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

Par Jacqueline Sala

Focus Cybersécurité. Novembre 2026. Infrastructures critiques, cyberactivisme prorusse et intelligence artificielle : un mois sous le signe de la déstabilisation numérique. Yannick Pech

Le mois d'octobre 2026 illustre une tendance forte : la cybersécurité s'inscrit au croisement des tensions géopolitiques, de la protection des infrastructures essentielles et la maîtrise des technologies numériques. En témoignent les attaques revendiquées par des collectifs prorusses contre des ports, entreprises de défense et institutions françaises, les compromissions de systèmes réfrigérants de grandes surfaces ou encore les vulnérabilités critiques affectant des composants logiciels largement déployés...



> *Dans le même temps, l'intelligence artificielle franchit une nouvelle étape : en plus de concourir à la découverte de vulnérabilités techniques et à l'assistance des chercheurs en sécurité, elle est également envisagée comme un moyen d'action offensive autonome. Derrière ces événements se dessine une même problématique : l'hyper-dépendance des organisations à des systèmes interconnectés dont la compromission peut produire des conséquences très concrètes : économiques, opérationnelles et parfois physiques.*

LE CYBERESPACE COMME PROLONGEMENT DES TENSIONS GÉOPOLITIQUES : LES INFRASTRUCTURES FRANÇAISES EN LIGNE DE MIRE

Le mois d'octobre a été marqué par une campagne de cyberattaques revendiquées par le collectif prorusse NoName057(16), visant plusieurs organisations françaises. Ports maritimes, entreprises du secteur de la défense, transporteurs et institutions publiques figurent parmi les cibles annoncées dans le cadre de l'opération menée sous le mot d'ordre #OpFrance.

Le grand port de Marseille, le port atlantique La Rochelle, plusieurs compagnies maritimes ainsi que des acteurs industriels comme Eurenco, GICAT ou Gaztransport&Technigazontnotammentétécitésdanslesrevendicationsducollectif.LeM-CERT,centrederéponseauxincidentscyberdusecteur maritime français, a d'ailleurs diffusé une alerte le 14 octobre, signalant des attaques par déni de service distribué (DDoS) en cours ou susceptibles d'être lancées de manière imminente. Le ciblage du Secrétariat général de la défense et de la sécurité nationale (SGDSN), rapporté à la suite d'un incident survenu le 13 octobre, renforce la dimension institutionnelle de cette séquence d'attaque.

Il convient toutefois de distinguer les revendications des attaquants des incidents effectivement corroborés. Les attaques DDoS cherchent principalement à rendre indisponibles des serveurs Internet (avec impact indirect sur les serveurs Web) ; elles ne signifient pas nécessairement que les systèmes internes ou les infrastructures physiques ont été compromis. Aucune interruption majeure des opérations portuaires n'a été publiquement établie. De même, si NoName057(16) affiche ouvertement son soutien à la Russie, les éléments disponibles ne permettent pas d'affirmer que ces opérations ont été directement commanditées par le Kremlin.

Cette campagne rappelle néanmoins la place prise par le cyberactivisme dans les stratégies de déstabilisation. Même lorsque les effets techniques restent limités, la multiplication des revendications et le ciblage d'organisations symboliques entretiennent un climat de pression sur les institutions et les secteurs stratégiques. La menace est d'autant plus sensible qu'elle s'inscrit dans un contexte européen où les infrastructures de transport, d'énergie et les administrations demeurent régulièrement visées par des opérations à motivation (géo)politique.

SUPERMARCHÉS : QUAND UNE CYBERATTAQUE PERTURBE DIRECTEMENT LA CHAÎNE DU FROID

L'un des incidents les plus marquants du mois concerne les systèmes de réfrigération de plusieurs grandes surfaces françaises. Dans la nuit du 11 au 12 octobre, des installations pilotées à distance ont été compromises, provoquant des dysfonctionnements dans la gestion de la température et des cycles de dégivrage. Des magasins, notamment plusieurs enseignes de la grande distribution, ont dû jeter d'importantes quantités de produits surgelés à la suite de ces perturbations.

