Visit of a delegation of Jordan to the C-PROC
Bucharest, Romania, 18 November 2014

The Budapest Convention on Cybercrime

What benefits for Jordan?

Alexander Seger
Council of Europe

www.coe.int/cybercrime

Jordan and the Budapest Convention – what benefits?

Part I - Cooperation against cybercrime: the approach of the Council of Europe

Part II - The Budapest Convention on Cybercrime: what impact?

Part III - Jordan and the Budapest Convention
I. The approach of the Council of Europe

www.coe.int

in order to promote democracy rule of law human rights

Measures against Cybercrime

Established in 1949
Currently 47 member States

I. The approach of the Council of Europe

1 Common standards: Budapest Convention on Cybercrime and relates standards

“Protecting you and your rights in cyberspace”

2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC ➤
Technical cooperation programmes
I. The approach of the Council of Europe

Budapest Convention
Ratified/acceded: 44
Signed: 9
Invited to accede: 10
= 63

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

Further States drawing on Budapest Convention for legislation = 43+

1 Standards

ETS 182 - Budapest Convention on Cybercrime
ETS 189 – Protocol on Xenophobia and Racism

ETS 108 – Convention on Data Protection
CETS 201 – Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse
CETS 198 – Convention on the Laundering, Search, Seizure and Confiscation of Proceeds from Crime and the Financing of Terrorism
CETS 196 – Convention on the Prevention of Terrorism
ETS 30 – Convention on Mutual Legal Assistance in Criminal Matters

http://conventions.coe.int
I. The approach of the Council of Europe

2 Cybercrime Convention Committee (T-CY)
Established under Article 46 Budapest Convention

Membership (status March 2014):
- 44 Members (State Parties)
- 19 Observer States

Functions:
- Assessments of the implementation of the Convention by the Parties
- Guidance Notes
- Draft legal instruments
- Etc.

Guidance Notes adopted:
- Notion of “Computer Systems”
- Botnets
- Identity theft
- DDoS attacks
- Critical Infrastructure Attacks
- Malware

Guidance Notes under negotiation:
- SPAM
- Article 32 b (Transborder access)
I. The approach of the Council of Europe

2. Cybercrime Convention Committee (T-CY)

2nd round of T-CY Assessments:

Efficiency of international cooperation provisions:
- Article 31 on mutual assistance regarding accessing of stored computer data.
- And related Articles 23, 25, 26, 27, 28 and 35.

Aim:
- Better use of existing provisions
- Additional solutions

Procedure and status:
- Questionnaire February 2013.
- Plenary discussions June 2013, Dec 2013, June 2014.
- Revised report to be discussed (adopted) in December 2014.

3. Capacity building programmes

Focus on:
- Cybercrime strategies
- Legislation and safeguards
- Cybercrime units
- Law enforcement training
- Judicial training
- Financial investigations
- Protecting children
- Public/private cooperation
- International cooperation

Council of Europe global and regional projects:
- 600+ activities with 125+ countries & 130+ organisations and private sector since 2006
- Encouraging other donors to provide assistance to countries in implementing Budapest Convention
I. The approach of the Council of Europe

3. Capacity building programmes

Projects under way:

- GLACY project on Global Action on Cybercrime
- Cybercrime@EAP
- Cybercrime@Octopus

All projects are managed by:

✓ C-PROC (Cybercrime Programme Office of the Council of Europe, Bucharest, Romania)

I. The approach of the Council of Europe

Part I (Council of Europe approach)

Q & A
II. The Budapest Convention on Cybercrime

Opened for signature November 2001 in Budapest

As at November 2014:

- 44 parties (35 European, Australia, Dominican Republic, Japan, Mauritius, Panama and USA)
- 9 signatories (European, Canada, South Africa)
- 10 States invited to accede (Argentina, Chile, Colombia, Costa Rica, Israel, Mexico, Morocco, Philippines, Senegal, Tonga)

= 63 States are parties/are committed to become parties/participate in Cybercrime Convention Committee at present

- Additional invitations to accede are in process
- Many more have used Budapest Convention as a guideline for domestic legislation

Reach of the Budapest Convention

Budapest Convention
Ratified/acceded: 44
Signed: 9
Invited to accede: 10
= 63

Other States with laws/draft laws largely in line with Budapest Convention = 20
Further States drawing on Budapest Convention for legislation = 43+
### Scope of the Budapest Convention on Cybercrime

