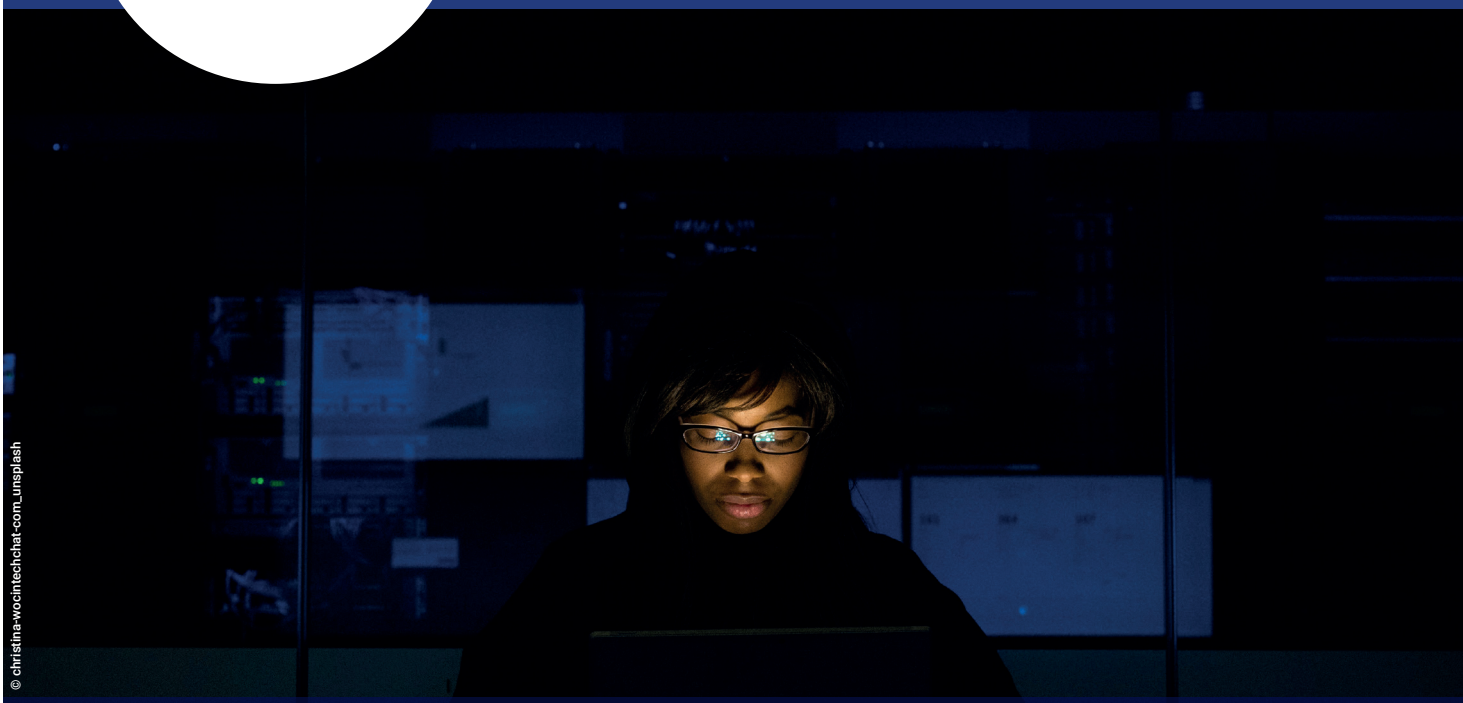
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

EXPERTISE FRANCE
GROUPE AFD

Expertise France and cyber-resilience



© christina-wocintechchat-com_unsplash

100+
experts deployed on short and long-term assignments

€27 m
committed since 2014

38
countries covered

Expertise France plays a critical role in reinforcing security and improving resilience in cyberspace around the world. Working closely alongside national and international partners, the agency spearheads a number of ambitious projects to shield individuals, organisations and critical infrastructure against an increasingly sophisticated and multi-faceted range of cyber threats.

