

## **GR-J**

### **Rapporteur Group on Legal Co-operation**

**GR-J(2014)10**

12 November 2014<sup>1</sup>

---

## **Council of Europe Convention on Cybercrime (ETS No. 185) – Request by Sri Lanka to be invited to accede**

### **For consideration by the GR-J at its meeting of 8 December 2014**

---

1. By letter dated 4 April 2014, registered at the Secretariat General on 23 April 2014, Ms Kshenuka Senewiratne, Secretary to the Ministry of External Affairs of Sri Lanka, informed the Secretary General about the wish of the Government of Sri Lanka to be invited to accede to the aforementioned Convention (see Appendix 1).
2. In line with the constant practice of the Council of Europe, the Secretariat proceeded to an informal consultation of the member States, asking them to communicate to the Secretariat whether their authorities would object to the accession of Sri Lanka to the Convention on Cybercrime if the request to be invited to accede was formally submitted to the Committee of Ministers. The deadline for replying was 16 June 2014. Following requests from delegations, the original deadline was extended to 27 June 2014 and then to 5 September 2014. Objections were communicated to the Secretariat but were later withdrawn.
3. An information note of the Secretariat on co-operation with Sri Lanka appears in Appendix 2.
4. The relevant provisions of the Convention on Cybercrime can be summarised as follows:
  - a. **Summary of the Convention**
5. The Convention on Cybercrime (ETS No. 185) was opened for signature by the member States of the Council of Europe and by non-member States having participated in its elaboration, in Budapest, on 23 November 2001. It entered into force on 1 July 2004. The chart of signatures and ratifications appears in Appendix 3.
6. The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also provides a series of procedural powers, such as the search for computer networks and the interception of data. Its main objective, set out in the preamble, is “to pursue a common criminal policy aimed at the protection of society against cybercrime, *inter alia* by adopting appropriate legislation and fostering international co-operation”.
7. The Convention has been complemented by an Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), which was opened for signature on 28 January 2003 and entered into force on 1 March 2006.

---

<sup>1</sup> This document has been classified restricted at the date of issue; it will be declassified in accordance with Resolution Res(2001)6 on access to Council of Europe documents.

**b. Procedure for accession**

8. Article 37, paragraph 1 of the Convention on Cybercrime stipulates as follows:

*“After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any state which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.”*

9. Given the above, the Deputies may wish to take note of the requests of Sri Lanka to be invited to accede to the Convention on Cybercrime and assess whether there is an agreement in principle towards granting such requests, in accordance with the applicable provisions of the Convention.

10. If the Deputies agree in principle to invite Sri Lanka to accede to the Convention on Cybercrime, they could agree to instruct the Secretariat to consult the non-member States which are Contracting States thereto, i.e. Australia, the Dominican Republic, Japan, Mauritius, Panama and the United States of America, and set 13 February 2015 as the deadline for a reply.

11. In respect of such consultation, the Deputies may decide that, if there is no objection from Australia, the Dominican Republic, Japan, Mauritius, Panama or the United States of America before the expiration of the term of 13 February 2015, the decision to invite Sri Lanka to accede to the Convention on Cybercrime would be regarded as adopted on 18 February 2015 (1220th meeting of the Deputies).

12. The Deputies may decide to resume consideration of this item if the above-mentioned non-member States which are Contracting States raised an objection concerning the accession of Sri Lanka to the Convention.



විදේශ කටයුතු අමාත්‍යාංශය  
வெளிவிவகார அமைச்சு  
MINISTRY OF EXTERNAL AFFAIRS

ජනරජ ගොඩනැගිල්ල, කොළඹ 1, ශ්‍රී ලංකාව குடியரசுக் கட்டிடம், கொழும்பு 1, இலங்கை Republic Building, Colombo 1, Sri Lanka

මගේ අංකය } L/E/GEN/869  
எனது இல }  
My No }

ඔබේ අංකය }  
உமது இல }  
Your No }

දිනය } 04.04.2014  
திகதி }  
Date }

HE Thorbjørn Jagland  
The Secretary General  
Council of Europe  
Avenue de l'Europe  
F - 67075 Strasbourg Cedex  
France,

Fax +33 (0)3 88 41 27 99  
Email : [private.office@coe.int](mailto:private.office@coe.int)

Your Excellency,

**Request to Accede to the Budapest Convention on Cybercrime (ETS No.185)**

I am pleased to inform you that the Government of Sri Lanka appreciates the measures taken by the Council of Europe to enact the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copy rights, computer-related fraud, child pornography, hate crimes and violations of network security.


I am also pleased to inform that the Government of Sri Lanka has taken a number of initiatives to develop and promote the ICT sector for the benefit of its people. In order to achieve our development goals in the ICT sector, the Government has taken measures to enact legislation in line with the Convention and introduce policies based on international best practices.

