

T-CY
CYBERCRIME CONVENTION COMMITTEE
COMITÉ DE LA CONVENTION CYBERCRIMINALITÉ

T-CY(2013)29rev

Strasbourg, France
8 July 2019

# T-CY GUIDANCE NOTES

**Adopted by the 8th, 9th, 12th, 16th and 21st Plenary of the T-CY**

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

**www.coe.int/cybercrime**

## About Guidance Notes

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[1]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[2] This is to ensure that new forms of malware or crime would always be covered by the Convention.

**Contact**


Alexander Seger
Secretary of the Cybercrime Convention Committee (T-CY)
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email: alexander.seger@coe.int


[1] See the mandate of the T-CY (Article 46 Budapest Convention).

[2] Paragraph 36 of the Explanatory Report

# Contents

1 Guidance Note on the notion of "computer system" ..... 4

2 Guidance Note on provisions of the Budapest Convention covering botnets ..... 6

3 Guidance Note on Transborder access to data (Article 32) ..... 9

4 Guidance Note on identity theft and phishing in relation to fraud ..... 14

5 Guidance Note on DDOS attacks ..... 18

6 Guidance Note on critical information infrastructure attacks ..... 20

7 Guidance Note on new forms of Malware ..... 22

8 Guidance Note on Spam ..... 24

9 Guidance Note on Production orders for subscriber information (Article 18 Budapest Convention) ..... 26

10 Guidance Note on Terrorism ..... 33

11 Guidance Note on Aspects of election interference by means of computer systems covered by the Budapest Convention ..... 36

# 1 Guidance Note on the notion of "computer system"[3]

## Introduction

The T-CY at its 1st meeting (Strasbourg, 20-21 March 2006) discussed the scope of the definition of "computer system" in Article 1.a Budapest Convention in the light of developing forms of technology that go beyond traditional mainframe or desktop computer systems.

Since the time of the drafting of the Convention new devices were developed such as modern generation mobile phones or "smart" phones, PDAs, tablets, and others that produce, process or transmit data. There has thus been a need to discuss whether these new devices are included in the concept of "computer system" of the Budapest Convention.

T-CY, in 2006, agreed that these devices were covered by the definition of "computer system" of Article 1.a.

The present Guidance Note states this common understanding of the Parties as reflected in the report of the 1st meeting (document T-CY(2006)11).

## Article 1.a. Budapest Convention on Cybercrime (ETS 185)

Text of the Convention

> **Article 1 – Definitions**
>
> For the purposes of this Convention:
>
> a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

Extract of the Explanatory Report

> 23. A computer system under the Convention is a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities. It may stand alone or be connected in a network with other similar devices "Automatic" means without direct human intervention, "processing of data" means that data in the computer system is operated by executing a computer program. A "computer program" is a set of instructions that can be executed by the computer to achieve the intended result. A computer can run different programs. A computer system usually consists of different devices, to be distinguished as the processor or central processing unit, and peripherals. A "peripheral" is a device that performs certain specific functions in interaction with the processing unit, such as a printer, video screen, CD reader/writer or other storage device.
>
> 24. A network is an interconnection between two or more computer systems. The connections may be earthbound (e.g., wire or cable), wireless (e.g., radio, infrared, or satellite), or both. A network may be geographically limited to a small area (local area networks) or may span a large area (wide area networks), and such networks may themselves be interconnected. The Internet is a global network consisting of many interconnected networks, all using the same protocols. Other types of networks exist, whether or not connected to the Internet, able to communicate computer data among computer systems. Computer systems may be connected to the network as endpoints or as a

[3] adopted by the T-CY at its 8th Plenary

means to assist in communication on the network. What is essential is that data is exchanged over the network.

## T-CY statement on the notion of "computer system" (Article 1.a. Budapest Convention)

Article 1.a of the Convention defines "computer system" as any "device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data".

The T-CY agrees that this definition includes, for example, modern mobile telephones which are multifunctional and have among their functions the capacity to produce, process and transmit data, such as accessing the Internet, sending e-mail, transmitting attachments, upload contents or downloading documents.

Similarly the T-CY recognises that personal digital assistants, with or without wireless functionality, also produce, process and transmit data.

The T-CY underlines that, when these devices perform such functions, they are processing "computer data" as defined by Article 1.b. Furthermore, the T-CY considers that when they perform these functions they create "traffic data" as defined by Article 1.d.

Therefore, in processing such data, they are acting as a "computer system" as defined in Article 1.a.

The T-CY agrees that this is consistent with the interpretation of "computer system" set forth in the Convention's Explanatory Report and that the Convention is intended to cover these devices in that capacity.

## Conclusion

T-CY agrees that the definition of "computer system" in Article 1.a covers developing forms of technology that go beyond traditional mainframe or desktop computer systems, such as modern mobile phones, smart phones, PDAs, tablets or similar.

## 2 Guidance Note on provisions of the Budapest Convention covering botnets[4]

### Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[5]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of botnets.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[6] This is to ensure that new forms of malware or crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to botnets.

### Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

The term 'botnet' may be understood to indicate:

> "a network of computers that have been infected by malicious software (computer virus). Such a network of compromised computers ('zombies') may be activated to perform specific actions, such as attacking information systems (cyber attacks). These 'zombies' can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This 'controlling' computer is also known as the 'command-and-control centre'".[7]

Computers may be linked for criminal or good purposes.[8] Therefore, the fact that botnets consist of computers that are linked is not relevant. The relevant factors are that the computers in botnets are used without consent and are used for criminal purposes and to cause major impact.

Botnets are covered by the following sections of the convention, depending on what each botnet actually does. Each provision contains an intent standard ("without right", "with intent to defraud" etc.) which should be readily provable when botnets are involved.

| **Relevant Articles** | **Examples** |
|---|---|
| Article 2 – Illegal access | The creation and operation of a botnet requires illegal access to computer systems.[9]<br>Botnets may be used to illegally access other computer systems. |
| Article 3 – Illegal interception | Botnets may use technical means to intercept non-public transmissions of computer data to, from, or within a computer system. |

[4] Adopted by the 9th Plenary of the T-CY (4-5 June 2013)

[5] See the mandate of the T-CY (Article 46 Budapest Convention).

[6] Paragraph 36 of the Explanatory Report

[7] Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (com (2010) 517 final)

[8] Networks of computers may be created voluntarily for a criminal purpose. The crimes committed by such networks are covered by the Convention but are not discussed in this Note.

