Newsletter - Octobre 2025 Eastrategies

Défense & Sécurité – Perspectives France & Roumanie

Perspectives et coopération France & Roumanie dans les domaines de la défense, de la cybersécurité et de l'innovation

La France et la Roumanie collaborent étroitement dans les domaines de la défense, de la cybersécurité et de l'innovation, avec des coopérations concrètes comme l'achat de missiles MISTRAL, le rôle de la France en tant que nation-cadre de l'OTAN en Roumanie via la mission AIGLE, et des initiatives de cybersécurité pour protéger les entreprises et les infrastructures. Ces collaborations visent à renforcer la défense collective de l'Europe sur le flanc Est, à améliorer la posture de sécurité des deux pays et à promouvoir le développement économique et technologique mutuel.

Coopération en matière de défense

- **Achats militaires conjoints :** La Roumanie a manifesté son intention d'acquérir le système de missiles antiaériens portables MISTRAL 3 auprès de la France, dans le cadre d'un programme d'achat groupé européen.
- **Mission AIGLE :** Depuis 2022, la France est la nation-cadre du groupement de l'OTAN déployé en Roumanie, assurant un engagement visible et réactif sur le flanc Est de l'Europe.

Coopération en matière d'innovation

L'innovation est encouragée, et de nombreux partenariats économiques existent, soutenus par des organisations spécialisées des deux pays.

- **Partenariats industriels :** Les deux pays cherchent à renforcer leurs liens en matière d'innovation, notamment à travers des partenariats industriels et la collaboration dans le cadre de programmes de recherche et développement.
- **Projets concrets :** La coopération entre les deux pays est portée par des projets concrets visant à doter les forces armées roumaines d'équipements modernes et à renforcer la souveraineté numérique européenne.

Coopération en matière de cybersécurité

La coopération franco-roumaine en matière de cybersécurité se manifeste principalement par l'hébergement par la Roumanie du Centre européen de compétences industrielles, technologiques et de recherche en cybersécurité (ECCC) à Bucarest, un projet de l'Union européenne auquel la France est un soutien majeur. Cette coopération s'articule autour du renforcement des capacités, de la recherche, de l'innovation et de la lutte contre les cybermenaces, dans le cadre de stratégies nationales et européennes.

Axes de coopération :

- **Accueil du Centre européen de compétences en cybersécurité (ECCC) :** La Roumanie a été choisie pour accueillir le siège de l'ECCC, un centre clé pour l'Europe en matière de cybersécurité. La France soutient ce centre qui vise à renforcer la cyberrésilience européenne, à soutenir les entreprises du secteur et à stimuler la recherche et l'innovation.
- **Renforcement de la recherche et de l'innovation :** Le centre de Bucarest joue un rôle important en mettant en relation les acteurs de la recherche, de l'industrie et du secteur public pour développer des solutions innovantes et renforcer la compétitivité européenne.
- **Lutte contre la criminalité et les menaces :** La coopération inclut un volet lutte contre la cybercriminalité, notamment par le biais de collaborations bilatérales et au sein d'organismes comme le Bureau du Programme sur la cybercriminalité (C-PROC) du Conseil de l'Europe, qui est hébergé à Bucarest.
- **Soutien aux entreprises et aux PME :** Des événements organisés en Roumanie, avec la participation du Centre Européen de Compétences en Cybersécurité (ECCC) à Bucarest, visent à favoriser les contacts commerciaux entre les entreprises françaises et les acteurs locaux, y compris les grandes entreprises roumaines et les partenaires technologiques.
- **Développement et renforcement des capacités :** La Roumanie a également développé sa propre stratégie nationale de cybersécurité, et la France, avec son expertise, joue un rôle moteur dans la définition des orientations stratégiques de l'UE, qui incluent le développement de capacités minimales de cybersécurité dans tous les États membres. La France et la Roumanie collaborent pour répondre à l'augmentation des cyberattaques en Roumanie, avec un accent mis sur les PME françaises et les acteurs locaux.

Bucarest accueille le Cyber Centre de l'UE

Le Centre européen de compétences en matière de cybersécurité a ouvert ses portes le 9 mai 2023, à Bucarest, en présence du premier ministre roumain, Nicolae Ciuca et d'autres hauts responsables européens. L'objectif de ce Centre est d'appuyer l'innovation et la politique industrielle dans le domaine de la cybersécurité, ainsi que de développer et de coordonner les projets de l'UE en la matière. Aux dires de Nicolae Ciuca, la présence d'un tel centre dans cette partie de l'Europe reconfirme l'attention que l'UE prête aux efforts communs de protéger l'économie, les citoyens et les institutions publiques.