In 2007, the Government enacted legislation to combat Cyber Crime, which is manifested in the Computer Crimes Act No. 24 of 2007. In the preparation of this legislation, the principles and features contained in the Council of Europe Convention on Cyber Crime (Budapest Convention) were used. Since the enactment of this Legislation, the ICT Agency of Sri Lanka (ICTA) has been collaborating closely with the Cyber Crime & Data Protection Divisions of the Council of Europe on a number of initiatives.

Consequently, several related events have been hosted in Sri Lanka jointly by ICTA and the Council of Europe.

I wish to declare that the Government of Sri Lanka is keen to accede to the Council of Europe Convention on Cyber Crimes (Budapest Convention) - ETS No.185. Therefore, on behalf of Government of Sri Lanka, I would like to request an invitation by the Council of Europe for the Government of Sri Lanka to accede to the Council of Europe Convention on Cyber Crimes with an intimation of the procedure for such accession.

Please accept Excellency the assurances of my highest consideration.

  
Kshenuka Senewiratne  
Secretary/External Affairs

Cc. Mr. Lalith Weeratunga, Secretary to HE the President  
Mr. Jayantha Fernando, Director/Legal Advisor, ICTA

I2014-10



Ref: EU/PRO/6/68

The Mission of the Democratic Socialist Republic of Sri Lanka to the European Union and the Embassy of Sri Lanka to Belgium and Luxembourg based in Brussels presents its compliments to the Office of the Secretary General of the Council of Europe and further to the latter's Note Verbale Ref: EU/PRO/6/65 of 07 April 2014, has the honour to forward herewith the original of the letter addressed to H. E. Thorbjørn Jagland, the Secretary General of the Council of Europe from Ms. Kshenuka Senewiratne, Secretary to the Ministry of External Affairs of Sri Lanka.

The Mission appreciates receiving the requested invitation by the Council of Europe for Government of Sri Lanka to accede to the Council of Europe Convention on Cyber Crimes with an intimation of the procedure for such accession, at the earliest possible.

The Mission of the Democratic Socialist Republic of Sri Lanka to the European Union and the Embassy of Sri Lanka to Belgium and Luxembourg based in Brussels avails itself of this opportunity to renew to the Office of the Secretary General of the Council of Europe, the assurances of its highest consideration.

A handwritten signature in blue ink, appearing to be 'K. Senewiratne'.

Brussels, 15 April 2014



## Appendix 2

### 1. Introduction

The Government of Sri Lanka, by letter signed by the Secretary External Affairs dated 4 April 2014, submitted a request for accession to the Budapest Convention on Cybercrime. The purpose of the present note is to provide supplementary information on the state of co-operation with Sri Lanka in cybercrime matters, including an overview of implementation of the principles of the Budapest Convention.

### 2. Co-operation with Sri Lanka

The authorities of Sri Lanka and the Council of Europe have been co-operating in cybercrime matters since 2008 when the Information and Communication Technology Agency (ICTA) of Sri Lanka and the Council of Europe jointly held a workshop on cybercrime for judges, prosecutors, lawyers and investigators (27-28 October 2008). That workshop followed the adoption of the Computer Crimes Act of 2007 which had brought domestic legislation in line with the Budapest Convention.

In April 2011, the ICTA of Sri Lanka and the Council of Europe held an international workshop in Sri Lanka on Co-operation against Cybercrime in South Asia involving representatives of Bangladesh, Maldives, India, Pakistan and Sri Lanka. This not only contributed to improved sub-regional co-operation in matters related to cybercrime and electronic evidence but also led to legislative reforms in Maldives and Pakistan on the basis of the Budapest Convention.<sup>2</sup>

In October 2013, the ICTA of Sri Lanka and the Council of Europe organised a workshop on capacity building on cybercrime and electronic evidence for judges, prosecutors and law enforcement of Sri Lanka, Maldives and Pakistan.<sup>3</sup>

Moreover, representatives of Sri Lanka participated with speakers and moderators in all Octopus Conferences on Cybercrime since 2008 as well as in a number of workshops organised by the Council of Europe at Internet Governance Fora. Sri Lanka supported observer status of the Council of Europe in the Governmental Advisory Committee (GAC) of ICANN.

### 3. Cybercrime legislation

#### 3.1 Substantive and procedural laws

In 2007, Sri Lanka adopted the Computer Crimes Act no. 24 of 2007<sup>4</sup> which brought the domestic legislation largely in line with the Budapest Convention:<sup>5</sup>

Provisions of Budapest Convention	Equivalent in domestic legislation
Definitions (Art. 1)	Art. 38 Computer Crimes Act 2007
<b>Substantive law</b>	
Illegal access (Art. 2)	Art. 3 and 4 CCA
Illegal interception (Art 3)	Art. 8 CCA
Data interference (Art. 4)	Art. 5 and 6 CCA
System interference (Art. 5)	Art. 5 and 6 CCA
Misuse of devices (Art. 6)	Art. 9 CCA
Forgery (Art. 7)	General criminal law provisions apply
Fraud (Art. 8)	General criminal law provisions apply

<sup>2</sup> [http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy\\_activity\\_sri\\_lanka\\_apr\\_11/2079\\_south\\_asia\\_wsrep\\_v2%20\\_20april11.pdf](http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_activity_sri_lanka_apr_11/2079_south_asia_wsrep_v2%20_20april11.pdf).