<table>
<thead>
<tr>
<th>Criminalising conduct</th>
<th>Procedural tools</th>
<th>International cooperation</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Illegal access</td>
<td>- Expedited preservation</td>
<td>- Extradition</td>
</tr>
<tr>
<td>- Illegal interception</td>
<td>- Search and seizure</td>
<td>- MLA</td>
</tr>
<tr>
<td>- Data interference</td>
<td>- Interception of computer data</td>
<td>- Spontaneous information</td>
</tr>
<tr>
<td>- System interference</td>
<td></td>
<td>- Expedited preservation</td>
</tr>
<tr>
<td>- Misuse of devices</td>
<td></td>
<td>- MLA for accessing computer data</td>
</tr>
<tr>
<td>- Fraud and forgery</td>
<td></td>
<td>- MLA for interception</td>
</tr>
<tr>
<td>- Child pornography</td>
<td></td>
<td>- 24/7 points of contact</td>
</tr>
<tr>
<td>- IPR-offences</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Harmonisation

<table>
<thead>
<tr>
<th>The Budapest Convention on Cybercrime</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Considerations:</strong></td>
</tr>
<tr>
<td>- A criminal justice treaty for specific criminal investigations</td>
</tr>
<tr>
<td>- Common criminal policy aimed at the protection of society against cybercrime</td>
</tr>
<tr>
<td>- Cooperation between States and private industry</td>
</tr>
<tr>
<td>- Balance interests of law enforcement and respect for fundamental human rights, including right to privacy and the protection of personal data</td>
</tr>
</tbody>
</table>

**Specific aims:**

1. Criminalise conduct against and by means of computer systems, networks and data
2. Allow for law enforcement powers to investigate and prosecute cybercrime and electronic evidence
3. Provide for efficient international cooperation
**Effectiveness/Impact of the Budapest Convention**

- Stronger and more harmonised legislation
- More efficient international cooperation between Parties
- Better cybersecurity performance
- More investigation, prosecution and adjudication of cybercrime and e-evidence cases
- Trusted partnerships and public/private cooperation
- Catalyst for capacity building
- Contribution to human rights/rule of law in cyberspace

= “Protecting you and your rights”

---

**Interim summary: A dynamic framework**

- Protocols
- Guidance Notes
- Enlarged membership in Convention
- Political commitment
- Cybercrime policies and strategies

- Standards
- “Protecting you and your rights in cyberspace”
- Capacity building
- T-CY

- Tools and concepts
- Training materials
- Good practice studies
- Resource mobilisation
- Partnerships
- Trust
II. The Budapest Convention on Cybercrime

Part II (Budapest Convention)

Q & A

III. The Budapest Convention on Cybercrime and Jordan

Review of Jordanian law against the Budapest Convention

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

Procedural tools
- Expedited preservation
- Search and seizure
- Interception of computer data

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

Harmonisation
III. The Budapest Convention on Cybercrime and Jordan

Substantive criminal law

<table>
<thead>
<tr>
<th>Article</th>
<th>Budapest Convention</th>
<th>Laws of Jordan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 2</td>
<td>Illegal access</td>
<td>2010 Act, art. 3</td>
</tr>
<tr>
<td>Art. 3</td>
<td>Illegal interception</td>
<td>2010 Act, art. 5; 1995 Act, art. 76</td>
</tr>
<tr>
<td>Art. 4</td>
<td>Data interference</td>
<td>2010 Act, art. 3(b)</td>
</tr>
<tr>
<td>Art. 5</td>
<td>System interference</td>
<td>2010 Act, art. 4</td>
</tr>
<tr>
<td>Art. 6</td>
<td>Misuse of devices</td>
<td>2010 Act, art. 4 (in part)</td>
</tr>
</tbody>
</table>

III. The Budapest Convention on Cybercrime and Jordan

Article 3 of the Convention: illegal interception

- Establish as criminal offences under 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.

Jordan: Article 5 Information System Crime Law 2010

A person is guilty of an offence, if he retains or intercepts any data or information sent over the internet or any information system and shall be liable to imprisonment for a term not less than one month and not exceeding a year and to a fine not less than two hundred Jordanian Dinars and not exceeding a thousand Jordanian Dinars, or to both.
III. The Budapest Convention on Cybercrime and Jordan

Article 5 of the Convention: system interference

Establish as criminal offences under 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.

