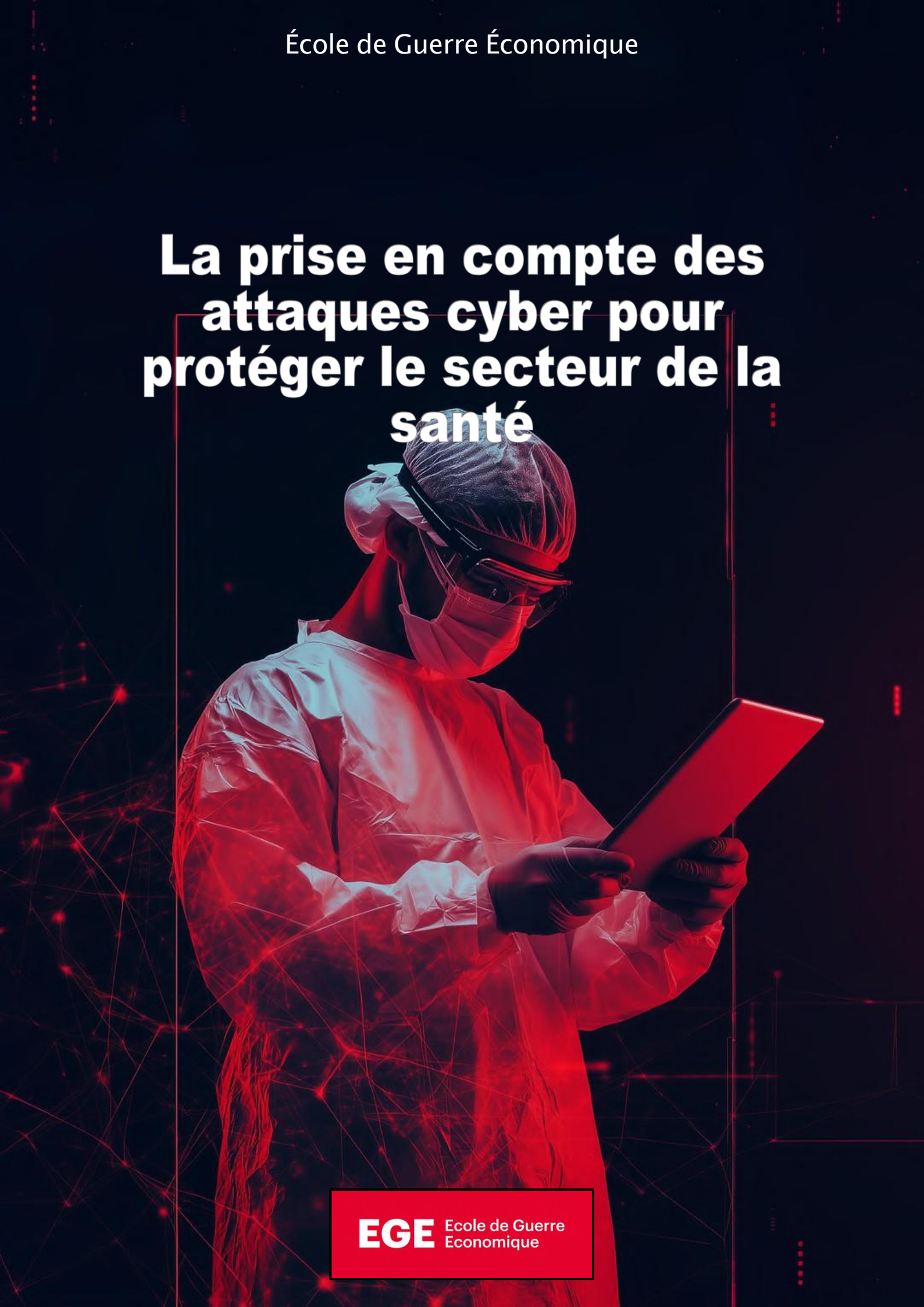
École de Guerre Économique

# La prise en compte des attaques cyber pour protéger le secteur de la santé



EGE Ecole de Guerre Economique

# TABLE DES MATIÈRES

# 1.

# CYBERSÉCURITÉ DANS LES ÉTABLISSEMENTS DE SANTÉ : DES NORMES ET FINANCEMENTS DÉCONNECTÉS DE LA RÉALITÉ

Le secteur de la santé, considéré comme hautement critique car touchant directement à la vie des personnes, est en proie à un retard important en matière de cybersécurité. En effet, les établissements de santé (ES) et les établissements et services médico-sociaux (ESMS) sont de plus en plus exposés aux cyberattaques et incidents informatiques, notamment en raison d'une dématérialisation croissante avec la numérisation des dossiers médicaux, la télémédecine et les objets connectés (IoT) – que sont par exemple les équipements d'imagerie médicale connectés tels que les IRM ou les scanners, qui transmettent directement les résultats aux praticiens.

Bien que le nombre d'incidents déclarés par les ES et ESMS soit en baisse depuis quelques années – passant de 733 en 2021 à 592 en 2022, pour atteindre 581 signalements en 2023 –, il reste trop élevé au regard du caractère critique du secteur de la santé. Les incidents informatiques et les cyberattaques qui l'affectent peuvent engendrer des conséquences significatives sur le fonctionnement des établissements, souvent contraints de fonctionner en mode dégradé, ce qui perturbe la prise en charge des patients, l'accès aux soins et la confidentialité des données.

Il est donc essentiel de prendre conscience de l'importance de la sécurité des systèmes d'information des ES et ESMS, et du retard accumulé dans le traitement des incidents et des cyberattaques qui y ont trait.

# I. CYBERSÉCURITÉ DES ÉTABLISSEMENTS DE SANTÉ EN FRANCE : UNE PRISE DE CONSCIENCE TARDIVE DES PROBLÈMES STRUCTURELS

La cybersécurité s'est révélée comme une préoccupation majeure pour le secteur de la santé au lendemain des deux cyberattaques de Versailles et Corbeil-Essonnes. Celles-ci ont mis en évidence la fragilité de la résilience numérique des établissements, le manque cruel de financement et l'absence de volonté politique.

## A. LE RÉVEIL POLITIQUE FACE AUX ENJEUX DE CYBERSÉCURITÉ DANS LES ÉTABLISSEMENTS DE SANTÉ

L'année 2022 et les deux cyberattaques majeures ciblant le Centre Hospitalier Sud Francilien (CHSF) de Corbeil-Essonnes et l'hôpital André-Mignot de Versailles marquent le réveil tardif des pouvoirs publics face aux enjeux de cybersécurité dans les établissements de santé.

### La résilience contestable de l'État face aux crises passées : l'exemple du Covid-19

La prise de conscience tardive du politique pose question. L'impréparation et la lenteur du gouvernement face aux crises dans le secteur de la santé ne sont pas nouvelles. En 2020 déjà, le gouvernement avait été vivement critiqué pour sa gestion de Covid-19, la pandémie ayant mis en lumière les faiblesses structurelles et organisationnelles du système de santé français.

Parmi elles, le manque de préparation et de prévoyance illustré par l'insuffisance des stocks stratégiques, qui a exposé les soignants et les citoyens à des risques importants dès le début de la pandémie, et l'anticipation défaillante du gouvernement, dans la mesure où, malgré les alertes sur le risque sanitaire, la réponse à la crise a été lente et désorganisée.

Les tensions sur les hôpitaux et le manque de moyens étaient également soulignés à l'époque, la pandémie ayant mis en lumière le sous-investissement chronique dans les établissements de santé français, alors que ces faiblesses étaient déjà connues avant la crise sans avoir été corrigées (manque de lits, pénurie de personnel…).

## Deux cyberattaques marquantes : les cas de Corbeil-Essonnes et Versailles

Le Centre Hospitalier Sud Francilien (CHSF) de Corbeil-Essonnes a été la cible d'une cyberattaque revendiquée par le groupe LockBit 3.0 dans la nuit du 20 août 2022. Les cyber-attaquants ont exigé une rançon de 10 millions de dollars, sous peine de publier des données sensibles qui avaient été dérobées fin septembre 2022. En réponse, l'établissement a immédiatement activé son plan blanc, un dispositif permettant à toute structure de santé de mobiliser l'ensemble de ses ressources pour faire face à une situation d'urgence. L'attaque a paralysé l'ensemble des systèmes informatiques de l'hôpital, compromettant la prise en charge des patients.

Le samedi 3 décembre 2022, c'est l'hôpital André-Mignot de Versailles qui a été victime d'une cyberattaque par ransomware (rançongiciel en français). Pour limiter la propagation de l'intrusion, l'établissement a immédiatement désactivé son système informatique ainsi que les communications téléphoniques. Des équipes techniques ont été dépêchées sur place afin d'analyser la situation et d'évaluer l'ampleur des dommages subis. Cette attaque a fortement perturbé le fonctionnement de l'hôpital et l'accueil des patients. Deux jours après l'incident, l'établissement reçut une demande de rançon, dont le montant reste inconnu à ce jour. En réponse à l'attaque, un plan blanc a été activé, l'accueil des patients a été limité aux urgences et une cellule de crise a été mise en place.

**L'affaire de l'hôpital de Versailles a rapidement pris une tournure politique,** avec l'intervention de Jean-Noël Barrot, alors ministre délégué chargé de la Transition numérique, qui a déclaré sur Twitter : « Honte aux criminels qui s'en prennent ainsi à nos établissements hospitaliers et donc aux plus fragiles. » Accompagné du ministre de la Santé de l'époque, François Braun, il s'est rendu sur place pour évaluer l'ampleur des dégâts subis et assurer aux personnels que l'État les soutiendrait face à la crise. Les équipes de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ont été mobilisées au sein de la cellule de crise que l'établissement a mise en place.

## Un sous-investissement chronique flagrant et une mauvaise répartition des fonds

Si à l'époque les ministres dénoncent fermement les deux attaques, ces dernières soulevaient néanmoins la question des enjeux de la cybersécurité dans les établissements de santé. En effet, le secteur subit les conséquences d'un sous-investissement chronique en matière de sécurité numérique.

En 2021 déjà, Emmanuel Macron lançait la Stratégie nationale d'accélération pour la cybersécurité, qui incluait un volet dédié à la santé. Elle prévoyait un financement, mêlant à la fois fonds publics et privés, à hauteur d'1 milliard d'euros. Bien que positive, cette initiative montre la difficulté des pouvoirs publics de se saisir efficacement, et au moment opportun, de la question de la cybersécurité dans les établissements publics.

Dès l'année suivante, après l'attaque contre l'hôpital de Corbeil-Essonnes, le ministre de la Santé annonçait une enveloppe supplémentaire de 20 millions d'euros pour renforcer la cybersécurité des hôpitaux. L'ANSSI, chargée de piloter ces efforts, supervise alors la mise en place de « parcours de cybersécurité » adaptés aux différents établissements, souvent regroupés au sein des groupements hospitaliers territoriaux (GHT).

D'autres initiatives du gouvernement français ont suivi en réponse à ces incidents, comme la création d'une « task force » en 2022 pour renforcer la maturité du secteur de la santé en matière de cybersécurité. Il est donc clair que ces deux cyberattaques majeures de 2022 ont éveillé **une vraie prise de conscience politique** – très tardive – sur l'importance de la cybersécurité dans les établissements de santé.

## B. PANORAMA DE PROBLÈMES STRUCTURELS DANS LES ÉTABLISSEMENTS DE SANTÉ

Les crises des années précédentes mettent sur le devant de la scène des problèmes déjà identifiés auparavant mais rarement adressés, le plus souvent par manque de moyens et de volonté politique.

### Un manque de personnel dédié à la cybersécurité

De manière générale, les établissements de santé ne disposent pas d'équipes dédiées à la cybersécurité, comme une équipe défensive (Security Operations Center, SOC) ou un Responsable de la Sécurité Systèmes d'Information (RSSI). Trop souvent, c'est le personnel IT de l'institution qui endosse la responsabilité de la cybersécurité, alors qu'il n'en a ni le temps ni les compétences – être qualifié en informatique ne signifie pas être qualifié en cyber.

De nombreux acteurs, comme l'ANSSI, ont déjà alerté sur l'importance du recrutement de talents cyber, avec une politique de rémunération adaptée. Malheureusement, le marché du travail connaît une véritable pénurie de compétences cyber, et ce dans tous les secteurs d'activité.

Selon le rapport 2024 Cybersecurity Skills Gap de Fortinet, 4 millions de nouveaux professionnels seraient nécessaires pour combler l'écart entre offre et demande sur le marché mondial de la cybersécurité. Les profils qualifiés s'arrachent à prix d'or, les salaires sont extrêmement élevés et le secteur de la santé ne peut pas rivaliser.

### Une manque de sensibilisation du personnel soignant aux questions cyber

La formation du personnel sur les bonnes pratiques, telles que la gestion des mots de passe, la reconnaissance des courriels de phishing ou l'application régulière des mises à jour, demeure largement insuffisante. Cette lacune expose non seulement les systèmes informatiques, mais également les patients, à des violations de confidentialité et à des interruptions potentiellement dangereuses des soins. Les formations se font de plus en plus nombreuses, mais le manque de moyens reste un frein majeur. Soulignons tout de même que cette faille structurelle tend à se combler, puisque la sensibilisation du personnel médical aux enjeux cyber a fortement progressé ces dernières années.

### Une complexité organisationnelle du secteur de la santé

La complexité organisationnelle du secteur de la santé français pose des défis significatifs en matière de cybersécurité. Le système de santé français se caractérise par une structure tentaculaire, avec une multitude d'acteurs aux niveaux national, régional et local, ainsi qu'une gouvernance partagée entre l'État et l'Assurance maladie. Cette organisation complexe, associée à la multiplication des logiciels et applications, à la présence de connexions peu sécurisées entre les systèmes d'information des hôpitaux et ceux de leurs prestataires, ainsi qu'au développement des dispositifs médicaux connectés, rend les infrastructures SI particulièrement vulnérables aux cyberattaques. L'installation fréquente de logiciels non approuvés par les services informatiques (Shadow IT) aggrave cette situation.

### Une insuffisance dans le partage de connaissances entre les acteurs

Il existe un manque flagrant d'échanges entre les acteurs du secteur de la santé français. Cette insuffisance de communication et de collaboration se manifeste à plusieurs niveaux : entre les établissements de santé eux-mêmes, entre les institutions de santé et les autorités de régulation, ainsi qu'entre le secteur public et le secteur privé. Ce cloisonnement entrave la diffusion rapide des informations relatives aux menaces émergentes, limite le partage des bonnes pratiques et des retours d'expérience, et freine la mise en place de stratégies de défense coordonnées.

En conséquence, les acteurs du secteur de la santé se trouvent souvent isolés face aux cybermenaces, chacun réinventant des solutions déjà existantes ailleurs ou restant vulnérable à des attaques pourtant connues et maîtrisées par d'autres.

## L'interdépendance des systèmes d'information au sein des Groupements hospitaliers de territoire (GHT)

Les Groupements hospitaliers de territoire (GHT) ont été créés afin d'optimiser la gestion des ressources limitées dont disposent les établissements de santé. La mutualisation des moyens garantit aux GHT une meilleure prise en charge des patients. La prise en compte du manque de personnel compétent a néanmoins conduit à la création d'une vulnérabilité majeure, à savoir l'absence de segmentation dans l'architecture même des systèmes d'information. La segmentation permet d'éviter une interconnexion des systèmes sans barrières de sécurité. Cela permet d'éviter la chute de tout le système d'information en cas d'attaque et de paralyser tous les établissements de santé du GHT.

L'ANSSI a pourtant identifié le problème, et recommande une segmentation des systèmes d'information.

La dette technologique du secteur de la santé crée des failles de sécurité importantes. Les outils utilisés sont souvent vieillissants, avec un cycle de vie d'environ quinze ans. Faute de mises à jour de sécurité, les logiciels deviennent vulnérables aux attaques. Ils ne sont donc plus adaptés pour protéger le capital informationnel qu'ils contiennent face aux attaques qui sont toujours plus sophistiquées.

A noter que le règlement Cyber Resilience Act (CRA), adopté récemment au niveau européen, offre une réponse normative à l'ancienneté des parcs informatiques, en obligeant les fabricants à fournir des mises à jour tout au long du cycle de vie des produits, et à concevoir les outils et les logiciels avec une approche Security by Design, soit dès les premiers stades de la conception.

