OBSERVATOIRE DE L'AUTONOMIE STRATEGIQUE

Observatoire 6 – 5 mai 2026

Etats-Unis :

"L'Europe sans Trump, Ou l'Europe malgré Trump" - Jean Dominique Guiliani, le 5 avril 2026 https://www.jd-giuliani.eu/

Malgré des protections législatives, l'imprévisibilité de Trump neutralise l'efficacité de l'OTAN et la garantie de défense mutuelle envers l'Europe. Ce retrait de fait exauce les vœux de la Russie, forçant les Européens à assumer seuls leur propre sécurité. En s'appuyant sur des alliances élargies (Royaume-Uni, Canada), ils doivent désormais formaliser une solidarité militaire continentale. Cette autonomie stratégique est l'unique réponse possible face à l'accroissement de la menace russe.

"PNT - GPS - GNSS : Gouvernance à réformer, temps à sécuriser, et solutions à déployer avant la prochaine crise, le temps pour agir nous est compté" Stéphane Morico, le 11 avril 2026
https://www.linkedin.com/pulse/pnt-gps-gnss-gouvernance-%C3%A0-r%C3%A9former-temps-s%C3%A9curiser-st%C3%A9phane-morico-zojdf/

La fragmentation du pouvoir et la dépendance au GPS affaiblissent le leadership américain en PNT face aux avancées chinoises et russes. Cette vulnérabilité technologique expose la sécurité et l'économie nationale à des risques majeurs de brouillage et de sabotage. Pour réagir, l'auteur prône une gouvernance unifiée avec un responsable unique et une architecture hybride (spatial, terrestre, fibre). L'objectif est de déployer des infrastructures résilientes sous cinq ans afin de combler ce retard stratégique et protéger le pays.

"Agriculture Department kicks off $300M Palantir deal on IT, national security work", Matt Bracken, Le 22 avril 2026, Federscoop **-** https://fedscoop.com/palantir-deal-with-agriculture-department-usda-farmers/

Le USDA a sélectionné Palantir pour moderniser ses systèmes IT via un accord de 300 millions de dollars, avec le projet « One Farmer, One File » centralisant les données des agriculteurs en une plateforme unique, simplifiant leur accès aux services et réduisant les formalités administratives. Ce projet, axé sur la sécurité des données et sans partage inter-agences, implique des acteurs externes comme DOGE et vise à renforcer la résilience des chaînes d'approvisionnement et la protection contre la fraude.

France :

"Au ministère des Armées, le réarmement informatique passe par des cloud", Reynald Fléchaux, le 1 er avril 2026 https://www.cio-online.com/actualites/lire-au-ministere-des-armees-le-rearmement-informatique-passe-par-des-cloud-16940.html

Le CND centralise les compétences IT des Armées pour accélérer la transition vers des clouds souverains et sécurisés. Doté d'un budget d'un milliard d'euros, il vise une montée en gamme technique pour migrer 1 400 applications. L'objectif est de réduire la dette technologique tout en limitant l'externalisation pour garantir la maîtrise des données. Ce virage stratégique cherche

à concilier agilité opérationnelle et souveraineté numérique malgré des défis organisationnels majeurs.

"Souveraineté numérique : L'État jette Microsoft hors de ses systèmes critiques et accélère la reprise en main de ses données les plus sensibles" - Alice Vitard, le 9 avril 2026 https://www.usine-digitale.fr/souverainete/souverainete-numerique-letat-jette-microsoft-hors-de-ses-systemes-critiques-et-accelere-la-reprise-en-main-de-ses-donnees-les-plus-sensibles.6QKIJYRCVJGYXMI7B54U7GRUIA.html

L'État français a décidé d'exclure les solutions Microsoft de ses systèmes critiques pour garantir sa **souveraineté numérique** et protéger ses données sensibles. Sous l'impulsion de la DINUM, les administrations doivent migrer vers des infrastructures certifiées **SecNumCloud** et des logiciels européens. Cette stratégie vise à éliminer la dépendance aux lois extraterritoriales américaines tout en favorisant l'écosystème technologique local.