Jordan: Article 4 Information System Crime Law 2010

A person is guilty of an offence if he uses, introduces or publishes a programme on the internet or an information system with the intent to delete, cancel, add, destroy, hide, adapt, edit, transfer or copy data or information or impair the operation of any information system or to change or cancel or destroy or edit the contents of a website or assuming its identity or the identity of its owner. The offender shall be liable to imprisonment for a term not less than three months and not exceeding a year or to a fine not less than two hundred Jordanian Dinars and not exceeding a thousand Jordanian Dinars, or to both.

<table>
<thead>
<tr>
<th>Article</th>
<th>Budapest Convention</th>
<th>Laws of Jordan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 7</td>
<td>Computer-related forgery</td>
<td>2010 Act, art. 3(b) and 4 re: Identity theft Penal Code, arts. 260-271</td>
</tr>
<tr>
<td>Art. 8</td>
<td>Computer-related fraud</td>
<td>2010 Act, art. 6(b) Penal Code, art. 417</td>
</tr>
<tr>
<td>Art. 9</td>
<td>Child pornography</td>
<td>2010 Act, art. 8</td>
</tr>
<tr>
<td>Art. 10</td>
<td>IPR offences</td>
<td>Copyright Act 1992, art. 51 et seq. (in part)</td>
</tr>
<tr>
<td>Art. 11</td>
<td>Attempt, aiding, abetting</td>
<td>2010 Act, art. 13 (in part)</td>
</tr>
<tr>
<td>Art. 12</td>
<td>Corporate liability</td>
<td>-</td>
</tr>
</tbody>
</table>
III. The Budapest Convention on Cybercrime and Jordan

Article 8 Convention - Computer-related fraud
Establish as criminal offences under 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.

Jordan: Article 6 (b) Information System Crime Law 2010
(b) If a person uses the internet or any information system with the intention to obtain information or data on credit cards or information that are used to execute financial or banking transactions with the intent to retain information, data, money or services of others to himself or to others, he shall be liable to imprisonment for a term not less than one year and to a fine not less than one thousand Jordanian Dinars and not exceeding five thousand Jordanian Dinars.

III. The Budapest Convention on Cybercrime and Jordan

Article 9 Convention - Child pornography

1. Establish as criminal offences when committed intentionally and without right, the following conduct:

a. producing child pornography for the purpose of its distribution through a computer system;
b. offering or making available child pornography through a computer system;
c. distributing or transmitting child pornography through a computer system;
d. procuring child pornography through a computer system for oneself or for another person;
e. possessing child pornography in a computer system or on a computer-data storage medium.
III. The Budapest Convention on Cybercrime and Jordan

Article 9 Convention - Child pornography

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
   a a minor engaged in sexually explicit conduct;
   b a person appearing to be a minor engaged in sexually explicit conduct;
   c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Jordan: Article 8 Information System Crime Law 2010

(a) A person is guilty of an offence, if he sends or publishes any written, audible or visual material that contains pornography involving sexual exploitation of minors and shall be liable to imprisonment for a term not less than three months and to a fine not less than three hundred Jordanian Dinars and not exceeding five thousand Jordanian Dinars.

(b) If a person uses the internet or any other information system to produce, save, process, publish, print or promote for pornography with the intent to influence minors or mentally or psychologically disabled people or direct them to committing an offence, he shall be liable to imprisonment for a term not less than two years and to a fine not less than one thousand Jordanian Dinars and not exceeding five thousand Jordanian Dinars.

