www.coe.int/cybercrime

Strasbourg, version 27 November 2018

T-CY (2018)36

Cybercrime Convention Committee (T-CY)

T-CY 20

20th Plenary Meeting of the Cybercrime Convention Committee

Item 5: 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 20th Plenary session on 27 November 2018.

Given that only limited time is available during the one-day plenary, delegations were invited to submit written updates under item 5 of the T-CY 20 Agenda to be published as part of the Plenary documentation.

By 27 November 2018, four Parties and one Observer had provided such information.

The present document represents a compilation of the replies received.

Table of contents

1 Information received

1.1 Costa Rica

Update from Costa Rica regarding the capacity building activities on cybercrime and electronic evidence:

For more details, please see Report of activities carried out within the framework of the GLACY+ Project in Costa Rica.

1.2 Japan

Japan's Update on Efforts of Countering Cybercrime

In July 2018, Government of Japan developed New Cybersecurity Strategy as the second "basic plan for Cybersecurity" under the Basic Act of Cybersecurity. Far-seeing 2020, the Strategy stipulates and demonstrates domestically and internationally basic position and vision of Japan on cybersecurity, and its objectives and implementation policies in next 3 years (2018-2021). In the Strategy, it is stated that Japan enhances measures against cybercrimes so as to build a safe and secure society for the people, and that Japan will disseminate its position in the international fora, ensure its national security by utilizing existing frameworks, and promote international collaboration in order to ensure a free, fair, and secure cyberspace from the viewpoint of contribution to the peace and stability of the international community and Japan's national security. For more details please refer to the website below.
http://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf
http://www.nisc.go.jp/eng/pdf/cs-senryaku2018-zentaigaiyou-en.pdf
http://www.nisc.go.jp/eng/pdf/cs-senryaku2018-shousaigaiyou-en.pdf

To promote cooperation within or beyond the ASEAN region regarding capacity development, training, law enforcement, policy coordination, legal matters and information exchange concerning cybercrime, Japan continuously supports ASEAN Cyber Capacity Development Project (ACCDP) coordinated by INTERPOL through the Japan-ASEAN Integrated Fund (JAIF). Since this July, 2 workshops were held: "Cybercrime Training for Managers" in August and "Cyber Research Seminar" in September on the initiative of INTERPOL. Participants of the workshops discussed on issues including digital evidence, current trend of cybercrime and international cooperation. INTERPOL is preparing country reports for each ASEAN country, which describe challenges and need for countering cybercrime.

Following the previous year's training, from November 5 to 16 in this year, National Police Agency (NPA) of Japan and Japan International Cooperation Agency (JICA) jointly provided the training to 10 officials of Vietnam Public Security Ministry who engage in combating cybercrime. The program aimed at providing knowledge and experiences related to cybercrime and strengthening the cooperation between law enforcement authorities of Japan and Vietnam. In addition, from January 28 to February 15 in 2019, NPA and JICA will hold training for 24 law enforcement agencies in 24 countries by Japan's Official Development Assistance (ODA), to develop capacities of coping with cybercrime.

From December 4 to 6 in this year, NPA is to hold 19th Counter-cybercrime Technology and Investigation Symposium. Nineteen organizations from Asia-Pacific and other regions will take part in the Symposium to improve the capabilities to perform analysis of information technology of law enforcement agencies in Asia-Pacific region by sharing best practices, knowledge and experiences regarding analysis of information technology.

Now, Japan is preparing for the 3rd Japan-ASEAN Cybercrime Dialogue in Brunei in January in 2019. We are going to share trend of cybercrime and good practices to counter cybercrime with ASEAN countries, and grasp the outcome of capacity building assistance for ASEAN countries and each challenge of them. To that end, we continue to conduct more meaningful and effective capacity building assistance for them.

1.3 Nigeria

Update on developments in Nigeria

Accession: The Federal Executive Council has not yet given the final approval for Nigeria's accession to the Budapest Convention. Consultations are still ongoing, and we remain hopeful that this may happen at any time from now.

Legislation: The development of the Data Protection legislation in Nigeria is at an advanced stage. With the support of the GLACY+ Project, a Data Protection legislation Legislative Drafting Retreat with all stakeholders was held in Calabar from 10 – 14 September 2018 and a harmonized draft Data Protection Bill, 2018 was produced and exposed for public comments. This was followed by a public Validation Workshop held on 08th November 2018, at which suggested amendments, corrections, and additions to the exposure draft were considered and it was unanimously validated subject to the corrections. The Draft Data Protection and Privacy Bill, 2019 is undergoing final editing and will be submitted to the Senate on 03 December 2018, after which the Senate will pass it and attain concordance with the Data Protection Bill that was passed by the House of Representatives, then sent for Presidential assent.

