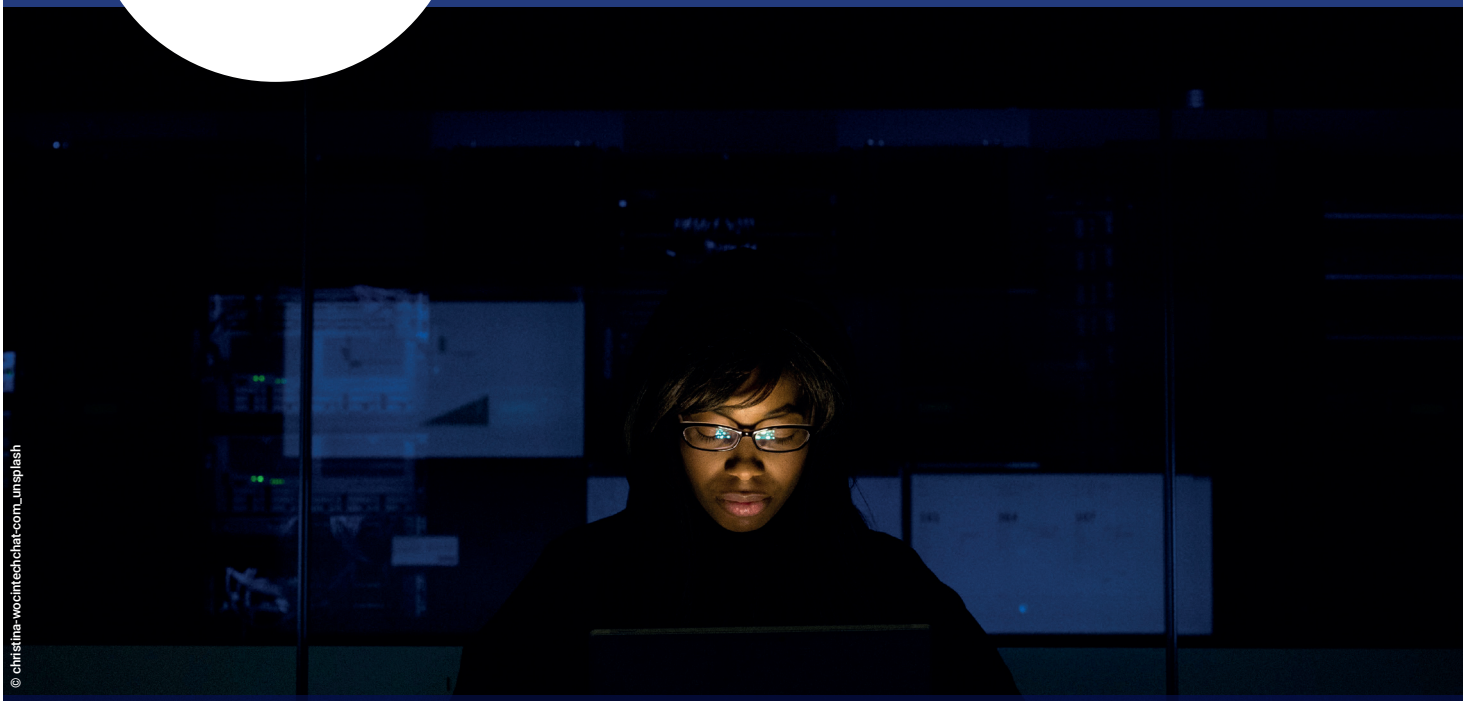
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

EXPERTISE FRANCE
GROUPE AFD

Expertise France et

la cyber-résilience



© christina-wocintechchat-com_unsplash

+100
experts déployés sur des missions court et long terme

27 M€
engagés depuis 2014

38
pays couverts

Expertise France joue un rôle crucial dans le renforcement de la sécurité et la résilience du cyberespace à travers le monde. En collaboration avec des acteurs nationaux et internationaux, l'agence met en œuvre des projets ambitieux visant à protéger les individus, les organisations et les infrastructures critiques contre les cybermenaces aussi bien sophistiquées que multiformes.

