www.coe.int/cybercrime

Strasbourg, version 5 July 2019 T-CY (2019)23

Cybercrime Convention Committee (T-CY)

T-CY 21

21st Plenary Meeting of the Cybercrime Convention Committee

Item 8: 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 21st Plenary session on 8 July 2019.

Given that only limited time is available during the one-day plenary, delegations were invited to submit written updates under item 8 of the T-CY 21 Agenda to be published as part of the Plenary documentation.

By 5 July 2019, six Parties and one Observer organization, as well as the CoE Lanzarote Committee (T-ES) had provided such information.

The present document represents a compilation of the replies received.

Table of contents

1 Information received 4
1.1 Australia 4
1.2 Chile 6
1.3 Costa Rica 7
1.4 Czech Republic 7
1.5 France 7
1.6 Norway 8
1.7 Slovenia 10
1.8 ENISA 10
1.9 T-ES (Lanzarote Committee) 12

1 Information received

1.1 Australia

Detailed below are updates on some of Australia's recent domestic legislative reforms that target cybercrime.

Telecommunications and Other Legislation Amendment (Assistance and Access) Ac 2018 (Assistance and Access Act)

The Australian Government has passed legislation to equip Australia's law enforcement and national security agencies with the necessary tools to operate in, and adapt to, the evolving technological environment. The *Telecommunications and Other Legislation Amendment (Assistance and Access) Ac 2018* (Assistance and Access Act) passed the Australian parliament on 6 December 2018 and went into force on 9 December 2018. The Assistance and Access Act has been through a review by the Australian Commonwealth Parliamentary Joint Committee on Intelligence and Security, and is now subject to a further review by that parliamentary committee, and Australia's Independent National Security Legislation Monitor.

Changes in the technological environment, particularly ubiquitous encryption, present a significant obstacle to the lawful access of communications by Australia's law enforcement and security community. Ninety-five per cent of the communications of the Australian Security Intelligence Organisation's most dangerous counter-terrorism targets and 90 per cent of communications lawfully intercepted by the Australian Federal Police (AFP) are encrypted and unreadable.

The Australian Government supports the use of technologies, like encryption, which are critical to maintaining cybersecurity and securing devices and networks. However, technology and the communications environment are evolving at a rapid pace and the law, and the agencies it governs, must keep up. The Assistance and Access Act modernised the powers of Australia's law enforcement and security agencies in two distinct ways.

1) It established a technologically neutral industry assistance framework. The framework established a structure through which Australian agencies and the modern communications industry can work together to address technological obstacles to investigations into serious crimes and national security threats.
2) It enhanced investigatory and procedural powers to improve agencies' ability to search for, and collect, data. Today, most information is held in digital format and the Assistance and Access Act modernises the search warrant framework to account for this new reality.

The industry assistance framework establishes a clear structure for cooperative engagement between Australia's law enforcement and national security agencies, and the modern communications industry. Traditional Australian telecommunications providers have long had an obligation to provide reasonably necessary assistance to Australian authorities under section 313 of the *Telecommunications Act 1997* (Telecommunications Act). However, this regime does not recognise the growing role of new, innovative and global providers in the Australian communications supply chain. Increasingly, the communications services and devices used by Australians are being supplied by a wide range of providers both within and outside of Australia. The nature, operation and location of these services is a significant departure from the way communications have been delivered to Australia in the past. The Assistance and Access Act introduced new provisions into the Telecommunications Act as an evolution of the older regime in section 313. This responds to shifts in the Australian communications market and changes in technology.

The Assistance and Access Act introduced three new measures to facilitate this cooperative approach:

- Technical assistance requests (TARs) – ensures providers are immune to civil liability when voluntarily assisting agencies.
- Technical assistance notices (TANs) – establishes a legal obligation for assistance, where the assistance falls within a provider's existing business functions.
- Technical capability notices (TCNs) – allows Australia's first law-officer, the Attorney General, to require that a provider build a capability to assist law enforcement and national security agencies.

