Cybercrime@EAP II

International Cooperation under the Partnership for Good Governance with Eastern Partnership countries

2015/DGI/JP/3312
July 2017

Findings and recommendations concerning 24/7 point of contact in Georgia

Prepared by Council of Europe experts under the Cybercrime@EAP II Project

Partnership for Good Governance

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Contents

This review has been prepared by independent Council of Europe expert Branko Stamenkovic, with inputs from Council of Europe experts Aleksandra Tukisa and Aleksandrs Bebris, with the support of the Cybercrime Programme Office of the Council of Europe.

This document was produced with the financial assistance of the European Union. The views expressed herein do not necessarily reflect positions of the European Union or the Council of Europe.

Contact:
Cybercrime Programme Office of the Council of Europe, Bucharest Romania. Email: cybercrime@coe.int

1. Background

The primary purpose of international cooperation in cybercrime investigations and proceedings is the preservation and production of admissible and reliable evidence that can be used in pre-trial and trial proceedings in criminal cases. Electronic evidence in cases of offences against and by means of information technology is usually difficult to collect and relatively volatile; it is therefore crucial that, in investigating and prosecuting cybercrime, the states parties to the Convention on Cybercrime are prepared to employ a variety of international cooperation modalities available under the Convention in an efficient and timely manner.

The Cybercrime@EAP II project aims to support the criminal justice institutions in the Eastern Partnership states in strengthening their capacities for international cooperation in cybercrime and electronic evidence (as a Result of the project). However, the issue of cooperation under the Budapest Convention on Cybercrime, due to its focus on electronic evidence in any criminal cases, is extremely wide in scope. Criminal justice authorities of the states are thus supposed to explore all possibilities for cooperation under the Budapest Convention, including effective use of cooperation channels established under this treaty, such as network of 24/7 points of contact under Article 35 Budapest Convention.

In this context, the Cybercrime@EAP II project noted certain concerns as regards limited role, responsibilities and action by the 24/7 point of contact at the Ministry of the Interior of Georgia.

Lack of legislation implementing provisions of Articles 16-18 of the Cybercrime Convention and lack of internal regulations that define precisely what is expected from a 24/7 point of contact have been already pointed out and discussed with the country team.

Les obvious but still important challenge remains lack of understanding and willingness of the higher-level management at the Ministry of the Interior, Prosecution Service and other key agencies to accord the 24/7 unit its functions as required by the Convention, including direct follow up with investigative actions where necessary, its role in the mutual legal assistance process, and its supportive role with regard to electronic evidence for the entire criminal justice system - not just for the cybercrime unit.

Based on these preliminary indications and following a series of meetings with Georgian counterparts on 10-12 July 2017 within the framework of the Cybercrime@EAP II project, the Council of Europe experts[1] developed several recommendations, outlined below, meant to improve the functioning of the 24/7 point of contact in Georgia in the longer term.

[1] Branko Stamenkovic (Serbia), Aleksandrs Bebris (Latvia) and Aleksadra Tukisa (Latvia).

2. Meetings held and findings

2.1. Preparatory meeting at the Council of Europe Tbilisi office

Representatives of Cybercrime@EAP II project Georgian national team were present, namely from Prosecution Service and Ministry of the Interior. Ministry of the Interior was represented by cybercrime unit and 24/7 contact point, and from Prosecution Service - by head of the international legal assistance unit for Chief Prosecutor's Office.

The goals of the mission was agreed: to establish how 24/7 network and contact points are organized; study legal basis for operation of contact points; establish criminal investigation capacities with regards to cybercrime/electronic evidence-related offences; and share international experience in cybercrime and electronic evidence.

Georgian criminal procedural framework was kept constantly in mind during the meetings. It was emphasized that mission should primarily offer support and transfer experience and knowledge about importance, operational setup and strength of 24/7 point of contact, through open discussion in visited institutions - as a fact-finding mission with some of the agencies with regards to their competencies.

Due to on-going reforms and some concerns related to independence of judiciary, meetings with the Financial Police and the Tbilisi City Court did not take place.

2.2. Ministry of the Interior

Meeting was organized in operational building of the Ministry in Tbilisi. Head of international crimes department, representative of Research and Development department, T-CY representative, Head of the regional cooperation service, Head of Cybercrime department and members, representatives of 24/7 contact point and of the Police Academy were present.

