CyberEast

**Action on Cybercrime for Cyber Resilience
in the Eastern Partnership region**

Արևելյան Գործընկերություն
Східне партнерство
Eastern Partnership
აღმოსავლეთ პარტნიორობა
Parteneriatul Estic
Şərq tərəfdaşlığı
Partenariat Oriental

WEBINAR

Election Interference: attacks on critical information systems

Date and hour	**04/06/2020,** 12h00 (Eastern European Summer Time: GMT +3 hours)
Speakers	— **Andrii OKAEVICH**, Head of SCIRT, Department of Cybersecurity, Security Service of Ukraine — **Matthew MOORHEAD,** Commonwealth Secretariat - Commonwealth best practice Guide to cybersecurity in elections 2020 — **Merle MAIGRE**, CybExer Technologies — **Kannan GNANASIHAMANI**, Senior Director (Technology Crime), Attorney-General's Chambers of Singapore (TBC)
Objectives	The purpose of this webinar is to identify the current threats to critical information systems which are used to organize, conduct or support election process. Information will be provided on legal, organisational, technical and other aspects, pointing out current shortcomings and making recommendations to further ensure protection and deterrence against such attacks. The webinar is designed to encourage an interactive participation and to facilitate information sharing among participants, discussing relevant experiences, good practices, challenges and opportunities.
Expected outcomes	• Identify and discuss threats to election systems in terms of cybersecurity and cybercrime; • Discuss roles and responsibilities of various institutions and actors, including law enforcement, in deterring and handling of these threats; • Present good practices of tackling election interference; • Agree on basic principles for making elections more secure and safe in terms of cybersecurity and cybercrime.
Participants	Around 200 participants are expected. The webinar is deemed particularly useful for officials from policy makers responsible for cybercrime and cybersecurity, criminal justice authorities (judges, prosecutors, law enforcement agencies), staff from the national CSIRTs, as well as researchers/academia having interest in the subject. Each registered participant will receive a confirmation email one day prior to the webinar with instructions on how to connect and rules of engagement.

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

Implemented
by the Council of Europe

CONSEIL DE L'EUROPE

Background	Attacks against information systems supporting election process go beyond mere concepts of cybersecurity threats or cybercrime offences, but rather represent direct attacks on democracy as a principle, and threaten security and stability of states in ways that are difficult to anticipate.
	At the same time, this presents an opportunity for cooperation for both cybersecurity community and criminal justice authorities alike, as there should be little doubt that information systems that support electoral process represent classic example of critical information infrastructure that needs proper protection.
	Specifically, information security rules including target hardening and damage mitigation, expeditious incident and crime reporting, coordination between agencies in case of attacks against such systems are just a few examples that would contribute to resilience and stability of such systems and electoral process in general.
	Moreover, in times of ongoing COVID-19 pandemic and remaining restrictions, as well as uncertainty about the application and extension of the latter, the use of ICT for the elections may become even more prevalent and thus critical in terms of cybercrime and cybersecurity threats.
Expected duration	1h30' (50 min presentations + 40 min discussion)
Relevant resources	Commonwealth Secretariat, Cybersecurity for Elections: A Commonwealth Guide on Best Practice, (2020) ENISA, Election cybersecurity - Challenges and opportunities, (2019) Council of Europe, Resources of the 2019 Octopus Conference on Cooperation against Cybercrime, Workshop 5 (2019)
C-PROC related activities	The webinar is carried out under Output 2.5 of the CyberEast project, aiming to reinforce mechanisms for trusted cooperation between the private sector, citizens and criminal justice authorities.

www.coe.int/cybereast