These measures do not replace the need for agencies to obtain a warrant or authorisation to intercept communications, conduct digital surveillance, or access data. Rather, the framework is designed to facilitate the use of these underlying powers and provide structure to law enforcement requests for industry help. All requests and notices provide civil immunity and limited criminal immunity. By default, providers are compensated for their efforts.

Keeping with the Australian Government's support for strong cyber-security, the Assistance and Access Act contains an express prohibition against building or implementing any weakness or vulnerability in software or physical devices that would jeopardise the security of innocent users. The Act makes clear that any assistance that makes a system's encryption or authentication less effective for general users is strictly prohibited. The construction of new decryption capabilities and requirements that would prevent a company from patching security flaws in their systems is also prohibited.

Enhanced investigatory and procedural powers round out the holistic approach to tackling the challenges of the modern technological environment. Modernised computer access warrants will give law enforcement greater ability to collect information at a point where it is not encrypted, ensuring agencies can view communications without compromising encryption technology, and limits interference with property and risk of harm to law enforcement. Improvements to search warrants allow law enforcement to collect and analyse evidence from devices remotely, and gives greater incentives for persons to give investigators access to devices when a lawful request is made.

The Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019

The Australian community continues to be concerned at the increasing use of the internet and social media by terrorists and violent extremists and interprets a need for immediate, effective measures to mitigate the dissemination of terrorist and violent extremist content.

The Christchurch terrorist attacks of 15 March 2019 demonstrated how live streaming could be abused by terrorists to amplify their messages in the immediate aftermath of terrorist attacks.

In response to the Christchurch terrorist attack, the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (the Abhorrent Violent Material Act), was enacted on 6 April 2019.

Broadly, the Abhorrent Violent Material Act created two new offences:

- Criminalising content services and content hosting platforms located anywhere in the world, as well as internet service providers in Australia, that do not notify the Australian Federal Police within a reasonable time of them becoming aware their service can be used to access abhorrent violent material, where the underlying conduct has occurred or is happening in Australia.

- Criminalising content services (including social media) and content hosting platforms that fail to remove abhorrent violent material expeditiously.

The scope of the offences are limited to very specific categories of the most violent audio-visual material produced by the perpetrator of the abhorrent violent conduct or their accomplice.

- It captures recording or streaming of actual acts of murder, rape, torture and terrorism involving physical harm and/or violent kidnapping.

In addition to the offences, Australia's e-Safety Commissioner has been empowered to issue notices that bring this type of material to the attention of social media companies.
As soon as a social media company receives a notice, they will be deemed to be aware of the material, meaning the clock starts ticking for the platform to remove the material or face serious criminal penalties.

1.2 Chile

After Chile joined the Budapest Convention on August 2017, a series of measures have been adopted. Since the last T-CY held in November 2018, where Chile shared its latest developments, Chile had the following events and outcomes:

- The draft bill that adapts our cybercrime national legislation to the Budapest Convention standards in terms of substantive and procedural law it is still being discussed before our Congress. The Public Prosecutor's Office has been actively participating in the ongoing discussion of the bill, together with the Ministry of Interior and national experts. We foresee that this draft bill could be approved during the year 2020 an important step forward in the prosecution of new kinds of cybercrime offences, as well as providing procedural tools for law enforcement agencies, since it includes the possibility to use a series of special investigative techniques.

- On June 25th and 26th, Chile hosted the second meeting of *CiberRed,* a network of Ibero-American prosecutors specialized on cybercrime, which is coordinated by the Portuguese Prosecution Service with the support of Glacy+, the Council of Europe and the European Union. *CiberRed* is composed by 19 countries that are part of the Ibero-American Association of Public Prosecutors (AIAMP). During this year's meeting participants shared common problems encountered in cybercrime investigations and discussed about the necessity of having a national legislation that matches international standards in order to allow international cooperation.

- In terms of capacity building, Chile has completed the basic and advanced training for Judges and Prosecutors of the Glacy+ project. Last April in Santiago Chile received experts from the Council of Europe who provided advance training in completion of the Judicial Course, which aims to prepare national trainers that can share the knowledge acquired with their peers. Also, as part of the Glacy+ project, Chilean law enforcement agents have been invited to attend a high number of courses and other activities held in other countries.

