联合国

A/CONF.187/L.10

第十届联合国预防犯罪和罪犯待遇大会

2000年4月10日至17日，维也纳

Distr.: Limited
16 April 2000
Chinese
Original: English

议程项目5
有效地预防犯罪：紧跟新的发展

第二委员会的报告

计算机网络犯罪问题讲习班

导言

1. 2000年4月15日举行了由亚洲和远东预防犯罪和犯罪待遇研究所主办的计算机网络犯罪问题讲习班。讲习班讨论了有关这一议题的背景性文件（A/CONF.187/10）。

2. 该研究所所长 Mikinao Kitada 先生作了介绍性发言。

3. 加拿大司法部长兼总检察长尊敬的 Anne McLellan 女士在主旨演说中注意到国内和跨国计算机犯罪日益严重，并指出了制订有效的法律和程序管制计算机犯罪并避免对新技术正当而有益的作用作不应有的干预的重要性。

4. 讲习班举行了一系列专题小组讨论。第一个专题小组审查了计算机犯罪所涉犯罪学问题。第二个专题小组的讨论是依法搜查和没收计算机网络数据所产生的技术问题和法律问题的主题研究设想方案。第三个专题小组的讨论是多国网络中的计算机通信追查的主题研究设想方案。第四个也是最后一个专题小组的讨论涉及执法与计算机和因特网行业之间的联系。在讨论期间，9个国家的政府代表和17名专家作了发言。*

一般性讨论

5. 与会者指出，新技术的发展为刑事罪犯创造了新的机会。“涉及计算机的犯罪”一词系指下述两种情况：针对计算机、网络及其用户的全新形式的犯罪，及利用或借用计算机设备进行的形式较为传统的犯罪。与会者对打击新的犯罪的法律对策进行了审查。审查时强调指出，鉴于这类犯罪时很容易在跨越国境下进行，所以各国都应制订充分的刑法规定。

6. 与会者注意到，由计算机网络创造的新环境使法律制度中许多传统的假设受到了挑战。会议讨论了更新法律以紧跟技术发展的需要。有的与会者指出，诸如财产、偷窃和占有等法律概念在各国的刑法中普遍适用，但这些概念不一定适用于在性质上属于无形的计

* 专家名单载于本报告附件。

算机数据。数据易于更改这一事实也造成了与数据收集、保存并在法律诉讼中用作证据有关的新的法律问题。

7. 与会者注意到，由于下述原因，对计算机网络进行卓有成效地调查所需的权力和技术也引起了对人权和隐私权的严重关切。这既是因为其具有侵入性，也是因为在计算机网络上储存和传送的个人数据和其他数据很多的缘故。与会者一致认为，今后各国政府面临的根本问题之一是需要在公民个人隐私权和执法需要之间寻求适当的平衡。有的与会者注意到，在一些情况下可能会出现隐私权问题。有些与会者还注意到，某些国家的法律对搜查和拦截传送中的数据与搜查已储存的数据作了区分，而在其他法域中，这种区分可能不很明确。与会者指出，如果数据被视为传送中通信并因此应受拦截，而不是被扣押，则对争取必要批准和有关进行搜查的保障措施需做出更为严格的规定。因此，与会者认为，执法机构搜查的证据可与有关事项的商务记录或医疗记录或第三方的这些记录等其他资料混合起来。

8. 与会者注意到，执法当局试图从因特网服务提供者那里获取信息的情况可能会引起很多问题。其中包括如何找到提供服务的公司中在需要时可与之联络的人的实际问题，以及提供者是否可主动透露资料的法律问题。有的与会者还指出，某些国家的隐私权或数据保护法禁止提供者在未获法院指令的情况下透露有关其客户通信的某些或所有资料，而且，对于提供者是否应保留通信内容或交易记录以便若于以后调查需要时进行查找的问题，法律上也是并不明确的。