## L'incapacité d'appliquer les recommandations de l'ANSSI par un manque de financement chronique

L'ANSSI alerte depuis longtemps sur les enjeux et les risques liés aux établissements de santé, et ses recommandations, en contraste avec les moyens réels des établissements de santé, ne peuvent être appliquées par tous. Leur mise en œuvre permettrait aux établissements ciblés de réagir rapidement et efficacement face aux crises et aux attaques.

Les mesures de prévention et de gestion des risques ne sont pas adaptables dans l'état actuel du système de santé. L'inconsidération politique du cyber dans le secteur se reflète dans le manque de financement. Depuis le pic de financement dû au Covid-19, le déficit des établissements de santé repart à la hausse. En 2021, la proportion d'établissements déficitaires était de 52%, contre 42% en 2020. Cette augmentation illustre le déficit chronique de financement subi par la majorité des établissements de santé français.

# II. UN CADRE NORMATIF FRANÇAIS ET EUROPÉEN EN DEMI-TEINTE

Malgré un renforcement du cadre réglementaire, la cybersécurité des hôpitaux français reste fragile. Des lois et directives ambitieuses mais trop généralistes se heurtent à des réalités de terrain complexes, notamment un manque chronique de financement et de personnel qualifié.

## A. LA LOI DE PROGRAMMATION MILITAIRE (LPM) : UN EFFORT FRANÇAIS LOUABLE, MAIS INSUFFISANT

La Loi de Programmation Militaire (LPM) est un texte législatif, adopté tous les quatre à sept ans, qui traduit en chiffres et en objectifs la vision stratégique de la France pour sa politique de défense et de projection de puissance. Elle joue un rôle crucial dans la protection des **Opérateurs d'Importance Vitale (OIV)**, à savoir les organisations publiques ou privées désignées par l'État français comme essentielles pour le fonctionnement du pays et la sécurité nationale. Ces opérateurs exercent des activités dans des secteurs critiques tels que l'alimentation, les transports, l'énergie ou encore – vous l'aurez deviné – la santé.

La dernière LPM en date, qui couvre la période 2024-2030, comporte un volet cyber renforcé, et impose aux OIV un certain nombre d'obligations en matière de cybersécurité, telles que des normes standardisées et l'adoption de mesures de sécurité renforcées pour leurs systèmes d'information d'importance vitale (SIIV). Ces 20 normes se veulent complètes en encadrant l'ensemble du SIIV : gouvernance, gestion des systèmes, des risques et des incidents.

Toutefois, la lecture de la LPM 2024-2030 révèle **deux écueils majeurs en ce qui concerne le secteur de la santé :**

1. **Une absence de financement spécifique** pour la santé ;
2. **Une approche trop généraliste** qui ne prend pas en compte les problèmes structurels du secteur.

En effet, bien que le budget alloué à la cybersécurité ait augmenté de manière significative, passant de 1,6 milliard d'euros (0,54% du budget global) en 2019-2025 à 4 milliards d'euros (0,97% du budget global) en 2024-2030, il reste global et ne prévoit **pas d'enveloppe spécifique pour le secteur de la santé.** Or, ce secteur souffre d'un sous-investissement chronique en matière de cybersécurité, et les établissements de santé manquent cruellement de moyens financiers pour se conformer aux exigences de la LPM.

Ensuite, de par son approche générale, **la LPM ne prend pas en compte les problèmes structurels du secteur** de la santé (manque de personnel qualifié, dette technologique importante, etc.), entravant de fait son adoption. Par exemple, la première étape requise par la LPM, qui est la mise à niveau des systèmes d'information, est déjà irréalisable par les établissements en raison du manque de fonds. Des sanctions sont bien prévues en cas de non-respect des règles (jusqu'à 750 000€ d'amende), mais elles s'annoncent peu dissuasives pour les établissements de santé qui manquent déjà cruellement de moyens financiers ou sont dépendants de l'État financièrement.

## B. L'ÉVEIL EUROPÉEN EN CYBERSÉCURITÉ, LA FRANCE À LA TRAÎNE

La prise de conscience quant à la nécessité de renforcer la résilience numérique des secteurs critiques n'a pas lieu qu'en France. **L'Union européenne a également introduit quatre initiatives réglementaires de taille :**

- le European Health Data Space (EHDS) ;
- la directive NIS2 ;
- la directive Critical Entities Resilience (CER) ;
- le Cyber Resilience Act (CRA).

### Le European Health Data Space (EHDS)

L'Espace européen des données de santé (EHDS) est un règlement européen adopté en mai 2022 visant à créer un espace harmonisé de données de santé dans l'Union Européenne. Il s'agit d'un texte important puisqu'il vise à permettre aux citoyens de contrôler leurs données de santé, d'améliorer la coordination des soins, de favoriser la recherche et l'innovation, et de créer un marché unique pour les dossiers médicaux électroniques (DME).

Cependant, l'EHDS n'est pas un texte spécifiquement consacré à la cybersécurité dans la santé, bien qu'il comprenne un volet cyber axé sur la sécurisation des DME au sein de son système centralisé. Son rôle est ailleurs, et il ne faut pas attendre de lui qu'il améliore la résilience numérique des établissements de santé.

## La directive NIS2

La directive NIS 2 (Network and Information Security) s'inscrit dans le prolongement de la première directive NIS de 2016. Elle symbolise la prise de conscience européenne de la nécessité d'améliorer la résilience informatique des secteurs critiques, auxquels les établissements de santé appartiennent.

## Les œillères de la France face à NIS 2

NIS 2 a été adoptée par l'Union européenne le 10 novembre 2022, et prévoyait prévoit un délai de 21 mois pour sa transposition de le droit national de chaque Etat membre, soit jusqu'au 17 octobre 2024. Cependant, la France ne l'a toujours pas transposée, et selon Vincent Strubel, directeur général de l'ANSSI, aucun contrôle de conformité ne sera effectué avant 3 ans.

Cette absence de transposition dans le droit français s'explique par trois facteurs : l'instabilité politique, le manque de financement et le faible degré de priorité accordé à la cybersécurité.

L'instabilité politique visible en France en 2024 est récente, postérieure à l'adoption de NIS 2 qui offrait un délai de 21 mois pour la transposition. Le manque d'importance accordée à la cybersécurité par le législateur résulte en une absence de transposition, ce qui handicape davantage le secteur de la santé. Cette absence de transposition en droit français entraîne un risque pour la sécurité des patients et du personnel hospitalier, comme nous l'a confirmé Christophe Mattler, directeur de projets au Ministère de la santé, chargé du pilotage du programme CaRE à la Délégation au Numérique en Santé (DNS). Ce nouveau retard pour le secteur de la santé est d'autant plus regrettable que beaucoup d'efforts ont été faits pour combler celui de la dette technologique.

Par ailleurs, même si la directive n'est pas transposée, elle reste d'application directe dans chaque État membre de l'UE, comme le rappelle l'avocat et RSSI Marc-Antoine Ledieu sur son site Technique et droit du numérique.

Ainsi, le domaine de la santé est tout de même tenu de respecter les exigences de NIS 2 sous peine d'amendes administratives pouvant aller jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires annuel. Malheureusement, le secteur de la santé, contrairement à d'autres secteurs comme la banque ou l'énergie, ne ressent pas la pénalité financière comme une menace, car il dispose déjà de très peu de fonds et sa priorité est plutôt de trouver des lits d'hôpitaux. La responsabilité des établissements de santé en France en cas de non-respect d'une obligation NIS 2 semble donc peu dissuasive.

# Feuille de route des programmes cyber

**Union Européenne**

**France**

DEP
Janvier 2021
Plan de financement sur le numérique

Ségur
mars 2021
Plan de financement sur la cybersécurité sur le secteur de la santé

NIS 2
Décembre 2022
Sécurité des Réseaux et des Systèmes d'Information

CER
Décembre 2022
Résilience des Entités Critiques

CRA
Mars 2024
Règlement sur la Résilience Cyber

EHDS
Avril 2024
Espace Européen des Données de Santé

ANSM
Septembre 2022
Un plan de recommandations cyber s ur les dossiers de santé

LPM
Juillet 2023
Programmation militaire r enforcement des entités critiques

CCF
Aout 2023
Etats lieux de la Cour des comptes du financement des Etablissements de santé

CARE
Décembre 2023
Un programme d'accompagnement des Etablissements de santé en cybersécurité

CERT S
Mai 2024
Rapport sur les incidents des systèmes d'information du secteur de la santé

ANSSI
Novembre 2024
Etat de la menace informatique du secteur de la santé

- Portée: tous les secteurs
- Portée :secteur de la santé

## Le manque de considération de NIS 2 à l'égard des particularités de la santé

Au-delà d'une absence de fonds disponibles pour les établissements de santé, NIS 2 ne porte aucune considération aux problèmes structurels de la santé. A l'instar de la LPM, aucune mention spécifique n'est faite des difficultés du secteur de la santé telles qu'elles sont évoquées par l'ANSSI. Les problèmes structurels et la question du financement, qui sont au cœur du sujet, sont complètement mis de côté.

## La directive Critical Entities Resilience (CER)

Le CER est une autre directive européenne adoptée fin 2022, qui aborde elle aussi la question de la résilience des entités critiques. Là où NIS 2 met l'accent sur la résilience numérique, exigeant une gestion proactive des risques et la mise en place de plans de continuité solides, le CER se concentre sur un cadre de résilience global, qui inclut par exemple la sécurité physique des infrastructures.
Malheureusement, le CER fait preuve des mêmes travers que NIS2 à l'égard de la santé : beaucoup d'obligations mais pas de propositions de financement, ainsi qu'une approche multisectorielle qui ne prend pas en compte les spécificités du secteur médical.
Le CER est encore dans l'attente d'une transposition dans le droit français, attendue début 2025. Toutefois, le chaos législatif pourrait retarder les choses, et pour l'instant, peu de consignes claires émanent de l'État français, notamment en ce qui concerne les établissements de santé.

## Le Cyber Resilience Act (CRA)

Le **Cyber Resilience Act (CRA)** complète NIS 2 en se focalisant sur la sécurité des produits et services numériques. Il vise à renforcer la robustesse des produits qui embarquent du numérique au sein de l'UE en imposant des exigences de sécurité aux fabricants.

Le CRA n'apporte pas de solutions aux questions de cybersécurité dans la santé, et ce n'est pas son rôle. En effet, il réglemente donc des produits et non des secteurs d'activité. D'ailleurs, les dispositifs médicaux professionnels sont spécifiquement exclus du périmètre de la loi, puisque soumis aux règlements (EU) 2017/745 et (EU) 2017/746. Les systèmes de dossiers médicaux électroniques (DME) sont quant à eux réglementés par le CRA, mais doivent être évalués selon le Chapitre III de l'EHDS.

Néanmoins, le CRA a **un effet positif indirect majeur** sur la sécurité numérique des établissements de santé : il renforce la sécurité de la chaîne d'approvisionnement IT.

En effet, le faible niveau de cybersécurité des produits numériques, autant logiciels que matériels, est une faiblesse générale au sein de l'Union européenne. Le secteur de la santé ne fait pas exception, comme mis en évidence par le CERT-Santé, le service national français qui se consacre à la gestion des incidents de cybersécurité dans les établissements de santé et les structures médico-sociales. Ce dernier a observé que l'une des principales causes d'incidents dans les établissements de santé était le dysfonctionnement des prestataires IT.

Ce constat s'inscrit dans la droite lignée du rapport Threat Landscape de l'Agence de l'Union européenne pour la cybersécurité (ENISA), qui explique que les **attaques via la chaîne d'approvisionnement IT** sont l'une des principales menaces cyber, tout secteur confondu. Le CRA s'attaque donc à la racine du problème : en rendant les produits numériques plus sûrs au sein de l'Union, il sécurise la chaîne d'approvisionnement IT de tous les secteurs d'activité, le médical compris. Notons que l'Agence nationale de sécurité du médicament et des produits de santé (ANSM) propose également 68 recommandations techniques et détaillées spécifiquement pour les établissements de santé, là où le CRA adresse la chaîne de sous-traitance IT tout secteur confondu.

## C. DES NORMES INADAPTÉES AUX BESOINS SPÉCIFIQUES DES ÉTABLISSEMENTS DE SANTÉ

L'absence de financement chronique et l'approche trop généraliste de la LPM et des normes et directives européennes témoignent d'une certaine déconnexion des réalités terrain du secteur de la santé, et freinent leur mise en œuvre par les établissements, même s'ils en mesurent pleinement la nécessité. Certes, ces textes de loi brandissent la menace de sanctions en cas de non-conformité, mais cela n'a que peu d'effet sur le secteur de la santé.

La plupart des autres secteurs jugés critiques, tels que le bancaire ou les télécommunications, subissent d'autres formes de pression qui les enjoignent à se mettre en conformité, et à investir dans leur propre cybersécurité. Pour la majorité des secteurs d'activité, ne pas se conformer aux exigences cyber des normes nationales et européennes revient à s'exposer à quatre risques :

1. **Des sanctions financières :** les normes prévoient des amendes en cas de non-respect des obligations. Pour NIS 2 par exemple, jusqu'à 10 millions d'euros d'amendes ou 2% du chiffre d'affaire annuel mondial de l'entreprise ;
2. **Le retrait d'agrément :** les entreprises non conformes peuvent se voir retirer leurs autorisations d'exercer temporairement ou définitivement tout ou partie de leur activité ;
3. **Une perte de chiffre d'affaires :** les incidents et les cyberattaques peuvent générer un ralentissement ou une interruption de l'activité économique, et donc un manque à gagner ;
4. **Un risque réputationnel :** une forte médiatisation peut découler d'une atteinte aux systèmes d'information d'une entreprise et de ses conséquences, contribuant à donner une image négative à l'entité cible.

Dans la plupart des secteurs, les acteurs économiques ont donc tout intérêt à se conformer aux obligations de la LPM et des normes européennes en matière de cybersécurité, dans la mesure où les risques encourus pourraient compromettre leurs activités, voire leur survie. En revanche, ces risques n'ont pas les mêmes impacts pour le secteur de la santé.

Ce dernier, et tout particulièrement dans le domaine public, est moins sensible aux menaces de sanctions économiques puisqu'il ne sert pas d'objectifs de rentabilité. Financés par l'État, les établissements de santé qui ne détiennent pas de fonds propres n'ont que faire des amendes administratives. Et quand bien même, il semble saugrenu de sanctionner financièrement des acteurs qui manquent déjà cruellement d'argent.

Les retraits d'agrément au motif d'une politique défaillante en matière de cybersécurité ne concernent pas non plus le secteur de la santé : le caractère vital des activités d'un hôpital rend inconcevable toute interdiction d'exercer.

Aussi, un établissement de santé pourrait difficilement pâtir d'une mauvaise image, génératrice d'une baisse de fréquentation à la suite d'un incident informatique ou d'une cyberattaque – on choisit un hôpital pour la qualité de ses soins, pas pour la qualité de son système informatique. Lorsqu'une entreprise subit une cyberattaque et voit les données de ses clients compromises, elle est montrée du doigt par l'opinion publique comme ayant manqué à son devoir de sécurisation. En revanche, lorsqu'un hôpital est attaqué, l'opinion publique va honnir les criminels mais il est peu probable qu'il accuse l'établissement de ne pas avoir suffisamment investi dans la cybersécurité.

Il ne faut pas s'étonner que la cybersécurité ne soit pas un sujet dont la santé s'empare à bras le corps, puisque la menace des sanctions est inefficace, le financement insuffisant et l'approche sectorielle inexistante. Sur l'année 2023, en matière d'accompagnement en cas de crise, 462 établissements de santé ont déclaré avoir eu un incident informatique, 165 d'entre eux ont demandé un accompagnement du CERT Santé (appuyé par l'ANSSI et le FSSI), seulement 69 ont été suivis par les autorités. Cette prise en charge a baissé de 11,5 %, par rapport à 2022. Une telle diminution témoigne d'une surcharge pour les autorités et un manque de moyens. Cela montre de manière assez évidente que même les structures gouvernementales n'ont pas la capacité à répondre à toutes ces demandes
.

**Pour assurer un passage à l'échelle global de la cybersécurité dans le secteur de la santé, il faut :**

- Des investissements financiers accrus ;
- Une meilleure prise en compte des besoins et contraintes spécifiques des établissements de santé.

