THE IMPACT OF THE BUDAPEST CYBERCRIME CONVENTION ON SRI LANKAN LEGAL SYSTEM

Jayantha Fernando[1]
Director / Legal Advisor
ICT Agency of Sri Lanka

1. Introduction

On 1st September 2015, Sri Lanka became a state party to the Council of Europe Convention on Cybercrime (ETS 185 of 2001), better known as the "*Budapest Convention*" (and sometimes referred to as the "*Cybercrime Convention*")[2]. This was a historic policy achievement, because Sri Lanka became the first country in South Asia[3] (the 2nd country after Japan, in Asia) and the fastest, (according to Council of Europe records), to accede to this important Convention[4].

The Budapest Convention is the only international legally binding treaty on Cybercrime in the world today and seeks to harmonize national laws, adopts improved investigative powers based on international standards, enhances criminal justice cooperation among State Parties in order to effectively combat the threat against cybercrime and also deals with electronic evidence issues at a global scale. Over the years it has had a tremendous impact as well as influence internationally and is considered the de facto legal standard to bench mark legislation on cybercrime and electronic evidence worldwide[5].

In an era where there is rapid adoption of digitization strategies and use of cloud based services by financial services sector, legal measures to combat Cybercrime and gather electronic evidence for successful investigation and prosecution of cybercrime cases is an important consideration. This article illustrates the nature and scope of cybercrime and its challenges, the significance of the Cybercrime Convention; its features and its impact both from a global as well as Sri Lankan legal context, and how the said Convention can be used as a tool for criminal justice cooperation at an International level

2. The nature and scope of Cybercrime

In November 1988, computer users globally were struck by one of the first large-scale malware attacks, known as the "Morris Worm", which paralysed an estimated 10% of all computers connected to the internet. This singular incident motivated the creation of CERTs

(Computer Emergency Readiness Teams), dedicated to cyber-security and information security incident/ threat management & mitigation now spread at a global scale[6].

The internet itself has gone through dramatic changes since then. In the late 1980s, it connected about 60,000 computers. Today there are about 3.2bn Internet users, roughly 40% of the world's population. By 2020, every single electronic device we use, including smart phones, tabs, watches, pace-makers & health related devices, washing machines and even refrigerators would have a distinct Internet Protocol (IP) address[7], and with such devices connected to the Internet, the "number of connected devices" is expected to reach 50bn. Attacks on these devices could damage the core functions of society, threatening the health and well-being of citizens and the security of any state.

Predictions are that cybercrime will grow significantly in 2016 and beyond. Reasons include technical vulnerabilities which may affect hundreds of millions of users and the security of organisations. Examples exposed in recent times are mobile malware threats[8], defects such as Heartbleed[9], the hacking of the UMTS standard for mobile phone communications[10], the cloning of biometric data such as fingerprints[11] or irises[12] or concerns over the security of cloud services for the storage of data[13].

Big data and "Internet of things"[14] create further risks to security and privacy under new business models created on the Internet, which relies increasingly on the exploitation of personal data. Such data although collected for business purposes, may be used for criminal purposes, such as harvesting data through new forms of criminal trends, such as "*crime-as-a-service*"[15]. New forms of electronic payments, including mobile money, provide new opportunities for fraud and financial crime.

Reportedly, trillions of security incidents are noted on networks each year[16] and millions of attacks against computer systems and data are recorded every day[17]. Cybercrime is a primary concern to governments, societies and individuals[18]. Cybercrime also has a tremendous economic cost and undermines human development opportunities through ICT[19].

Some estimates suggest that the global economic loss from cybercrime is reaching hundreds of billions (USD) per year, although no clear estimates are possible due to lack of reporting. Cybercrime is also a threat to international peace and stability and military conflicts and political disagreements are increasingly accompanied by cyber attacks[20].

Therefore, in our contemporary Internet era cybercrime is a reality. It is not just a matter of attacks against machines but a threat to the core values of democratic societies[21]. Cybercrime has no boundaries and throughout the world this is illustrated by the proliferation of private data theft[22]; committed through cyber-attacks against the media, civil society organisations, parliaments and individuals; denial-of-service attacks against public institutions and critical

infrastructure[23]; sexual violence against children; xenophobia, racism and recent trends in Internet based radicalization[24]; and terrorist misuse of information technologies.