L'alerte publiée le 12 octobre par le CERT-FR confirme l'existence de nombreuses compromissions de contrôleurs à distance utilisés dans les installations frigorifiques. Plusieurs familles d'équipements sont concernées : les séries AK-SM et AK-SC de Danfoss, les superviseurs Copeland xweb et Dixell xweb. L'ANSSI recommande notamment de supprimer leur exposition directe à l'Internet, de vérifier les configurations, de rétablir les accès au moyen d'un VPN sécurisé et d'appliquer les mises à jour préconisées par les constructeurs.

L'affaire met en lumière la fragilité structurelle des environnements industriels connectés. Des équipements conçus pour assurer une fonction technique précise — ici, le maintien de la chaîne du froid — deviennent des points d'entrée potentiels lorsqu'ils sont accessibles depuis l'Internet sans protections suffisantes. La compromission ne se limite alors plus à une atteinte à la confidentialité d'un système : elle peut entraîner des pertes matérielles, des perturbations commerciales et des conséquences directes sur l'activité voire l'intégrité physique des personnels et des clients (certains dispositifs réfrigérants ont vu leurs systèmes instrumentés de sécurité détournés et occasionner des élévations de température dangereuses, menant parfois à des départs d'incendie). C'est la propriété d'intégrité puis, par cascade, de disponibilité qui a été visée, avec un objectif de déstabilisation via un impact psychologique, et de désorganisation à travers une attaque cyber-physique.

Une question reste en suspens : une vulnérabilité du reste qualifiée (CVE-2025-41450, score CVSS : 8,2) de certains contrôleurs Danfoss (2765 ; faiblesse d'authentification sur des versions antérieures de la série AK-SM 8xxA) avait été identifiée dès mai 2025 par l'entreprise israélo-américaine Claroty. Cette faille n'aurait néanmoins pas fait l'objet de corrections généralisées (*patching*) de la part des entreprises concernées. En tout état de cause, en se plaçant du côté de la distribution, il faut imaginer les ruptures opérationnelles que cela aurait engendré le cas échéant et l'impact commercialassocié.Toutefois,l'ANSSIn'apasimputélevecteurtechniquedescompromissionsàcetteCVE.L'incidentillustredoncavanttoutles risques liés à l'exposition d'interfaces de gestion industrielles (OT), aux carences en termes de *patching* et au maintien en condition opérationnelle (MCO, et aussi de sécurité — MCS) d'équipements insuffisamment sécurisés.

ATTAQUE CONTRE UN SOUS-TRAITANT : LA CHAÎNE DE CONFIANCE FRAGILISÉE

Le 13 octobre, le groupe luxembourgeois Solutions30 a confirmé avoir subi un incident de sécurité ayant pu entraîner la consultation ou la divulgation non autorisée de certaines données relatives à ses clients. L'entreprise, qui intervient notamment dans l'installation et la maintenance d'équipements télécoms et de compteurs communicants, a indiqué avoir déposé plainte et engagé les démarches de notification auprès des autorités compétentes.

Un acteur malveillant a revendiqué le vol de 10,38 millions de fiches contenant notamment des noms, adresses et numéros de téléphone. Ce volume et la nature exacte des informations dérobées n'ont toutefois pas été confirmés par l'entreprise. Solutions30 n'a pas non plus précisé publiquement le nombre de clients concernés. Ces derniers doivent être informés individuellement.

L'incident souligne une nouvelle fois la vulnérabilité de la chaîne de sous-traitance. Les prestataires techniques disposent souvent d'informations détaillées sur les clients finaux et interviennent directement à leur domicile ou dans leurs infrastructures. Une compromission de leurs systèmes peut ainsi exposer indirectement les utilisateurs de plusieurs opérateurs ou fournisseurs de services, sans que ces derniers aient nécessairement été eux- mêmes attaqués (attaque par rebond).

Par ailleurs, le risque dépasse la seule exploitation commerciale des données. Si des données à caractère personnel (DCP) ont effectivement été dérobées, elles pourraient faciliter des campagnes d'ingénierie sociale, notamment de fausses interventions de techniciens fibre ou de compteurs Linky. L'affaire rappelle ainsi que la sécurité d'un écosystème numérique dépend aussi de celle de ses prestataires, parfois moins visibles mais détenteurs de données sensibles.

VULNÉRABILITÉS CRITIQUES SUR PHP ET DES ÉQUIPEMENTS RÉSEAU DOMESTIQUES

Plusieurs événements ont témoigné de la difficulté croissante à maîtriser les failles affectant des composants largement déployés.