# III. UN SURSAUT FRANÇAIS PLOMBÉ PAR DES FINANCEMENTS INSUFFISANTS

La cybersécurité des établissements de santé en France fait face à des défis majeurs, amplifiés par la récente crise du Covid-19 et les exigences européennes. L'incertitude politique et la stagnation budgétaire freinent une anticipation efficace des cybermenaces. Cette section vise à analyser l'efficacité des politiques françaises liées à la feuille de route numérique en santé et au **programme CaRE** (Cybersécurité accélération et Résilience des Établissements).

## A. UNE FEUILLE DE ROUTE 2023-2027 PERTINENTE MAIS PARALYSÉE

L'Europe, grâce au plan Ségur, a tenté de combler le déficit de financement dans les établissements de santé. En réponse, la France a mis en place la feuille de route 2023-2027 et a fixé les objectifs à atteindre. Toutefois, l'instabilité politique freine les projets et aggrave le manque de fonds.

### Les financements européens en matière de cybersécurité dans les établissements de santé

L'Europe a réalisé qu'après la crise de Covid-19, la cybersécurité des établissements de santé des États membres se trouvait dans un état critique et présentait de nombreuses vulnérabilités. Plusieurs pays européens n'ont pas pris conscience de l'importance d'une politique de cybersécurité efficace des établissements de santé. Cette cécité a notamment généré des problèmes de sécurité importants pour les patients, le personnel médical et les établissements de santé français.

Réalisant que les États membres ne seraient pas en mesure d'appliquer les normes européennes sans aide financière, l'Europe a mis en place le **plan Ségur**. Dans le même registre, le **Digital Europe Programme** et l'**EU4Health** sont des aides financières européennes qui visent à pallier aux failles des politiques en matière de cybersécurité dans les États membres. Ces plans de financements contraignent les États membres à adopter un comportement conforme aux exigences de l'Union européenne en matière de cybersécurité dans les ES.

La feuille de route du numérique en santé est la condition essentielle pour percevoir ces financements. À la suite du plan Ségur, la France a donc rédigé une feuille de route du numérique en santé valable de 2023 à 2027. Cependant, l'approche française de ce domaine témoigne d'un tel retard que, quelques mois après seulement, l'argent avait déjà été utilisé pour le combler.

## Les objectifs de la feuille de route du numérique en santé 2023-2027

La feuille de route du numérique, qui répond aux exigences européennes, est une feuille prévisionnelle des objectifs de cybersécurité que le gouvernement souhaite atteindre d'ici 2027 dans les établissements de santé. Elle aborde plusieurs points :

- **Le besoin de former le personnel** de santé aux enjeux du numérique et de la cybersécurité ;
- **Le besoin de mettre en place une certification** pour pousser les établissements de santé à se conformer aux critères de cybersécurité ;
- **La mise en place d'un schéma directeur** en cas de nouvelle crise sanitaire majeure ;
- **Le programme CaRE** ;
- La mise en place d'**exercices de gestion de crise** ;
- Des objectifs relatifs à la **part de budget accordé au cyber** par les établissements de santé.

## Un contexte politique prégnant et un manque de perspective pour l'avenir

L'instabilité politique qui frappe la France fait stagner le ministère de la Santé. Il est évident que les trois changements de gouvernement sur un an ont ralenti l'activité du ministère, et la réalisation de certains objectifs dans le secteur. Malgré tout, il ne s'agit pas d'un problème récent. Les œillères de l'État depuis toutes ces années coûtent aujourd'hui encore plus cher au gouvernement, aux Français et aux établissements de santé.

Après analyse de la feuille de route du numérique en santé, un autre problème émerge : **ses objectifs servent surtout à rattraper la dette technologique et technique** générale dans les établissements de santé. Pour ainsi dire, le gouvernement tente surtout de combler son retard pour que le système ne s'effondre pas, en mettant à jour les systèmes d'information de ces établissements par exemple. En revanche, il n'y a toujours pas de politique proactive et d'investissements tournés vers le futur, qui permettraient d'anticiper les menaces cyber pour l'avenir.

### Une carence budgétaire pour atteindre les objectifs de la feuille de route

D'un point de vue légal, cette feuille de route montre la prise de conscience du politique dans le secteur, bien que tardivement : les problèmes structurels ont été pris en compte et abordés. Le retard induit par la dette technologique et technique est en train d'être comblé. En revanche, la feuille ne s'accorde pas aux réalités des menaces cyber pour l'avenir.

La France possède encore des difficultés pour atteindre les objectifs qu'elle s'est fixée dans ce domaine. Le manque d'argent reste le problème majeur, mais l'instabilité politique que subit le pays depuis plusieurs mois ne permet pas de poursuivre sereinement un travail pourtant essentiel.

Pour autant, ayant déjà utilisé les fonds européens, le ministère de la Santé est contraint de réviser fréquemment ces objectifs. Entre février et mars 2025, une mise à jour conforme aux besoins financiers et au contexte politique sera publiée par le ministère de la Santé. C'est pourquoi il utilise le programme CaRE comme outil, espérant trouver une solution de financement pérenne pour l'avenir. Preuve, s'il en fallait une, que le ministère de la Santé a compris les enjeux cyber du secteur, et ne souhaite pas proposer une solution à court terme.

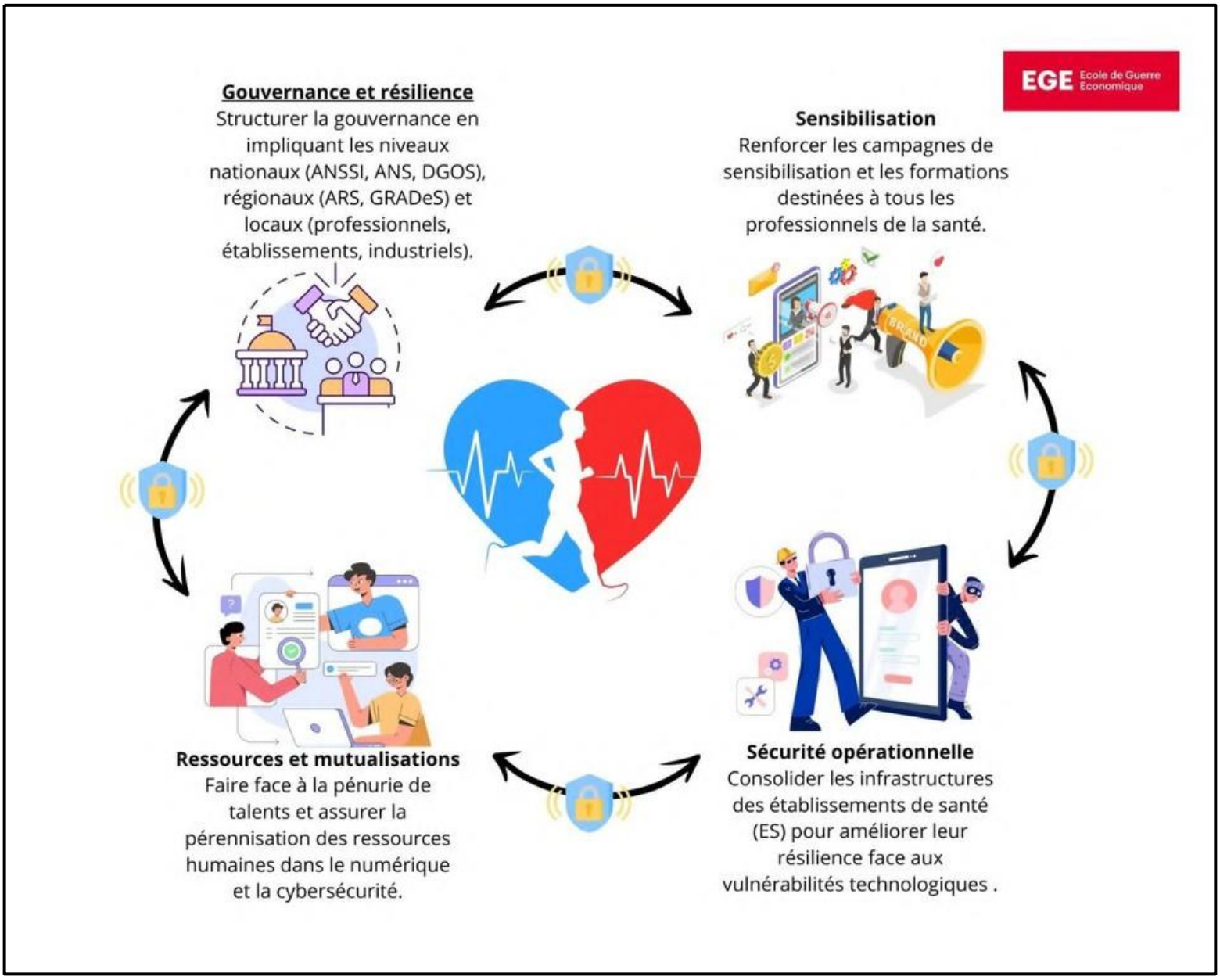
## B. LE PROGRAMME CARE COMME OUTIL DE RATTRAPAGE ET ESPOIR DE FINANCEMENTS PÉRENNES

Le programme CaRE (Cybersécurité accélération et Résilience des Établissements) résulte de l'observation d'une augmentation de la cybermenace dans les établissements de santé.

L'objectif principal du programme est d'accélérer la mise à niveau des systèmes d'information des établissements de santé (ES) afin de renforcer durablement leur résilience. Ce programme a été présenté le 18 décembre 2023 au centre hospitalier de Versailles, lequel avait été victime d'une cyberattaque dévastatrice un an auparavant. Aurélien Rousseau, ancien ministre de la Santé et de la Prévention, et Jean-Noël Barrot, ministre délégué chargé du Numérique, présentent alors le programme CaRE, qui s'inscrit dans la feuille de route du numérique de la santé 2023-2027. Cette démarche est dotée d'un investissement de 750 millions d'ici 2027, dont 250 millions d'euros d'ici 2025.

**Le programme CaRE est fondé sur 4 grands axes :**

- la gouvernance et la résilience ;
- les ressources et mutualisations ;
- la sensibilisation ;
- la sécurité opérationnelle.




De l'autre côté de la Manche, suite à l'attaque WannaCry en 2017, le gouvernement britannique avait alloué 150M£ (180M€) pour renforcer la cybersécurité des systèmes de santé entre 2018 et 2021. Malgré l'ampleur de la cyberattaque ayant frappé son voisin, la France n'a pas su en tirer les leçons à temps pour anticiper et renforcer la sécurisation numérique de ses établissements de santé.

## Un dispositif plébiscité par les établissements de santé

Le programme CaRE, bien que doté d'un budget conséquent, présente encore des dispositifs en cours de développement, dont la mise en œuvre complète est freinée par un manque d'investissement. Les premiers financements ont été accordés pour rattraper les dettes techniques et technologiques générales des établissements de santé français.

Les principaux dispositifs du programme inachevés, faute de financement, sont :

- **Le Plan de Continuité et de Reprise d'Activité (PCRA) ;**
- **La sécurisation des accès de la télémaintenance.**

## Le Plan de Continuité et de Reprise d'Activité (PCRA)

Le Kit national PCRA a été conçu pour mieux anticiper les cyberattaques. Les retours d'expérience démontrent le besoin de simulations d'incidents pour tester la capacité de réaction des équipes en cas d'attaque, et la nécessité d'avoir un plan de reprise d'activités (PRA) et un plan de continuité des activités (PCA). Le premier sert à codifier la marche à suivre en cas d'interruption de l'activité, le second sert à codifier la marche à suivre en cas d'incident, afin que l'activité perdure sans interruption.

De fait, l'absence d'un PCRA (PCA + PRA) mettrait en danger la continuité des soins en cas d'incident, et donc la vie des patients. Cette initiative devrait être généralisée dans 80% des établissements de santé d'ici 2026, à la condition qu'un financement supplémentaire soit débloqué pour la mise en œuvre. L'interruption du Kit national PCRA sera un véritable coup dur pour les établissements.

## La sécurisation des accès de la télémaintenance

La sécurisation des accès de la télémaintenance a été identifiée comme domaine d'investissement prioritaire pour le programme CaRE . L'objectif est de protéger les systèmes d'information des hôpitaux (SIH) contre les intrusions qui pourraient survenir via les connexions à distance. Cependant, l'élaboration des actions et indicateurs pour ce domaine sont encore en cours de co-construction par les parties prenantes de la Task Force cyber française. Un budget de 60 millions d'euros est alloué spécifiquement aux établissements de santé, mais les sources de financement ne sont pas identifiées.

### Problème de financement pour un projet à fort impact

De la même manière que les pouvoirs publics luttent activement contre les inégalités, ils devraient fournir un effort similaire pour garantir la sérénité et la sécurité des trois structures de la santé, que sont le soignant, le soigné et la technostructure. De toute évidence, la pression fiscale à l'œuvre depuis plus de 30 ans n'a jamais empêché de subventionner certains projets sous l'impulsion d'endettements.

Toujours dans l'optique de garantir une sécurité pérenne des établissements de santé, ces socles cyber devraient être chaque année plus ambitieux, avec un financement à la hauteur des objectifs à atteindre. On prend pour exemple le premier appel à projet doté (60M€) qui a été lancé fin 2023 pour soutenir les établissements dans la mise en place de plans de remédiation visant à corriger les vulnérabilités et à diminuer le risque d'intrusion de logiciels malveillants.

L'alignement du programme CaRE avec le programme France 2030 témoigne d'une ambition de transformation numérique durable, bien que la dépendance aux fonds publics soulève des questions sur la pérennité et la faisabilité des projets. Bien qu'existantes, les actions régionales restent en retrait par rapport aux besoins locaux. Enfin, la gouvernance et la coordination à tous les niveaux seront déterminantes pour maximiser l'impact des investissements.

Partant d'un constat général, il est difficile de déterminer quel dispositif serait le plus efficace, car les stratégies de cybersécurité sont en constante évolution pour s'adapter aux nouvelles technologies et menaces. Cependant, l'arbitrage budgétaire, le transfert de moyens, le transfert de compétences du personnel et sa mise à niveau dépendent en grande partie de Bercy, et non du ministère de la Santé (ou des autres ministères potentiellement concernés). Cela génère un véritable rapport de force administratif entre les ministères, loin de toutes les politiques régaliennes. Le cyber fonctionne de manière implacable : pendant que les administrations s'emploient à évaluer l'ampleur des attaques et à rechercher des fonds, les cybercriminels poursuivent leurs actions en exploitant les vulnérabilités.

## C. UNE PROACTIVITÉ NÉCESSAIRE FREINÉE PAR LA LENTEUR CHRONIQUE DE LA FRANCE

Finalement, le manque d'anticipation des menaces de la part des pouvoirs publics doit être souligné. En effet, les nombreux rapports et alertes émis par des agences telles que l'ANSSI avaient mis en garde contre le risque croissant que représentaient les cyberattaques ciblant les secteurs critiques tels que celui de la santé.

Ces avertissements n'ont pourtant pas conduit à des actions suffisamment rapides et concrètes.

La réponse apportée par les pouvoirs publics aux failles de cybersécurité dans le secteur de la santé semble plus réactive que proactive. En effet, bien que des initiatives comme le programme CaRE aient été mises en place, elles ont été perçues comme des réponses relativement tardives aux crises plutôt que des mesures préventives, qui seraient plus appropriées en termes de cybersécurité.

À cet égard, le plan doté de 750 millions d'euros – suivant la feuille de route 2023-2027 – n'est par exemple arrivé qu'après une série d'attaques majeures, alors que les besoins avaient déjà été identifiés bien en amont. Les obligations concernant la cybersécurité n'ont pas fait l'objet de directives claires et adaptées aux réalités du terrain, ce qui induit des disparités importantes dans les niveaux de protection d'un établissement à un autre.