It was noted that Georgia ratified Cybercrime Convention of the Council of Europe in June 2012, which entered into force in October 2012. Ministry of Interior formed on December 2012 a new Cyber Crime Division. Criminal Code of Georgia in Chapter XXXV is providing cybercrime criminal acts. It is noted that some provisions regulating the setup of National contact bureau for Interpol, special investigation measures, bilateral and multilateral cooperation and 24/7 Council of Europe Network contact point are in place, but they are not sufficient.

Cybercrime division of the Ministry of Interior is an operative and technical unit in essence, but also performs investigations and performs 24/7 contact point functions. It actively uses mails and phones of two officers and is live 24/7 for this cooperation. Several requests from some countries were recorded by the use of the network so far.

Most important challenges noted were acquiring basic subscriber information without court order (impossible at the moment), lack of regulation for data preservation and lack of internal regulations for 24/7 national contact point. Unclear obligations on the side of the ISPs for data retention, due to on-going legal debates, were noted, which makes cybercrime investigations difficult. Due to voluntary nature of preservation, complied requests are sent to requesting states with indication that the obtained information does not have evidentiary value.

With regard to 24/7 POC network, some amendments are planned by drafting changes to Decree of Statute of the Criminal Police. However, representatives were of the view that

there are no problems in international cooperation between Georgian and foreign police services and Ministries of Interior. There are no reported delays in response to 24/7 request from Georgian side. Problems are primarily within legal environment which hinders cooperation.

Cooperation with prosecutors in the process of 24/7 request processing was noted as a necessity but also as a hurdle from operational perspective. Based on the national legislation, Prosecution has overseeing role but it does not participate in investigation.

With regard to outgoing requests, it seems that problem is lack of awareness about importance of functioning of the 24/7 network, especially when it related to production of evidence for criminal proceedings and not just exchange of intelligence. Some questions were raised by experts about competent authority for criminal law mutual legal assistance by Georgian legal framework, as the evidence acquired in the course of the police investigation should be finally acceptable as court evidence. It has been established that Chief Prosecutor's Office is the sole competent authority with regard to mutual legal assistance in all areas, including production of evidence, which, if collected in line with the domestic legal framework, can be used in court proceedings.

The prevailing impression of the meetings with the police representatives is that 24/7 point of contact is viewed as primarily police to police cooperation and operational/intelligence exchange platform. General concerns of electronic evidence in potentially all criminal cases seem to be addressed as overall police capacity and training problems, rather than strategic and institutional priorities.

2.3. Ministry of State Security

Ministry of State Security has competence for covert investigations, and it was separated from the Ministry of Interior a couple of years ago. The Agency created for data retention purposes under the Ministry claims to have the strongest digital evidence forensic lab. They don't have investigative functions, only technical and they are not using 24/7 network for the time being. They are not the only lab, there are other labs like ones in the Ministry of the Interior and Ministry of Justice, but they are confident that Agency one is the strongest.

With regards to the electronic evidence analysis, Ministry of Interior and Prosecution can ask for digital forensics. Court involvement is restricted to certain procedural tools, like orders for search and seizure. Regarding data retention, data is not retained by ISPs but by the Agency itself; however, this setup is still under on-going constitutional review. That's why new separate division of the security agency for data was formed and now they have exclusive data retention authority. The controlling mechanism in the form of Personal Data Inspector oversees how data has been retained in real-time through rather unique technical solution.

The Agency retains all basic subscriber information and traffic data, but not content data. The overall period for retaining data is one year. Interception orders can be issued only by the Court: general criminal courts are issuing order for criminal cases, while Supreme Court special judge issues orders related to National Security cases.

The Agency does not have direct involvement in 24/7 POC process because it is not directly connected to the network and other criminal law institutions in the country. Legal way for asking for involvement of the Agency would be: 24/7 Council of Europe Network requesting party sends request to the Georgian counterpart; request is forwarded request to prosecution; prosecutor files motion to the Court about engaging Agency; the Agency will respond back using same channel of communication.

This lengthy process is considered as a shortcoming and Agency representatives believe there should be more involvement into cooperation within 24/7 Network, due to Agency's technical and human capabilities. At the same time, almost entire activity of the Agency is driven by judicial orders.