Know how in common

Supporting our partners in improving their cybersecurity

Rapidly spreading information technologies, digital transformation and interconnected systems across Expertise France's partner countries leave the door wide open to a host of potential vulnerabilities and serious risks, including cybercrime, attacks waged on critical services and infrastructure, and attempts to destabilise democracies through digitally enabled interference.
These risks are rising, especially when technology advances too quickly. The economic and social benefits of cyberspace cannot be achieved without a safe and secure underlying digital environment. Expertise France is taking action to guide its partners in tightening up security in their cyberspace.

Accelerating the uptake of new technologies features high on the priority list at Expertise France, which is leading actions in a number of sub-areas, such as developing artificial intelligence, digitally transforming government services, promoting digital entrepreneurship, and harnessing spatial data.

In today's world, IT plays a vital role in managing many critical systems, such as energy, health, telecommunications and financial systems. Incidents can bring essential sectors to a standstill, exacerbate humanitarian crises, and put the brakes on economic growth, especially in developing countries.

Cyberattacks, whether phishing, ransomware or malware, are striking with greater frequency and sophistication, not only representing a threat to businesses and government institutions, but also citizens.

Numerous examples of recent cyberattacks paint a revealing picture of the devastating effects that these threats can potentially cause:

- In December 2024, Namibia's national telecommunications operator, Telecom Namibia, fell victim to a major ransomware attack. The hack resulted in the breach and leak of sensitive customer data, with almost 500,000 records stolen.
- In December 2021, several departments of Brazil's Ministry of Health fell prey to a ransomware attack that led to the loss of Covid-19 vaccination data for millions of people.
- According to estimates, some 46% of Vietnam's public agencies and companies reported being the target of at least one cyberattack in 2024.

Therefore, investing in cybersecurity and, more generally, cyber-resilience across developing countries is key to ensuring inclusive and ustainable digital growth, while minimising the number of vulnerabilities in an ever interconnected world. This process is fully consistent with the European Union's international digital strategy known as the Global Gateway.

Expertise France is actively involved in efforts to ramp up cybersecurity by proposing approaches geared towards the needs of partner countries, with particular focus on strengthening digital security and resilience to withstand today's cyber threats.