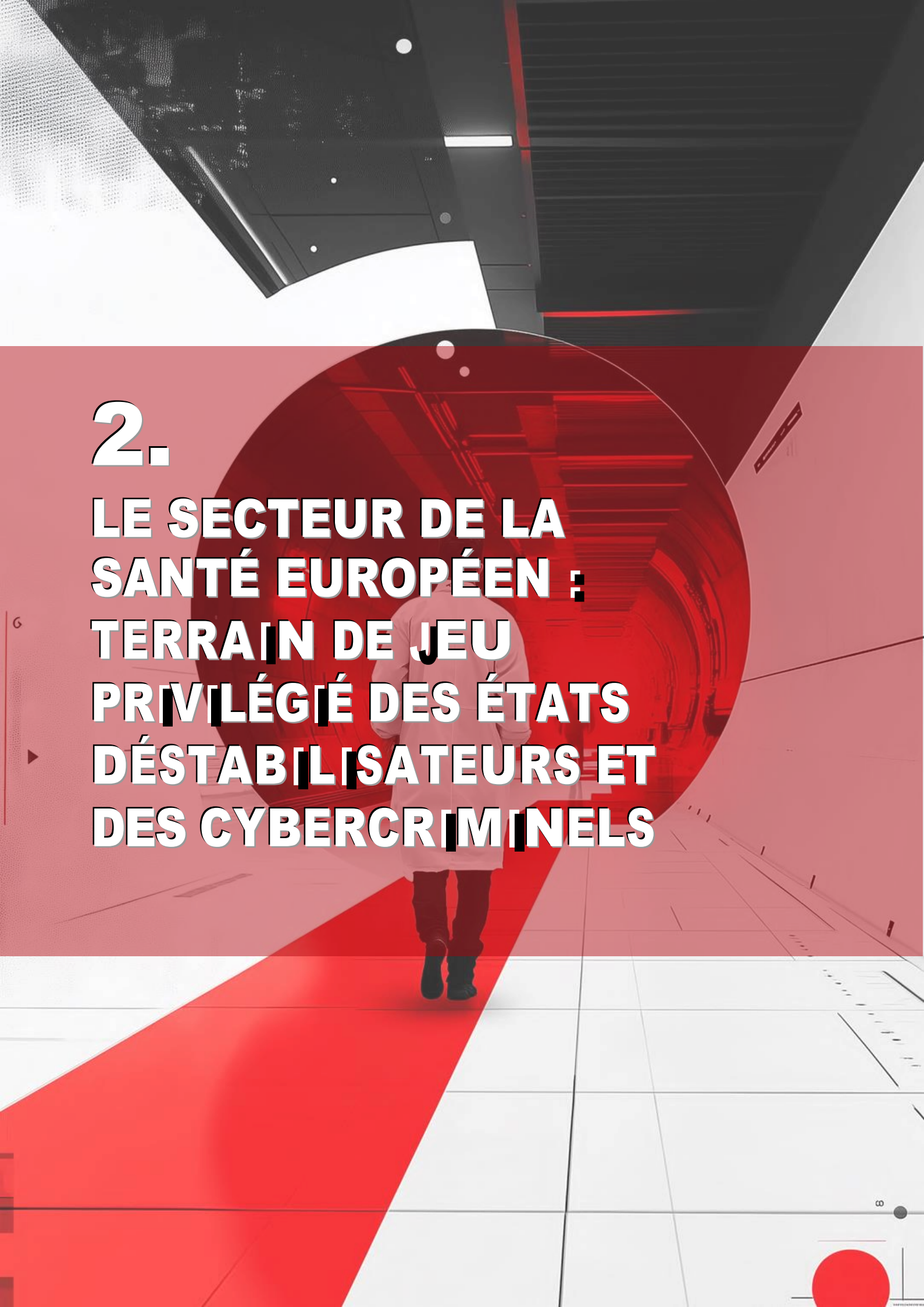
## LA SANTÉ, UN SYSTÈME MALADE

Malgré une prise de conscience politique et l'existence de normes relatives à la cybersécurité, **le secteur de la santé demeure le-laissé-pour-compte des pouvoirs publics.**

Pour que les établissements de santé puissent répondre efficacement aux défis croissants que pose la cybersécurité, **il est crucial que l'État adopte une approche stratégique en la matière.**

Cette dernière doit être allier un financement accru et pérenne, ainsi qu'une prise en compte des **besoins spécifiques** et des **contraintes structurelles** des établissements de santé. En l'état actuel, ceux-ci sont généralement sous-dotés et confrontés à une dette technologique importante, les exposant à des incidents informatiques et des cyberattaques susceptibles de paralyser leur fonctionnement. Ils ont donc besoin d'investissements substantiels pour moderniser leurs systèmes d'information, recruter et former du personnel qualifié, et mettre en œuvre des plans d'action adaptés.

Au lieu de se limiter à une approche réactive, il est nécessaire d'adopter une politique proactive, intégrant une **approche sectorielle** et des f**inancements ciblés à la hauteur des objectifs identifiés.** Une telle démarche permettrait de renforcer la résilience des infrastructures critiques que sont les établissements de santé, tout en assurant la continuité des soins et la sécurité des données.



# 2.

# LE SECTEUR DE LA SANTÉ EUROPÉEN : TERRAIN DE JEU PRIVILÉGIÉ DES ÉTATS DÉSTABILISATEURS ET DES CYBERCRIMINELS

## « Si les hôpitaux français sont attaqués, c'est parce que c'est facile : leur sécurité est nulle. »

Tels sont les mots de Guillaume Poupard, ancien directeur de l'ANSSI, évoquant la problématiques des cyberattaques sur les établissements de santé.

De son côté, le directeur de l'Organisation Mondiale de la Santé (OMS) déclarait devant l'ONU en novembre 2024 que la défense des établissements de santé n'est pas seulement une question de sécurité et de confidentialité, mais bien une question de « vie ou de mort ».

Le constat est dur, et le problème ne peut plus être cantonné au seul domaine de la cybersécurité. Le secteur de la santé, du fait de son caractère vital et régalien, nécessite une adaptation stratégique à l'échelle nationale et européenne. Des dispositifs de réponse aux cyberattaques maillent le territoire européen, mais des attaques protéiformes et toujours plus novatrices continuent de s'abattre sur les différentes structures.

Dans ce contexte, il est nécessaire de dresser un panorama des menaces et des cyberattaques dont les pays européens font l'objet. Leur analyse permet d'aborder l'épineuse question de l'attribution des offensives à des groupes précis, et de leurs motivations supposées.

Comme nous allons le voir, les interprétations économiques des attaques, comme les demandes de rançons, ne peuvent plus constituer la seule grille de lecture des cyberattaques. La dimension géopolitique joue un rôle prépondérant, le secteur de la santé se révélant trop souvent être la victime collatérale de campagnes offensives aux motivations politiques, lancées sans retenue sur l'ensemble du territoire de l'Union européenne.

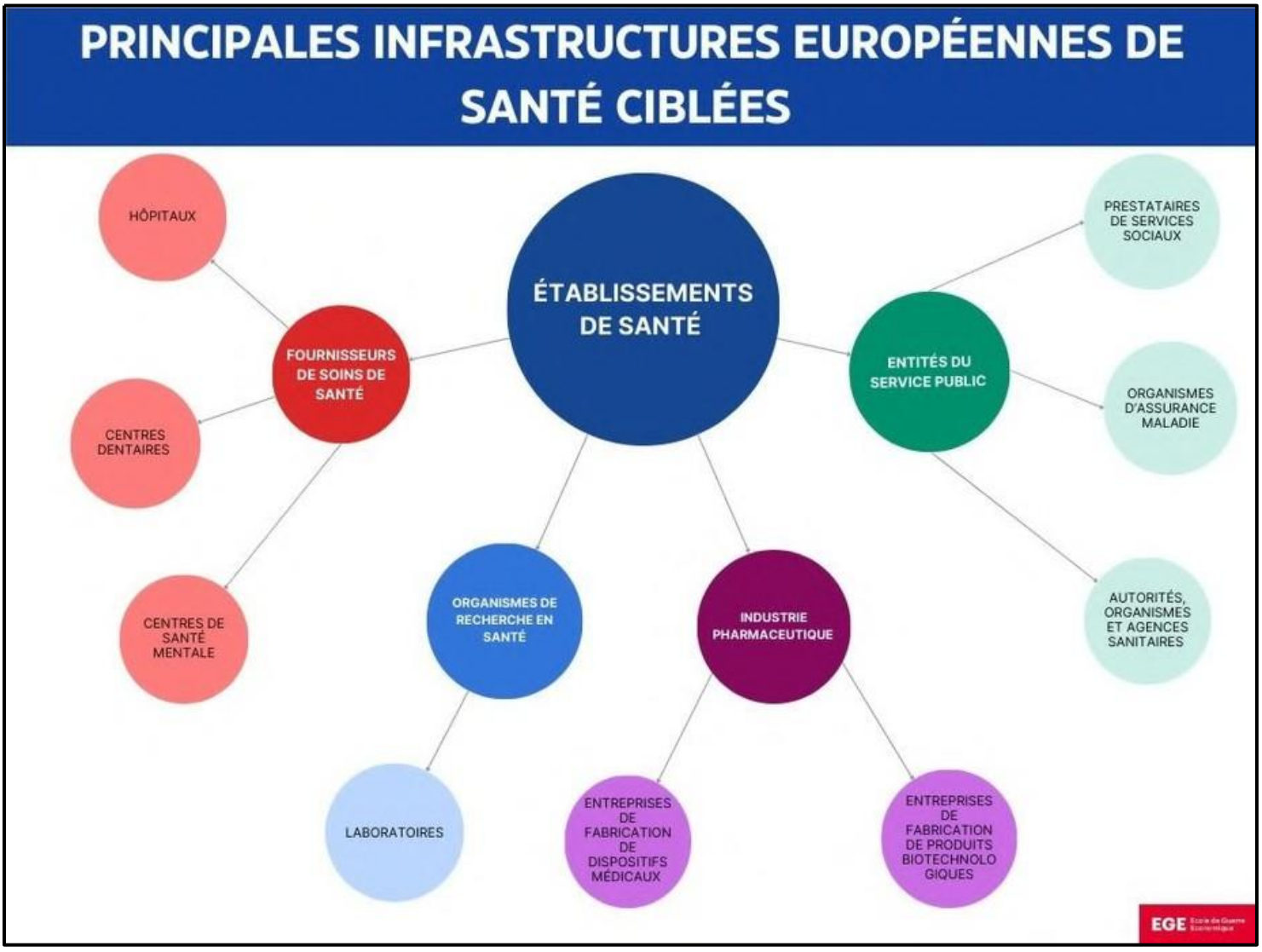
Face à ces menaces, le secteur européen de la santé présente des lacunes visibles qui appellent une harmonisation et un renforcement extrêmement urgents des stratégies européennes et nationales.

# I. LE SECTEUR DE LA SANTÉ EN EUROPE FACE AUX MENACES ET AUX CYBERATTAQUES

Depuis la pandémie de Covid-19, le secteur de la santé est confronté à de nouveaux défis. Tous les établissements de santé, quelle que soit leur taille, font face à une augmentation de cyberattaques protéiformes aux impacts multiples. Pour comprendre l'impact de ces attaques, l'analyse de la typologie de ces cyberattaques, puis de leurs cibles, est une étape nécessaire.

## A. TYPOLOGIE DES ATTAQUES ET DES ACTEURS DÉFENSIFS

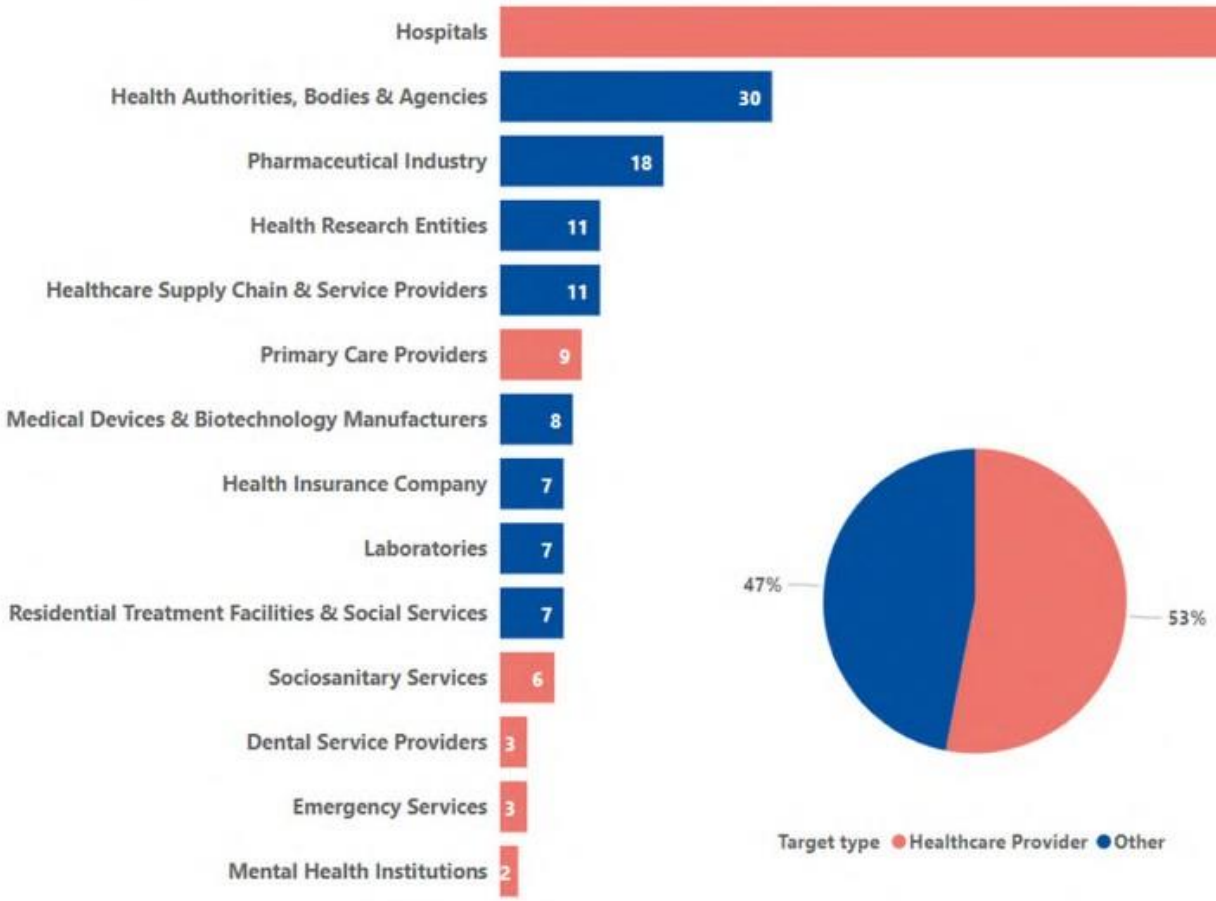
Un rapport de l'ENISA (Agence de l'Union Européenne pour la cybersécurité), intitulé Health Threat Landscape, met en évidence, sur la base des incidents recensés entre janvier 2021 et mars 2023, les cibles privilégiées par les cyberattaques en Europe.



L'analyse de l'ENISA couvre non seulement les États membres de l'Union européenne, mais également des pays voisins tels que la Norvège, la Suisse et le Royaume-Uni.

Cette approche offre une vision assez globale de la proportion et de l'impact des cyberattaques dans le secteur de la santé. Ainsi, selon ce rapport, la majorité des incidents affectent les fournisseurs de soins de santé (53%) du total des attaques) et en particulier les hôpitaux qui sont les cibles de 42% du total des attaques. Outre les fournisseurs de soins de santé, d'autres entités du secteur sont également touchées par les cyberattaques notamment les autorités, organismes et agences de santé (14%) et les entités de l'industrie pharmaceutique (9%).

**Figure 4:** Targets (number of incidents per entity type)




Source : ENISA, Health Threat landscape

Les observations à l'échelle européenne sont corroborées au niveau national. En France, un rapport de l'ANSSI souligne qu'entre janvier 2022 et décembre 2023, 86% des incidents et signalements reçus dans le secteur de la santé concernaient des établissements de santé.

Au vu de cet état des lieux à l'échelle nationale et européenne, un examen des typologies de menaces qui pèsent sur le secteur s'impose.

