A SILK ROUTES PARTNERSHIP FOR MIGRATION BUDAPEST PROCESS

Budapest Process

3rd Meeting of the Community of Law Enforcement Practitioners

Topic: Law Enforcement in the Digital Sphere

Date: 04 May 2023

Location: Virtual

Draft Summary

The third meeting of the Community of Law Enforcement Practitioners (COLEP) was held virtually. The purpose of the meeting was to better understand the specific usages of digital tools by smugglers and traffickers as well as the specific challenges related to digital-crime; learn from the good practices that COLEP partners have undertaken to counter Smuggling of Migrants and Trafficking in Persons, in the digital sphere; and to explore opportunities to build and improve capacities to address the challenges, in particular by supporting trans-national collaboration and coordination.

Officers from the following countries attended this meeting of COLEP:

Azerbaijan, Bangladesh, Bosnia and Herzegovina, Bulgaria, France, Hungary, Iraq, North Macedonia, and Pakistan

The meeting was opened by the co-chairs of COLEP, Iraq and Bulgaria and a short summary of the outcomes of the first two meetings was presented by the Budapest Process Secretariat.

Main Points of Discussion

Challenges

- Sophisticated Organised Crime Groups (OCGs) are now using a lot of technology – thousands of mobile phones, lots of encrypted chat platforms, and dark web technology to coordinate activities across countries which makes it much tougher to detect those criminals and to identify them, more so because they are increasingly skilled in not leaving digital traces. Prosecution also becomes harder as there is a separation between the place where a criminal activity is performed and the place where the main offenders are located. Moreover, identities of the victim and perpetrators are easier to hide and anonymise using modern digital tools;
- In regards to Smuggling of Migrants (SOM), digital technologies have opened up different opportunities for criminal groups and the usage of the tools varies based on the type of crimes involved, for example:
    - Smugglers can advertise their services on social media and encrypted messaging platforms (like *telegram*, *signal*, *tik tok*, and *whatsapp*);
    - Migrants (clients) can ask for information regarding smugglers and routes via social media and messaging platforms as well using applications like *maps.me* for offline navigation;
    - Smugglers and migrants use encrypted technology to keep in contact during journeys.
- In regards to Trafficking in Persons (TIP), the impact of digital tools on Trafficking in Persons (TIP) is of particular concern in relation to two stages of the process: recruitment and exploitation;

- Sexual exploitation can occur via "lover-boy / Boyfriend model" where online grooming occurs prior to entrapment and trafficking; false job advertisements is also a common method;
- Labour exploitation usually occurs via online job advertisements as well as targeted messaging to vulnerable groups.

- In terms of capacities and capabilities:
  - The high volume of encrypted data from online exchanges can be hard for law enforcement agencies to analyse;
  - Criminals often quickly adapt and respond to law enforcement actions (re-publishing of advertisements that have been taken down is cheap so there must be vigilance for this);
  - There are difficulties in getting social media companies to take down messages or cooperate in investigations; and when they do cooperate, the process takes too long;
  - Lack of specialised police units (trained in online investigations, covert cyber-investigations, etc.) and/or lack of investigators with advanced IT skills;
  - Due to lack of digital skills of frontline and investigative officers, collecting forensic evidence in a proper manner has become a problem;
  - Lack of technical equipment and difficulties in keeping it up-to-date.
- In terms of Prosecution:
  - Lack of relevant and neutral witnesses complicates the prosecution process;
  - Lack of training among prosecutors on digitally-facilitated TiP and SoM and on procedures to request electronic evidence from private companies or other countries;
  - Several countries have legally stipulated time periods (like 90 days) within which an investigation has to be concluded, however, given the complexity of digital investigations, these time periods are unrealistic;
  - Courts are often unprepared to deal with digital evidence presented by prosecutors.

Good Practices

- Establish cyber security training and research centres for training frontline and back-end investigation officers; the centres provide needs based trainings and also conduct research on the latest trends and practices;
- Establish 'central data centres' that store, monitor and respond to cyber threats and conduct sophisticated data analysis, with specific monitoring and analysis of TIP and SOM as well as providing tailor made IT services to various law enforcement agencies;
- Enact and amend legal frameworks that facilitate investigation, prosecution and prevention of digital crimes; policies that allow significant investments in digital skills of law enforcement officers; courts whose capacities are built to allow for effective and timely prosecution;
- Create a permanent cyber patrol unit in a country's central investigation agency. The goal of this new unit would be to conduct forensic analysis, data extraction, as well as social media observation to detect upstream crimes and build a case that will be much easier for investigative and prosecution officers to deal with;

- Establish Specialist units under each jurisdictional office of a law enforcement agency / border control force, so as to not overburden the central anti-cybercrime agency;
- Conduct awareness raising campaigns to prevent misinformation and disinformation on migration routes, inter alia, via internet resources; campaigns that use methods that particularly reach out to youth and socio-economically vulnerable groups; also important to target post-conflict regions;
- Enable victim support services to allow the victim to feel safe and therefore cooperate with law enforcement in regards to mobile phone extraction and other intelligence gathering procedures.

Opportunities

- Ensure that law enforcement agencies have the right training to collect electronic evidence, including being able to utilise Open Source Intelligence (OSINT) conduct cyber-patrols and deploy digital undercover officers; it is especially important for frontline officers to be trained in dealing with electronic evidence;
- Provide the right tools to law enforcement agencies, such as web crawlers; It is important to make sense of the 'bread crumbs' (trail) that are left behind by traffickers when using the digital sphere. The internet allows one to trace these bread crumbs;
- Enable a robust cooperation between government agencies and NGOs and private companies, especially using digital technology (web, chats, instant messaging) to reach out to potential victims;
- Facilitate partnership with private companies to design content analytics to detect TIP cases and allow users to flag up suspicious activities (in particular by working with banks);
- Mobile phone data extraction remains a key area where more capacities of frontline and investigative officers can be built;
- Gather electronic evidence also through internet monitoring and OSINT; Big data analytics and social network analysis.

Next Steps

It was discussed that:

- Police to police cooperation, especially in terms of information sharing, is essential in cracking down on transnational criminals and to facilitate rapid investigation processes;
- SOM and TIP in the digital sphere is a major issue for all countries, and it is clear that a lot has to be done to catch up to the criminals, hence this topic should be considered for further discussion and knowledge sharing at the next meeting of COLEP;
- The co-chairs of COLEP, with the support of the Budapest Process Secretariat, will organise the next meeting of COLEP, sometime in September or October, in Sofia Bulgaria. Details about the meeting will be shared well in advance. In-person participation is encouraged.