



European  
Commission

Results and  
Indicators for  
Development

# Cybersecurity

International  
Cooperation and  
Development

**EUROPEAN COMMISSION**

Directorate-General for International Partnerships

Unit D4 - Performance, Results and Evaluation; Internal  
Communication, Knowledge Management and Collaborative Methods

Contact us at [INTPA-EU-RESULTS@ec.europa.eu](mailto:INTPA-EU-RESULTS@ec.europa.eu)

*Version June 2021*

# Results and Indicators for Development

## General Introduction

This **guidance for action design** has been developed by INTPA Unit D4 “Performance, Results and Evaluation; Internal Communication, Knowledge Management and Collaborative Methods” jointly with INTPA Thematic Units.

It is **addressed** to all colleagues involved in the preparation of action documents and project documents and offers a handy tool to develop solid logical framework matrices. It identifies clear and measurable results statements that are in line with INTPA policy priorities, as well as with the UN Sustainable Development Goals (SDGs), along with a range of good indicators to monitor progress. It will be updated regularly to reflect evolving priorities.

Its **main objective** is to enhance the quality of DEVCO interventions – both in terms of design as well as of monitoring and reporting in the course of implementation.

The **need for this type of guidance** was identified in the framework of the results-reporting process led by INTPA D4, as well as through its systematic review of all action documents presented to Quality Review Group meetings.

The present guidance covers INTPA strategies in various sectors, and presents for each sector:



**1. EU policy priorities:** a short narrative explaining EU policy priorities and commitments as articulated in key policy and strategic documents.



**2. Results Chain:** a diagram showing the main results (impact, outcomes, outputs) that EU development interventions are expected to achieve in the sector, reflecting EU policy priorities and commitments.



**3. List of Sector Indicators:** examples of measurable indicators associated to each result statement are provided, that may be used in Logframe Matrices at project/ programme level.



You can access the online Sector Indicator Guidance at <https://europa.eu/capacity4dev/results-and-indicators>. For further information and/or to provide feedback please contact INTPA Unit 04 at [INTPA-EU-RESULTS@ec.europa.eu](mailto:INTPA-EU-RESULTS@ec.europa.eu)

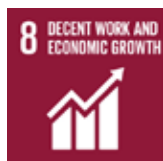


# 1. EU Policy Priorities



Ever-evolving Information and Communications Technologies (ICTs) have revolutionised how we work over the past 20 years, resulting in profound global implications and scale-up of digital technologies. However, risks and challenges associated with improved access to ICTs and the growing of internet penetration are often underestimated. Therefore, cyber capacity building is crucial to promote cyber security across the globe.

Since the adoption of its Cybersecurity Strategy in 2013, the EU has been leading on international cyber capacity building and systematically linking these efforts with its development cooperation funds. Moreover, in 2017 there was a clear recognition at the EU level that cybersecurity should be considered a transversal issue in development cooperation that can contribute to the realisation of the 2030 Agenda for Sustainable Development, as stipulated in the EU's Digital4Development policy framework. In the cybersecurity sector, the desired impact/overall objective is to provide the citizens of developing countries an open, free, secure, resilient and peaceful cyberspace. Reference to this can be found as a target under SDG 9 "Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation", as well as under SDG 4 "Quality education", SDG 8 "Decent work and economic growth", SDG 16 "Peace, Justice and Strong Institutions".



The significance of efforts to build national resilience in third countries as a means of increasing the level of cybersecurity globally, with positive consequences for the EU, was also recognised in the 2017 Joint Communication on “Resilience, deterrence and defence: Building strong cybersecurity for the EU”.

EU interventions in this field strengthen the legislative, institutional and civil society capacities for promoting cyber security, cyber hygiene and awareness. They also help to develop new mechanisms for effective information sharing, consultation and coordination on cyber incidents.

The outcomes of these interventions include the adoption and implementation of a coherent, holistic and actionable national approach to cyber resilience; the operationalisation of cyber crisis management structures; increased trust of users, organisations, and companies in the use of cyberspace; as well as the alignment of legislation on cybercrime and electronic evidence with international standards.

