联合国 A/55/140

大 会

Distr.: General
10 July 2000
Chinese
Original: Arabic/English/Russian

第五十五届会议

临时议程*项目 69

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**

目录

页次

一. 导言 2

二. 各国政府的答复 2

约旦 2

卡塔尔 2

俄罗斯联邦 3

* A/55/150。

** 本报告根据会员国提交的材料编写。

一. 导言

1. 大会在其 1999 年 12 月 1 日关于从国际安全的角度来看信息和电信领域的发展的第 54/49 号决议的第 2 和第 3 段内，请所有会员国就下列问题提出它们的意见与评估：(a)对信息安全问题的一般看法，(b)有关信息安全的各种基本概念的定义，包括未经许可干扰或滥用信息和电信系统及信息资源，(c)是否宜订立国际原则，加强全球信息和电信系统的安全，协助打击信息恐怖主义和犯罪，并请秘书长向大会第五十五届会议提交报告。

2. 秘书长于 2000 年 3 月 14 日向会员国发出一份普通照会，请它们依照大会的邀请提出意见。本报告第二章载有迄今各国政府的答复。其他答复收到后将作为本报告的增变印发。

二. 各国政府的答复

约旦

[原件：阿拉伯文]
[1999 年 5 月 16 日]

1. 技术和信息系统的使用在维持稳定与和平方面为国际社会取得了积极成果，但滥用这些新的进展和技术便会：

(a) 鉴于迅速传布的能力，容易组织起其份子散布广大地理区域的恐怖主义网络；

(b) 由于技术复杂性迅速变化以及大多数国家现存法律限制干涉个人通讯的自由，因而难以对现代通讯进行监测。

2. 我们承诺要采取适当措施，对恐怖主义活动进行防范，我们建议如下：

(a) 拟订一项特别紧急法令，准许保安业务进入或部分控制掌管先进系统的那些公司的控制中心；

(b) 同涉及通讯的公司和机构进行协调，推动培训保安业务专家以在危机时刻掌管这些系统；

(c) 支持信息和电信技术部门及其有关的安全概念，提供基础结构及适当培训以增进维持国际和平与安全的工作。

卡塔尔

[原件：阿拉伯文]
[1999 年 5 月 17 日]

1. 间谍：防止未经许可的方面取得全球信息和电信系统的内容。

2. 破坏：防止对全球信息和电信系统的部分或全面破坏。

3. 登记：登记经由全球信息和电信系统发出的信息，包括知识财产。

4. 仿冒：防止经由全球信息和电信系统传送仿冒信息。

5. 保护：发展经由全球信息和电信系统传送信息的电子保护。

6. 立法：为所有电子交易制定必要法律以确保参与者的权利和惩罚违法者。

俄罗斯联邦

[原件：俄文]
[1999 年 5 月 12 日]

国际信息安全原则

使用的名词

为国际信息安全原则，兹使用下列名词：

1. **信息领域** — 活动的范畴涉及创造、转变或使用信息，包括个人和社会意识、信息和电信基础结构及信息本身。

2. **信息资源** — 信息基础结构（创造、处理、储存和传递信息的硬体和系统）包括数据档案和数据库以及信息本身及其流通。

3. **信息战争** — 国家之间在信息领域进行对抗，目的在损坏信息系统、程序与资源和重要结构，并破坏政治、经济和社会制度，同时对人民进行群众心理操控，以期破坏其社会和国家的安定。

4. **信息武器** — 为损坏一国的信息资源、程序和系统，对一国的国防、行政、政治、社会、经济及其他重要系统施加负面的信息影响，以及对人民进行群众心理操控以期破坏社会和国家的安定所使用的手段和方法。

5. **信息安全** — 保护个人、社会和国家在信息领域的根本利益，包括信息和电信基础结构及信息本身的特征，诸如信息的完整性、客观性、可用性和机密性。

6. **对信息安全的威胁** — 在信息领域危及个人、社会和国家的根本利益的各种因素。

7. **国际信息安全** — 排除在信息领域侵犯国际稳定、造成对国家和国际社会安全威胁的国际关系状态。

8. **非法使用信息和电信系统和信息资源** — 未得到相关许可而使用电信和信息系统及资源，或使用时违反既定规章、法律或国际法规范。

9. **未经许可干预信息和电信系统及信息资源** — 干预对信息的收集、持有、累积、储存、展示、搜求、散布或使用的进程，以期打断信息系统的正常运作或破坏信息资源的完整性、机密性或可获性。

