Action of the European Union and the Council of Europe on Cybercrime and Electronic Evidence

Approach and action in the Eastern Partnership region

10 YEARS EaP Eastern Partnership

Prepared by the Cybercrime Programme Office of the Council of Europe (C-PROC)

Visibility and Communication Campaign of the CyberEast Project

Initial concept for discussion

Background

Political commitment in the Eastern Partnership region:

- 2013 Declaration on Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership region: source and inspiration for capacity building

- Lack of visibility beyond the project partners

- Need to put the joint action of the EU and the Council of Europe at the forefront

- Also discussed at the capacity building planning meeting in Bucharest in October 2018

- Result: Draft Terms of Reference for Visibility in EaP region

General visibility/communication actions

- Create and moderate an Online Forum/Platform where EaP region related stakeholders can share valuable information, such as training manuals on E-First, OSINT, Darkweb, Judicial Training etc.
- Create a Blog page on the CyberEast page to disseminate Case Studies of successful stories, important developments in the project and the region
- Create a CyberMap of the CyberEast project to promote the agencies/institutions and other initiatives fighting cybercrime in the EaP region (e.g. Restorative Justice Council could be used as a model)
- Identify Influencers on YouTube interested in the large area of social change and partner with them in spreading the capacity building developments on cybercrime and e-evidence
- Catchy Country Factsheets to highlight the developments on cybercrime in EaP countries, or Fast Quiz Cards (e.g. during large events) to have audiences engage with us and learn more about cybercrime
- Develop and share via social media interactive quick quizzes on cybercrime and e-evidence to reach young audiences
- Thematic videos on 5 different subjects
- Possibly reach to larger public by conducting independent opinion surveys on victimization and perception cybercrime, and sharing/disseminating results through national authorities

Activity-specific communication items

- Draft visibility items (notebooks/agendas, pens, roll-ups, posters, banner, registration desk cover, folders, desktop backgrounds, badges, nametags, other printings such as outline, presence list, and feedback form etc., informative signs at the venue entrance, on transfer vehicles etc., T-shirts and memorabilia for regional exercises, and other promotional materials)
- Pre-event info pack
- Press-release
- News item post-event
- Press briefing
- Interviews with key delegates
- Interviews with students in planned Master Programme
- Photo/Video recording
- Dedicated event webpage
- Follow-up information package, including take away notes
- Stories shared on the blog
- Etc.

Stakeholders and roles

EU/EC/agencies/EUDs	EU will monitor all activities under CyberEast, feedback will be integrated in all communication aspects CyberEast will particularly work closely with EUDs in the EaP region before and during events, where necessary and asked by Delegations
Project partners	Disseminating information on cybercrime in the EaP region through their communication channels
C-PROC	Different other projects in the office can help with communication of joint events
Project Team	Roles split mainly between PM and CO, with other team members supporting
CoE Offices in EaP	Facilitating communication with media outlets in the respective countries, visibility providers and any other third party + country-specific visibility
Coe Experts	Spread information via other channels (other events, LinkedIn, etc.)
CoE institutions	Support the activities of CyberEast by posting on their social media
CyberEast teams	Identifying media outlets in their area of expertise and disseminating further information via their communication channels (e.g. press officers)
NGOs/CSOs	Disseminating further specialized work (e.g. CSAM, cyberviolence, etc.) through own or affiliated channels
Mass Media	Partnering with different media outlets at international level or local level
Influencers	Social media influencers can have an innovative involvement in the communication strategy of CyberEast - they can reach large number of people and many hours of views on different subjects

Work breakdown and structure

Phase 1
by end of 2019

- Determine the EU regulations related to communication
- Establish communication at team level
- Establish relations with all stakeholders
- Start drafting a database of media outlets and a Media Folder
- Draft first items of communication and visibility
- Start different online and offline platforms
- Contribute to and complete the entries at the Cybercrime Octopus Community

