SUBMISSION NO. 31

Parliament of Australia
House of Representatives
Standing Committee on Communications

Inquiry into cybercrime

Submission by the Council of Europe[1]

1 Nature and prevalence of e-security risks (item "a" of the ToR)

Given the reliance of societies on information and communication technologies (ICT), societies and individuals are vulnerable to risks. This not only applies to those actively using computer and communication systems but to anybody benefiting from public or private infrastructure. Risks include in particular cybercrime which may involve a combination of the following types of conduct:

- Offences against the confidentiality, integrity and availability of computer data and systems such as
  - illegal access to a computer system
  - illegal interception
  - data interference
  - system interference
  - misuse of devices.

- Offences committed through computer data and systems such as
  - Computer-related forgery and fraud
  - Content-related offences (child pornography, xenophobia, racism)
  - Offences related to intellectual property rights and similar rights.

There seems to be general agreement, that globally the following trends can be observed:

- Cybercrime increasingly takes the form of economic crime targeted at generating illicit proceeds through identity theft and related fraud as well as a multitude of other types of scams
- Offenders are increasingly organising to commit cybercrime
- Spam is spreading not only as a nuisance but as a vector for malware
- A proliferation of child abuse materials and offenders is noted and with it the commercial sexual exploitation of children
- Terrorists use ICT, including
  - for propaganda, fund raising, recruitment and training
  - for logistical purposes such as target identification, communication or money laundering
  - the possible risk of terrorist attacks against critical infrastructure
- Asymmetric conflicts are facilitated through ICT

There also appears to be general agreement that botnets are the key tool for the commission of cybercrime.

---

[1] The Council of Europe comprises 47 European countries and was established in 1949 with the primary aims of promoting human rights, democracy and the rule of law in Europe (www.coe.int).

The reliance on ICT and the nature and prevalence of cybercrime entails particular challenges for criminal justice:

- Evidence not only related to cybercrime but in relation to any crime may be stored on a computer system or a multitude of different devices with increasing storage capacity. And electronic evidence is volatile evidence that needs to be preserved in an urgent and efficient manner while following due process

- Cybercrime is transnational crime. The crime scene is global and the place of action and the crime site are independent of each other. Evidence such as traffic data, subscriber information or content data may be stored in multiple jurisdictions. This problem will be further exacerbated by the trend towards cloud computing. This underlines the need for urgent and efficient action by criminal justice authorities at the international level, as well as a minimum level of harmonization of substantive criminal law provisions

- The investigation of cybercrimes in many cases requires the cooperation between law enforcement and Internet service providers. Such cooperation is necessary but can also be problematical considering the different roles of law enforcement (to uphold the law) and ISPs (to provide services to their clients) and the need for both to protect privacy, freedom of expression and other fundamental rights of internet users

- In 2008 the German Constitutional Court stated that as people rely on ICT to communicate, express themselves and store their private information, the confidentiality, integrity and availability of computer data and systems was a fundamental right. Thus, while criminal justice needs to act efficiently against cybercriminals and protect society and individuals, enhanced and efficient investigative and procedural law tools need to be accompanied by appropriate safeguards and conditions.

2 Legislative and regulatory initiatives (item "d ii" of the ToR)

2.1 The Convention on Cybercrime[2]

The Convention on Cybercrime of the Council of Europe (the so-called "Budapest Convention") helps countries address the above challenges:

- Substantive criminal law measures, that is, conduct that is to be made a criminal offence (illegal access and interception, system and data interference, misuse of devices, child pornography, computer-related fraud and forgery, copy right infringements and others). Countries that are parties to the Convention will in this way have comparable provisions in their law; what is an offence in one country, similarly is an offence in another country. This is a pre-condition for international cooperation. Furthermore, full implementation of articles 2 to 13 means that a country will have comprehensive legislation addressing the types of cybercrime indicated above

[2] See http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG for the Convention, explanatory report, status of signatures and ratifications etc. or www.coe.int/cybercrime for additional information on activities of the Council of Europe in this field.