[9] See also Guidance Note 1 on the Notion of „Computer System"

| | |
|---|---|
| Article 4 – Data interference | The creation of a botnet always alters and may damage, delete, deteriorate or suppress computer data.<br>Botnets themselves damage, delete, deteriorate, alter or suppress computer data. |
| Article 5 – System interference | Botnets may hinder the functioning of a computer system. This includes distributed denial of service attacks.[10] |
| Article 6 – Misuse of devices | All botnets are devices as defined in Article 6 because they are designed or adapted primarily to commit the offences established by Articles 2 through 5.[11]<br>Programmes themselves that are used for the creation and operation of botnets also fall under Article 6.<br>Therefore, Article 6 criminalizes the production, sale, procurement for use, import, distribution or otherwise making available as well as the possession of devices such as botnets or programmes used for their creation or operation. |
| Article7 – Computer-related forgery | Depending on the botnet's design, it may input, alter, delete, or suppress computer data with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic. |
| Article 8 – Computer-related fraud | Botnets may cause one person to lose property and cause another person to obtain an economic benefit from the inputting, altering, deleting, or suppressing of computer data and/or interfering with the function of a computer system. |
| Article 9 – Child pornography | Botnets may distribute child exploitation materials. |
| Article 10 – Infringements related to copyrights and related rights | Botnets may illegally distribute data that is protected by intellectual property laws. |
| Article 11 – Attempt, aiding and abetting | Botnets may be used to attempt or to aid or abet several crimes specified in the treaty. |
| Article 13 – Sanctions | Botnets serve multiple criminal purposes some of which have serious impact on individuals, on public or private sector institutions or on critical infrastructure.<br><br>A Party may foresee, however, in its domestic law a sanction that is unsuitably lenient for botnet-related crime, and it may not permit the consideration of aggravated circumstances, attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law.<br><br>Therefore, Parties should ensure, pursuant to Article 13, that criminal |

[10] See separate Guidance Note.

[11] Parties that take reservations to Article 6 must still criminalize the sale, distribution or making available of devices covered by this Article.

| | |
|---|---|
| | offences related to botnets "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions.<br><br>Parties may also consider aggravating circumstances, for example, if botnets affect a significant number of systems or attacks causing considerable damage, including deaths or physical injuries, or damage to critical infrastructure. |

## T-CY statement

The above list of Articles related to botnets illustrates the multi-functional criminal use of botnets and criminal provisions that may apply.

Therefore, the T-CY agrees that the different aspects of botnets are covered by the Budapest Convention.

# 3 Guidance Note on Transborder access to data (Article 32)[12]

## Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[13]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of transborder access to data under Article 32 Budapest Convention.[14]

Article 32b is an exception to the principle of territoriality and permits unilateral transborder access without the need for mutual assistance under limited circumstances. Parties are encouraged to make more effective use of all the international cooperation provisions of the Budapest Convention, including mutual assistance.

Overall, practices, procedures as well as conditions and safeguards vary considerably between different Parties. Concerns regarding procedural rights of suspects, privacy and the protection of personal data, the legal basis for access to data stored in foreign jurisdictions or "in the cloud" as well as national sovereignty persist and need to be addressed.

This Guidance Note is to facilitate implementation of the Budapest Convention by the Parties, to correct misunderstandings regarding transborder access under this treaty and to reassure third parties.

The Guidance Note will thus help Parties to take full advantage of the potential of the treaty with respect to transborder access to data.

## Article 32 Budapest Convention

Text of the provision:

> Article 32 – Trans-border access to stored computer data with consent or where publicly available
>
> A Party may, without the authorisation of another Party:
>
> a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
>
> b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

[12] Adopted by the 12th Plenary of the T-CY (2-3 December 2014)

[13] See the mandate of the T-CY (Article 46 Budapest Convention).

[14] The preparation of this Guidance Note represents follow up to the findings of the report on "Transborder access and jurisdiction" (T-CY(2012)3) adopted by the T-CY Plenary in December 2012. http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

Extract of the Explanatory Report:

> 293. The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorised, nor precluded.
>
> 294. Article 32 (Trans-border access to stored computer data with consent or where publicly available) addresses two situations: first, where the data being accessed is publicly available, and second, where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system. Who is a person that is "lawfully authorised" to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.

## T-CY interpretation of Article 32 Budapest Convention

With regard to Article 32a (transborder access to publicly available (open source) stored computer data) no specific issues have been raised and no further guidance by the T-CY is required at this point.

It is commonly understood that law enforcement officials may access any data that the public may access, and for this purpose subscribe to or register for services available to the public.[15]

If a portion of a public website, service or similar is closed to the public, then it is not considered publicly available in the meaning of Article 32a.

Regarding Article 32b, typical situations may include:

- A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.[16]

- A suspected drug trafficker is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another Party, police may access the data under Article 32b.

[15] Domestic law, however, may limit law enforcement access to or use of publicly available data.

[16] Paragraph 294 Explanatory Report.

Other situations are neither authorised nor precluded.[17]

With regard to Article 32b (transborder access with consent) the T-CY shares the following common understanding:

**General considerations and safeguards**

Article 32b is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14.[18]

As pointed out above, it is presumed that the Parties to the Convention form a community of trust and that rule of law and human rights principles are respected in line with Article 15 Budapest Convention.[19]

---

[17] Paragraph 293 Explanatory Report. See also Article 39.3 Budapest Convention.

[18] Article 14 – Scope of procedural provisions
1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
b other criminal offences committed by means of a computer system; and
c the collection of evidence in electronic form of a criminal offence.
3 a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
i is being operated for the benefit of a closed group of users, and
ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

[19] Article 15 – Conditions and safeguards
1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

The rights of individuals and the interests of third parties are to be taken into account when applying the measure.
Therefore, a searching Party may consider notifying relevant authorities of the searched Party.

**On the notion of "transborder" and "location"**

Transborder access means to "unilaterally access computer data stored in another Party without seeking mutual assistance".[20]

The measure can be applied between the Parties.

Article 32b refers to "stored computer data located in another Party". This implies that Article 32b may be made use of if it is known where the data are located.

Article 32b would not cover situations where the data are not stored in another Party or where it is uncertain where the data are located. A party may not use article 32b to obtain disclosure of data that is stored domestically.

Article 32b "neither authorise[s], nor preclude[s]" other situations. Thus, in situations where it is unknown whether, or not certain that, data are stored in another Party, Parties may need to evaluate themselves the legitimacy of a search or other type of access in the light of domestic law, relevant international law principles or considerations of international relations.

**On the notion of "access without the authorisation of another Party"**

Article 32b does not require mutual assistance, and the Budapest Convention does not require a notification of the other Party. At the same time, the Budapest Convention does not exclude notification. Parties may notify the other Party if they deem it appropriate.

**On the notion of "consent"**

Article 32b stipulates that consent must be lawful and voluntary which means that the person providing access or agreeing to disclose data may not be forced or deceived.[21]

Subject to domestic legislation, a minor may not be able to give consent, or persons because of mental or other conditions may also not be able to consent.

In most Parties, cooperation in a criminal investigation would require explicit consent. For example, general agreement by a person to terms and conditions of an online service used might not constitute explicit consent even if these terms and conditions indicate that data may be shared with criminal justice authorities in cases of abuse.

**On the applicable law**

In all cases, law enforcement authorities must apply the same legal standards under Article 32b as they would domestically. If access or disclosure would not be permitted domestically it would also not be permitted under Article 32b.

