T-CY 20 / item 4:

Proposal for a Guidance Note on election interference

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Background

15th European Conference of Electoral Management Bodies "Security in Elections“

(Oslo, 19-20 April 2018, organised by the Venice Commission and the Section for Elections of the Ministry of Local Government and Modernisation of Norway)

Conclusions:

“Cyber-attacks against the confidentiality, integrity and availability of ICTs and data are a real threat to the integrity of electoral processes. They are criminalised under the Council of Europe’s Budapest Convention on Cybercrime. Member States should therefore prosecute them as a priority. Evidence of violations related to elections, party financing, campaign, data protection, stored on computer systems (electronic evidence) should be secured for investigation and criminal prosecution.”

Background

Octopus Conference (11-13 July 2018):

Panel on “democracy under attack”

Key messages

“Interference with elections through attacks against computers and data used in elections and election campaigns combined with disinformation operations, as experienced in particular since 2016, violate rules to ensure free, fair and clean elections and represent attacks against, and undermine trust in, democracy. While rules on elections need to be adapted to the realities of the information society and while systems need to be made more secure, greater efforts need to be undertaken to prosecute such interference.”

Cybercrime in the election process: threats

Elections rely on computer systems at all stages.

Types of interference:

- Attacks against the confidentiality, integrity and availability of election computers and data
  - Compromising voter databases or registration systems (e.g. hacking systems, deleting, changing, adding data)
  - Tampering with voting machines to manipulate results
  - Interference with the function of systems on election day (e.g. distributed denial of service attacks)
  - Illegal access to computers to steal, modify, disseminate sensitive data (e.g. related to election campaigns) for information operations
- Information operations with violations of rules to ensure free, fair and clean elections
  - Data protection rules
  - Rules on political finances
  - Rules on media coverage of electoral campaigns
  - Rules on broadcasting and political advertising

Possible elements of a Guidance Note

Attacks against the confidentiality, integrity and availability of election computers and data

- Compromising voter databases or registration systems
- Tampering with voting machines to manipulate results
- Interference with the function of systems
- Illegal access to computers to steal, modify, disseminate sensitive data for information operations

Information operations with violations of rules to ensure free, fair and clean elections

- Data protection rules
- Rules on political finances
- Rules on media coverage of electoral campaigns
- Rules on broadcasting and political advertising

Budapest Convention

Substantive criminal law provisions

- Article 2 Illegal access
- Article 3 Illegal interception
- Article 4 Data interference
- Article 5 System interference
- Article 6 Misuse of devices
- Article 7 Forgery
- Article 8 Fraud
- Article 11 Attempt, aiding, abetting

Procedural powers and international cooperation to secure electronic evidence and prosecute offenders

- Articles 16, 17, 29 and 30 for data preservation
- Article 18 Production orders
- Article 19 Search and seizure
- Etc. (incl. cooperation with service providers