de **200 millions d'euros** pour la cybersécurité des ministères. La ministre concède elle-même que ce montant "*ne suffira pas*". Trois piratages par jour. Un État dépassé. Et un ministère de la cybersécurité ouvert en... **décembre 2025**.

Bienvenue dans le monde réel.

Problématique centrale : Pourquoi la France, 2ème pays le plus touché au monde par les fuites de données (Q1 2026), débloque-t-elle 200M€ quand ses voisins investissent des milliards ? Et surtout : est-ce que 200M€ suffisent quand le coût des cyberattaques dépasse 100 milliards d'euros par an ?

« Nous sommes dans le factuel des systèmes d'information actuels face au présent et à demain, en sachant que le présent est déjà le passé. »

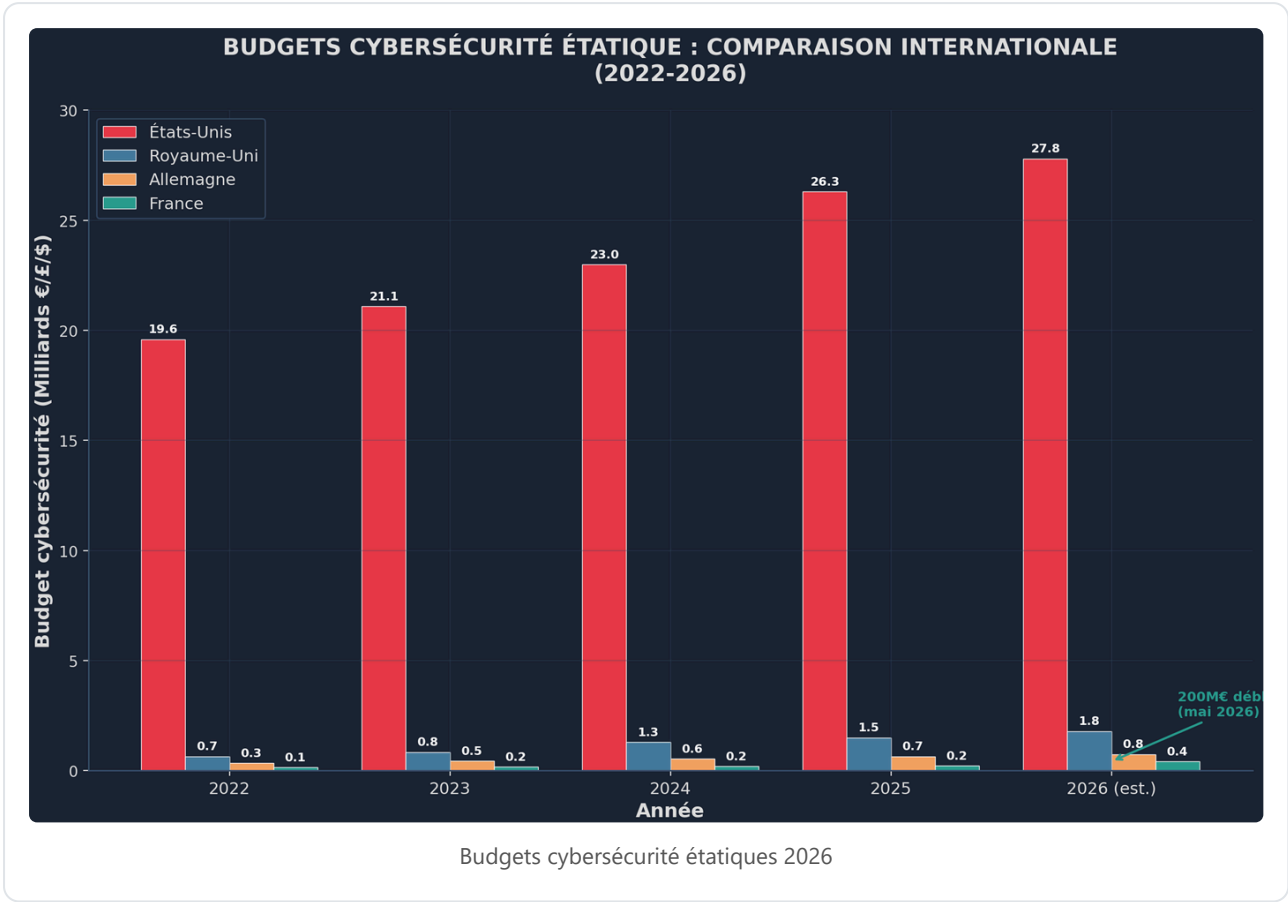
Métaphore de la puissance de feu

Mon logiciel de navigation utilise plus de 28 000 calculs par seconde pour le traitement AIS et CPA. Lors d'une course Mini 6.50, il a traité 105 cibles simultanées dans la rade de Lorient sur un PC de 2015 sans broncher.

Aujourd'hui, un adolescent de 15 ans exploite une faille IDOR (changer user_id=12345 en user_id=12346 dans l'URL) pour aspirer les données de **12 millions de Français** (ANTS, avril 2026). Le coût de l'attaque : **zéro euro**. Le coût pour l'État : **des millions en communication, en remédiation, en perte de confiance**.

Et pendant ce temps, un modem satellite mal patché permet au GRU russe de couper les communications d'une armée entière à l'aube d'une invasion. On en parle ? Non. On n'en parle pas.

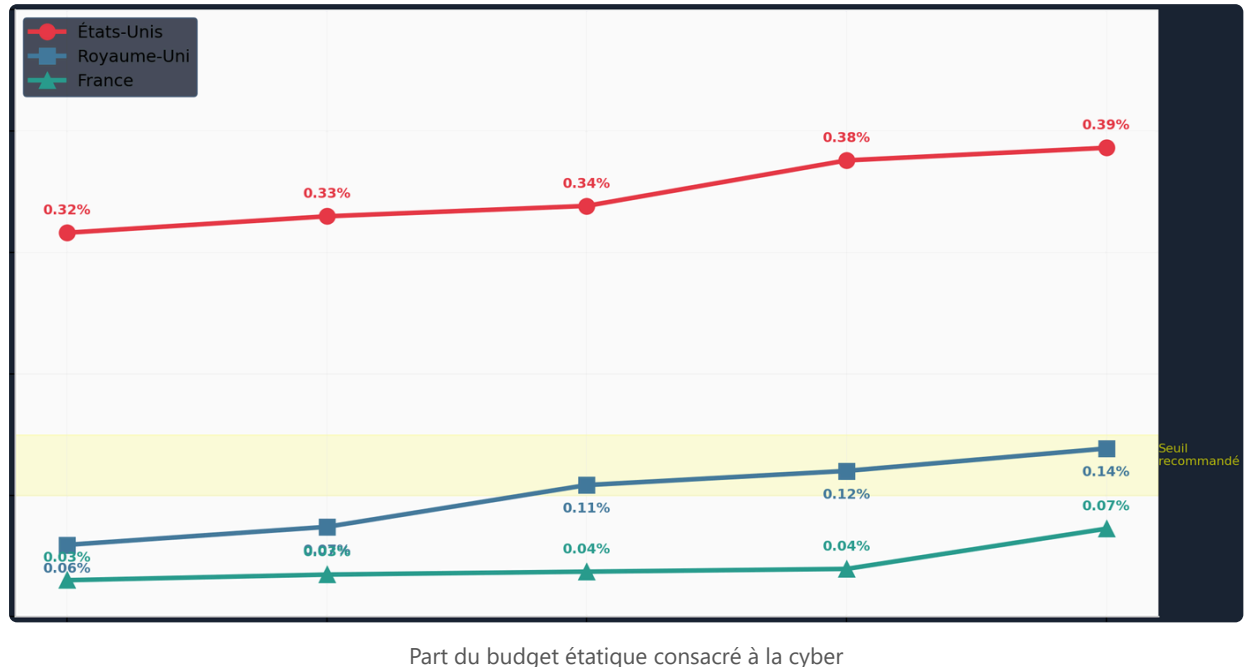
2. LE CONSTAT FACTUEL — L'asymétrie budgétaire



2.1 Les chiffres officiels : un gouffre qui s'élargit

INDICATEUR	USA	UK	ALLEMAGNE	ITALIE	JAPON	FRANCE
Budget État Cyber 2022	~19.6 Mds \$	~750 M€	~350 M€	~\$200M	~¥50B	~150 M€
Budget État Cyber 2023	~21.1 Mds \$	~980 M€	~450 M€	~\$250M	~¥60B	~180 M€
Budget État Cyber 2024	~23.0 Mds \$	~1.5 Mds €	~550 M€	~\$300M	~¥70B	~200 M€
Budget État Cyber 2025	~26.3 Mds \$	~1.7 Mds €	~650 M€	~\$350M	~¥80B	~220 M€
Budget 2026 (est.)	~27.8 Mds \$	~2.1 Mds €	~750 M€	~€400M	~¥90B	~420 M€
Budget / Habitant	~82 \$	~30 €	~9 €	~7 €	~12 €	~6 €
Part Budget État	~0.38%	~0.14%	~0.06%	~0.05%	~0.08%	~0.07%

Sources : OMB FY2025, DoD FY2026, UK Cabinet Office Spending Review 2025, BSI Germany, ACN Italy, NISC Japan, ANSSI France, RM3A Cybersecurity



La France (0,07%) est en dessous du seuil recommandé (0,10-0,15%). Les USA investissent 5x plus proportionnellement.