Phase 2
by end of 2020

- Re-draft communication and visibility items
- Constantly update online and offline platforms
- Constantly update the database of media outlets and the Media Folder
- Create 2 thematic videos
- Define and launch a campaign to run on social media
- Identify and partner with influencers on YouTube
- Collect communication stats and draft an annual communication report
- Start online surveys in countries wishing to run them

Phase 3
by end of project

- Reiterate communication rules with the donor
- Re-draft communication and visibility items
- Constantly update online and offline platforms
- Constantly update the database of media outlets and the Media Folder
- Create 3 more videos
- Continue the campaign on social media
- Design and launch a CyberMap
- Continue to partner with influencers on YouTube
- Collect communication stats and draft an annual communication report

Reach to different stakeholders: trust

- Civil society organizations (EuroDIG Internet Governance community so far, specialized NGOs, etc.)
- Meetings with civil society to enhance transparency
- Work with data protection authorities
- Internet regulatory agencies
- Defence attorneys
- Support to local events bringing together industry and government
- Focus on reporting systems

Project CyberEast:

Joint EU/CoE Action on Cybercrime for Cyber Resilience in the Eastern Partnership region

Cybercrime action background in EaP

Budapest Convention and related standards, including work of the T-CY

EU Milestones/Deliverables 2020 for the Eastern Partnership:

- Full implementation of the Budapest Convention on Cybercrime
- Procedural law powers
- Interagency cooperation
- Public/private cooperation
- International cooperation
- Strong cybercrime investigative units

Political commitment in the Eastern Partnership region:

- 2013 Declaration on Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership region: source and inspiration for capacity building

Project CyberEast: an overview

Project title:	**CyberEast - Action on Cybercrime for Cyber Resilience in the Eastern Partnership region**
Project area:	Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine
Duration:	36 months (20 June 2019 – 20 June 2022)
Budget:	~EUR 4.200.000
Funding:	European Union European Neighbourhood Instrument (90%) and Council of Europe (10%)
Implementation:	Cybercrime Programme Office (C-PROC) of the Council of Europe
Context:	EU4Digital Programmme: Improving Cyber Resilience in the Eastern Partnership countries

CyberEast Objective 1
Legislative and policy frameworks

Immediate Outcome 1 of the project aims at adoption and further improvement of legislative and policy frameworks compliant to the Budapest Convention as well as related standards, such as Istanbul and Lanzarote Conventions.

The Outputs under this Outcome focus on:

- Development of national action plans or similar strategic documents regarding the criminal justice response to cybercrime and electronic evidence;
- Revision and improvement of substantive criminal law (where necessary) in line with Articles 2 to 12 of the Budapest Convention with additional focus on Istanbul and Lanzarote Conventions; and
- Improvement of procedural law for the purposes of domestic investigations in line with Articles 16 to 21 of the Budapest Convention. Human rights and rule of law approach is ensured, primarily but not exclusively, by supporting reform of regulatory framework on the basis of updated Study on Article 15 Safeguards in the Eastern Partnership region.

CyberEast Objective 2
Reinforce capacities and interagency cooperation

Immediate Outcome 2 of the project seeks to reinforce the capacities of judicial and law enforcement authorities and interagency cooperation, seeking to encompass all criminal justice stakeholders in the EaP countries into coherent, sustainable and skills-oriented experience sharing and training framework.

To achieve this, the Outputs under this Outcome aim at:

- Strengthening skills and institutional setup of operational cybercrime units in law enforcement authorities.
- Improving interagency cooperation of relevant law enforcement and criminal justice authorities, agencies and bodies including through improved data sharing.
- Internal and external accountability and oversight including role of civil society organisations reinforced.
- Improved public communication and transparency on cybercrime actions.
- Reinforce mechanisms for trusted cooperation between the private sector, citizens and criminal justice authorities.

CyberEast Objective 3
International and public/private cooperation

Immediate Outcome 3 of the Project pursues the increase of efficient international cooperation and trust on criminal justice, cybercrime and electronic evidence, as well as trust between criminal justice and private entities.