- Chile has continued to have an active participation in the Drafting Group of the Second Protocol of the Budapest Convention.

Chile's authorities have made cybercrime a priority matter which we believe will lead to the modernization of our domestic law and politics, as well as the aiming for more capacity building.

1.3 Costa Rica

For more details, please see "Update from Costa Rica on key developments" (*in Spanish only*), as well as its Annexes (*in Spanish only*).

1.4 Czech Republic

The Czech Republic has adopted a new legal regulation in Criminal Procedure Code laying down explicit rules for an expedited preservation of stored computer data in national cases and thus implementing more effectively the requirements of Article 16 of the Budapest Convention. Accordingly, Act on International Judicial Cooperation in Criminal Matters newly comprises the rules for preservation of data in transnational cases, thus meeting better the requirements of Article 29 of the Budapest Convention. These amendments are in effect since 1 February 2019.

Proposal for withdrawal of a reservation made by the Czech Republic pursuant Article 29 paragraph 4 of the Budapest Convention (requirement of dual criminality in relation to the request of another state for expedited preservation of stored computer data) has been approved by the Senate on 19 June 2018 and by the Chamber of Deputies on 18 April 2019. President of the State has signed the proposal on 3 July 2019. Now the confirmation of the Secretary General of the Council of Europe on depositing the instrument and the subsequent publication in the Czech Collection of International Treaties is pending.

1.5 France

(in French only)

1.5.1. Evolutions législatives

La France a connu courant 2018 et au premier semestre 2019, plusieurs initiatives législatives fortes permettant de renforcer la lutte contre la cybercriminalité :

- une proposition de loi visant à lutter contre la haine sur internet déposée le 20 mars 2019, qui prévoit notamment un retrait ou une inaccessibilité du contenu haineux en ligne dans un délai maximal de 24 heures, ainsi qu'un régime de responsabilité administrative applicable aux opérateurs de plateformes à fort trafic. Son examen devant le Parlement a commencé début juillet ;
- un paquet législatif (une loi ordinaire n° 2018-1202 du 22 décembre 2018 et une loi organique) relatif à la lutte contre la manipulation de l'information en période électorale, qui vise à permettre à un candidat ou parti politique de saisir le juge des référés pour faire cesser la diffusion délibérée, artificielle ou automatisée et massive par le biais d'un service de communication au public en ligne, de fausses informations en période électorale ; cette innovation n'est pas essentiellement de nature pénale mais pénalise le non-respect d'un certain nombre de règles permettant de garantir la transparence des opérateurs de plateforme en ligne sur leurs sources de financement ; il permettra ainsi de lutter efficacement contre la désinformation en ligne en période électorale.

1.5.2. Innovation opérationnelle

Elle a par ailleurs mis en œuvre une innovation opérationnelle très pratique à la suite de la constitution d'un groupe de travail sous l'égide du ministère de la justice : la publication d'un guide méthodologique du recueil de la preuve numérique en matière pénale.

L'importance du respect de la vie privée, notamment dans le cadre du secret des communications a conduit les industriels à offrir des outils numériques garantissant la confidentialité du contenu des échanges de bout en bout. Confrontés à ce phénomène, les services enquêteurs et les experts doivent disposer de moyens juridiques et techniques adaptés. En outre, la question de la souveraineté numérique se révèle fondamentale, et ce tout particulièrement en matière de terrorisme et de crimes commis en bande organisée où les investigations sont la plupart du temps transfrontalières.

Or les dispositions concernant le recueil de la preuve numérique apparaissent complexes à interpréter et à articuler entre elles. La pluralité des cadres juridiques applicables et la variété des technologies de l'information et de la communication militent en faveur d'une meilleure maîtrise juridique et technique des méthodes de recueil de la preuve numérique et d'exploitation des matériels informatiques.