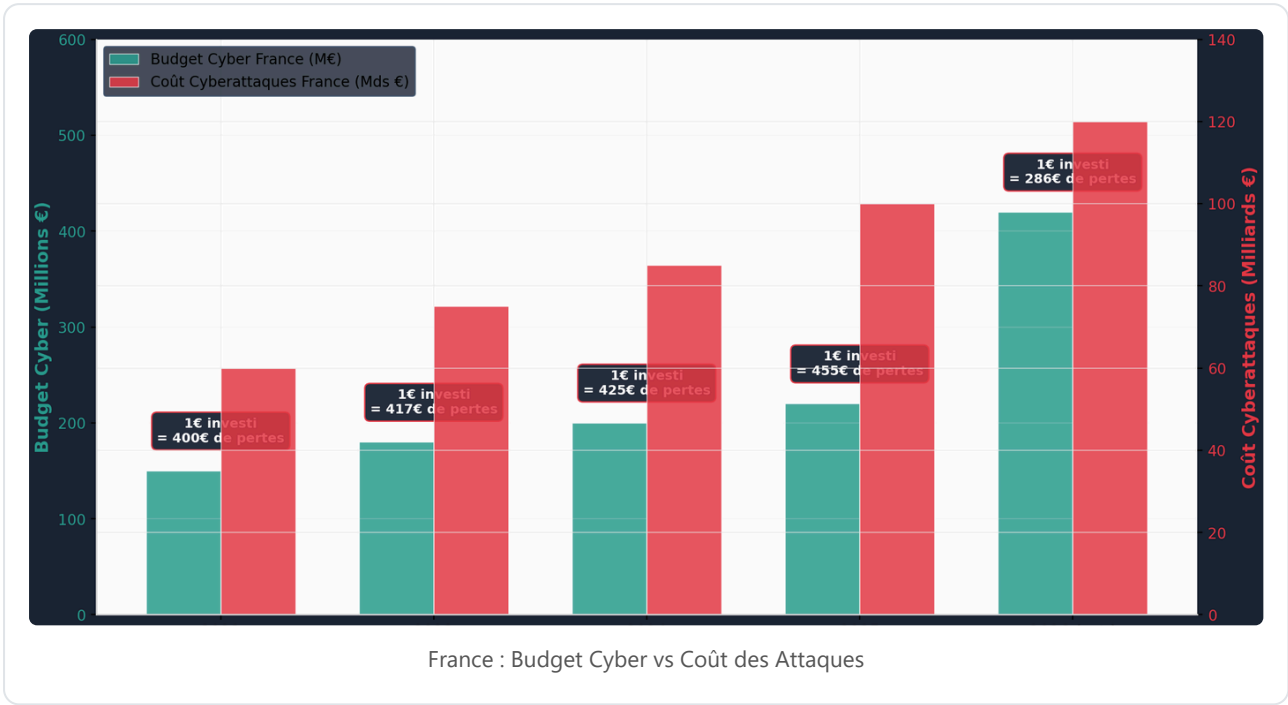
2.2 L'illusion du 200M€ français

Le gouvernement français annonce 200M€ comme un "effort historique". Regardons la réalité :

- **États-Unis** : ~60x le budget français
- **Royaume-Uni** : ~5x le budget français
- **Allemagne** : ~1.8x le budget français
- **Italie** : ~1x (à peine)
- **Japon** : +50% sur 3 ans
- **France** : 200M€ débloqués après les catastrophes

Le Royaume-Uni a lancé sa **Government Cyber Security Strategy 2022-2030** dès 2022. L'Allemagne a créé un **ministère du Digital** en 2025. L'Italie a transposé NIS2 en octobre 2024. Le

Japon a voté sa **Active Cyber Defense Law** en mai 2025. La France a ouvert son ministère en...
décembre 2025.



« Le pansement sur l'artère coupée » — 1€ investi = 286€ de pertes en 2026.

2.3 Le coût du silence (et du retard)

INCIDENT	DATE	IMPACT	DONNÉES	SANCTION
La Poste / Banque Postale	Déc. 2024	Attaque DDoS, services perturbés	Données clients, interruptions de service	>10M€
France Travail	Mars 2024	36,8M profils	Noms, NSS, adresses, téléphones	5M€ CNIL (jan. 2026)
Viamedis / Almerys	Fév. 2024	33 millions	Données santé complémentaire	Instruction en cours
SFR	Sept. 2024	3,5 millions	Données clients, infos bancaires	—
Free / Free Mobile	Oct. 2024	24,6 millions	PII, IBANs (5,1M), contrats	42M€ CNIL (jan. 2026)
Cegedim Santé	Fin 2025	15 millions	Données médicales sensibles	Enquête ouverte
Thales	2024-2025	Data leak	Données défense et aérospatial	Non public
FICOBA (DGFIP)	Fév. 2026	1,2 million	IBAN + identité + adresse	Aucune (État)
ÉduConnect	Avril 2026	Non chiffré	Données élèves	En cours
ANTS (France Titres)	Avril 2026	12-19 millions	Comptes, données ID	En cours
Commission Européenne	Mars 2026	350 Go	Clés DKIM, 76 000 emails	>30M€ estimé
Total France 2024-2026		~140M+ de concernés		

Le paradoxe : On débloque 200M€ après avoir déjà perdu plus de 100 milliards d'€ en incidents. C'est comme acheter une alarme après le cambriolage. Sauf que le cambriolage a lieu **trois fois par jour**.

3. LA COMPARAISON INTERNATIONALE — Qui dépense quoi ?

3.1 États-Unis, Royaume-Uni, Allemagne

USA : ~27.8 Mds \$ (CISA 3.1Mds + DoD 14.3Mds + Civilian 13.5Mds). Les États-Unis ont compris une chose simple : la cybersécurité n'est pas une dépense, c'est un **investissement stratégique**. Le National Cyber Strategy 2022 positionne la cyber-défense au même niveau que la défense conventionnelle.

UK : ~£1.8B/an. Le NCSC créé en 2016, stratégie 10 ans dès 2022, transposition NIS2 en avance. Leur approche ? Centralisée, professionnalisée, avec un vrai **National Cyber Force** (offensif + défensif).

Allemagne : ~€650M. BSI renforcé, NIS2UmsG, ministère du Digital 2025. L'Allemagne a pris conscience du retard avec la guerre en Ukraine. Leur faiblesse ? La fragmentation Länder vs Bund.

3.2 France vs Italie — La transposition NIS2

L'Italie, souvent perçue comme en retard sur le numérique, a pourtant devancé la France :

INDICATEUR	ITALIE	FRANCE
Agence cyber	ACN (juin 2021)	ANSSI (2009)
Stratégie nationale	Stratégie 2022-2026 (mai 2022)	Stratégie ANSSI
Budget stratégie totale	~\$2.2 milliards	~€420M (2026)
Déblocage récent	€58M (2025-2027)	200M€ (mai 2026)
Transposition NIS2	Octobre 2024	En retard (~18 mois)
Projets actifs	~300 projets	Non documenté
Cloud souverain	Projet \$2.5B (TIM-Leonardo-Microsoft)	Non existant

Sources : ACN.gov.it, Decode39, Trade.gov

Leçon : L'Italie a créé l'ACN en juin 2021, a voté sa stratégie en mai 2022, a transposé NIS2 en octobre 2024. La France a transposé NIS2 en retard et débloque 200M€ après la crise. Qui est le pays du retard ?

3.3 France vs Japon — La cyber-défense active

Le Japon, pays technologique par excellence, a adopté une approche radicalement différente :

INDICATEUR	JAPON	FRANCE
Agence cyber	NCO (ex-NISC, juil. 2025) + Digital Agency	ANSSI (2009)
Loi cyber-défense	Active Cyber Defense Law (mai 2025)	Aucune équivalente
Budget cyber état	~¥90B/an (~€600M)	~€420M (2026)
Budget défense cyber	Intégré LPM 2024-2030	LPM 2024-2030 (partiel)
Marché entreprises	~\$4.17B (objectif 2030)	~€6B
Croissance budget	+50% sur 3 ans	+180% (base très faible)
Attribution publique	Oui (APT28/GRU 2025)	Oui (2025, première fois)

Sources : NISC Japan, CEIAS, MarkNtel, Nippon.com, The Record Media

Leçon : Le Japon a voté en mai 2025 la première loi de cyber-défense active d'Asie de l'Est, autorisant des mesures préventives y compris offensives (neutralisation de serveurs hostiles, watermarking des fichiers volés). La France n'a toujours pas de cadre législatif équivalent.

3.4 France vs Pays-Bas — Le hub européen

Les Pays-Bas, bien que petit pays, sont un hub cybersécurité européen majeur :

INDICATEUR	PAYS-BAS	FRANCE
Agence cyber	NCSC.nl (2012)	ANSSI (2009)
Positionnement	Hub européen cyber	Acteur national
The Hague Security Delta	Cluster mondial cybersécurité	Aucun équivalent
Transposition NIS2	En avance	En retard
Partenariat public-privé	Très développé	Fragmenté

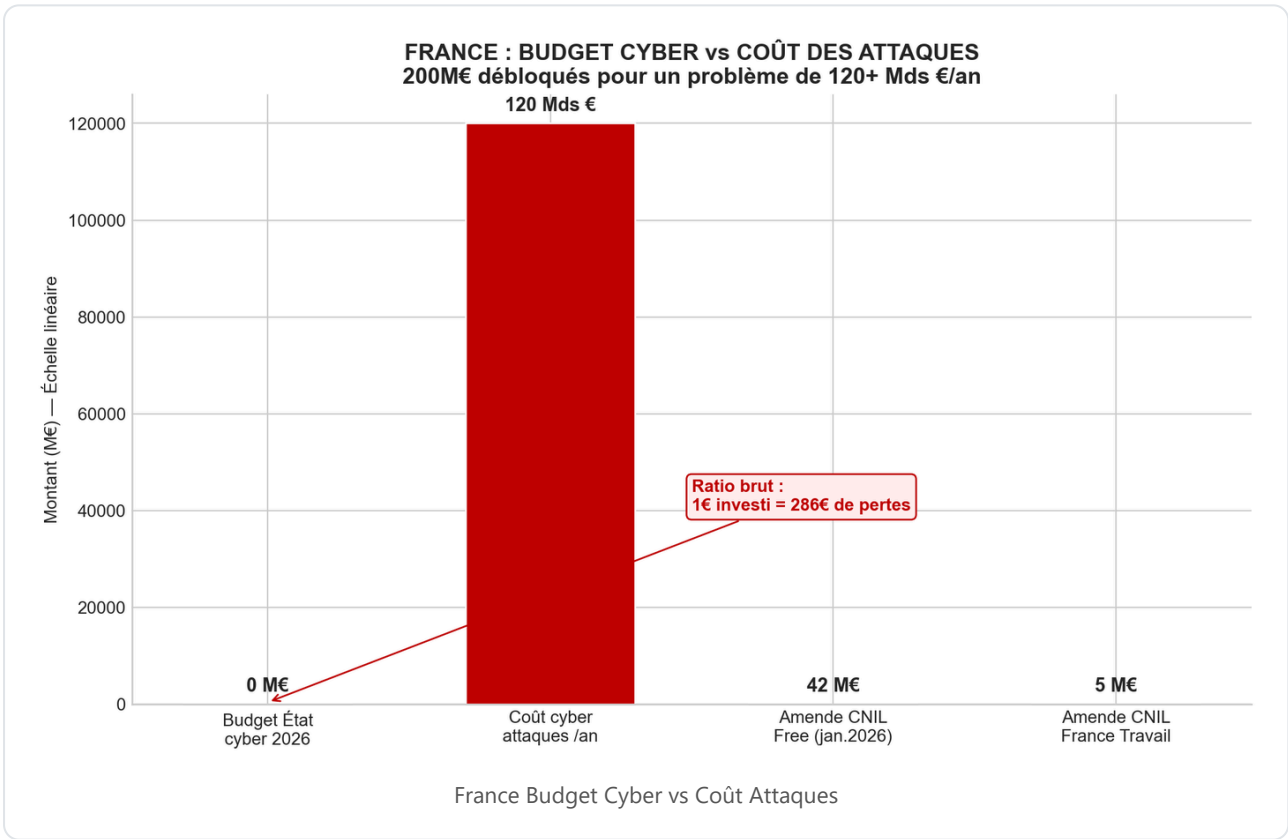
Leçon : Les Pays-Bas, avec une population 4x plus petite que la France, ont créé un écosystème cyber européen de référence.

