**Навчальним закладам та
неурядовим організаціям**
(за списком)

*Щодо круглого столу
проєкту CyberEast*

28.01.2021 проєкт CyberEast спільно з проєктом CyberSecurity East проводитиме круглий стіл у форматі відеоконференції з метою обговорення національних політик по кібербезпеці та боротьбі з кіберзлочинністю, а також відповідних планів дій (інформація про захід додається).

Круглий стіл має на меті обговорити прогрес в імплементації Кіберстратегії України; сприяти приватно-публічному партнерству у питаннях забезпечення кібербезпеки та боротьбі з кіберзлочинністю, у тому числі роботі з електронними доказами відповідно до Будапештської конвенції. Запланована участь представників органів державної влади, академічних кіл та громадянського суспільства.

Учасникам буде надіслано посилання для переходу в онлайн кімнату (на платформі KUDO). Захід проводитиметься англійською мовою з послідовним перекладом українською, кількість учасників необмежена. Після проходження учасники отримають сертифікати.

У зв'язку із вищевикладеним, просимо опрацювати можливість залучення представників вашої організації до практичного семінару і зареєструватися за посиланням:
https://docs.google.com/forms/d/e/1FAIpQLSfFP9Y6M8_DmcI29_euCpjrWbt6vOFRJRZik8isp_tM66ylkg/viewform .

Додаток: на 3 арк.

Директор Департаменту
Європейського Союзу і НАТО   Марина МИХАЙЛЕНКО

Вик. Б. Мартинюк, 279 78 97
bogdana.martyniuk@mfa.gov.ua

Вхід. № 07
"20" 01 2021р.

Activity Code 1.1.3 / PMM 96792

2088_49 Roundtable discussion on cybercrime/cybersecurity policies and action plans

28 January 2021, Kyiv, Ukraine (online)

Organized by the European Union and Council of Europe CyberEast project

Outline

Background

Cybersecurity is critical to both prosperity and security. As our daily lives and economies increasingly rely on digital technologies, we become more and more exposed to malicious cyber-attacks. These are spreading in terms of both who is involved and what they seek to achieve. Harmful and hostile cyber activities have both criminal and political motivations, threatening our economies, democratic freedoms and values; thus, the vulnerability of evolving economic and public infrastructure has been put into focus.

Cybercrime policies and - in general - criminal justice action in cyberspace are crucial pillars of ensuring security in cyberspace. Countries of the Eastern Partnership have committed to implement the Budapest Convention on Cybercrime as a framework for domestic measures and for international cooperation on cybercrime and access to electronic evidence. Furthermore, the EaP countries adopted in October 2013 (Kyiv, Ukraine) a Declaration on Strategic Priorities for the Cooperation against Cybercrime in the EaP Region. They committed to pursue the necessary actions in key areas, such as procedural law, safeguards and guarantees, data protection and protection of children against online sexual abuse and exploitation with the objective of adopting an overarching effective framework to combat cybercrime on the basis of the Budapest Convention.

CyberEast project also looked into the subject matter of cybercrime and cybersecurity strategies in the Eastern Partnership region since 2015, with latest Report on Cybercrime and cybersecurity strategies in the Eastern Partnership region from January 2019.

Ukraine has employed a hybrid approach to cybersecurity and cybercrime policies, as manifested in its National Cybersecurity Strategy adopted by Presidential decree on 15 February 2016. Cybercrime and in particular implementation of the Budapest Convention are part of the Strategy. However, as annual Action Plans for this Strategy have been only adopted in the initial years and have not been followed up recently, there is concern about the applicability and viability of the Strategy as a practical document.

Therefore, the workshop, organized under joint efforts of the CyberEast and CyberSecurity EAST projects funded by the EU, intends to facilitate discussion with national counterparts on the progress so far and further plans with regard to the Cybersecurity Strategy of Ukraine, with particular focus on cybercrime policies and action necessary in COVID-19 conditions.

Expected outcome

Organized by joint EU/Council of Europe CyberEast and CyberSecurity EAST project funded by the EU, the event contributes directly to output 1.1 of the CyberEast project (*National action plans or similar strategic documents regarding criminal justice response to cybercrime and electronic evidence developed*); more specifically, the event is a part of series of national discussions in the Eastern Partnership states on the need to enforce effective cybercrime and cybersecurity policies in line with the Budapest Convention on Cybercrime, and devise possible project support to implementation of such policies.

By the end of event, participants are expected to agree on the ways in which the joint action between CyberSecurity EAST and CyberEast projects can further support the implementation of cybercrime and cybersecurity policies in Ukraine.

Participants

The event is conducted virtually with simultaneous interpretation into Ukrainian, therefore there is no limitation on the number of interested participants; the only requirement is to register for the event at the following link. The following participants will benefit the most from taking part in the workshop:

- CyberEast project country team members for Ukraine;
- Representatives of the State Security Service, Ministry of Internal Affairs/National Police, Prosecutor's Office and judiciary working and/or interested in cybercrime and electronic evidence matters;
- National Security and Defence Council and State Security Service personnel working on cybersecurity;
- Representatives of relevant Parliamentary Bureaus or offices/divisions responsible for cybercrime/criminal justice legislation and cybersecurity/defence;
- National and governmental CSIRT/CERT teams, including State Centre for Cyber-defence and Counteraction to Cyber Threats;
- Internet service providers/companies' representatives, including Internet Association of Ukraine and Telecom Association of Ukraine as stakeholders in the process;
- Civil society organizations active on matters covered by the workshop.

Administrative arrangements and location

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

Simultaneous interpretation between Ukrainian and English will be available throughout the event.

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

Programme

10h45	**Opening session** • EU Delegation Ukraine • Council of Europe • CyberSecurity EAST project
11h00	**Current state of cybersecurity and cybercrime policies, strategies and action plan in Ukraine** • Representative(s) of the Ukrainian authorities
11h40	**Main elements of modern cybercrime and cybersecurity strategies: an overview** • Invited experts
12h20	**COVID-19: what has changed for Ukraine in terms of necessary cybercrime and cybersecurity policies?** • Open discussion moderated by experts
13h00	**Lunch break**
14h00	**Main elements of cybersecurity and cybercrime policies in Ukraine: what works now and what could work better in the future** • Open discussion moderated by experts
14h40	**Way forward for Ukraine: how can dedicated projects support the reform in the short and mid-term?** • Open discussion moderated by experts
15h20	*End of event*

Contacts

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

Ukraine:

Bogdana MARTYNIUK
Attaché
Political, security and defence cooperation
Directorate General for the EU and NATO
Ministry of Foreign Affairs of Ukraine
bogdana.martyniuk@mfa.gov.ua

Cybersecurity East Project:

Besnik LIMAJ
Team Leader
CyberSecurity EAST Project
besnik.limaj@gfa-group.de
https://www.gfa-group.de/