C'est la raison pour laquelle la direction des affaires criminelles et des grâces du ministère de la Justice a souhaité la création d'un groupe de travail spécifique consacré au recueil de la preuve numérique. Son objectif était de clarifier l'interprétation des dispositions existantes et diffuser de bonnes pratiques. Installé en mai 2018, il a associé les représentants de l'ensemble des services d'enquête concernés (police, gendarmerie et douanes), ainsi que de l'autorité judiciaire (membres du ministère public et juges) et a procédé à de nombreuses consultations et visites sur sites.

Après un an de travaux, il a établi un rapport le 12 avril 2019 sous la forme d'un guide méthodologique diffusé aux magistrats et services de sécurité intérieure et de douanes.

1.5.3. Actions de coopération international

Dans le cadre de ses activités internationales de renforcement de compétentes, la police judiciaire française a contribué à plusieurs missions du Conseil de l'Europe au Maroc, en Turquie et en Côte d'Ivoire notamment, en fournissant une expertise sur les questions de coopération opérationnelle (POC 24/7) et sur les questions de traitement des signalements en ligne par une plateforme centrale, en appui à l'extension de la Convention de Budapest.

1.6 Norway

On March 28, 2019, the Norwegian Supreme Court made a decision regarding access to electronic evidence stored on cloud services. The case in question was a criminal investigation, and one key issue was jurisdiction.

Summary

In connection with an investigation of possible computer fraud, the prosecution authority had requested a warrant to conduct a search at a company that was not itself a suspect, see section 192 (3) of the Criminal Procedure Act, to access information stored by this company on servers abroad, and that was assumed to shed light on the possible fraud. The Supreme Court, having conducted an oral hearing, concluded that under Norwegian internal law, there was nothing that prevented the search from being conducted. Nor were there treaty provisions or any custom under international law preventing it.

A search in a case like this would also not entail any violation of other states' exclusive enforcement jurisdiction. In this regard, it was emphasised that the coercive measure had been commenced on

Norwegian soil, and that the relevant data had been made available by a coercive measure against a Norwegian company with offices in Norway. The decision was made by Norwegian courts while maintaining general rule of law guarantees. The search would only give access to data that the company itself had stored, and that the company could freely retrieve from the storage place abroad. The data also remains on the foreign server, and no changes are made to the information. The court of appeal dismissed the company's appeal against the district court's order to allow the search. The appeal against the court of appeal's order was dismissed.

The Supreme Court referred to the Budapest Convention:

> (36) The Convention imposes the states to adopt any measures necessary to combat cybercrime. For instance, Article 18 sets out that each state must ensure the same access as that established in Norwegian law under section 199 a of the Criminal Procedure Act. Articles 29 et seq. contain provisions relating to mutual assistance. However, the Convention only establishes minimum obligations for the states, see Norwegian Official Report 2007: 2 Legislative measures to combat cybercrime, page 47. As none of the articles directly deals with a measure like that in the case at hand, I will not address this Convention any further.
> (37) Nor are there other treaty provisions specifically preventing the relevant type of search. In fact, no legal basis is established under any treaty for conducting a search in a case like the one we are dealing with.
> (…)
> (52) As for other European countries, I confine myself to referring to case law reviews by expert groups of the Council of Europe in 2012 and 2016, and a working group under the EU Commission in 2018.
> (53) The result of the review of the expert group of the Council of Europe in 2012 is thoroughly presented in Swedish Official Report 2017: 89 on pages 469 et seq. This presentation shows that it is not unusual that the state deems itself entitled to conduct a search like that in the case at hand, also if it is clear that the data is stored on a foreign server. Another expert group of the Council of Europe submitted a report on 16 September 2016 titled "Criminal justice access to electronic evidence in the cloud …". As regards practice, the following is stated on page 16 in paragraph 45:
> **"It seems to be widespread practice that law enforcement in a specific criminal investigation access data not only on the device of the suspect but also on connected devices such as email or other cloud service accounts if the device is open or the access credentials have been obtained lawfully even if they know that they are connecting to a different, known country."**
> (54) The inquiry carried out by the EU group leaves the same impression. The following is stated on page 11 of the report called SWD (2018) 112, dated 17 April 2018:
>
> **"The national law in at least 20 Member States empowers authorities, subject to judicial authorisation, to seize and search a device and remotely stored data accessible from it ..."**

From the conclusion in the Supreme Court decision:

> (65) The court of appeal emphasised that the coercive measure – the decision to conduct a search in Tidal's data and the order to give access to the company's computer system – is initiated on Norwegian soil, at Tidal's office in Oslo.
> (66) As the proceedings have demonstrated, the decision to allow a search is made by Norwegian courts while maintaining general rule of law guarantees.

