Veille Newsletter
www.veillemag.com
Le magazine des professionnels de l'information stratégique

Par Jacqueline Sala

Focus Cybersécurité. Mai 2026. Cyberpuissance, intelligence artificielle et infrastructures critiques : les grandes lignes de fracture cyber. Par Yannick Pech

Le mois de mai 2026 confirme une évolution de fond observée depuis plusieurs mois : la cybersécurité ne peut plus être appréhendée comme une simple problématique technique. Elle s'inscrit désormais pleinement dans les rapports de force politiques, économiques et technologiques qui structurent l'environnement international. Derrière la multiplication des vulnérabilités critiques, des attaques par rançongiciel ou des fuites de données, émergent des enjeux plus profonds liés à la maîtrise des capacités numériques, la protection des infrastructures critiques et la souveraineté technologique. Le cas Mythos,
le nouveau modèle d'IA d'Anthropic, la montée des tensions cyber entre États, les alertes visant les infrastructures critiques américaines et la pression persistante exercée sur les collectivités territoriales européennes sont autant d'événements qui consacrent résolument le cyberespace comme champ d'expression de la puissance.

MYTHOS OU L'ÉMERGENCE D'UN PROTECTIONNISME TECHNOLOGIQUE

L'une des actualités les plus significatives du mois concerne le modèle **Mythos**, développé par Anthropic et présenté comme une avancée majeure dans l'identification automatisée des vulnérabilités informatiques.

Au-delà des performances revendiquées par l'entreprise, c'est surtout la politique d'accès retenue — sous contrainte du gouvernement US — qui a suscité de nombreuses réactions. En limitant l'utilisation du modèle à un cercle restreint d'acteurs américains, **Anthropic a ouvert un débat inédit sur**
le contrôle souverain des capacités d'intelligence artificielle appliquées à la cybersécurité, en s'inscrivant *de facto* dans le cadre export des armes conventionnelles et des technologies militaires/duales (**lois ITAR et EAR américaines**).

Cette décision révèle une évolution majeure : les outils IA avancés ne sont plus uniquement considérés comme des innovations commerciales mais comme des **actifs stratégiques susceptibles d'influencer les équilibres de puissance** entre États et entre blocs économiques.

Pour les acteurs européens, l'enjeu dépasse largement la seule question de l'accès à une technologie. Il **interroge la capacité du Vieux continent à conserver une autonomie stratégique** dans un environnement où les capacités de détection, d'analyse et d'anticipation des menaces deviennent des ressources critiques.

L'affaire Mythos marque ainsi l'apparition d'une **nouvelle forme de dépendance numérique**, dans laquelle l'accès aux outils de cybersécurité les plus performants pourrait progressivement devenir un facteur déterminant de souveraineté. Ce qui ne manque pas de rappeler le **cas Palantir** et son emprise sur des acteurs étatiques et privés européens.

LE CYBERESPACE, PROLONGEMENT DES CONFRONTATIONS GÉOPOLITIQUES

Le mois de mai a également illustré la **place croissante du cyber dans les rapports de puissance** internationaux.

L'intrusion attribuée à des acteurs liés au **ministère iranien du Renseignement** (VAJA/VEVAK) contre **l'autorité des transports de Los Angeles** constitue à cet égard un signal fort. S'inscrivant dans un contexte de tensions persistantes entre Washington et Téhéran, l'opération confirme que **les infrastructures civiles demeurent des cibles privilégiées des stratégies de guerre hybride**.

Cette évolution s'observe également à travers les mesures de protection déployées par les autorités américaines à l'approche de la **Coupe du Monde** 2026. Les **alertes répétées visant les automates industriels utilisés dans les secteurs de l'eau et de l'énergie** traduisent la crainte de voir des acteurs étatiques ou criminels exploiter l'événement pour **mener des actions de déstabilisation à forte portée symbolique**.