[20] Paragraph 293 Explanatory Report to the Budapest Convention.

[21] In some countries, consenting to avoid or reduce criminal charges or a prison sentence also constitutes lawful and voluntary consent.

It is presumed that the Parties to the Convention form a community of trust and that rule of law and human rights principles are respected in line with Article 15 Budapest Convention.

**On the person who can provide access or disclose data**

As to "who" is the person who is "lawfully authorised" to disclose the data, this may vary depending on the circumstances, laws and regulations applicable.

For example, it may be a physical individual person, providing access to his email account or other data that he stored abroad.[22]

It may also be a legal person.

Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their users' data under Article 32. Normally, service providers will only be holders of such data; they will not control or own the data, and they will, therefore, not be in a position validly to consent. Of course, law enforcement agencies may be able to procure data transnationally by other methods, such as mutual legal assistance or procedures for emergency situations.

**Domestic lawful requests versus Article 32b**

Article 32b is not relevant to domestic production orders or similar lawful requests internal to a Party.

**On the location of the person consenting to provide access or disclose data**

The standard hypothesis is that the person providing access is physically located in the territory of the requesting Party.

However, multiple situations are possible. It is conceivable that the physical or legal person is located in the territory of the requesting law enforcement authority when agreeing to disclose or actually providing access, or only when agreeing to disclose but not when providing access, or the person is located in the country where the data is stored when agreeing to disclose and/or providing access. The person may also be physically located in a third country when agreeing to cooperate or when actually providing access. If the person is a legal person (such as a private sector entity), this person may be represented in the territory of the requesting law enforcement authority, the territory hosting the data or even a third country at the same time.

It should be taken into account that many Parties would object – and some even consider it a criminal offence – if a person who is physically in their territory is directly approached by foreign law enforcement authorities who seek his or her cooperation.

## T-CY Statement

The T-CY agrees that the above represents the common understanding of the Parties as to the scope and elements of Article 32.

[22] See the example given in Paragraph 294 Explanatory Report.

# 4 Guidance Note on identity theft and phishing in relation to fraud[23]

## Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[24]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of identity theft and phishing and similar acts[25] in relation to fraud.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[26] This is to ensure that new forms of crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to identity theft in relation to fraud and involving computer systems.

## Identity theft and phishing

While there is no generally accepted definition nor consistent use of the term, identity theft commonly involves criminal acts of fraudulently (without his or her knowledge or consent) obtaining and using another person's identity information. The term "identity fraud" is sometimes used as a synonym, although it also encompasses the use of a false, not necessarily real, identity.

While personally identifiable information of a real or fictitious person may be misused for a range of illegal acts, the present Guidance Note focuses on identity theft in relation to fraud only.

This may entail the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent. These identity details are then used to obtain goods and services in that person's name.

Related acts may include "phishing", "pharming", "spear phishing", "spoofing" or similar conduct, for example, to obtain password or other access credentials, often through email or fake websites.

Identity theft affects governments, businesses and citizens and causes major damage. It undermines confidence and trust in information technologies.

In many legal systems there is no specific offence of identity theft. Perpetrators of identity theft are normally charged with more serious offences (e.g. financial fraud). Obtaining a false identity normally implies a crime, such as the forgery of documents or the alteration of computer data. A false identity facilitates many crimes, including illegal immigration, trafficking in human beings, money laundering, drug trafficking, financial fraud against governments and the private sector, but is most generally seen in conjunction with fraud.

---

[23] Adopted by the 9th Plenary of the T-CY (4-5 June 2013)

[24] See the mandate of the T-CY (Article 46 Budapest Convention).

[25] Similar acts to phishing are known under various names such as spear phishing, SMiShing, pharming and vishing.

[26] Paragraph 36 of the Explanatory Report

Conceptually, ID theft can be separated into three distinct phases:

- Phase 1 – The obtaining of identity information, for example, through physical theft, through search engines, insider attacks, attacks from outside (illegal access to computer systems, Trojans, keyloggers, spyware and other malware) or through the use of phishing and or other social engineering techniques.
- Phase 2 – The possession and disposal of identity information, which includes the sale of such information to third parties.
- Phase 3 – The use of the identity information to commit fraud or other crimes, for example by assuming another's identity to exploit bank accounts and credit cards, create new accounts, take out loans and credit, order goods and services or disseminate malware.

In conclusion: identity theft (including phishing and similar conduct) is generally used for the preparation of further criminal acts such as computer related fraud. Even if identity theft is not criminalised as a separate act, law enforcement agencies will be able to prosecute the subsequent offences.

## T-CY interpretation of the criminalisation of identity theft in relation to fraud under the Budapest Convention

The Budapest Convention is focusing on criminal conduct and not specifically on techniques or technologies used. It does, therefore, not contain specific provisions on identity theft or phishing. However, full implementation of the Convention's substantive law provisions will allow States to criminalise conduct related to identity theft.

The Convention requires countries to criminalise conduct such as the illegal access to a computer system, the illegal interception of data, data interference, system interference, the misuse of devices and computer related fraud:

| **Phase** | **Article of convention** | **Examples** |
|---|---|---|
| Phase 1 – Obtaining of identity information | Article 2 – Illegal access | While a criminal is "hacking", circumventing password protection, keylogging or exploiting software loopholes, the computer may be illegally accessed in the acts of ID theft/phishing.<br><br>Illegal access to computer systems is one of the most common offences committed in order to obtain sensitive information such as identity information. |
| | Article 3 illegal interception | ID theft often entails the use of keyloggers or other types of malware for the illegal interception of non-public transmissions of computer data to, from or within a computer system containing sensitive information such as identity information. |
| | Article 4 – Data interference | ID theft/phishing may involve damaging, deleting, deteriorating, altering or suppressing computer data.<br><br>This is often done during the process of obtaining illegal access by installing a keylogger to obtain sensitive information. |

| | | |
|---|---|---|
| | Article 5 – System interference | ID theft/phishing may involve hindering the functioning of a computer system in order to steal or facilitate the theft of identity information. |
| | Article 7 – Computer related forgery | ID theft/phishing may involve the inputting, altering, deleting, or suppressing of computer data with the result that inauthentic data is considered or acted upon as if it were authentic.<br><br>Phishing is possibly the most common representation of computer related forgery (e.g. a forged web page of a financial institution) and as a consequence the most common illegal activity through which sensitive information is collected, such as identity information. |
| Phase 2 – Possession and disposal of identity information | Article 6 – Misuse of devices | Stolen identity information – including passwords, access credentials, credit cards and others – may be considered "devices, including a computer program, designed and adapted for the purpose of committing any of the offences established in accordance with articles 2 through 5" of the Convention, or "a computer password, access code, or similar data by which the whole of any part of a computer system is capable of being accessed". |
| Phase 3 – Use of the identity information to commit fraud or other crimes | Article 8 – Computer related fraud | The use of a fraudulent identity by inputting, altering, deleting or suppressing computer data, and, or interfering with the function of a computer system will result in the exploitation of bank accounts or credit cards, in taking out loans and credit, or ordering goods and services, and thus causes one person to lose property and causes another person to obtain an economic benefit. |
| All Phases | Article 11 – Attempt, aiding and abetting | The obtaining, possession and disposal of identity information may constitute attempt, aiding and abetting of several crimes specified in the Convention. |
| | Article 13 – Sanctions | Identify theft serves multiple criminal purposes, some of which cause serious damage to individuals and public or private sector institutions.<br><br>A Party may foresee, however, in its domestic law a sanction that is unsuitably lenient for identity theft, and it may not permit the consideration of aggravated circumstances. This may mean that Parties need to consider amendments to their domestic law.<br><br>Therefore, Parties should ensure, pursuant to Article 13, that criminal offences related to identity theft "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For |

| | | |
|---|---|---|
| | | legal persons this may include criminal or non-criminal sanctions, including monetary sanction.<br><br>Parties may also consider aggravating circumstances, for example if identity theft affects a significant number of people or causes serious distress or exposes a person to danger. |