The desired long-term impact is that citizens of developing countries enjoy an open, free, secure, resilient and peaceful cyberspace.

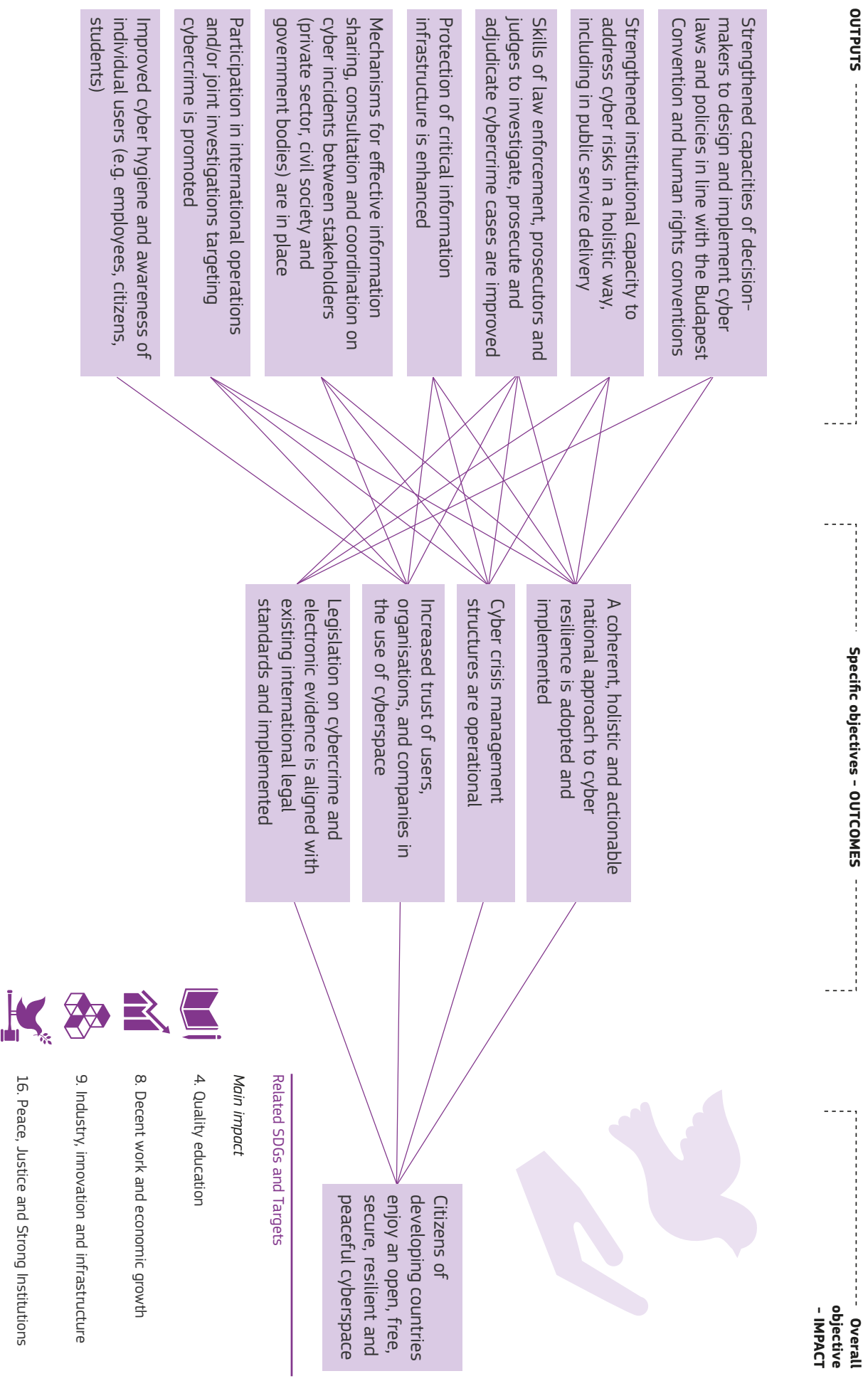
### **EU strategic priorities**

In order to leverage the threats and challenges related to cybersecurity, EU action is structured around the following strategic priorities, as defined in the Joint Communication:

- Promoting legislative reforms and strengthening the capacity of decision-makers to design and implement cyber laws and policies in line with the Budapest Convention and human rights conventions;
- Supporting an overarching strategic framework and strengthening institutional capacity to address cyber risks in a holistic way, including in public service delivery;
- Developing education, professional training and expertise in this field and improving cyber hygiene and awareness of individual users;
- Enhancing mechanisms for effective information sharing, consultation and coordination on cyber incidents between stakeholders (private sector, civil society and government bodies).





## 2. Results Chain







## 3. List of Sector Indicators

Result	Indicators
<p> <b>Impact</b></p> <p><b>Citizens of developing countries enjoy an open, free, secure, resilient and peaceful cyberspace</b></p>	<ul style="list-style-type: none"> <li> <p>✔ Country score in the ITU Global Cybersecurity and Cyberwellness Index (Score)  <i>data source</i> Global Cybersecurity and Cyberwellness Index website</p> </li> <li> <p>✔ Country score in the World Economic Forum's Network Readiness Index (Score)  <i>data source</i> World Economic Forum, Network Readiness Index</p> </li> <li> <p>✔ Country score in the Freedom on the Net - Freedom House (Score: 0=Most Free, 100=Less Free) (Score)  <i>data source</i> Freedom on the Net Report  <a href="https://freedomhouse.org/report/freedom-net">https://freedomhouse.org/report/freedom-net</a></p> </li> <li> <p>✔ Existence of independent national human rights institutions in compliance with the Paris Principles (Qualitative)  <i>data source</i> Global SDG Indicators Database</p> </li> </ul>
Result	Indicators
<p> <b>Outcome</b></p> <p><b>A coherent, holistic and actionable national approach to cyber resilience is adopted and implemented</b></p>	<ul style="list-style-type: none"> <li> <p>✔ Extent to which cybercrime is mentioned in a national strategic framework / cyber strategy (Qualitative)  <i>data source</i> National strategic documents, Baseline and endline studies conducted and budgeted by the EU-funded intervention</p> </li> <li> <p>✔ Status of national strategic framework on cybersecurity (Qualitative)  <i>data source</i> Strategies and policy documents and baseline and endline studies conducted and budgeted by the EU-funded intervention</p> </li> <li> <p>✔ Status of an implementation plan (or roadmap) for delivering on the strategic commitments in the field of cybersecurity (Qualitative)  <i>data source</i> Government Implementation plan/Roadmap documents and reports</p> </li> <li> <p>✔ Status of a cybercrime/high-tech crime units in the relevant government institutions (Qualitative)  <i>data source</i> Government organization charts and systematization documents, Baseline and endline studies conducted and budgeted by the EU-funded intervention</p> </li> <li> <p>✔ Number of locally-based organisations that contribute to dialogue with central authorities and cybersecurity actors  <i>data source</i> Baseline and endline surveys conducted and budgeted by the EU-funded intervention mappings conducted by the EU-funded intervention</p> </li> </ul>



Result	Indicators
<p> <b>Outcome</b></p> <p><b>Cyber crisis management structures are operational</b></p>	<ul style="list-style-type: none"> <li> <p>✔ Existence of a cyber-related budget line (in particular linked to CERT/CSIRT) in the national budget (Qualitative)  <i>data source</i> National budget</p> </li> <li> <p>✔ Amount of the national budget allocated to agencies with cybersecurity competence (EUR) <i>data source</i> National budget and Baseline and endline studies conducted and budgeted by the EU-funded intervention</p> </li> <li> <p>✔ Status of national body mandated with cyber crisis management (Qualitative)  <i>data source</i> NLaws and regulations, Government reports and organizational charts</p> </li> <li> <p>✔ Status of policy provisions defining the responsibilities and resources of institutions competent for prevention, protection and recovery from cyber attacks and/or accidental failures  <i>data source</i> Laws and regulations and baseline and endline studies conducted and budgeted by the EU-funded intervention</p> </li> <li> <p>✔ Status of cyber-related inspection and/or audit services within the individual institutions and bodies responsible for incident and crisis management (Qualitative)  <i>data source</i> National legislation and policies, Government reports, Organizational charts</p> </li> </ul>