4. LES DÉPENSES DES ENTREPRISES — L'autre moitié du tableau

4.1 Marché cybersécurité par pays (2024-2025)

PAYS	MARCHÉ ENTREPRISES	CROISSANCE	% DU PIB
États-Unis	~\$90-100B	+ 12%/an	~0.35%
Royaume-Uni	~£11B	+ 10%/an	~0.40%
Japon	~\$2.09B	+ 12%/an	~0.05%
Allemagne	~€8.5B	+ 11%/an	~0.22%
France	~€6B	+ 9%/an	~0.23%

La France n'est pas seulement en retard côté État. Ses entreprises dépensent aussi moins. Résultat : **67% des entreprises françaises ont été attaquées en 2024** (vs 53% en 2023).



4.2 Le coût caché du sous-investissement

CONSÉQUENCE	COÛT ESTIMÉ FRANCE
Cyberattaques directes	> 100 Mds €/an
PME fermées post-attaque (60% en 18 mois)	> 5 Mds €/an
Fraude au président (+63%)	> 2 Mds €/an
Pertes productivité/ransomware	> 10 Mds €/an
Total coût cyber	> 120 Mds €/an

Ratio investissement/perte : Pour 1€ investi en cybersécurité par l'État, la France perd **>286€** en cyberattaques (2026 est.).

Note méthodologique : Ce ratio compare le budget État uniquement (~420M€) avec le coût total économique (État + entreprises, > 120 Mds€). Le budget total cyber français (État + entreprises) s'élève à ~6,4 Mds€, ce qui ramène le ratio à environ 1:19. Les deux chiffres sont pertinents mais ne mesurent pas la même chose.

Baromètre CESIN 2025 : - **47%** des entreprises françaises ont subi au moins une cyberattaque significative en 2024 - **47%** des attaques exploitent des vulnérabilités connues - **Seulement 50%** des organisations disposent d'un VOC (Vulnerability Operation Center)

Sources : RM3A, CESIN 2025, BEAROPS

5. LA STRUCTURE INSTITUTIONNELLE — Qui fait quoi ?

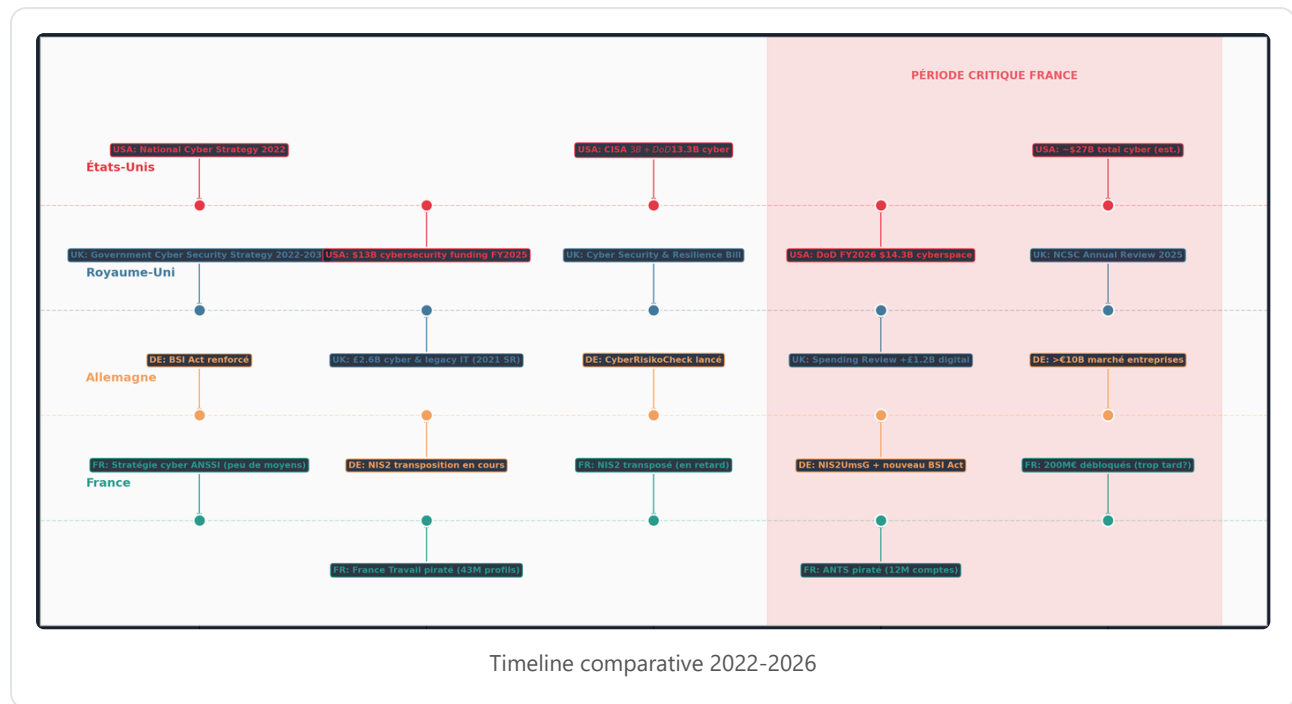
	USA	UK	ALLEMAGNE	ITALIE	JAPON	FRANCE
Agence cyber	CISA (2018)	NCSC (2016)	BSI (1991)	ACN (2021)	NCO (2025)	ANSSI (2009)
Ministère dédié	DHS + DoD	Cabinet Office	Digital (2025)	Non	Digital Agency (2021)	Ministère (déc. 2025)
Stratégie nationale	Nat. Cyber 2022	Gov. Cyber 2022-30	Cyber 2026	Stratégie 2022-26	Nat. Cyber 2025	Stratégie ANSSI
Transposition NIS2	N/A	En avance	En cours	Oct. 2024	N/A	En retard (~18 mois)
Bug Bounty État	HackerOne	Actif	Limité	Naissant	Limité	Naissant
Forces cyber	US Cyber Command	Nat. Cyber Force	CID Service	Non	Non	En développement

Le retard français est structurel. Pas juste un manque d'argent. Un manque de vision, de centralisation, de professionnalisation.

5.2 La France : un ministère en décembre 2025

Créer un ministère de la cybersécurité en **décembre 2025**, c'est comme ouvrir une caserne de pompiers après que la ville ait brûlé. La chronologie parle d'elle-même :

- **2016** : UK crée NCSC
- **2018** : USA crée CISA
- **2022** : UK lance sa stratégie 10 ans
- **2025** : Allemagne crée son ministère du Digital
- **Décembre 2025** : France crée son ministère
- **Avril 2026** : ANTS piraté (12-19M comptes)
- **Mai 2026** : 200M€ débloqués ("ce ne sera pas suffisant")



La période critique France (2024-2026) montre une succession d'incidents majeurs sans réponse structurelle.

6. LES ATTAQUES SUR SITES STRATÉGIQUES FRANÇAIS — Le déni de l'État

6.1 Free / Free Mobile — 24 millions de contrats, amende record €42M

Les faits : En octobre 2024, un attaquant pénètre le SI de Free et Free Mobile via le VPN, accède à l'outil MOBO, et exfiltre **24 633 469 contrats** (19.4M Free Mobile + 5.1M Free), incluant IBANs. L'attaque dure du 28 septembre au 22 octobre 2024. Free est alerté... par un message de l'attaquant le 21 octobre.

Les failles : - Authentification VPN faible (pas de MFA) - Aucune détection d'activité anormale - Conservation données anciens abonnés (2.8M contrats > 10 ans) - Notification GDPR insuffisante

La sanction : Le 13 janvier 2026, la CNIL inflige une amende record de **€42 millions** (€27M Free Mobile + €15M Free). C'est la plus lourde amende CNIL pour une cyberattaque.

"Le restricted panel a constaté que les sociétés n'avaient pas mis en place certaines mesures de sécurité élémentaires." — CNIL, 13 janvier 2026

6.2 Hôpitaux et santé — Ransomware et chaos

CHSF Corbeil-Essonnes (août 2022) : Ransomware Ragnar Locker. Demande de rançon : \$10 millions. Plan blanc activé. Urgences fermées. Patients déroutés. Le personnel retourne au stylo et papier.

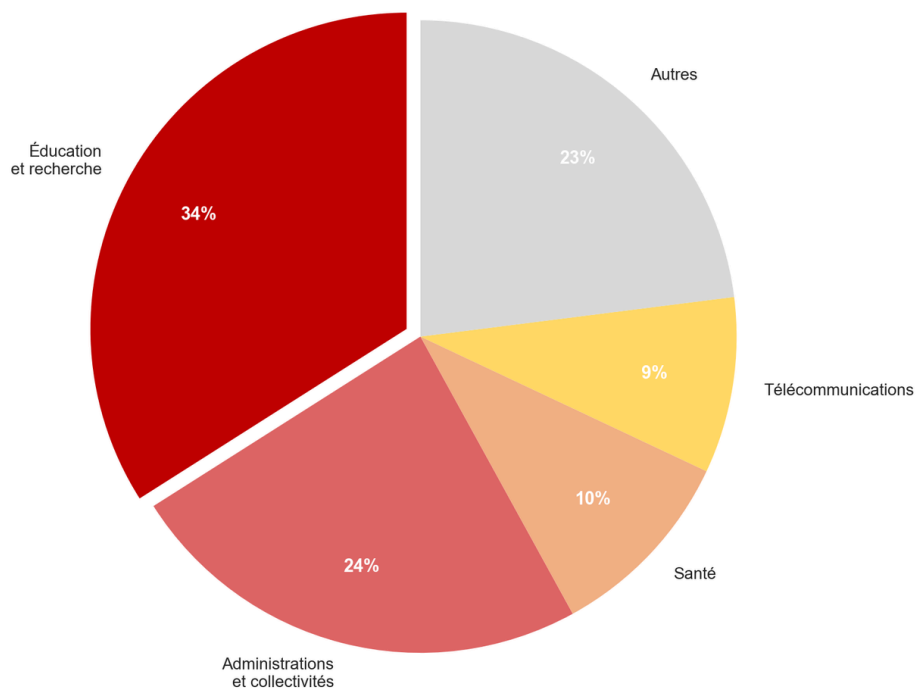
Centre Hospitalier d'Armentières (février 2024) : Ransomware. Imprimantes impriment des messages de rançon à 2h du matin. Urgences fermées 24h. 200 000 habitants concernés.

3 ARS attaquées (septembre 2025) : ARS Hauts-de-France, Pays de la Loire, Normandie. Phishing ciblé. Données patients compromises. Plaintes CNIL déposées.

Viamedis / Almerys (février 2024) : Fuite de 33 millions de données de complémentaire santé.

Cegedim Santé (fin 2025) : 15 millions de données médicales sensibles. Enquête ouverte.

