www.coe.int/cybercrime

Strasbourg, version 3 July 2018

T-CY (2018)21

Cybercrime Convention Committee (T-CY)

T-CY 19

19th Plenary Meeting of the Cybercrime Convention Committee

Item 7: Information provided by parties and observers and status of signatures, ratifications, accessions to the Budapest Convention and its Protocol

Compilation of replies

www.coe.int/TCY

Background

The Cybercrime Convention Committee (T-CY) holds its 19th Plenary session on 9 July 2018.

Given that only limited time is available during the one-day plenary, delegations were invited to submit written updates under item 7 of the T-CY 19 Agenda by 20 June 2018 to be published as part of the Plenary documentation.

By 2 July 2018, five Parties had provided such information.

The present document represents a compilation of the replies received.

Table of contents

1 Information received

1.1 Croatia

The Croatian delegation's updates on major legislative developments and changes:

1. Due to structural reorganisation of the Ministry of Interior, General Police Directorate, since the beginning of 2018 a new established Crime Intelligence Sector, Cyber Security Department has been taking the tasks and responsibilities of Croatian 24/7 Network point of contact in accordance with Art. 35 of the Convention on Cybercrime, instead of previous point of contact within the General Police Directorate (National Police Office for Suppression of Corruption and Organised Crime, Economic Crime and Corruption Service, High-tech Crime Department). The telephone number and e-mail address for receiving and sending requests remains the same.

2. In June 2018 the Ministry of Justice has prepared the Draft Law Amending the Criminal Code of the Republic of Croatia and informed the interested public on the Draft Law for the purpose of consultations in procedures of adopting laws.

According to proposed law amendments, the legal description of a criminal offence of damaging to computer data (Art. 268 (1) CC) should be slightly amended in „Whoever damages, alters, deletes, destroys, suppress or renders inaccessible, in full or in part, another's computer data or programmes without right shall be sentenced to imprisonment for a term of up to three years." Current legal description of Art. 268 (1) CC) reads as follows: "Whoever damages, alters, deletes, destroys, renders unusable or inaccessible, or presents as inaccessible, in full or in part, another's computer data or programmes without right shall be sentenced to imprisonment for a term of up to three years."

Additionally, in order to clarify a possible misunderstandings it has been proposed to expressly put in the Criminal Code that the object of illegal access (Art. 266 CC) can be both the whole and a part of the computer system and that misuse of devices (Art. 272 CC) includes distribution as well.

In order to comply with the Directive (EU) 2017/541 of the European Parliament and the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA it has been proposed to expand a legal description of the criminal act of terrorism (Art. 97 CC) by adding illegal system interference against a critical infrastructure information system as terrorist offence where commited with the aim of seriously intimidating a population or unduly compelling a government or an international organisation to perform or abstain from performing any act or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.

1.2 Czech Republic

Update from the Czech Republic on legislative ammendments and proposals:

Competent authorities of the Czech Republic are focusing on the issue of cybercrime over a long period of time. Lately, an amendment of the Code of Criminal Procedure was proposed. At this moment, the draft of the law passed the 2nd reading at the Chamber of Deputies of the Czech Republic Parliament.

In accordance with Article 16 of Convention on Cybercrime this amendment incorporates an explicit provision into the Code regarding expedited preservation of stored data in order to preserve and maintain

the integrity of data, where there are grounds to believe that the data (in the form of evidence shall be used in the criminal proceedings) is particularly vulnerable to its loss or modification.

In addition to that, Ministry of Justice of the Czech Republic proposed a withdrawal of the reservation to Article 29 par. 4 of the Convention on Cybercrime, which is now being discussed in the Czech Parliament as well. The aim of the withdrawal of the reservation is to shift consideration of a condition of dual criminality to the seizure/search/disclosure stage (not in the stage of data preservation) so that international cooperation as well as mutual legal assistance in the area of cybercrime shall be more effective.

Czech Republic expects that both issues will be adopted soon and T-CY Committee will be informed on the progress in due time.

1.3 Japan

Japan's update on efforts of countering cybercrime:

Japan supports to hold workshops coordinated by INTERPOL through the Japan-ASEAN Integrated Fund (JAIF) to promote cooperation within or beyond the ASEAN region regarding capacity development, training, law enforcement, policy coordination, legal matters and information exchange concerning cybercrime. Since last November, 3 workshops have been held: "Cybercrime Workshop for Law Enforcement Agencies and Judicial Authorities" and "Meeting of Decision-Maker and Heads of Cybercrime Units" in April, and "Training on Darknet and Cryptocurrencies" in May. More workshops in this area will be held throughout this year.

From January 29 to February 16 of 2018, National Police Agency (NPA) and the Japan International Cooperation Agency (JICA) held a training program for law enforcement authorities of Japan's Official Development Assistance (ODA) recipient countries, to develop capacities especially in enhancing knowledge and experience as well as cooperation among law enforcement authorities in combating cybercrime. 17 law enforcement officials from 15 countries participated in this training program in Japan. In addition, NPA and JICA will give capacity development training for cyber security and countering cybercrime to officials of Vietnam Public Security Ministry in October of 2018, following the previous year's training.

In February, Japan joined the workshop on the Budapest Convention hosted by the United States held in Malaysia (High Level Round Table Discussion on Budapest Convention on Cybercrime) and made a presentation on our past efforts in concluding the Convention and its good results.