Pour sa part, le directeur général des réseaux de communication, du contenu et des technologies de la Commission européenne, Robert Viola, a affirmé que Bucarest a été préféré à cinq autres villes européennes en raison des compétences des chercheurs roumains en matière de cybersécurité.

Ce fut en décembre 2020, à l'issue d'une compétition qui incluait aussi la Belgique, l'Allemagne, l'Espagne, le Luxembourg, la Pologne et la Lituanie que la Roumanie a été choisie par les représentants des Etats de l'UE pour accueillir une importante agence communautaire. Il s'agit du centre européen de sécurité cybernétique, censé protéger l'économie et la population contre les attaques cybernétiques, soutenir la recherche dans ce domaine et aider les entreprises européennes à développer leurs capacités de cybersécurité. Parmi les atouts de Bucarest ont figuré, entre autres : la vitesse élevée d'Internet, l'exemption du centre et de ses employés de différentes taxes et impôts et le fait que cette ville était une des quelques capitales européennes à ne pas accueillir une agence européenne.

La date de l'inauguration de cette agence a été choisie le 9 mai – un repère important de l'UE.

> « Le centre européen de compétences en matière de sécurité cybernétique est chargé de la gestion des fonds de l'UE pour actuel exercice budgétaire élargi de l'UE, à savoir pour la période 2021 – 2027. Plus précisément, ses objectifs sont d'adopter les programmes de travail en matière de sécurité cybernétique et de gérer les projets dans le cadre des programmes « L'Europe numérique » et « Horizon Europe » »

Ce qui plus est, le programme doit également gérer les projets relatifs aux centres d'opérations sécuritaires, dans le cadre de la proposition de la Commission d'instituer un bouclier cybernétique européen et collaborera avec un réseau de centres nationaux de coordination dont le but est de créer un écosystème pour l'innovation et la compétitivité en matière de sécurité cybernétique à travers l'Union européenne.

> « La sécurité cybernétique est une priorité essentielle et la protection de notre souveraineté numérique implique des efforts communs » précise Thierry Breton, commissaire au marché intérieur cité dans le communiqué. Il rappelle que « Le centre européen de compétences en matière de sécurité cybernétique réunit des ressources et des experts de très haut niveau de toute l'Union européenne afin de développer des solutions novatrices aux menaces cybernétiques et pour augmenter la résilience aux attaques. Travaillant ensemble, nous pouvons construire un monde numérique plus sûr et plus sécurisé pour tous les européens. »

Le centre européen de sécurité cybernétique déroulera des investissements de 4 milliards et demi d'euros. Sur ce montant, deux milliards d'euros proviendront de fonds européens, et le reste sera couvert par les Etats membres de l'Union.

Faiblesses qui exposent les organisations aux cyberattaques

Selon le dernier rapport Picus, les attaques par compromission d'identifiants et par exfiltration de données restent les plus grandes faiblesses de la cyberdéfense.

En tant que professionnels de la cybersécurité, nous nous concentrons souvent sur l'identification des vulnérabilités les plus complexes et des techniques d'attaque les plus avancées. Nous analysons les failles zero-day, les exploits sophistiqués ou les campagnes APT hautement coordonnées. Cependant, en réalité, les attaques les plus efficaces ne reposent pas sur ces méthodes avancées, mais sur des éléments apparemment anodins : **mots de passe faibles et comptes compromis**.

Malgré des investissements massifs dans les infrastructures, les technologies modernes et des efforts constants de sensibilisation, le rapport Picus Blue 2025 révèle que les organisations continuent de rencontrer des difficultés dans deux domaines fondamentaux : la prévention des violations de mots de passe et la détection des comptes valides utilisés abusivement par des attaquants. Les données présentées mettent en évidence un contraste inquiétant entre le niveau de défense avancé mis en œuvre et leur efficacité face à des techniques d'attaque aussi anciennes et courantes, mais toujours aussi efficaces.

L'augmentation alarmante des attaques utilisant des identifiants faibles

L'édition 2025 du rapport Picus Blue, basé sur au moins 160 millions de simulations d'attaques, révèle une réalité inquiétante : dans **46 % des environnements testés**, au moins un mot de passe (hachage) a été déchiffré et converti en texte clair, contre 25 % l'année dernière. Cela met en évidence l'utilisation de politiques de mots de passe faibles et d'algorithmes de hachage obsolètes. Les attaques utilisant des comptes valides (Valid Accounts – MITRE ATT&CK T1078) ont enregistré un taux de réussite de **98 %**, confirmant que l'authentification faible reste l'une des méthodes d'accès les plus exploitées.

Ces chiffres nous montrent avec quelle facilité les attaquants peuvent s'infiltrer et rester indétectés une fois qu'ils parviennent à mettre la main sur un ensemble d'informations d'identification valides.