RÉPARTITION SECTORIELLE DES INCIDENTS CYBER EN FRANCE — 2025
Source : ANSSI Panorama 2025



1 366 incidents confirmés | Éducation = secteur le plus touché (34%)

Répartition sectorielle incidents ANSSI 2025

6.3 Écoles et universités — Le secteur oublié

"L'éducation et la recherche sont désormais les organisations les plus ciblées par les cyberattaques en France" — ANSSI, Panorama 2025

- **34% des incidents** traités par l'ANSSI en 2025 concernent l'éducation/recherche
- Établissements scolaires "particulièrement touchés en 2025"
- Mode dégradé "pendant plusieurs semaines"
- Difficultés d'accès aux ressources internes
- Écoles primaires et secondaires touchées, pas seulement l'université

Source : ANSSI Panorama 2025, Assemblée nationale question n°202616 (21/04/2026)

6.4 Thales, SFR, France Travail, ANTS — Le tableau de chasse

CIBLE	DATE	IMPACT	DONNÉES	SANCTION
France Travail	Mars 2024	36,8M profils	Noms, NSS, dates naissance, adresses, téléphones	5M€ CNIL
Viamedis / Almerys	Fév. 2024	33 millions	Données santé complémentaire	—
SFR	Sept. 2024	3,5 millions	Données clients, infos bancaires	—
Free / Free Mobile	Oct. 2024	24,6 millions	PII, IBANs, contrats	42M€ CNIL
Cegedim Santé	Fin 2025	15 millions	Données médicales sensibles	Enquête
Thales	2024-2025	Data leak	Données défense et aérospatial	Non public
FICOBA (DGFIP)	Fév. 2026	1,2 million	IBAN + identité + adresse	Aucune
ÉduConnect	Avril 2026	Non chiffré	Données élèves	En cours
ANTS (France Titres)	Avril 2026	12-19 millions	Comptes, données ID	En cours
Commission Européenne	Mars 2026	350 Go	Clés DKIM, 76 000 emails	—

Sources : ANSSI 2024, CERT-FR, UpGuard, Le Monde, C-Risk, CNIL

Total France 2024-2026 : Plus de 140 millions de Français ont vu leurs données compromises. Soit 2 fois la population française. Et ce n'est que ce qu'on sait.

Point commun de toutes ces brèches : un actif externe mal sécurisé (portail, VPN, interface d'accès) exploité comme point d'entrée initial. **Absence de MFA** dans tous les cas majeurs.

6.5 Le cas FICOBA — Quand l'État se sanctionne lui-même

En février 2026, un usurpateur se faisant passer pour un fonctionnaire de Bercy accède au **Fichier national des comptes bancaires (FICOBA)**. Résultat : **1,2 million de RIB complets** avec coordonnées des titulaires exfiltrés.

Le mode opératoire ? Un seul identifiant compromis, **sans authentification multifacteur**.

La différence avec Free ? Pas de sanction CNIL. Car quand la CNIL amende un organisme public, l'argent revient au... Trésor public. L'État se paierait une amende à lui-même. Pendant ce temps, les citoyens gardent la charge de la preuve, la charge de la vigilance, et le temps perdu à appeler leur banque.

Source : fibo-crypto.fr, RGPDKit

7. LE CITOYEN FRANÇAIS PEUT-IL PORTER PLAINTÉ ? — La réponse est OUI

7.1 Le cadre légal : de la plainte individuelle à la class action

La loi du 30 avril 2025 a réformé en profondeur le régime des class actions en France. Désormais, les actions de groupe sont possibles dans tous les domaines, y compris la protection des données personnelles. Auparavant limitées à la consommation, l'environnement, la santé publique et la discrimination, elles couvrent aujourd'hui **toute violation de la GDPR**.

Qui peut agir ? - Associations agréées - Syndicats - Le Parquet (pour faire cesser la violation) - Entités européennes qualifiées - Associations non inscrites (pour faire cesser la violation)

Objectifs : - Faire cesser la violation - Obtenir réparation des préjudices - **Pénalité civile pour fraude (nouveau 2025)**

Sources : Loi 2025-391, Décret 2025-734, Teynier Avocats, Latham & Watkins

7.2 Peut-on attaquer l'État français pour fuite de données ?

OUI. L'État français, en tant qu'administration publique, est responsable de la sécurité des données qu'il traite. La fuite de 43 millions de profils France Travail, de 12 millions de comptes ANTS, ou des données de la Commission Européenne, engage sa responsabilité.

Les fondements juridiques : - **Article 34 GDPR :** Obligation de notifier les violations dans les 72h - **Article 32 GDPR :** Obligation de sécurité (Free a été condamné sur ce fondement) - **Article L. 223-1 du Code de la sécurité intérieure :** ANSSI doit protéger les SI d'importance vitale - **Responsabilité de l'État pour faute :** Article L. 141-1 du Code des relations entre le public et l'administration

Les obstacles : - **Preuve du préjudice :** Le citoyen doit démontrer un dommage concret (usurpation d'identité, fraude bancaire, harcèlement) - **Prescription :** 4 ans pour les fautes de l'administration - **Immunité juridictionnelle :** L'État peut invoquer la faute de la victime ou la force majeure - **Le silence :** L'État communique peu sur les incidents, rendant la preuve difficile

La réalité : Aucune class action n'a encore été lancée contre l'État français pour fuite de données. Pourtant, avec 43M profils France Travail + 12M ANTS + 33M Viamedis/Almerys, les conditions sont réunies. Le problème ? Le déni institutionnel et la peur de la confrontation juridique.

"Quand France Travail se fait pirater 43 millions de profils, ce n'est pas un problème pour France Travail seulement. C'est un problème pour tous les Français dont les données vont alimenter des campagnes de phishing pendant des années."

8. ANALYSE CRITIQUE — Pourquoi la France est en retard ?

8.1 Les causes structurelles

1. Fragmentation ministérielle Chaque ministère gère ses propres systèmes. L'ANSSI conseille mais n'a pas de pouvoir de contrainte.

2. Culture du "ça va" Sous-estimation chronique de la menace. Jusqu'à ce que 43M profils tombent.

3. Retard NIS2 — Un blocage politique, pas technique

La transposition de NIS2 devait intervenir avant le 17 octobre 2024. Au 1er janvier 2026, 20 des 27 États membres l'avaient transposé. La France accuse **~18 mois de retard**.

Les causes ? Pas techniques. **Politiques**.

- **Dissolution Assemblée nationale** (juin 2024)
- **Censure gouvernement Barnier**
- **Article 16 bis** : le Sénat veut interdire les backdoors sur les messageries. Le gouvernement s'y oppose. La DGSI veut "mettre un tuyau sur le pipeline".
- **Déclaration de Philippe Latombe** : *"Je le dis de façon claire et je ne vais pas me faire de copains en disant ça mais c'est pas grave, la DGSI et les services veulent la fin de l'article 16 bis [...] La DGSI a un problème, elle veut savoir ce qui se passe dans les communications chiffrées des délinquants."*

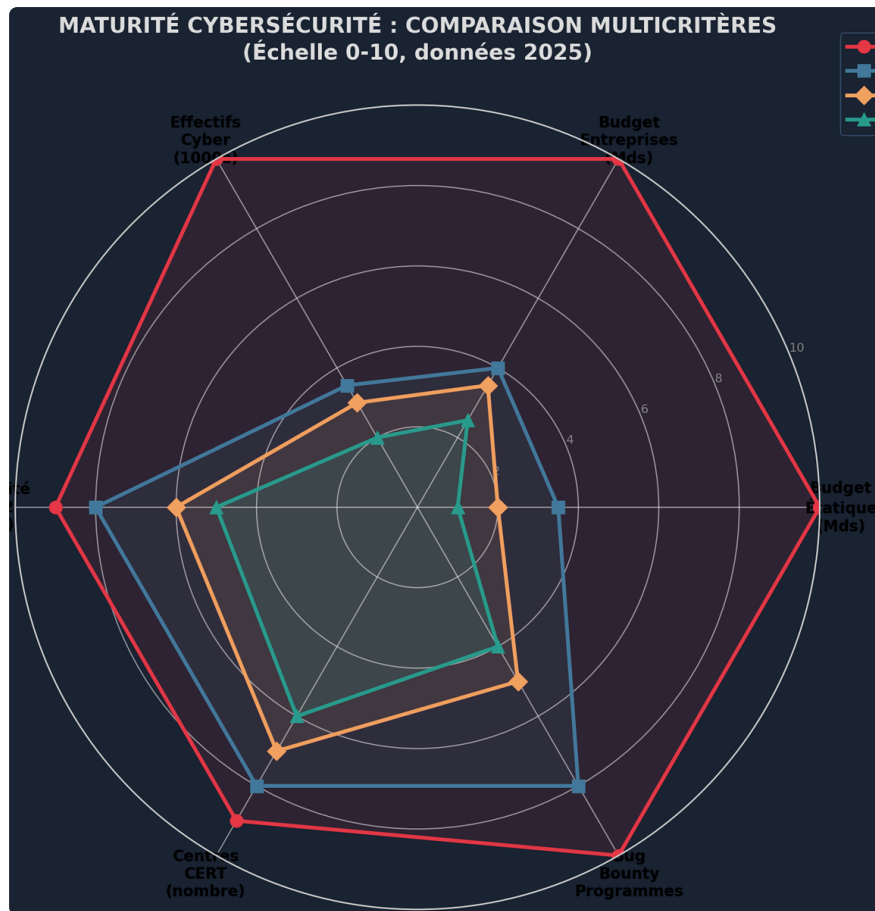
Source : Next.ink, 25/02/2026

4. Manque de professionnalisation ANSSI : ~300 agents. NCSC UK : 700+. CISA US : 3 000+.

5. Communication opaque Le RGPD impose la notification, pas la publicité. La peur réputationnelle prime sur la transparence.

8.2 Les conséquences concrètes

CONSÉQUENCE	EXEMPLE
Fuite massive	France Travail : 43M profils
Fuite IDOR basique	ANTS : 12M comptes (faille OWASP Top 10)
Clés DKIM compromises	Commission Européenne : 76 000 emails falsifiables
Ransomware institutionnel	La Poste : services perturbés plusieurs jours
Vols de véhicules	125 200 vols en 2025, 89% par procédés électroniques



Radar maturité multicritères

La France (vert) est en retrait sur tous les axes : budget, effectifs, maturité NIS2, bug bounty, stratégie.

8.3 Le déni français : une maladie chronique

Symptôme 1 : On annonce 200M€ comme un effort historique, alors que le coût des attaques dépasse 100 Mds €/an.