In March, Japan held a training program on the theme of "New types of Evidence" in Japan as a series of the project for Capacity Development of Legal, Judicial and Relevant Sectors in Myanmar. We gave lectures on the Budapest Convention and the handling of scientific evidence and provided tours to related facilities for judges, prosecutors, law enforcement agents, members of Parliament from Myanmar for the purpose of providing expertise in scientific investigation, countering cybercrime and current digital forensic technique in Japan.

Also, Japan is now preparing for holding the 3rd Japan-ASEAN Cybercrime Dialogue in Brunei in August.

We continue to actively support the capacity building in countering cybercrime. And we advocate the importance of the Budapest Convention at every opportunity, and encourage especially Asian countries to conclude the Budapest Convention.

1.4 Liechtenstein

Liechtenstein's revisions to their cybercrime legislation:

Liechtenstein currently conducts a revision of its criminal code. This revision includes some minor developments in Liechtenstein's cybercrime legislation. It encompasses a legal definition of the term "critical infrastructure" and the criminalization of any illegal access, illegal interception and data or system interference of a computer system of said critical infrastructure. Furthermore, the revision proposes an extension of the offence "illegal access", so that all forms of "Hacking", for example Bot-Nets, will be covered as criminal offences. The revision also includes the criminalization of acts that can be summarised under the term "Cybermobbing". To achieve this, a new paragraph was included in the criminal code.

The revision is scheduled to be discussed in the Liechtenstein parliament in October or November this year. Therefore, its adoption is expected in 2019.

1.5 Slovakia

Since the last plenary session of the T-CY, no substantial facts have been noted.

However, some things may be reported. As regards activities of **the General Prosecutor's Office of the Slovak Republic**, a significant point that can be mentioned is the evaluation of the task of the main tasks of the General Prosecutor's Office - **assessment of the speed and accuracy of prosecutors' progress in the expedited preservation of computer data and the execution of MLA in the field of computer-related crime** (application of international and European legal instruments and national provisions, in particular Section 90 and Section 116 of the Criminal Code in conjunction with Part V of Code of Criminal Procedure) for the period 2016-2017. The matter would be further discussed by the General Prosecutor's Office on June 25, 2018.

Furthermore, several activities flowing from standard tasks of General Prosecutor's Office are relevant:

- educational activities (for example, a lecture at the working meeting of the criminal prosecution department of the General Prosecutor's Office for specialists in juvenile or minor delinquency crimes, crimes committed against children and violence in families on the topic "Proof of crimes committed against children and relatives by means of the Internet and electronic means." The lecture focused on providing evidence through MLA from the United States, on the specific aspects of such cooperation, the extent of data that can be secured, legal and other related issues),
- the activities of the **National Network of Prosecutors for Combating Cybercrime** - the initiation of a meeting on application problems related to cooperation with providers
- **Active participation in the activities of the European Judicial Cybercrime Network** (including active cooperation of the network's contact points in joint NL/SK case), an opinion on WHOIS was adopted within the EJCN, which can be accessed on website of EUROJUST,
- Intensive cooperation between the International Department of the Prosecutor General's Office and the Computer Crime Department of the Criminal Police Office of the Presidium of the Police Force continues. Apart from usual tasks, the participation of a representative of the General Prosecutor's Office at the workplace of the mentioned cybercrime department within the framework of the Slovak Republic involvement in the exercise organized by ENISA - CYBER EUROPE 2018 (more on http://www.cyber-europe.eu/) can be highlighted.

Experts from **Ministry of Justice of the Slovak Republic and General Prosecutor's Office** also actively participate in n the negotiations on **new legislative proposals in the EU** – Proposal for a Regulation on

European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings

Furthermore, the **first legislation on cybersecurity** within the Slovak Republic came into force on 1 April, 2018. The **Act on cybersecurity** transposes the European Directive on Network and Information Security (NIS Directive). The act covers eleven sectors and establishes **minimum security and notification requirements for responsible entities** (operators of essential services and digital service providers) with the aim to provide cybersecurity in the Slovak Republic. At the same time it regulates **jurisdiction of public administration bodies** in the field of cybersecurity, **organisation and competencies of CSIRT units**, it established **Cybersecurity Single Information System**, to ensure education and awareness building. The Cybersecurity Act also includes inspection mechanisms and sanctions.

The National Security Authority with relevant sectoral authorities have been working together at the **secondary legislation** necessary to implement specific aspects of NIS Directive. **Three implementation decrees** (Regulation on Criteria of Essential Services, Regulation on identification criteria for respective categories of cybersecurity incidents and details of cybersecurity incidents reporting, Regulation on details of the technical and technological equipment and staffing of the CSIRT Unit) entered into force on 15 June, 2018.

The new Act on cybersecurity established the **National CSIRT** Unit (SK-CERT), the **Governmental CSIRT Unit** and **Centre for Cyber Defence** of the Slovak Republic including the **Military CSIRT**.

SK-CERT unit has already become a full member of the community of Security and Incident Response Teams by gaining the accredited status, the second level of membership within the Trusted Introduces Service on 3 May 2018. This event together with the membership in CSIRT Network and the membership in the international Forum of Incident Response and Security Teams represent an important step for a development of a CSIRT unit and gaining international recognition in the cyber community.
Slovakia reached the top place in the Global Index of Cybersecurity NCSI (National Cyber Security Index) earning maximum scores in seven of twelve evaluated indicators.