www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 5 June 2013 T-CY (2013)11E Rev

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #6

Critical information infrastructure attacks

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

Contact:

Alexander Seger
Secretary Cybercrime Convention Committee
Head of Data Protection and Cybercrime Division
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 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.[1]

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".[2] 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.

2 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.

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

[2] Paragraph 36 of the Explanatory Report

3 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.

4 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.

5 Appendix: Extracts of the Budapest Convention

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data;
b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.