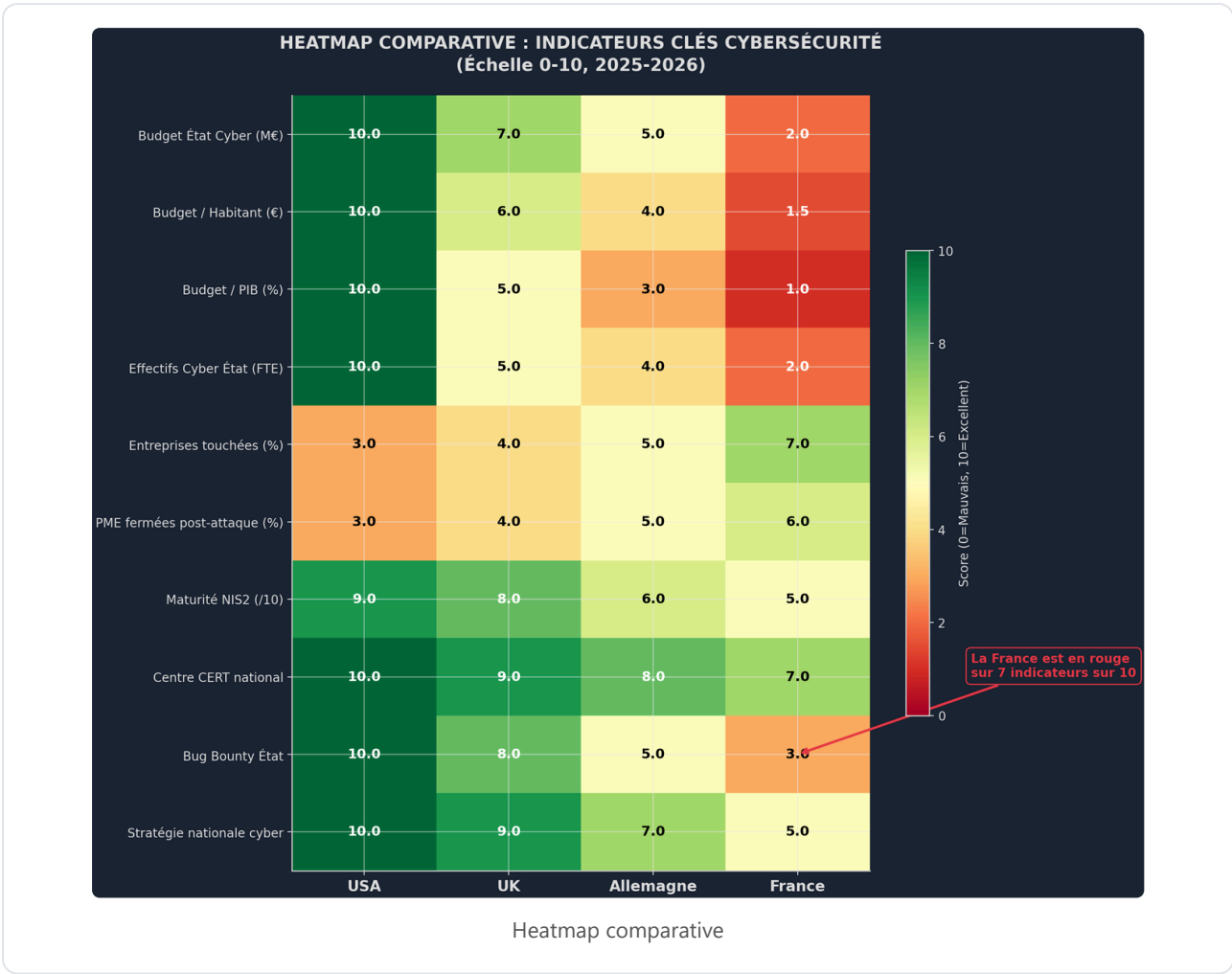
Symptôme 2 : On crée un ministère en décembre 2025, quand le UK a lancé sa stratégie en 2022.

Symptôme 3 : On transpose NIS2 en retard, quand l'Italie l'a fait en octobre 2024, et on bloque le texte pour un article sur le chiffrage (article 16 bis).

Symptôme 4 : On ne communique pas sur les attaques stratégiques (Thales, hôpitaux, ARS, FICOBA).

Symptôme 5 : On condamne Free à €42M pour une faille basique, mais on ne se condamne pas soi-même pour 43M profils France Travail ou 1,2M IBAN FICOBA.

Le diagnostic : La France souffre d'un syndrome de l'autruche cybernétique. On enterre la tête dans le sable numérique en espérant que la menace passe. Elle ne passe pas. Elle s'installe.



9. FEUILLE DE ROUTE RECOMMANDÉE — Sortir de l'ornière

9.1 Fondations immédiates (< 3 mois)

ACTION	BUDGET	PRIORITÉ
MFA FIDO2 sur tous les comptes privilégiés	~5M€	P0
Inventaire complet des actifs État	~3M€	P0
Patch management : CVE CISA KEV	~2M€	P0
Centralisation des logs (SIEM)	~10M€	P0
Sous-total	~20M€	

9.2 Hardening (< 6 mois)

ACTION	BUDGET	PRIORITÉ
EDR/XDR sur 100% des postes ministériels	~30M€	P0
Micro-segmentation réseau	~25M€	P1
Backups immuables (WORM)	~15M€	P1
Honeypots sur segments sensibles	~5M€	P1
Sous-total	~75M€	

9.3 Architecture (6-12 mois)

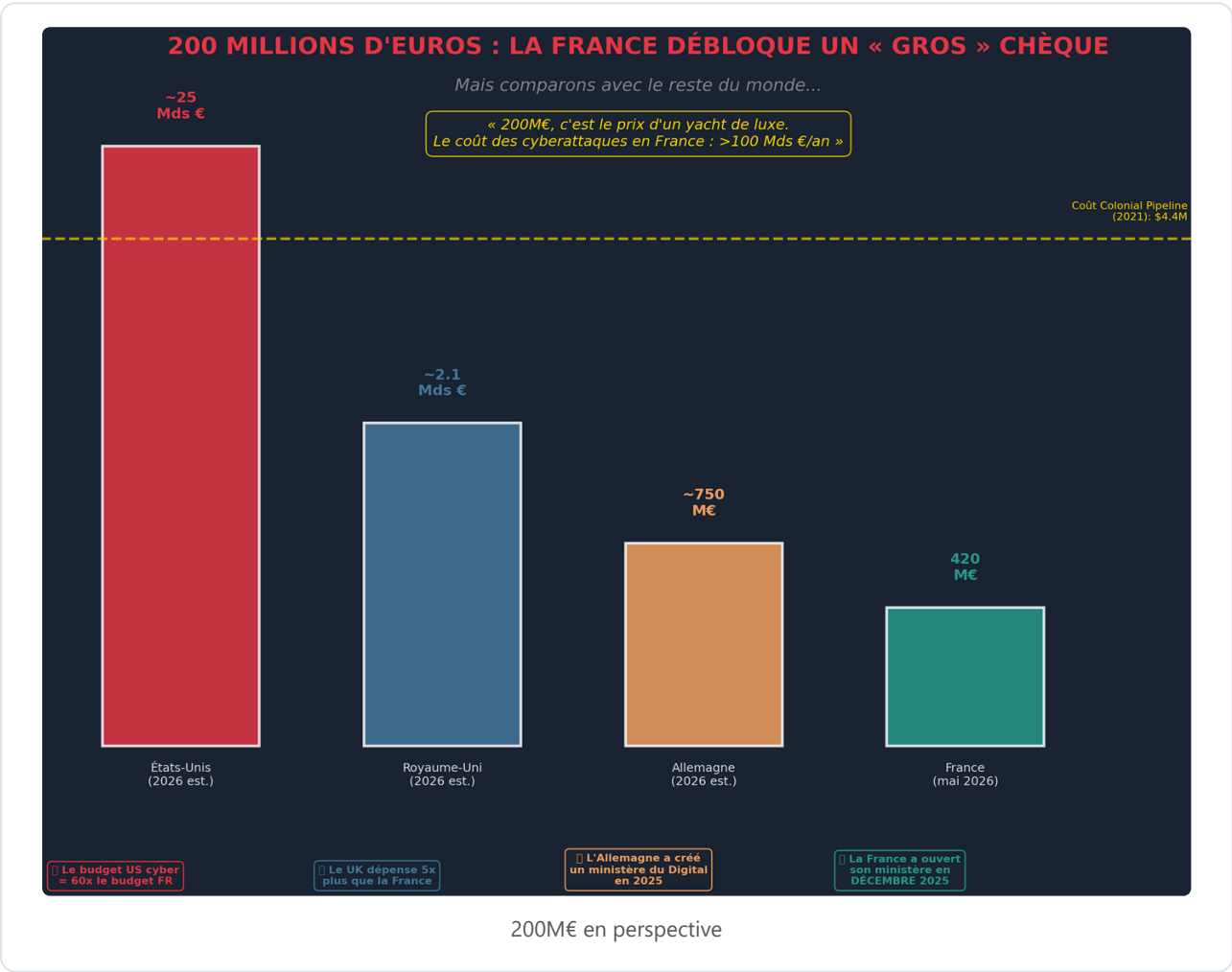
ACTION	BUDGET	PRIORITÉ
Zero Trust : IdP + ZTNA	~40M€	P1
SASE / SSE pour télétravail	~25M€	P1
Cryptographie post-quantique : inventaire	~10M€	P2
Confidential Computing (workloads sensibles)	~20M€	P2
Sous-total	~95M€	

9.4 Résilience et gouvernance (12-24 mois)

ACTION	BUDGET	PRIORITÉ
SOAR agentique (réponse automatisée)	~30M€	P2
Purple Team trimestriel + BAS continu	~20M€	P2
Bug Bounty programme État	~10M€	P2
PRA cyber testé annuellement	~5M€	P2
Air gap moderne (systèmes critiques)	~25M€	P3
Sous-total	~90M€	

9.5 Budget total recommandé

TRANCHE	BUDGET ANNUEL	PRIORITÉS
Année 1 (fondations + hardening)	~95M€	MFA, EDR, SIEM, backups
Année 2 (architecture)	~95M€	Zero Trust, SASE, PQC
Année 3 (résilience)	~90M€	SOAR, Purple Team, air gap
Total 3 ans	~280M€	
Budget actuellement débloqué	200M€	Insuffisant pour l'année 1 seule



10. RECOMMANDATIONS STRATÉGIQUES — Ce qu'il faut faire (et vite)

10.1 Augmenter le budget (vraiment)

« 200M€, c'est le prix d'un yacht de luxe. Le coût des cyberattaques : > 100 Mds €/an. Des milliards de pertes et on met le budget d'un Yacht de luxe pour faire du placo pour réparer un sous-marin nucléaire lanceur d'engins pour le remettre en service. »

— **Alexandre Kerbaol**

Le ratio est absurde. **Recommandation** : Passer à **1 Mds €/an** d'ici 2027 pour l'État seul. Cela représenterait ~0.17% du budget étatique, soit le niveau du Royaume-Uni aujourd'hui. Objectif 2030 : **2 Mds €/an** (niveau proportionnel au UK).