Des savoir-faire en commun

Appuyer nos partenaires afin de mieux sécuriser leur cyberespace

La diffusion rapide des technologies de l'information, la transformation numérique et l'interconnexion des systèmes des pays partenaires d'Expertise France, apportent avec elles de potentielles vulnérabilités, et de graves risques, comme la cybercriminalité, les attaques contre les services et infrastructures critiques ou encore la déstabilisation des démocraties face aux ingérences numériques.
Ces risques augmentent, notamment lorsque la technologie avance trop vite. Les avantages économiques et sociaux du cyberespace ne peuvent pas se réaliser indépendamment d'un environnement numérique sous-jacent sécurisé et sûr. Expertise France agit pour appuyer ses partenaires afin de mieux sécuriser leur cyberespace.

L'accélération de l'adoption des nouvelles technologies est l'une des priorités d'Expertise France, qui agit dans de nombreux sous-domaines : développement de l'intelligence artificielle, transformation numérique des administrations, entrepreneuriat numérique, exploitation des données spatiales, etc.

L'informatique est devenue un élément essentiel à la gestion de nombreux systèmes critiques comme l'énergie, la santé, les télécommunications et les systèmes financiers. Un incident peut paralyser des secteurs essentiels, exacerber des crises humanitaires et ralentir le développement économique, en particulier dans les pays en développement.

Les cyberattaques, telles que le phishing, les ransomwares, et les malwares, augmentent en fréquence et en sophistication, menaçant non seulement les entreprises et les institutions gouvernementales, mais aussi les citoyens.

Nombreux sont les exemples de cyberattaques récents qui montrent les effets potentiellement dévastateurs de ces menaces :

- En décembre 2024, Telecom Namibia, la société nationale de télécommunications, a été victime d'une importante attaque par ransomware. Cet incident a entraîné la violation et la fuite de données sensibles de clients, couvrant près de 500 000 enregistrements.
- En décembre 2021, plusieurs services du Ministère de la Santé au Brésil ont été victimes d'un ransomware, ce qui a entraîné la perte des données de vaccination au Covid-19 de millions de personnes;
- Au Vietnam, il est estimé que 46 % des agences publiques et entreprises ont déclaré avoir subi au moins une cyberattaque en 2024.

Investir dans la cybersécurité et plus généralement dans la cyber-résilience dans les pays en développement est donc essentiel pour garantir une croissance numérique inclusive et durable, tout en réduisant les vulnérabilités dans un monde de plus en plus interconnecté. Cette démarche s'inscrit pleinement dans le Global Gateway, et la stratégie internationale numérique de l'Union Européenne.

Expertise France intervient en matière de cybersécurité, en proposant des approches adaptées aux besoins des pays partenaires, en visant particulièrement à renforcer la sécurité numérique et la résilience face aux cybermenaces.

