www.coe.int/TCY

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 8 July 2019 T-CY(2019)4

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #9
Aspects of election interference by means of computer systems covered by the Budapest Convention

Adopted by T-CY 21 (8 July 2019)

Contact

Alexander Seger
Executive Secretary Cybercrime Convention Committee
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.

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.

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

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

2.1 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.

2.2 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.

2.3 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 devices	The sale, procurement for use, import, distribution or other acts making 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. 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". 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.

3 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.