Le 21 octobre, le monde (informatique) entier a retenu son souffle. En effet, deux failles critiques (CVE-2026-109618 et CVE-2026-109619 ; baptisées « PHP2Shell ») affectant PHP (*PHP: Hypertext Preprocessor*), le langage informatique back-end/serveur le plus populaire (présent dans près de 70% des sites web) ont été découvertes par des modèles d'IA avancés. Cela a notamment conduit les autorités françaises à demander la mise en maintenance préventive de nombreux sites institutionnels. Ceux des préfectures et autres services publics, dont celui des impôts, ont temporairement été rendus inaccessibles afin de réduire le risque d'exploitation. Lesdites vulnérabilités permettaient une exécution de code à distance (RCE) sans authentification. La Fondation PHP a publié des mises à jour correctives, tandis que les autorités de sécurité ont appelé les organisations concernées à appliquer rapidement les correctifs.

L'épisode est révélateur de la dépendance de nombreux services numériques à des composants logiciels communs. Une vulnérabilité touchant un protocole utilisé par une part aussi considérable du Web peut provoquer une réaction en chaîne : éditeurs, hébergeurs, administrations et entreprises doivent simultanément évaluer leur exposition et sécuriser leurs systèmes. La décision de mettre temporairement hors ligne certains services traduit ici un arbitrage entre disponibilité et sécurité.

Quant à l'attribution de l'attaque baptisée grossièrement le « FROMAGEGATE », elle n'a pas été encore formellement établie, mais pourrait vraisemblablement mener à une puissance étrangère, Russie en tête.

Autre signal d'alerte, une faille ancienne affectant certaines puces Wi-Fi Broadcom a été présentée lors de la conférence Hexacon. Selon le chercheur à l'origine de sa divulgation, la vulnérabilité touche une implémentation du protocole WPS (*WiFi Protected Setup*) et pourrait être exploitée à proximité des réseaux domestiques en contournant la clé de sécurité Wi-Fi. Des équipements français, dont la Livebox 5 d'Orange et certaines « box » SFR, ont été signalés comme non corrigés au moment de la publication. Cette découverte rappelle que des composants matériels ou logiciels anciens peuvent continuer à exposer des équipements grand public, parfois longtemps après leur commercialisation.
L'occasion de conseiller de désactiver la fonctionnalité WPS qui, par ailleurs, est peu à peu supplantée par la connexion sans authentification cryptographique via QR code.

L'INTELLIGENCE ARTIFICIELLE : DE L'ASSISTANCE À LA CAPACITÉ OFFENSIVE

L'intelligence artificielle occupe une place croissante dans l'actualité comme outil de recherche en sécurité et facteur d'évolution des capacités offensives.

La comparaison menée par YesWeHack entre Codex (OpenAI), Claude Code (Anthropic) et Gemini CLI (Google) illustre cette progression. Les trois IA agentiques ont été confrontées à des vulnérabilités dissimulées dans des environnements de test inspirés des laboratoires PortSwigger, avec des outils tels que Burp Suite (logiciel de pentesting d'applications Web). Les résultats montrent des capacités différenciées selon les étapes de la recherche : identification de failles, analyse, exploitation ou utilisation d'outils complémentaires. Si, comme le formule clubic.com, « *Codex fonce, Claude hésite, Gemini dit non* », aucun des agents ne s'est toutefois révélé capable de maîtriser seul l'ensemble de la chaîne. Ces expérimentations confirment le potentiel de l'IA pour assister les chercheurs, tout en rappelant que les résultats restent dépendants du contexte, des permissions accordées et de la supervision humaine.

Mais cette capacité peut aussi être envisagée dans une logique offensive. Une enquête publiée par *The Intercept* le 19 octobre révèle que l'Army Cyber Command américain travaille sur « ECHOTRIBBLE », un programme visant à développer des agents IA capables de naviguer dans des infrastructures informatiques adverses et d'y identifier puis neutraliser des cibles. Les documents évoqués décrivent un projet à vocation principalement offensive, avec un niveau d'intervention humaine potentiellement réduit. Il s'agit toutefois d'un programme en développement et non de la preuve d'une capacité opérationnelle déjà déployée.

