联合国 A/65/201

大会

Distr.: General
30 July 2010
Chinese
Original: English

第六十五届会议

临时议程* 项目 94

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发展政府专家组

秘书长的说明

秘书长谨随函转递从国际安全的角度来看信息和电信领域发展政府专家组的报告。该专家组是根据大会第 60/45 号决议第 4 段设立的。

* A/65/150。

10-46956 (C) 170810 180810

从国际安全的角度来看信息和电信领域发展的政府专家组的报告

摘要

信息安全领域现有和潜在的威胁是二十一世纪最严峻的挑战之一。这种威胁的来源多种多样，表现形式是针对个人、企业、国家基础设施和政府的破坏性活动。其结果给公共安全、国家安全和整个全球链接的国际社会的稳定带来重大危险。

重要基础设施越来越多地使用信息和通信技术(信通技术)，这就造成了新的脆弱性和破坏机会。由于电信和因特网复杂的互连性，任何信通技术装置都可以成为手段日益高超的滥用的来源或目标。由于信通技术固有的双重用途性质，支持繁荣电子商业的技术也可以用来威胁国际和平与国家安全。

破坏的起源、犯罪人身份或动机可能会难以确定。这种犯罪人往往只能从目标、效果或其他间接证据来推断，他们可以在几乎任何地方采取行动。这些特点便利使用信通技术从事破坏性活动。犯罪归属的不确定和缺乏共同理解，造成不稳定和误解的危险。

更多报道说，各国正在将信通技术发展成战争和情报工具，并用于政治目的。日益令人关注的是，有个人、团体和组织，包括犯罪组织代替别人从事破坏性在线活动。犯罪手段越来越高超，范围越来越大，提高了有害行动的潜力。尽管很少有迹象显示恐怖分子利用信通技术实施破坏性活动，但今后可能会增多。

应对二十一世纪的挑战有赖于志同道合伙伴之间的成功合作。各国之间以及国家、私营部门和民间社会之间的协作很重要。改进信息安全的措施必须有广泛的国际合作才能有效。政府专家组的报告就各国之间进一步对话以减少风险和保护国家和国际重要基础设施提出了建议。

目录

秘书长的前言

十年前，我们无法预见信息技术和电信会如何深入我们的日常生活，或我们对它们的依赖会有多大。这些技术创造了一个全球链接的国际社会。这种链接虽然带来了巨大好处，但也带来了脆弱性和风险。

在应对新技术的影响方面取得了相当大的进展。但是任务是艰巨的，我们刚刚开始制定新信息环境所需的规范、法律和合作方式。

考虑到这一点，我任命了一个由来自 15 个国家的专家组成的政府专家组，研究这个领域现有和潜在的威胁，并建议应对方法。我感谢专家组组长和各位专家，他们勤奋和认真工作产生了这份报告，其中扼要说明了问题所在和今后可能的步骤。

大会在加强国家和国际两级的信息技术和电信安全方面可以发挥重要作用。会员国间对话是形成共同看法的关键。务实合作也至关重要，以分享最佳做法、交流信息和建设发展中国家的能力，并减少误解的危险。误解会妨碍国际社会管理网络空间重大事件的能力。

这是今后工作的充实议程。本报告是要朝向建设这些新技术所需的国际安全与稳定框架迈出第一步。我向会员国和广大全球受众推荐这份报告的分析和建议。

送文函

谨此提交从国际安全的角度来看信息和电信领域的发展政府专家组的报告。专家组是根据大会第 60/45 号决议第 4 段在 2009 年设立的。作为专家组组长，我很高兴地告诉你，就报告达成了协商一致。

在题为“从国际安全的角度来看信息和电信领域的发展”的该决议中，大会要求按公平地域分配于 2009 年设立一个政府专家组，继续研究信息安全领域的现存威胁和潜在威胁及为对付这些威胁可能采取的合作措施，以及旨在加强全球信息和电信系统安全的概念。还要求秘书长向大会第六十五届会议提交关于这一研究结果的报告。

按照该决议的规定，任命了来自 15 个国家的专家：白俄罗斯、巴西、中国、爱沙尼亚、法国、德国、印度、以色列、意大利、卡塔尔、大韩民国、俄罗斯联邦、南非、大不列颠及北爱尔兰联合王国和美利坚合众国。专家名单载列于附件。

政府专家组举行了四次会议：第一次是 2009 年 11 月 24 日至 26 日在日内瓦，第二次是 2010 年 1 月 11 日至 15 日在联合国总部，第三次是 2010 年 6 月 21 日至 25 日在日内瓦，第四次是 7 月 12 日至 16 日在联合国总部。