## T-CY Statement

The T-CY agrees that the above illustrates the various scope and elements of identity theft and phishing and the criminal provisions that may apply.

Therefore, the T-CY agrees that the different aspects of such crimes are covered by the Budapest Convention.

# 5 Guidance Note on DDOS attacks[27]

## Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[28]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of denial of service (DOS) and distributed denial of service (DDOS) attacks.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[29] This is to ensure that new forms of malware or crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to DOS and DDOS attacks.

## Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

Denial of service (DOS) attacks are attempts to render a computer system unavailable to users through a variety of means. These may include saturating the target computers or networks with external communication requests, thereby hindering service to legitimate users. Distributed denial of service (DDOS) attacks are denial of service attacks executed by many computers at the same time. There are currently a number of common ways by which DOS and DDOS attacks may be conducted. They include, for example, sending malformed queries to a computer system; exceeding the capacity limit for users; and sending more e-mails to e-mail servers than the system can receive and handle.

DOS and DDOS attacks are covered by the following sections of the convention, depending on what each attack actually does. Each provision contains an intent standard ("without right", "with intent to defraud," etc) which should be readily provable in DOS and DDOS cases.

## T-CY interpretation of the criminalisation of DDOS attacks

| **Relevant Articles** | **Examples** |
|---|---|
| Article 2 – Illegal access | Through DOS and DDOS attacks a computer system may be accessed. |
| Article 4 – Data interference | DOS and DDOS attacks may damage, delete, deteriorate, alter or suppress computer data. |
| Article 5 – System interference | The objective of a DOS or DDOS attack is precisely to seriously hinder the functioning of a computer system. |
| Article 11 – Attempt, aiding and abetting | DOS and DDOS attacks may be used to attempt or to aid or abet several crimes specified in the treaty (such as Computer-related forgery, Article 7; Computer-related fraud, Article 8; Offences related to child pornography, Article 9; and Offences related to infringements of copyright and related rights, Article 10). |

[27] Adopted by the 9th Plenary of the T-CY (4-5 June 2013)

[28] See the mandate of the T-CY (Article 46 Budapest Convention).

[29] Paragraph 36 of the Explanatory Report

| | |
|---|---|
| Article 13 – Sanctions | DOS and DDOS attacks may be dangerous in many ways, especially when they are directed against systems that are crucial to daily life - for example, if banking or hospital systems become unavailable.<br>A Party may foresee in its domestic law a sanction that is unsuitably lenient for DOS and DDOS attacks, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13, that criminal offences related to such attacks "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions.<br><br>Parties may also consider aggravating circumstances, for example, if DOS or DDOS attacks affect a significant number of systems or cause considerable damage, including deaths or physical injuries, or damage to critical infrastructure. |

## T-CY statement

The above list of Articles related to DOS and DDOS attacks illustrates the multi-functional criminal use of such attacks.

Therefore, the T-CY agrees that the different aspects of such attacks are covered by the Budapest Convention.

# 6 Guidance Note on critical information infrastructure attacks[30]

## Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[31]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of critical information infrastructure attacks.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[32] This is to ensure that new forms of malware or crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to critical information infrastructure attacks.

## Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

Critical infrastructures can be defined as systems and assets, whether physical or virtual, so vital to a country that their improper functioning, incapacity or destruction would have a debilitating impact on national security and defence, economic security, public health or safety, or any combination of those matters. Countries define critical infrastructures differently. However, many countries consider critical infrastructures to include the energy, food, water, fuel, transport, communications, finance, industry. defence and governmental and public services sectors.

Critical infrastructures are often run by computer systems, including those known as industrial control systems (ICS) or supervisory control and data acquisition (SCADA) systems. In general, such systems are known as critical information infrastructures.

According to private and governmental sources, a large but unknown number of attacks on critical information infrastructures worldwide takes place every year. These attacks use the same techniques as other electronic crime does. The difference is in the effect of such attacks on society: they may drain money from government treasuries, or shut down water systems, or confuse air traffic control, and so on.

Both current and future forms of critical information infrastructure attacks are covered by the following sections of the convention, depending on the character of the attack. Each provision contains an intent standard ("without right", "with intent to defraud," etc) which should be taken into consideration when officials decide how to charge a crime.

[30] Adopted by the 9th Plenary of the T-CY (4-5 June 2013)

[31] See the mandate of the T-CY (Article 46 Budapest Convention).

[32] Paragraph 36 of the Explanatory Report

## T-CY interpretation of the criminalisation of Critical information infrastructure attacks

| Relevant Articles | Examples |
|---|---|
| Article 2 – Illegal access | Critical information infrastructure attacks may access a computer system. |
| Article 3 – Illegal interception | Critical information infrastructure attacks may use technical means to intercept non-public transmissions of computer data to, from, or within a computer system. |
| Article 4 – Data interference | Critical information infrastructure attacks may damage, delete, deteriorate, alter or suppress computer data. |
| Article 5 – System interference | Critical information infrastructure attacks may hinder the functioning of a computer system; in fact, this may be their primary goal. |
| Article 7 – Computer-related forgery | Critical information infrastructure attacks may input, alter, delete, or suppress computer data with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic. |
| Article 8 – Computer-related fraud | Critical information infrastructure attacks may cause one person to lose property and cause another person to obtain an economic benefit by inputting, altering, deleting, or suppressing computer data and/or interfering with the function of a computer system. |
| Article 11 – Attempt, aiding and abetting | Critical information infrastructure attacks may be used to attempt or to aid or abet crimes specified in the treaty. |
| Article 13 – Sanctions | The effects of critical information infrastructure attacks vary (they may differ in different countries for technical, cultural or other reasons), but governments normally care about them when they cause serious or widespread harm.<br>A Party may foresee in its domestic law a sanction that is unsuitably lenient for critical information infrastructure attacks, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13, that criminal offences related to such attacks "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions.<br><br>Parties may also consider aggravating circumstances, for example, if critical information infrastructure attacks affect a significant number of systems or cause considerable damage, including deaths or physical injuries. |

## T-CY statement

The above list of Articles related to critical information infrastructure attacks illustrates their multi-functional criminal use.