Capacity building: The GLACY+ Project has continued to provide support in this area, which has enabled several of our LEAs to participate in international trainings, collaborative meetings and relevant conferences. The support of the Council of Europe and other partners towards the actualization of the first African Forum on Cybercrime from 16-18 October 2018 in Addis Ababa, Ethiopia, must be applauded. In country, some capacity building activities have been planned in Nigeria such as the Training of trainers for First Responders course which is scheduled to take place from the 10th to 14th of December 2018 and the Judicial Training slated for early 2019.

The Cybercrime Advisory Council has also finalized plans to roll out a cybersecurity awareness campaign in 2019 to drive citizen enlightenment and general cyber hygiene.

1.4 Serbia

Update from Serbia on the progress made in the field of combating cybercrime by Special Prosecution for High-Tech Crime of Republic of Serbia in the period June – December 2018

Special Prosecutor’s Office for High-Tech Crime was founded by the Law on Organisation and Competences of Government Authorities in Fight against High-Tech Crime of 25 July 2005.

According to the Law on Amendments of this Law, which entered into force on 01 January 2010 the subject-matter jurisdiction of the Special Prosecutor's Office includes prosecuting of the perpetrators of criminal offences against the security of computer data, as well as criminal offences against intellectual property, assets, commerce and legal traffic, where the object of an offence or means to commit it are computers, computer systems, computer networks and computer data as well as their products in a tangible or

electronic form if number of items of copyrighted work exceeds 2,000 copies or if the material damage exceeds the amount of 1,000,000.00 dinars. Also, this Prosecution is in charge of processing criminal offenses against the rights and freedoms of man and citizen, gender freedom, public order and the constitutional system and security of the Republic of Serbia, which according to the way or the means of execution can be considered cybercrime.

As for the territorial jurisdiction, this Special Prosecution is competent for this type of criminal offences on the entire territory of the Republic of Serbia.

1.3.1 Statistical data

Comparative review of the total number of criminal complaints per year according to criminal registers KT (known adult perpetrators), KTN (unknown perpetrators) and KTR (various criminal cases) since the establishment of this Prosecution shows a visible increase in committing these criminal offences.

	Kt registry	Ktn registry	Ktr registry	Total	Increase/decrese percentage in comparison to the previous year
2006.	19	0	0	19	
2007.	75	11	68	154	710.53%
2008.	110	14	60	184	19.48%
2009.	91	42	114	247	34.24%
2010.	116	13	443	572	131.58%
2011.	130	28	502	660	15.38%
2012.	114	65	609	788	19.39%
2013.	160	243	558	961	21.95%
2014.	294	352	770	1.416	47,35%
2015.	198	570	1.306	2.074	46,47%
2016.	240	580	1.237	2.057	-0,77%
2017.	213	945	1.213	2.371	15,21%
30.09.2018.	234	904	1.024	2.162	
TOTAL	1.994	3.767	7.904	13.665	

Special Public Prosecutor's Office for High-Tech Crime in the framework of conducting activities for suppression of cybercrime, devotes special attention to the suppression of the hate crime on the Internet. The practice so far has been of particular importance in the area of special prevention and has deterrent effect on the potential perpetrators of hate crimes due to race and religion, national or ethnic affiliation, gender, sexual orientation or gender identity of another person. Significant results in particular, the prosecution has significant results in suppressing criminal offenses against members of the LGBT population.

1.3.2 Strategic documents aimed at suppressing High-Tech crime

The European Agenda on Security for the period from 2015 to 2020 recognizes terrorism, organized crime and the cyber-crime as the three most serious threats to EU security and the key priorities to be addressed.

In addition, IOCTA (Internet Organized Crime Threat Assessment 2017) - Assessment of the threat of Internet organized crime conducted by the Europol Center for High-Tech Crime identified the following threats in the field of high-tech crime:

- Cyber dependant crime
- Child sexual exploitation online
- Payment fraud
- Online criminal markets
- The convergence of cybercrime and terrorism
- Cross-cutting crime factors

Pursuant to the above mentioned documents, numerous strategic documents of the Republic of Serbia recognize the necessity of combating high-tech crime. Thus, the **Strategy for the Development of Information Security** in the Republic of Serbia for the period from 2017 to 2020 identified the suppression of high-tech crime as one of the priority areas for the development and improvement of information security in the Republic of Serbia.

In this regard, in the area of combating high-tech crime, the following strategic objectives have been identified:

• Improving mechanisms for detecting high-tech crime and prosecuting perpetrators;
• Raising awareness of the dangers of high-tech crime;
• Improving international cooperation in the fight against high-tech crime.

