Council of Europe and European Commission organise regional cyber training for East and South-East European countries

Bucharest, 03.03.2022 – In the light of current events, strengthening capacities on cybercrime and cybersecurity is more important than ever. Therefore, the Council of Europe Cybercrime Programme Office (C-PROC) and the European Commission will organise, from 7 to 11 March in Athens (Greece), a regional cyber exercise involving co-operation between the cybersecurity community (mainly computer security incident response teams – CIRTs) and law enforcement agencies on handling and investigating a malware attack orchestrated by a criminal group.

The training is organised in the framework of the "CyberEast: Action on Cybercrime for Cyber Resilience in the Eastern Partnership Region" project and the "iPROCEEDS-2: Targeting Crime Proceeds on the Internet and Securing Electronic Evidence in South-East Europe and Turkey" project, in partnership with the Cybersecurity East project, funded by the European Union.

CyberEast and iPROCEEDS-2 projects build on the success of the previous joint EU and Council of Europe projects (implemented since 2010) and aim at adopting legislative and policy frameworks compliant with the Budapest Convention on Cybercrime and related instruments, reinforcing the capacities of judicial and law enforcement authorities and interagency co-operation, and increasing effective international co-operation and trust in criminal justice, cybercrime and electronic evidence, including between service providers and law enforcement authorities.

The Regional Cybercrime Exercise will bring together 50 participants, mostly from four of the six countries of the Eastern Partnership region (Armenia, Azerbaijan, Georgia, and Republic of Moldova) and seven countries from South-East Europe: Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Serbia and Kosovo[1] and Turkey.

The exercise will require the participants to detect and identify cyber security incidents and/or potential cybercrime, and then follow the money and criminal proceeds. It will also apply OSINT, malware analysis and digital forensics skills to identify potential perpetrators and collect potential intelligence and evidence. Lastly, it will coordinate activities and recover data necessary for cyber investigations and prevention of further incidents.

In addition, a regional conference, organised with the contribution of the **European Union Agency for Cybersecurity (ENISA)**, will focus on principles and procedures of co-operation between law enforcement and CSIRTs, to be adopted by participating countries.

The trainers include experts on cybercrime and cybersecurity from the UK, Australia, the Netherlands and Romania.

[1] ** All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo.*