Guide on 24/7 Points of Contact under the Budapest Convention on Cybercrime

Concept note for discussion

Prepared by Cybercrime Programme Office
Council of Europe

Background

- Recognition as one of the more “tangible” achievements of the Budapest Convention

- Follow-up to the CoE 2009 Discussion Paper on function of the 24/7 points of contact

- Based on Recommendations from the Assessment report on the mutual legal assistance provisions of the Budapest Convention on Cybercrime

- GLACY project focus (e.g. April 24/7 training in Sri Lanka)

- Skips some obvious descriptions of 24/7 functions

- Offers some principles for further discussion and development

- Remains a draft as of now (last version August 2016)

Institutional setup

- Proliferation of cybercrime and electronic evidence

- Article 35 BCC: "*collection of evidence in electronic form of a criminal offence*".

- Ever-increasing number of criminal cases that require international assistance in preservation, processing and handover of the electronic evidence

- Role beyond data preservation specialists: institution specialized in handling of electronic evidence in the context of international cooperation, as prescribed by the BCC

- Institutional setup: 24/7 points of contact as integral part of cybercrime/high-tech crime investigative units

- 2009 Discussion Paper: "most effective, best resourced and most sustainable option is to have as the CP an office or service specialised in high-tech crime within which a few individuals are identified by name".

Legal basis for operation

-Designation of 24/7 points of contact as electronic evidence processing experts: need for clear legal basis for the operation of such units;

- Analogy to the mutual legal assistance process: criminal procedure or specialized legislation;

- 2009 Discussion Paper: “a specific legal basis could “responsibilise” CP, make them accountable for results achieved, make them known and facilitate cooperation with authorities at the national level, and give them powers for preservation and possibly MLA”.

- Three major sets of regulation:
    - Incorporating regulations/MLA element;
    - Procedural powers under the Convention;
    - Focus on safeguards and guarantees.

- Overall, choice for applicable legal framework rests with the state in question.

Prosecutorial oversight and coordination

- Prosecutors focus on presenting and supporting evidence of the state in criminal proceedings + oversight role for the conduct of investigations.

- Many different investigative agencies and units: Prosecutor/Attorney General's for coordinating functions for requests concerning electronic evidence in criminal cases (e.g. TCY 2014 Report: "establish, where feasible, contact points in prosecution offices to permit a more direct role in mutual legal assistance and a quicker response to requests").

- Coordinating roles may be limited to automatic copying of 24/7 request and authority for immediate assignment of the request to specific investigative authority + follow-up of all data preservation communications

- Prosecutor/Attorney General's as MLA authorities in pre-trial: data preservation requests should be followed by the mutual legal assistance request for production of evidence or for further investigative actions;

- 24/7 point of contact can also receive copies of MLA requests: dependent on clear criteria to single out MLA requests that concern electronic evidence.

Required competences

-2014 T-CY Assessment report: “trained and equipped personnel is available to facilitate the operative work and conduct or support MLA activities”.

- Mix of competences for 24/7: advanced experience in criminal investigations, strong IT/forensics background and knowledge of the legal framework.

-Request depends on knowledge of the contact details, legal requirements and best practices: reliance on already available sources of information/practice guides.

- Transparency with regard to national requirements: reasons for refusing cooperation.

-Use of standard templates or standard checklists

- Automated or semi-automated confirmation of receipt

- Filtering to single out and focus on most urgent and priority requests (e.g. terrorism, child abuse, threat to critical infrastructure and other recognized criteria), etc.

Expediency as an essential feature of the 24/7 process

-2009 Discussion Paper: “The functions of a CP do not require particular investments in infrastructure or technology other than email, fax, telephone, mobile phone, blackberry or similar devices. Some CPs have secure communication system available but do not necessarily use it in this context.”

- Expected expediency with timely response to the actual request: delayed by referral to other law enforcement units for follow-up or lack of immediate explanation of the legal requirements for compliance

- Due diligence of the 24/7 points of contact in following on each and every request in the shortest time possible.

- Realistic expectations as to delays or other difficulties should be conveyed to the requesting party as soon as they become known.

- The point where previously achieved partnerships and cooperation with both public authorities and private players could make a considerable difference.

Interagency and public-private cooperation

-Focus of 24/7 on data preservation implies exclusive interaction with foreign counterparts, national police forces/criminal investigation units and Internet service providers

-24/7 units as international interface for handling electronic evidence in criminal cases: contacts with other units (financial, military, environmental, state security or other criminal investigations)

- Operative memoranda or other formal cooperation frameworks.

-ISPs as focus group for 24/7 points of contact: data preservation

- Cooperation with service providers is crucial in terms of ensuring timely response: uncooperative service providers may tie 24/7 down in legal, technical or managerial issues of compliance

- Formal commitments and cooperation agreements with the Internet Service Providers, preferably along the lines of the 2008 Council of Europe on the Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime

- Start minimal: establish ground for dialogue and availability of contacts as a minimum framework subject to further expansion

- Informal meetings or workshops: matching IT skills.

Communication and visibility

-24/7 point of contact should invest time and effort into making itself known to the rest of the possible stakeholders.

- The 2009 Discussion Paper: “a major problem is that in many countries CP are not known to their own authorities. They should thus make themselves and their role known to relevant institutions.”

- Communication and visibility: not awareness campaigns but active involvement in the national meetings of law enforcement, focusing on cybercrime and electronic evidence

- Rather obvious: 24/7 points of contact should pursue attendance at relevant international events for networking and up-to-date knowlegde.

Thank you for your attention

Cybercrime Programme Office
Council of Europe - Conseil de l'Europe
Bucharest, Romania