(67) Also, it is clear that the data is made available through a coercive measure against a Norwegian company with an office in Norway, which means that Norwegian authorities are not, on their own, intruding into data stored abroad.

(68) In this respect, I add that it is clear that Norwegian authorities have enforcement jurisdiction over the Norwegian company and its employees present in this country. On these grounds, Norwegian authorities may order the company and these persons to provide the information necessary for Norwegian authorities to access the data. On a national level, the legal basis in this regard is section 1999 a of the Criminal Procedure Act. The relevant search was carried out by using the access credentials the company had given to Økokrim.
(69) The court of appeal's ruling sets out that the search only involves access to information the company itself has stored. And the company is at any time free to retrieve the data from the foreign storage place.

(70) Finally, it is clear that the data remains on the server abroad. Also, no changes are made to the stored information, for instance in the form of deletion of encryption. A possible seizure is carried out by copying the data onto storage media in Norway.
(71) At any rate, in a situation is like the one at hand, I cannot see that the search will affect another state to an extent that it constitutes a violation of the principle of sovereignty.
(72) Consequently, the court of appeal has correctly applied the relevant legal standards, and the appeal should be dismissed.

(73) I add that questions with regard to limitations to the possibility to seize information found in the search – here as in other situations – must be decided under the relevant rules in the Criminal Procedure Act, in particular section 204 that deals with the protection of lawyer-client correspondence and trade secrets. Any dispute concerning the access to evidence may be brought before the court as usual, see section 205 subsections 2 and 3 and section 208. Also, submissions that a seizure will result in a violation of the defendant's rights – for instance under the Norwegian Constitution and ECHR on the right to privacy and the right to a fair trial – may be legally tried in this manner.

For more details, please see official English translation of the court decision.

1.7 Slovenia

Update by Slovenia on legislative developments

In 2019 the new Criminal procedure act was implemented in Slovenia. This amendment introduces implementation of article 29 Expedited preservation of stored computer data of the Budapest Convention on Cybercrime, transposed into art 149. e) of Criminal procedure act of Slovenia.

1.8 ENISA

ENISA update on CISRT-LE Cooperation in the EU

In 2019, ENISA continues supporting the cooperation between CSIRTs and law enforcement agencies while seeking to extend its activities to aspects of cooperation with the judiciary as appropriate. This line of policy

support work underpins EU efforts on the fight against cybercrime and stems from a collaboration framework with EU stakeholders, notably, EUROPOL/EC3, CERT-EU and EUROJUST, to a certain extent; clearly, the goal of this collaboration also includes select stakeholders at Member States level.

1.8.1. Roadmap of further activities on csirt and le cooperation

In 2019, ENISA collected input from key stakeholders and prepared a roadmap to further enhance cooperation between the CSIRTs and the law enforcement agencies along with their interaction with the judiciary. The roadmap will not necessarily be made public; it is likely to be distributed instead to select stakeholders within the EU Institutions and Bodies, as well as Member States agencies.

The aim of this roadmap is to collect input, analyse and draw up main directions for further cooperation initiatives and directions for policy initiatives. ENISA is preparing this roadmap as a continuation of previous years' work, that include the 7th ENISA/EC3 workshop and the following reports:

- Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects (2017), https://www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement
- Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement (2017), https://www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement
- Cooperation between CSIRTs and law enforcement: interaction with the judiciary (2018), https://www.enisa.europa.eu/publications/csirts-le-cooperation/
- Review of Behavioural Sciences Research in the Field of Cybersecurity (2018), https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/

When CSIRTs, law enforcement agencies and the judiciary cooperate, they face challenges that have been categorized across technical, legal, organizational and cultural strands. Understanding these challenges is essential in an effort to tackle them, further enhance the cooperation and better organise the response in the fight against cybercrime. In this roadmap, technical, legal, organizational and cultural aspects of this cooperation will be presented. ENISA has collected input from representatives of Member States' and EU institutions and Bodies by means of desk research (subject-matter expert interviews) and an online survey.