The foremost challenge is that in addition to gathering evidence on cybercrime offences (ie offences against and by means of computers) other crime investigations increasingly require access to electronic evidence stored on computers and electronic devices, including on servers somewhere on the Internet (most often referred to as "evidence in the cloud")[25]. Since the Internet has challenged traditional notions of jurisdictional boundaries, electronic evidence trail in an investigation would not be confined to one state or territory. As such, electronic evidence is volatile and securing it for criminal justice purposes is fraught with technical, practical and legal complexities.

Governments cannot argue the problems away. They have an obligation to protect society and individuals against crime in cyberspace. Progress has been made in recent years, across the world, to establish the required legal frameworks[26], set up specialised cybercrime units at police[27] and prosecutorial services, and intensify international cooperation.

Although it has been difficult to agree on a meaningful definition of cybercrime there is unanimous agreement on the classification of Cybercrime and that such offences are transnational and multi-jurisdictional in nature[28]. Therefore, the effective fight against cybercrime requires a country investigating a crime to obtain electronic evidence stored on computer systems and networks in other countries. The Budapest Convention on Cybercrime serves as an effective tool for criminal justice cooperation in this regard for a growing number of countries.

3. Background and Key Provisions of the Budapest Convention

In April 1997, the Council of Europe embarked on the adoption of a Convention on the subject of Cybercrime, which its Member States would have a legal obligation to implement. In November 2001, the Council of Ministers adopted the 'Council of Europe Convention on Cybercrime ETS 185'[29] ('Cybercrime Convention'), which was opened for signature in Budapest on 23 November 2001. The Convention entered into force as of the 18 March 2004,

However, the most significant aspect which enhanced the international status of the Convention was that four non-members of the Council of Europe, namely, the United States, Japan, South Africa and Canada, were involved in the drafting process and subsequently became signatories[30]. The Convention also contains a provision whereby other non-members may be invited by the Council of Europe to accede, provided there is "unanimous consent of the contracting states" to admit a non-member Country into the Convention"[31].

The Cybercrime Convention consists of four chapters[32]:

Chapter I, titled "Use of terms" includes definitions of "computer system," "computer data," "service provider," and "traffic data."

Chapter II, titled "Measures to be taken at the national level," consists of three sections: "Substantive criminal law" (Section 1), "Procedural law" (Section 2), and "Jurisdiction" (Section 3). All sections in the Convention are further subdivided into "Titles." The section on substantive criminal law is divided into five titles with the first four titles classifying offenses which constitute Cybercrime, namely :-

"Offences against the confidentiality, integrity and availability of computer data and systems" which include offenses such as illegal access, illegal interception, data interference, system interference, and misuse of devices.

"Computer related offences " which include forgery and fraud.

"Content-related offences" which include offences related to child pornography.

"Offences related to infringements of copyright and related rights."

Section 2 on procedural law includes "Common provisions" (Title 1) that apply to the Convention's articles on substantive criminal law, "other criminal offences [sic] committed by means of a computer system," and to "the collection of evidence in electronic form" relating to criminal offences. There is also a title on "Expedited preservation of stored computer data" and includes provisions dealing with "Production order," "Search and seizure of stored computer data," "Real-time collection of traffic data," and "Interception of content data."

Chapter III on "International co-operation" includes general principles relating to "international cooperation," "extradition," "mutual assistance," and "spontaneous information." The chapter also contains procedures pertaining to "requests for mutual assistance in the absence of applicable international agreements" and to "Confidentiality and limitation on use" including "Specific Provisions (Section 2) on "Mutual assistance regarding provisional measures," (Title 1), "Mutual assistance regarding investigative powers," (Title 2) and on a "24/7 Network."[33]

Chapter IV titled "Final provisions" contains standard provisions found commonly in Council of Europe treaties. Importantly, in accordance with Article 40, any state may "declare that it avails itself of the possibility of requiring additional elements" as provided for under certain articles.

The Convention uses technology-neutral language, so as to enable it to be applied in respect of both current and future internet based technologies. Offenses must be committed intentionally for criminal liability to arise. Additional specific intentional elements only apply to certain offenses—for instance, to computer-related fraud, with the requirement of fraudulent or dishonest intent of procuring economic benefit.

The transnational nature of cybercrime can give rise to complex jurisdictional issues; involving persons and electronic evidence located in many different countries. Even where the suspect and his electronic devices are located in the same jurisdiction, relevant electronic evidence may reside on a server located in another jurisdiction, such as a "Yahoo", 'Hotmail' or "Gmail" account. In terms of locating cybercrime, the transnational dimension encompasses both the commission of offences and the obtaining and collation of evidence used in the prosecution of such offences. As mentioned previously, traditional concepts and principles are sometime challenged by the nature of the technologies involved.