(c) A person is found guilty of an offence, if he uses the internet or any other information system with the intention to involve minors or mentally or psychologically disabled people in any act of prostitution or pornography and shall be liable to temporary hard labour and to a fine not less than five thousand Jordanian Dinars and not exceeding fifteen thousand Jordanian Dinars.
### III. The Budapest Convention on Cybercrime and Jordan

#### Conclusion: Laws of Jordan cover many of the substantive criminal law provisions of the Budapest Convention.

<table>
<thead>
<tr>
<th>Article</th>
<th>Budapest Convention</th>
<th>Laws of Jordan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 2</td>
<td>Illegal access</td>
<td>2010 Act, art. 3</td>
</tr>
<tr>
<td>Art. 3</td>
<td>Illegal interception</td>
<td>2010 Act, art. 5; 1995 Act, art. 76</td>
</tr>
<tr>
<td>Art. 4</td>
<td>Data interference</td>
<td>2010 Act, art. 3(b)</td>
</tr>
<tr>
<td>Art. 5</td>
<td>System interference</td>
<td>2010 Act, art. 4</td>
</tr>
<tr>
<td>Art. 6</td>
<td>Misuse of devices</td>
<td>2010 Act, art. 4 (in part)</td>
</tr>
<tr>
<td>Art. 7</td>
<td>Computer-related forgery</td>
<td>2010 Act, art. 3(b) and 4 re: identity theft Penal Code, arts. 260-271</td>
</tr>
<tr>
<td>Art. 8</td>
<td>Computer-related fraud</td>
<td>2010 Act, art. 6(b) Penal Code, art. 417</td>
</tr>
<tr>
<td>Art. 9</td>
<td>Child pornography</td>
<td>2010 Act, art. 8</td>
</tr>
<tr>
<td>Art. 10</td>
<td>IPR offences</td>
<td>Copyright Act 1992, art. 51 et seq. (in part)</td>
</tr>
<tr>
<td>Art. 11</td>
<td>Attempt, aiding, abetting</td>
<td>2010 Act, art. 13 (in part)</td>
</tr>
<tr>
<td>Art. 12</td>
<td>Corporate liability</td>
<td>-</td>
</tr>
</tbody>
</table>

### III. The Budapest Convention on Cybercrime and Jordan

#### Investigative powers in procedural law

<table>
<thead>
<tr>
<th>Article</th>
<th>Budapest Convention</th>
<th>Laws of Jordan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 15</td>
<td>Conditions and safeguards</td>
<td>Unclear as procedural law incomplete</td>
</tr>
<tr>
<td>Art. 16</td>
<td>Expedited preservation</td>
<td>-</td>
</tr>
<tr>
<td>Art. 17</td>
<td>Expedited preservation and partial disclosure of traffic data</td>
<td>-</td>
</tr>
<tr>
<td>Art. 18</td>
<td>Production order</td>
<td>-</td>
</tr>
<tr>
<td>Art. 19</td>
<td>Search and seizure</td>
<td>2010 Act, art. 12 (in part)</td>
</tr>
<tr>
<td>Art. 20</td>
<td>Real-time collection traffic data</td>
<td>1995 Act, art. 29 (in part)</td>
</tr>
<tr>
<td>Art. 21</td>
<td>Interception of content data</td>
<td>Trials Code, art. 88</td>
</tr>
<tr>
<td>Art. 22</td>
<td>Jurisdiction</td>
<td>2010 Act, art. 16</td>
</tr>
</tbody>
</table>
Article 15 Convention - Conditions and safeguards

1. Each Party shall ensure that ... the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Article 16 of the Convention – Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. ....

Laws of Jordan
III. The Budapest Convention on Cybercrime and Jordan

Article 17 Convention - Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:
   a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
   b ensure the expeditious disclosure to the Party’s competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

Laws of Jordan -

Article 18 - Production order

1 ...measures to empower competent authorities to order:
   a a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium; and
   b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control.

3 For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
   a the type of communication service used, the technical provisions taken thereto and the period of service;
   b the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
   c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Laws of Jordan -
Article 19 Convention - Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
   a a computer system or part of it and computer data stored therein; and
   b a computer-data storage medium in which computer data may be stored in its territory.

2 Measures to ensure that where authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Measures to empower competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
   a seize or similarly secure a computer system or part of it or a computer-data storage medium;
   b make and retain a copy of those computer data;
   c maintain the integrity of the relevant stored computer data;
   d render inaccessible or remove those computer data in the accessed computer system.

4 Measures to empower competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
Jordan: Article 12 Information System Crime Law 2010

(a) With the permission of the attorney general or the concerned court, police officers may enter any place if evidence shows that it was used to commit any of the offences mentioned under this law. They also may inspect any devices, equipment, systems and programmes that are suspected to have been used in committing the offence, provided that they respect the laws and regulations and the rights of the suspect. In all cases, police officers conducting the inspection shall prepare a report and present it to the attorney general.

