联合国 A/60/95/Add.1

大会

Distr.: General
21 September 2005
Chinese
Original: English

第六十届会议

议程项目 86

从国际安全的角度来看信息和电信领域的发展

从国际安全的角度来看信息和电信领域的发展

秘书长的报告

增编

目录

05-51876 (C) 071005 071005

二. 从会员国收到的答复

巴西

[原件：英文]

[2005 年 6 月 24 日]

在分析信息和通信技术发展对国际安全的影响时，人们必须首先认识到不能把社会同技术发展之间的关系说成是简单的单方向作用关系。这种关系是基于各种必要性、创造性、企业行动和共同利用技术等各种因素之间的复杂互动关系。21 世纪是一个新纪元的开始，在这个新纪元“信息社会”的兴起看来将决定人类活动的所有领域，从个人活动和社会活动到经济生产和国家治理方式，都将发生深刻转变。

信息已成为各国财富和财产的一个关键组成部分，今天被正确地视为最宝贵的资源之一。私人公司、银行、股票市场和政府组织（包括国防部门）都通过世界范围的信息网络相互联系，这种网络对于经济进步就象电力和供水一样不可或缺。然而，这种高度的、并日益加强的联系也可能成为政府和经济新的易受攻击的薄弱环节，可能被用在军事冲突以及犯罪活动和恐怖主义活动中。

近几十年来，在战争中广泛使用技术和自动化使各国之间的冲突能够更加集中于军事目标，避免造成附带破坏。同时，媒体和组织起来的民间社会对展开军事行动施加了许多压力。现代战争应是“干净”或甚至是“外科手术型”的。

这正符合“计算机网络战争”带来的各种可能性。一些武装部队已部署了特种军事部队，其人员经过训练和配备了有关设备，能够通过信息网络的入侵和破坏，使关键基础设施瘫痪或甚至被摧毁。根据所要达到的目标和采用的手段，这种攻击的作用从对敌人的武器或传感系统进行“软杀伤”直至使全国电力网遭受灾难性摧毁。获得许多此种能力，可能只需要相对较小的投资，这就更提高了这种形式战争的效率。鉴于这些因素，计算机网络战争很可能在不远的将来成为助长国家间军事冲突的因素。恐怖主义组织也会利用这些弱点，可能造成更加严重和更难以预料的有害后果。

尽管从其造成的后果来看规模还比较小，但犯罪分子已在广泛利用这种攻击性信息技术工具：每年都有许多金融机构、企业和政府机构的信息和技术系统受到那些企图非法牟取好处和（或）重要信息的个人或团体的网络攻击。

巴西认识到这个问题对于维护国际和平与安全的重要性，建议从两个不同的方面处理这个问题。第一，国际社会应努力制定适当的措施来对付涉及信息技术的犯罪活动和恐怖主义活动。另一种起补充作用的方式是，考虑到出现计算机网

络战争的影响，以及可能必须在裁军和不扩散制度中以及在关于战争的法律中考虑到计算机网络战争的多方面影响。

考虑到可能出现的恐怖行为和犯罪行为，我们建议联合国带领会员国合作制定以下措施：

- 建立应急和备用网络来保护关键基础设施。
- 检查各自的网络结构，分析相互依赖关系，以及确定有效的保护方法。
- 促进政府同私营部门之间的互动，以期使在各组织之间流动的信息的安全程度达到应有的水平。
- 建立保护制度，以避免或尽可能减轻网络攻击的影响。
- 使用有关工具和措施，使当局能够追踪网络攻击的来源。
- 使国家机构能够对信息系统的安全程度进行检测和评价。
- 谈判和通过一项关于计算机网络罪行的国际公约。
- 推动和开发有关技术，以加强信息安全的手段和方法。
- 保证全体公众能获得现有的信息和信息技术。
- 避免建立可能阻碍各国获得电信和信息系统领域高级技术的机制；
- 建立关于在国家主管机构之间相互通知网络攻击威胁的程序。
- 对公众进行网络安全重要性的教育