Under international criminal law the general principle is that a crime committed within a State's territory may be tried there, although the territoriality of criminal law does not coincide with territorial sovereignty[34]. Under English law, the general principle for determining jurisdiction is where the actus reus is completed[35]. This echoes the civil law principle lex loci delicti commissi, whereby torts are governed by the law of the place where the act was committed[36].

The Cybercrime Convention addresses this by stipulating that "jurisdiction" may be invoked by a State Party if the Cybercrime offences are committed, (a) in the territory of the State Party; or (b) on board a ship flying the flag of that Party; (c). on board an aircraft registered under the laws of that Party; or (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State[37].

The Convention covers both substantive and procedural aspects of Cybercrime, which state parties are obliged to implement, and also enables international criminal justice cooperation. The comprehensive nature of the Convention, as well as the geographical spread of its signatories, means it is likely to remain the most significant international legal instruments in the field for the foreseeable future.

4. Article 15 Safeguards under the Convention

Articles 14 to 21 of the Budapest Convention cover procedural aspects of Cybercrime enabling law enforcement authorities with effective tools to investigate cybercrime and collect electronic evidence. Article 14 defines the scope of procedural provisions.

However, Article 15 stipulates that the procedural powers adopted by Parties to the Convention are to be "subject to conditions and safeguards provided for under its domestic law which shall provide for the adequate protection of human rights and liberties..."[38]. The safeguards and conditions in Article 15 are required to be applied with respect Articles 16-21 of the Budapest Convention. Articles 16 to 21, state that "the powers and procedures referred to in this article shall be subject to Articles 14 and 15[39]

Thus, Article 15 of the Budapest Convention is an important safeguard founded on the basic tenets of Rule of Law, establishing principles and requirements that should be followed to ensure that State Parties to the Convention meet their positive obligation to protect people and their rights against cybercrime while at the same time respecting their fundamental rights when investigating offences.

As pointed out in the Explanatory Report[40] to the Convention, it is recognized that Article 15 conditions and safeguards are governed by domestic law and since Parties to the Convention represent "many different legal systems and cultures", the said conditions and safeguards cannot be defined in detail. However, Parties must adhere to certain principles. "These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments". For member States of the Council of Europe the main instrument applicable is the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Protocols to which they are Party, as well as the case law of the European Court of Human Rights.

The European Court of Human Rights has delivered a series of judgments directly or indirectly referring to Internet or information technologies. A large number of judgements, while not specifically referring to the Internet or cybercrime, are related to procedural powers of law enforcement authorities, such as search and seizure or interception of communications[41]. These cases provide further guidance on the fundamental principles to be respected under Article 15.

Many judgments are related to Article 8 of the European Convention on Human Rights (respect for private and family life). The primary objective of this article is to protect the individual against arbitrary interference by public authorities. This covers the protection of personal data[42], which is of fundamental importance, as well as the privacy of mail, telephone, email and other forms of communication. In K.U. vs Finland[43] specific reference was made to the procedural provisions contained in the Budapest Convention[44] and the need to ensure cooperation between service providers and criminal justice authorities to serve the interest of Justice.

In relation to Non-Member states of the Council of Europe this area is addressed when supporting countries in the implementation of the Budapest Convention through the Council of Europe capacity building programme on cybercrime.

5. Budapest Convention and its Significance as a Tool for Criminal Justice Cooperation

The significance and impact of the Budapest Cybercrime Convention as a tool for criminal justice cooperation may be demonstrated with reference to some recent cases. .

In a sextortion case reported recently to the Sri Lanka Police "High Tech Crime Unit" a suspect used a fake Facebook account to add many women as "friends". The suspect then altered the "friend's" photos and sought to extort money from these victims, threatening to post the photos of victims on the fake account if money's were not paid. Investigators eventually managed to uncover the genuine facebook account of the suspect and arrested him when he came to a hotel to collect a ransom. The matter is still before Courts.

The arrest and recent conviction in April 2016 of two hackers responsible for "SpyEye" Malware is perhaps one of the most successful cases, which saw unprecedented levels of cooperation between 26 international law enforcement agencies and the private sector (such as Dell, Microsoft, Flashpoint etc.), highlighting the effective use of the Budapest Convention. [45].