Therefore, the T-CY agrees that the different aspects of such attacks are covered by the Budapest Convention.

## 7 Guidance Note on new forms of Malware[33]

### Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[34]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of new forms of malware.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[35] This is to ensure that new forms of malware or crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to new forms of malware.

### Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

There are many current forms of malware, which has been defined by the Organization for Economic Cooperation and Development as "a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners."[36] Commonly-known forms include worms, viruses, and trojans. Current forms of malware can steal data by copying it and sending it to another address; they can manipulate data; they can hinder the operation of computer systems, including those that control critical infrastructures; ransomware can delete, suppress or block access to data; and specially-tailored malware can target specified computer systems.

According to private and governmental sources, vast numbers of new forms of malware are developed and discovered every year. These new forms vary in their objectives. Like older forms, new forms of malware may steal money, or shut down water systems, or threaten users, and so on.

The numbers and variety of forms of malware are so vast that it would not be possible to describe even currently-known forms in a criminal statute. The Cybercrime Convention deliberately avoids terms such as worms, viruses, and trojans. Because fashions in malware change, using such terms in a convention would quickly make it obsolete and be counterproductive.

It is also not possible, of course, to describe future forms in a statute.

For these reasons, it is important to focus on the objectives and effects of the malware. These are already known and can be described in a statute.

Thus both current and future forms of malware are covered by the following sections of the convention, depending on what the malware actually does. Each provision contains an intent standard ("without right," "with intent to defraud," etc) which should be taken into consideration when officials decide how to charge a crime.

---

[33] Adopted by the 9th Plenary of the T-CY (4-5 June 2013)

[34] See the mandate of the T-CY (Article 46 Budapest Convention).

[35] Paragraph 36 of the Explanatory Report

[36] http://www.oecd.org/internet/ieconomy/40724457.pdf

## T-CY interpretation of the criminalisation of new forms of malware

| Relevant Articles | Examples |
|---|---|
| Article 2 – Illegal access | Malware can be used to access computer systems. |
| Article 3 – Illegal interception | Malware can be used to intercept non-public transmissions of computer data to, from, or within a computer system. |
| Article 4 – Data interference | Malware damages, deletes, deteriorates, alters or suppresses computer data. |
| Article 5 – System interference | Malware may hinder the functioning of a computer system. |
| Article 6 – Misuse of devices. | Malware is a device as defined in Article 6 (parties that take reservations to Article 6 must still criminalize the sale, distribution or making available of covered devices). This is because it will normally be designed or adapted primarily to commit the offences established by Articles 2 through 5. In addition, the article criminalizes the sale, procurement for use, import, distribution or other making available of computer passwords, access codes, or similar data by which computer systems may be accessed. These elements are frequently present in malware prosecutions. |
| Article 7 – Computer-related forgery. | Malware may input, alter, delete, or suppress computer data with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic. |
| Article 8 – Computer-related fraud. | Malware may cause one person to lose property and cause another person to obtain an economic benefit by inputting, altering, deleting, or suppressing computer data and/or interfering with the function of a computer system. |
| Article 11 – Attempt, aiding and abetting | Malware may be used to attempt or to aid or abet several crimes specified in the treaty. |
| Article 13 – Sanctions | The effects of new forms of malware vary widely. Some malware is relatively trivial; other malware is dangerous to people, to critical infrastructures, or in other ways. The effects may differ in different countries for technical, cultural or other reasons.<br><br>A Party may foresee in its domestic law a sanction that is unsuitably lenient for malware attacks, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13, that criminal offences related to such attacks "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions.<br><br>Parties may also consider aggravating circumstances, for example, if malware attacks affect a significant number of systems or cause considerable damage, including deaths or physical injuries, or damage to critical infrastructure. |

## T-CY statement

The above list of Articles related to all forms of malware illustrates the multi-functional criminal use of such attacks.

Therefore, the T-CY agrees that the different aspects of all forms of malware are covered by the Budapest Convention.

# 8 Guidance Note on Spam[37]

## Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[38]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of spam. The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[39] This is to ensure that new forms of malware or crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to spam.

## Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

Spam is often defined as unsolicited bulk email, where a message is sent to a significant number of email addresses, where the recipient's personal identity is irrelevant because the message is equally targeted at many other recipients without distinction.

There are separate issues relating to:

- the content of spam,
- the action of sending spam, and
- the mechanism used to transmit spam.

The content of spam may or may not be illegal, and where the content is illegal (such as offering fake medicines or fraudulent financial offerings) the offence may fall under the relevant national legislation for those offences. The action of transmitting spam (including bulk transmission of non-objectionable content) may be a civil or criminal offence in jurisdictions.

The Convention does not cover spam the contents of which is not illegal and does not cause system interference, but may be a nuisance to end-users.

The tools used to transmit spam may be illegal under the Budapest Convention, and spam may be associated with other offences not listed in the matrix below (see, for example, Article 7).

As with other guidance notes, each provision contains an intent standard ("without right", "with intent to defraud," etc). In some spam cases this intent may be difficult to prove.

[37] Adopted by the 12th Plenary of the T-CY (2-3 December 2014)

[38] See the mandate of the T-CY (Article 46 Budapest Convention).

[39] Paragraph 36 of the Explanatory Report

## T-CY interpretation of provisions addressing spam

| Relevant Articles | Examples |
|---|---|
| Article 2 – Illegal access | Spam may contain malware that may access or enable access to a computer system. |
| Article 3 – Illegal interception | Spam may contain malware that may illegally intercept or enable the illegal interception of transmissions of computer data. |
| Article 4 – Data interference | Spam may contain malware that may damage, delete, deteriorate, alter or suppress computer data. |
| Article 5 – System interference | The transmission of spam may seriously hinder the functioning of computer systems. Spam may contain malware that seriously hinders the functioning of computer systems. |
| Article 6 – Misuse of devices | Devices as defined by Article 6 may be used for the transmission of spam. Spam may contain devices as defined by Article 6. |
| Article 8 – Computer-related fraud | Spam may be used as a device for input, alteration, deletion or suppression of computer data or interference with the functioning of a computer system for procuring illegal economic benefit. |
| Article 10 – Offences related to infringements of copyright | Spam may be used for advertising the sale of fake goods, including software and other items protected by copyright. |
| Article 11 – Attempt, aiding and abetting | Spam and the transmission of spam may be used to attempt or to aid or abet several crimes specified in the treaty (such as Article 7 on computer-related forgery or Article 8 on computer-related fraud). |
| Article 13 – Sanctions | Spam may serve multiple criminal purposes some of which have serious impact on individuals, or public or private sector institutions.<br><br>Even if a Party does not criminalise spam *per se*, it should criminalise spam-related conduct such as the above offences, and it may consider aggravated circumstances.<br><br>Parties should ensure, pursuant to Article 13, that criminal offences related to spam "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions. |

## T-CY statement

The above list of Articles illustrates the multi-functional criminal use of spam and spam-related offences.