Also, by the **Strategy of Information Society Development** in the Republic of Serbia until 2020, the fight against high-tech crime has been recognized as one of the strategic priorities in the field of information security.

Governemtn of Serbia in October 2018 adopted **Strategy for the Fight against Cyber Crime** for the period 2019-2023, which stipulates four specific goals in the field of high-tech crime, namely:
1. Improved and harmonized legislation of the Republic of Serbia with legal norms and standards of the European Union in the field of combating high-tech crime
2. Improved organizational, personnel, technical and operational capacity of the state authorities competent for suppression of high-tech crime
3. Improved preventive and proactive approach in the fight against high-tech crime
4. Improved cooperation at the national, regional and international level.

It is also necessary to point out the **Proposal of the Strategy for the Development of Intellectual Property** for the period from 2018 to 2022, which emphasized the important role of the Special Prosecutor's Office for High-Tech Crime in the field of protection of intellectual property rights, that is, the prosecution of perpetrators of intellectual property offenses when the objects or means of committing criminal offenses are computers, computer systems, computer networks, computer data, as well as their products in material or electronic form, in particular computer programs and copyrights that can be used in electronic form.

1.3.3 Activities in relation to EU integration process

Special Public Prosecutor’s Office for High-Tech Crime has continued to participate in the negotiation process for Chapter 24 - Justice, Freedom and Security and Chapter 7 - Intellectual Property Law.

In order to complete the activity *Analyse the current legislative framework in order to determine the level of its alignment with the acquis and EU standards* which is prescribed by the Action plan for Chapter 24, on 30-31 March 2016, TAIEX expert mission was held in the Republic Public Prosecution with the aim to assess the level of alignment of the legal framework with the EU acquis. In cooperation with representatives of the Republic Public Prosecutor's Office, Special Public Prosecutor's Office for High-Tech Crime, Ministry of Interior - Department for combating cybercrime and the Ministry of Trade, Tourism and Telecommunications, an expert analysed the national legal framework and made recommendations to amend the relevant regulations in order to comply with the EU acquis. In accordance with those recommendations, the Republic Public Prosecution submitted an initiative to Ministry of Justice to amend relevant regulations in this field.

In order to complete the activity *Develop and sign Agreements on cooperation among state authorities and civil society institutions in fighting cyber-crime*, apart from previously established cooperation with a civil society organization – "Fund B92" that resulted in activating a web portal Net Patrol (online tool for reporting illegal or harmful content on the Internet), the Special Prosecution for High-Tech Crime also established cooperation with the international civil society organization "Save the Children" within a Judicial Academy program for developing a plan and training programs for judges and public prosecutors in the field of cyber-crime and protection of minors on the Internet. Signing a Cooperation Agreement with the organization "Save the Children" is under consideration having in mind already established cooperation.

Action Plan of the Republic of Serbia for Chapter 24 also prescribes the activity *Strengthening capacities of the Special Prosecutor's Office for Cyber-crime* which stipulates staff increase by 2 deputy public prosecutors, 2 prosecutors' assistants, 3 administrative staff members, adequate material and technical conditions as well as special training of new staff. By the decision of the Republic Public Prosecutor of May 8, 2017 two deputy public prosecutors were appointed to the Special Prosecutor for High-tech Crime. At the moment, four deputy public prosecutors and a special prosecutor are working in this prosecution. When it comes to administrative staff by the internal reorganization of employees in the reporting period, two prosecutorial assistants were assigned to this prosecutor's office, and now there are five of them. Also, the remaining 3 positions for administrative staff (registrants) are expected to be filled in.

In terms of strengthening the technical capacities of the Special Prosecutor's Office for high-tech crime, the IPA 2017 project envisages procurement of equipment for the needs of the Special Prosecution Office and the Department of High-Tech Crime of the Ministry of Internal Affairs of RS.

When it comes to training of the staff of the Special Prosecution Offices and general prosecutor's offices for combating high-tech crimes, we underline that within the project *Improving Training for Judicial Authorities in the field of child protection against violence on the Internet*, which was financially supported by an international civil society organization Save the children, a plan and training program for judges and public prosecutors in the field of high-tech crime and protection of minors on the Internet was developed. Training in this field was included in the training program of the Judicial Academy, and since January 2017, their implementation started.

Also, within the aforementioned project **"A Guide for Judges and Prosecutors on the topic of high-tech crime and protection of minors in the Republic of Serbia**", was prepared. It contains clear guidelines for prosecutors and judges on acting in these cases, including first responding to electronic evidence, international standards in this field, domestic legal and institutional framework, as well as the protection of children in criminal proceedings.