(b) Police officers may confiscate any devices, money, equipment or programmes that were used to commit the offence or gained as a result of it.

(c) The concerned court may give the permission to confiscate any devices, equipment, money or programmes that were used to commit any offence mentioned in this law or gained as a result of it.

Conclusion: further reform of procedural law would be needed.

<table>
<thead>
<tr>
<th>Article</th>
<th>Budapest Convention</th>
<th>Laws of Jordan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 15</td>
<td>Conditions and safeguards</td>
<td>Unclear as procedural law incomplete</td>
</tr>
<tr>
<td>Art. 16</td>
<td>Expedited preservation</td>
<td>-</td>
</tr>
<tr>
<td>Art. 17</td>
<td>Expedited preservation and partial disclosure of traffic data</td>
<td>-</td>
</tr>
<tr>
<td>Art. 18</td>
<td>Production order</td>
<td>-</td>
</tr>
<tr>
<td>Art. 19</td>
<td>Search and seizure</td>
<td>2010 Act, art. 12 (in part)</td>
</tr>
<tr>
<td>Art. 20</td>
<td>Real-time collection traffic data</td>
<td>1995 Act, art. 29 (in part)</td>
</tr>
<tr>
<td>Art. 21</td>
<td>Interception of content data</td>
<td>Trials Code, art. 88</td>
</tr>
<tr>
<td>Art. 22</td>
<td>Jurisdiction</td>
<td>2010 Act, art. 16</td>
</tr>
</tbody>
</table>
Chapter III of the Convention - International cooperation

Section 1 – General principles

- Art 23 General principles on international cooperation
- Art 24 Principles related to extradition
- Art 25 Principles related to mutual legal assistance
- Art 26 Spontaneous information
- Art 27 MLA in the absence of applicable international instruments
- Art 28 Confidentiality and limitation on use

Section 2 – Specific provisions

- Art 29 - Expedited preservation of stored computer data
- Art 30 - Expedited disclosure of preserved computer data
- Art 31 - Mutual assistance regarding accessing stored computer data
- Art 32 - Trans-border access to stored computer data (public/with consent)
- Art 33 - Mutual assistance in real-time collection of traffic data
- Art 34 - Mutual assistance regarding interception of content data
- Art 35 - 24/7 network

Laws of Jordan: ?
Conclusion:

1. Substantive law: Many provisions available. Adjustments recommended

2. Procedural law: Most provisions missing. Reforms required

3. International cooperation: To be clarified

Acceding to the Budapest Convention
### III. The Budapest Convention on Cybercrime and Jordan

#### Treaty open for accession by any State (article 37)

<table>
<thead>
<tr>
<th>Phase 1:</th>
<th>Phase 2:</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ If a country has legislation in place or advanced stage: Letter from Government to CoE expressing interest in accession</td>
<td>▪ Domestic procedure (e.g. decision by national Parliament)</td>
</tr>
<tr>
<td>▪ Consultations (CoE/Parties) in view of decision to invite</td>
<td>▪ Deposit the instrument of accession at the Council of Europe</td>
</tr>
<tr>
<td>▪ Invitation to accede</td>
<td></td>
</tr>
</tbody>
</table>

**Acceded:** Australia, Dominican Republic, Mauritius, Panama  
**Invited:** Argentina, Chile, Colombia, Costa Rica, Israel, Mexico, Morocco, Philippines, Senegal, Tonga

---

**Could Jordan request accession to the Budapest Convention?**

**Possibly YES if there is a commitment to reform procedural law.**
III. The Budapest Convention on Cybercrime and Jordan

Benefits of joining Budapest

- Trusted and efficient cooperation with other Parties
- Participation in the Cybercrime Convention Committee (T-CY)
- Participation in future standard setting (Guidance Notes, Protocols and other additions to Budapest Convention)
- Enhanced trust by private sector
- Technical assistance and capacity building

“Cost”: Commitment to cooperate

Disadvantages?

---

CoE/Jordan cooperation on cybercrime

The way ahead:

- CoE/Jordan cooperation on reform of criminal law?
- Workshop/s 2015
- Participation by Jordan in Octopus Conference June 2015?