De fait, le cyberespace apparaît toujours plus comme un champ de confrontation complémentaire aux domaines terrestre, maritime, aérien, spatial ou encore informationnel, de sucroît transerval. Les infrastructures critiques deviennent des cibles stratégiques dont la compromission vise autant la **perturbation économique** que le **sapage psychologique** des populations.

VULNÉRABILITÉS CRITIQUES : UNE COURSE PERMANENTE ENTRE DÉFENSEURS ET ATTAQUANTS

On note actuellement l'accélération du cycle de vie des vulnérabilités.

Plusieurs incidents ont démontré que le délai séparant la divulgation d'une faille de son exploitation active continue de se réduire. Les campagnes automatisées de détection permettent désormais aux attaquants d'identifier et de cibler les systèmes vulnérables dans des délais extrêmement courts.

Parmi les événements marquants figurent la divulgation de **l'exploit YellowKey**, permettant de contourner certaines protections **BitLocker sur Windows 11**, la publication d'exploits **visant PostgreSQL** ainsi que la révélation d'une **vulnérabilité ancienne affectant le noyau Linux**

Ces découvertes rappellent que des composants considérés comme robustes peuvent continuer à receler des faiblesses exploitables pendant de nombreuses années.

Le concours Pwn2Own 2026 **de Berlin** a lui-même illustré cette réalité avec la découverte de **quarante-sept vulnérabilités inédites** affectant navigateurs web, systèmes d'exploitation et solutions de virtualisation. Malgré les progrès réalisés en matière de sécurisation logicielle, **la surface d'attaque continue de croître** au rythme de la **complexification des systèmes** numériques.

FOCUS | LES TENSIONS ENTRE ÉDITEURS ET BUG BOUNTERS AUTOUR DE LA DIVULGATION DES FAILLES DE SÉCURITÉ

L'affaire Nightmare-Eclipse a constitué l'un des épisodes les plus commentés du mois dans la communauté cyber. À l'origine du différend, la **divulgation publique de plusieurs vulnérabilités *zero-day* affectant Windows**, dont certaines déjà exploitées activement avec, parmi elles, la précitée YellowKey.

Microsoft a vivement réagi en dénonçant une divulgation jugée irresponsable et en engageant des démarches visant à limiter la diffusion des preuves de concept (PoC) publiées.

Au-delà de la controverse technique, cette affaire révèle une **problématique plus profonde : celle du contrôle de la vulnérabilité comme levier et ressource stratégiques.** Dans un contexte où les délais d'exploitation des failles se réduisent continuellement, la capacité à révéler, qualifier ou au contraire restreindre la circulation de l'information relative aux vulnérabilités devient un enjeu de pouvoir. Cette séquence illustre ainsi les **tensions croissantes entre éditeurs, chercheurs et plateformes numériques autour de la gouvernance de la sécurité** informatique, à mesure que **les failles deviennent elles-mêmes des actifs stratégiques.**

L'INTELLIGENCE ARTIFICIELLE : ACCÉLÉRATEUR DE DÉFENSE... ET DE MENACE

L'actualité mensuelle met également en lumière les effets ambivalents de l'IA dans le domaine de la cybersécurité. D'un côté, les nouveaux modèles permettent d'automatiser la détection de vulnérabilités, l'analyse de code ou encore l'identification de comportements anormaux ; de l'autre, ils favorisent la production massive de contenus, de rapports ou de scripts dont la qualité reste parfois difficile à évaluer.

Les alertes formulées par plusieurs responsables du développement du noyau Linux illustrent cette problématique. **La multiplication de rapports de sécurité générés automatiquement par des systèmes d'IA tend à saturer les mécanismes traditionnels de traitement des vulnérabilités** et à compliquer le travail des équipes chargées de distinguer les menaces réelles des **faux positifs**

Cette situation révèle un **paradoxe** : les technologies conçues pour renforcer la cybersécurité peuvent également contribuer à mutliplier et diluer l'activité de traitement et d'analyse, et ainsi **encombrer la charge cognitive des défenseurs**.