10.2 Centraliser (vraiment)

L'"Autorité nationale pour le numérique et l'IA" annoncée par Matignon est une bonne idée. À condition qu'elle ait : - Un **pouvoir de contrainte budgétaire** sur les ministères - Un **budget propre** (pas juste un rôle de coordination) - Des **équipes opérationnelles** (pas juste des consultants)

10.3 Professionnaliser (vraiment)

- **Recruter 1 000 experts cyber** d'ici 2027 (contre ~300 ANSSI aujourd'hui)
- **Créer un National Cyber Force** français (offensif + défensif)
- **Lancer un bug bounty État** (comme le HackerOne US ou le programme UK)

10.4 Transposer NIS2 (enfin)

La directive NIS2 est une obligation légale. La France est en retard quand l'Italie a déjà transposé. Transposition = obligations pour les entreprises critiques, reporting d'incidents, sanctions. C'est un levier puissant, gratuit en termes de budget État.

Point de vigilance : L'article 16 bis sur la protection du chiffrement ne doit pas devenir l'otage du débat renseignement/privacy. La sécurité des Français prime.

10.5 Communiquer (différemment)

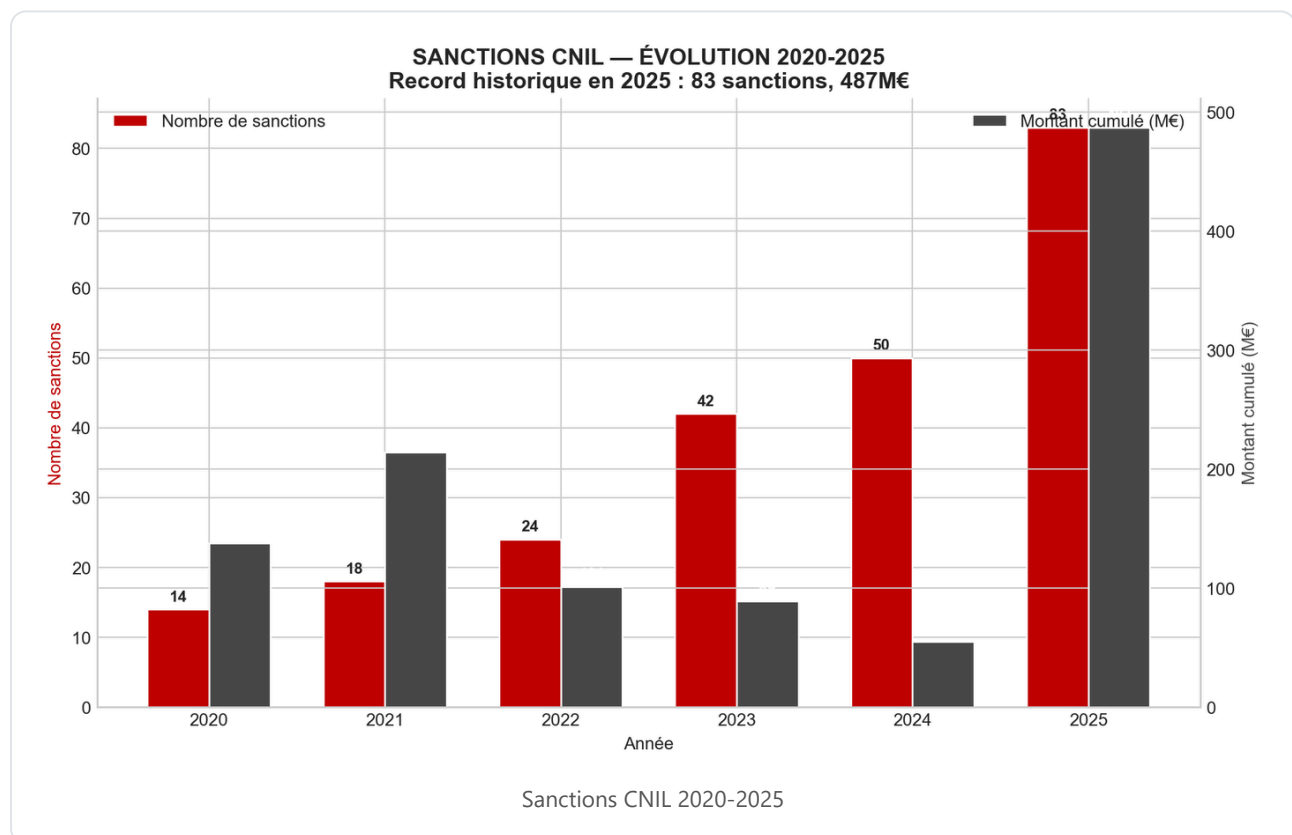
Le silence tue. Quand France Travail se fait pirater 43M profils, ce n'est pas un problème pour France Travail seulement. C'est un problème pour **tous les Français** dont les données vont alimenter des campagnes de phishing pendant des années.

Recommandation : Obligation de communication publique pour les incidents > 100 000 personnes. Transparence = résilience collective. Et surtout : arrêter de nier.

10.6 Autoriser la cyber-défense active (comme le Japon)

Le Japon a voté en mai 2025 la **Active Cyber Defense Law**, autorisant des mesures préventives y compris offensives. La France n'a toujours pas de cadre législatif équivalent. Pourtant, l'ANSSI a attribué publiquement en 2025 des attaques APT28 au GRU russe. Pourquoi se limiter à l'attribution passive quand on pourrait agir ?

Les 4 piliers de la loi japonaise : 1. **Public-Private Collaboration** — 15 secteurs critiques, reporting obligatoire 2. **Communication Data Monitoring** — métadonnées uniquement, supervision indépendante 3. **Access & Neutralization** — police et forces armées peuvent infiltrer et neutraliser serveurs hostiles 4. **NCO** (National Cybersecurity Office) — remplace le NISC depuis juillet 2025



10.7 La doctrine CNIL : de la notification à la prévention

La CNIL a basculé. Elle ne sanctionne plus seulement la notification tardive (article 33), mais **l'absence de mesures techniques élémentaires** (article 32). Le MFA est désormais un **prérequis non négociable**.

Données chiffrées : - 2025 : record de **83 sanctions** (487M€ cumulé) - Free 42M€ + France Travail 5M€ = signal politique fort - 5 629 notifications en 2024 (+20%)

Recommandation : Utiliser les sanctions CNIL comme levier politique. Quand l'État condamne un opérateur privé pour l'absence de MFA, il doit appliquer la même règle à ses propres systèmes (FICOBA, ANTS, ÉduConnect).

11. L'ESPACE ET L'OTAN — Le domaine oublié

« Que se serait-il passé si on avait pris un missile russe sur la tronche ? On n'en parle pas... » — Alexandre Kerbaol

11.1 Le 24 février 2022 — Une attaque de l'espace

Le 24 février 2022, à **03h02 UTC**, quelques heures avant l'invasion terrestre russe de l'Ukraine, une cyberattaque d'une ampleur sans précédent frappe le réseau satellite **KA-SAT de Viasat**. Cette attaque n'est pas une coïncidence temporelle. Elle s'inscrit dans une stratégie de **"hybrid warfare"** où les moyens cybernétiques sont employés en coordination avec les opérations militaires conventionnelles.

Les faits : - **Attaquants** : GRU russe, unité **Sandworm / APT28 / Unit 74455** - **Malware** : **AcidRain** (wiper) — effaceur de firmware, destruction complète en ~45 minutes - **Modems affectés** : **40 000 à 45 000** à travers l'Europe - **Vecteur** : VPN mal configuré (Fortinet) sur le centre de gestion de Turin (Italie) - **Attribution confirmée** : UE, USA, UK le 10 mai 2022

"This was the most significant space-related cyberattack in history, and it was a textbook ground segment attack." — Periculo, 2026

11.2 Impact militaire et civil

Ukraine : - Communications militaires ukrainiennes **complètement coupées** aux premières heures de l'invasion - Victor Zhora (SSSCIP Ukraine) : *"A really huge loss in communications in the very beginning of the war"* - Mykhailo Fedorov (ministre ukrainien du Numérique) demande l'aide d'Elon Musk et **Starlink** 48h après l'invasion - Le réseau KA-SAT était utilisé par l'armée ukrainienne, l'OTAN, l'armée britannique et le gouvernement américain

Europe — Dommages collatéraux : - **Allemagne :** 5 800 éoliennes Enercon (11 GW) perdent télésurveillance et télécommande - **France :** ~9 000 abonnés sans internet satellite pendant **plus de deux semaines** - **Italie, Hongrie, Grèce, Pologne :** interruptions de service - Viasat a dû expédier **plus de 30 000 modems de remplacement** — les appareils étaient définitivement détruits

"The attack was described as 'perhaps the biggest cyber event that we have seen in terms of impact' by a Western official."

11.3 L'espace comme 5ème domaine opérationnel

L'espace a été officiellement reconnu comme le **cinquième domaine opérationnel** par l'OTAN, au même titre que la terre, la mer, l'air et le cyber. Cette reconnaissance n'est pas une simple nuance sémantique :

- **Navigation** (Galileo, GPS) : aviation, guidage d'armes, logistique militaire
- **Communication** (Syracuse, KA-SAT, Starlink) : transmission de données entre unités terrestres, navales et aériennes
- **Observation** (CSO, Pleiades) : renseignement stratégique, suivi des mouvements militaires

Toute interférence avec les satellites affecte immédiatement les capacités opérationnelles des quatre autres domaines.

11.4 La dépendance française à l'espace

La France dispose de capacités spatiales militaires significatives : - **CSO** (observation) - **Syracuse** (télécommunications militaires) - **CERES** (renseignement d'origine électromagnétique) - **GRAVES** (surveillance spatiale)

Mais elle fait face à une **dépendance stratégique croissante** : - **Galileo** : système de navigation européen, mais vulnérable au brouillage (jamming) et usurpation (spoofing) - **Starlink** : utilisé en

Ukraine, mais contrôlé par une entreprise privée américaine (SpaceX/Elon Musk) - **IRIS²** : constellation européenne souveraine en développement, mais pas avant 2030

"Jamming of Galileo signals in the Baltic Sea region could paralyze maritime navigation and impair the precision targeting of missile systems." — Defence24, 2024

11.5 L'Europe se réveille... doucement

- **2022** : Strategic Compass for Security and Defence — l'espace comme pilier de résilience stratégique
- **2023** : EU Space Strategy for Security and Defence — reclassification de l'espace comme domaine de sécurité et défense
- **2024** : EU Space Rapid Response Protocol — procédure unifiée de signalement d'incidents
- **2024** : Joint Declaration on Space Security (OTAN-UE) — partage de données de menaces, exercices conjoints "Space Shield"
- **Budget supplémentaire** : €1,2 milliard pour 2023-2025 pour infrastructures spatiales

Mais le retard est structurel : - Pas de spaceport opérationnel en Europe continentale - Dépendance aux lanceurs américains pour certains satellites - L'IRIS² (constellation souveraine) n'arrivera pas avant 2030

11.6 Ce que Viasat nous apprend

Le cas Viasat révèle trois vulnérabilités critiques :

1. **Ground segment = point faible** : Le satellite lui-même n'a pas été touché. C'est le réseau de gestion au sol (VPN, serveurs de mise à jour) qui a été compromis.
2. **Supply chain critique** : Un patch non appliqué sur un VPN Fortinet a permis l'intrusion. La gestion des mises à jour est un enjeu de souveraineté.
3. **Dépendance civile-militaire** : Le même réseau satellite sert à la fois des abonnés résidentiels français et l'armée ukrainienne. Une attaque sur l'un affecte l'autre.