Intelligence artificielle

AI Act, RGPD, Data Act : "il est temps de considérer la réglementation européenne comme une arme plutôt qu'un obstacle", Pascale Déchamps, le 31 mars 2026

https://www.lesechos.fr/idees-debats/cercle/ai-act-rgpd-data-act-il-est-temps-de-considerer-la-reglementation-europeenne-comme-une-arme-plutot-quun-obstacle-2223094

L'UE doit transformer ses régulations (AI Act, RGPD) en outils stratégiques offensifs plutôt qu'en simples barrières administratives. S'inspirant du lobbying américain, les entreprises européennes sont incitées à influencer activement les futurs standards numériques mondiaux. L'usage de la DG COMP est préconisé pour rééquilibrer la concurrence face aux géants technologiques et protéger l'autonomie régionale. L'objectif final est de faire de l'Europe un architecte des marchés numériques mondiaux pour garantir sa souveraineté économique.

"Interdiction de deepfakes sexuels, reports sur la conformité… Ce qui change dans l'IA Act", Marina Alcaraz, le 31 mars 2026 https://www.lesechos.fr/tech-medias/intelligence-artificielle/interdiction-de-deepfakes-sexuels-reports-sur-la-conformite-ce-qui-change-dans-lia-act-2223290

Le Parlement européen a adopté le 26 mars 2026 deux mesures clés de l'AI Act : l'interdiction des deepfakes sexuels non consensuels, avec une exception pour les systèmes d'IA dotés de mesures de sécurité robustes. Parallèlement, les délais de conformité ont été repoussés pour soulager les entreprises européennes. Le marquage des contenus générés par IA est exigé à partir de novembre 2026, et les systèmes "à haut risque" bénéficient de reports jusqu'à août 2028.

Anthropic ne publiera pas Claude Mythos : une IA jugée trop dangereuse en cybersécurité - Charlotte Rabatel, le 9 avril 2026 https://www.solutions-numeriques.com/anthropic-ne-publiera-pas-claude-mythos-une-ia-jugee-trop-dangereuse-en-cybersecurite/

Anthropic renonce à diffuser largement son IA **Claude Mythos**, jugée trop performante pour découvrir et exploiter de manière autonome des failles de sécurité critiques. Ce modèle capable de créer des cyberattaques complexes restera réservé à des partenaires de confiance pour des missions de défense. Parallèlement, le programme **Project Glasswing** est lancé pour renforcer la sécurité des logiciels mondiaux face à cette nouvelle menace.

"Claude Mythos : trop puissante, l'IA est-elle devenue trop dangereuse ?", Victor Storchan, Le 15 avril 2026,

https://legrandcontinent.eu/fr/2026/04/15/claude-mythos-trop-puissante-lia-est-elle-devenue-trop-dangereuse/

L'auto-amélioration des agents IA (comme Claude Mythos) accélère leur développement tout en exposant entreprises et laboratoires à des risques cyber inédits (serveurs non sécurisés, attaques sur la supply chain). Entre compétitivité économique (modèles propriétaires, réduction des coûts) et menaces croissantes (exfiltration de données, zero-day), la maîtrise sécurisée de l'IA devient un impératif urgent.

"Les impacts d'Anthropic Claude Mythos sur les RSSI", Cynthia Brumfield, Le 14 avril 2026, https://www.lemondeinformatique.fr/actualites/lire-anthropic-bloque-l-acces-a-openclaw-pour-des-abonnes-a-claude-99848.html

Le projet Glasswing d'Anthropic, révélant les capacités de l'IA comme Claude Mythos à détecter et exploiter autonomement des vulnérabilités en quelques heures, marque un tournant dans la cybersécurité, exacerbant l'asymétrie entre attaquants et défenseurs. Les experts de la CSA et de l'AISI alertent sur l'urgence pour les RSSI de renforcer leurs défenses (correctifs, contrôles d'accès, collaboration) face à des attaques désormais plus rapides, accessibles et automatisées. Cette évolution structurelle impose une refonte des stratégies de sécurité, intégrant l'IA tant comme menace que comme levier de défense.