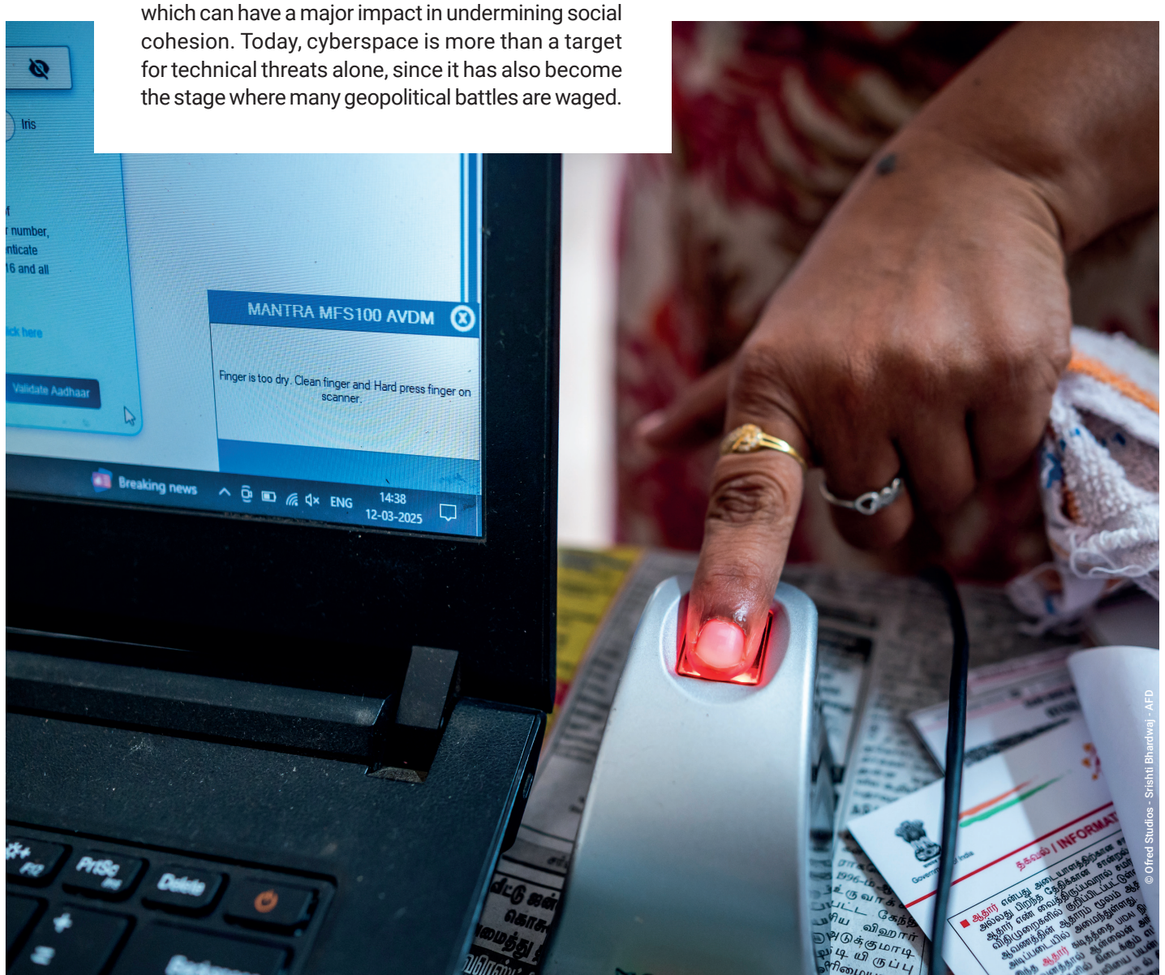
Expertise France's strategy dovetails seamlessly with France's ambitions to improve international cooperation on cybersecurity, by helping build cyber-resilience and bolster cybersecurity in voluntary countries suffering from the weakest protection against threats, with the overriding aim of bringing greater overall stability to cyberspace.

Expertise France is committed to championing French - and European - public and private expertise in this particular area and galvanising the national ecosystem into action (French Cybersecurity Agency - ANSSI, Viginum, Campus Cyber, and so on).

Expertise France embraces a holistic approach. In addition to its involvement in shaping public policy, legislation and regulations, it also delivers on-the-ground support by providing its partners with the response capabilities, expertise and solutions to tackle failures or attacks.

We can harness our broad array of services to stand firmly beside our partners in fighting against digital threats in the geopolitical arena, such as manipulated information or public opinion over digital channels, which can have a major impact in undermining social cohesion. Today, cyberspace is more than a target for technical threats alone, since it has also become the stage where many geopolitical battles are waged.

Expertise France's partner countries are facing an increasingly hybrid and advanced set of threats, which can combine several tactics (human error or negligence, malicious acts, disinformation, and so on) to harm their targets by disrupting the economy or democratic processes. Expertise France is capable of rolling out technical support to thwart certain destabilisation strategies, providing resources and methods for collecting intelligence, improving prevention and restoring systems in the wake of an outage or attack, and deploying operational defence and response strategies to counter malicious acts. For example, Expertise France can offer guidance in defining strategies aimed at injecting greater physical security into telecommunications infrastructures.



© Ofred Studios - Srishti Bhardwaj - AFD

Our focus areas for action and projects implemented

GREECE

SUPPORTING CYBERSECURITY REFORMS

EU | €400 k | 2025-2026

The project aims to support Greece in designing, developing and implementing cybersecurity reforms in line with the NIS2 Directive and the national regulatory framework. The main objective is to strengthen sector governance, increase the security of the critical infrastructure supply chain, especially in the public sector, and raise greater awareness among key stakeholders.