Result	Indicators
<p> <b>Outcome</b></p> <p><b>Increased trust of users, organisations, and companies in the use of cyberspace</b></p>	<ul style="list-style-type: none"> <li> <p>✔ Percentage of individuals who report trust in the use of the cyberspace (disaggregated by sex and age)  <i>data source</i> Baseline and endline surveys of users conducted by the EU-funded intervention</p> </li> <li> <p>✔ Percentage of internet penetration in the country (Percentage)  <i>data source</i> World Bank data on individuals using the Internet</p> </li> <li> <p>✔ Percentage of organisations and companies that report trust in the use of the cyberspace (disaggregated by sex of company/organisation director) (Percentage)  <i>data source</i> Baseline and endline public perception surveys conducted by the EU-funded intervention</p> </li> <li> <p>✔ Percentage of population that expresses confidence in the capacity of the law enforcement and judicial bodies to tackle cybercrime effectively (disaggregated by sex and age) (Percentage)  <i>data source</i> Baseline and endline public perception surveys conducted by the EU-funded intervention</p> </li> <li> <p>✔ Number of individuals falling victims to cyber attacks (disaggregated by sex) (Number of)  <i>data source</i> National statistical report and baseline and endline surveys conducted and budgeted by the EU-funded intervention</p> </li> <li> <p>✔ Number of companies and organisations falling victims to cyber attacks (Number of)  <i>data source</i> National statistical report and baseline and endline surveys conducted and budgeted by the EU-funded intervention</p> </li> </ul>

Result	Indicators
<p> <b>Outcome</b></p> <p><b>Legislation on cybercrime and electronic evidence is aligned with existing international legal standards and implemented</b></p>	<ul style="list-style-type: none"> <li> <p>✔ Status of legal provisions / regulations on cybercrime and electronic evidence (Qualitative)  <i>data source</i> National statistical report and baseline and endline surveys conducted and budgeted by the EU-funded intervention</p> </li> <li> <p>✔ Status of the accession to/ratification of the Budapest Convention (Qualitative)  <i>data source</i> Council of Europe</p> </li> <li> <p>✔ Number of domestic and/or international prosecutions and cases adjudicated on cybercrime (Number of)  <i>data source</i> Reports from the Ministry of Justice</p> </li> <li> <p>✔ Percentage of cybercrime complaints that are investigated (Percentage)  <i>data source</i> Reports by cybercrime units and prosecution offices</p> </li> </ul>