<sup>3</sup> [http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Docs2013/2571\\_Sri%20Lanka\\_ws%20\\_agenda\\_v3.pdf](http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Docs2013/2571_Sri%20Lanka_ws%20_agenda_v3.pdf).

<sup>4</sup> <http://www.icta.lk/pdf/ComputerCrimesActNo24of2007.pdf>.

<sup>5</sup> For the background and additional information see:

[http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079if09pres-SriLanka\\_Jayantha.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079if09pres-SriLanka_Jayantha.pdf).

Child pornography (Art. 9)	Art 286A, B and C Penal Code as amended [further laws are under consideration]
Copyright and related rights (Art. 10)	Intellectual Property Act 2003 and implementing regulation of 2006 as amended
Attempt, aiding and abetting (Art. 11)	Art. 11, 12 and 13 CCA
Corporate liability (Art. 12)	Art 30. CCA
<b>Procedural law</b>	
Scope (Art. 14)	The CCA complements the Code of Criminal Procedure which may also be used to investigate offences under the CCA. Art. 26 for admissibility of evidence
Safeguards and conditions (Art. 15)	(See below)
Expedited preservation (Art. 16)	Art. 19 CCA
Expedited preserv. & partial disclosure (Art. 17)	No specific provision but Art 19 combination with Art. 18 may apply
Production order (Art. 18)	Art. 23 and 24 CCA
Search and seizure (Art 19)	Art. 18, 21 and 22 CCA
Real-time collection of traffic data (Art. 20)	Art. 18
Interception of content data (Art. 21)	Art. 18 CCA
<b>International co-operation</b>	
Chapter III	Art. 33 – 36 CCA

Sri Lanka, for the past ten years, has systematically built up its legal framework related to information and communication technologies. In addition, the institutional framework was strengthened as part of the Sri Lanka initiative “to develop the economy of Sri Lanka, reduce poverty and improve the quality of life of the people”.<sup>6</sup> In 2006, the Lanka Computer Emergency Readiness Team/Co-ordination Centre (Sri Lanka CERT/CC) was established.<sup>7</sup> Measures against cybercrime are thus part of a broader approach.

Challenges remain with respect to criminal justice capacities, including, in particular, the ability of judges and prosecutors regarding cybercrime and electronic evidence. The ICTA/Council of Europe workshop held in October 2013 confirmed that criminal justice authorities are prepared to co-operate with the Council of Europe in capacity building activities.

As a country having requested accession, Sri Lanka will benefit from support under the joint project of the European Union and the Council of Europe on Global Action on Cybercrime (GLACY), in particular with respect to judicial training. The resources to back up an invitation to accede through capacity building are thus available.

### 3.2 Safeguards and conditions

Article 15 of the Budapest Convention requires Parties to:

“... ensure that the establishment, implementation and application of 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.”

Article 15 safeguards and conditions have been discussed constructively in the three workshops held in Colombo in 2008, 2011 and 2013.

Under the Computer Crimes Act of 2007, intrusive investigative measures, such as search and seizure of computers or the interception of a communication, are subject to a warrant by a magistrate (see Article 18 CCA).

<sup>6</sup> <http://www.icta.lk/en/e-sri-lanka.html>

<sup>7</sup> <http://www.slcert.gov.lk/>

The Constitution of Sri Lanka stipulates fundamental rights in Chapter III.

Capital punishment is legal and the death sentence continues to be imposed. However, it is not executed. The year of the last known execution is 1976.

Sri Lanka is Party to a number of international human rights treaties such as the International Covenant on Economic, Social and Cultural Rights, the International Covenant on Civil and Political Rights, the Convention on the Rights of the Child, the Convention against Torture and Cruel, Inhuman or Degrading Treatment of Punishment and others.

At the same time, human rights concerns persist, primarily in relation to the accountability for abuses at the close of the civil war in 2009.

#### **4. Conclusion**

The authorities of Sri Lanka for more than ten years have built up a legal and institutional framework in order to make use of information and communication technology for economic development and poverty reduction. Measures against cybercrime are an important part of this approach.