It seems that some bigger ISP's are retaining data, depending on their business and operational strength. Data retention in this way is not forbidden, but it's not mandatory either (questions about data protection perspective on this practice are inevitable). Legal changes are envisaged, after which prosecutors will be able to ask Agency for basic subscriber information and traffic data without court orders; currently, the amendments are in the Parliament but the priority is given to current constitutional debates.

2.4. Ministry of Justice, Data Exchange Agency and CERT.GOV.GE

Initial inquiry went in direction of how data exchange is occurring between CERT, legal enforcement agencies and judiciary, if at all, and what's their role in international cooperation. From the legal perspective, Georgian CERT is based on the law and internal regulations, and it represents both national and government CERT. Also, law defines critical incidents which are in the base of the Georgian CERT competence.

There is a mandatory obligation by government officials to report incidents against critical infrastructure to CERT.GOV.GE. After receiving report, CERT.GOV.GE analyses the incident and makes recommendations. Sometimes they notify victim through the corresponding ISP by informal communication. If there is to be cooperation between LEA and CERT, law encourages for memorandum of cooperation as an effective tool for separation of responsibilities and powers. At the moment, they are conducting their interactions on informal basis.

Criminal Code stipulates that if there is a grave or serious crime which includes cyber-attacks on critical infrastructure, it must be reported by the CERT to criminal police; otherwise, it can be characterized as criminal act of non-reporting. CERT doesn't have legal obligation to report all potential criminal acts to the police. However, they do have a good informal cooperation with LEA and they do report their observations to them. Question remains as to how CERT technical staff recognizes criminal acts and then makes decision what to report to the police.

International cooperation between CSIRTs is driven by membership of European and international associations, as well as bilateral memoranda of cooperation with other CERTs, especially the ones from Europe, but not only with them (e.g. private sector companies). Good local and regional cooperation exists, as well as CERT to CERT direct level communication. Voluntary cooperation is in place as well, exchanging data about incidents and know-how for solving problems. Depending on the counterpart for communication, CERT to CERT and CERT to government (foreign one especially) communication is good, while there are problems of communication with private sector. Still, often there is no formal follow-up after initial exchange of information.

By Information Security Act, CERT services are envisaged for all government institutions but not in mandatory way. However, it's very much recommended to all institutions to use the services of CERT. CERT staff is directly involved in removing of the threat in the affected institution, once when incident has been reported and established. They have competence to react not only in case of Government attacks, but also private sector and even in case of attacks against individuals. They don't have competence only over Ministry of Interior and Defence and State Security Agency. CERT reporting and cooperation is although obligatory for critical information infrastructure.

Cooperation with law enforcement on specific cases was discussed, but seems to be subject to the same one-way communication: CERT notifies and handles the incident including expert support, but no follow up is happening after handover of the case to criminal police.

International cooperation is very much needed between CSIRTs. It is noted that there should be legal obligation for CERT experts to know what they can do on their own with regard to the attacks, without necessity to contact prosecutors or police for consultations on frequent basis. Frequent changes of legal framework or capacities are not good and are not making sustainable environment. One way communication represents a problem.

CERT.GOV.GE is of the opinion that at the moment staffing is appropriate (5 members). Georgian CERT exists for 7 years now, but start was difficult with regard to establishing trust; situation is much better now and government institutions have good knowledge and appreciation of their value.

2.5. Prosecution Service of Georgia

Prosecution office represents single central authority for Georgia for mutual legal assistance in criminal matters. Prosecution Service is part of the Ministry of Justice. Prosecutors of international cooperation unit are analysing requests for MLA and making prioritization of the cases based on urgency criteria and benefits when making decision which cases are going to be attended immediately. That means that if the case is important and there is interest for Georgia, request is going to be served in a matter of hours and days.

Office is handling 200-300 sent cases per year in average and about 2000-3000 incoming cases. Average time for processing is around four months, although the execution time can range between few hours (depending on the urgency and prioritization of a case) to a full year. Preservation requests can be handled by prosecution, although it's mainly a police activity. If requested, preservation request would come directly to the General Prosecution Office. Request should be marked as "urgent" if requesting country wants immediate reaction.