Principales recommandations pour les organisations en Roumanie

Pour atténuer ces vulnérabilités, le rapport Picus recommande :

1. Valider en continu les expositions, non seulement en les inventoriant, mais aussi en testant leur exploitabilité réelle
2. Renforcer les défenses contre l'exfiltration de données grâce à des solutions de prévention des pertes de données (DLP), la surveillance du trafic sortant et la détection comportementale
3. Adopter des politiques de mots de passe strictes et supprimer les algorithmes de hachage obsolètes
4. Adoption généralisée de l'authentification multifacteur (MFA), et pas seulement pour les comptes privilégiés
5. Tester en permanence les contrôles de sécurité pour identifier les dégradations au fil du temps
6. Améliorer le pipeline de détection, en augmentant la couverture des journaux et en les transformant en alertes exploitables

Conclusion

Le rapport Picus Blue 2025 envoie un message clair : même si des progrès sont réalisés dans certains domaines, le manque de contrôles efficaces sur les mots de passe et l'exfiltration de données laisse les organisations extrêmement vulnérables.

Pour les entreprises roumaines, où la digitalisation rapide présente des avantages mais aussi des risques élevés, ce rapport est incontournable. Investir dans la validation continue, des politiques d'identité strictes et des contrôles des données n'est plus une option : il est essentiel pour prévenir le prochain incident majeur. Les organisations doivent adopter une mentalité de « présomption de violation », en partant du principe qu'un échec est possible à tous les niveaux de défense et que ces faiblesses doivent être découvertes avant les adversaires.

Conformité NIS2 – Obligation d'enregistrement auprès du DNSC avant le 19 septembre 2025

La directive NIS2 introduit un nouveau cadre réglementaire en matière de cybersécurité, mis en œuvre en Roumanie par l'ordonnance d'urgence n° 155/2024. Les entreprises et les institutions publiques fournissant des services essentiels à l'économie et à la société sont désormais soumises à de nouvelles obligations légales en matière d'enregistrement et de conformité aux exigences DNSC.

Le 20 août 2025, la Direction nationale de la cybersécurité (DNSC) a publié l'arrêté n° 1/2025 et l'arrêté n° 2/2025, qui établissent le processus de notification et les méthodes de soumission des informations et la méthodologie d'évaluation des risques et les seuils permettant de déterminer une interruption de service.

Date limite d'inscription : 19 septembre 2025.

L'obligation de notification et d'enregistrement s'applique aux entités essentielles et importantes des secteurs critiques, notamment :

- énergie, transport, approvisionnement en eau potable,
- soins de santé et infrastructures critiques,
- services numériques, marchés et centres de données,
- administration publique,
- ainsi que d'autres secteurs couverts par l'ordonnance d'urgence n° 155/2024.

Comment fonctionne le processus de notification

La notification est soumise via l'outil NIS, disponible sur le site web du DNSC (www.dnsc.ro). Bien que les étapes techniques paraissent simples, le processus implique bien plus que le simple remplissage d'un formulaire :

- Évaluer si l'entreprise est considérée comme une entité essentielle ou importante ;
- Évaluer le score de risque cyber et préparer les pièces justificatives requises ;
- Choisir la stratégie de notification appropriée (notification standard ou conservatrice) ;
- Soumettre la notification au DNSC, soit par voie électronique avec une signature qualifiée, soit sur papier avec des pièces justificatives.

Pourquoi le score de risque est important

Conformément à l'ordonnance DNSC n° 2/2025, chaque entreprise reçoit un score de cyber-risque basé sur :

- taille de l'entreprise,
- exposition potentielle aux cyberattaques,
- l'impact potentiel sur l'économie et la société.

En fonction du score, les entreprises sont classées en trois niveaux :

- **Niveau de base** → exigences minimales en matière de cybersécurité ;
- **Niveau important** → obligations intermédiaires, audits périodiques et rapports d'incidents ;
- **Niveau essentiel** → exigences strictes en matière de cybersécurité, politiques internes obligatoires, procédures détaillées et rapports accélérés au DNSC.

En pratique : plus le score de risque est élevé, plus les obligations légales sont strictes.

La Roumanie se dotera d'un centre de réponse aux incidents de cybersécurité dans le secteur de l'énergie

Le ministère de l'Énergie a publié, pour débat public, le projet d'ordonnance d'urgence portant création et fonctionnement du Centre de réponse aux incidents de cybersécurité énergétique. La création de ce centre répond à la nécessité pour le secteur de l'énergie de se préparer à faire face à des cybermenaces complexes et en constante évolution.