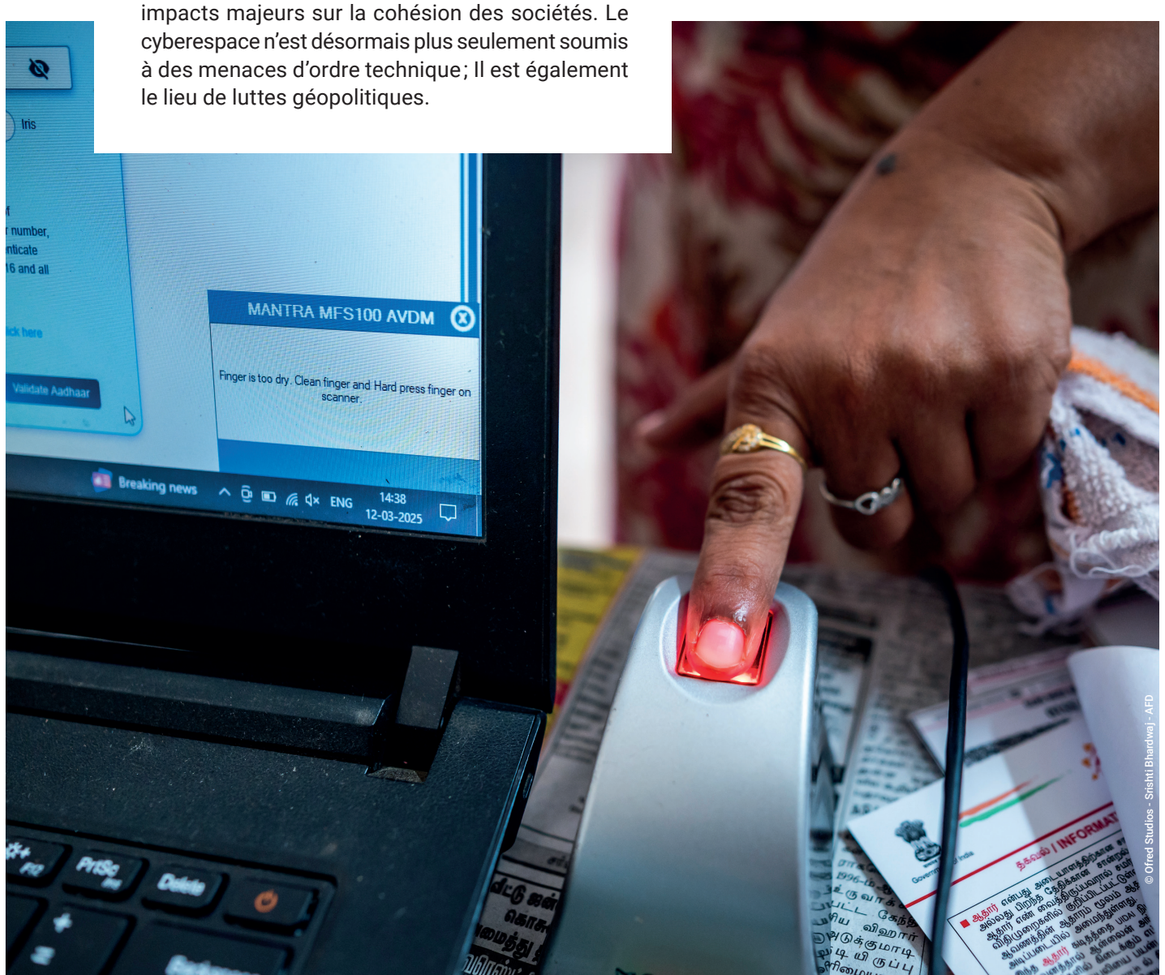
La démarche d'Expertise France s'inscrit dans les ambitions françaises en matière de coopération internationale dans le domaine de la cybersécurité, en contribuant à la cyber-résilience et au renforcement de la cybersécurité des pays volontaires les moins protégés face aux menaces, afin de contribuer à la stabilité globale du cyberespace.

Expertise France s'attache à valoriser l'expertise publique et privée française - et européenne - en la matière et à mobiliser l'écosystème national (ANSSI, Viginum, Campus Cyber, etc.).

L'approche d'Expertise France est holistique. Elle intervient à la fois au niveau des politiques publiques, des cadres législatifs et réglementaires, mais également au niveau opérationnel en dotant les partenaires de capacité de réponse, de savoir-faire et d'outils face aux pannes ou aux attaques.

Notre offre de service permet également d'accompagner nos partenaires dans la lutte contre les menaces numériques géopolitiques, comme la manipulation de l'information ou de l'opinion publique, via des canaux numériques, qui peuvent avoir des impacts majeurs sur la cohésion des sociétés. Le cyberespace n'est désormais plus seulement soumis à des menaces d'ordre technique; Il est également le lieu de luttes géopolitiques.

