联合国 A/56/164/Add.1

大会

Distr.: General
3 October 2001
Chinese
Original: Russian

第五十六届会议

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

增编

目录

二. 各国政府的答复

俄罗斯联邦

[原件：俄文]
[2001 年 6 月 21 日]

对信息领域问题的总的评估

对国际信息安全的威胁

大会第 55/28 号决议第 1 段吁请会员国进一步推动审议信息安全领域的现存威胁和潜在威胁。在俄罗斯联邦提出的题为“与国际信息安全有关的基本概念”（见 A/55/140，第二章）的提案草案中，对信息安全的威胁的定义为危害个人、社会和国家在信息领域的基本利益的因素。

俄罗斯联邦认为，这种威胁如下：

1. 发展、建立和使用影响或破坏另一国信息资源和电信系统的手段

- 非法（不合宪法）的组织、武装组织、恐怖主义集团或个人为临时或永久消除电子设施或系统而采用的电子或其他手段；
- 影响电子控制单元的软件资源以摧毁这种控制单元或改变其运作系统的手段；
- 影响信息通信进程以通过干扰信号发布环境及其运作而终止或打乱这种进程的手段；
- 传播假情报或在信息领域制造部分或完全不符合现实的虚拟图象的手段；
- 对人的头脑和下意识产生作用以使其丧失方向、丧失意志力或暂时丧失平衡的手段。

2. 蓄意使用信息来影响另一国的要害结构

针对军事和民用建筑以及国家系统和机构使用信息武器尤为危险，因为扰乱其正常运行对国家安全构成直接威胁。

例如，未经许可进入电脑化的电力控制系统可以使一国的生命维持基础设施彻底瘫痪，如果涉及核电站的话，还可以造成类似切尔诺贝利悲剧的灾难性结果。

犯罪或恐怖主义团体非法取得有关国防方面或双重用途的科技研究资料可以用来为其犯罪目的或为政治敲诈生产最先进的武器。

可以利用外来信息歪曲或彻底销毁执法机构的数据基和其他信息资源，从而严重干扰司法部门的运作、打击犯罪的活动和维持法律和秩序的工作。

通过未经许可转让或直接盗窃银行资源、“关闭”帐户、特别是发起电子攻击封锁中央银行机构的电脑网络的手段影响信贷和金融领域的信息资源显然不仅可以在该领域造成危机局势，而且还可以使一国的经济彻底崩溃，从而不可避免地在其国际关系中造成严重影响。

利用信息武器大规模破坏电信基础设施等于是攻击国家控制和决策系统。

敌方利用信息攻击防空、反导弹和其他防卫通讯和控制系统可以使一国在潜在的侵略者面前束手无策，使它无法行使其正当的自卫权。

故意破坏生产进程也可以对化工、生物和燃料业技术或环境风险高的企业产生灾难性的影响。

破坏专门负责拯救生命或处理自然灾害或其他紧急情况的通讯、控制和运输系统往往可能增加在这种情况下的生命和财产损失。

3. 使用信息技术破坏另一国的经济和社会制度，从心理上控制一国的居民，以破坏社会稳定

故意利用信息损害对手或竞争者并不是一项新玩意。然而，如今由于广泛使用现代电信技术、组成全球信息网，进行这种滥用的可能性就大为增加了。

开展大规模和全面信息攻击的机会意味着，信息武器已经不是一项辅助工具，而是已经成为一项基本的战斗手段。

与此同时，信息领域正在成为每个社会的生活中的一项决定因素，对国家安全的几乎每个方面都积极发生着影响。随着信息技术的进步，这种影响将会增加。由于有限的信息来源占主导地位，可能有人利用由此产生的压力故意对某国全体居民或关键部门、行政和政府服务部门以及立法机构的工作人员施加负面的心理影响。

使人们感到无力解决自己的问题、不相信国家机制或感到束手无策、攻击他们的意志力或挑起宗教、种族或其他冲突，便是破坏国家的基础，破坏社会的稳定。最终，这种局势可能导致各社会团体之间的敌对情绪、内战和国家的彻底解体。

4. 未经批准对信息和电信系统及信息资源进行干扰并加以非法利用

现代社会的几乎每个国家都遇到或可能遇到未经批准干扰其信息系统的情况；事实上，这种活动有明显增长的趋势。这种干扰的危险是，它可能引起一系列危险的连锁反应：犯罪团伙可能利用“骇客”的经验，他们的“成就”反过来也可能被用作在政府间一级开展敌对、甚至军事行动的武器。

而且，现代的社会和经济发展状况更加剧了社会对扩大取得信息的机会和自由交流信息的需要与显然必须对取得和交流这种资料加以限制之间的矛盾。

与此同时，尽管每个国家可以在其法律和规章中确定未经批准干扰信息系统或加以非法利用的定义，但这种定义在各国的差距很大，有的是轻微的行政错误，有的则是刑事犯罪。许多国家根本没有确定对这种活动的态度。

因此，罪犯可能从母国境内操纵国际信息系统渠道，完全身在其本国的立法范围内，而不属于他犯罪其实所针对的国家的管辖范围。

一个解决办法可以是改进对信息网络的技术保护，但这只有拥有必要的技术以及首先是财政资源的国家才能做得到。

显然，这种局势需要统一现有的国家立法、建立确定谁应对这种罪行负责的普遍适用的国际法律基础。

5. 操纵和控制信息领域的行动

全球化进程在信息领域的特点是高度的标准化，这便于经济和信息基础发达的国家进入发展中国家的电信市场。较不发达国家别无选择，只有接受这种标准，允许在其信息领域使用新技术。鉴于信息技术市场的放宽和信息的自由流通，它们处于别国占主导地位的信息领域，其结果可能对其国家安全不利。