In order to investigate and prosecute both the above-mentioned cases criminal justice authorities would require access to various types of data. Usually the types of data required for the investigation of above mentioned types of cases may include, "Subscriber information"[46], "Traffic data"[47] and "Content data"[48]. Consequent to an assessment of the mutual legal assistance provisions of the Budapest Convention, the Council of Europe recommended that State Parties should consider a light regime for international requests for a "limited set of subscriber information"[49].

Subscriber information is likely to be held by service providers "offering its services in the territory" of a Party, although in practical terms the information may actually be stored on servers in a jurisdictions outside the usual place of business or country of incorporation of the service provider[50]. Consequently, it may not be always clear to whom a request for subscriber information should be addressed. In this context, Article 18 (1)(b) Budapest Convention offers a practical solution whereby competent authorities of a State Party should be able to request subscriber information from a service provider "offering a service on its territory" irrespective of where the information is actually stored. In other situations, the service provider may be in the territory of the Party but the data may be stored elsewhere. Article 18(1)(a) offers a solution in such instances, requiring a service provider to respond to a lawful production order even if the data is another jurisdiction. The Cybercrime Convention Committee (T-CY) is currently considering a Guidance Note to provide further clarification on Article 18 of the Budapest Convention.

Gaining access to the aforesaid data is getting increasingly more complex due to the corporate policies governing criminal justice cooperation adopted by global service providers (eg:- Google, Yahoo, Microsoft, Facebook and Apple) and also in part due to recent rulings by the European Court of Justice[51], compelling Service Providers based in Europe to carry out more vigorous reviews of law enforcement request for data.

However, a series of measures have been adopted by the Council of Europe under the Budapest Convention over the years[52] to create a framework to facilitate access to such data[53], enabling investigators to identify perpetrators of cybercrime and ensure safer internet

environment for bona fide users. Further, efforts are underway to ensure greater cooperation between global service providers and criminal justice authorities of State Parties to the Convention. For instance, as part of Council of Europe's efforts to clarify the scope of Article 18(1) (b) of the Cybercrime Convention it a "*Hearing on Criminal Justice Access to Electronic Evidence on the Cloud*", on 30th November 2015, where there was a common understanding that, "***clear domestic and international legal frameworks are needed to ensure greater legal certainty for law enforcement and industry and to remove obstacles for businesses***"[54]. Consequent to a detailed discussion with Service Providers, the hearing reached the following conclusions:That current procedures should be improved while building on good practices already available;

The Council of Europe should develop an online tool to facilitate access (a) by law enforcement to policies and tools (such as law enforcement portals) of Service Providers, and (b) by Service Providers to relevant legislation of requesting state parties;

The Cybercrime Convention Committee (T-CY) and Service Providers should explore the preparation of guidelines to facilitate cooperation.

The aforesaid efforts demonstrates that the Budapest Cybercrime Convention is the only International Treaty which facilitates international Criminal Justice cooperation in an effective and foresighted manner and gives Countries the ability to obtain electronic evidence stored on computer systems and networks in other countries. The Convention greatly enhances the gathering of electronic evidence, the investigation of cyber laundering and other serious crimes.

6. Accession to the Budapest Convention by Sri Lanka

Sri Lanka was invited by the Council of Europe to accede to the Budapest Cybercrime Convention on 20th February 2015[55]. The Ministry of Foreign Affairs supported by ICT Agency of Sri Lanka (ICTA) expedited the process[56] and our Instrument of Accession was deposited with the Secretary General of the Council of Europe by Sri Lankan Ambassador to Brussels on 29th May 2015. Thus, Sri Lanka became the first in South Asia and the fastest country to accede to the Convention. This was also first time Sri Lanka became a State Party to an ICT related convention as well as to a European convention.

Sri Lanka's fast track accession to the Cybercrime Convention was possible due to a variety of reasons. Firstly, the Computer Crimes Act No. 24 of 2007[57] was modeled on the Convention and most of its features were based on the said Convention. Thus, Sri Lanka was one of the first Countries in the region to harmonise legislation and demonstrate its commitment to implement the Convention. Secondly, through a number of interventions facilitated by ICTA[58], Sri Lanka actively cooperated with the Council of Europe. Since 2008, ICTA hosted a series of workshops and seminars on cybercrime & electronic evidence related subjects for criminal justice authorities and judges in close cooperation with the Council of Europe and Ministry of Justice. Thirdly, Sri Lanka also demonstrated its commitment and readiness to accede to the Convention by obtaining the

required approvals of the Cabinet of Ministers, both in respect of authorizing the Ministry of Foreign Affairs to make a request to the Council of Europe to be invited to join the Convention as well as to accede when Sri Lanka was invited. Both approvals were obtained in one singular Cabinet Memorandum.