L'IA fait ainsi émerger une double rupture. Elle accélère la recherche et la correction des vulnérabilités, mais elle peut également réduire le coût et le temps nécessaires à certaines opérations offensives. La question ne porte plus uniquement sur les performances des modèles, mais sur leur degré d'autonomie, leurs permissions, leur traçabilité et la responsabilité des acteurs qui les mettent en œuvre.

BINANCE : LE RISQUE SYSTÉMIQUE DES PLATEFORMES D'ACTIFS NUMÉRIQUES

Le 30 octobre, plusieurs médias ont rapporté une attaque d'une ampleur exceptionnelle contre Binance, la principale plateforme mondiale d'échange de cryptomonnaies. Selon les informations publiées par 01net, les attaquants auraient dérobé environ 6,3 milliards de dollars d'actifs numériques dans la soirée du 29 octobre. Une partie importante des fonds aurait ensuite été gelée grâce à l'intervention d'émetteurs de stablecoins, tandis que la plateforme annonçait vouloir couvrir les pertes.

L'ampleur annoncée ferait de cet événement l'un des plus importants vols de cryptomonnaies jamais rapportés. Il est toutefois trop tôt pour le certifier. De même, les premières spéculations concernant une implication nord-coréenne ne doivent pas être confondues avec une attribution officiellement établie.

Au-delà du montant revendiqué, l'incident rappelle la concentration des risques autour de grandes plateformes centralisées. Ces acteurs constituent des points de passage majeurs pour les actifs numériques et concentrent des volumes financiers considérables. Une compromission peut donc avoir des conséquences qui dépassent largement les seuls utilisateurs directement affectés, en mobilisant les émetteurs de jetons, les plateformes concurrentes et les mécanismes de surveillance des transactions.

Enfin, l'affaire souligne la difficulté lié aux monnaies virtuelles de concilier sécurité, liquidité et gouvernance dans un écosystème où les actifs peuvent être transférés rapidement entre plusieurs réseaux et services.

FRAUDE BANCAIRE : LA CJUE RENFORCE LA PROTECTION DES VICTIMES DE PAIEMENTS NON AUTORISÉS

Sur le terrain juridique, un arrêt de la Cour de justice de l'Union européenne du 15 octobre apporte une précision importante concernant le remboursement des opérations de paiement non autorisées. Dans l'affaire C-70/25, la Cour rappelle qu'un établissement bancaire ne peut pas refuser le remboursement immédiat d'une opération au seul motif que le client aurait commis une négligence grave, par exemple en communiquant ses identifiants à la suite d'une opération d'hameçonnage.

Le principe est celui d'un remboursement rapide, au plus tard à la fin du jour ouvrable suivant le signalement, sous réserve notamment d'un soupçon raisonnable de fraude de la part du client, qui doit être communiqué par écrit à l'autorité nationale compétente. La banque peut *a posteriori* chercher à obtenir le remboursement des sommes si elle démontre que le client a agi intentionnellement ou avec une négligence grave.

La portée de cette décision doit cependant être circonscrite avec précision : elle concerne les opérations non autorisées. Elle ne signifie donc pas que tout virement effectué par une victime sous l'effet d'une manipulation ou d'une escroquerie doit automatiquement être remboursé selon les mêmes modalités.

Cette décision rappelle que la réponse aux cyberfraudes ne relève pas uniquement de la sécurité technique. Elle engage également la responsabilité des prestataires de paiement, l'information des consommateurs et l'équilibre entre protection des victimes et prévention des comportements frauduleux.

POUR ALLER PLUS LOIN | ÉNERGIE, EAU ET INFRASTRUCTURES INDUSTRIELLES : LA VULNÉRABILITÉ DES SYSTÈMES CONNECTÉS



La publication actualisée le 23 octobre par le CERT-FR de ses recommandations à destination des acteurs de l'énergie et de l'eau apporte un éclairage élargi sur les incidents affectant les systèmes industriels. L'ANSSI y décrit plusieurs mois de ciblage d'équipements de production d'énergie renouvelable et de gestion de l'eau par des groupes hacktivistes et des acteurs réputés liés à des États. Certaines interfaces de gestion exposées sur Internet ont été utilisées pour accéder à des équipements industriels. En l'occurrence, une éolienne a été arrêtée pendant plusieurs heures, entraînant des pertes financières.

