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

CYBERSECURITY
EAST

WEBINAR
Technical webinar: preparation for elections security

Date and hour	**4 September 2020** Session I: 11h00-13h00 (Tbilisi Time: GMT +4 hours) Session II: 14h00-16h00 (Tbilisi Time: GMT +4 hours) Link: https://bluejeans.com/388808269
Speakers	— Opening remarks from EC DG NEAR and EU Delegation in Georgia — Opening remarks by the Venice Commission of the Council of Europe — **Merle Maigre**, Senior Expert on Cyber Security, E-Governance Academy, Estonia - Cybersecurity EAST Project — **Richard Barrett,** Member of the Venice Commission for Ireland, Council of Europe — **Marjan Stoilkovski,** Head of Cybercrime Unit, North Macedonia
Objectives	The purpose of one-day webinar for the Georgian authorities is to bring together all relevant national stakeholders and focus on awareness raising, inter-institutional coordination, information sharing, best practices, previous experiences, and lessons learnt in terms ensuring cyber-security of elections. The webinar is intended to focus on the following aspects of elections security: - Identifying critical infrastructures/systems/potential "weak links" for elections security and ensuring resilience against cyber-attacks; - Tackling social engineering, fake news and online disinformation campaigns, especially from foreign actors; - Coordination and joint response needs and responsibilities. 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; • Present experience and good practices of tackling election interference; • Discuss roles and responsibilities of various institutions and actors, including law enforcement, in deterring and handling of these threats; • If possible, agree on basic principles for making upcoming elections 2020 more secure and safe in terms of cybersecurity and cybercrime.
Participants	Up to 40 participants are expected.

	Each registered participant will receive a confirmation email one day prior to the webinar with instructions on how to connect and rules of engagement.
Background	Cyberattacks against elections security go beyond mere concepts of cybersecurity threats or cybercrime offences, but rather represent direct attacks on democracy and threaten security and stability of the states in ways that are difficult to anticipate. Specifically, in case of Georgian Parliamentary elections in October 2020, there is an established pattern of similar attacks in different states and contexts, including most recent examples of United Kingdom and North Macedonia. Given the history of large-scale cyber-attacks against Georgian state and society in 2008, this calls for specific caution and preparation against such threats. There is thus a necessity for cooperation for between policy makers, cybersecurity community, criminal justice authorities and private sector, as information systems that support electoral process are classic example of critical information infrastructure that needs proper protection against cyber threats. Specifically, information security rules including target hardening and damage mitigation, proactive response to online disinformation and social engineering efforts, timely incident and crime reporting, and 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.
Expected duration	4 hours (two sessions separated by 1 hr lunch break)
Relevant resources	European Union, Directive on security of network and information systems - NIS Directive (2016) Council of Europe, T-CY Guidance Note no. 9 on Aspects of election interference by means of computer systems covered by the Budapest Convention (2019) Commonwealth Secretariat, Cybersecurity for Elections: A Commonwealth Guide on Best Practice (2020) Joint Report of Venice Commission and DGI on Digital Technologies and Elections (2019) My Cyber Hygiene, Free cyber hygiene e-learning course in 13 languages (2020) ECEAP, Election Interference in Ukraine in the Digital Age (2019) ENISA, Training Resources (2020) ENISA, Election cybersecurity challenges and opportunities (2019) IDEA, Cybersecurity in elections (2019) Council of Europe, Resources of the 2019 Octopus Conference on Cooperation against Cybercrime, Workshop 5 (2019) Council of Europe, Cybercrime and COVID-19 resources page

Related activities	The webinar is carried out under Output 2.2 of the CyberEast project, aiming at improvement of interagency cooperation of the relevant law enforcement and criminal justice authorities, agencies and bodies including through improved data sharing (Activity code 2.2.2, PMM 92147).