Therefore, the T-CY agrees that these aspects of spam are covered by the Budapest Convention.

# 9 Guidance Note on Production orders for subscriber information (Article 18 Budapest Convention)[40]

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[41]

While not binding, Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note[42] addresses the question of production orders for subscriber information under Article 18, that is, situations in which:

- a person ordered to submit specified computer data is present in the territory of a Party (Article 18.1.a);[43]
- a service provider ordered to submit subscriber information is offering its services in the territory of the Party without necessarily being located in the territory (Article 18.1.b).

A Guidance Note on these aspects of Article 18 is relevant given that:

- subscriber information is the most often sought data in criminal investigations;
- Article 18 is a domestic power;
- the growth of cloud computing and remote data storage has raised a number of challenges for competent authorities seeking access to specified computer data – and, in particular, subscriber information – to further criminal investigations and prosecutions;
- currently, practices and procedures, as well as conditions and safeguards for access to subscriber information vary considerably among Parties to the Convention;
- concerns regarding privacy and the protection of personal data, the legal basis for jurisdiction pertaining to services offered in the territory of a Party without the service provider being established in that territory, as well as access to data stored in foreign jurisdictions or in unknown or multiple locations "within the cloud" need to be addressed.

The service and enforceability of domestic production orders against providers established outside the territory of a Party raises further issues which cannot be fully addressed in a Guidance Note. Some Parties may require that subscriber information be requested through mutual legal assistance.

Article 18 is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14 Budapest Convention. Orders are thus to be issued in specific cases with regard to specified subscribers.

## Article 18 Budapest Convention

### Text of the provision

**Article 18 – Production order**

[40] Adopted by the T-CY following the 16th Plenary by written procedure (28 February 2017)

[41] See the mandate of the T-CY (Article 46 Budapest Convention).

[42] This Guidance Note is based on the work of the T-CY Cloud Evidence Group.

[43] It is important to recall that Article 18.1.a of the Budapest Convention is not limited to subscriber information but concerns any type of specified computer data. This Guidance Note, however, addresses the production of subscriber information only.

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

Extract from the Explanatory Report:

173. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement.

Under paragraph 1(b), a Party shall also provide for the power to order a service provider offering services in its territory to "submit subscriber information in the service provider's possession or control". As in paragraph 1(a), the term "possession or control" refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company). The term "relating to such service" means that the power is to be available for the purpose of obtaining subscriber information relating to services offered in the ordering Party's territory.[44]

**What is "subscriber information?"**

The term "subscriber information" is defined in Article 18.3 of the Budapest Convention:

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

[44] Paragraph 173 Explanatory Report.

Paragraph 177 Explanatory Report furthermore notes:

> 177. "Subscriber information" is defined in paragraph 3. In principle, it refers to any information held by the administration of a service provider relating to a subscriber to its services. Subscriber information may be contained in the form of computer data or any other form, such as paper records. As subscriber information includes forms of data other than just computer data, a special provision has been included in the article to address this type of information. "Subscriber" is intended to include a broad range of service provider clients, from persons holding paid subscriptions, to those paying on a per-use basis, to those receiving free services. It also includes information concerning persons entitled to use the subscriber's account.

Obtaining subscriber information may represent a lesser interference with the rights of individuals than obtaining traffic data or content data.

**What is a "service provider?"**

The Budapest Convention on Cybercrime applies a broad concept of "service provider" which is defined in Article 1.c of the Budapest Convention.

For the purposes of this Convention:

> c "service provider" means:
>
> i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
>
> ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

Article 18.1.b is to be applied with respect to any service provider offering its services in the territory of the Party.[45]

## T-CY interpretation of Article 18 Budapest Convention with respect to subscriber information

**The scope of Article 18.1.a**

- The scope is broad: a "person" (which may include a "service provider") that is present in the Party's territory.
- With respect to computer data, the scope is broad but not indiscriminate: any "specified" computer data[2] (hence Article 18.1.a is not restricted to "subscriber information" and covers all types of computer data).
- The specified computer data is in that person's possession or, if the person has no physical possession, that person freely controls the computer data to be submitted under Article 18.1.a from within the Party's territory.
- The specified computer data is stored in a computer system or a computer-data storage medium.
- The production order is issued and enforceable by the competent authorities in the Party in which the order is sought and granted.

[45] European Union instruments distinguish between providers of electronic communication services and of Internet society services. The concept of "service provider" of Article 1.c Budapest Convention encompasses both.

**The scope of Article 18.1.b**

The scope of Article 18.1.b is narrower than that of Article 18.1.a:

- Subsection b is restricted to a "service provider".[46]
- The service provider to which the order is issued is not necessarily present, but offers its services in the territory of the Party.
- It is restricted to "subscriber information."
- The subscriber information relates to such services and is in that service provider's possession or control.

In contrast to Article 18.1.a which is restricted in scope of application to "persons present in the territory of the Party", 18.1.b is silent on the issue of the location of the service provider. Parties could apply the provision in circumstances in which the service provider offering its services in the territory of the Party is neither legally nor physically present in the territory.

**Jurisdiction**

Article 18.1.b is restricted to circumstances in which the criminal justice authority issuing the production order has jurisdiction over the offence.

This may include situations in which the subscriber is or was resident or present in that territory when the crime was committed.

The present interpretation of Article 18 is without prejudice to broader or additional powers under the domestic law of Parties.

Agreement to this Guidance Note does not entail consent to the extraterritorial service or enforcement of a domestic production order issued by another State nor creates new obligations or relationships between the Parties.

**What are the characteristics of a "production order?"**

A "production order" under Article 18 is a domestic measure and is to be provided for under domestic criminal law. A "production order" is constrained by the adjudicative and enforcement jurisdiction of the Party in which the order is granted.

Production orders under Article 18 refer:

> to computer data or subscriber information that are in the possession or control of a person or a service provider. The measure is applicable only to the extent that the person or service provider maintains such data or information. Some service providers, for example, do not keep records regarding the subscribers to their services.[47]

The Explanatory Report[48] to the Budapest Convention refers to production orders as a flexible measure which is less intrusive than search or seizure or other coercive powers and further states that:

> the implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary

[46] The "person" is a broader concept than "a service provider", although a "service provider" can be "a person".

[47] Paragraph 172 Explanatory Report.

[48] Paragraph 171 Explanatory Report.

basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.

**What effect does the location of the data have?**

The storage of subscriber information in another jurisdiction does not prevent the application of Article 18 Budapest Convention as long as such data is in the possession or control of the service provider. The Explanatory Report states with respect to:

- Article 18.1.a that "the term 'possession or control' refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory."[49]

- Article 18.1.b that "the term 'possession or control' refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company)."[50]

Regarding Article 18.1.b, a situation may include a service provider that has its headquarters in one jurisdiction, but stores the data in another jurisdiction. Data may also be mirrored in several jurisdictions or move between jurisdictions according to service provider discretion and without the knowledge or control of the subscriber. Legal regimes increasingly recognise that, both in the criminal justice sphere and in the privacy and data protection sphere, the location of the data is not the determining factor for establishing jurisdiction.