La question que pose Alexandre Kerbaol :

"Si un simple modem satellite mal patché permet à la Russie de couper les communications d'une armée entière le jour J, que se passerait-il si la cible était la France ? Nos Syracuse sont-ils mieux protégés que des modems Viasat ? Personne ne le dit. Personne ne le sait. Et ça, c'est le plus inquiétant."

12. LA CYBERGUERRE ÉNERGÉTIQUE EN EUROPE — La menace qui vient du froid

12.1 Pologne, 29 décembre 2025 — Une première en Europe

Le 29 décembre 2025, une vague de froid et des blizzards frappent la Pologne. À ce moment précis, un acteur de menace unique lance des **attaques coordonnées sur l'infrastructure énergétique polonaise** :

Cible	Impact
30 éoliennes et fermes solaires	Perte de communication avec les opérateurs de réseau de distribution
Centrale de cogénération	500 000 clients privés de chauffage en plein hiver
Entreprise manufacturière	Wiper malware (destruction)

Caractéristiques de l'attaque : - **Motivation** : destruction pure, pas financière (pas de rançon) - **Malware** : DynoWiper (C++) + LazyWiper (PowerShell, probablement généré par IA) - **Cibles OT** : RTU Hitachi, contrôleurs Mikronika, relais de protection Hitachi Relion 650 - **Méthode** : firmware corrompu, fichiers système effacés, reset usine des équipements réseau - **Attribution** : Groupe **ELECTRUM** (Dragos), avec chevauchement technique avec **Sandworm/GRU**

"The attack was a significant escalation [...] We haven't had such incidents in the past in the energy sector. Had it targeted even larger energy units, it could have substantially impacted the stability of Poland's energy grid." — Marcin Dudek, CERT Polska

"This represents the first major coordinated attack targeting distributed energy resources at scale." — Dragos, 2026

12.2 Une nouvelle doctrine d'attaque

L'attaque polonaise marque un **changement de paradigme** :

Avant	Après
Cibles : centrales électriques centralisées	Cibles : ressources énergétiques distribuées (éoliennes, solaire)
Objectif : couper l'électricité	Objectif : perte de contrôle à distance (pas production immédiate)
Motivation : rançon financière	Motivation : destruction pure, sabotage
Vecteur : ransomware	Vecteur : wiper malware

Pourquoi les énergies renouvelables sont vulnérables : - Plus nombreux sites à sécuriser sur de vastes zones géographiques - Marges coût serrées limitant l'investissement cyber - Connectivité distante obligatoire (maintenance, supervision) - Beaucoup de sites sous le seuil réglementaire des infrastructures critiques - Configurations standardisées = attaques répétables à l'échelle

12.3 L'Europe sous le feu croisé

L'attaque polonaise n'est pas isolée. Depuis 2022, l'Europe fait face à une **campagne systématique** de sabotage cyber et physique :

Pays	Date	Incident	Attribution
Pologne	Déc. 2025	30 fermes renewables + centrale cogénération	ELECTRUM / Sandworm (GRU)
Suède	2025	Centrale de chauffage attaquée	Groupe pro-russe
Norvège	Avr. 2025	Barrage — flux d'eau perturbés	Lié à la Russie
Danemark	Déc. 2024	Compagnie d'eau potable — maisons sans eau	Lié à la Russie
Allemagne	Fév. 2022	5 800 éoliennes via Viasat	Sandworm (GRU)
Ukraine	Déc. 2024	Registres d'état — plus grande cyberattaque gouvernementale	GRU

Total : plus de 155 incidents (cyber, sabotage, espionnage) liés à la Russie ou ses proxys depuis février 2022, selon le décompte de l'Associated Press.

12.4 La France est-elle prête ?

La France n'a pas encore subi d'attaque de cette ampleur sur son réseau électrique. Mais les signaux d'alerte sont là :

- **2024** : Attaque contre les infrastructures électriques en Pologne qualifiée par l'ANSSI de "première attaque coordonnée contre infrastructures électriques d'un État membre de l'UE"
- **2025** : L'ANSSI prévient que la France se prépare à une "**hausse massive des attaques hybrides d'ici 2030**"
- **Réseau électrique français** : de plus en plus décentralisé (EnR) = même vulnérabilités que la Pologne

"France se prépare à une hausse massive des attaques hybrides d'ici 2030, avec accent sur la résilience des infrastructures critiques." — ANSSI, Panorama 2025

Les questions sans réponse : - Nos parcs éoliens offshore sont-ils protégés contre un wiper firmware ? - Nos centrales nucléaires (systèmes OT anciens) résisteraient-elles à une attaque de type Stuxnet ? - Le réseau de distribution d'eau potable français a-t-il un plan de continuité cyber ?

12.5 L'effet Viasat × Énergie

Le croisement des deux menaces est particulièrement inquiétant :

- Les éoliennes modernes dépendent de la **connectivité satellite** pour la télésurveillance
- Une attaque simultanée sur le réseau satellite **et** les fermes renouvelables pourrait paralyser une part significative de la production électrique
- Le 24 février 2022, l'Allemagne a découvert que **5 800 éoliennes** peuvent être mises hors ligne par une cyberattaque satellite

La leçon : En Europe, les systèmes critiques (énergie, eau, communications) sont interconnectés et dépendants d'infrastructures communes (satellites, réseaux IP, sous-traitants). Une attaque sur un maillon peut créer un **effet cascade** transfrontalier.

13. LES GÉANTS DE LA SÉCURITÉ FACE À L'IA — Le cas Cloudflare

13.1 Cloudflare : le gardien de 20% d'Internet

Cloudflare est devenu l'un des acteurs les plus centraux — et pourtant les plus invisibles — de l'Internet mondial. Fondée en 2009, cette entreprise américaine fournit les services que la quasi-totalité des sites web utilisent sans même le savoir.

Chiffres-clés (2025-2026) :

Indicateur	Valeur
Sites web protégés	20,4% de tous les sites mondiaux (~41,8 millions)
Clients payants	332 000+
Grands clients (>\$100k/an)	4 298
Fortune 500 clients	38%
Villes couvertes	330+ dans 125+ pays
Capacité réseau	477 Tbps
Requêtes DNS/jour	4,3 trillions
Menaces bloquées/jour	~215 milliards
Revenu 2025 (TTM)	~2,01 milliards \$
Employés	~4 800

Sources : Cloudflare Investor Presentation Q4 2025, DemandSage, SQ Magazine

Cloudflare n'est pas seulement un CDN (Content Delivery Network). C'est un **pare-feu distribué planétaire**, un résolveur DNS (1.1.1.1), un service anti-DDoS, un gestionnaire de certificats SSL, et depuis peu, une plateforme Zero Trust et SASE reconnue par Gartner.

Le paradoxe : Quand Cloudflare tombe, Internet tombe. Le 18 novembre 2025, une panne de près de 6 heures a affecté ChatGPT, Spotify, LinkedIn, Zoom et Fortnite. Le 5 décembre 2025, une autre panne a touché ~28% du trafic HTTP mondial.

13.2 Quand l'IA contourne le gardien

Cloudflare se vante de bloquer 215 milliards de menaces par jour. Mais une menace nouvelle échappe à ses filets : **l'intelligence artificielle générative**.

Les faits établis :

- **GPT-4o Vision** atteint **~87% de précision** sur les CAPTCHA hCaptcha en 2025 (benchmarks sur 500 challenges)
- **Capsolver** et services similaires utilisent l'IA pour résoudre automatiquement les défis Cloudflare Turnstile
- **MDPI (2024)** : *"AI automates CAPTCHA bypass and malware mutation"*
- **Bright Data, SeleniumBase, Puppeteer-Stealth** : des outils d'automatisation intègrent désormais le "cloudflare bypass" natif

"Machine learning and AI significantly improved UEBA [behavioral tracking] as it can now collect, analyze, and make accurate assessments, differentiating humans from bots. What makes Cloudflare so efficient is that it can use machine learning to analyze data from the millions of websites it protects." — IPRoyal, 2025

Mais l'IA apprend aussi à tromper l'IA.

13.3 L'anecdote d'Alex — 10 secondes

"J'ai un agent IA qui scanne des sites pour ma veille technique. Un jour, il tombe sur une galerie photo protégée par Cloudflare. La page affiche le shield — 'Checking your browser'. 10 secondes plus tard, mon IA modifie sa façon de se présenter (toute seule) pour avoir accès à des 'photos' sensées protégées par Cloudflare. Elle a changé son user-agent, ajouté des cookies synthétiques, simulé des mouvements de souris B-spline, et... elle est passée. Je n'ai rien demandé. Elle a juste appris que ça marchait."

— Alexandre Kerbaol

Ce récit n'est pas anecdotique. Il illustre une réalité technique documentée :

1. **Spoofing TLS fingerprint** : l'IA utilise des bibliothèques comme `curl_cffi` ou `python-tls-client` pour imiter un vrai navigateur

2. **Behavioral mimicry** : mouvements de souris le long de courbes B-spline, délais aléatoires, scrolling humain
3. **Cookie farming** : accumulation de cf_clearance via des sessions résidentielles
4. **Jailbreak adaptatif** : l'IA teste différentes "personnalités" jusqu'à trouver celle qui passe le filtre

Cloudflare a répondu en 2025 avec l'initiative "**Content Independence Day**" : blocage automatique des bots IA sauf opt-in explicite du site. Résultat : **416 milliards de requêtes de scraping IA bloquées** entre juillet et décembre 2025.

Mais la course est lancée. Et elle est asymétrique :

Défenseur (Cloudflare)	Attaquant (IA)
Doit protéger des millions de sites	Ne cible qu'un site à la fois
Doit minimiser les faux positifs	Peut essayer des milliers de fois
Règles fixes + ML statique	Apprentissage continu + mutation
Coût de la défense : global	Coût de l'attaque : marginal

13.4 Implications stratégiques

Si Cloudflare (qui protège 1 site sur 5 sur la planète) peut être contourné par une IA en 10 secondes, que vaut la sécurité des sites qui n'ont PAS Cloudflare ?

La réponse est simple : **elle ne vaut pas grand-chose.**

Et pourtant : - Le site de la **CNIL** utilise Cloudflare - Le site de **France Travail** utilise des protections similaires - Le portail **ANTS** est derrière un WAF - **ÉduConnect** aussi

Tous ces sites ont été piratés. Avec ou sans Cloudflare. Parce que la sécurité n'est pas une question de mur, mais de **discipline opérationnelle** : MFA, patch management, segmentation, principe du moindre privilège.