Georgia has ratified European convention on mutual legal assistance in criminal matters and Second additional protocol, but with reservation about direct judicial cooperation. Local prosecution offices are not contacting foreign ones by them own, they are consulting central authority. Police-Prosecution cooperation depends mostly on departmental level and executive level cooperation. Police basically has reduced competence with recent changes in the legal framework, with Prosecution taking over more of the jurisdiction over investigation. Court approval on motions is decreasing because standards are getting higher with regard to standard of proof (probable cause standard is applicable to production, search and interception warrants), which is directly related to misunderstanding of the police about quality of evidence and thus lack of cooperation with the Prosecution Service.

Since Prosecution is a central authority for MLA, Chief Prosecutor's Office is interested in enhancing the capacities of the 24/7 contact point in the Police, especially with a view of lack of police powers for mutual legal assistance in criminal matters. At the same time, the General Prosecutors Office already has similar (albeit not identical) capacities for fast handling of international cooperation requests due to efficient practical arrangements, like having multinational service providers' requests being sent by the Prosecution directly. This is again due to practical reasons as e.g. Facebook would accept requests for disclosure of basic subscriber information from the police, but the compliance rate would much higher for requests sources from the Prosecution Service. In this sense, International Department of the Prosecution Service serves as an actual contact point for multinational service providers,

which however does not replace the primary functions and responsibility of the 24/7 point of contact in the police which is a designated 24/7 POC for these purposes. In any case, direct involvement of the Prosecution Service in cooperation with MSPs should be commended in the sense of having more effective and faster mutual legal assistance when it comes to cybercrime.

It has been noted that General Prosecution Office of Georgia is one of the lead agencies in implementation of the National Strategy on Cybercrime (part of Organized Crime Strategy). It has more roles towards overseeing on the policy and strategic levels, not to conduct actual cases, although criminal investigation is driven and/or supervised by prosecution.

Prosecution Service has one prosecutor who is overseeing the police cybercrime unit and their investigations. It also has been noted that Prosecution Service would like to establish policy guidelines when it comes to the functioning of 24/7 network and handling of the cybercrime cases coming from that source.

3. Conclusions and recommendations

The meetings with the Georgian authorities have both confirmed initial indications of the need to advocate for stronger and more effective 24/7 point of contact, as required by the Budapest Convention, but have also uncovered a positive trend of steps being taken to remedy the situation at legal, regulatory and organizational level. Interagency cooperation to ensure proper processing of the requests received and sent by 24/7 network of the points of contact is important element for its efficient work.

The following proposals are therefore submitted for consideration by the authorities of Georgia:

- Further strengthening of the Cybercrime Unit at the Organized Crime Department of the Ministry of the Interior, including its 24/7 point of contact, in terms of more human and technical resources available, including specialized training and selection procedures for the officers of the unit, taking into account not only cybercrime cases but also electronic evidence challenges;
- Ensure better coordination between the officers of 24/7 point of contact and International Cooperation services of the Ministry of the Interior, with a view of coordinating requests processed through other networks (e.g. INTERPOL);
- Raising awareness amongst Ministry of Interior executives about necessity for better cooperation and coordination with Prosecution Service - and vice versa;
- As a part of improving interagency cooperation, consider signing Memorandum of Understanding and Cooperation between Ministry of Interior – International and Cybercrime Departments - and Chief Prosecutor's Office on matters of international cooperation with regard to cybercrime and electronic evidence;
- Adoption and introduction of internal legal framework/regulations pertaining to organization, functioning and procedures of the 24/7 contact point in the Ministry of the Interior;
- Observe and follow further developments regarding legal framework for retention of communications data and access to data by the law enforcement, including compliance with international cooperation requests;
- Stronger involvement of CERT.GOV.GE capacities in cooperation, consultation and training of criminal justice authorities;
- Encourage adoption of a set of rules and/or agreements in areas of incident/crime reporting, coordination between CSIRT/law enforcement cooperation channels, and general division of responsibilities for security of cyberspace;
- Consider feasibility of establishing specialized department, division or office for cybercrime and electronic evidence within the prosecution system of Georgia;
- Consider the necessity for establishing second 24/7 national contact point for Cybercrime Convention within Chief Prosecutors' Office;
- Strengthening capacities of the Prosecution Service for tackling cybercrime at all levels (central, district and local), including training of the prosecutors on cybercrime and electronic evidence.

The Council of Europe remains available to provide further assistance to on the subject of 24/7 point of contacts within the overall theme of international cooperation on cybercrime and electronic evidence.