CENTRAL ASIA - KYRGYZSTAN, KAZAKHSTAN, UZBEKISTAN, TURKMENISTAN & TAJIKISTAN

TEI DIGITAL CENTRAL ASIA - CYBER COMPONENT

EU | €20 m | 2025-2028

Expertise France promotes access to and use of satellite connections, especially for women, young people and minority groups, with the aim of improving their inclusion in society and the economy through digital technology.

WEST AFRICA - ECOWAS STATES: BENIN, CAPE VERDE, CÔTE D'IVOIRE, GAMBIA, GHANA, GUINEA,GUINEA-BISSAU, LIBERIA, NIGERIA, SENEGAL, SIERRA LEONE, TOGO - MAURITANIA

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

EU | €7.5 m | 2019-2024

Expertise France has contributed to stepping up cybersecurity and the fight against cybercrime in the ECOWAS States and Mauritania by implementing the OCWAR-C project. The project has been instrumental in building a more resilient and robust information infrastructure, improving local anti-cybercrime capabilities by establishing strategic and legal frameworks,strengthening cybersecurity institutions, raising greater awareness of digital hygiene, and creating and increasing national capabilities for responding to cyber incidents.

ASIA - INDIA, INDONESIA, JAPAN, MALAYSIA, PHILIPPINES, SOUTH KOREA, SINGAPORE, THAILAND, VIETNAM

ESIWA/ESIWA+

EU | €15 m + €9 m | 2020-2027

As the European Union's flagship programme in the Indo-Pacific, the **ESIWA project** aims to forge Europe's status as a relevant player in enhancing security and defence in the region. By implementing the project's cybersecurity component, Expertise France has supported the EU's efforts to promote international law in cyberspace, disseminate cyber-diplomacy principles and strengthen cooperation on cybersecurity by fostering dialogue and organising conferences in close liaison with national and regional cybersecurity agencies and Member States.
The second phase of the ESIWA+ project builds on the action that has been taken since 2020 to carve the European Union's reputation as a relevant player in security and defence issues in the Indo-Pacific region.

LATIN AMERICA AND THE CARIBBEAN

EU-LAC DIGITAL ALLIANCE

EU | €11 m | 2023-2027

Expertise France is implementing the cybersecurity component of Pillar 1 of the EU-LAC Digital Alliance, which is focused on ramping up the digital transition across the Latin America-Caribbean region, while strengthening the EU's role as a partner and leading force in the field of digital technology. By bringing together policy-makers from the LAC region and the EU, the project endeavours to standardise digital regulations, improve digital governance on a national, intra-regional and bi-regional scale, and strengthen the capacity of specialised institutions for developing digital policies.

KENYA

CYBER KENYA: STRENGTHENING THE RESILIENCE OF KENYA'S CYBERSECURITY ECOSYSTEM

EU | €3 m | 2025-2028

The project is aimed at bolstering the resilience of Kenya's cybersecurity ecosystem so that citizens can benefit from an open, free, secure, gender-responsive and peaceful cyberspace. Expertise France is involved in improving the cybersecurity regulatory and legal frameworks, strengthening cybersecurity incident management capabilities, and increasing users' cybersecurity culture and capacities.

DJIBOUTI, KENYA, SOMALIA

INITIATIVE FOR DIGITAL GOVERNMENT AND CYBERSECURITY (IDGC)

EU and BMZ | 2022-2025

Funded jointly by the European Union and the German Federal Ministry for Economic Cooperation and Development (BMZ), the "Initiative for Digital Governance and Cybersecurity" is designed to help Member States in the Horn of Africa, particularly Kenya, Somalia and Djibouti, improve the delivery of public services through enhanced and secure digital channels. Expertise France implemented the cybersecurity component, thereby contributing to the improvement of the institutional, regulatory and operational frameworks, while raising awareness of cybersecurity issues.

