Міністерство
закордонних справ
України

Михайлівська площа, 1
м. Київ, 01018, Україна
(044) 238 17 48, (044) 238 18 88 (fax), zsmfa@mfa.gov.ua, Код ЄДРПОУ 00026620

Ministry
of Foreign Affairs
of Ukraine

1 Mykhailivska Square
Kyiv, 01018, Ukraine
mfa.gov.ua

04 грудня 2020 р. № 311/16-690-1850

Виконавчому директору
Інтернет Асоціації України

В.В. Куковському

Щодо тренінгу проєкту CyberEast

Шановний Володимире Васильовичу!

14-15.12.2020 проєкт CyberEast, який спільно фінансується Радою Європи та Європейською Комісією, проводитиме практичний семінар «Ефективний доступ до програми даних» для представників правоохоронних органів та інтернет-провайдерів (інформація про захід додається).

Тренінг включатиме симуляційні вправи щодо реагування на потенційні кіберзлочини та перевірятиме співпрацю між інтернет-провайдерами та правоохоронними органами в режимі реального часу (протягом п'яти сесій). Короткий семінар, який відбуватиметься після навчань (Сесія 6), узагальнить досвід та сприятиме подальшій комунікації між правоохоронними органами та приватним сектором щодо найбільш ефективних процедур та практик для забезпечення доцільного та збалансованого доступу до даних для розслідування кримінальних справ.

Захід проводитиметься онлайн англійською мовою з послідовним перекладом українською, кількість учасників необмежена.

У зв'язку із вищевикладеним, просимо поширити інформацію серед кола зацікавлених осіб. Для реєстрації на захід та отримання посилання просимо звертатися до контактної особи від МЗС – третього секретаря Департаменту ЄС і НАТО Богдани Мартинюк (ел. пошта bogdana.martyniuk@mfa.gov.ua;т. (044)-279-78-97).

Додаток: на 4 арк., надіслано на адреси dir@inau.ua; info@inau.ua.

З повагою

Директор Департаменту
Європейського Союзу і НАТО **Марина МИХАЙЛЕНКО**

Вик. Б. Мартинюк

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

November 2020

Activity Code 2.2.6 / PMM 92162

2088_87 Effective Access to Data Programme: practical exercise for law enforcement and Internet service providers

Kyiv, Ukraine
14-16 December 2020

Developed by CyberEast project funded jointly by the European Union and the Council of Europe

Outline

Background and justification

In the world of today, the increasing number of attacks against or realized through the means of computer systems and data is a growing concern for both cyber security professionals and the law enforcement, affecting societies at large.

The growing threat of cybercrime is further exacerbated by difficulties of access to and securing of electronic evidence, especially if information vital for criminal investigations is in the hands of private companies and is found beyond national borders, or stored in the cloud. However, even where realization of these threats and challenges by policy makers and professional communities is as strong as ever, successful response to these is often hampered by lack of coordination and common approach of these communities to the ultimate common goal – ensuring safer cyberspace for all.

Effective cooperation between criminal justice authorities and private sector entities, in particular Internet Service Providers (ISPs), is thus essential to protect societies against crime. Such cooperation concerns primarily access by police and prosecution services to data held by service providers for criminal justice purposes, making use of the existing binding legislative framework as well as through voluntary cooperation, and extends further to the sharing of information and experience, as well as common training programs.

In this context, the CyberEast project, in continuation of the Cybercrime@EaP projects, aims to support the countries of the Eastern Partnership in building and maintaining partnerships with private sector entities, primarily ISPs, for reinforcing mechanisms for trusted cooperation between the private sector, citizens and criminal justice authorities.

Such mechanisms of trusted cooperation, beyond legislation and cooperation agreements, can benefit greatly from practical focus on skills and experience necessary to provide effective and balanced access to data, keeping in mind the possibilities offered by the Budapest Convention. Ultimately, informal or formal procedures and protocols for exchange of data, processing of requests and overall matters facilitating cooperation could be another factor contributing to improved cooperation.

To this end, the CyberEast project will hold series of practical exercise scenarios, which will include a standard scenario of a simulated computer incident/potential cybercrime and test cooperation between the ISPs and law enforcement in real time (in five sessions). The workshop following the exercise (Session 6) will summarize the experience of the exercise and facilitate agreement between law enforcement and industry on most efficient procedures and practices to ensure expedient and balanced access to data for the purposes of criminal investigations.

To address the current circumstances and challenges presented by COVID-19 pandemic, both exercise and workshop will be delivered online. In cases where this is possible and safe, the actual teams participating in the exercise/workshop (industry and authorities) can be gathered at a specific location.

Expected outcome

Organized by the joint European Union and Council of Europe CyberEast project, the exercise contributes directly to Output 2.2 of the project (*Improvement of interagency cooperation of the relevant law enforcement and criminal justice authorities, agencies and bodies including through improved data sharing*) by aiming to develop practical skills of public-private cooperation through practical exercise scenarios in real time.

By the end of the exercise and workshop, the participants will be able to establish closer links between professional communities of cybercrime investigators, cybersecurity players and private sector representatives. The need for established procedures and practices for effective and balanced access to data should become an accepted practice.

Participants

The event will be attended by the following participants:

- International experts on cybercrime and electronic evidence;
- Representatives of the national Internet industries;
- Cybercrime investigators/law enforcement;
- Prosecutors tasked with cybercrime investigations oversight;
- CSIRT/national CERT experts (on availability and interest);
- C-PROC staff.

Administrative arrangements and location

The meeting will be conducted virtually, on Council of Europe’s KUDO platform to address needs of virtual meetings with interpretation.

Unless specified otherwise, all times indicated in the programme correspond to Chisinau local time.

PROGRAMME

Day I - Monday, 14 December 2020

10h45	**Opening session** – European Commission (TBC) or EU Delegation (TBC) – CyberEast, Council of Europe
11h00	**Session 1** – Introductions of participants – Introduction to the purpose of the exercise – Crime/incident reporting systems – introduction of first injects
13h00	*Lunch break*
15h00	**Session 2** – Network analysis, identifying suspects and data – Preparing grounds for preservation request
17h00	*End of Day 1*

Day II - Tuesday, 15 December 2020

11h00	**Session 3** – Expedited preservation of stored computer data – Production order – Collating data from various sources
13h00	*Lunch break*
15h00	**Session 4** – Data forensics and analysis – Planning investigation
17h00	*End of Day 2*

Day III - Wednesday, 16 December 2020

11h00	**Session 5** – Global arrest planning phase – Joint Investigative Team
13h00	*Lunch break*
15h00	**Session 6** – Presentation of the key points from Session 1-5 – Mapping of processes or procedures – Conclusions
17h00	*End of event*

Contacts

European Commission:

Roberto SEGUNDO NAVARRO
Good Governance and Security
Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR)
Directorate Neighbourhood East – Unit C1
European Commission
ec.europa.eu

Council of Europe:

Giorgi JOKHADZE
CyberEast Project Manager
Cybercrime Programme Office
Tel: +40-21-201-784
Giorgi.Jokhadze@coe.int

Cybercrime Programme Office of the
Council of Europe (C-PROC)
Bucharest, Romania
www.coe.int/cybercrime