OSCE Deutschland 2016

CIO.GAL/224/16
8 February 2017

ENGLISH only

Regional Workshop on Countering the Use of the Internet for Terrorist Purposes for Judges, Prosecutors and Investigators from South Eastern Europe

16-17 November 2016, Skopje

Executive Summary

A two-day regional workshop on Countering the Use of the Internet for Terrorist Purposes for Judges, Prosecutors and Investigators from South Eastern Europe was organized jointly by the Transnational Threats Department (TNTD) in co-operation with the OSCE Mission to Skopje and the national Academy for Judges and Public Prosecutors. Seventy participants and experts from five participating States, international organizations, the academic and the private sector participated in the workshop together with representatives from the OSCE Secretariat and OSCE field operations from the region.

The workshop was divided into six sessions, each with a thematic focus.

- Session I served to frame the topic by reviewing the pertinent national and international legal frameworks including universal counter-terrorism legal instruments and international human rights law.
- Session II focused on how the Internet is used by terrorists (including for the purposes of violent radicalization, recruitment, planning of terrorist acts and communication) while taking into account the phenomenon of terrorists acting alone. The discussion further presented good practices, lessons learned, general guidelines and practical examples of specialized investigative techniques for gathering digital evidence stored on computers or mobile devices utilized, as well as for the investigation of cases where the Internet had been used for terrorist purposes.
- Session III presented good practices, lessons learned, general guidelines and practical examples on the collection, documentation and retrieval of relevant digital evidence and forensic data stored on utilized computers or mobile devices and the preservation of data sources integrity for court proceedings.
- Session IV focused on Public-Private Partnerships (PPP) in investigating the use of the Internet for terrorist purposes. As the majority of digital data is retained by private companies, discussions highlighted the need for closer co-operation between public authorities and the private sector.
- Session V discussed investigations and the use of specialized investigative techniques for cases in which the Internet had been used for the collection and transfer of funds for financing terrorist activities.
- Session VI discussed good practices, lessons learned and general guidelines on how to build networks among national judiciary authorities to co-operate on the regional and international levels when investigating cases in which the Internet had been used for terrorist purposes.

The following key findings and non-binding recommendations emerged during the discussion:

For OSCE participating States and Partners for Co-operation:

Session 1: Legal frameworks on countering the use of the Internet for terrorist purposes and related crimes

- To ensure the adoption of effective national legal and policy frameworks in order to criminalize, in full respect with human rights standards, unlawful, terrorism-related acts involving activities on the Internet.
- To provide Law Enforcement Agencies (LEAs) with appropriate investigative powers and technical capability (tools and expertise), that strictly meet the principles of legality, necessity and proportionality required for any interferences with human rights, to facilitate the effective prosecution of crimes related to terrorism in full respect of the rights of suspects and other individuals involved in criminal proceedings.
- To promote and facilitate international co-operation as well as effective partnerships between relevant authorities, including the private sector.

Session 2: Investigations of the different components pertaining to the use of the Internet for terrorist purposes

- To ensure that investigators and prosecutors are provided with substantive information and knowledge about how the Internet and cyberspace work and how terrorists are using them for their purposes.
- To ensure that undercover monitoring of social media is always conducted in compliance with international human rights standards, and strictly adhered to the principles of legality, necessity and proportionality and implemented in accordance with the rule of law and in a non-discriminatory manner.
- To ensure that undercover activities on the Internet are co-ordinated domestically and where relevant information is exchanged, consistent with relevant national laws and regulations, with international counterparts.

Session 3: Protection and recovery of forensic data in investigations on countering the use of the Internet for terrorist purposes

- To provide judges, prosecutors and investigators with specialized online (ELearning modules) and offline training pertaining to cybercrime and the Use of the Internet for Terrorist Purposes including on the specificity of digital forensics.
- To consider including the topic of cybercrime in the curriculum of police academies and training institutions for the judiciary.
- To encourage judges, prosecutors and investigators to exchange and share best practices on handling digital evidence while respecting the right to privacy as well as the other fundamental human rights.
- To always follow four principles of computer-based electronic evidence[1].
- To ensure that digital evidence has been collected in line with the applicable legal standards for it to withstand judicial scrutiny.
- To ensure that evidence is preserved according to the chain of custody principle.
- To assess the relevance and accuracy of collected data on a regular basis, to store data in line with applicable international standards and domestic laws, and to update or delete any data that are inaccurate or no longer relevant for the purpose for which they were collected.
- To invest in basic training for judges, prosecutors and investigators on digital evidence and digital forensics related to cybercrime.

[1] The four principles are: not to change data, to only let experts have access to the original data, to keep an audit record of all electronic evidence processes, to keep in mind that the case officer has the overall responsibility

Session 4: Public-private partnerships (PPP) in investigating the use of the Internet for terrorist purposes

- To promote a more proactive approach by the Internet industry and work on an automated approach to identify terrorist material from the outset, in accordance with freedom of the media, freedom of speech and other human rights.
- To make use of existing tools such as the EU Awareness Network (RAN) Centre of Excellence to facilitate knowledge and expertise, including on alternative and counter-narratives online.
- To explore possibilities to establish the so-called "web-constable" system which is built on community policing principles and aims at increasing networking and trust between police and Internet users.[2]
- To consider using the expertise of the private sector in investigating the use of the Internet for terrorist purposes, including financial service providers.

Session 5: Investigations on terrorist financing on-line

- To increase and improve judges', prosecutors' and investigators' knowledge about the DarkNet, ransomware, new payment methods, products and services such as crypto currencies (Bitcoin, Mastercoin, etc.).
- To enhance the knowledge of law enforcement agents on Financial Action Task Force (FATF) typology characteristics.
- To recognize the value of financial investigations conducted simultaneously with and in parallel to the pro-active investigations of terrorist acts.
- To promote the implementation of EU Anti-Money Laundering (AML) directives and recommendations of FATF to combat money laundering and terrorist financing and to implement them in a manner that is compliant with international human rights standards.
- To enhance sharing of intelligence between relevant authorities, especially the Financial Intelligence Units (FIU) and AML teams, in full respect of the right to privacy and other fundamental human rights.

Session 6: Judicial co-operation at the regional and international levels on countering the use of the Internet for terrorist purposes

- To take into account existing sources of good practices such as the eleven recommended best practices identified by the Informal Expert Working Group (EWG) in the report on Mutual Legal Assistance (MLA) Casework Best Practice[3] including the General Checklist for Requesting MLA as well as Good Practice 9 of the Global Counterterrorism Forum's (GCTF) Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector.[4]

[2] Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach: http://www.osce.org/atu/111438?download=true

[3] Informal Expert Working Group Report on Mutual Legal Assistance (MLA) Casework Best Practice: https://www.unodc.org/pdf/lap_mlaeg_report_final.pdf

[4] GCTF Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector: https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/A/GCTF-Rabat-Memorandum-ENG.pdf