Figure 1: Data collection

Data Collection	
Subject matter expert interviews	**Online Survey**
31 interviews	33 replies
▪ 21 Members States	▪ 21 Members States
▪ 2 EFTA countries	▪ 3 EFTA countries

1.8.2. Training material

A key recommendation in the 2018 ENISA report was that ENISA, EC3, Eurojust and CEPOL (need) to facilitate joint trainings across the three communities on aspects of their cooperation. As a result, four hands-on training tracks on the area of CSIRT-LE cooperation have also been included in the agenda of the

7th ENISA/EC3 Workshop. The feedback received by the participants was very positive, as they had highlighted the need for less policy discussion and more trainings. More hands-on training tracks are due for delivery in this year's workshop.

In 2019, ENISA took the initiative to develop training material focusing on the cooperation across the CSIRTs, law enforcement and the judiciary. The aim is to appeal to these communities with training themes of shared interest and act as a conduit and bring them together, in an effort to bridge gaps. In 2018 and 2019, ENISA also responded to topical training requests from CEPOL.

1.8.3. Annual ENISA EC3 workshop

The 8th ENISA/EC3 Workshop will retain the scope of cooperation between national/governmental CSIRTs in Europe and their national Law Enforcement counterparts, aspects of the cooperation with judiciary authorities will also be discussed. This event will be co-organised with EC3 (EUROPOL).

1.8.4. Report on tools for enhancing cooperation between CSIRTS and LE

In 2019, ENISA is also planning for a concise report on tools that CSIRTs, law enforcement and the judiciary need in order to cooperate throughout the cybercrime investigation lifecycle. The perceived outcome of this report will be to bridge some of the cooperation gaps that have been identified over time and assess the launching of new policy initiatives. A recommendation of the 2018 ENISA report was that CSIRTs, law enforcement agencies and the judiciary need to use common tools to facilitate cooperation and interaction. The existence of a common platform where the three communities can share information about threats and those involved in threats, cybersecurity incidents, cyber-attacks and associated tactics, techniques and procedures (TTPs) seems to be of great importance. This need has also been highlighted in the 2019 survey results.

This report seeks to identify key functionalities and weaknesses concerning tools used across the three reference communities and gaps needed to be filled to facilitate cooperation and interaction. Possible recommendations of this work may include a proposal with technical specifications for designing a common platform that will be accessible by these three communities and proposed policy directions.

ENISA is likely to collect input from designated stakeholders representing Member States' CSIRT/LE/Judiciary communities as well as EU institutions and Bodies.

1.9 The CoE Lanzarote Committee (the Committee of the Parties to the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, T-ES)

According to point 2.2.1 of the list of decisions of the Lanzarote Committee's 24th meeting:

The Lanzarote Committee adopted on its 24th meeting an Opinion on child sexually suggestive or explicit images and/or videos generated, shared and received by children, highlighting in particular that:

- Children are increasingly generating and sharing sexually suggestive or explicit images and/or videos of themselves placing themselves at risk of harm as these images and/or videos are easily targeted and exploited by sexual offenders;

- The Lanzarote Committee does not endorse children's exploring and expressing their sexuality by sharing self-generated sexually suggestive or explicit images and/or videos;

- It is however determined to ensure that the best interests of the child be a primary consideration in all decisions concerning child self-generated sexually suggestive or explicit images and/or videos;

- It therefore sets out in its opinion guidance to support Parties in identifying situations when:
  1) children should be addressed to victim support and not subject to criminal prosecution;
  2) children's conduct does not amount to the "production, possession, offering or making available, distributing or transmitting, procuring, or knowingly obtaining access to child pornography";
  3) children's harmful behaviour calls for criminal prosecution as a last resort only.