Les menaces auxquelles font face les états partenaires d'Expertise France sont de plus en plus hybrides et sophistiquées. Elles peuvent combiner plusieurs actions (erreurs ou négligences humaines, actes malveillants, désinformation, etc.) pour nuire à leurs cibles en perturbant l'économie ou les processus démocratiques. Expertise France est en mesure de déployer de l'assistance technique de manière à lutter contre certaines tactiques de déstabilisation, en apportant des ressources et méthodes permettant de faire de la veille, de la prévention, et de la restauration suite aux pannes et aux attaques, et déployer des stratégies opérationnelles de défense et de riposte face aux actes de malveillance. Expertise France peut par exemple intervenir en appui pour définir des stratégies de renforcement de la sécurité physique des infrastructures de télécommunication.



© Ofred Studios - Srishti Bhardwaj - AFD

Nos axes d'intervention et projets mis en œuvre

GRÈCE

ACCOMPAGNER LES RÉFORMES EN MATIÈRE DE CYBERSÉCURITÉ

UE | 400 k€ | 2025-2026

Le projet vise à accompagner la Grèce dans la conception, le développement et la mise en œuvre de réformes en matière de cybersécurité, conformément à la directive NIS2 et au cadre réglementaire national. Il a pour objectif principal de renforcer la gouvernance du secteur, la sécurité de la chaîne d'approvisionnement des infrastructures critiques, notamment dans le secteur public, ainsi que la sensibilisation des parties prenantes clés.

ASIE CENTRALE - KIRGHIZISTAN, KAZAKHSTAN, OUZBEKISTAN, TURKMÉNISTAN, TADJIKISTAN

TEI DIGITAL ASIE CENTRALE - COMPOSANTE CYBER

UE | 20 M€ | 2025-2028

Expertise France favorise l'accès et l'utilisation à la connexion satellitaire, en particulier pour les femmes, les jeunes et les minorités, afin de renforcer leur inclusion socio-économique par le numérique.

AFRIQUE DE L'OUEST - PAYS CEDEAO : BÉNIN, CAP-VERT, CÔTE D'IVOIRE, GAMBIE, GHANA, GUINÉE, GUINÉE-BISSAU, LIBERIA, NIGERIA, SÉNÉGAL, SIERRA LEONE, TOGO - MAURITANIE

ORGANISED CRIME: WEST AFRICAN RESPONSE ON CYBERSECURITY AND FIGHT AGAINST CYBERCRIME (OCWAR-C)

UE | 7,5 M€ | 2019-2024

Expertise France a contribué au renforcement de la cybersécurité et à la lutte contre la cybercriminalité dans les États de CEDEAO et en Mauritanie grâce à la mise en œuvre du projet OCWAR-C. Le projet a amélioré la résilience et la robustesse des infrastructures de l'information, les capacités locales de lutte contre la cybercriminalité, avec la mise en place de cadres stratégiques et légaux, le renforcement des institutions de cybersécurité, la sensibilisation à l'hygiène numérique et la création et l'amélioration des capacités nationales de réponse aux incidents informatiques.

ASIE - INDE, INDONÉSIE, JAPON, MALAISIE, PHILIPPINES, RÉPUBLIQUE DE CORÉE, SINGAPOUR, THAÏLANDE, VIETNAM

ESIWA/ESIWA+

UE | 15+9 M€ | 2020-2027

Programme phare de l'Union européenne dans l'Indopacifique, le **projet ESIWA**, a pour objectif de promouvoir dans la région l'Europe comme acteur pertinent sur les questions de sécurité et défense. En mettant en œuvre la composante cybersécurité du projet, Expertise France a soutenu les efforts de l'UE dans la promotion du droit international dans le cyberespace, la dissémination des principes de cyber-diplomatie, le renforcement de la coopération en matière de cybersécurité, par l'organisation de dialogues et de conférences en coopération étroite avec les agences de cybersécurité nationales et régionales, et des États membres.
La seconde phase du projet ESIWA+, poursuit l'action menée depuis 2020 pour promouvoir dans la région Indopacifique l'Union Européenne comme acteur pertinent sur les questions de sécurité et défense.