As a continuation of the previous capacity building efforts in the EaP on international and public/private cooperation, the Outputs under this Outcome:

- Further strengthen skills, set up and competencies of the 24/7 points of contact.
- Put in place guidelines and procedures for mutual legal assistance and data requests.
- Strengthen operational skills for international judicial and police authorities cooperation on cybercrime, and
- Implement existing agreements on public/private cooperation while concluding such agreements in the remaining countries.
- Human rights and rule of law component is addressed through continued public-private dialogue, work with ISP regulators and data protection authorities, and review of cybercrime reporting systems with focus on citizens' security.

CyberEast: Planned activities

Types of activities

- Assessment visits:
  - Inception (training)
  - Reporting systems
  - Crime proceeds

- National workshops
  - Strategies/action plans
  - Legislation including Art. 15 (continued)
  - Cooperation memoranda
  - Procedures for access to data
  - CERT business analysis
  - Support to national events
  - Work with DPAs and ISP regulators
  - Roundtables and mock trials with defense attorneys
  - MLA step-by-step guidelines
  - Crime proceeds exercises and workshops

CyberEast: Planned activities

- National trainings
  - Design of all courses (FR, judicial, specialized)
  - Direct delivery
  - Audit/review of advanced delivery
  - Templates for cooperation (repeated)
  - Support to national cyber exercises
  - Effective access to data programme for LEA and ISPs

- Regional meetings or exercises
  - Project "milestones" discussed in next slides

- Regional studies
  - Data protection study in the EaP
  - Substantive law study (BCC)
  - Studies on Istanbul and Lanzarote Conventions

- Other/new activities
  - Support to Europol operational meetings
  - Master Programme support
  - Support to local research contributing to Europol iOCTA
  - EaP-wide communications campaign

CyberEast: Planned activities

Project milestones: regional and international activities

- Launching and Closing Events
- Steering Committee Meetings (once or twice a year)
- Trademark joint regional exercises in different locations every year
- Regional meeting on cooperation with MSPs (Feb 2020 Georgia)
- High-level Regional Meeting of policy makers (Autumn 2020)
- Regional meeting on criminal money flows on the Internet
- Regional case simulation exercises on international cooperation
- Regional meeting on adoption of MLA guidelines
- Regional meeting on efficiency of cybercrime/incident reporting systems

CyberEast: Planned activities

Project milestones: regional and international activities

- Sending participants to and contributing otherwise to:
  - International meetings hosted by EaP states;
  - Yearly EuroDIG meetings + perhaps SEEDIG;
  - Yearly INTERPOL/Europol conferences;
  - T-CY/Octopus twice a year;
  - Pompidou Group possible joint event on drugs online;
  - Eurojust meetings (seems to become yearly);
  - UN sessions discussing the Convention (depending on progress);
  - Possible C-PROC regional events (e.g. Forums);
  - Possible joint events with parallel cybersecurity project under EU4Digital.

CyberEast: Major stakeholders

Project country teams

- Ministries of Internal Affairs, national police units and specialized investigative agencies (such as Investigative Committees, financial investigators, etc.);
- Ministries/Agencies responsible for State Security (cybercrime investigations, operative activities and international cooperation);
- Ministries of Justice (legislative units, cybercrime/security strategies and international cooperation officers);
- Prosecution Offices (cybercrime prosecutions and international cooperation);
- Judiciary (cybercrime/electronic evidence related criminal justice capacities);
- Training institutions for all above criminal justice agencies (Police Academies, Prosecution training centres, Judicial Schools, etc.)
- Governmental or national Computer Security Incident Response Teams (CSIRTs);
- National communications regulators;
- Personal data protection agencies;
- Internet service providers and industry associations.

Coordination

- Steering Committees once or twice per year
- Ministries of Foreign Affairs as designated country team coordinators
- Increased integration with local EU delegations and Council of Europe Offices
- Visibility and communication – new rules/identity
- Parallel project on Cybersecurity – starting by end 2019

Thank you for your attention

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Giorgi Jokhadze
Project Manager
Cybercrime Programme Office
Council of Europe - Conseil de l'Europe
Bucharest, Romania
Giorgi.Jokhadze@coe.int