Selon le projet d'acte normatif, la création du centre est nécessaire « compte tenu de la multiplication des cyberattaques dans le secteur de l'énergie, susceptibles d'interrompre la production, l'approvisionnement et le transport d'électricité, de gaz naturel ou d'énergie thermique, ce qui constitue une situation exceptionnelle à laquelle sont confrontés l'État roumain et ses partenaires européens et transatlantiques ». Les auteurs du projet affirment que la libéralisation du marché national de l'énergie, les fluctuations des prix et la présence de plus en plus d'entreprises énergétiques sur le marché des capitaux constituent la prémisse à partir de laquelle les cyberattaquants partent lorsqu'ils mènent une opération contre l'État roumain, mais aussi le fait que les cyberattaques peuvent influencer directement les prix de l'énergie et la stabilité du système électrique national et influencer indirectement le fonctionnement des services publics et de l'économie nationale, qui dépendent tous deux de l'approvisionnement en électricité et en chaleur.

D'autres raisons invoquées pour justifier la création du Centre sont : « le contexte de risques croissants pour la défense et la sécurité nationale de la Roumanie, dans le contexte des cyberattaques générées par la guerre de la Fédération de Russie en Ukraine, qui nécessite la création d'un Centre sectoriel de réponse aux incidents de cybersécurité dans le domaine de l'énergie, ci-après dénommé CSIRT, capable de soutenir l'effort national et interinstitutionnel de prévention et de lutte contre les cyberattaques contre les entreprises et les infrastructures énergétiques. »

L'urgence d'adopter le GEO est également justifiée par « la possibilité accrue d'une cyberattaque multiple, susceptible d'affecter des éléments de l'infrastructure nationale dans le secteur cybernétique, ce qui créerait la panique parmi la population civile, ainsi que de nuire à la position de certaines entreprises du secteur de l'énergie sur le marché des capitaux, influençant à terme les prix de l'énergie », mais aussi en tenant compte du fait qu'il est impératif de renforcer la cybersécurité de la plupart des entreprises publiques et des opérateurs économiques bénéficiaires de projets financés par le Fonds de modernisation afin de mieux faire face aux cybermenaces complexes et avancées, ainsi que de sensibiliser davantage à l'importance de la cybersécurité au niveau sectoriel.

Le projet d'OGE mentionne que la création du Centre de réponse aux incidents de cybersécurité énergétique est essentielle pour assurer une surveillance continue, une réponse rapide aux incidents, des enquêtes médico-légales et une autoprotection contre les cyberattaques, en tant qu'éléments de la politique énergétique nationale.

> « Étant donné que le retard dans la mise en œuvre de la législation nationale et européenne sur l'opérationnalisation des CSIRT dans le secteur de l'énergie a conduit et continue de conduire à une vulnérabilité des composants du système énergétique dans le contexte des cybermenaces actuelles, c'est pourquoi la création d'un CSIRT sectoriel est nécessaire, et en son absence, les dommages générés par les cyberattaques peuvent être majeurs, avec des conséquences sur le prix de l'énergie »

Le projet souligne également que la Roumanie, en tant que fournisseur d'électricité de la République de Moldavie et de l'Ukraine, ainsi que fournisseur de sécurité au niveau régional, a l'obligation de renforcer d'urgence sa cybersécurité dans le secteur de l'énergie afin de préserver ce statut et de fournir des connaissances stratégiques à d'autres secteurs et États partenaires à l'avenir.

Identifier des solutions appropriées pour assurer une résilience accrue des infrastructures critiques - Projet ENDURANCE

La Direction nationale de la cybersécurité (DNSC) bénéficie d'une subvention non remboursable pour la mise en œuvre du projet « Stratégies et services pour une résilience et une coopération renforcées face aux perturbations en Europe – ENDURANCE ». Le projet est financé par l'Agence exécutive du Conseil européen de la recherche (AEC) au titre du programme Horizon Europe, dans le cadre de l'appel à projets HORIZON-CL3-2023-INFRA-01, type d'action : Actions d'innovation HORIZON.

Le projet ENDURANCE vise à répondre au besoin crucial de renforcer les services essentiels européens face aux perturbations potentielles, en allant au-delà de l'approche conventionnelle qui se concentre exclusivement sur les actifs critiques existants. Dans le monde hautement interconnecté d'aujourd'hui, les infrastructures critiques sont de plus en plus exposées à un large éventail de risques, allant des cyberattaques et sabotages physiques aux erreurs humaines et aux catastrophes naturelles. De telles perturbations peuvent avoir des conséquences considérables, affectant la sécurité publique, la stabilité économique et la continuité des services essentiels en Europe. Cette vulnérabilité croissante incite l'Europe à prendre des mesures proactives et coordonnées pour protéger ces infrastructures.