KENYA

CYBER KENYA : RENFORCER LA RÉSILIENCE DE L'ÉCOSYSTÈME DE CYBERSÉCURITÉ DU KENYA

UE | 3M€ | 2025-2028

Le projet vise à renforcer la résilience de l'écosystème de cybersécurité du Kenya pour faire en sorte que les citoyens bénéficient d'un cyberespace ouvert, gratuit, sécurisé, sensible aux questions de genre et pacifique. Expertise France intervient dans l'amélioration des cadres réglementaires et juridiques en matière de cybersécurité, le renforcement des capacités de gestion des incidents de cybersécurité et l'amélioration de la culture et des capacités des utilisateurs en matière de cybersécurité.

DJIBOUTI, KENYA, SOMALIE

INITIATIVE FOR DIGITAL GOVERNMENT AND CYBERSECURITY (IDGC)

UE et BMZ | 2022-2025

Cofinancé par l'Union européenne et le ministère fédéral allemand de la Coopération économique et du Développement (BMZ), le projet « Initiative en faveur de l'administration numérique et de la cybersécurité », a pour but d'aider des États membres de la Corne de l'Afrique, particulièrement le Kenya, la Somalie et Djibouti, à renforcer la fourniture de services publics en améliorant et en sécurisant les moyens de diffusion numériques associés. Expertise France a mis en œuvre la composante cybersécurité, en contribuant sur l'amélioration des cadres institutionnel, réglementaire, et opérationnel et sur la sensibilisation à la cybersécurité.

AMÉRIQUE LATINE ET CARAÏBES

EU-LAC DIGITAL ALLIANCE

UE | 11 M€ | 2023-2027

Expertise France met en œuvre la composante Cybersécurité du Pilier 1 de l'Alliance numérique UE-ALC (EU-LAC Digital Alliance), qui a pour objectif d'accélérer la transition numérique dans la région Amérique Latine – Caraïbes, en tout en renforçant le rôle de l'UE en tant que partenaire et acteur clé dans le domaine numérique. En rapprochant les décideurs politiques de la région ALC et de l'UE, le projet tend à harmoniser les réglementations relatives au numérique, à améliorer la gouvernance numérique à l'échelle nationale, intra-régionale et bi-régionale et à renforcer les capacités des institutions spécialisées en matière de développement de politiques numériques.