Result	Indicators
<p><b>Output</b></p> <p><b>Strengthened capacities of decision-makers to design and implement cyber laws and policies in line with the Budapest Convention and human rights conventions</b></p>	<ul style="list-style-type: none"> <li> <p>✔ Status of the national strategic framework on cybersecurity supported by the EU-funded intervention (Qualitative)  <i>data source</i> Draft National Strategy on Cybersecurity, Minutes from the strategy workgroups</p> </li> <li> <p>✔ Status of legislation and/or regulation addressing cyber risks supported by the EU-funded intervention (Number of)  <i>data source</i> Draft laws, Action's progress reports</p> </li> <li> <p>✔ Status of legislation and/or regulation addressing Critical Information Infrastructure Protection (CIIP) supported by the EU-funded intervention (Number of)  <i>data source</i> Database of draft documents (policies and laws), Minutes from the policy development workgroups</p> </li> <li> <p>✔ Status of cyber risk management framework/ guidelines for national authorities supported by the EU-funded intervention (Qualitative)  <i>data source</i> Database of draft documents (guidelines), Minutes from document development workgroup</p> </li> <li> <p>✔ Number of decision-makers trained by the EU-funded intervention who increased their knowledge and/or skills on the importance of cyber policies, design and implementation of national cybersecurity strategies (disaggregated by sex and institution)(Number of)  <i>data source</i> Database participants, pre- and post-training tests</p> </li> <li> <p>✔ Status of constitutional, statutory, policy guarantees for cybercrime and electronic evidence legislation supported by the EU-funded intervention(Qualitative)  <i>data source</i> Database of draft documents (policies), Minutes from the policy development workgroups</p> </li> <li> <p>✔ Status of regulations on the cybersecurity technical standards in line with the international best practices supported by the EU-funded intervention (Qualitative)  <i>data source</i> Database of draft documents (technical standards), Minutes from document development workgroup</p> </li> <li> <p>✔ Status of assessment of existing legislation for compatibility with the Budapest Convention supported by the EU-funded intervention(Qualitative)  <i>data source</i> Baseline and endline studies conducted and budgeted by the EU-funded intervention</p> </li> <li> <p>✔ Extent to which provisions promoting cyber hygiene and technical standards in line with international best practices are integrated in draft laws, regulations and government tenders thanks to support of the EU-funded intervention (Qualitative)  <i>data source</i> Database of draft documents (draft standards and policies), Minutes from the policy development workgroups</p> </li> <li> <p>✔ Number of staff in Ministries/ Parliament mentored by the EU-funded intervention on legislative/ regulatory measures on cyber risks (disaggregated by sex and institution) (Number of)  <i>data source</i> Database of training participants maintained by the Action (disaggregated by sex)</p> </li> <li> <p>✔ Extent to which the national cooperation framework/guidelines were applied in case of a large scale cyber incident or crisis thanks to support provided by the EU-funded intervention(Qualitative)  <i>data source</i> Baseline and endline studies conducted and budgeted by the EU-funded intervention</p> </li> </ul>

Result	Indicators
<p><b>Output</b></p> <p><b>Strengthened institutional capacity to address cyber risks in a holistic way, including in public service delivery</b></p>	<ul style="list-style-type: none"> <li> <p>✔ Number of institutions and organisations participating in periodic cyber risk assessments with support of the EU-funded intervention (Number of)  <i>data source</i> Cyber risk assessment meeting notes, attendance records</p> </li> <li> <p>✔ Number of cyber risk assessments conducted with support of the EU-funded intervention (Number of)  <i>data source</i> Cyber risk assessment reports</p> </li> <li> <p>✔ Number of government representatives trained/mentored by the EU-funded intervention who increased their knowledge and/or skills on cyber hygiene practices and technical standards (disaggregated by sex and institution) (Number of)  <i>data source</i> Database participants and pre- and post-training tests</p> </li> </ul>

Result	Indicators
<p><b>Output</b></p> <p><b>Skills of law enforcement, prosecutors and judges to investigate, prosecute and adjudicate cybercrime cases are improved</b></p>	<ul style="list-style-type: none"> <li> <p>✔ Number of requests handled by national 24/7 points of contact with support of the EU-funded intervention (Number of)  <i>data source</i> National 24/7 points reports</p> </li> <li> <p>✔ Number of table top exercises or mock operations supported by the EU-funded intervention (Number of)  <i>data source</i> Reports on table top exercises and mock operations</p> </li> <li> <p>✔ Number of cybercrime units participating in domestic and international investigations with support of the EU-funded intervention (Number of)  <i>data source</i> Reports on cybercrime domestic and international investigations</p> </li> </ul>