Prior to Sri Lanka's accession, there was an assessment of the Country's cybercrime legislative framework. The assessments carried out by the Council of Europe focused on the manner in which Computer Crimes offences are investigated (especially under Computer Crimes Act & applicable Procedural law). One key assessment was the adequacy of safeguards to match the Council of Europe standards. Sri Lanka was found to have safeguards consistent with the Convention standards and the "unanimous approval" of all state parties was obtained before Sri Lanka could be invited to Accede to the Convention.

Thus, Sri Lanka's substantive offences embodied in Sections 3-10 of the Computer Crimes Act No. 24 of 2007 are based Articles 2-11 of the Convention. Although Section 286A, added to the Penal Code through (Amendment) Act No. 22 of 1995, addresses many of the Child Pornography related offences, efforts are being made to repeal and replace the Obscene Publications Ordinance to fully operationalize Article 9 of the Budapest Convention in Sri Lanka. Although some of the procedural provisions in Part II of the Computer Crimes Act may need to be strengthened based on Article 16-21 of the Convention, provisions have already been made in our law for Interception, real time collection of traffic data as well as to make preservation requests. Such provisions are subject to safeguards consistent with Article 15 of the Budapest Cybercrime Convention[59]. The definitions in the Sri Lankan Cybercrime legislation are also consistent with the Convention and the Mutual Assistance in Criminal Matters Act No. 25 of 2002 has been incorporated by reference into the Computer Crimes Act. Further, the Council of Europe assessment in Sri Lanka found that provisions contained in the Intellectual Property Act No. 36 of 2003 were adequate to meet the requirements imposed under Article 10 of the Budapest Convention.

However, it may be useful to consider some reforms in the long term to ensure that Sri Lanka's legislation is consistent with international best practices. Legislative reforms should keep pace with development in technology and evolving international best practices. For instance a policy decision is required to be made whether the provisions of the Mutual Assistance in Criminal Matters Act No. 25 of 2002 should be made "applicable to state parties to the Budapest Convention". This would ensure effective mutual assistance in cybercrime matters between Sri Lanka and State Parties to the Budapest Cybercrime Convention, using the provisions of the Computer Crimes Act as well as the Convention as an effective tool for criminal justice cooperation at an international level. Further, Sri Lanka may also need to consider formulating regulations under the Act defining the period for data retention, consequent to a review of global best practices.

The Evidence (Special Provisions) Act No. 14 of 1995, which was enacted prior to the Internet era, is another statute which may need to be reviewed in the context of the admissibility of subscriber information, traffic data and content data in criminal proceedings. Despite some of the

archaic provisions requiring notice to be served on parties to enable them to inspect machines and devices etc, the provisions governing presumptions in Section 9 as well as "*Casus Omisus*" provisions in Section 3 may be invoked to admit such evidence in criminal proceedings.

The Budapest Cybercrime Convention is a criminal justice convention and therefore it is a criminal justice response to cybercrime offences. The Convention does not deal with Internal Security & Intelligence matters, which in most countries (including Sri Lanka) are dealt with under other laws. Internal Security & intelligence laws deal with prevention etc, whereas Cybercrime laws deal with investigations after an offence is committed and a complaint is formally lodged.

Some concerns have been raised whether "warrantless wiretapping" would be legitimized or enhanced because of the Interception provisions contained in Section 18 of the Act. A close review of the Computer Crimes Act of Sri Lanka would show that, it is the exception rather than the rule. Under the provisions of the Computer Crimes Act, a Magistrate's Court order is a "sine quo non" for such interceptions, thus, meeting the standards prescribed by the Budapest Cybercrime Convention. So called "*warrantless wiretaps*" (Interceptions) in most countries take place under national security provisions by gaining access to telecommunication systems using security related regulatory regimes.

Finally, an advantage of Sri Lanka becoming a state party to the Convention is that it will be under regular review, both in terms of compliance with the Convention and use of its provisions, through the work of the Cybercrime Convention Committee (T-CY). As a result Sri Lanka will be obliged to improve on its practices.

Reaching improvements on investigative practices with better human rights safeguards was one of the objectives, when the Government pushed for Sri Lanka's accession to this Convention, also in view of a better and safer criminal justice system in the long term. Accession to the Convention has created a paradigm shift in the manner in which the investigation of cybercrime offences are carried out and also set the stage for data protection and privacy legislation to be enacted, drawing on European best practices thus, enabling Sri Lanka to meet the "*adequacy standards*" for smooth transborder flows of data.