"OpenAI défie Claude Mythos avec GPT-5.4-Cyber", Dominique Filippone, Le 15 avril 2026

https://www.lemondeinformatique.fr/actualites/lire-openai-defie-claude-mythos-avec-gptet-8209-54-cyber
99931.html?utm_source=ActiveCampaign&utm_medium=email&utm_campaign=NL+LMI+Selection+19042026&ep_ee=5d746af879ec59c7bc74b03d9c1f1ef3d3d905e9&vgo_ee=eNMzSlc%2FBA03rQjFWLaSKGGiTO0jb3E9GChyUIaAvWRRw%2BCcKBASSIdV%3AYzPdtPPmHmTlnLDpEmy5xtzOEuT%2FbGKS

OpenAI dévoile GPT-5.4-Cyber, un modèle d'IA conçu pour la cybersécurité, capable de détecter des malwares et des vulnérabilités sans accès au code source. L'accès à ce modèle est restreint via le programme Trusted Access for Cyber pour éviter les mauvais usages, avec une ouverture à un millier d'experts et des centaines d'équipes de sécurité. Les performances des

modèles d'OpenAI en cybersécurité sont mises en avant, avec des scores élevés aux tests CTF et CVE-Bench, et le succès de Codex Security et Codex for Open Source, ayant permis de corriger des milliers de vulnérabilités. La compétition entre Anthropic et OpenAI s'intensifie, avec des implications majeures pour les RSSI et les équipes de sécurité, qui doivent adapter leurs stratégies face à ces nouvelles capacités.

Union européenne :

"Sovereign washing : « C'est qu'il y a un marché qui est en train de se créer », Eric Haddad (Numspot)" - Charlotte Rabatel, le 7 avril 2026 https://www.solutions-numeriques.com/sovereign-washing-cest-quil-y-a-un-marche-qui-est-en-train-de-se-creer/

Le "sovereign-washing" désigne l'utilisation opportuniste de l'argument de souveraineté par des fournisseurs cloud pour séduire un marché européen en quête d'indépendance. Cette tendance masque souvent des dépendances technologiques persistantes sous un vernis marketing de localisation de données. Pour contrer ce phénomène, les acteurs européens appellent à une définition plus rigoureuse et opérationnelle de la souveraineté numérique. L'objectif est de protéger l'économie locale et la sécurité des données face aux menaces juridiques et techniques étrangères.

"Dépendance numérique : l'Europe sous influence américaine ?",CASSINI, le 8 avril 2026

https://www.linkedin.com/posts/cassini_d%C3%A9pendance-num%C3%A9rique-leurope-sous-influence-activity-7447523666994552832-j2cN?utm_source=share&utm_medium=member_desktop&rcm=ACoAADfwNwIBhTWvD20gFm7am_VSQhE-Jc8P2i4

L'Europe est ultra-dépendante des géants américains dans le numérique : 99,8 % des IA conversationnelles (ChatGPT), 95 % des systèmes d'exploitation (Android, Apple) et 70–88 % des réseaux sociaux (Meta, X). Seules des alternatives comme TikTok (chinois) ou Mistral AI (européen) résistent marginalement, tandis que les solutions souveraines (Qwant, Ecosia) peinent à dépasser 1 % de part de marché. Cette dépendance géopolitique expose l'UE à un risque de paralysie en cas de décision unilatérale de Washington, malgré des initiatives comme le DMA ou Gaia-X. Un fossé persistant entre les ambitions européennes et la réalité du marché.

"Les plateformes continuent d'analyser les messages malgré l'incertitude juridique en Europe", Camille Suard, le 8 avril 2026

https://www.solutions-numeriques.com/les-plateformes-continuent-danalyser-les-messages-malgre-lincertitude-juridique-en-europe/

Les géants tech (Google, Meta, Microsoft) maintiennent l'analyse automatisée des messages privés malgré la fin du cadre européen temporaire, s'appuyant sur leurs propres règles plutôt que sur la loi. Ce flou juridique crée un dilemme : protéger les utilisateurs contre les contenus illicites ou respecter leur vie privée, sans cadre clair. Cette pratique, désormais intégrée à leurs

services, concerne aussi les entreprises utilisant leurs outils (ex. : Microsoft 365), posant la question de la transparence et du contrôle sur ces analyses.

"Digital Omnibus", Stéphane Morico, Le 28 avril 2026
https://www.linkedin.com/feed/update/urn:li:activity:7454765224752082944/

En février 2026, l'eurodéputée Aura Salla (PPE), ex-lobbyiste anti-RGPD et anti-AI Act chez Meta (2020-2023), est nommée rapporteure du Digital Omnibus, un texte adopté en mars 2026 qui reporte les échéances de conformité de l'AI Act (de 2026 à 2027-2028). 7 ONG dénoncent un conflit d'intérêts et une capture réglementaire, tandis que seuls 8 États membres ont désigné leur autorité de contrôle. Les régulateurs alertent sur un affaiblissement des garde-fous contre Big Tech, avec des risques de réduction de responsabilité et de transparence.