Cybercrime and terrorism:
The criminal justice response

Webinar 12 June 2020

Co-organized by the UN Office of Counter-Terrorism and the Council of Europe

Date and hour	**12/06/2020,** 11h00 GMT
Speakers	- Fernando PUERTO MENDOZA, Programme Officer, UN Office of Counter-Terrorism - Balques AL RADWAN, Associate Expert, UN Office of Counter-Terrorism - Philippe VAN LINTHOUT, Investigating Judge, Court of First Instance of Antwerp, Belgium - Jan KERKHOFS, Federal Magistrate, Section Organized Crime – Cyber Unit, Federal Prosecutor's Office, Belgium - Giulia Lucchese, Counter-Terrorism Division, Department of Information Society and Action against Crime, Council of Europe
Expected duration	2h00 75' presentations (including dedicated questions) + 45' general discussion
Facilitator	Alexander SEGER, Head of Cybercrime Division, Council of Europe
Objectives	- To discuss the criminal justice response to cyber-enabled terrorism and assess the status of adoption and implementation of international standards in the field. - To discuss good practices and problematic areas in investigating terrorist attacks and ensuring a coordinated response, also through case studies and recent examples. 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	At the end of the webinar participants are expected: To have increased their knowledge on current forms of cyber-enabled terrorist activities.

	• To have gathered information on available tools and procedures, legal and technical, to support counter-Terror on-line investigations, and to have identified relevant challenges and good practices. • To have identified the type of support that can be provided through global capacity building initiatives.
Participants	The webinar is deemed particularly useful for officials from national governments and policy makers responsible for cybercrime and national cyber security, for criminal justice authorities involved in cybercrime and counter-terrorism areas, including judges, prosecutors and law enforcement agencies, as well as non-governmental organizations, academia and other researchers interested in the subject. Up to 200 participants are expected. On-line registration and additional information on the webinar will be made available on the webinar's page. 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	Facts show that Internet is increasingly used by terrorist organizations as a communication platform to facilitate contacts among members, to spread propaganda materials, and to transmit information on, as well as material support for, planned acts of terrorism. Many countries are Parties to numerous international treaties, and subject to UN Security Council Resolutions, that require criminalization of different forms of terrorism, facilitation of terrorism, support for terrorism, and preparatory acts. In terrorism cases, countries often rely on offenses that derive from those topic-specific treaties, as well as additional offenses in national legislation. However, this phenomenon poses several challenges to criminal justice authorities, not only due to the specific technical knowledge that is requested for the effective investigation of these offences, but also for the heterogeneous legal framework that governs the cross-country handling of electronic evidence. To this regard, although the Budapest Convention on Cybercrime is not focused on terrorism, the substantive crimes in it may be carried out as acts of terrorism, to facilitate terrorism, to support terrorism, including financially, or as preparatory acts. In addition, the procedural and international mutual legal assistance tools in the Convention are available to terrorism and terrorism-related investigations and prosecutions.
Relevant resources	• UN Office of Counter-Terrorism, Cybersecurity • UN Security Council, Resolution 2341 on the Protection of Critical Infrastructure from Terrorist Attacks • Council of Europe Cybercrime Convention Committee, T-CY Guidance Note #11 - Aspects of Terrorism covered by the Budapest Convention, 2016 • Council of Europe Division on Counter-Terrorism

C-PROC related activities	The webinar is carried out under Activity 1.3.7 of the GLACY+ project, aiming to review and provide advice on the strengthening of legislation on emerging cybercrime threats and issues, Activity 2.5.2 aimed at strengthening international police-to-police cooperation through training workshops, and Activity 3.3.4 aimed at providing training for authorities involved in international judicial cooperation.

www.coe.int/cybercrime