Area 1

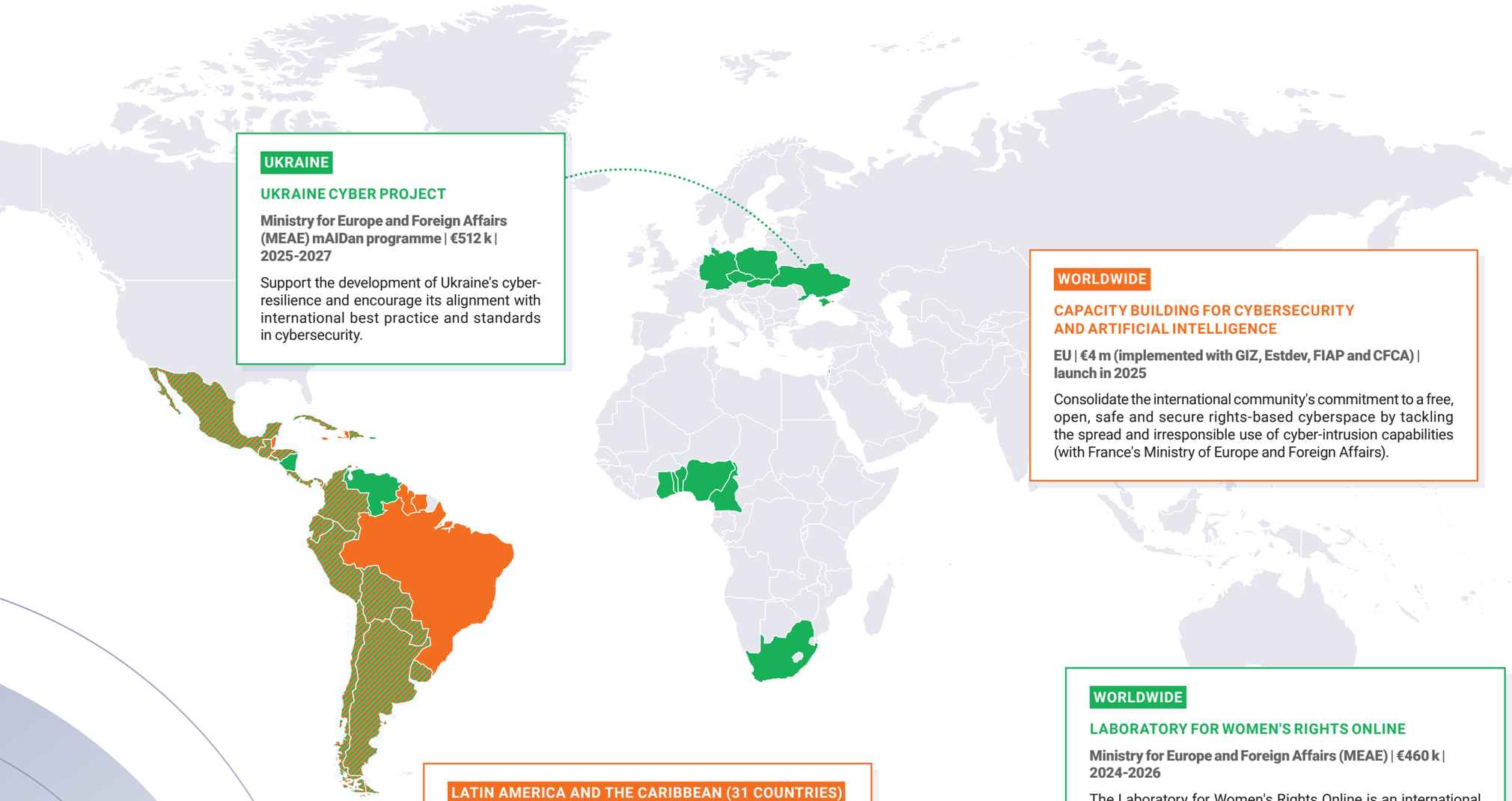
DEVELOP AND STRENGTHEN STRATEGIC, REGULATORY AND LEGAL FRAMEWORKS AND FOSTER POLICY DIALOGUE

The agency supports partner countries in setting up effective legal, strategic and policy frameworks to improve cybersecurity on a national and regional level, based on an overarching, multi-stakeholder and inclusive approach. Expertise France fosters dialogue and convergence between public policies on this issue and promotes the European approach and its standards in this area.