**What is "offering its services in the territory of a Party?"**

The growth of cloud computing has raised questions as to when a service provider is considered to be offering its services in the territory of the Party and thus may be issued a domestic production order for subscriber information. This has led to a range of interpretations across multiple jurisdictions by courts in both civil and criminal cases.

With regard to Article 18.1.b, Parties could consider that a service provider is "offering its services in the territory of the Party", when:

- the service provider enables persons in the territory of the Party to subscribe to its services[51] (and does not, for example, block access to such services);

and

- the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.

[49] Paragraph 173 Explanatory Report. A "person" in Article 18.1.a Budapest Convention may be a physical or legal person, including a service provider.

[50] Paragraph 173 Explanatory Report.

[51] Note Paragraph 183 Explanatory Report: "The reference to a "service agreement or arrangement" should be interpreted in a broad sense and includes any kind of relationship on the basis of which a client uses the provider's services."

The sole fact that a service provider makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country. Therefore, the requirement that the subscriber information to be produced is relating to services of a provider offered in the territory of the Party may be considered to be met even if those services are provided via a country code top-level domain name referring to another jurisdiction.

**General considerations and safeguards**

The Parties to the Convention are expected to form a community of trust that respects Article 15 Budapest Convention.

> Article 15 – Conditions and safeguards
> 1 – Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights against pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
> 2 – Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
> 3 - To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

**Applying Article 18 with respect to subscriber information**

The production of subscriber information under Article 18 Budapest Convention could, therefore, be ordered if the following criteria are met in a specific criminal investigation and with regard to specified subscribers:

<table>
<tr><td colspan="3">IF<br>The criminal justice authority has jurisdiction over the offence;</td></tr>
<tr><td colspan="3">AND IF<br>the service provider is in possession or control of the subscriber information;</td></tr>
<tr><td colspan="3">AND IF</td></tr>
<tr><td>Article 18.1.a<br>The person (service provider) is in the territory of the Party.</td><td>OR</td><td>Article 18.1.b<br>A Party considers that a service provider is “offering its services in the territory of the Party” when, for example:<br><br>– the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services);<br>and<br>– the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by</td></tr>
</table>

| | | |
|---|---|---|
| | | providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.[1] |
| AND IF | | |
| | | – the subscriber information to be submitted is relating to services of a provider offered in the territory of the Party. |

**T-CY statement**

The T-CY agrees that the above represents the common understanding of the Parties as to the scope and elements of Article 18 Budapest Convention with respect to the production of subscriber information.

## 10 Guidance Note on Terrorism[52]

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[53]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses how different Articles of the Convention could apply to terrorism.

Many countries are Parties to numerous treaties, and subject to UN Security Council Resolutions, that require criminalization of different forms of terrorism, facilitation of terrorism, support for terrorism, and preparatory acts. In terrorism cases, countries often rely on offenses that derive from those topic-specific treaties, as well as additional offenses in national legislation.

The Budapest Convention is not a treaty that is focused specifically on terrorism. However, the substantive crimes in the Convention may be carried out as acts of terrorism, to facilitate terrorism, to support terrorism, including financially, or as preparatory acts.

In addition, the procedural and international mutual legal assistance tools in the Convention are available to terrorism and terrorism-related investigations and prosecutions.

The scope and limits are defined by Articles 14.2 and 25.1 Budapest Convention:

> Article 14.2
> 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
> a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
> b other criminal offences committed by means of a computer system; and
> c the collection of evidence in electronic form of a criminal offence.
>
> Article 25.1
> "The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."

See also Articles 23 and 27.1 Budapest Convention as well as other Guidance Notes, such as the Guidance Notes on critical infrastructure attacks or distributed denial of service attacks.

[52] Adopted by the 16th Plenary of the T-CY (14-15 November 2016)
[53] See the mandate of the T-CY (Article 46 Budapest Convention).

## Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

### Procedural provisions

The Convention's procedural powers (Articles 14-21) may be used in a specific criminal investigation or proceeding in any type of case, as Article 14 provides.

In fact, the specific procedural measures can be very useful, for example in terrorism cases, if a computer system was used to commit or facilitate the offence or if the evidence of that offence is stored in electronic form or if a suspect can be identified through subscriber information, including an Internet Protocol address. Thus, in terrorism cases, Parties may use expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools to collect electronic evidence in terrorism and terrorism-related investigations and prosecutions within the scope set out above.

### International mutual legal assistance provisions

The Convention's international cooperation powers (Articles 23-35) are of similar breadth.

Thus, Parties must make available expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools, as well as other international cooperation provisions, in order to cooperate with other Parties in terrorism and terrorism-related investigations and prosecutions within the scope set out above.

### Substantive criminal law provisions

Finally, as noted above, terrorists and terrorist groups may carry out acts criminalized by the Convention as part of achieving their goals.

| **Relevant Articles** | **Examples** |
|---|---|
| Article 2 – Illegal access | A computer system may be illegally accessed to obtain personally identifiable information (e.g. information about government employees to target them for attack). |
| Article 3 – Illegal interception | Non-public transmissions of computer data to, from, or within a computer system may be illegally intercepted to obtain information about a person's location (e.g. to target that person). |
| Article 4 – Data interference | Computer data may be damaged, deleted, deteriorated, altered, or suppressed (e.g. a hospital's medical records can be altered to be dangerously incorrect, or interference with an air traffic control system can affect flight safety). |
| Article 5 – System interference | The functioning of a computer system may be hindered for terrorist purposes (e.g. hindering the system that stores stock exchange records can make them inaccurate, or hindering the functioning of critical infrastructure). |
| Article 6 – Misuse of devices | The sale, procurement for use, import, distribution or other acts making available of computer passwords, access codes, or similar data by which computer systems may be accessed may facilitate a terrorist attack (e.g. it can lead to damage to a country's electrical power grid). |
| Article 7 – Computer-related forgery | Computer data (for example the data used in electronic passports) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic. |
| Article 8 – Computer-related fraud | Computer data may be input, altered, deleted, or suppressed, and/or the function of a computer system may be interfered with, causing other persons to lose property (for example, an attack on a country's banking system can |

| | |
|---|---|
| | cause loss of property to a number of victims). |
| Article 11 – Attempt, aiding and abetting | Crimes specified in the treaty may be attempted, aided or abetted in furtherance of terrorism. |
| Article 12 – Corporate liability | Crimes covered by Articles 2-11 of the Convention in furtherance of terrorism may be carried out by legal persons who would be liable under Article 12. |
| Article 13 – Sanctions | Crimes covered by the Convention may pose a threat to individuals and to society, especially when the crimes are directed against systems that are crucial to daily life, for example public transport, banking systems or hospital infrastructure. The effects may differ in different countries, depending also on their degree of interconnectedness and their dependence on such systems.<br><br>A Party may provide in its domestic law a sanction that is unsuitably lenient for terrorism-related acts in relation to Articles 2 - 11, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13 that criminal offences related to such acts "are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty".<br><br>Parties may also consider aggravating circumstances, for example if such acts affect a significant number of systems or cause considerable damage, including deaths or physical injuries, or damage to critical infrastructure. |

Other crimes covered by the Convention but not mentioned specifically above, including the production of child exploitation materials or trafficking in stolen intellectual property, may also be carried out in connection with terrorism.