Lancée en octobre 2024, cette initiative, dotée de 5 millions d'euros et financée par l'UE, durera 36 mois et développera des solutions interopérables pour renforcer la défense européenne. Le projet fournira des méthodologies robustes, des technologies de pointe et des cadres stratégiques pour renforcer la résilience des infrastructures critiques et garantir leur capacité à se remettre d'incidents physiques et informatiques.

Le consortium, composé de 23 partenaires de 7 pays européens, comprend 7 autorités, 5 opérateurs d'infrastructures critiques de 6 secteurs clés et 11 entités expertes dans différents domaines. Il est coordonné par EVIDEN TECHNOLOGIES SRL (Roumanie). Les partenaires roumains du projet sont :

- DIRECTION NATIONALE DE LA CYBERSÉCURITÉ
- MINISTÈRE DE LA SANTÉ
- DIRECTION GÉNÉRALE DE LA PROTECTION INTÉRIEURE
- DR. MUNTEAN GYNÉCOLOGIE CLINIQUE SRL

Afin de maximiser l'impact des développements et des résultats du projet, la DNSC a créé le **Groupe de travail paneuropéen sur la résilience aux perturbations (WGDR)**. L'objectif de ce réseau d'experts est de former un écosystème favorisant l'échange d'informations afin de fournir aux acteurs des infrastructures critiques les meilleures pratiques et les nouvelles connaissances nécessaires à l'amélioration de la résilience de leurs infrastructures. En facilitant la collaboration entre les acteurs et en harmonisant les efforts sur la directive sur la résilience des entités critiques (CER) et la directive NIS2 (Directive sur les réseaux et les systèmes d'information), le projet ENDURANCE jouera un rôle clé dans la sécurisation des infrastructures européennes contre un large éventail de menaces en constante évolution.

La mission du projet ENDURANCE est représentée par :

- améliorer la collaboration et la coopération stratégique des acteurs du secteur des infrastructures critiques (réunissant plus de 100 praticiens et experts concernés au niveau européen) ;
- développement d'ensembles de données, de registres, de méthodologies, de technologies et de services (niveau TRL 6-7) pour le partage et le traitement agrégé des données CER pertinentes, l'évaluation conjointe des risques pertinents et de la résilience, ainsi que les tests à grande échelle de la préparation ;
- fournir une stratégie unitaire et pragmatique pour assurer la continuité des services essentiels interconnectés (adoptée par plus de 20 autorités européennes compétentes en matière d'infrastructures critiques au niveau sectoriel et national).

Défense européenne & OTAN

La Roumanie et le flanc est de l'OTAN

La Roumanie contribue à la stabilité et la sécurité du Flanc est de l'OTAN, aux côtés de ses partenaires et soutient la consolidation de la sécurité dans la région de la mer Noire, a souligné le président par intérim, Ilie Bolojan. Il a précisé que Bucarest allouait déjà 2,5% de son PIB à la défense et a affirmé qu'il était préparé à augmenter les investissements dans le domaine. Au sujet de la situation en Ukraine, le président Bolojan a souligné le besoin d'une paix juste et durable ainsi que l'importance du maintien du soutien à ce pays.

Le secrétaire général de l'OTAN a remercié la Roumanie pour le fait d'être un Etat membre qui agit d'une manière responsable en tant que facteur important de sécurité et de stabilité dans la région de la mer Noire et sur le flanc est. De l'avis de Mark Rutte, ces efforts sont d'autant plus importants dans l'actuel contexte sécuritaire et a exprimé le soutien de l'OTAN à la consolidation de la présence alliée dans la région. Le secrétaire général a réaffirmé l'engagement de l'OTAN et des Etats-Unis envers la défense collective et l'article 5, soulignant les efforts des Etats-Unis pour une paix durable en Ukraine. Le haut responsable otanien a conclu par saluer la majoration du budget de défense de la Roumanie et a souligné le besoin que d'autres alliés européens adoptent une approche similaire. Les deux leaders ont décidé de maintenir un dialogue constant sur ces sujets. Le président de la Roumanie et le secrétaire général de l'OTAN avaient participé à Londres au Sommet informel sur des thèmes de sécurité européenne convoqué par le premier ministre britannique Kier Starmer.

Roumanie et France – Coopération renforcée en matière de défense sur le flanc oriental

Le 22 juillet 2025, le ministre de la Défense nationale, Liviu-Ionuț Moșteanu, a eu un entretien avec le directeur français de la Direction générale de l'armement, le général Gaël Diaz de Tuesta, en visite à Bucarest, et avec l'ambassadeur de France en Roumanie, S.E. Nicolas Warnery.

