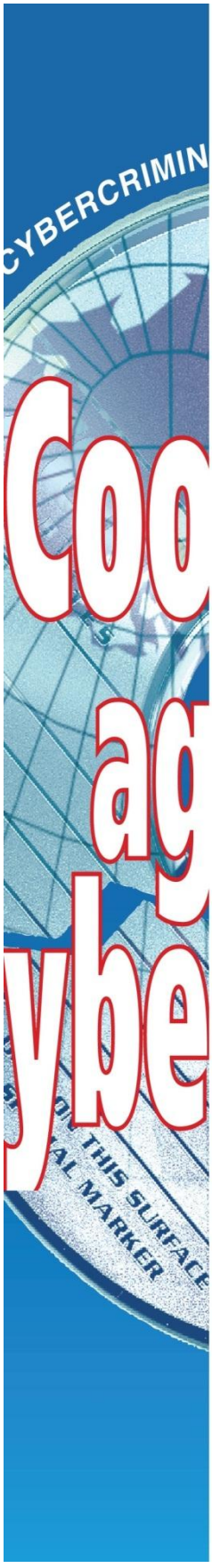

Cybercrime Convention Committee (T-CY)

T-CY GUIDANCES NOTES

Adopted by the 8th and 9th Plenaries of the T-CY

T-CY (2013)29

Strasbourg, version 8 October 2013

www.coe.int/TCY

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

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"[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 (CETS 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 (5-6 December 2012).

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 (CETS 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.

[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.

Relevant Articles	Examples
Article 2 – Illegal access	The creation and operation of a botnet requires illegal access to computer systems.[9] 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.
Article 4 – Data interference	The creation of a botnet always alters and may damage, delete, deteriorate or suppress computer data. 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] Programmes themselves that are used for the creation and operation of botnets also fall under Article 6. 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

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

[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.

	infrastructure. 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. Therefore, Parties should ensure, pursuant to Article 13, that criminal 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. 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 DDOS attacks[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 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".[14] 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 (CETS 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

[12] [12] Adopted by the 9th Plenary of the T-CY (4-5 June 2013)

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

[14] Paragraph 36 of the Explanatory Report

	rights, Article 10).
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. 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. 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.

4 Guidance Note on identity theft and phishing in relation to fraud[15]

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.[16]

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[17] 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".[18] 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,

[15] [15] Adopted by the 9th Plenary of the T-CY (4-5 June 2013)

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

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

[18] Paragraph 36 of the Explanatory Report

drug trafficking, financial fraud against governments and the private sector, but is most generally seen in conjunction with fraud.

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:

Phases	**Articles of the 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. 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.

		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. 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. 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.

		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. 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 critical information infrastructure attacks[19]

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.[20]

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".[21] 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 (CETS 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.

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

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

[21] 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. 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. 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.

6 Guidance Note on new forms of Malware[22]

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.[23]

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".[24] 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 (CETS 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."[25] 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

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

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

[24] Paragraph 36 of the Explanatory Report

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

right," "with intent to defraud," etc) which should be taken into consideration when officials decide how to charge a crime.

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. 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. 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.