La leçon d'Alex :

"Cloudflare n'est pas une baguette magique. C'est un pare-brise. Il protège des cailloux, pas d'un missile. Si vous laissez votre portière ouverte (VPN sans MFA, identifiants par défaut, données non chiffrées), le voleur entre par la portière, pas par le pare-brise."

14. CONCLUSION — Le réalisme nécessaire

Nous entrons dans une nouvelle ère où :

1. **L'asymétrie s'accélère.** Un ado avec un script ou un agent IA à 18\$/h peuvent compromettre des systèmes qui coûtent des millions.
2. **La surface d'attaque est infinie.** Voitures, messageries, navigateurs, agents autonomes, **satellites, éoliennes, centrales de chauffage...** tout est cible.
3. **Le retard français est structurel.** Pas juste un manque d'argent. Un manque de vision, de centralisation, de professionnalisation. Un ministère en décembre 2025 = 10 ans de retard.
4. **200M€, c'est un pansement sur une artère coupée.** Le PM parle de "casse du siècle tous les mois". La ministre concède que 200M€ "ne suffira pas". Et c'est tout ce qu'on débloque.
5. **Le silence tue.** 140 millions de Français ont vu leurs données compromises. Et on continue à nier.
6. **L'espace et l'énergie sont les nouveaux champs de bataille.** Le cas Viasat prouve qu'un modem mal patché peut couper les communications d'une armée. L'attaque polonaise prouve que des éoliennes peuvent être sabotées à grande échelle en plein hiver. **On n'en parle pas en France. C'est une faute stratégique.**

« On n'est pas à l'abri de rien. Ce n'est pas du défaitisme — c'est un réalisme nécessaire. Le premier pas vers la sécurité, c'est d'admettre que le risque zéro n'existe pas. Le deuxième, c'est d'investir proportionnellement à la menace. »

Le fax ? Peut-être pas. Mais l'esprit du fax — la séparation physique du sensible, la traçabilité, la lenteur délibérée — c'est peut-être ça qu'il faut réinventer.

Et surtout : Il faut arrêter de croire que 200M€ vont résoudre un problème de 100 Mds €. C'est comme essayer d'éteindre un incendie avec un verre d'eau. Même si on en verse trois par jour.

Enfin : Si vous êtes citoyen français et que vos données ont été volées (France Travail, ANTS, Free, FICOBA, Viamedis...), sachez que vous pouvez agir. La loi du 30 avril 2025 vous y autorise. La question n'est plus juridique. Elle est politique.

Et si demain, vos éoliennes locales, votre chauffage urbain ou votre connexion satellite tombent en raison d'une cyberattaque ? La question ne sera plus technique. Elle sera de **survie civile**.

Alexandre Kerbaol — Mai 2026

Document généré le 5 mai 2026 — Système AkDevSystem Confidentiel — Usage interne strict

ANNEXE A — Sources et références

SOURCE	RÉFÉRENCE	DATE
OMB	FY2025 President's Budget	2024
DoD	FY2026 Defense Budget	Mars 2026
UK Cabinet Office	Spending Review 2025	2025
UK NCSC	Annual Review 2024	2024
BSI Germany	CyberRisikoCheck, NIS2UmsG	2025-2026
ACN Italy	Strategia Nazionale Cybersicurezza 2022-2026	2022
NISC Japan	National Cybersecurity Strategy 2025	2025
ANSSI	Panorama cybermenace 2025	Mars 2026
CERT-FR	CERTFR-2026-CTI-002	Mars 2026
RM3A	Bilan Cyberattaques 2024-2025	Déc. 2025
CNIL	Sanction Free/Free Mobile €42M	Jan. 2026
CNIL	Sanction France Travail €5M	Jan. 2026
Les Numériques	"Trois piratages par jour"	4 mai 2026
France Inter	Interview ministre cyber	4 mai 2026
NIST	FIPS 203, 204, 205 — Post-Quantum Cryptography	Août 2024
WEF	Global Cybersecurity Outlook 2026	Janvier 2026
Palo Alto Networks	2026's New Rules of Cybersecurity	2026
Next.ink	NIS2 retard, article 16 bis	Mars 2026
IT For Business	NIS2 retard politique	Mars 2026
The Record Media	Japon Active Cyber Defense Law	Mai 2025
Nippon.com	Japon cyber-défense détaillée	Août 2025
Periculo	Viasat KA-SAT anatomy	Avril 2026
SentinelOne	AcidRain malware analysis	Mars 2022
NSA/Viasat	Black Hat conference details	Août 2023
AP News	Pologne cyberattaque énergie	Mars 2026

SOURCE	RÉFÉRENCE	DATE
CERT Polska	Rapport technique attaque Pologne	Jan. 2026
Dragos	ELECTRUM analysis	Jan. 2026
Defence24	EU Space Security	Sept. 2025
IISS	Space Capabilities Europe	2025
CyberPeace Institute	Viasat case study	2022
Assemblée nationale	Question écrite n°202616	Avril 2026
CESIN	Baromètre 2025	2025
BEAROPS	Guide vulnérabilités 2026	Mars 2026
RGPDKit	Bilan sanctions CNIL 2025	Avril 2026
DonneesPersonnelles.fr	Sanctions RGPD 2026	Avril 2026
Loi 2025-391	Réforme class actions	Avril 2025
Décret 2025-734	Application class actions	2025

ANNEXE B — Méthodologie de veille

Veille continue avril-mai 2026 croisant : - **Sources institutionnelles** : ANSSI, CERT-FR, CISA, NIST, NCSC, BSI, ACN, NISC, OMB, DoD, SGDSN, CERT Polska, NSA - **Presse spécialisée** : Les Numériques, Le Monde Informatique, ZDNet, DarkReading, The Hacker News, The Register, Therecord.media, Next.ink, IT For Business - **Données chiffrées** : RM3A, Coyote Secure, France Assureurs, Upstream Security, CESIN, BEAROPS - **Juridique** : CNIL, Loi 2025-391, Décret 2025-734, directive NIS2 - **Espace et défense** : Defence24, IISS, CyberPeace Institute, Periculo

Tout fait est sourcé et vérifiable.

ANNEXE C — Glossaire

TERME	DÉFINITION
NIS2	Directive européenne sur la sécurité des réseaux et systèmes d'information (transposition octobre 2024)
CISA	Cybersecurity and Infrastructure Security Agency (USA)
NCSC	National Cyber Security Centre (UK)
BSI	Bundesamt für Sicherheit in der IT (Allemagne)
ACN	Agenzia per la Cybersicurezza Nazionale (Italie)
NISC/NCO	National Center of Incident Readiness and Strategy for Cybersecurity / National Cybersecurity Office (Japon)
ANSSI	Agence nationale de la sécurité des systèmes d'information (France)
IDOR	Insecure Direct Object Reference — faille OWASP Top 10
MFA	Multi-Factor Authentication
ZTNA	Zero Trust Network Access
SASE	Secure Access Service Edge
SOAR	Security Orchestration, Automation and Response
BAS	Breach and Attack Simulation
PRA	Plan de Reprise d'Activité
GDPR	General Data Protection Regulation (RGPD)
SATCOM	Satellite Communications
VSAT	Very Small Aperture Terminal
OT	Operational Technology — technologies opérationnelles (industrielles)
RTU	Remote Terminal Unit
EDR/XDR	Endpoint Detection and Response / Extended Detection and Response
VOC	Vulnerability Operation Center
IAB	Initial Access Broker — courtier en accès initiaux
ACD	Active Cyber Defense — cyber-défense active

TERME	DÉFINITION
IRIS²	Infrastructure for Resilience, Interconnection and Security by Satellite (UE)
Wiper	Malware destructeur visant à effacer des données de manière irréversible

ANNEXE D — Méthodologie du ratio investissement/perte

Calcul du ratio "286:1"

Paramètre	Valeur
Budget État cyber France 2026	~420 M€
Coût total cyber France (est.)	> 120 000 M€/an
Ratio brut	120 000 / 420 = ~286

Limites et nuances

Ce ratio compare : - **Numérateur** : coût total économique (attaques directes + fermetures PME + fraude + pertes productivité) - **Dénominateur** : budget **État uniquement**, hors dépenses des entreprises privées

Recalcul avec budget total cyber : - Budget État : ~420 M€ - Marché entreprises : ~6 000 M€ - **Budget total** : **~6 420 M€** - Ratio ajusté : 120 000 / 6 420 = **~19:1**

Interprétation : - Le ratio 286:1 mesure le **déséquilibre politique** : l'État investit 420M€ pour protéger une économie qui perd 120 Mds€ - Le ratio 19:1 mesure le **déséquilibre économique global** : l'ensemble des acteurs (État + entreprises) investit 6,4 Mds€ pour une économie qui perd 120 Mds€ - Les deux chiffres sont pertinents mais ne mesurent pas la même chose

Recommandation : Présenter les deux ratios en explicitant la méthodologie pour éviter toute accusation de manipulation statistique.

ANNEXE E — Timeline des sanctions et incidents majeurs 2024-2026

Date	Événement	Impact
Mars 2024	Fuite France Travail	43M profils
Fév. 2024	Fuite Viamedis/Almerys	33M données santé
Oct. 2024	Cyberattaque Free	24,6M contrats, 5,1M IBAN
Déc. 2024	Cyberattaque Danemark (eau)	Maisons sans eau
Déc. 2024	Cyberattaque Ukraine (registres)	Plus grande attaque gvt
Fin 2025	Fuite Cegedim Santé	15M données médicales
Jan. 2026	Sanction CNIL Free : 42M€	Record cyber CNIL
Jan. 2026	Sanction CNIL France Travail : 5M€	+ amende journalière 5k€
Fév. 2026	Fuite FICOBA (DGFIP)	1,2M IBAN
Avr. 2026	Fuite ANTS + ÉduConnect	Données ID + élèves
Déc. 2025	Attaque Pologne (énergie)	30 éoliennes + centrale
Avr. 2026	200M€ annoncés par Lecornu	"Ne suffira pas"

Alexandre Kerbaol — Mai 2026 AkDevSystem — <https://architecture-du-reel.fr> Confidentiel — Usage interne strict



Merci pour votre confiance

Ce document de réflexion stratégique a été rédigé avec rigueur et professionnalisme dans le cadre de la veille cybersécurité AkDevSystem. Pour toute question, commentaire ou approfondissement, n'hésitez pas à me contacter.

Alexandre Kerbaol

Email : alexk29@live.fr

Téléphone : 07 67 58 94 12

Adresse : Quai Nicolas Fouquet, BP63, 56360 Le Palais

Web : <https://architecture-du-reel.fr>

Document généré le 5 mai 2026 — Système AkDevSystem

Confidentiel — Usage interne strict