Les entretiens ont porté sur le renforcement de la coopération bilatérale en matière d'acquisition d'équipements et sur l'exploitation des opportunités offertes par les initiatives européennes de défense, notamment par le biais du mécanisme SAFE. Les responsables ont souligné l'importance du partenariat stratégique franco-roumain pour la consolidation de la position alliée sur le flanc oriental et la contribution de la France au groupement tactique roumain de l'OTAN déployé à Cincu.

Les responsables ont convenu de la nécessité d'un dialogue stratégique constant et d'une coopération opérationnelle et industrielle renforcée dans le contexte des défis sécuritaires dans la région de la mer Noire et dans les Balkans occidentaux. Ils ont également réitéré leur engagement commun à soutenir l'Ukraine et la République de Moldavie.

La Roumanie commande 200 systèmes Mistral 3 dans le cadre d'un achat européen

La Roumanie franchit une nouvelle étape dans la modernisation de son armée. En effet, selon Defense Romania, le ministère de la Défense (MApN) roumain prévoit l'acquisition de plus de 200 systèmes portables de défense antiaérienne Mistral 3, assortis d'un millier de missiles, pour un montant estimé à 626 millions d'euros. Cette commande s'inscrit non seulement dans un effort de rééquipement national, mais également dans une logique de coopération européenne renforcée. Concrètement, cet achat bénéficie du programme EDIRPA (European Defence Industry Reinforcement through Common Procurement Act), un mécanisme de l'Union européenne visant à encourager les acquisitions groupées. Ainsi, en novembre 2024, la Commission européenne a validé un achat commun de 1500 missiles Mistral 3. Celui-ci est mené par la France au nom de neuf pays : la Belgique, Chypre, l'Estonie, la Hongrie, le Danemark, la Slovénie, l'Espagne, la Roumanie et la France.

Par conséquent, la Direction générale de l'armement (DGA) assurera la passation du marché auprès du missilier MBDA, garantissant des conditions tarifaires identiques pour tous les États participants.

En termes opérationnels, le Mistral 3 est un missile sol-air de très courte portée, léger (moins de 20 kg) et facilement déployable. Grâce à son mode de fonctionnement « tire et oublie », il peut intercepter une large variété de menaces : drones, hélicoptères, avions à basse altitude, voire missiles de croisière. De ce fait, il constitue un outil stratégique pour protéger rapidement des unités mobiles ou des infrastructures critiques. Parallèlement, la Roumanie finalise un second programme majeur dans le domaine de la défense aérienne : le projet SHORAD/VSHORAD, destiné à couvrir les besoins à courte et très courte portée. Ce contrat, évalué à 4,2 milliards d'euros, prévoit l'acquisition de 41 systèmes pour les forces terrestres et aériennes. Le groupe israélien Rafael a d'ailleurs été sélectionné pour livrer ces équipements, avec une signature attendue d'ici la fin de l'année. En outre, ces investissements s'inscrivent dans une stratégie plus globale de transformation des forces armées roumaines. Actuellement, plus de 70 programmes d'armement sont en cours ou en préparation, dont l'achat de 246 blindés d'infanterie (2,5 milliards d'euros) et de 200 000 armes individuelles de standard OTAN (400 millions d'euros).

Au sein d'une coopération militaire étroite, la France intervient en Roumanie dans le cadre de la mission AIGLE, qui en fait la nation-cadre du groupement de l'OTAN déployé dans le pays depuis 2022.

La France envoie 2 500 soldats supplémentaires en Roumanie. Quelle sera la mission de l'armée française ?

La France envoie 2 500 soldats supplémentaires en Roumanie, portant le nombre total de soldats présents dans notre pays à 4 000. L'OTAN étend ainsi le groupement tactique avancé consolidé en Roumanie, du niveau brigade au niveau bataillon. L'augmentation du nombre de militaires intervient dans un contexte de menace croissante posée par la Russie aux pays de l'OTAN sur le flanc oriental.

> „À l'automne prochain, nous procéderons à un exercice de déploiement à grande échelle pour cette brigade. L'objectif est de passer à un niveau supérieur, mais pour une durée limitée. Autrement dit, de tester ce déploiement sur le plan logistique ou stratégique, mais seulement pendant une durée déterminée. Le système que la France a choisi, comme d'autres nations cadres dans d'autres pays du flanc oriental, est de disposer d'un groupement tactique important et de pouvoir le consolider en peu de temps", a déclaré le général Loïc Girard, haut représentant militaire de la France en Roumanie.