专家组就从国际安全的角度来看信息和电信领域的发展进行了全面深入的意见交流。此外，专家组考虑到在会员国对大会分别题为“从国际安全的角度来看信息和电信领域的发展”的第 60/45、61/54、62/54 和 63/37 号决议提交的答复以及专家组个别成员提供的投入和背景文件中表达的看法。

专家组希望对联合国裁军研究所的投入表示赞赏。该研究所担任了专家组的顾问，其代表是 James Lewis 和 Kerstin Vignard。专家组还希望对担任专家组秘书的秘书处裁军事务厅新闻和外联处新闻干事 Ewen Buchanan 及协助专家组的秘书处其他官员表示感谢。

专家组组长

安德烈·**克鲁茨基赫**(签名)

2010 年 7 月 16 日

一. 导言

1. 信息安全领域现有和潜在的威胁是二十一世纪最严峻的挑战之一。这种威胁可以给经济及国家和国际安全造成很大损害。威胁的来源多种多样，其表现形式是针对个人、企业、国家基础设施和政府的破坏性活动。其结果给公共安全、国家安全和整个全球链接的国际社会的稳定带来重大危险。

2. 信息和通信技术(信通技术)具有独特属性，使各国和其他用户难以应对可能面临的威胁。信通技术无处不在，可以广泛获取。它们本身既不专属民用，也不专属军用，其使用目的主要取决于用户的动机。在许多情况下，网络由私营部门或个人拥有和经营。由于电信和互联网复杂的互连性，任何信通技术装置都可以是手段日益高超的滥用的来源和目标。信通技术的恶意使用很容易隐藏。破坏活动的起源、犯罪人身份或动机可能会难以确定。这种犯罪人往往只能从目标、效果或其他间接证据来推断。威胁行为人可以在几乎任何地方采取行动而在很大程度上不受惩罚。这些特点便利使用信通技术从事破坏性活动。

3. 考虑到这些事态发展对国际安全的影响，联合国大会要求秘书长在政府专家的协助下，研究信息安全领域的现存威胁和潜在威胁以及有关的国际概念，并建议可能的合作措施以加强全球信息和通信系统的安全。

二. 威胁、风险和脆弱性

4. 全球信通技术网络已成为破坏性活动的舞台。破坏动机十分不同，从单纯展示技术实力，到偷窃金钱或信息，或作为国家冲突的延伸。这些威胁的来源包括犯罪分子和可能的恐怖分子之类非国家行为体，以及国家本身。信通技术可用来破坏信息资源和基础设施。由于其固有的双重用途性质，支持强大电子商务的信通技术也可以用来威胁国际和平与国家安全。

5. 许多恶意的工具和方法起源于犯罪分子和黑客的活动。犯罪活动的手段日趋高超，范围越来越大，增加了有害行动的潜力。

6. 到目前为止，很少有迹象显示恐怖分子企图损坏或瘫痪信通技术基础设施或利用信通技术实施行动，但今后可能会增多。目前，恐怖分子大多依靠这些技术来沟通、收集信息、招募、组织、宣传其思想和行动及募捐，但最终可能会利用信通技术实施攻击。

7. 更多报道说，各国正在开发信通技术作为战争和情报工具，并为政治目的服务。犯罪归属的不确定性以及在可接受的国家行为方面缺乏共同理解，可能造成不稳定和误解的危险。

8. 日益令人关注的是，有个人、团体和组织，包括犯罪组织代替别人从事破坏性在线活动。这些代理人，无论动机是经济利益还是其他原因，都可能向国家和非国家行为体提供一系列恶意服务。

9. 重大基础设施越来越多地使用信通技术创造了新的脆弱性和破坏机会。越来越多地使用移动通信设备和网络运行服务也是这样。

10. 各国还担心，信通技术供应链会受到影响或破坏而妨碍正常、安全、可靠地使用信通技术。在信通技术中安装恶意隐蔽功能会破坏对产品和服务的信心，削弱商业信任，并影响国家安全。

11. 不同国家之间不同程度的信通技术能力和安全，增加了全球网络的脆弱性。国家法律和做法的差异会给实现一个安全和抵御力强的数字环境带来挑战。

三. 合作措施

12. 与全球互联网络相关的风险需要协调一致的反应。会员国在过去十年中多次申明，有必要为抵御信通技术安全领域的威胁开展国际合作，以打击犯罪性滥用信息技术的行为，建立全球网络空间安全文化。并促进可以降低风险的其他重要措施。