- Procedural law, that is, measures for more effective and efficient investigations of cybercrime. It should be underlined that the procedural measures of articles 16 to 21 can be used for any criminal offence involving a computer system. For example, they can be used in the case of fraud, terrorism, money laundering, trafficking in human beings, corruption or other serious crimes where ICT are involved. There are very few other international treaties with such a strong focus on procedural law measures. The need to establish appropriate safeguards and conditions while providing law enforcement with efficient tools is addressed in article 15. Several articles refer to the role of service providers. In order to facilitate such cooperation in practice, in April 2008 a global conference on cybercrime organised by the Council of Europe adopted guidelines that have been elaborated by a working of industry and law enforcement representatives.[3]

- Efficient international cooperation with general principles of cooperation (that is, general principles on international cooperation, principles related to extradition, principles related to mutual legal assistance, spontaneous information etc.) as well as specific provisions for more effective cooperation (articles 23 to 35). These permit parties to the Convention to apply procedural tools also internationally. This section provides for the creation of a network of contact points which are available on a 24/7 basis to facilitate rapid cooperation.

While this Convention was elaborated by the Council of Europe, it was from the beginning designed to have a global scope. Some non-European countries participated in the preparation of the treaty and subsequently signed (Canada, Japan and South Africa) or ratified it (USA). Any country can seek accession according to Article 37 and then be invited to accede. So far, Chile, Costa Rica, Dominican Republic, Mexico and Philippines have been invited to accede. It is expected that by the time of accession they have harmonised their legislation with the Convention.

By end June 2009, 26 countries were full parties to the Convention, while an additional 20 had signed it and another 5 had been invited to accede. A further 50 to 70 countries are using the Convention as a guideline and have or are in the process of adapting their cybercrime legislation along the lines of this treaty.

The Convention is supplemented by an "Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems" (CETS 189). Parties to the Convention can also become a party to this protocol.[4]

2.2 Australian legislation

It seems that Australian legislation (in particular Cybercrime Act n°161, 2001) has been inspired by the Convention on Cybercrime (which was opened for signature also in 2001). Many of the substantive law provisions thus appear to be covered, although – perhaps due to the specificities of the Australian legal system – a different approach seems to have been

---

[3] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf

[4] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=&CL=ENG

followed for some of them. For example: in some Australian legal provisions different types of conduct listed in the Convention have been combined (e.g. illegal access, data interference, system interference) or individual provisions of the Convention are reflected in several different provisions in Australia. This is compatible with the Convention but may create difficulties in international cooperation when applying dual criminality.

Amendments to the Criminal Code on child abuse and child pornography material in March 2005 suggest that Australia fully complies with Article 9 of the Convention on Cybercrime.

With regard to procedural law and practice, it seems that some tools (search and seizure, production orders etc.) are available, while others are not (e.g. expedited preservation).

However, with regard to both procedural and substantive law a detailed analysis would be required to assess whether Australian legislation and practice is fully in line with the Convention on Cybercrime. The Council of Europe would be prepared to assist in such an analysis if necessary.

3 International cooperation (item "d iv" of the ToR)

Efficient international cooperation is of crucial importance against the transnational phenomenon of cybercrime and to secure evidence on computer systems. For that reason, the Convention contains a range of general and specific measures to facilitate cooperation and allow the use of domestic measures (such as the expedited preservation) also in relation to international cooperation.

Harmonisation of national legislation with the Convention on Cybercrime is essential. However, in order to make use of this treaty as a framework or legal basis for international cooperation, a country like Australia would have to become a party to it.

Australia has established a 24/7 point of contact (see Article 35 of the Convention) and participates in the network of the G8.

4 Future initiatives to mitigate e-security risks to Australia (item "e" of the ToR)

Full implementation of and accession to the Convention on Cybercrime in the near future would thus bring a number of benefits to Australia and help further mitigate e-security risks:

- It will help Australia to further strengthen its cybercrime legislation and practices and ensure harmonisation and compatibility of Australian criminal law provisions on cybercrime with those of other countries.

- It will provide further tools to Australian law enforcement for the gathering of electronic evidence and tools for the investigation of cyber laundering, cyber terrorism and other serious crime. Through the Convention these tools can also be applied in international cooperation.

- The Convention will serve as a legal basis for international cooperation in cybercrime cases. Parties to the Convention can make full use of the provisions of Chapter III on

international cooperation, which provides the legal basis for international law enforcement and judicial cooperation with other parties to the Convention.

- Although Australia did not participate in the drafting of the Convention, as a Party Australia would participate in the Cybercrime Convention Committee (T-CY). This Committee follows the implementation of the Convention and also initiates future work related to the Convention, such as the preparation of additional protocols etc. This means that Australia would be involved in the elaboration of future international cybercrime standards.