Innovation & technologies duales

Roumanie et Ukraine s'allient : la fabrique de drones qui terrorise déjà Moscou

Le 30 septembre 2025, à 21h15, une annonce fracassante vient de secouer les fondations de la sécurité européenne : la Roumanie et l'Ukraine s'apprêtent à produire conjointement des drones défensifs sur le territoire roumain, transformant le flanc oriental de l'OTAN en forteresse technologique capable de repousser les incursions aériennes russes. La ministre roumaine des Affaires étrangères, Oana Toiu, vient de révéler à l'ONU ce partenariat explosif qui changera à jamais l'équilibre des forces en Europe orientale. Ce n'est plus seulement l'Ukraine qui combat : c'est désormais tout le flanc est de l'Alliance atlantique qui s'arme avec la technologie éprouvée par 1315 jours de guerre totale.

Cette alliance révèle l'ampleur de la révolution stratégique en cours où l'Ukraine passe du statut de pays secouru à celui de nation exportatrice de savoir-faire militaire vers ses voisins de l'OTAN. La Roumanie, qui partage 650 kilomètres de frontière avec l'Ukraine et a subi plus de 20 violations de son espace aérien par des drones russes, découvre que la meilleure défense consiste à s'équiper avec les armes forgées dans le feu de la guerre ukrainienne. Ce partenariat marque peut-être l'acte de naissance d'une nouvelle doctrine de sécurité européenne : apprendre de ceux qui combattent l'agresseur plutôt que de théoriser dans des académies militaires déconnectées du réel.

La révélation tombe en pleine Assemblée générale des Nations Unies, transformant cette tribune diplomatique en champ de bataille géopolitique où la Roumanie annonce officiellement son intention de devenir le centre névralgique de la production de drones défensifs pour tout le flanc oriental de l'OTAN. Cette déclaration révèle que Bucarest ne se contente plus d'observer passivement la guerre à ses frontières mais décide de transformer son territoire en arsenal technologique.

Cette tribune internationale révèle également la stratégie roumaine de légitimation diplomatique d'une alliance militaro-industrielle avec l'Ukraine. En annonçant ce partenariat depuis l'ONU, Bucarest transforme une coopération bilatérale en projet continental destiné à protéger l'ensemble des pays de l'Est européen face aux menaces russes.

Ce partenariat s'inscrit dans le cadre du programme européen SAFE, qui met à disposition de la Roumanie la somme colossale de 16,6 milliards d'euros pour renforcer ses capacités de défense sur les cinq prochaines années. Cette manne révèle l'ampleur de l'investissement européen dans la sécurisation de son flanc oriental face à une Russie perçue comme menace existentielle permanente.

Ce financement révèle également l'évolution de la doctrine de défense européenne qui privilégie désormais l'investissement massif dans les capacités nationales plutôt que la dépendance exclusive aux systèmes d'armes américains. Cette européanisation de la défense révèle que le Vieux Continent comprend enfin qu'il doit prendre en main sa propre sécurité.

La Roumanie prévoit d'investir 200 millions d'euros dans la construction d'une usine ultramoderne de production de drones qui sera opérationnelle dès 2026, révélant l'urgence perçue par Bucarest face aux menaces qui pèsent sur son espace aérien. Cette usine révèle la transformation de la Roumanie de consommateur d'armes en producteur d'armements sophistiqués.

Cette industrialisation révèle également l'émergence d'un nouveau modèle économique de défense où les pays de l'Est européen ne se contentent plus d'acheter des armes occidentales mais développent leurs propres capacités industrielles. Cette autonomisation révèle que l'Europe orientale prend son destin sécuritaire en main.

Une opportunité historique : la Roumanie peut se positionner sur la scène mondiale de l'IA grâce à une stratégie nationale qui capitalise sur l'impact de l'initiative chinoise DeepSeek

La Roumanie possède deux atouts majeurs dans la compétition mondiale : son école traditionnelle de mathématiques et d'informatique, qui a formé des centaines de milliers de spécialistes de haut niveau pour les plus grandes entreprises technologiques mondiales, et son infrastructure Internet haut débit, qui facilite le développement de l'industrie technologique. Il est nécessaire que les programmes des écoles techniques et des universités soient alignés sur les cursus nécessaires à l'obtention de certificats internationaux dans le domaine des TI, afin que les diplômés soient de véritables spécialistes en TI et soient rapidement absorbés par le marché.

La Roumanie a désormais une opportunité historique, qui se présente tous les dix ans, voire tous les cent ans, de s'affirmer sur la scène internationale des technologies de l'intelligence artificielle (IA), avec la démocratisation de l'accès aux modèles d'IA les plus avancés réalisée par les Chinois de DeepSeek, qui ont démontré que l'IA peut fonctionner avec beaucoup moins de ressources technologiques.

La Roumanie dispose de deux atouts historiques majeurs : une excellente école de mathématiques et d'informatique et l'internet haut débit, ainsi qu'une stratégie nationale bien développée dans ce domaine, à commencer par l'éducation. Si elle s'appuyait sur ces atouts, la Roumanie pourrait se hisser au sommet mondial de l'IA.