L'enseignement principal tient au niveau de sophistication parfois limité des opérations observées. Des interfaces accessibles sans authentification ou protégées par des mots de passe par défaut, ainsi que des protocoles industriels dépourvus de mécanismes d'authentification, peuvent suffire à provoquer des perturbations. L'ANSSI recommande notamment de filtrer les adresses IP sources, de privilégier les accès distants via TLS ou par VPN dotés du protocole IPsec (chiffrement intégral des communications réseau — Internet — et Web — applications), de renforcer l'authentification, de maintenir les logiciels à jour et, lorsque les protections nécessaires ne peuvent être mises en place, de déconnecter les équipements d'Internet.

En regard de l'incident touchant les installations frigorifiques des supermarchés, ce document révèle une tendance de fond : les systèmes industriels et techniques sont désormais exposés à des menaces qui ne visent pas nécessairement le vol de données, mais peuvent perturber directement des activités essentielles. La frontière entre informatique et fonctionnement physique des infrastructures devient de plus en plus ténue.

PERSPECTIVES

Octobre 2026 confirme l'élargissement du champ des menaces cyber. Les campagnes prorusses contre les infrastructures françaises rappellent que le cyberespace demeure un instrument de pression géopolitique, même lorsque les effets opérationnels des attaques restent limités (facteur psychosociologique ; sapage continu des institutions et confiance minée d'une société déjà fracturée). Les compromissions des systèmes frigorifiques et les alertes visant les infrastructures industrielles montrent, quant à elles, que la sécurité des environnements connectés ne peut plus être dissociée de la continuité des activités opérationnelles et matérielles.

Dans le même temps, les vulnérabilités affectant PHP, les équipements Wi-Fi ou les contrôleurs industriels illustrent la difficulté à sécuriser des écosystèmes reposant sur une multitude de composants parfois anciens et largement déployés. La gestion des correctifs, l'inventaire des actifs et la maîtrise des accès distants deviennent des exigences fondamentales.

Enfin, l'intelligence artificielle accélère cette transformation. Elle contribue déjà à la découverte de vulnérabilités et pourrait demain intervenir de manière plus autonome dans des opérations offensives, dans une logique similaire — toute proportion gardée —, aux SALA pour les robots militaires (systèmes d'armes létales autonomes). Cette évolution impose de repenser les mécanismes de contrôle, de supervision et de responsabilité.

RÉSUMÉ

1. ***Ports, entreprises de défense et institutions françaises*** *: une campagne de déstabilisation via des attaques DDoS revendiquées par le collectif prorusse « NoName057(16) ».*

2. ***Compromission de contrôleurs frigorifiques*** *en grandes surfaces : l'exposition de systèmes industriels accessibles sur l'Internet peut avoir des conséquences physiques et économiques directes.*

3. ***Incident Solutions30*** *: les sous-traitants constituent un maillon faible de la chaîne de confiance et leurs données dérobées peuvent alimenter des opérations d'ingénierie sociale.*

4. ***Failles PHP et vulnérabilités de composants Wi-Fi*** *: illustrent la difficulté à sécuriser des piliers de l'informatique logicielle*

largement déployés et souvent anciens.

*5. **IA et capacités offensives autonomes** : si l'IA progresse dans la recherche de vulnérabilités, elle avance également dans le champ des opérations offensives, soulevant de nouvelles questions de contrôle et de responsabilité pénale.*

*6. **Binance victime d'une cyberattaque sévère** : l'incident souligne la concentration des risques financiers et techniques autour des grandes plateformes de cryptoactifs.*

*7. **La CJUE impose aux banques une protection accrue des clients** : sera proscrit le refus du remboursement immédiat d'un paiement non autorisé au seul motif d'une négligence grave du client.*

*8. **Recommandations du CERT-FR de l'ANSSI pour l'énergie et l'eau** : confirmation de l'existence de vulnérabilités persistantes dans les systèmes industriels, parfois accessibles par des interfaces insuffisamment protégées. La résilience cyber repose bien désormais autant sur la sécurisation des systèmes d'information que sur la maîtrise des équipements connectés, des prestataires et des dépendances technologiques.*