10. **重要结构** — 对可能造成直接影响国家安全后果的信息资源产生影响的国家设施、系统和机构（直接影响国家安全者包括运输、能源供应、信贷和金融、电讯、国家行政机关、国防系统、法律-执法机关，战略情报资源、以及作为高度技术和环境风险、自然灾难和其他紧急情况的缓解机关的科学设施和科技发展和装置）。

11. **国际信息恐怖主义** — 为恐怖主义目的在国际信息领域使用电信和信息系统及资源以及影响这些系统或资源。

12. **国际信息犯罪** — 为非法目的在国际信息领域使用电信和信息系统及资源，或影响这些系统和资源。

原则一

1. 每个国家及受国际法约束的其他方面在国际信息领域的活动应有助于社会和经济的全面发展，并应在实践中符合维持全球稳定和安全、其他各国主权权利、安全利益、和平解决争端和冲突原则、不使用武力、不干涉内政、尊重人权和自由各项目标。

2. 这些活动还应符合联合国有关文件中所载列的关于个人有寻求、接受和散布信息和想法的权利，但铭记这一权利可能受到每个国家为保护安全利益的限制。

3. 同时，每个国家和受国际法约束的其他方面应有保护其信息资源和重要结构免于受到非法使用或未经许可的信息干预的平等权利，并能得到世界社会的支持以实现这些权利。

原则二

各国将致力于在国际信息安全领域约束威胁，并为此目的而不从事：

(a) 发展、创造和使用影响或破坏他国信息资源和系统的手段；

(b) 有意使用信息影响他国的重要结构；

(c) 利用信息破坏一国的政治、经济及社会制度，对其人民进行心理操控以达到破坏其社会安定之目的；

(d) 未经许可干预信息和电信系统及信息资源，以及其非法之使用；

(e) 采取行动主宰和控制信息领域；

(f) 防止取得最近的信息技术，创造情势使他国在信息化范畴内处于技术依赖的地位以达到有损该国的目的；

(g) 鼓励国际恐怖主义者、极端份子或犯罪协会、组织、集团或个人不法之徒，造成威胁一国信息资源和重要结构的行动；

(h) 拟就并采取计划或主义，以提供信息战争的可能性并能够挑起军备竞赛，造成国家间的紧张关系，引起信息战争；

(i) 利用信息技术和手段在信息领域有损人权和自由；

(j) 跨界散布有违国际法原则和规范以及某些国家国内法的信息；

(k) 操控信息流通，散布假信息和封闭信息以破坏一国社会的心理和精神环境，毁蚀其传统文化、道德、伦理和美学价值；

(l) 进行信息扩张和取得对他国国家信息和电信基础结构的垄断，包括其在国际信息领域的运作的垄断。

原则三

联合国和联合国系统的适当机构将推进国际合作，以便在国际信息安全领域达到约束威胁的目的，并为此建立国际法律基础以：

(a) 查明信息战争的特征，并予以分类；

(b) 查明信息武器的特征并予以分类，并查明可能被当作信息武器的方法和手段；

(c) 限制信息武器的贩运；

(d) 禁止发展、散布或使用信息武器；

(e) 防止信息战争的威胁；

(f) 认识到信息武器对重要结构的威胁，相当于使用大规模毁灭性武器的威胁；

(g) 根据普遍承认的国际法规则和原则，为信息的公平和安全的国际交流创造条件；

(h) 防止为恐怖主义或其他犯罪目的使用信息技术和手段；

(i) 防止为破坏社会和国家安全的目的而使用信息技术和手段来影响社会意识；

(j) 拟订相互通知的程序并防止未经许可利用信息来影响其他国家；

(k) 创造国际监测系统追踪信息领域的威胁；

(l) 创造机制监测遵循国际信息安全制度的条件；

(m) 创造机制解决信息安全领域的冲突局势；

(n) 创造国际制度核实信息和电信、技术和手段（包括软件和硬件）以期保证其信息的安全；

(0) 发展执法机构间的国际合作制度，以防止和取缔信息领域的犯罪；

(p) 在自愿方式下协调国家立法以确保信息安全。

原则四

各国和受国际法约束的其他方面应对在它们管辖下或在它们所属为成员的国际组织主持下由它们进行的信息领域的活动负有国际责任，并应负有国际责任确保这类活动符合本文件所载列的各项原则。

原则五

各国和受国际法约束的其他方面之间在适用本各项原则发生任何争端时，应利用和平解决争端的既定程序予以解决。