COLLECTIVITÉS TERRITORIALES : LE MAILLON FAIBLE DE LA CYBERSÉCURITÉ FRANÇAISE

Le mois de mai a également été marqué par plusieurs attaques visant des collectivités territoriales françaises et européennes.

L'incident ayant affecté la **commune d'Eyguières**, revendiqué par le groupe **Qilin**, illustre les **difficultés persistantes rencontrées par les administrations locales** face à la professionnalisation des groupes cybercriminels.

Comme de nombreuses collectivités, **les communes concentrent aujourd'hui des volumes importants de données** administratives, financières et personnelles tout **en disposant demoyens humains et budgétaires souvent limités** pour assurer leur protection. Cette situation crée un **déséquilibre croissant entre la sophistication des attaquants et les capacités de défense** des structures locales.

Les incidents recensés en France, au Portugal, en Allemagne ou au Brésil démontrent que les collectivités constituent une cible privilégiée des *ransomgangs*. Leur **dépendance aux services numériques et leur faible tolérance à l'interruption de service** en font des **cibles particulièrement vulnérables**. Leur résilience passera en premier lieu par l'élaboration de **PCA/PRA** (plans de continuité/reprise d'activité) dédiés.

FUITES DE DONNÉES ET ÉCONOMIE SOUTERRAINE : LE CHAOS INFORMATIONNEL

C'est l'arroseur arrosé. Voilà un événement inhabituel : la compromission d'un *ransomgang*, **The Gentlemen**, l'un des opérateurs les plus actifs et responsable d'environ **10 % de toutes les attaques de rançongiciels** cette année, dont les propres données internes ont donc été piratées et exposées. Cela rappelle, l'attaque — plus légère — qu'avait subie LockBit il y a précisément un an (défacement et extraction de mots de passe administrateurs).

La fuite a révélé des informations relatives à ses affiliés, ses infrastructures (**8 200 lignes de conversations** montrant les **opérations du groupe**, la **gestion de l'infrastructure et les techniques d'intrusion**) et à certaines de ses victimes (secteurs de la santé, industrie, assurances, infrastructures étatiques, et entreprises ayant signé des accords de confidentialité (NDA) avec des géants comme **Sony** et **Barclays**). Elle illustre le niveau de structuration atteint par les organisations criminelles, mais également leur propre vulnérabilité. On sait notamment que le groupe utilise un *malware* écrit en **langage Go** capable de **propagation automatique** — de type ver informatique — à travers le réseau sans intervention humaine, pour chiffrer les données des cibles.

Bien qu'on manque de détails sur l'intrusion, les données suggèrent que le groupe a été **compromis via des identifiants volés sur des équipements réseau** (comme Fortinet) ou à travers **une faille dans leur infrastructure interne**. Un utilisateur sur le forum *Breached* a initialement proposé de vendre les données complètes pour 10 000$ avant de les exposer gratuitement.

Une fois n'est pas coutume : cette fuite fait **le bonheur cette fois desanalystes CTI** (*Cyber Threat Intelligence*), révélant les **TTPs** (tactiques, techniques et procédés) : **tactiques** du groupe, **outils** (comme l'utilisation de dépôts GitHub ouverts) et **méthodes** d'évitement de la détection.

Dans une perspective plus globale, la **prolifération des données compromises** contribue à l'émergence d'un **véritable chaos informationnel** dans lequel **la donnée devient simultanément une ressource économique, un outil de pression et un vecteur d'influence**.

LES TENDANCES DE FOND : DÉPENDANCES ET RÉSILIENCE

Au-delà des événements ponctuels, plusieurs tendances structurantes se dégagent en cette fin de printemps. La première concerne la **vulnérabilité persistante de la chaîne logistique logicielle**. Les incidents observés tout au long du mois montrent que les fournisseurs de logiciels, les bibliothèques *open source* et les prestataires techniques demeurent des cibles privilégiées.