7. Conclusions

The text of the Budapest Cybercrime Convention has remained unchanged since its adoption in 2001 and the Convention will be celebrating its 15th Anniversary in November (2016). Through Guidance Notes, representing "the common understanding of the Parties" – and which are negotiated and adopted by the T-CY – the Convention is kept up to date and shows how it can address phenomena and situations that may not have existed at the time when the treaty was drafted.

The "Cloud Evidence Working Group" of the T-CY is currently identifying additional solutions to address the challenge of evidence in on cloud servers. Solutions may include an additional Protocol. The triangle of (a) standards (the Budapest Convention), (b) follow up (Cybercrime Convention Committee, T-CY) and (c) capacity building (through the Cybercrime Programme Office of the Council of Europe in Bucharest, Romania) represents a dynamic approach to the ever-evolving challenge of cybercrime and electronic evidence. The recent 3-0 decision in the Microsoft Case (delivered by the 2nd US Circuit Court of Appeal in Manhattan on 14th July 2016) makes the on-going work of the T-CY more relevant, although the verdict is regarded as a defeat for Criminal Justice authorties and a victory for privacy advocates and technology companies offering cloud computing services around the world[60].

Accession to the Budapest Convention significantly enhances the ability of Sri Lanka to carry out successful investigation and prosecution of cybercrime and other offences involving electronic evidence. It facilitates law enforcement and judicial cooperation at international level with other Parties to this treaty. And at the same time it helps ensure that human rights and rule of laws requirements are met. Protecting individuals and their rights in cyberspace is the leitmotif of this Convention.

Reference

1 Director/ Legal Advisor, ICT Agency of Sri Lanka, Chairman, LK Domain Name Registry, "Cloud Evidence Group" member and "Bureau Member", The Cybercrime Convention Committee (T-CY), Council of Europe

2 Council of Europe Convention on Cybercrime, Nov. 11, 2001, E.T.S. No. 185, available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=1&DF=01/09/2009&CL=ENG

3 http://www.ft.lk/article/465871/Sri-Lanka-becomes-first-South-Asian-country-to-adopt-Cybercrime-Convention

4 As per the Rules of the Convention, a country has to be "invited" by the Council of Europe to join. On 4th April 2014 Sri Lanka expressed its wish to be invited to accede. On 20th February 2015 Sri Lanka was "invited to accede" and deposited the Instrument of Accession on 29th May 2015. Philippines was invited to join in 2008 and will become the 3rd country in the Asian region to become a State Party to the Cybercrime Convention in 2016. Relevant domestic laws have been enacted, consistent with the Budapest Convention and as a Country generating over USD 20 Billion from the IT/BPO Sector it has demonstrated its Commitment to implement the Convention.

5 As at 1st August 2016, the Budapest Cybercrime Convention has 49 State Parties, including Australia, Canada, Israel, Japan, Mauritius, Sri Lanka and USA. 14 countries in Latin America, Asia-Pacific & Africa have been invited to accede and another 7 countries have signed the Convention. Over 130 countries have Legislation based on or inspired by the Budapest Convention (See, Supra, Note 3)

6 Sri Lanka's own national CERT (Sri Lanka CERT:CC) was established by ICTA in 2006 (www.slcert.gov.lk). It was one of the first South Asian CERTs to become a full member of the global "Forum for Incident Response and Response Teams" (See www.first.org) as well as Asia Pacific CERT (www.apcert.org)

7 Internet Service Providers keep logs of IP addresses assigned to a connected device. IP addresses, in principle, allow the identification of a connected device in a network. Such a traceback to a device and through the device to a user is essential in a criminal investigation. Given the limited number of available addresses under Internet Protocol Version 4 (IPv4), for many years now, ISPs often do not allocate a stable (static) IP address to a specific device of an endcustomer, but a range of

IP addresses is assigned to an edge-network where IP addresses are then dynamically assigned to devices as they log on to the edge-network.

