

EU-LAC Digital Alliance Cyber Collaboration Platform

Action Area I: Diplomatic level

Specific objective	Reinforce cyber diplomacy capacities and foster closer bi-regional cooperation
Information Sharing	1. Identify priorities and share good practices aimed at strengthening cyber diplomacy.
Cyber Capacity Building	2. Showcase and scale-up existing cyber diplomacy capacity-building offers (e.g. trainings, exercises) to strengthen the framework of responsible state behaviour in cyberspace, in particular regarding: <ul style="list-style-type: none">a. building capacities of MFA points of contacts according to the needs of each country (e.g. cyber ambassadors, coordinators)b. national capacities for the application of international law in cyberspacec. implementation of the existing norms of responsible state behaviour in cyberspaced. supporting joint participation of EU and LAC region experts in multilateral discussions, such as regular institutional dialogue and the future Programme of Action (PoA) at the UN.
Joint Initiatives	3. Strengthen cooperation and confidence-building measures at the regional and global levels through organising an annual meeting of cyber diplomats from the EU and LAC and supporting existing global and regional efforts for directories of points of contact (i.e. by UN, OAS), to ensure bi-regional communication.

EU-LAC Digital Alliance Cyber Collaboration Platform

Action Area II: Policy level

Specific objective	Strengthen national, regional and bi-regional cyber ecosystems, as well as promotion of triangular cooperation
Information Sharing	<ul style="list-style-type: none">4. Exchange good practices and information in relation to cyber threats, incidents, vulnerabilities, awareness-raising initiatives, training, exercises and skills, capacity building, standards and technical specifications, with particular focus on strengthening the participation of the private sector, academia and civil society.5. Exchange advice and cooperate on emerging cybersecurity policy initiatives and the overall consistency of sector-specific cybersecurity requirements.

OPERATIONAL TAKEAWAYS

6. Share best practices and set-up specific policy dialogues at national and/or sub-regional level focusing on risk mitigating measures to be promoted to ensure trusted digital connectivity (including the European 5G toolbox principles).

Cyber Capacity Building

7. As part of the Team Europe³ contribution to the EU-LAC Digital Alliance, providing technical assistance in strengthening regulatory, policy and institutional capacities at national, sub-regional and regional levels, relying on the existing tools, including:
 - a. Tallinn Summer School of Cyber Diplomacy for Points of Contacts and/or Cyber ambassadors (EU & EE);
 - b. Study visit: capitalising on existing expertise in European Union Member States for in-person knowledge sharing (i.e., CZ, FR, ES, EE);
 - c. Technical assistance, including through the transfer of technology, supporting the development, revision, and/or implementation of cybersecurity strategies, establishment of national cybersecurity agencies, SOCs and CSIRTs leveraged through EU-Delegations, EU Knowledge Hub Digital and EU CyberNet (including LAC4);
 - d. Table-top exercises and awareness raising initiatives focused on developing sound cyber hygiene and cyber culture, especially among youth (ENISA, EU CyberNet/LAC4);
 - e. Triangular cooperation on strengthening of capacity building in the area of cybersecurity within the EU-LAC Digital Alliance.

Joint Initiatives

8. Identify means to develop and implement adequate cybersecurity risk-management measures, in particular regarding incidents and associated cyber threats, risks and vulnerabilities, including all relevant stakeholders.

EU-LAC Digital Alliance Cyber Collaboration Platform

Action Area III: Technical level

Specific objective

Boost resilience of critical infrastructure to ensure that societies are protected and can fully benefit from the human-centric digital transformation.

³ [Team Europe](#) consists of the European Union, EU Member States — including their implementing agencies and public development banks — as well as the European Investment Bank (EIB) and the European Bank for Reconstruction and Development (EBRD). As outlined in the 2017 European Consensus for Development, it is an approach that coordinates key European development actors to join forces in a coordinated and committed way, to combine resources and expertise.



OPERATIONAL TAKEAWAYS

Information Sharing

9. Sharing good practices, models, threat intelligence, and lessons in support of the identification and protection of critical infrastructure, including in testing, developing and introducing secure networks, among others.
10. Developing cooperation with the private sector, industry, leading security professionals, international organisations and all relevant stakeholders to promote trusted connectivity.

Cyber Capacity Building

11. As part of the Team Europe contribution to the EU-LAC Digital Alliance, providing relevant information and demand-based technical assistance in:
 - a. Framework and guides for LAC countries to support the identification of critical infrastructure and implementation of industry standards, including by sharing concrete step-by-step approaches and guidance.
 - b. national and regional capacities for LAC countries to develop large-scale cybersecurity incident and crisis response plans (e.g. identification of national preparedness measures and objective, tasks and responsibilities of cyber crisis management authorities, identification of the relevant public and private structures involved).
 - c. strengthening cybersecurity capacities of officials, civil society and private sector.

Joint Initiatives

12. Support the development of a shared situational awareness for cybersecurity incidents and crises as well as support institutional responses in relation to such incidents and crises.