> « C'est un moment historique crucial. Nous avons l'internet haut débit en Roumanie, nous avons des cerveaux. Et à mon avis, nous devons nous concentrer sur un seul domaine en tant que pays. Concentrons-nous tous sur un seul domaine de l'IA et excellons dans ce domaine. Tel est l'avenir, tel que je le vois. Je dirais que c'est une opportunité qui ne se présente qu'une fois par siècle, et non tous les 25 ans, pour un pays de se concentrer sur l'objectif de devenir un leader mondial dans les domaines de la santé et de l'agriculture : tous ces domaines sont interconnectés et l'IA peut les améliorer de manière exponentielle », a déclaré George Haber, investisseur en haute technologie et l'un des Roumains les plus connus de la Silicon Valley (États-Unis).

La première usine d'intelligence artificielle en Roumanie, dans le cadre d'une initiative de l'UE, sera construite par Politehnica Bucarest et ICI

L'Institut national de recherche et de développement en informatique - ICI Bucarest et l'Université nationale des sciences et technologies Politehnica Bucarest construiront la première usine d'IA du pays, dans le cadre du programme EuroHPC - AI Factories de l'UE, en collaboration avec un consortium de partenaires universitaires, de recherche et industriels.

La Roumanie fait partie des six pays européens sélectionnés lors de la dernière évaluation du programme EuroHPC – AI Factories, une initiative européenne dédiée au développement de l'intelligence artificielle et des centres de calcul intensif. Ce projet deviendra une référence pour l'IA en Roumanie, intégrée au cadre européen EuroHPC.

Construire l'usine de l'IA implique l'acquisition et l'exploitation d'un supercalculateur de pointe, optimisé pour l'intelligence artificielle, et le développement d'un ensemble de services et d'infrastructures avancés dédiés à la recherche, à l'environnement des affaires et au secteur public.

Les domaines d'application prioritaires comprennent : la fabrication et l'industrie, la cybersécurité, les sciences de la vie, les services publics numériques et les systèmes autonomes.

L'initiative soutiendra à la fois les chercheurs et les universités, ainsi que les startups, les PME et les institutions publiques, en leur donnant accès à des ressources de calcul haute performance, à des ensembles de données, à des outils logiciels et à des programmes de formation.

> « Grâce à cet investissement stratégique, la Roumanie rejoint les principaux acteurs européens de l'intelligence artificielle. L'Université Politehnica Bucarest possède la tradition, l'expertise et les ressources humaines nécessaires pour transformer ce projet en moteur de progrès scientifique et économique. C'est une occasion unique de développer ici, en Roumanie, des technologies de pointe qui influenceront l'ensemble de la société », a déclaré Mihnea Costoiu, recteur de l'Université Politehnica Bucarest.

Sous la coordination de l'ICI Bucarest, le projet vise à transformer les PME de simples utilisateurs de technologie en acteurs actifs de l'innovation, en offrant des services, des formations et un accès à des infrastructures modernes d'intelligence artificielle.

> « Ce résultat confirme que la Roumanie peut jouer un rôle important dans la transformation numérique de l'Europe. RO AI Factory constituera la pierre angulaire des futurs projets européens d'infrastructures d'IA, ouvrant la voie à de nouveaux investissements, collaborations et partenariats internationaux », a déclaré le Dr Adrian-Victor Vevera, ingénieur et directeur général d'ICI Bucarest.

RO AI Factory sera hébergé et coordonné par ICI Bucarest et Politehnica Bucarest, réunissant un consortium solide de partenaires nationaux de la recherche, de l'éducation et de l'industrie :

- Université Technique de Cluj-Napoca (UTCN) ;
- Institut national de recherche et de développement en sciences biologiques (INCDSB), Association informatique de Transylvanie (ATIT) ;
- Institut de recherche en intelligence artificielle (ICIA) ;
- Conseil national des petites et moyennes entreprises privées de Roumanie (CNIPMMR) ;
- Association des pôles d'innovation numérique en Roumanie (RoDIH).

Les autres projets sélectionnés lors de cette étape finale proviennent de la République tchèque, de l'Espagne, de la Pologne, de la Lituanie et des Pays-Bas.

Contactez Eastrategies

Marc Pascal Huot, Président/CEO

NOVASTEA/EASTRATEGIES

Ensemble, développons vos opportunités en Europe de l'Est et en Grèce

Téléphone Mobile France: +33 6 74 89 23 18

Téléphone Mobile Roumanie: +40756718674

Téléphone Bureau: +33 2 99 09 84 43

Email: marc.huot@novastea.fr

Site Web Eastrategies.fr

Réseaux Sociaux : https://www.linkedin.com/company/eastrategies-roumanie/

Partenaires