The accession by Australia to the Convention on Cybercrime may also serve as an example to other countries and trigger the strengthening of legislation and practices as well as accession by other countries of the Asia-Pacific region, in particular of those whose legislation has been inspired by Australia (such as Brunei, Malaysia or Singapore).

The accession process would be initiated by a request sent from the Australian Government to the Council of Europe. This request would then be processed by the Council of Europe General Secretariat according to Article 37 (see appendix). Once invited, it would then be up to the Government and Parliament of Australia to complete the internal process that is necessary before depositing the instrument of accession at the Council of Europe. By the time of accession, Australian legislation should be in line with the Convention.

With regard to the sexual exploitation and abuse of children Australia may furthermore want to consider accession to the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201).[5] It would seem that Australia already implemented many of the provisions that are foreseen in this treaty, including "grooming".

With regard to the terrorist use of the Internet, Australia may also consider the Convention on the Prevention of Terrorism (CETS 196)[6]. While the Convention on Cybercrime criminalises possible denial of service attacks (e.g. through botnets) through provisions on data and system interference, and contains investigate tools and means for efficient international cooperation, the Convention on the Prevention of Terrorism also covers issues such as incitement, recruitment and training, defining them, in particular, as criminal offences.

[5] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=7/2/2009&CL=ENG

[6] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=196&CM=8&DF=7/2/2009&CL=ENG

Appendix:

NOTE FOR INFORMATION[7]

Subject : **Accession to the Convention on Cybercrime (ETS No. 185) by States which are not member States of the Council of Europe**

Participation in the Convention on Cybercrime is not exclusively limited to member States of the Council of Europe. The Convention belongs to the "open" ones, open to accession by non-member States, even non-European States, provided that they have been formally invited to accede by the Committee of Ministers of the Council of Europe. The relevant provisions - Article 37(1) of the Convention on Cybercrime - read 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."

The procedure for the accession of a State which is not a member of the Council of Europe may be summarised as follows:

1. In principle, the Committee of Ministers may take the initiative of inviting a non-member State to accede to a specific Convention. It is nevertheless customary for the non-member State to request accession in a letter addressed to the Secretary General of the Council of Europe. The letter should be signed by the Minister for Foreign Affairs or a diplomatic representative acting upon instructions of his or her government.

2. At the request of the acceding State and before formally inscribing the point on the agenda of the Committee of Ministers, the Secretariat may informally ascertain the opinion of Contracting States. It is highly recommended to make use of this informal procedure which has been used frequently in the past.

3. Formal requests for accession are examined by the Committee of Ministers or, where appropriate, by one of its rapporteur groups. Once there is agreement in principle within the Committee to give a positive reply to a request, the Committee of Ministers instructs the Secretariat to consult the other non-member States which are Parties to the Convention in question. The non-member States are given a precise time-limit for the expression of their consent, usually two months.

4. Following the consultation of the non-member States which are Parties to the Convention in question, the decision inviting the non-member State becomes definitive. In the case of the Convention concerned, the invitation has to be unanimously agreed by those States which have ratified the Convention.

5. An invitation to accede to the Convention in question is notified to the State concerned, which, prior to acceding, has to take the necessary measures to ensure that its domestic law allows the Convention to be implemented.

---

[7] Note prepared by the Treaty Office of the Council of Europe.

6. It is customary for the instrument of accession to be deposited at the seat of the Council of Europe in Strasbourg, in the presence of a representative of the acceding State and of the Secretary General of the Council of Europe or his/her deputy. The representative of the acceding State brings with him/her the instrument of accession, and a procès-verbal of deposit is signed by both Parties. Should it prove difficult for the acceding State to send a representative to Strasbourg, the instrument of accession may be sent by diplomatic courier. Deposit of the instrument of accession is notified to the members of the Council of Europe and to the other Parties to the Convention.

7. The Convention has been complemented by an Additional Protocol (ETS No. 189). States having acceded to the Convention may also accede to the Protocol.

8. Subject to the applicable provisions of each treaty and in line with the Vienna Convention on the Law of Treaties, any declarations or reservations are to be made when depositing the instrument of accession. For reasons of legal certainty and in order to ensure the uniform implementation of European conventions, reservations may not be made at any later date.

9. The text of the Convention, its explanatory report, the chart of signatures and ratifications and all declarations and reservations made with regard to it can be consulted on the web site of the Council of Europe's Treaty Office on http://conventions.coe.int