Area 2

PROTECT CRITICAL INFRASTRUCTURE

Faced with an onslaught of attacks targeting critical infrastructure, Expertise France is stepping up its efforts to protect these essential systems. The agency assists partner countries in assessing and managing cyber risks by promoting the adoption of cybersecurity standards and best practice. France Expertise also encourages international cooperation for setting up incident response mechanisms.



UKRAINE

UKRAINE CYBER PROJECT

Ministry for Europe and Foreign Affairs (MEAE) mAIDan programme | €512 k | 2025-2027

Support the development of Ukraine's cyber-resilience and encourage its alignment with international best practice and standards in cybersecurity.

WORLDWIDE

CAPACITY BUILDING FOR CYBERSECURITY AND ARTIFICIAL INTELLIGENCE

EU | €4 m (implemented with GIZ, Estdev, FIAP and CFCA) | launch in 2025

Consolidate the international community's commitment to a free, open, safe and secure rights-based cyberspace by tackling the spread and irresponsible use of cyber-intrusion capabilities (with France's Ministry of Europe and Foreign Affairs).

LATIN AMERICA AND THE CARIBBEAN (31 COUNTRIES)

EL PACCTO 2.0

EU | €58 m | 2023-2027

EL PAcCTO (Europe-Latin America Programme of Assistance against Transnational Organised Crime) is an international cooperation programme funded by the European Union that seeks to contribute to security and justice in Latin America by supporting the fight against transnational organised crime.
The programme includes actions to strengthen the security forces' capabilities in fighting against cybercrime, especially the malicious uses of artificial intelligence.

WORLDWIDE

LABORATORY FOR WOMEN'S RIGHTS ONLINE

Ministry for Europe and Foreign Affairs (MEAE) | €460 k | 2024-2026

The Laboratory for Women's Rights Online is an international French initiative that brings together governments, international organisations, civil society organisations, private platforms, researchers and all those involved in advocating and defending women's rights online.
As such, Expertise France is implementing a project to identify, prevent and curb gender-based violence online. The objective is to provide operational and technical support in leading a platform where stakeholders can discuss and coordinate their efforts, as well as support tangible initiatives for delivering technical solutions and producing research into gender-based violence online.

Area **3**

BUILD CAPACITIES, RAISE AWARENESS AND PROVIDE TRAINING

Capacity-building, awareness-raising and training are key elements of Expertise France's approach. The agency develops and implements programmes to educate citizens, professionals and political decision-makers on cybersecurity issues. It also proposes specific initiatives to the public and private sector for enhancing cybersecurity skills.

Area **4**

COMBAT HYBRID THREATS AND FOREIGN INTERFERENCE ONLINE

Expertise France has developed several services and partnerships to shore up national security in response to the growing threat posed by foreign interference, cyber-attacks and manipulated information, which are increasingly spread over digital channels and involve the use of AI. Expertise France's action is aimed at pioneering strategies to detect and counter such threats, strengthening international cooperation, promoting information sharing, and tackling activities looking to destabilise the political system (disinformation campaigns, manipulated public opinion, etc.).

Expertise France is the inter-ministerial public agency for international technical cooperation and a subsidiary of the Agence Française de Développement (AFD) Group. The second largest agency in Europe, it designs and implements projects that sustainably strengthen public policies in developing and emerging countries. Governance, security, climate, health, education... It works in key areas of development and contributes alongside its partners to achieving the Sustainable Development Goals (SDGs).

For a world in common.

© Kit_Unsplash

October 2025

Design LUCIOLE