8 See joint study of Kaspersky Lab and Interpol (October 2014) on mobile phone threats at: http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2014/10/report_mobile_cyberthreats_web.pdf

9 http://blogs.mcafee.com/consumer/what-is-heartbleed

10 See http://www.sueddeutsche.de/digital/mobilfunkstandard-umts-ultimativer-abhoeralbtraum-1.2281898 and also see http://www.sueddeutsche.de/digital/abhoeren-von-handys-so-laesst-sich-das-umts-netz-knacken-1.2273436-2

11 http://www.bbc.com/news/technology-30623611 and also see http://www.macrumors.com/2014/12/29/ccc-reproduce-fingerprints-public-photos

12 example see http://www.heise.de/security/meldung/31C3-CCC-Tueftler-hackt-Merkels-Iris-und-von-der-LeyensFingerabdruck-2506929.html

13 See http://www.denverpost.com/breakingnews/ci_26452892/apple-says-some-celebrity-accounts-compromised and also see http://arxiv.org/pdf/1404.2697v1.pdf

14 See http://www.ft.com/cms/s/0/685fe610-9ba6-11e4-950f-00144feabdc0.html#axzz3QULEgVI1 and see also http://drivingsalesnews.com/bmw-companies-want-our-driver-data/

15 See latest News item from Europe, dated 1st October 2016 on the use of the "Dark Net" to provide criminal services on the Internet - http://www.news18.com/news/tech/cybercrime-as-a-service-europol-hints-at-militants-usingdarknet-1297646.html

16 http://www.symantec.com/deepsight-products/

17 See for example http://www.sicherheitstacho.eu/?lang=en

18 http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

19 For links between cybercrime and human development see http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/cyber%20CB_v1y.pdf

20 For example See http://www.bbc.com/news/world-europe-30453069 https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf

21 For Example in the days following the "Charlie Hebdo" tragedy on 7th January 2015, more than 20,000 websites In France were under attack http://www.lefigaro.fr/secteur/high-tech/2015/01/15/01007-20150115ARTFIG00333-lafrance-face-a-une-vague-sans-precedent-de-cyberattaques.php

22 See http://www.zdnet.com/pictures/2014-in-security-the-biggest-hacks-leaks-and-data-breaches/ http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

23 The Sony attacks of November/December 2014 is an example. http://www.nbcnews.com/storyline/sony-hack/sony-hack-most-serious-cyberattack-yet-u-s-interests-clapper-n281456 http://www.bbc.com/news/entertainment-arts-30512032

24 See http://www.liberation.fr/monde/2014/09/14/la-radicalisation-des-futurs-jihadistes-est-rapide-la-plupart-sont-des-convertis_1100395

25 For more details See T-CY(2015) 10 "Criminal Justice Access to Data in the Cloud : Challenges – Discussion Paper", prepared by the CEG of TCY – May 2015

26 In Sri Lanka, the Computer Crimes Act No. 24 of 2007 was enacted along with legislation such as Payment Devices Frauds Act No. 30 of 2006

27 Eg:- the proposed "High Tech Crime Unit" for the Sri Lanka Police (2015)

28 For a detailed description See Walden, Ian, ***"Computer Crime & Information Misuse***", pp. 681, Chapter 12 in *Computer Law* (7th edition, eds. Reed and Angel), Oxford University Press, 2011

29 *Supra*, Note 3

30 As at 1st February 2016, Canada, Japan & United States have ratified the Budapest Convention while South Africa is in the process of ratifying the said Convention

31 See Article 37 of the Budapest Cybercrime Convention

32 *supra* note 3.

33 The Sri Lankan 24/ 7 contact point under Article 35 is the IT Division of the Sri Lanka Police 34 Cassese, A., *International Criminal Law*, Oxford University Press (2003), page 277 35 *Manning* (1998) 2 Cr App R.

36 Walden, I., and E. McCormack, "Retaining and accessing communications data", pp. 220-224, *Communications Law*, vol. 8, no. 2, 2003

37 Article 22 of the Budapest Cybercrime Convention. This formed the basis for Section 2 of the Computer Crimes Act No. 24 of 2007

38 See Also para 142-144 of the Explanatory report of the Budapest Convention.

39 The Preamble of the Budapest Convention states the need for a balance between law enforcement interests and respect for fundamental human rights as well as the right to the protection of personal data 40 *supra*, Note 35

41 As a search of the database of the Court will show.
Http://cmiskp.echr.coe.int/tkp197/search.asp?sessionid=78598907&skin=hudoc-en

42 S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 41, 4 December 2008

43 No. 2872/02 of 2nd December 2008, See http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=843777&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649