13. 在过去十年中，国际社会特别是以下组织为打击网络犯罪威胁作出了努力：上海合作组织、美洲国家组织、亚太经合组织论坛、东南亚国家联盟(东盟)区域论坛、西非国家经济共同体、非洲联盟、欧洲联盟、欧洲安全与合作组织和欧洲委员会。各国还为此作出了双边努力。

14. 跨国关注的非犯罪领域应该得到适当的注意，其中包括对与国家利用信通技术有关的国际准则缺乏共识而造成的误解危险，这可能会影响发生重大事故时的危机管理。这要求制订争取在可能的领域加强合作的措施。还可以制订旨在分享最佳做法、管理事故、建立信任、减少风险及提高透明度和稳定性的措施。

15. 随着利用信息和通讯技术进行的破坏活动变得越来越复杂和危险，明显的是，没有一个国家能够单独应对这些威胁。面对二十一世纪的挑战有赖于志同道合的伙伴之间的成功合作。各国之间以及国家、私营部门和民间社会之间的协作非常重要，改进信息安全的措施需要广泛的国际合作才能有效。因此，国际社会应审查是否需要合作行动和机制。

16. 现有的协议纳入了与国家使用信通技术有关的准则。鉴于信通技术的独特属性，可以与时俱进逐渐制订更多的准则。

17. 能力建设对于成功确保全球信通技术安全，协助发展中国家努力加强其重大国家信息基础设施的安全，以及缩小目前的信通技术鸿沟至关重要。必须开展密切的国际合作，才能建设在应对信通技术安全方面可能需要援助的国家的能力。

四. 建议

18. 考虑到信息安全领域现有和潜在的威胁、风险和脆弱性，政府专家组认为有必要建议进一步的建立信任措施和其他措施，以减少信通技术受到干扰所造成的误解风险：

㈠ 各国之间的进一步对话，以讨论与国家使用信通技术有关的准则，降低集体风险并保护关键的国家和国际基础设施；

㈡ 建立信任、稳定和减少风险的措施，以应对国家使用信通技术的影响，包括在冲突中使用信通技术交换国家看法；

㈢ 就国家立法及国家信息和通信技术安全战略和技术、政策和最佳做法进行信息交流；

㈣ 确定支持欠发达国家能力建设的措施；

㈤ 寻求制定与大会第 64/25 号决议有关的共同术语和定义的可能性。

附件

从国际安全的角度来看信息和电信领域的发展政府专家组成员名单

白俄罗斯外交部国际安全和军控司司长
Vladimir N. Gerasimovich 先生

白俄罗斯共和国常驻联合国日内瓦办事处代表团参赞
Aleksandr Ponomarev 先生(第三次会议)

巴西国防部政策、战略和国际事务秘书处
巴西海军陆战队、巴西海军中校
Alexandre Mariano Feitosa 先生

中国外交部军控司副司长
李松先生(第一和第二次会议)

中国外交部军控司副司长
康勇先生(第三和第四次会议)

爱沙尼亚信息技术大学助理教授
Linnar Viik 先生

法国国防和国家安全总秘书处
国家信息系统安全局
国际关系
Aymeric Simon 先生

德国联邦外交部常规武器控制司司长
Gregor Koebel 先生

印度信息技术部印度计算机应急小组高级主任
B. J. Srinath 先生

以色列外交部军控司司长
Rodica Radian-Gordon 女士

意大利部长理事会主席团通信安全部门主任
Vincenzo Della Corte 先生(第一和第三次会议)

意大利部长理事会主席团通信安全部门
Walter Mecchia 先生(第二和第四次会议)

卡塔尔埃米里通信兵部队
陆军信号连连长
Rashid A. Al-Mohannadi 先生(第一次会议)

卡塔尔国防部(工兵)中校
Saad M.R.Al-Kaabi 先生

大韩民国外交和贸易部大使
Lew Kwang-chul 先生

俄罗斯联邦外交部新挑战和威胁司副司长
Andrey V. Krutskikh 先生

南非通信部因特网治理副主任
Palesa Banda 女士(第一次会议)

南非国防部政府信息技术干事
Mario Silvino Brazzoli 少将

大不列颠及北爱尔兰联合王国国家信息保证技术局国际关系小组
Gavin Willis 先生

美利坚合众国国务院网络事务办公室高级政策顾问
Michele G. Markoff 女士