



Chairs' Conclusions

The EU-LAC High Level Dialogue on Cybersecurity, held in Santo Domingo (Dominican Republic) in February of 2024 is the first policy dialogue advancing from the 2023 EU-LAC Digital Alliance Days in Cartagena (Colombia). The dialogue was co-chaired by the Dominican Republic and the European Commission. This document outlines the chairs' conclusions on actions identified by participants of the dialogue as valuable opportunities for bi-regional cooperation in cybersecurity.

As per the 2023 Joint Declaration for an EU-LAC Digital Alliance¹, signed by the European Union Member States and 21 governments of Latin America and the Caribbean, the EU-LAC Digital Alliance is a voluntary partnership based on shared values and a mutual vision for a human-centric digital transformation and efforts towards bridging the digital divides. These action areas and joint collaborations reflect this vision for the partnership in the field of cybersecurity.

As part of the Global Gateway strategy, the EU-LAC Digital Alliance will work to implement the proposed actions, which constitute the roadmap towards the EU-CELAC Summit in 2025.

These chairs' conclusions constitute an invitation for the governments and multistakeholder community to cooperate by building on the existing initiatives, avoiding duplication of existing efforts and identifying new opportunities for joint actions.²

Overall objective of the Digital Alliance High-Level Policy Dialogue on Cybersecurity	LAC and EU cybersecurity frameworks promote a human-centric digital transformation and are effectively implemented to provide open, safe, secure, stable, accessible, peaceful and human-centric digital space for all citizens, businesses, and governments.
Overall mode of action towards the EU-CELAC Summit in 2025	Establishment of a bi-regional cyber collaboration fostering an enabling environment towards cyber resilience in the EU and LAC.

¹ [EU-LAC: Joint Declaration on a Digital Alliance \(europa.eu\)](https://ec.europa.eu/europea/en/eu-lac/joint-declaration-digital-alliance). These are the 20 LAC countries that adopted the Joint Declaration in the margins of the 2023 EU-CELAC Summit: Argentina, Bahamas, Barbados, Brazil, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Panama, Paraguay, Peru, Suriname, Trinidad and Tobago and Uruguay. In 2024, Belize, Guyana and Grenada also joined the Digital Alliance as additional members and so did Bolivia in 2025.

² These activities will be carried out within the framework of the EU-LAC Digital Alliance, reflecting the mutual interest to promote collaboration between both regions. It is important to emphasize that these activities are of a non-binding nature, and therefore do not generate any obligations for LAC countries, nor for the European Union. The only prerequisite to participate in these activities is to be a member of the Digital Alliance. This can be done by adhering to the Joint Declaration on a Digital Alliance.

OPERATIONAL TAKEAWAYS

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	<ol style="list-style-type: none">1. Identify priorities and share good practices aimed at strengthening cyber diplomacy.
Cyber Capacity Building	<ol style="list-style-type: none">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:<ol 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	<ol style="list-style-type: none">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	<ol 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

Cyber Capacity Building	<p>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).</p> <p>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:</p> <ul style="list-style-type: none">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	<p>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.</p>

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	<ol style="list-style-type: none">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	<ol style="list-style-type: none">11. As part of the Team Europe contribution to the EU-LAC Digital Alliance, providing relevant information and demand-based technical assistance in:<ol style="list-style-type: none">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	<ol style="list-style-type: none">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.

