SEC.GAL/139/15
15 July 2015
OSCE+
ENGLISH only

Organization for Security and Co-operation in Europe

Regional Workshop for Central Asian participating States and Afghanistan on Cybercrime Units and Law Enforcement Capacities

11-12 June 2015

Almaty, Kazakhstan

Key Findings and Outcomes

The workshop was organized by the Strategic Police Matters Unit of the OSCE Transnational Threats Department, in co-operation with the OSCE Programme Office in Astana and in co-ordination with the United Nations Office on Drugs and Crime (UNODC). The two-day event brought together criminal justice experts from Kazakhstan, Uzbekistan and Afghanistan as well as from Belarus, the Russian Federation, Turkey and the United States of America, OSCE executive structures and UNODC, and an expert from the private sector. Participants shared their experience and exchanged their views on the development of cybercrime units and law enforcement capacities.

In light of the 2008 and 2012 OSCE Annual Police Experts Meetings devoted to "Fighting the Threat of Cyber Crime", and based on the presentations and discussions at the workshop, the following findings and outcomes were compiled:[1]

Strengthening Cybercrime Units and Law Enforcement Capacities

Organizational Framework

- The scope of the use of Information and Communication Technology (ICT) for criminal purposes can take different forms in different countries. Needs assessments are very valuable to adapt the structure, tasks and responsibilities of cybercrime units to the national range.

- Since the Internet user is often the first victim of cybercrime, it is strongly recommended to include prevention as one of the key aspects of national cybercrime strategies. Private-public partnership is a real asset to develop and implement awareness raising programmes for the public.

- The use of ICT for criminal purposes requires the adaptation of national legislations in such areas as the definition of criminal offences, special investigative powers, criteria for admissibility of electronic evidence into Court, international co-operation as well as tasks and responsibilities of cybercrime units and their co-operation with other law enforcement agencies.

- There is a need to ensure inter-agency co-operation between the different law enforcement executive structures addressing the use of ICT for criminal purposes, including cybercrime units, specialized investigators from Ministries of Internal Affairs, Investigative Committees, National Security Committees and forensics examiners, at central, regional and local levels.

- The development of guidelines at the national level, built on cybercrime unit experience, may improve the inter-agency co-operation as well as the conduct of investigations of ICT use for criminal purposes, including admissibility of electronic evidence into Court.

[1] This is a non-exhaustive list which does not imply consensus among the participants or endorsement by, Kazakhstan, Uzbekistan nor Afghanistan, or by the OSCE executive structures.

- The establishment of hotlines allows people to report illegal content anonymously and reduces the time needed to initiate investigations. The illegal content to be reported may be adapted to specific States' priorities, such as child pornography, illicit drug trafficking via the Internet, incitement to suicide.

Capacity Building Activities

- Cybercrime training strategies, built on thorough assessments, should address the different needs of first responders, specialized units of Ministries of Internal Affairs/Investigative Committees/National Security Committees, forensics examiners and trainers.

- Cybercrime training strategies should also address the needs of prosecutors and judges to ensure the effective prosecution and conviction of the offenders using ICT for criminal purposes.

- Trainings should address specific technical challenges when dealing with electronic evidence, such as:
    - Collecting electronic evidence;
    - Storing them;
    - Transferring electronic evidence to experts and defining specific questions;
    - Analysing the result of the examination together with other evidence;
    - Using the result of the examination in Court.

- Regular trainings should be organized to keep experts updated to the changing and evolving forms of ICT use for criminal purposes.

- INTERPOL purple notices are useful to gather information on new modus operandi, objects, devices and concealment methods used by criminals.

- Partnerships with other authorities dealing with different aspects of cyber threats as well as academia and the private sector strongly reinforce law enforcement proficiency. Cybercrime centres of excellence are relevant tools to combine expertise from academic research groups, industry players and public organizations at the national level.

- Learning by practicing, through hands-on workshops or internship programmes, critically improves law enforcement officers know-how in cybercrime investigation.

- Specialized trainings, including on asset recovery of virtual currencies, online counterfeit goods and on the use of Internet for terrorist purposes would be useful for practitioners in the region.

Improving International Co-operation for Obtaining Electronic Evidence

- Gathering information from Internet Service Providers (ISPs) in line with clear cut national legislation and policy was identified as the main purpose of international co-operation in the field of electronic evidence.

- Legal requirements for satisfying foreign requests for obtaining electronic evidence vary in different countries. Generally, the more intrusive of the person's privacy the evidence is sought, the more grounds are required to satisfy a foreign request. For example, ISPs possess the stored and real-time data/evidence. The stored and real-time data/evidence can be divided into three types depending on the level of privacy protection, i.e. information about (i) a person who uses on-line services (subscriber information), (ii) others with whom this person communicates, and (iii) content of his/her communication (e.g. content of e-mails sent and received).

Direct contact with Internet Service Providers

- Direct contact with ISPs may allow law enforcement agencies to gather basic information, such as IP address, and preserve data. Prior contact with law enforcement agencies in the country hosting the ISP would allow checking:
    - If the ISP will be able and willing to reply to the request;
    - If the ISP is linked to organized crime networks;
    - If the ISP will notify the user about the data request. For example, in the United States of America, law enforcement agencies need a Court order to ask for the confidentiality of their request.

Criminal Justice System Co-operation

- Different relevant conventions, treaties and mechanisms facilitate effective and efficient co-operation between law enforcement and judicial institutions.

- Bilateral or multilateral agreements, such as the Council of Europe Convention on Cybercrime signed in Budapest on 23 November 2001, can be more specific on operational provisions of co-operation for obtaining electronic evidence.

- Requesting law enforcement agencies may contact their counterparts in the country hosting the ISP to get knowledge of the type of information which would require mutual legal assistance or could be gathered by direct police to police co-operation. For example, US FBI legal attaché officers assist foreign agencies with requests for investigative assistance in the United States of America.

- The use of INTERPOL channels allows the access to numerous databases such as the International Child Sexual Exploitation Database (ICSE) and the Counterfeit Payment Cards Database and may facilitate contacts with some industries.

- When mutual legal assistance is required to gather information - for example to obtain the content of a communication after having directly contacted ISP for data preservation - requesting authorities may informally consult with the requested authority before making their request and throughout the request implementation, to

ensure mutual understanding of the respective legal systems and requirements of the requesting and requested States. Information provided may include:

  - Justification for the request, depending on the types of evidence sought and emergency situations;
  - Types of certification required for gathering the requested evidence in a way it will be admissible in Court.

- Joint investigations between law enforcement agencies of the requesting country and of the country hosting the ISP, facilitate the implementation of requested special investigative techniques, such as live data forensics.

The Strategic Police Matters Unit of the OSCE Transnational Threats Department stands ready to continue facilitating, according to the "OSCE Strategic Framework for Police-Related Activities" (PC.DEC/1049), at the regional and national levels, capacity-building and the exchange of information and best practices in investigating cybercrime and dealing with cyber evidence, for Central Asian participating States and Afghanistan, at their requests and subject to the availability of funds, and in close co-ordination with other OSCE executive structures and relevant international and regional entities.