44 In addition to the Budapest Convention the Court referred also to the following:
"A global conference "Cooperation against Cybercrime" held in Strasbourg on 1-2 April 2008 adopted "***Guidelines for the cooperation between law enforcement and internet service providers against cybercrime***." Their purpose is to help law enforcement authorities and Internet service providers structure their interaction in relation to cybercrime issues. In order to enhance cyber-security and minimise use of services for illegal purposes, it was considered essential that the two parties cooperate with each other in an efficient manner. The guidelines outline practical measures to be taken by law enforcement agencies and service providers, encouraging them to exchange information in order to strengthen their capacity to identify and combat emerging types of cybercrime. In particular, service providers were encouraged to cooperate with law enforcement agencies to help minimise the extent to which services are used for criminal activity

45 https://www.justice.gov/usao-ndga/pr/two-major-international-hackers-who-developed-spyeye-malware-get-over-24-years-combined

46 "Subscriber information" is essential to identify the user of a specific Internet Protocol (IP) address or, vice versa, the IP addresses used by a specific person. Identifying the subscriber of an IP address is the most often sought information in domestic and international criminal investigations related to cybercrime and electronic evidence. (The term "Subscriber

information" is defined in Article 18.3 Budapest Convention). Subscriber information also includes data from registrars on registrants of domain names.

47 "traffic data" has been defined in Article 1(d) of the Convention as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service". Traffic data helps determine the physical location of computer systems and users

48 See paragraph 209 of the Explanatory Report of the Budapest Convention – "Content Data" is not defined in the Convention but refers to the Communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data). Content data (such as an email, images, movies, music, documents or other files) in a cloud context is held by service providers providing services on the territory of a Party although the information may actually be stored on servers in other jurisdictions

49 http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

50 For example, Google has also several data centres in Europe (http://www.google.com/about/datacenters/inside/locations/index.htm, Microsoft has "more than 100 data centres" including in Amsterdam and Dublin http://download. microsoft.com/download/8/2/9/8297F7C7-AE81-4E99-B1DB-D65A01F7A8EF/Microsoft_Cloud_Infrastructure_ Datacenter_and_Network_Fact_Sheet.pdf

51 Ruling of the European Court of Justice on the EU Data Retention Directive - http://curia.europa.eu/juris/document/document.jsf?text=Data%2BRetention&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&c id=305870#ctx1

52 Eg:- In December 2014, the TCY adopted a study on the "Rules on subscriber Obtaining Subscriber Information" and pointed that in domestic information is the most sought out diverse rules and international investigations. The information in Parties subscriber for obtaining subscriber is whereby T-CY as traffic information particular treated the noted addresses),while data requirements in to in some information in (in The relation obtaining way harmonization are others T-CY for dynamic IP procedures for between lower. on recommended subscriber obtaining state the greater rules and subscriber parties conditions, information". http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/TCY(2014)17_Report_Sub_Info_v7adopted.pdf
See also See page123 of http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/TCY(2013)17_Assess_report_v50adopted.pdf

53 For more details See T-CY(2015) 10 "Criminal Justice Access to Data in the CEG Cloud of : Challenges – Discussion Paper", prepared by TCY – May 2015

54 http://www.coe.int/en/web/cybercrime/hearing

55 Consequent to Cabinet Decision, dated 7th March 2014, Sri Lanka sent a request to to the Secretary General of Council of Europe, dated 4th April 2014, expressing its wish to be invited to accede to the Budapest Convention.

56 http://www.dailymirror.lk/73639/icta-helps-fast-track-sri-lanka-s-entry-to-budapest-cybercrime-convention & http://www.ft.lk/article/424633/icta-helps-fast-track-sri-lanka%C3%A2%E2%82%AC%E2%84%A2s-entry-to-budapestcybercrime-convention

57 In addition, other statutes such as the Payment Devices Frauds Act
No. 30 2006, Penal Code (Amendment) Act 16 22 of
1995, Penal Code (Amendment) Act No. 36 of 2003
and the Intellectual Property Act No. 2006 are
also relevant

58 ICT Agency of Sri Lanka (www.icta.lk)

59 Under the Computer Crimes Act No. 24 of 2007, intrusive
investigative measures, such as search and seizure of computers
or the interception by a magistrate (Section 18). The subject
to a warrant Sri Lanka stipulates and guarantees several
Constitution of Rights in Chapter III. Sri Lanka is
Fundamental a number of international human rights also
Party to the International Covenant on Economic, Social treaties
such as Convention on Civil and Political
Cultural Rights, the against Torture Rights and the Child, the
Convention Punishment and others. Inhuman or Degrading Treatment of

60 See - http://www.reuters.com/article/us-microsoft-usa-warrant-idUSKCN0ZU1RJ