La seconde touche à la **raréfaction des compétences capables de maintenir certains systèmes historiques**. Les **difficultés croissantes à recruter des experts maîtrisant les environnements *legacy*** (systèmes hérités), notamment **dans les secteurs publics et financiers**, créent des fragilités durables. À mesure que ces compétences disparaissent, la capacité à sécuriser certains systèmes critiques se réduit.

Enfin, les débats autour des ***deepfakes*** dans le milieu scolaire soulignent **l'émergence de nouveaux risques sociétaux liés à l'IA**. Les outils de manipulation numérique deviennent accessibles à un public toujours plus large alors même que les **cadres réglementaires peinent à suivre le rythme de l'innovation**

Comme l'a dit le sociobiologiste Edward O. Wilson, « ***nous avons des émotions paléolithiques, des institutions médiévales et une technologie digne des dieux***. »

POUR ALLER PLUS LOIN | MATURITÉ CYBER DE L'UE : DES RAISONS D'ESPÉRER ?

La dernière édition du rapport NIS360 de l'Agence de l'Union européenne pour la cybersécurité (ENISA) révèle une **amélioration notable de la maturité cyber des secteurs critiques de l'UE**, tandis que leur niveau de criticité reste globalement stable. Ce rapport sert d'outil d'évaluation annuel pour les autorités nationales et les décideurs dans le cadre de la directive NIS2.

Évolution de la criticité : la criticité est évaluée selon la pertinence systémique, l'exposition aux risques et l'impact d'une éventuelle perturbation. Les secteurs suivants restent les plus critiques :

- Banque, électricité, aéronautique, spatial et infrastructures numériques (télécommunications, cloud, centres de données) ;
- Nouveautés : le **secteur spatial** rejoint ce groupe de haut niveau, reflétant son rôle croissant dans la société et les dépendances accrues. Le **secteur ferroviaire** voit également sa criticité augmenter en raison de son important rôle dans la logistique militaire et de son exposition croissante aux cybermenaces.

Progrès en matière de maturité : la maturité mesure l'efficacité et la constance avec laquelle les secteurs gèrent les risques et leurs capacités de cybersécurité. On observe une tendance à la hausse grâce à :

- Un meilleur partage d'informations et une collaboration renforcée.
- Une mise en œuvre améliorée des mesures de gestion des risques.
- L'influence de la législation sur la cybersécurité qui stimule les investissements.

Secteurs en progression : trois secteurs sont passés dans la **catégorie "haute maturité"** :

1. Services de confiance ;
2. Aéronautique ;
3. Infrastructures de marchés financiers (IMF).

Quatre autres secteurs ont consolidé leur position dans la **catégorie "maturité modérée"** : gaz, infrastructures routières, maritime et santé.

Méthodologie : l'évaluation adopte une approche globale incluant **quatre dimensions-clés** : la législation et son efficacité, la préparation des entreprises, la capacité institutionnelle des autorités et l'efficacité des écosystèmes sectoriels.

Au bilan, bien que les menaces et les dépendances évoluent (augmentant la criticité de certains secteurs comme le spatial et le ferroviaire), **la réponse collective des acteurs européens en termes de préparation et de conformité s'améliore progressivement**.

PERSPECTIVES

Le mois de mai 2026 confirme que la cybersécurité ne se limite pas à la protection des systèmes d'information. Elle s'inscrit désormais au **croisement de la souveraineté technologique**, de la **résilience des infrastructures** critiques, de la **compétition internationale** et de l'**intelligence artificielle**

L'affaire Mythos illustre les nouveaux **rapports de force fondés sur la maîtrise des capacités numériques les plus avancées**. Dans le même temps, les attaques contre les collectivités territoriales, les infrastructures critiques et les chaînes logicielles rappellent que **les vulnérabilités structurelles demeurent nombreuses.**

La question centrale est celle de la **capacité des États, des entreprises et des territoires à conserver leur autonomie** dans un environnement numérique devenu un espace de puissance à part entière.