Furthermore, Special Prosecutor for High-Tech Crime participated in drawing up the negotiating positions for Chapter 24. As for Chapter 7, the Special Prosecutor for High-Tech Crime is a member of the Negotiation Team so he had an active role in drawing up negotiating positions for the Intergovernmental conference on the accession of the Republic of Serbia to the European Union.

1.3.4 Implementation of the Council of Europe Convention on Cybercrime (ETS 185), with additional Protocol and review of current projects and programmes financed by the foreign aid for development assistance

As a representative of the Republic of Serbia, the Special Prosecutor for High-Tech Crime continued his participation in work of the **T-CY committee** of the Budapest Convention consisted of authorised representatives of the countries which ratified this Convention.

Additionally, the Special Prosecutor took part in the work of trans-border group of the T-CY Committee in preparation of updated guidelines for the implementation of the Convention, what provides a significant contribution to the development of international law in this area, bearing in mind that the area of cybercrime is regulated only by this Convention of the Council of Europe.

It is also important to emphasise that the Special Prosecutor participated in the work of the Group for cross-border crime of this Convention and in activities related to making further recommendations and guidelines for the implementation of the Convention, and in particular the development of the Second Additional Protocol to the Convention concerning international cooperation of the signatory countries.

Special Prosecutor's Office is involved in a joint project of the Council of Europe and the European Union's **Global Action on Cybercrime+ (GLACY+)**, which aims at comprehensive, planetary implementation of the Budapest Convention and at providing direct administrative and technical assistance to the countries that are covered by this project.

Special Public Prosecutor’s Office for High-Tech Crime continues its activities on implementing the project of the Council of Europe and the European Union **Cyber@OCTOPUS** in terms of participating in the conference activities and providing other assistance to the countries that are preparing implementation of the Budapest Convention and other related documents in the fields of interest for the Convention implementation, such data protection and protection of minors and children.

Besides the abovementioned activities, the Republic Public Prosecution and the Special Prosecution for High-Tech crime are involved in the **iPROCEEDS@IPA**, a joint project of the EU and the Council of Europe for South-Eastern Europe and Turkey. This project’s objective is to strengthen the capacity of authorities in charge for fight against cybercrime in the Republic of Serbia and the countries in the region to seize and confiscate cybercrime proceeds. Several expert missions, workshops and meetings were held within the project and a training plan was made which is already in its implementation phase.

1.3.5 Cooperation with other national and international state authorities and institutions

In relation to criminal prosecution of perpetrators of criminal offences of cybercrime, the Special Prosecutor’s Office cooperates mostly with the MOI’s department SBPOK – Department for Combating Cybercrime, and excellent cooperation has been established with the Department of Public Order of the Belgrade Police Directorate. Cooperation is on a high level and it starts at the beginning of work on particular cases, through consultations on the actions to be taken and by reporting to the Special Prosecutor's Office about the actions taken, discovered evidence and offenders, with the active participation

and presence of acting Deputy Public Prosecutor in undertaking procedural actions by the MOI during pre-investigation proceedings.

In relation to the possible "Darknet" and other peer to peer computer networks operations and cases, including overall actions taken within the field of combating cybercrime Department for Combating Cybercrime, together with Special Prosecutors Office for High-Tech crime, took active and crucial role in three largest international Law Enforcement actions in the fight against cybercrime in 2018, which marked the importance and necessity to suppress this criminal phenomenon. Actions are:

- Action "Shadow Web" - February 2018 - the take-over of one of the biggest criminal forums "In Fraud", dealing with stolen credit card information, one (1) suspected Serbian citizen was arrested and criminal report with charges was submitted.

- Action "Power Off" - April 2018 - the take-over of the largest criminal service for DDoS attacks in the world "Webstresser", two (2) suspected Serbian citizens were arrested and criminal reports with charges were submitted. In this action, Special Prosecution for Cybercrime commenced investigation against two suspects and what is more important, for the first time, from one of the suspects crypto currency was seized - 1.87465457 BTC.

- Action "The Dark Overlord" - May 2018. - Criminal group that stole personal data of citizens and blackmailed their owners.

Additionally, the Republic Public Prosecution and the Special Prosecution for the High-Tech crime have established cooperation with the Ministry of Trade, Tourism and Telecommunications regarding implementation of the Decree on the safety and protection of children in the use of information and communication technologies adopted by the Government of The Republic of Serbia in June 2016.

Also, cooperation with the Market Inspection in the work on combating the „grey economy" and criminal acts against intellectual property on the Internet is particularly significant.

1.5 Sri Lanka

Update by Sri Lanka on legislative and policy developments

- Enactment of the Mutual Assistance in Criminal Matter (Amendment) Act No. 24 of 2018.
- Approval and adoption of the National Cyber Security Strategy by the Cabinet of Ministers on 16th October 2018.