Axe 1

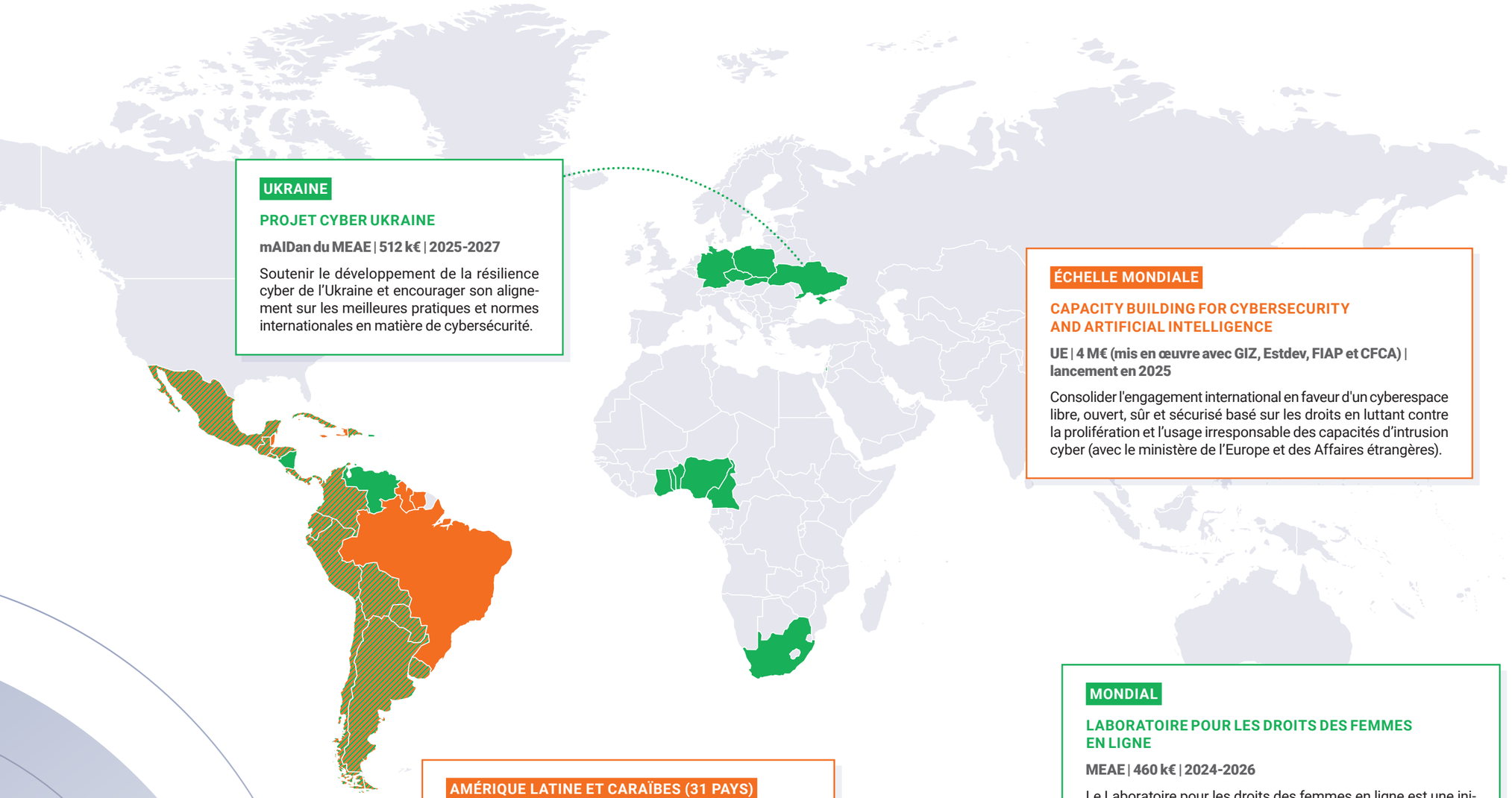
ÉLABORATION ET RENFORCEMENT DE CADRES STRATÉGIQUES, RÉGLEMENTAIRES ET LÉGAUX ET PROMOTION DE DIALOGUES POLITIQUES

L'agence accompagne les pays partenaires dans la mise en place de cadres légaux, stratégiques, politiques efficaces en matière de cybersécurité au niveau national et au niveau régional, en s'appuyant sur une approche holistique, multipartite et inclusive. Expertise France promeut le dialogue et la convergence entre les politiques publiques sur cette thématique et valorise l'approche européenne et ses standards en la matière.

Axe 2

PROTECTION DES INFRASTRUCTURES CRITIQUES

Face à l'augmentation des attaques ciblant les infrastructures critiques, Expertise France met l'accent sur la protection de ces systèmes essentiels. L'agence accompagne les pays partenaires dans l'évaluation et la gestion des risques cyber, en promouvant l'adoption de normes et de bonnes pratiques en matière de cybersécurité. Elle encourage également la coopération internationale pour la mise en place de mécanismes de réponse aux incidents.



UKRAINE

PROJET CYBER UKRAINE

mAIDan du MEAE | 512 k€ | 2025-2027

Soutenir le développement de la résilience cyber de l'Ukraine et encourager son alignement sur les meilleures pratiques et normes internationales en matière de cybersécurité.