Result	Indicators
<p> <b>Output</b></p> <p><b>Protection of critical information infrastructure is enhanced</b></p>	<ul style="list-style-type: none"> <li> <p>✔ Status of the list of national critical infrastructure supported by the EU-funded intervention (Qualitative) <i>data source</i> Infrastructure inventory reports</p> </li> <li> <p>✔ Status of governance framework for CIIP and cyber incident management supported by the EU-funded intervention (Qualitative) <i>data source</i> Action's progress reports</p> </li> <li> <p>✔ Extent to which the national CERT/CSIRT has established parameters for organizational structure, human resources, tools and processes thanks to support of the EU-funded intervention (Qualitative) <i>data source</i> Baseline and endline studies conducted and budgeted by the EU-funded intervention</p> </li> <li> <p>✔ Number of incident management/response cases monitored and handled by national CERT/CSIRT with support of the EU-funded intervention (Number of) <i>data source</i> CERT/CSIRT incident management/response reports</p> </li> <li> <p>✔ Number of CERT/CSIRT employees mentored/trained with support of the EU-funded intervention (disaggregated by sex) (Number of) <i>data source</i> Database of training participants, pre-and post-training tests</p> </li> </ul>
Result	Indicators
<p> <b>Output</b></p> <p><b>Mechanisms for effective information sharing, consultation and coordination on cyber incidents between stakeholders (private sector, civil society and government bodies) are in place</b></p>	<ul style="list-style-type: none"> <li> <p>✔ Number of MoUs between key private sector entities (CII operators, vendors) and governmental bodies signed with support of the EU-funded intervention (Number of) <i>data source</i> MoU documents</p> </li> <li> <p>✔ Status of membership in FIRST and TF.CSIRT/TI certification (Qualitative) <i>data source</i> FIRST and TF.CSIRT/TI certification reports, database of draft documents (on certification)</p> </li> <li> <p>✔ Number of stakeholders participating in public consultations organised by the EU-funded intervention on the development of national cybersecurity strategic framework (disaggregated by sector and sex of participant) (Number of) <i>data source</i> Consultation meeting notes and attendance records</p> </li> </ul>
Result	Indicators
<p> <b>Output</b></p> <p><b>Participation in international operations and/or joint investigations targeting cybercrime is promoted</b></p>	<ul style="list-style-type: none"> <li> <p>✔ Number of national or transnational operations and/or investigations conducted with capacities created or enhanced by the EU-funded intervention in line with EU policies and international human rights standards (Number of) <i>data source</i> Reports published by the EU-funded intervention</p> </li> <li> <p>✔ Number of international agreements/MoUs on combatting cybercrime signed between the private sector and CSOs with support of the Action (Number of) <i>data source</i> MoU documents</p> </li> <li> <p>✔ Number of international police-to-police requests prepared with support of the EU-funded intervention (Number of) <i>data source</i> Database of police-to-police requests</p> </li> <li> <p>✔ Status of public/public-private reporting mechanisms developed with support of the EU-funded intervention (Qualitative) <i>data source</i> Database of draft documents (public/public-private reporting mechanism procedures)</p> </li> </ul>
Result	Indicators
<p> <b>Output</b></p> <p><b>Improved cyber hygiene and awareness of individual users (e.g. employees, citizens, students)</b></p>	<ul style="list-style-type: none"> <li> <p>✔ Extent to which cyber hygiene and awareness is mentioned in a national strategic framework thanks to support of the EU-funded intervention (Qualitative) <i>data source</i> Draft National Strategy on Cybersecurity, Minutes from the strategy workgroups</p> </li> <li> <p>✔ Status of the Cyber Awareness Month campaign supported by the EU-funded intervention <i>data source</i> Cyber Awareness Month campaign report</p> </li> <li> <p>✔ Number of institutions and organisations reached by the EU-funded campaign promoting cyber hygiene and awareness (Number of) <i>data source</i> Press clipping, events records, online analytics reports</p> </li> <li> <p>✔ Number of individuals reached by the EU-funded campaign promoting cyber hygiene and awareness (disaggregated by sex and age) (Number of) <i>data source</i> Press clipping, events records, online analytics reports</p> </li> <li> <p>✔ Number of persons reached by the cyber awareness raising campaigns and training implemented with support of the EU-funded intervention (disaggregated by sex and age) (Number of) <i>data source</i> Press clipping, events records, online analytics reports</p> </li> </ul>