## Anatomie des menaces du secteur de la santé


**Données chiffrées (source ENISA) :**

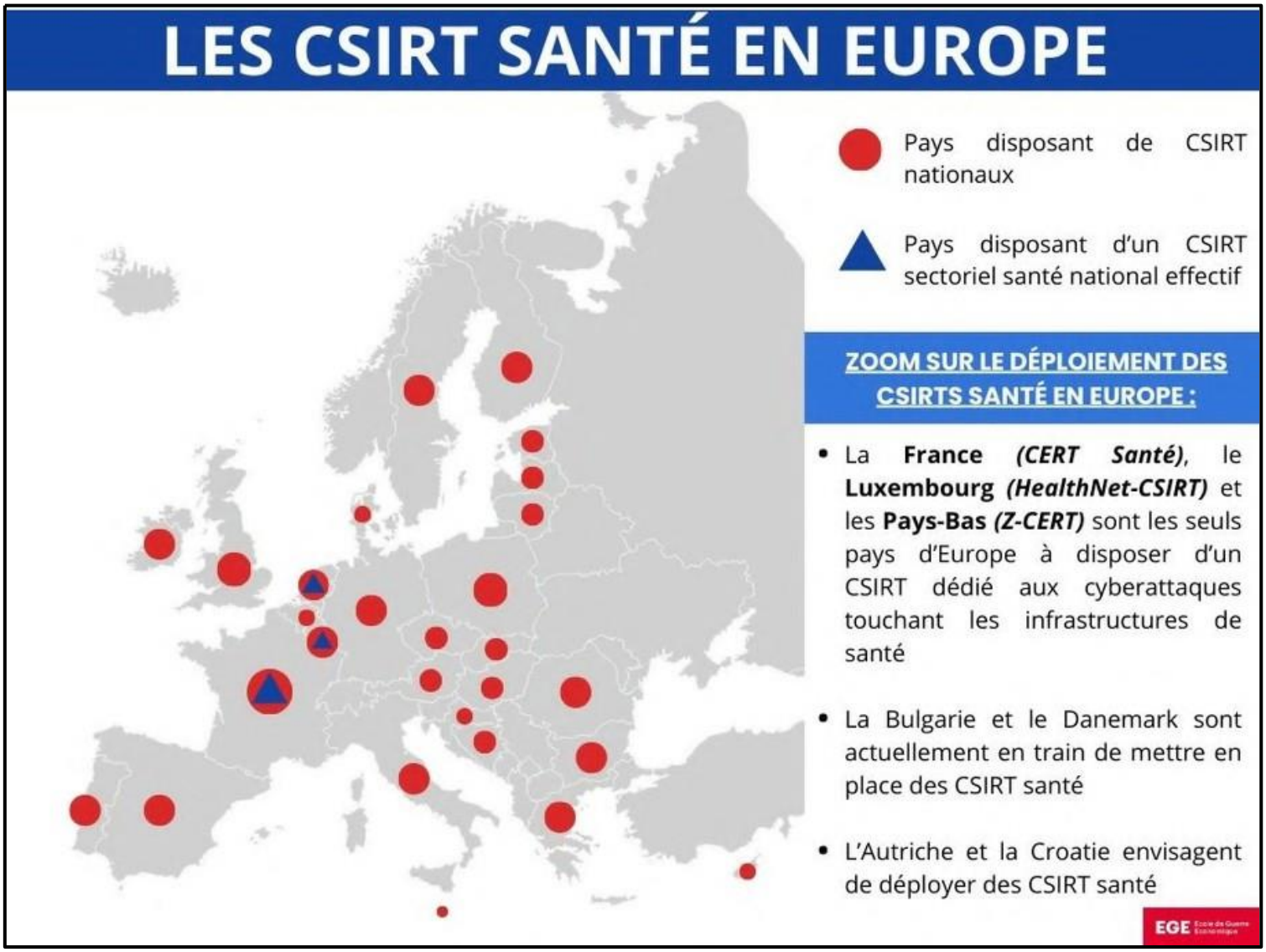
1. Ransomware (54%):
2. Menaces contre les données (46%)
3. Intrusion (13%)
4. Attaques par déni de service (DDoS) (9%)
5. Attaques de la chaîne d'approvisionnement (7%)
6. Malware (5%)
7. Erreurs, mauvaises configurations et mauvaises pratiques de sécurité (4%)
8. Menaces d'ingénierie sociale (4%)
9. Désinformation / Misinformation (1%)

Il est important de noter qu'un incident peut être classé dans plusieurs catégories de menaces, ce qui explique pourquoi le pourcentage total dépasse 100%.

Dans le secteur de la santé, les chances de concrétisation d'attaques sont plus élevées du fait de l'interdépendance des différents acteurs de ce secteur (hôpitaux, opérateurs de tiers payant, prestataires de santé indépendant etc.) et du manque de résilience des systèmes d'informations.

À l'échelle européenne, les ransomwares représentent la menace cyber la plus importante avec 54% des cyberattaques, soit plus de la moitié des incidents observés dans ce secteur vulnérable. À la seconde place on retrouve les menaces contre les données (46%). L'ENISA précise que cette catégorie inclut d'une part les violations de données, conséquences d'actions volontaires et malveillantes, et d'autre part les fuites de données, qui sont elles involontaires, en raison par exemple de mauvaises configurations ou d'erreurs humaines.

## Cartographie des CSIRT

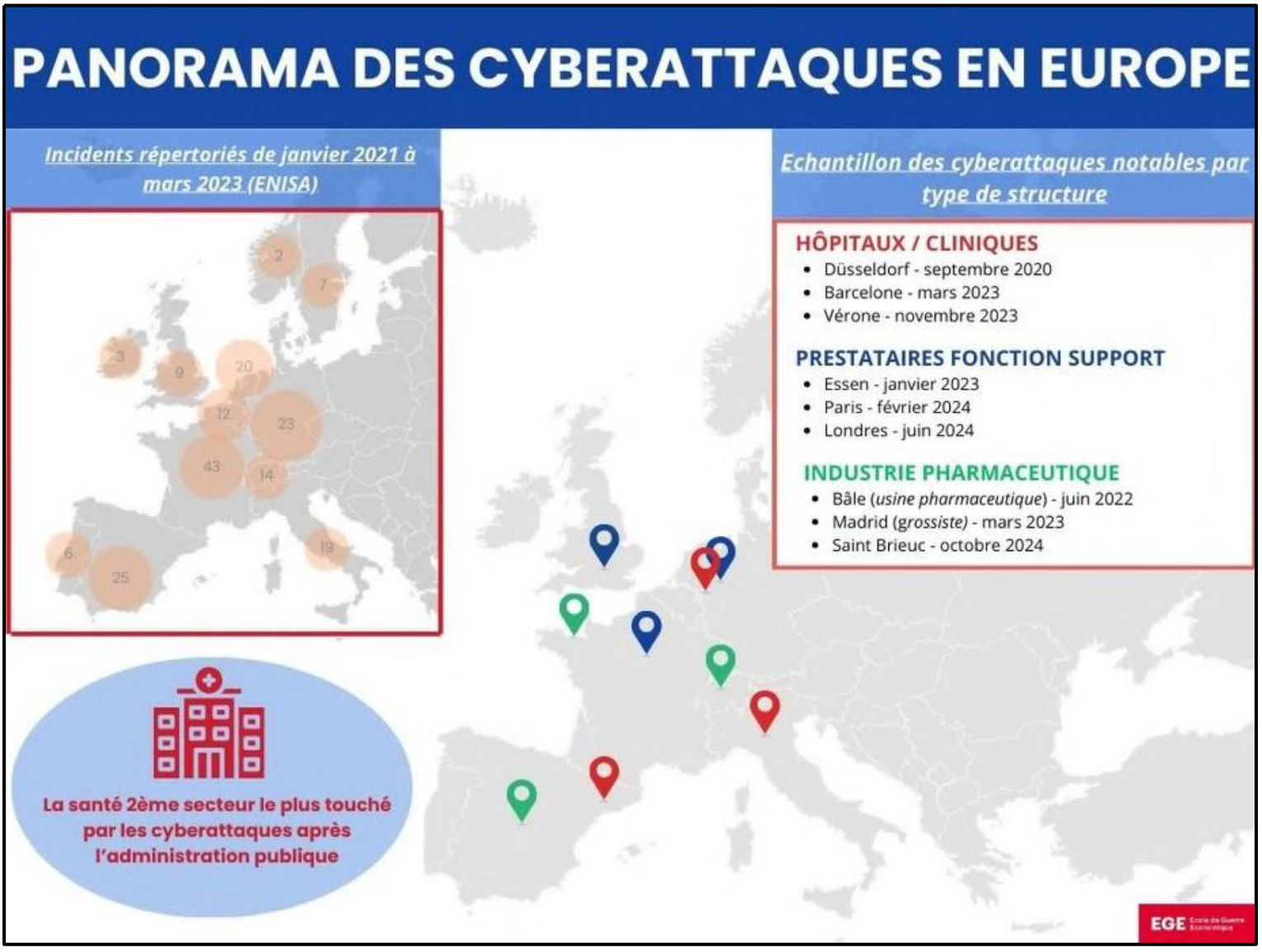


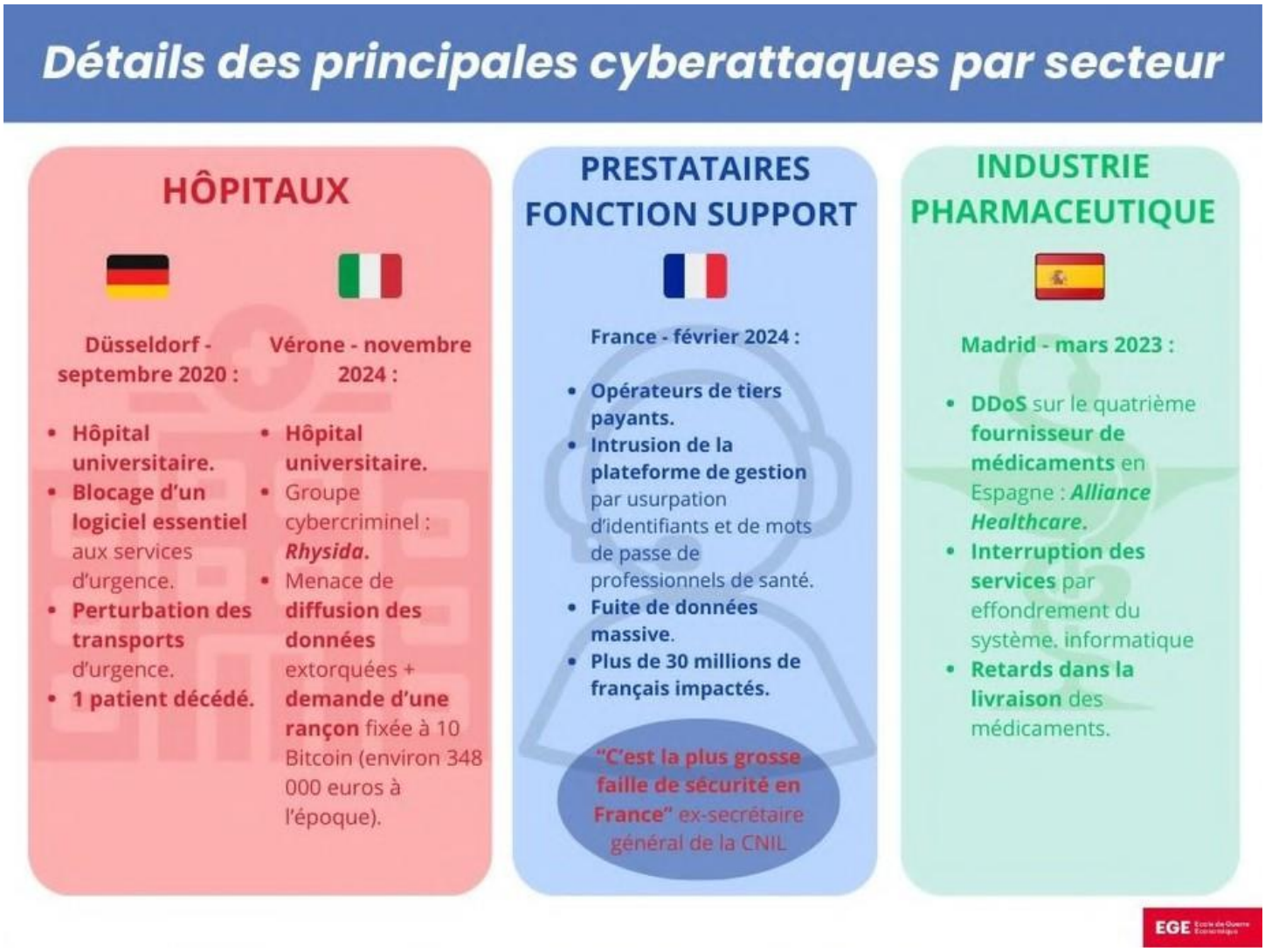
Les CSIRT, ou Computer Security Incident Response Team, sont des équipes opérationnelles chargées de répondre aux incidents cyber. Elles ont pour principales missions de centraliser les remontées d'incidents et apporter des réponses techniques au travers de recommandations. Elles peuvent également tenir à jour une base de données afin d'anticiper les menaces.

Aujourd'hui, si la majorité des pays européens disposent de CSIRT nationaux, seuls trois pays ont déployé un CSIRT spécialisé dans la gestion des incidents dans les établissements de santé : la France, le Luxembourg et les Pays-Bas.

Cependant, le fait que les autres États européens ne disposent pas (encore) de CSIRT sectoriel ne signifie pas pour autant que les incidents ne sont pas gérés : ils sont alors pris en charge par le CSIRT national ou les CSIRT privés mobilisés.

## B. CARTOGRAPHIE DES CYBERATTAQUES NOTABLES POST-COVID À 2024






## C. L'EUROPE ET LA FRANCE : DES CIBLES DE CHOIX

Le secteur de la santé, de par sa nature critique, génère des données sensibles et lucratives pour les cybercriminels. Celui de l'Europe et de la France est particulièrement vulnérable aux cyberattaques pour des caractéristiques qui lui sont propres.

### Les raisons du ciblage particulier du continent européen

Selon le rapport *Health Threat Landscape* de l'ENISA, le nombre de cyberattaques visant le secteur de la santé connaît une relative stabilité depuis 2021, bien qu'une légère augmentation ait été enregistrée au premier trimestre 2023. Il reste néanmoins le **deuxième secteur le plus attaqué après les administrations publiques.**

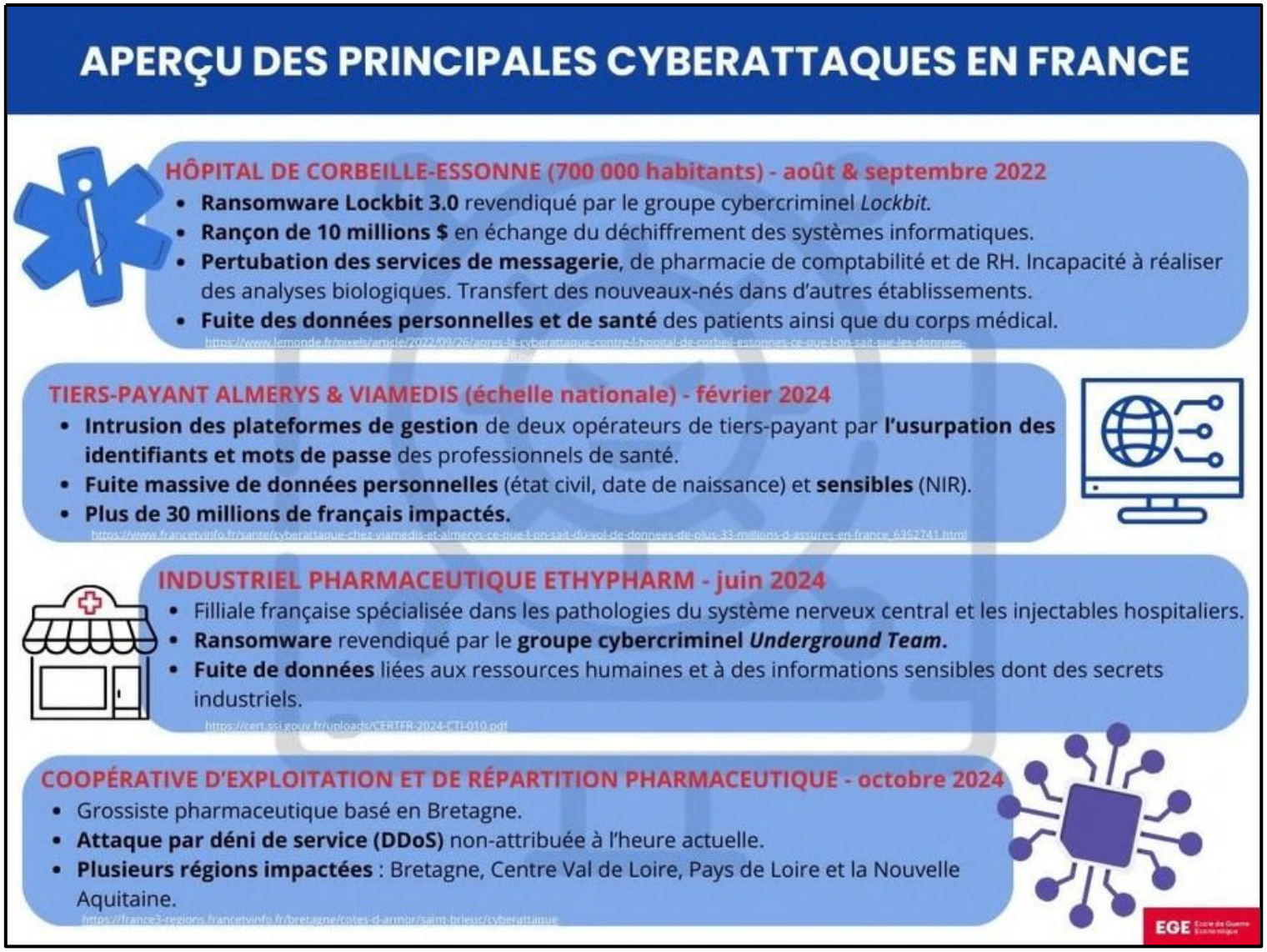
Un certain nombre de facteurs permettent d'expliquer la récurrence des cyberattaques dans le secteur de la santé en Europe :