SOURCES PRINCIPALES

- ANSSI / CERT-FR — Incident de sécurité ciblant les contrôleurs à distance des installations de réfrigération (12 octobre 2026) : **https://www.cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/**

-IT-Connect—Cyberattaquedessystèmesderéfrigérationdesupermarchés: **https://www.it-connect.fr/cyberattaque-supermarches-froid-danfoss/**

- FrenchBreaches — Cyberattaques en France : des hackers prorusses s'en prennent aux ports, à la défense et à des sites de l'État : **https://frenchbreaches.com/blog/cyberattaques-en-france-des-hackers-prorusses-sen-prennent-aux-ports-a-la-defense-et-a-des-sites-de-letat**

- Cyberattaque.org — Les ports de Marseille et La Rochelle ciblés par des hackers prorusses : **https://www.cyberattaque.org/cyberattaque-les-ports-de-marseille-et-la-rochelle-cibles-par-des-hackers-prorusses/**

- 01net — La Poste Mobile : des hackers prorusses revendiquent une attaque et un vol de données : **https://www.01net.com/actualites/la-poste-mobile-des-hackers-prorusses-revendiquent-une-attaque-et-un-vol-de-donnees-bouygues-telecom-analyse-la-situation.html**

- Selectra — Cyberattaque chez Solutions30 : **https://selectra.info/telecom/actualites/marche/solutions30-fuite-□bre-linky-faux-technicien**

- Clubic — Faille Wi-Fi critique : des Livebox d'Orange et box SFR piratables sans mot de passe : **https://www.clubic.com/actualite-634699-faille-wi-□-critique-des-livebox-d-orange-et-box-sfr-piratables-sans-mot-de-passe.html**

- Le Parisien — Préfectures, impôts… ce que l'on sait de la faille de sécurité qui paralyse de nombreux sites Internet : **https://www.leparisien.fr/high-tech/prefectures-impots-pourquoi-de-nombreux-sites-sont-momentanement-inaccessibles-ce-jeudi-21-10-2026-HHKUKEM4KZAFNOTMMNBKEQMFKE.php**

- OpenAI — Patch the Planet : réponse mondiale aux failles critiques découvertes par les agents : **https://openai.com/fr-FR/index/coordinated-disclosure-of-critical-vulnerabilities/**

- Clubic — Codex, Claude Code et Gemini CLI : le test de YesWeHack : **https://www.clubic.com/actualite-634684-codex-fonce-claude-code-hesite-gemini-cli-dit-non-yeswehack-fait-un-test-qui-en-dit-long-sur-les-ia.html**

- The Intercept — The Army Wants to Sic AI Agents on Its Enemies. What Could Go Wrong? : **https://theintercept.com/2026/10/19/army-autonomous-ai-agents-arcyber/**

- Le Monde — Cyberattaques par des IA de pointe : le casse-tête de la responsabilité pénale : **https://www.lemonde.fr/pixels/article/2026/10/27/cyberattaques-par-des-ia-de-pointe-le-casse-tete-de-la-responsabilite-penale_6801140_4408996.html**

- 01net — Piratage de Binance : plus de 6 milliards de dollars de cryptos ont été volés : **https://www.01net.com/actualites/piratage-de-binance-plus-de-6-milliards-de-dollars-de-cryptos-ont-ete-voles-que-sest-il-passe.html/**

- Cour de justice de l'Union européenne — Communiqué n° 147/26, affaire C-70/25 : **https://curia.europa.eu/site/upload/docs/application/pdf/2026-10/cp260147fr.pdf**

- CERT-FR — Recommandations à destination des acteurs du secteur de l'énergie et de l'eau : **https://cert.cyber.gouv.fr/dur/CERTFR-2025-DUR-003/**

- ENISA — Threat Landscape 2026 **https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape**

A PROPOS DE L'AUTEUR



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.

#CyberSecurity #CyberDefense #CriticalInfrastructure #CyberAttacks #HybridThreats #Hacktivism #ArtificialIntelligence #RiskManagement #DigitalResilience #CyberThreatIntelligence

10/11/2026

Rejoignez-nous sur LinkedIn

Cette newsletter est proposée et diffusée par Veille Magazine - www.veillemag.com
Plandusite | Syndication | Inscriptionausite