9. 有些与会者认为，如果执法机构所要得到的证据在某一合法企业的计算机系统之中，则搜查时如果干扰计算机操作便会对业务造成危害。与会者一致认为，在这种情况下，关键问题是既有效进行搜查又不中断正常的业务操作。

10. 与会者认为，许多计算机犯罪的跨国性可能使情况更为复杂化，更不必说所涉管辖权问题。适用哪一国的法律、进行取证和追查或鉴定罪犯的调查权、引渡罪犯的权力及随之由法院审问罪犯等问题，都在一定程度上要取决于罪行在何处发生；如果犯罪是利用计算机网络技术在一个以上地点进行的，则地点的确定便不明确。举出的一个例子是，一个国家的网址中列有某一其股份在另一国股票交易所进行交易的公司的欺诈性投机交易情况。因此，犯罪可能发生于一个国家、另一个国家或两个国家，或者在两个国家中都未发生，具体情况取决于有关国家的法律。

11. 与会者指出，在搜查人员位于一个法域而证据却在另一法域时，搜查和查抄措施也会变得复杂起来。例如，网络搜查的结果可能涉及存储于另一国的证据，这就出现了是否需要在取证方面获得第二国当局许可或是否应将正在进行这类搜查的事宜通知第二国当局的问题。与会者注意到，在有必要通过正式的司法互助渠道请求协助的情况下，为获得这种协助所需的时间可能相当长。如何使程序迅捷进行的问题，对于处理正在进行中的涉及计算机的犯罪的案件或证据可能在通过现有渠道寻求司法互助所需时间内被销毁的案件，是十分关键的。

12. 与会者注意到，涉及计算机的犯罪的跨国性质及电子数据的易被篡改的问题，是如何确定跨境搜查所获证据的可靠性的问题。这种确定需要规定一套供计算机搜查人员使用的程序或规程，以确保所查询到的数据的可靠性，并要有一套为确定可靠性所需的透明而安全的程序。与会者认为，有些国家可能存在着妨碍使用电子数据作为证据的正式规定。

13. 与会者一般都认为，各国应力求酌情协调统一与刑事定罪、证据和程序有关的规定。

结论

14. 讲习班所得出的结论如下：

(a) 应将涉及计算机的犯罪定为刑事犯罪；

(b) 需要制订对计算机罪犯进行调查和起诉的充分的程序法；

(c) 政府和业界应共同努力实现下述共同目标：预防和打击计算机犯罪，从而使因特网成为一个安全的空间；

(d) 需要改进国际合作，以便追查因特网罪犯；

(e) 联合国应就与计算机网络犯罪有关的技术合作和援助的提供采取进一步的行动。

附件

参加小组讨论的专家

Mr. Shri L. C. Amarnathan, Sikkim Police Headquarters, India

Mr. Cormac Callanan, European Internet Service Provider Association, Ireland

Mr. Peter N. Grabosky, Institute of Criminology, Australian

Mr. Masahito Inouye, University of Tokyo, Japan

Mr. Nigel Jones, Association of Chief Police Officers , United Kingdom of Great Britain and Northern Ireland

Mr. Ekkehart Kappler, Federal Crime Office, Germany

Mr. Henrik W.K. Kaspersen, Professor, Vrije Universiteit Amsterdam, Netherlands

Ms. Margo L. Langford, Barrister and Solicitor, Canada

Mr. Victor Lo, Hong Kong Police Force, China

Mr. Keith Mitchell, London Internet Exchange, United Kingdom of Great Britain and Northern Ireland

Mr. Hans G. Nilsson, Council of the European Union

Mr. Donald K. Piragoff, Department of Justice, Canada

Ms. Mary Riley, United States Secret Service, United States of America

Mr. Gregory P. Schaffer, Computer Security Consultant, United States of America

Mr. Ulrich Sieber, University of Munich, Germany

Mr. Vittorio Stanca, National Computer Crime Unit, Italy

Mr. Michael Sussmann, Department of Justice, United States of America