- **La gestion de données présentant une valeur critique :** Les établissements de santé détiennent des données confidentielles et sensibles, qui intéressent les cybercriminels qui peuvent les revendre à des fins d'extorsion ou de fraude à l'identité.
- **Le niveau de sécurité variable :** Le niveau de sécurité des systèmes informatiques des établissements de santé est souvent hétérogène. Les entités publiques ont, pour beaucoup, des infrastructures anciennes et des ressources limitées pour la cybersécurité ce qui les rend plus vulnérables aux attaques.
- **La pression sur la continuité des services de soins :** Les systèmes de santé doivent fonctionner sans interruption afin d'assurer la prise en charge des patients. Cela peut parfois pousser ces entités à payer les rançons demandées lors d'attaques par ransomware, faisant d'elles des cibles privilégiées pour ce type d'attaques.
- **La dépendance croissante aux technologies :** Le recours croissant à des dispositifs médicaux connectés et des plateformes de télémédecine ainsi que la numérisation dans la gestion des dossiers patients augmentent les surfaces d'attaques pour les cybercriminels.
- **Le contexte géopolitique :** Les cyberattaques d'infrastructures de santé peuvent avoir une dimension politique. Par leurs attaques, les cybercriminels cherchent à déstabiliser des pays en s'en prenant au secteur hautement critique que constitue celui de la santé.

Si tous ces facteurs sont partagés de manière générale par les pays européens, des spécificités sont observables à l'échelle nationale.

### La France : pays le plus touché d'Europe par les cyberattaques

La France conserve depuis quelques années la première position parmi les pays européens subissant des cyberattaques. 71% des organisations françaises tous secteurs compris ont été victimes de cyberattaques. Par ailleurs, l'ENISA recense 43 cyberattaques sur le sol français dans le secteur de la santé entre 2021 et mars 2023.




Plusieurs hypothèses pour expliquer le volume plus important d'attaques en France qu'ailleurs sont envisageables. D'un point de vue politique, il est raisonnable de se pencher sur la position particulière de la France à propos du conflit ukrainien. Les déclarations pro-ukrainiennes des représentants français ont en particulier pu activer des velléités de la part des cybercriminels pro-russes.

Dans la même logique, on pourrait considérer l'arrestation du PDG de la messagerie en ligne Telegram par les autorités françaises en août 2024. Celui-ci était accusé de ne pas avoir mis en place une modération suffisante pour mettre un terme à l'accroissement des activités criminelles s'organisant sur sa plateforme. Les utilisateurs de Telegram ont immédiatement accusé l'État français de censure, et ont appelé à la déstabilisation de ses institutions. Dans la période qui a suivi, plusieurs cyberattaques sur des entités françaises ont été signalées.

Cependant, cela ne signifie pas nécessairement que le nombre ou l'impact de ces attaques sont plus importants que dans les autres pays d'Europe. En effet, il est aussi possible que le niveau de maturité du système français en matière de détection et de signalement des incidents et des attaques soit plus avancé que celui de ses voisins.

En France, les institutions publiques et privées sont tenues de notifier à l'ANSSI tous les incidents de sécurité informatique sur leurs systèmes d'information. Cela implique une phase de détection, rapidement suivie de la qualification de l'incident en tant qu'acte malveillant ou non. La note est transmise au CERT-FR qui par la suite, met en contact le requérant avec un Prestataire qualifié de Réponse à Incidents de Sécurité (PRIS). Ce dernier apportera son aide pour gérer la crise et rétablir la communication interne et externe si les lignes ont été coupées.

Il est important de souligner que les entreprises privées peuvent être tiraillées entre leur obligation légale de signaler tous les incidents et leur volonté de préserver leur crédibilité auprès du grand public. En effet, les conséquences des cyberattaques telles qu'une fuite de données personnelles ou une interruption de services peuvent engendrer une perte de confiance des patients (ou clients) envers les entités attaquées. Certains acteurs du secteur privé peuvent donc avoir tendance à taire les incidents, trop apeurés de passer pour des "mauvais élèves".

De plus, le caractère sensible que revêt le secteur de la santé peut justifier d'une large exposition médiatique et d'une attention accrue du grand public, surtout lors de la pandémie mondiale de Covid-19.

Enfin, selon l'ANSSI, les établissements de la santé ne semblent pas être des cibles spécifiques pour les cybercriminels utilisant des rançongiciels. Ces derniers semblent principalement avoir des motivations pécuniaires, et agissent de manière opportuniste contre des entités issues de tous les secteurs d'activités.

Ce constat ne suffit pas seul à justifier les motivations des cybercriminels qui sont également soumis à des rapports de force qu'une grille de lecture géopolitique permet de mettre en lumière.

# II. LA GÉOPOLITIQUE DES CYBERATTAQUES DANS LE SECTEUR DE LA SANTÉ

Les cyberattaques visant le système de santé européen dépassent largement le cadre des simples attaques contre des hôpitaux ou des centres de santé. En France, comme dans plusieurs pays européens, l'hôpital incarne l'État à travers ses prérogatives régaliennes, notamment le droit de transplanter ou de mener des interventions lourdes.

Cette représentation étatique confère aux établissements de santé une double vulnérabilité : d'une part, leur rôle essentiel dans la protection de la vie humaine et, d'autre part, leur statut d'infrastructure stratégique, en faisant des cibles privilégiées dans des conflits géopolitiques. Cette dimension complexe mérite une analyse approfondie que nous nous proposons d'explorer.

## A. L'ATTRIBUTION DES CYBERATTAQUES ET L'IMPLICATION DES ACTEURS ÉTATIQUES

Depuis 1986, le droit international considère que la principale difficulté concernant l'attribution d'un acte commis par une personne privée ne réside pas tant dans l'établissement de son lien avec un État, mais plutôt dans la collecte de preuves matérielles permettant son identification. L'enjeu majeur est donc d'identifier les groupes privés impliqués et de démontrer leur connexion avec un État. Cette problématique, déjà complexe en droit international général, s'avère encore plus délicate dans le contexte du cyberespace.

L'attribution des attaques est surtout conditionnée par des enjeux politiques. Comme l'affirme Guillaume Poupard, ancien directeur général de l'ANSSI :

***« Toute attribution est une décision politique ».***

Il est donc nécessaire d'étudier les motivations et les attaques des différents acteurs malveillants contre les établissements de santé pour tenter de les affilier à des États.

Voici donc une infographie donnant un aperçu non-exhaustif des groupes cybercriminels liés à des états s'attaquant particulièrement au secteur de la santé européen.

# APERÇU DES GROUPES CYBERCRIMINELS AFFILIÉS À DES ÉTATS CIBLANT LE SECTEUR MÉDICAL EUROPÉEN

[redacted]

*Toutes les sources ayant servi à la construction de ce tableau sont disponibles dans la bibliographie.*

Pour les identifier, on utilise en général le terme Advanced Persistent Threat (APT) qui désigne un type d'attaque perpétré par des groupes professionnels, pilotés et financés par des Etats. Ces groupes combinent des activités lucratives et d'espionnage, visant à obtenir des données sensibles (concernant la recherche médicale entre autres) pour fournir un avantage stratégique à l'État auquel ils sont affiliés. En plus de l'espionnage, ces groupes pratiquent des campagnes de désinformation et de déstabilisation des processus démocratiques. Cette dynamique a été particulièrement visible durant la pandémie du Covid-19, avec des groupes comme APT29 (Cozy Bear, Nobelium), lié à la Russie, APT41 (Winnti Group), affilié à la Chine, Lazarus Group (également connu sous APT38 ou Zinc), associé à la Corée du Nord ou encore APT42 lié à l'Iran.

Certains grands groupes de cybercriminels, tels que LockBit, BlackCat, Anonymous Sudan sont difficilement affiliables à un État. Cela explique qu'ils ne figurent pas dans le tableau ci-dessus, bien qu'ils ciblent également le secteur médical. De plus, il est difficile de distinguer le ransomware utilisé du groupe qui l'exploite. Par exemple, LockBit, identifié comme pro-russe, fonctionne comme une plateforme commerciale de Ransomware-as-a-Service. En échange d'une rémunération, LockBit fournit l'infrastructure et les outils nécessaires à l'utilisation de son ransomware à divers groupes de cybercriminels afin qu'ils puissent, rendant difficile l'attribution à un acteur étatique en particulier.

Dans ce contexte géopolitique complexe, la place de la cyberguerre prend de l'ampleur et de nombreux groupes de cybercriminels mènent des attaques sur le secteur médical afin d'exposer leur soutien à un État. Par exemple, la France, accusée d'apporter son soutien à l'État hébreu, a été visée par une cyberattaque contre un hôpital revendiquée par le groupe Sylhet Gang-Sg. Bien que ce groupe soit difficilement rattachable à un courant politique précis, il manifeste un soutien apparent à des causes pro-russes ou anti-occidentales, reflétant les tensions liées à des conflits géopolitiques majeurs, tels que le conflit israélo-palestinien ou la guerre russo-ukrainienne.

## B. LES MOTIVATIONS FINANCIÈRES : UNE FAÇADE TROMPEUSE

Nous allons maintenant examiner comment les motivations financières servent souvent de paravent, permettant aux États d'agir et de déstabiliser. Dans un premier temps, nous analyserons les raisons pour lesquelles le système de santé est ciblé. Ensuite, nous présenterons quelques exemples de ransomwares potentiellement utilisés par des États. Pour finir, nous conclurons par une étude des modes opératoires de ces cybercriminels liés, voire dirigés, par des États.

## Les centres de santé, au cœur de la déstabilisation entre Etats

L'analyse des cyberattaques ciblant différents secteurs révèle que le domaine de la santé est le second plus touché sur la période de juillet 2022 à juin 2023. Parmi les menaces les plus courantes, comme évoqué précedement, l'utilisation des ransomwares occupe une place importante. L'utilisation de ces logiciels attire notre attention sur les réelles motivations derrière la recrudescence de ces cyberattaques.

Les ransomwares sont employés à des fins lucratives par des groupes criminels organisés, mais également dans des contextes géopolitiques par des entités étatiques présumées. Leur capacité à paralyser les systèmes d'information d'infrastructures vitales, tels que les hôpitaux ou les centres de santé, en font un outil stratégique de déstabilisation. La frontière entre les groupes criminels et les États semble floue et complexe, ce qui fait de ces attaques un nouveau sujet géopolitique.

Pour les acteurs étatiques, l'usage offensif de ces logiciels permet de cibler des infrastructures critiques tout en conservant un déni plausible. Ce concept du droit étasunien consiste à nier sa responsabilité en l'absence de preuves directes. De leur côté, les États victimes sont confrontés à un choix difficile : reconnaître leur difficulté à protéger leurs systèmes d'information, négocier avec des cybercriminels ou subir des interruptions de services aux conséquences potentiellement graves. Mais la vraie difficulté est de prouver – et de dire ou non publiquement – qu'ils ont été victimes d'un État en particulier, car cela tend instantanément les relations diplomatiques.

L'enjeu d'une attaque contre un hôpital ou un centre de recherche dépasse le simple cadre criminel pour devenir une attaque contre l'État lui-même, suscitant des crises politiques majeures. Le personnel en charge de la sécurité informatique des hôpitaux n'a pas toujours conscience du potentiel enjeu géopolitique de l'attaque subie. Il y a donc un fossé d'échelle important entre le personnel de cybersécurité et le groupe de cybercriminel étatique. En effet, les uns par leurs offensives déstabilisent un pays sur la scène internationale en le mettant en difficulté, tandis que les autres se concentrent sur la résolution de problèmes opérationnels.

## Cyberattaques nord-coréennes sur les données de santé.

Pendant la pandémie de Covid-19, la Corée du Nord a intensifié ses campagnes de cyberattaques ciblant les infrastructures de santé, notamment en Europe. Le groupe **Lazarus (APT38)**, affilié au Bureau 121 du renseignement militaire nord-coréen, a mené des campagnes agressives visant des centres de recherche sur les vaccins et des hôpitaux. Ces attaques visaient à voler des données biomédicales sensibles et à exiger des rançons élevées. Des institutions en Asie et en Europe ont été victimes de ces campagnes.

**Kimsuky (Velvet Chollima)**, un autre groupe lié aux services de renseignement civils nord-coréens, s'est concentré sur la collecte de données stratégiques. Il a lancé des campagnes de spear-phishing (Le spear phishing est une attaque ciblée visant à tromper une personne pour obtenir des données sensibles.) ciblant des chercheurs, des ONG médicales et des experts en gestion de crise sanitaire. Ces attaques visaient à obtenir des informations sur la gestion de la pandémie et les stratégies de vaccination en Europe.

En parallèle, **BeagleBoyz**, affilié à Lazarus, a mené des attaques financières ciblées sur le secteur de la santé. Bien que principalement connu pour des piratages bancaires, ce groupe a détourné des paiements liés à l'achat de matériel médical pendant la pandémie, illustrant l'interconnexion croissante entre criminalité financière et espionnage étatique. Ainsi, le cyberespace et donc dans certains cas les systèmes d'informations des établissements de santé deviennent un nouveau champ de bataille pour les États, qui se camouflent derrière des proxies.

## Une Guerre Cyber Déguisée

D'un point de vue géopolitique, il est difficile de prouver que tous les groupes utilisant des ransomwares sont directement affiliés à des États. Cependant, l'analyse des cibles révèle des schémas troublants. Par exemple, certaines attaques évitent systématiquement certains États comme la Russie, tout en ciblant des pays membres de l'OTAN. Ces sélections stratégiques suggèrent que des États pourraient se cacher derrière des groupes cybercriminels pour mener des attaques tout en conservant un déni plausible.

Ce phénomène rappelle l'utilisation de mercenaires dans les conflits armés récents, comme le groupe Wagner pour la Russie en Ukraine ou en Afrique de l'ouest. Dans le cyberespace, les groupes de cybercriminels agissent comme des proxies, créant une guerre asymétrique où les acteurs étatiques sont à la fois les commanditaires passif et parfois même actifs. Les États-Unis ont récemment annoncé que l'État chinois avait recourt à des cybercriminels notamment le groupe APT31. Les cybercriminels suspectés d'être recrutés seraient totalement équipés par les commanditaires et autorisés à toucher l'argent des ransomwares sous réserve de ne cibler que les compétiteurs stratégiques au régime. Cela montre une compréhension plus complète de la cyberguerre qui se joue entre les Etats, et une mobilisation des compétences qui sont encore aujourd'hui très rares.

L'étude des motivations réelles derrières ces attaques force les États et les institutions européens à élaborer une stratégie non seulement défensive mais dissuasive par la même occasion.

# III. UN CHANGEMENT DE PARADIGME NÉCESSAIRE POUR UNE ÉVOLUTION DES STRATÉGIES DE CYBERSÉCURITÉ

Le constat selon lequel la santé est victime de l'extension du champ de bataille cyber exige une adaptation des modes de défense des entités du secteur. Cela nécessite une coordination étroite et une synchronisation des actions, tant au niveau national qu'au niveau européen.

## A. EN EUROPE : UN BESOIN DE RENFORCEMENT DES CAPACITÉS D'INTERVENTION

Le renforcement des capacités de cybersécurité européen doit passer par une harmonisation opérationnelle des pratiques de cybersécurité dans le secteur de la santé, ainsi que par un élargissement des pouvoirs de l'ENISA.