Gageons que les progrès mentionnés dans le rapport de l'ENISA soient un oiseau de bon augure.

RÉSUMÉ

1. **Anthropic Mythos** ouvre un débat inédit sur l'accès aux capacités d'IA cyber les plus avancées et sur la souveraineté numérique européenne.

2. **Les tensions géopolitiques** confirment l'intégration du cyber dans les stratégies de guerre hybride et de confrontation interétatiques.

3. **Les vulnérabilités critiques** continuent d'être exploitées dans des délais toujours plus courts.

4. **Le cas Nightmare-Eclipse** est emblématique des tensions croissantes entre chercheurs et éditeurs autour du contrôle des vulnérabilités, désormais considérées comme des actifs stratégiques dans la gouvernance cyber.

5. **L'IA induit un paradoxe défensif :** si elle accélère la détection des menaces, elle sature aussi les équipes de faux positifs, transformant un outil de protection en source de bruit informationnel.

6. **Les collectivités territoriales**, cibles privilégiées des rançongiciels et dépositaires de données sensibles, subissent un déséquilibre croissant entre la sophistication des attaques et leurs moyens de défense limités.

7. **La compromission du groupe criminel "The Gentlemen"** inverse la logique habituelle : la fuite de ses données internes l'expose, offrant aux analystes de renseignement cyber une vue inédite sur les techniques, tactiques et procédés d'un *ransomgang* de première classe.

8. **Trois tendances lourdes** en cette fin de printemps : la vulnérabilité chronique de la chaîne logicielle, la pénurie de compétences pour sécuriser les systèmes historiques, et les risques sociétaux croissants liés aux *deepfakes*.

9. **Le rapport NIS360 de l'ENISA** montre une amélioration de la maturité cyber des secteurs critiques de l'UE, portée par la législation et la collaboration, malgré une criticité stable ou croissante pour le spatial et le ferroviaire. Cette progression témoigne d'une meilleure préparation collective face à des menaces et dépendances en constante évolution.

SOURCES PRINCIPALES

> - **VeilleCyber.fr (actualité mai 2026)**
> - **CERT-FR**
> - **Next.ink**
> - **Euronews**
> - **TechRadar Pro**
> - **Agence Europe**
> - **CISA (infra)** *;* **CISA (WorldCup)**

- **Pwn2Own Berlin 2026**
- **Notebookcheck (MS faces security community)**
- **Computer Weekly (MS hits out over irresponsible disclosure)**
- **OTAN**
- **Financial Times**
- *Publications de sécurité* **Linux** *et* **PostgreSQL** *(mai 2026)*
- **LeMagIT**
- **LeDauphine**
- **Checkpoint Research**
- **Databreaches**
- **ENISA | NIS360-2026 (European Network & Information Security Agency)**

Yannick PECH *est docteur en sciences de l'information-communication, spécialiste du renseignement et de la cybersécurité, détenteur d'une certification de Pentester junior (eJPT) et de la certification EBIOS Risk Manager de l'ANSSI.*
Chargé de cours en géopolitique, intelligence économique, sécurité numérique et OSINT dans le supérieur privé et public, chercheur associé au CEREGE de l'IAE de Poitiers, ancien veilleur-analyste à la Compagnie européenne d'intelligence stratégique (CEIS), consultant-analyste au CRR-FR (OTAN-France) et réserviste opérationnel-spécialiste de l'armée de Terre, il est désormais officier de la Réserve citoyenne de cyberdéfense au sein de la gendarmerie d'Occitanie.

#CyberResilience #DigitalSovereignty #AIThreatLandscape #SoftwareSupplyChain #LegacySystemsRisk #DeepfakeRisks #CriticalInfrastructureSecurity #CyberMaturity #EUCyberStrategy #HybridWarfareDynamics

01/06/2026