# Cybercrime and attacks against democracy: the role of the Budapest Convention

Alexander Seger
Executive Secretary
Cybercrime Convention Committee
Council of Europe
Strasbourg, France
alexander.seger@coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

## 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

## Budapest Convention on Cybercrime: scope

**Criminalising conduct**
- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

**Procedural tools**
- Expedited preservation
- Production orders
- Search and seizure
- Interception
- Limited by safeguards (article 15)

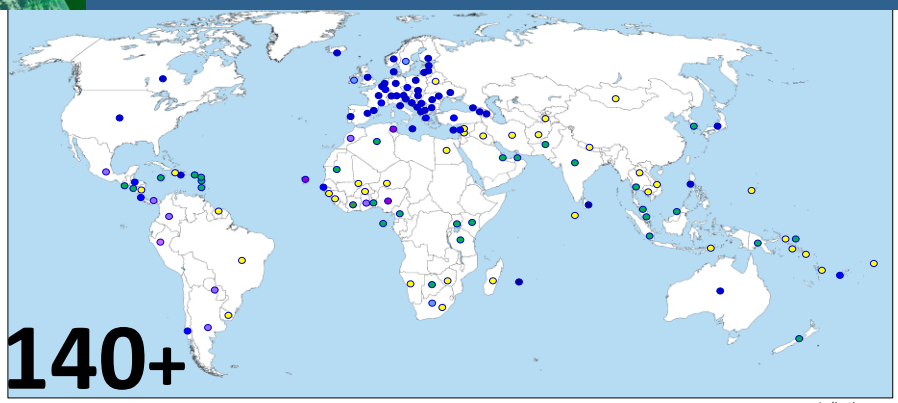
+

**International cooperation**
- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

**Procedural powers and international cooperation for ANY CRIME entailing evidence on a computer system!**

*Note: work on Protocol to Budapest Convention underway*

## Budapest Convention: Reach




Indicative map only

**Budapest Convention**
**Ratified/acceded: 60**
**Signed: 4**
**Invited to accede: 7**
**= 71**

**Other States with laws/draft laws largely in line with Budapest Convention = 20+**

**Further States drawing on Budapest Convention for legislation = 50+**

## Cybercrime and other offences in the election process: the role of the Budapest Convention

**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

## Cybercrime and other offences in the election process: the role of the Budapest Convention

## Conclusions

- Interference with elections involves cybercrime and/or electronic evidence
- Institutions responsible for elections need to understand risks and measures to be taken
- Invest in cybersecurity measures to protect systems used for elections and election campaigns
- Prosecute cybercrime related to elections (chapter I Budapest Convention)
- Secure electronic evidence and cooperate to identify and prosecute offenders (chapters II and III Budapest Convention)
  - Apply procedural powers to secure evidence
  - Interagency cooperation (involve specialised cybercrime and computer forensic units in investigations)
  - International cooperation to secure evidence in other jurisdictions
  - Cooperation with service providers (see work on Protocol to Budapest C.)