Le besoin d'harmonisation opérationnelle
L'harmonisation et l'amélioration de la collaboration européenne pourrait s'articuler autour de 3 recommandations :

- la création d'une task force cyber européenne ;
- l'amélioration des partenariats publics et privés ;
- la multiplication des CSIRT sectoriels.

### 1. Le besoin d'harmonisation opérationnelle

L'harmonisation et l'amélioration de la collaboration européenne pourrait s'articuler autour de 3 recommandations :

- la création d'une task force cyber européenne ;
- l'amélioration des partenariats publics et privés ;
- la multiplication des CSIRT sectoriels.

## La création d'une task force cyber européenne

En 2023, Charles Michel, alors président du Conseil européen, proposait la création d'une « force cybernétique européenne » qui constituerait un « élément fondamental » de la défense de l'Europe. Ce concept de task force européenne n'est pas nouveau et existe déjà pour plusieurs secteurs dont celui de la santé via la EUHTF (EU Health Task Force) qui est une initiative permettant de fournir une réaction opérationnelle aux épidémies et à la préparation aux crises liées aux maladies transmissibles ou aux maladies d'origine inconnue.

Au niveau européen cette task force cyber pourrait prendre la forme d'une unité de commandement centralisée composée d'experts en cybersécurité, d'analystes du renseignement et de conseillers juridiques, liée à des unités plus petites réparties dans les États membres de l'Union afin de garantir des réponses localisées et une action plus rapide.

**L'objectif de cette task force cyber** pour le secteur de la santé pourrait s'articuler autour de deux axes:

- **Identifier et neutraliser les cybermenaces** avant qu'elles ne frappent via des équipes de cyber threat intelligence.
- **Intervenir pour minimiser l'impact des attaques en cours** via la mutualisation de compétences pour restaurer les systèmes affectés.

## Le besoin d'une collaboration public-privé

L'implication d'acteurs privés dans les stratégies de cybersécurité de la santé est déjà en cours et semble prometteuse. On peut citer les Information Sharing and Analysis Centers (ISAC). Ces organisations à but non lucratif jouent le rôle d'intermédiaire et de base de ressources centralisées pour la collecte et le partage d'informations sur les cybermenaces, les incidents et la diffusion des pratiques de cybersécurité.

La collaboration entre les secteurs public et privé est essentielle pour renforcer la résilience de l'Europe face aux cybermenaces.

De plus, les chercheurs de Digital Europe militent aussi pour la création au niveau européen d'une unité mixte d'experts privée, composée de Responsables de la sécurité des Systèmes d'Information (RSSI en français ou bien CISO en anglais) et d'entreprises de premier plan opérant en Europe. L'objectif serait d'apporter des conseils concernant les stratégies et mesures visant à atténuer de manière proactive les cybermenaces.

Cette approche collaborative permettra, non seulement de renforcer la résilience face aux cyberattaques, mais aussi de promouvoir un marché intérieur sûr grâce à un partenariat public-privé efficace.

### La création de CSIRT sectoriels

Enfin, pour compléter le travail des ISAC, la création de CSIRT dédiés à la santé est une initiative que chaque État membre devrait lancer. Ces organismes pourraient donc épauler les ISAC dans leurs missions et diffuser à plus grande échelle leurs rapports et recommandations.

## 2. Un renforcement des pouvoirs de l'ENISA

Cependant les stratégies d'uniformisation et de renforcement de la collaboration européenne ne peuvent être développées sans une redéfinition du mandat de l'ENISA.

Aujourd'hui le mandat de l'organisme européen consiste à fournir des ressources techniques et humaines pour soutenir les États membres de l'UE, à procéder à des examens des politiques et menaces en matière de cybersécurité dans l'UE et faciliter l'échange de bonnes pratiques entre les États membres.

Ainsi, le mandat de l'ENISA est assez large car l'ambition de la commission lors de sa création était triple :

- **Renforcer** la coopération entre les États membres.
- **Harmoniser** les approches en matière de cybersécurité.
- **Protéger** les infrastructures critiques, les entreprises et les citoyens contre les menaces croissantes dans le cyberespace.

Hors, l'accomplissement de ces objectifs semble complexe au regard de la dotation de l'agence en ressources humaines et budgétaires. En effet, en 2023, elle disposait d'un budget de 44 millions d'euros et employait un peu plus de 100 personnes.

En comparaison, d'autres agences européennes disposent de budgets et de ressources humaines plus importantes, reflétant la diversité de leurs missions. Par exemple l'EMA, agence responsable de l'évaluation et de la supervision des médicaments dans l'UE, disposait en 2023 d'un budget de 417 millions d'euros, avec un effectif de plus de 900 employés.

Cependant, il faut saluer l'efficacité redoutable et le travail de titan abattu par les équipes de l'ENISA, malgré cette faible dotation comparée aux autres agences européennes. L'agence joue un rôle central dans l'amélioration de la sécurité des réseaux et de l'information à travers l'Europe. Le mandat de l'ENISA, qui a amplement prouvé sa valeur, doit maintenant évoluer pour faire face aux menaces pesant sur les secteurs vitaux européens comme la santé.

## Quelles stratégies pour renforcer ses pouvoirs ?

Bien que l'ENISA ait été créée pour renforcer la cybersécurité de l'UE, l'étendue de son mandat l'empêche de jouer un rôle de premier plan dans l'élaboration des politiques et l'attribution des ressources en matière de cybersécurité.

Pour parvenir à un environnement de cybersécurité homogène, le mandat de l'ENISA doit être élargi afin de développer et coordonner de manière proactive les politiques de cybersécurité dans les États membres de l'UE.

Pour ce faire, il est nécessaire que la Commission européenne et les États membres de l'UE reconnaissent l'importance de la cybersécurité dans leurs stratégies de défense commune. Ce faisant, l'UE pourrait reconsidérer sa dotation budgétaire à l'ENISA, en lui garantissant un rôle plus important, via par exemple un pouvoir de conseil sur les initiatives législatives en matière de cyber. L'objectif serait d'améliorer la cohérence et l'impact des politiques en matière de cybersécurité dans l'UE.

De plus, la stratégie du tout réglementaire jusque-là adoptée par l'UE pourrait être amendée. Car en plus de créer du délai dans l'élaboration des corpus législatifs et opérationnels, elle rend complexe la compréhension des responsabilités entre les différents acteurs du cyberespace européen.

Toujours pour les chercheurs de Digital Europe, une révision du mandat de l'ENISA pourrait aider à définir plus clairement les responsabilités et favoriser la collaboration entre les différents acteurs, et donc garantir que les ressources soient allouées efficacement sans que les tâches ne soient dupliquées.

À cette fin, un réexamen du mandat pourrait permettre à l'ENISA de se concentrer sur ses fonctions essentielles. Cela signifie par exemple se désengager de tâches qui peuvent être mieux gérées par d'autres institutions de l'UE ou par les États membres. L'objectif serait d'éviter la redondance et de s'assurer que les efforts de l'ENISA soient dirigés là où ils peuvent avoir l'impact le plus significatif.

Cependant le changement de stratégie de gouvernance au niveau européen ne peut être le seul levier d'action pour limiter les impacts des cyberattaques sur les services de santé. Elle doit s'articuler avec des stratégies nationales plus ambitieuses notamment en France.

## B. LE BESOIN D'UNE STRATÉGIE RENFORCÉE AU NIVEAU NATIONAL

Bien que pris à cœur par les autorités, le sujet de la cybersécurité du secteur de la santé révèle le besoin d'une transformation de la mentalité et des stratégies françaises qui doivent maintenant se concentrer sur le besoin d'une posture proactive de dissuasion, voire de riposte face aux acteurs cyber malveillants.

### 1. Un renforcement du rôle de l'état

Le secteur de la santé est vulnérable face aux cyberattaques en raison de l'interconnexion des acteurs de sa dépendance financière à l'État. Les hôpitaux sont considérés comme des vecteurs d'attaque contre l'État, qui doit donc intervenir davantage dans les efforts de cybersécurité de la santé.

#### Le constat de l'isolement du secteur de la santé

Comme expliqué précédemment, les établissements de santé sont considérés comme des OIV. Cependant, ce secteur présente des caractéristiques uniques qui ne sont pas forcément prises en compte dans les mesures et obligations incombant aux OIV.

Le rapport du CERT-FR de novembre 2024 indique que l'interconnexion et les dépendances entre différents services et établissements peut créer un effet domino si les criminels latéralisent leurs attaques. Ce risque de propagation d'une entité à une autre peut donc créer un « single point of failure » où un acteur moins protégé se fait corrompre et contamine le reste de la chaîne.

La question du financement par les OIV de leur mise en conformité peut constituer un point de rupture. Les frais sont à la charge des opérateurs, contrôlés par l'ANSSI et ils sont soumis à une obligation de résultat. Pour le secteur de la santé, cette logique est contreproductive car la nature du secteur n'est pas la rentabilité et leurs financements dépendent de la volonté de l'État.

Déjà évoquée auparavant, cette fragilité financière couplée aux failles des infrastructures numériques hospitalières font du secteur de la santé une cible de choix pour les cyber attaquants, d'autant plus que la santé est une mission régalienne de l'Etat.

Pour un acteur malveillant, s'attaquer aux hôpitaux est donc un bon vecteur pour déstabiliser et attaquer la France.

Le rôle de vecteur qu'endossent les hôpitaux lors de ces attaques contre l'Etat signifie donc que ce dernier doit être plus présent dans les schémas de cybersécurité des établissements de santé.

### Le besoin d'une intervention positive de l'Etat

La prise en compte du secteur de la santé dans les listes des opérateurs vitaux ou essentiels à la nation est une très bonne chose car l'Etat montre qu'il considère l'importance des soignants dans le bon fonctionnement de la nation ainsi qu'en cas de crise grave.

Néanmoins, les différences d'obligations de sécurité et la problématique du maillage territorial peuvent soit nuire à l'ensemble du plan, soit desservir tout un pan de la population dont les infrastructures de santé ne sont pas à la hauteur en cas d'attaque. En comparaison, les centrales nucléaires sont toutes des OIV et pas juste celles proches de gros bassins de population. Leur classification tient compte des potentiels dégâts sur l'ensemble du territoire en cas d'incident. Les hôpitaux et établissements de soins lourds doivent suivre cette logique.

La prise de conscience de l'administration doit s'accompagner d'une sensibilisation des professionnels de santé sur leur rôle stratégique. Les opérateurs de centrales nucléaires ont conscience des risques et conséquences de leurs activités en cas de cyberattaque réussie. Les soignants et administrateurs doivent prendre conscience du potentiel de déstabilisation et de crise qu'une attaque massive peut représenter.

Pour assurer une vraie cybersécurité des hôpitaux, **l'État doit prendre à sa charge la mise à niveau et les efforts de protection des infrastructures médicales.** Leur criticité pour le pays étant avérée, cette stratégie n'est pas hors des compétences de l'administration.

De plus, il serait judicieux de ne pas cantonner les autorités nationales, telles que l'ANSSI à un rôle de contrôleur et d'accompagnant, mais de les impliquer pleinement dans le pilotage des investissements et des stratégies de cybersécurité des hôpitaux voire intervenir directement pour épauler ou compléter les personnels des établissements.

## 2. Le besoin de la création d'une stratégie ambitieuse de cybersécurité

En comparant les stratégies cyber des Etats liés de manière directe ou indirecte aux attaques des établissements de santé, on peut mettre en avant les raisons du retard stratégique français et donc étudier les propositions pour l'amélioration des capacités de cyber-dissuasion française.

### L'exemple d'autres Etats ayants des stratégies cyber plus ambitieuse

On peut constater qu'au commencement du développement de la culture du hacking à l'aube des années 80-90, il y a eu une absence de prise en compte de cette culture dans la stratégie de défense française, contrairement à d'autres pays. En effet, cette dernière se distingue par une approche institutionnelle et centralisée, axée sur la réglementation, les capacités techniques et la coordination entre acteurs publics et privés. L'idée n'est pas de dire que rien n'a été fait mais plutôt qu'il existe actuellement trois mondes (acteurs cyber offensifs, Etats et entreprises privés) qui sont en interaction/coopération, mais ne communiquent pas bien entre eux ou ne se comprennent pas par manque de synergie.

Mais alors pourquoi certains pays sont plus offensifs dans leurs stratégies cyber ?

Comme démontré plus avant, les pays ciblant majoritairement les établissements de santé européen et français dans le cadre de campagnes de déstabilisation sont la Chine, la Russie et la Corée du Nord. Or si les raisons politiques sont sûrement prioritaires dans l'explication du rôle prépondérant que jouent ces acteurs dans le cyberespace, celles-ci ne constituent pas l'unique raison.

En effet c'est aussi car ces pays ont réussi à intégrer des hauts niveaux de capacités informatiques dans leurs stratégies défensives de secteurs d'importance vitaux mais également dans leurs offensives de déstabilisation. Cela s'explique notamment parce que :

- ces pays ont orienté leurs politiques éducatives vers la dévelopement d'une main d'oeuvre technologiquement qualifiée pour en tirer profit dans la mise en place de stratégie cyber ;
- du fait de l'imbrication de leurs secteurs public et privé, notamment via la création d'un complexe militaro-industriel puissant et travaillant de concert avec les armées nationales, et le développement de fleurons industriels dans les secteurs technologiques et dans l'aérospatiale.

## Le salut par la dissuasion cyber

En France, la stratégie établie peut être résumée par la formule de Guillaume Poupard – oui, encore une – : «la meilleure défense, c'est la défense». Elle reflète le choix d'un modèle distinctif, qui consiste à séparer les missions défensives de celles liées au renseignement et aux capacités offensives, afin de préserver la relation de confiance entre l'ANSSI et les différents acteurs concernés, tels que les opérateurs et les entreprises.

Cependant, certaines militent pour une stratégie de défense plus proactive basée sur le développement des capacités de cyberdéfense visant à détecter et contrer en amont activement les menaces. C'est le cas notamment au Sénat, où les sénateurs Olivier Cadic et Mickaël Vallet ont publié un rapport d'information pour une coordination de la cyberdéfense plus offensive dans la Loi de Programmation Militaire 2024-2030.

L'objectif est notamment d'inciter le gouvernement à adopter une stratégie plus offensive - une « cyber dissuasion » s'appuyant sur les capacités de cybersécurité de l'ANSSI et de caractérisation des attaques informationnelles relevant de Viginum.

Ainsi l'affirmation d'une stratégie de cyber-dissuasion permettrait d'investiguer et détecter en amont des possibles campagnes de cyberattaques étatiques contre des organismes d'importance vitale comme les établissements de santé. De plus, cette stratégie s'inscrit parfaitement dans le cadre français privilégiant le découragement des agressions plutôt que la riposte offensive.

# CONCLUSION.

Le secteur de la santé européen, et français en particulier, se trouve dans une **situation critique** face aux cybermenaces. Malgré une prise de conscience politique et des initiatives louables comme le programme CaRE, la santé reste le parent pauvre de la cybersécurité, minée par un sous-investissement chronique et une approche normative inadaptée à ses réalités.

L'augmentation des cyberattaques depuis la pandémie de Covid-19, menées par des groupes criminels mais aussi par des États hostiles cherchant à déstabiliser, met en lumière les faiblesses criantes du système. Les hôpitaux, cibles privilégiées en raison des données sensibles qu'ils détiennent et de leur rôle vital pour la Nation, sont en première ligne.

La France, particulièrement touchée, paie le prix de son retard. Son approche, principalement réactive, se révèle insuffisante face à des adversaires de plus en plus sophistiqués. Le manque de moyens financiers et humains, la dette technologique importante et l'absence d'une véritable culture de la cybersécurité au sein du personnel médical aggravent la situation.

Un **changement de paradigme** est indispensable. Au niveau européen, l'harmonisation des pratiques, le renforcement du rôle de l'ENISA et la création d'une Task Force cyber européenne dédiée à la santé sont des pistes à explorer. La collaboration public-privé, via des structures comme les ISAC, est également essentielle.

La France doit, quant à elle, revoir sa stratégie. **L'État doit prendre ses responsabilités** en pilotant et finançant la mise à niveau des infrastructures médicales. Une stratégie de cyber-dissuasion, alliant défense proactive et capacité de riposte, est plus que jamais nécessaire.