关于在国家间冲突中使用信息武器的问题，我们认为联合国应评价是否可能推动缔结关于以下问题的公约：

- 信息战争的识别、其特点和分类。
- 信息武器和可能用作信息武器的各种手段的识别及分类。
- 防止恐怖主义集团利用电脑控制的军事武器或知识。
- 制定关于使用信息武器的行为守则。
- 保证所有国家在保护本国不受网络攻击方面享有平等权利。
- 制定有关国际机制，就与电脑网络侵略有关的冲突解决办法提供指导。
- 建立载有主要信息安全用语的联合国词语汇编。

加拿大

[原件：英文]

[2005 年 8 月 4 日]

信息基础设施是加拿大关键基础设施的一个主要构成部分，这些基础设施包括以下部门：能源和公用事业、通信和信息技术、财政、保健、粮食、水、运输、政府和制造业。所有这些部门都面临同样的确保信息基础设施安全这一挑战，估计其中多达 90%的部门是私人拥有和管理的。加拿大信息基础设施对所有加拿大来说都具有重要意义，因而政府努力维护信息系统的安全和完整，使人们能够利用这些系统。政府还采取步骤防止出现网络事故，对网络中断的任何报告都迅速采取应对措施。

2003 年 12 月，我国总理宣布设立了一个新的公共安全和应急准备部。这个新设立的部把前关键基础设施保护和应急准备办公室、加拿大皇家骑警和加拿大安全情报局这三个负责网络安全的主要联邦机构并入同一个部。公共安全和应急准备部负责检测和分析对政府系统的网络威胁、是接收网络事故报告的中央机构、并向政府各部门发出关于新的威胁和易受袭击的薄弱环节的警报。加拿大安全情报局负责调查对国家安全构成威胁的各种事件。加拿大皇家骑警负责调查任何构成或可能构成犯罪行为的网络事件。此外，通信安全署是处理信息技术安全的技术问题的当局，负责制定系统认证和认可业务标准、进行风险和脆弱性分析、评价产品、维护系统安全以及分析网络安全情况。

2004 年 4 月，加拿大首次颁布了国家安全政策，其中提出旨在对付目前和今后各种威胁的综合战略和行动计划。这项计划特别说明网络安全是维护公共安全方面的一项挑战，并提议建立一个有政府和私营部门代表参加的高级别全国网络特别工作组，以制定一项全国网络安全战略来处理这个问题。特别工作组现正在组建之中。

2005 年 2 月，公共安全和应急准备部设立了一个加拿大网络事故应对中心，作为国家联络中心，协调对网络安全事故采取的应对行动，并监测出现网络威胁的环境。该中心在政府活动中心之外运作，后者每周七天、每天 24 小时都在运作，是加拿大全国应急系统的一部分。

加拿大各省和各领土的工作重点是保护各自的重要基础设施，包括网络系统和这些系统所依靠的联网。现正在制定各省之间的举措，例如建立协作网络监测能力。

私营部门积极参与网络安全倡议。私营部门公司保护自己的关键信息技术基础设施，并通过行业协会在各自行业交流关于网络脆弱环节、各种事故及其解决

办法的信息。各行业协会同公共安全和应急准备部在一个论坛内合作，从而能够在各行业部门之间广泛交流信息。

加拿大还参与关于网络安全的多边倡议。其中包括：八国集团高科技犯罪问题小组，该小组于 1997 年建立，通过了打击计算机犯罪的 10 项原则；欧洲委员会《网络犯罪公约》，其目的是统一各国界定罪行的法律，以及确定处理全球网络问题的调查和起诉程序，并建立一种迅速有效地展开国际合作的制度；美洲国家组织，其成员国商定“将考虑编写相关的美洲法律文书和示范法律，以便加强打击网络犯罪方面的半球合作，并将考虑保护隐私、保护信息、程序问题和预防犯罪方面的各种标准”。