ÉCHELLE MONDIALE

CAPACITY BUILDING FOR CYBERSECURITY AND ARTIFICIAL INTELLIGENCE

UE | 4 M€ (mis en œuvre avec GIZ, Estdev, FIAP et CFCA) | lancement en 2025

Consolider l'engagement international en faveur d'un cyberespace libre, ouvert, sûr et sécurisé basé sur les droits en luttant contre la prolifération et l'usage irresponsable des capacités d'intrusion cyber (avec le ministère de l'Europe et des Affaires étrangères).

AMÉRIQUE LATINE ET CARAÏBES (31 PAYS)

EL PACCTO 2.0

UE | 58 M€ | 2023-2027

EL PAcCTO (Programme Europe-Amérique latine d'assistance contre la criminalité transnationale organisée) est un programme de coopération internationale financé par l'Union européenne qui vise à contribuer à la sécurité et à la justice en Amérique latine en soutenant la lutte contre la criminalité transnationale organisée.
Le programme déploie des actions visant à renforcer les capacités des forces de sécurité dans la lutte contre la cybercriminalité, en particulier sur les usages malveillants de l'intelligence artificielle.

MONDIAL

LABORATOIRE POUR LES DROITS DES FEMMES EN LIGNE

MEAE | 460 k€ | 2024-2026

Le Laboratoire pour les droits des femmes en ligne est une initiative française d'envergure internationale réunissant des États, des organisations internationales, des organisations de la société civile, des plateformes privées, des chercheurs ainsi que tous les acteurs impliqués dans la promotion et la défense des droits des femmes en ligne.
Dans ce cadre, Expertise France met en œuvre un projet dont l'objectif est d'identifier, prévenir et combattre les violences fondées sur le genre en ligne. Il s'agit d'apporter un appui opérationnel et technique dans l'animation d'un espace de coordination et d'échanges entre les acteurs, et de soutenir des initiatives concrètes visant à apporter des solutions techniques et produire de la recherche en matière de violences en ligne fondées sur le genre.

Axe **3**

RENFORCEMENT DE CAPACITÉS, SENSIBILISATION ET FORMATION

Le renforcement de capacités, la sensibilisation et la formation constituent des éléments clés de l'approche d'Expertise France. L'agence développe et met en œuvre des programmes de sensibilisation à la cybersécurité destinés aux citoyens, aux professionnels et aux décideurs politiques. Elle propose également des actions spécifiques aux acteurs du secteur public et privé, afin de renforcer leurs compétences en matière de cybersécurité.

Axe **4**

LUTTE CONTRE LES MENACES HYBRIDES ET LES INGÉRENCES ÉTRANGÈRES EN LIGNE

Expertise France a développé une offre de service et des partenariats pour renforcer la sécurité nationale face aux menaces croissantes liées aux ingérences étrangères, aux cyberattaques et à la manipulation de l'information, qui passent de plus en plus par les canaux numériques et le recours à l'IA. L'action d'Expertise France vise à développer des stratégies pour détecter et contrer ces menaces, pour renforcer la coopération internationale, favoriser le partage d'informations et lutter contre les activités ayant des visées de déstabilisation politique (campagnes de désinformation, manipulation de l'opinion publique etc.)

Agence publique, Expertise France est l'acteur interministériel de la coopération technique internationale, filiale du groupe Agence française de développement (groupe AFD). Deuxième agence par sa taille en Europe, elle conçoit et met en œuvre des projets qui renforcent durablement les politiques publiques dans les pays en développement et émergents. Gouvernance, sécurité, climat, santé, éducation... Elle intervient sur des domaines clés du développement et contribue aux côtés de ses partenaires à la concrétisation des objectifs de développement durable (ODD).

Pour un monde en commun.

© Kit_Unsplash

Juillet 2025

Certifié PEFC / Ce produit est issu de forêts gérées durablement et de sources contrôlées. / pefc-france.org

Design LUCIOLE