L'enjeu est de taille. Il ne s'agit pas seulement de protéger des données, mais bien de garantir la résilience du secteur, la continuité des soins et la sécurité des patients. La santé, mission régalienne de l'État, ne peut plus être la **victime collatérale d'une cyberguerre** dont les enjeux sont bien plus importants qu'elle.

Des **investissements massifs** et une **approche globale** tenant compte des besoins et des contraintes structurelles du secteur, et impliquant tous les acteurs, sont les conditions sine qua non pour assurer la résilience numérique de la santé et garantir un avenir plus sûr.

# SOURCES


## 1. Cybersécurité des établissements de santé en France : une prise de conscience tardive des problèmes structurels du secteur

### A. Le réveil politique face aux enjeux de cybersécurité dans les établissements de santé

- Ministère de l'économie, *Cybersécurité : renforcement par le Gouvernement de la protection des citoyens, des administrations et des entreprises*, sans auteur, (18 janvier 2021).
- JP Informatique, *Quels sont les risques en travaillant avec un logiciel non maintenu chez les éditeurs ?*
- IT Social, *La dette technique n'est pas seulement technologique, elle peut être humaine aussi,* Mourad Krim, (20 octobre 2023).
- Le Monde informatique, *Le docteur Macron au chevet de la filière cybersécurité, Jacques Cheminat*, (18 février 2021).
-

### B. Un panorama de problèmes structurels dans les établissements de santé

- CERT-FR, *Bulletin CERTFR-2024-CTI-010 : Rapport sur les menaces cyber pour l'année 2024*, ANSSI, (7 novembre 2024).
- ENISA, *CSIRT Capabilities in healthcare sector,* ENISA, (novembre 2021).
- Direction de la recherche, des études, de l'évaluation et des statistiques, *Les établissements de santé en 2021,* sous la direction de Fabien Toutlemonde, (juillet 2023).

## II. Un cadre normatif français et européen en demi-teinte

**A.** La Loi de Programmation Militaire (LPM) : un effort français louable, mais insuffisant

- CERT-FR, *Bulletin CERTFR-2024-CTI-010 : Rapport sur les menaces cyber pour l'année 2024*, ANSSI, (7 novembre 2024).
- Squad, *Décryptage des régulations LPM, NIS2 et NIST2*, Guillaume TURCAS (23 mai 2024)
- RiskInsight, *L'homologation de sécurité, clé de voûte de la mise en conformité LPM*, 3tienneC@pgras (2017).
- aDvens, *Homologation : quand l'administration donne le ton*, sans auteur (5 février 2024)
- ANSSI, *Consultation publique sur le projet de décret concernant les mesures cyber de la LPM 2024- 2030*, (29/01/2024).
- ANSSI, *Guide d'homologation de sécurité en 9 étapes*, sans auteur, (août 2014).
- Synetis, *LPM : réussir la mise en conformité de ses systèmes d'informations d'importance vitale (SIIV)*, sans auteur, (6 juin 2019).
- Sokem, *LPM : les étapes pour une mise en conformité réussie*, sans auteur, (31 mars 2023).
- ANSSI, *FAQ : systèmes d'information d'importance vitale (SIIV)*, sans auteur, (18 août 2022 mis à jour le 3 décembre 2024).

## B. L'éveil européen en cybersécurité, la France à la traîne

- European Commission, *European Health Data Space*.
- Haas Avocats, *Cyber Resilience act (CRA) : définition, obligations et sanctions*, Gérard Haas et Romain Delangle, (3 octobre 2022).
- Houdart & associés avocats, *Focus sur deux nouveaux référentiels en matière de cybersécurité*, Céline Cadoret, (11 octobre 2022).
- Agence nationale de sécurité du médicament et des produits de santé, *Cybersécurité des DM et DMDIV*, sans auteur, (21 septembre 2022).
- La collection numérique de l'Agence de mutualisation des universités et établissements d'enseignement supérieur ou de recherche et de support à l'enseignement supérieur ou à la recherche, *Sécurité des SI : saison 2, La cybersécurité au cœur de la stratégie de l'ESRI*, sans auteur, (février 2024).
- HarfangLab, *La cybersécurité dans les établissements de santé*, Sarah Salis (4 novembre 2024)
- Mathias Avocats, *Résilience des entités critiques : focus sur la directive dite "REC"*, sans auteur, (15 octobre 2024).
- Journal officiel de l'Union européenne, *RECOMMANDATION DU CONSEIL du 8 décembre 2022 relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques*, sans auteur, (20 janvier 2023).
- Agence numérique en santé, *L'Observatoire des incidents I Portail du CERT Santé*, sans auteur, (14 novembre 2022).
- Assemblée Nationale, *Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à l'espace européen des données de santé*, sans auteur, (2 juin 2022).
- NIS 2 Directive, *Health Sector, Learn how the NIS2 directive affects organizations in the health sector,* sans auteur, (2024).
- Shoosmiths, *It's Final Countdown NIS 2: Implications for the Health Sector,* Sarah Moss, (19 octobre 2023).
- DSIH, *Directive NIS 2 : Comment les établissements de santé peuvent-ils s'y préparer ?* Kévin Delmotte, (14 octobre 2024).
- Axigate Link, *"Plusieurs milliers" d'établissements de santé seront concernés par la directive NIS 2 (Anssi)*, Marion-Jeanne Lefebvre (4 avril 2024).
- Le Monde informatique, *Les premiers pas de NIS 2 sur fond de transposition,* Jacques Cheminat (17 octobre 2024).
- Sigma, *Directive NIS 2 : quels impacts pour le secteur de la santé ?*.(11 juillet 2024) • ANSSI, *La directive NIS 2 en synthèse*.

## C. Des normes inadaptées aux besoins spécifiques des établissements de santé

- Ministère de l'économie, *Cybersécurité : renforcement par le Gouvernement de la protection des citoyens, des administrations et des entreprises*, sans auteur, (18 janvier 2021)
- Info Gouv, *Un plan à 1 milliard d'euros pour renforcer la cybersécurité ?*, sans auteur (18 février 2021)
- file:///Users/user/Downloads/2021_02_210218_dp_cyber_vfinale.pdf
- Rapport du gouvernement, *Cybersécurité, faire face à la menace : la stratégie française*, sans auteur, (18 février 2021)

## III. Un sursaut français plombé par des financements insuffisants

### A. Une feuille de route 2023-2027 pertinente mais paralysée

- L'ARS Auvergne-Rhône-Alpes, *Pilier 5 : le volet numérique du Ségur de la santé,* sans auteur (26 juillet 2023).
- Gouvernement-info.gouv.fr, Construire la France de demain, sans auteur (11 août 2021) L'ARS
- Auvergne-Rhône-Alpes, *Cybersécurité : plan de renforcement dans le secteur de la santé,* sans auteur, (19 octobre 2023).
- L'ARS Auvergne-Rhône-Alpes, *Le Ségur de la santé : transformer le quotidien des soignants.*
- E-santé - Feuille de route du numérique en santé 2023-2027, Mettre le numérique au service de la santé, Agence du numérique en santé.

### B. Le programme CaRE comme outil de rattrapage et espoir de financements pérennes

- Agence du numérique en santé (ANS), *Cybersécurité accélération et Résilience des Établissements (CaRE),* ANS.
- Agence du numérique en santé, *La cybersécurité pour le social et médico-social en 13 questions,* ANS, (octobre 2022).
- Webinaire de l'ANS, *Programme CaRE - Présentation du kit PCRA,* Elodie Chaudron, Nathalie Borgne et Selim Miled,(15 mars 2024).
- IREDIC, *Le programme CaRE : le nouveau plan d'actions du gouvernement pour protéger les hôpitaux face à la cybercriminalité,* Diane Michel, (2 janvier 2024).
- National Audit Office, *Investigation : WannaCry cyber attack and the NHS,* Amyas Morse, (27 octobre 2017).
- NHS England, *Cybersecurity,* sans auteur, (25 mai 2023 mis à jour le 16 août 2024).
- Stormshield, Top 5 des cyberattaques sur les hôpitaux, Marco Genovese, (23 juin 2023).
- Mailinblack, *Quels sont les impacts des cyberattaques sur les hôpitaux ?,* Juliette Pierre, (17 octobre 2024).

## 2. Le secteur de la santé européen : terrain de jeu privilégié des états déstabilisateurs et des cybercriminels

### I. Le secteur de la Santé en Europe face aux menaces et aux cyberattaques

A. Typologie des attaques et des acteurs défensifs

- ENISA. *Enisa threat landscape : health sector,* sans auteur (juillet 2024).
- ANSSI, *Secteur de la santé - Etat de la menace informatique,* sans auteur (7 novembre 2024).

B. Cartographie des cyberattaques notables post-Covid à 2024

- ENISA. *Enisa threat landscape : health sector,* sans auteur (juillet 2024).
- ANSSI, *Secteur de la santé - Etat de la menace informatique,* sans auteur (7 novembre 2024). Cyber
- Management School, *Les pays les plus avancés en matière de cybersécurité* (10 juin 2024). *Les bons*
- *réflexes en cas d'intrusion sur un système d'information - CERT-FR*. (s. d.).
- Franceinfo avec AFP, Cyberattaque chez Viamedis et Almerys : ce que l'on sait du vol de données de plus de 33 millions d'assurés, sans auteur (8 février 2024).

- Cyber Security 360, *Azienda Ospedaliera di Verona : dati in vendita, ma quelli sanitari sono una minima parte*, Dario Fadda (20 novembre 2023).
- Grégoire, C. Après l'arrestation de Pavel Dourov, une vague de cyberattaques cible la France. *Libération*. (2024, août 27).
- NHS England, *Update on cyber incident : Clinical impact in south east London*, sans auteur (26 septembre 2024).
- Sky News, *GP fears patients will suffer harm after NHS cyber attack*, Joshi A. (11 juin 2024)
- Swissinfo.ch., *El gigante farmacéutico Novartis ha sido objeto de un ciberataque,* sans auteur (24 janvier 2024).
- Cinco Días, *Un ciberataque pone en jaque al cuarto mayor distribuidor de medicamentos de España,* sans auteur (22 mars 2023).
- IT Digital Security, *El grupo de cibercrimen Ransomhouse es el autor del ciberataque en el Hospital Clínic de Barcelona*, sans auteur (30 mars 2023).
- Berliner Morgenpost, *Angriff auf Krankenkassen : Sind Gesundheitsdaten sicher ?*, Christiane Rebhan (28 avril 2023 ).
- Tagesschau, *Störungen bei Versicherungen : Cyberangriff auf Krankenkassen-Dienstleister,* sans auteur (27 avril 2023).

## II. La géopolitique des cyberattaques dans le secteur de la santé

A. L'attribution des cyberattaques et l'implication des acteurs étatiques

- Usine-digitale.fr, Covid-19 : Des hackers russes et nord-coréens ciblent la recherche médicale et vaccinale, Vitard.A, (16 novembre 2020).
- 01net.com, Des hackers russes ont tenté de dérober les recherches sur le vaccin contre le Covid-19, Simon-Rainaud.M, (17 juillet 2020).
- Usine-digitale.fr, 58 % des cyberattaques liées à des Etats proviennent de Russie d'après Microsoft, Vitard.A, (13 octobre 2021).
- HSE.ie, Conti cyber attack on the HSE, Commissioned by the HSE board in conjunction with the CEO and executive management team, (3 décembre 2021).
- Cybersecurity And Infrastructure Security Agency CISA, Conti Ransomware Attacks Impact Healthcare and First Responder Networks, FBI, (20 mai 2021).
- American Hospital Association, FBI Issues 'Conti' Ransomware Alert as High-impact Global Attacks Persist against Health Care and Critical Infrastructure, Advancing health in america, (21 mai 2021).
- Cyberveille.esante.gouv.fr, Cyberattaque contre le HCE : les leçons à retenir, Portail du CERT Santé, (29 septembre 2022).
- The hipaa journal, Healthcare Organizations Warned About Evil Corp. Cybercrime Syndicate, Alder.Steve, (31 août 2022).
- Le Monde Informatique, Cyber-espionnage : l'opération Epic Turla cible la France, Gros.Maryse, (7 août 2014).
- Kaspersky, Attaques Epic Turla (alias Snake/Uroburos), sans auteur, (sans date)
- MITRE ATT&CK®, Turla, IRON HUNTER, Group 88, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear, Secret Blizzard, BELUGASTURGEON, Group G0010, sans auteur, (31 mai 2017).

- MITRE ATT&CK®, APT41, Wicked Panda, Brass Typhoon, BARIUM, Group G0096, sans auteur, (23 septembre 2019).
- Global Security Mag Online, Comment la recherche médicale est devenue la cible du cyber espionnage chinois, Luke McNamara, (août 2019).
- Cyberveille.esante.gouv.fr, Mise en garde du H3C contre le groupe cybercriminel chinois APT41, Portail du CERT Santé, (10 octobre 2022).
- MITRE ATT&CK®, MenuPass, Cicada, POTASSIUM, Stone Panda, APT10, Red Apollo, CVNX, HOGFISH, BRONZE RIVERSIDE, Group G0045, sans auteur, (31 mai 2017).
- Netwitness community, The History of APT10, NathanOrth, (16 mai 2023).
- Kaspersky, L'acteur APT Lazarus cible désormais des entreprises en Europe, sans auteur, (23 novembre 2022).
- Citalid, Lazarus Group - Healthcare industry on the radar ?, sans auteur, (17 octobre 2023)
- Usine-digitale.fr, Les hackers nord-coréens de Lazarus se seraient attaqués à des organismes de santé, Defer. A, (28 août 2023).
- Cybersecurity And Infrastructure Security Agency CISA, North Korean Advanced Persistent Threat Focus : Kimsuky, CISA. FBI. Cyber National Mission Force, (27 octobre 2020).
- Cybersecurity And Infrastructure Security Agency CISA, North Korean Advanced Persistent Threat Focus : Kimsuky, CISA, (27 octobre 2020).
- Almond, Les groupes APT, une menace pour les organisations européennes, Almond, (4 mai 2023).
- CERT-XMCO, La France : cible de l'hacktivisme géopolitique, XMCO, (août 2024).


B. Les motivations financières : une façade trompeuse


- Department of Justice, Seven Hackers Associated with Chinese Government Charged with Computer. (2024b, avril 8).
- The Guardian. Sabbagh, D. Hackers accessed vaccine documents in cyber-attack on EMA. (2024b, novembre 8).
- Le Figaro. M Blin, G. Cyberattaques : « Le risque s'accroît avec les tensions géopolitiques » . (2024, 15 juillet).
- Gaubert, E. et Jallat, F. Une analyse de l'impact des cyberattaques sur les établissements de soins. Sécurité globale, N° 35(3), 147-157. (2023)
- Oversoc, Aline Cordier Simonneau, Cyberattaques : quels sont les secteurs d'activité les plus touchés ?» (8 février 2024)
- FBI, Wanted list Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft, ATP10 group, December 20, 2018
- Kempf, O. La France face au numérique : une souveraineté rénovée ? 2018

## II. Un changement de paradigme nécessaire pour une évolution des stratégies de cybersécurité

A. Europe: Un besoin de renforcement des capacités d'intervention


- Ministère de la Santé et de l'accès aux soins, Sécurité des Réseaux Informatiques des établissements de santé : Le gouvernement renforce sa Stratégie, Olivier Véran, (21 février 2021).
- SGDSN, La sécurité des activités d'importance vitale, sans auteur (18 mars 2016).
- ANSSI, Le dispositif SAIV, sans auteur (19 décembre 2023).
- APHP DAJDP, Arrêté du 17 avril 2023 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Établissements de santé » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense (2 juin 2023).


B. Le besoin d'une stratégie renforcée au niveau national


- Epic.*Strengthening healthcare cybersecurity : Focus on implementation, not new legislation - DIGITALEUROPE*. DIGITALEUROPE. (2024, 16 décembre).
- Poireault, K.. *New EU Commission to Unveil Healthcare Cybersecurity Plan in First 100 Days*. Infosecurity Magazine.
- Cesgeo. *Les enjeux géopolitiques et juridiques de l'attribution des cyberattaques*. GeoStrategia - L'agora Stratégique 2.0. (2022, 23 septembre).
- Iribarren, M. I. EU to toughen cyberattack defence strategy for healthcare sector. *Euronews*. (2024, 24 juillet).
- *EU Health Task Force (EUHTF)*. European Centre For Disease Prevention And Control. (2023, 13 novembre).