For Parties to the Budapest Convention which are also Parties to the Additional Protocol on Xenophobia and Racism Committed Through Computer Systems (ETS 189)[54], two articles of the Protocol are relevant as these may relate to radicalisation and violent extremism which may lead to terrorism. These are Article 4 of the Protocol covering racist and xenophobic motivated threat and Article 6 covering denial, gross minimisation, approval or justification of genocide or crimes against humanity.

## T-CY statement

The T-CY agrees that the substantive crimes in the Convention may also be acts of terrorism as defined in applicable law.

The substantive crimes in the Convention may be carried out to facilitate terrorism, to support terrorism, including financially, or as preparatory acts.

The procedural and mutual legal assistance tools in the Convention may be used to investigate terrorism, its facilitation, support for it, or preparatory acts.

[54] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

## 11 Guidance Note on Aspects of election interference by means of computer systems covered by the Budapest Convention[55]

### Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[56]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

Interference with elections through malicious cyber activities against computers and data used in elections and election campaigns undermines free, fair and clean elections and trust in democracy. Disinformation operations, as experienced in particular since 2016, may make use of malicious cyber activities and may have the same effect. Domestic election procedures may need to be adapted to the realities of the information society, and computer systems used in elections and related campaigns need to be made more secure.

In this context, greater efforts need to be undertaken to prosecute such interference where it constitutes a criminal offence: an effective criminal justice response may deter election interference and reassure the electorate with regard to the use of information and communication technologies in elections.

The present Note addresses how Articles of the Convention may apply to aspects of election interference by means of computer systems.

The substantive criminal offences of the Convention may be carried out as acts of election interference or as preparatory acts facilitating such interference.

In addition, the domestic procedural and international mutual legal assistance tools of the Convention are available for investigations and prosecutions related to election interference. The scope and limits of procedural powers and tools for international cooperation are defined by Articles 14.2 and 25.1 Budapest Convention:

> Article 14.2
> 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
> a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
> b other criminal offences committed by means of a computer system; and
> c the collection of evidence in electronic form of a criminal offence.
>
> Article 25.1
> The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

The procedural powers of the Convention are subject to the conditions and safeguards of Article 15.

### Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

[55] Adopted by T-CY 21 (8 July 2019)
[56] See the mandate of the T-CY (Article 46 Budapest Convention).

**Procedural provisions**

The Convention's procedural powers (Articles 14-21) may be used in a specific criminal investigation or proceeding in any type of election interference, as Article 14 provides.

The specific procedural measures can be very useful in criminal investigations of election interference. For example, in cases of election interference, a computer system may be used to commit or facilitate an offence, the evidence of that offence may be stored in electronic form, or a suspect may be identifiable through subscriber information, including an Internet Protocol address. Similarly, illegal political financing may be traceable via preserved email, voice communications between conspirators may be captured pursuant to properly authorised interception, and misuse of data may be illustrated by electronic trails.

Thus, in criminal investigations of election interference, Parties may use expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools to collect electronic evidence needed for the investigation and prosecution of such offences relating to election interference.

**International mutual legal assistance provisions**

The Convention's international cooperation powers (Articles 23-35) are of similar breadth and may assist Parties in investigations of election interference.

Thus, Parties shall make available expedited preservation of stored computer data, production orders, search and seizure of stored computer data, as well as other international cooperation provisions.

**Substantive criminal law provisions**

Finally, as noted above, election interference may involve the following types of conduct, when done without right, as criminalised by the Convention on Cybercrime. The T-CY emphasises that the examples below are merely examples – that is, since election interference is a developing phenomenon, it may appear in many forms not listed below. However, the T-CY expects that the Convention on Cybercrime is sufficiently flexible to address them.

| **Relevant Articles** | **Examples** |
|---|---|
| Article 2 – Illegal access | A computer system may be illegally accessed to obtain sensitive or confidential information related to candidates, campaigns, political parties or voters. |
| Article 3 – Illegal interception | Non-public transmissions of computer data to, from, or within a computer system may be illegally intercepted to obtain sensitive or confidential information related to candidates, campaigns, political parties or voters. |
| Article 4 – Data interference | Computer data may be damaged, deleted, deteriorated, altered, or suppressed to modify websites, to alter voter databases, or to manipulate results of votes such as by tampering with voting machines. |
| Article 5 – System interference | The functioning of computer systems used in elections or campaigns may be hindered to interfere with campaign messaging, hinder voter registration, disable the casting of votes or prevent the counting of votes through denial of service attacks, malware or other means. |
| Article 6 – Misuse of | The sale, procurement for use, import, distribution or other acts making |

| | |
|---|---|
| devices | available computer passwords, access codes, or similar data by which computer systems may be accessed may facilitate election interference such as the theft of sensitive data from political candidates, parties or campaigns. |
| Article 7 – Computer-related forgery | Computer data (for example the data used in voter databases) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic. For example, some countries require election campaigns to make public financial disclosures. Forgery of computer data could create the impression of incorrect disclosures or hide questionable sources of campaign funds. |
| Article 11 – Attempt, aiding and abetting | Crimes specified in the treaty may be attempted, aided or abetted in furtherance of election interference. |
| Article 12 – Corporate liability | Crimes covered by Articles 2-11 of the Convention in furtherance of election interference may be carried out by legal persons that would be liable under Article 12. |
| Article 13 – Sanctions | Crimes covered by the Convention may pose a threat to individuals and to society, especially when the crimes are directed against fundamentals of political life such as elections. Criminal actions and their effects may differ in different countries, but election interference may undermine trust in democratic processes, change the outcome of an election, require the expense and upheaval of a second election, or cause physical violence between election partisans and communities.<br><br>A Party may provide in its domestic law a sanction that is unsuitably lenient for election-related acts in relation to Articles 2 - 11, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13 that criminal offences related to such acts "are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty".<br><br>Parties may also consider aggravating circumstances, for example, if such acts affect an election significantly or cause deaths or physical injuries or significant material damage. |

## T-CY statement

The T-CY agrees that the substantive offences in the Convention may also be acts of election interference as defined in applicable law, that is, offences against free, fair and clean elections.

The substantive crimes in the Convention may be carried out to facilitate, participate in or prepare acts of election interference.

The procedural and mutual legal assistance tools in the Convention may be used to investigate election interference, its facilitation, participation in it, or preparatory acts.