Sri Lanka, since 2008, has been closely co-operating with the Council of Europe in cybercrime matters and several events have been organised in Colombo. This experience suggests:

- the legislation of Sri Lanka, in particular through the Computer Crimes Act of 2007, appears to be largely in line with the Convention on Cybercrime. Sri Lanka would be a Party with the capability to co-operate effectively;
- Sri Lanka can serve as a bridge to stronger co-operation with other countries of South Asia in cybercrime matters;
- while human rights concerns persist in areas not necessarily related to cybercrime, co-operation in (technical) cybercrime matters may serve as one avenue for international co-operation with Sri Lanka;
- capacity building activities on cybercrime and electronic evidence – including the training of judges – may help further strengthen Article 15's safeguards.

In case of need for additional information please 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](mailto:alexander.seger@coe.int)



## Appendix 3

### Convention on Cybercrime

**CETS No.: 185**

Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States

#### Opening for signature

Place: Budapest  
Date : 23/11/2001

#### Entry into force

Conditions: 5 Ratifications including at least 3 member States of the Council of Europe  
Date : 1/7/2004

**Status as of: 5/11/2014**

Member States of the Council of Europe

	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/6/2002	1/7/2004				X			
Andorra	23/4/2013									
Armenia	23/11/2001	12/10/2006	1/2/2007				X			
Austria	23/11/2001	13/6/2012	1/10/2012		X	X	X			
Azerbaijan	30/6/2008	15/3/2010	1/7/2010		X	X	X	X		
Belgium	23/11/2001	20/8/2012	1/12/2012		X	X	X			
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006				X			
Bulgaria	23/11/2001	7/4/2005	1/8/2005		X	X	X			
Croatia	23/11/2001	17/10/2002	1/7/2004				X			
Cyprus	23/11/2001	19/1/2005	1/5/2005				X			
Czech Republic	9/2/2005	22/8/2013	1/12/2013		X	X	X			
Denmark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Estonia	23/11/2001	12/5/2003	1/7/2004				X			
Finland	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Georgia	1/4/2008	6/6/2012	1/10/2012			X				
Germany	23/11/2001	9/3/2009	1/7/2009		X	X	X			
Greece	23/11/2001									
Hungary	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Iceland	30/11/2001	29/1/2007	1/5/2007		X		X			
Ireland	28/2/2002									
Italy	23/11/2001	5/6/2008	1/10/2008				X			
Latvia	5/5/2004	14/2/2007	1/6/2007		X		X			
Liechtenstein	17/11/2008									
Lithuania	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003	16/10/2014	1/2/2015				X			
Malta	17/1/2002	12/4/2012	1/8/2012			X				
Moldova	23/11/2001	12/5/2009	1/9/2009			X	X	X		
Monaco	2/5/2013									
Montenegro	7/4/2005	3/3/2010	1/7/2010	55	X		X			
Netherlands	23/11/2001	16/11/2006	1/3/2007				X	X		
Norway	23/11/2001	30/6/2006	1/10/2006		X	X	X			

	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Poland	23/11/2001									
Portugal	23/11/2001	24/3/2010	1/7/2010			X	X			
Romania	23/11/2001	12/5/2004	1/9/2004				X			
Russia										
San Marino										
Serbia	7/4/2005	14/4/2009	1/8/2009	55			X			
Slovakia	4/2/2005	8/1/2008	1/5/2008		X	X	X			
Slovenia	24/7/2002	8/9/2004	1/1/2005				X			
Spain	23/11/2001	3/6/2010	1/10/2010			X	X			
Sweden	23/11/2001									
Switzerland	23/11/2001	21/9/2011	1/1/2012		X	X	X			
The former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005				X			
Turkey	10/11/2010	29/9/2014	1/1/2015							
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			
United Kingdom	23/11/2001	25/5/2011	1/9/2011		X		X			

#### Non-members of the Council of Europe

	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Argentina										
Australia		30/11/2012 a	1/3/2013		X		X			
Canada	23/11/2001									
Chile										
Colombia										
Costa Rica										
Dominican Republic		7/2/2013 a	1/6/2013			X	X			
Israel										
Japan	23/11/2001	3/7/2012	1/11/2012		X	X	X			
Mauritius		15/11/2013 a	1/3/2014				X			
Mexico										
Morocco										
Panama		5/3/2014 a	1/7/2014				X			
Philippines										
Senegal										
South Africa	23/11/2001									
Tonga										
United States of America	23/11/2001	29/9/2006	1/1/2007		X	X	X			

Total number of signatures not followed by ratifications:	9
Total number of ratifications/accessions:	44

#### Notes:

(55) Date of signature by the state union of Serbia and Montenegro.

a: Accession - s: Signature without reservation as to ratification - su: Succession - r: Signature "ad referendum".

R.: Reservations - D.: Declarations - A.: Authorities - T.: Territorial Application - C.: Communication - O.: Objection.

Source: Treaty Office on <http://conventions.coe.int> – \* Disclaimer