6. 阻止获得最新信息技术，以及制造一种使其他国家在信息领域存在技术上依赖的状况

阻止或限制其他国家取得新信息技术的原因与对其他任何形式的高技术加以限制的原因相似。另一方面，实行限制也可能纯粹出于经济上的考虑、希望垄断市场的某一部分，或者也可能有政治动机，如制裁、针对“不友好”国家的行动或国家安全上的考虑。无论如何，都可能有人希望维持或这制造一种使一些国家在信息领域依赖其他国家的局势。

无论如何，事实是，在二十一世纪，信息技术对所有国家都至关重要，它们必须取得信息技术才能生存。

还必须考虑到，制造信息武器的一项关键因素是，适用的信息技术一般首先是出现民用部门，然后才转到军事部门。

鉴于所有这些因素，只有在防止利用信息技术作为武器或作为生产新形式的毁灭性武器的工具或用于非法目的或有损于普遍安全的目的的范围内，才应考虑限制取得信息技术的问题。出于其他任何理由对今后的任何国际信息安全制度施加限制性条件的做法都应被认为是不可接受的。

7. 国际恐怖主义、极端主义或犯罪集团、组织、团伙或违法个人采取行动，威胁一国的信息资源和要害机构

公司、国家和国际信息系统史无前例的发展和与此同时进入这些系统的机会的扩大已达到这样一种程度，如今几乎国际社会每个成员都将面临着遭到罪犯或恐怖主义分子的电子攻击的实际危险。当然，出现这种危险的可能性将与这种系统的全球基础设施的发展成比例地增加，并将不可避免的具有跨国界性质。

利用信息系统进行犯罪和恐怖主义活动都是非法活动，但两者的目的不同。罪犯利用信息技术纯粹是为了谋财或破坏，而恐怖主义分子在网络空间活动的目的与一般的政治恐怖主义相同的。

开展这种活动的手段可以包括各种信息工具。

恐怖主义分子利用特别的电脑软件、技巧和技术，可以：

- 摧毁、歪曲或操纵信息技术基础设施的各个部分；
- 偷窃重要情报；
- 为其自身的目的更改官方或事实数据；
- 占领或封锁大众传播媒介渠道，以散布假情报、制造恐慌、威胁采取恐怖主义行动或发表自己的要求；
- 利用人为的超载使通讯系统丧失能力；
- 在信息空间散发恐怖主义行动的威胁，造成严重的政治、经济、社会和其他危险的后果。

信息恐怖主义分子的手法是，让恐怖主义行为具有危险的后果、广为人知、并在社会上产生巨大的反响。不幸的是，不受保护的信息系统为这种活动提供了大量的机会。

8. 国家制定和采取各种计划或理论，规定可以发动信息战争，而且有可能引发军备竞赛并导致国家间关系出现紧张状况以及引发实际的信息战

如今许多技术先进的国家所采取的防卫战略的一项主要因素是，建立大量具有防卫和进攻性的军事潜力的情报。这种战略已纳入相应的国家理论。鉴于信息战的作用日增以及信息战的各种手段，现在正在对国家主权的威胁的传统定义、遵守国际法的原则与规范、经济竞争的性质以及各别国家在国际事务中作用的问题进行更加认真的审视。正在越来越多地注意战略情报战，这是一种全新形式的冲突。

由于经济力量与信息力量的结合，现在可以避免利用军事进行传统的“硬性”胁迫，但在影响某一国际政治局势的发展方面可以同样奏效。

这种新的战略的论据如下：

- 发展信息技术不会象不断积聚常规武器或更有甚者，积聚大规模毁灭性武器那样在别国引起极为负面的反响；
- 把重点放在发展信息系统有其吸引力，因为这种系统更符合双重用途技术的概念，而且在许多情况下，既可以作军用、也可以用作民用；
- 在发展和运用信息技术方面领先的国家强化其对战略信息获取的垄断，从而能够在发生国际紧张局势时做出更为有效的反应。

另一个因素是，与“传统的”军事行动相比，利用信息武器可以极大地减少损失和破坏。显然这就是为什么有人极力给人造成一种印象，即信息行动是“人道的”。

另一方面，显然每个国家都可以看到与发展信息技术有关的各种好处和风险，并将竭尽全力对局势的改变作出适当的反应。今后为信息战发展的各种计划和理论很可能导致有更多的国家拥有信息武器库，从

而能够在新的技术水平开始军备竞赛。武器控制局势最终可能恢复到冷战期间的状况。

9. 利用信息技术和手段来危害信息领域的人权和自由

信息领域所涉及的个人利益是，利用个人取得信息的权利和自由从事合法活动或精神和智力发展、保持个人或家庭隐私进行私人通信和其他电子通讯以及保护个人荣誉和尊严。

发展和广泛使用最新的信息技术和手段目前正在为实现信息权创造史无前例的机会。然而，在日常生活中更多地使用信息技术和信息网的发展的必然结果是，越来越多的关于个人私生活的信息可以在公开的数据基上得到。与此同时，当局有可能非法限制个人取得联邦机构、地方当局机构、档案库提供的公开信息资源或其他任何公开的、有社会意义的信息。

今后建立的任何国际信息安全制度都应该规定，统一禁止未经个人同意收集、储存、利用或散布关于个人私生活的信息，除非法律许可，禁止限制公众取得信息。

10. 违背国际法原则和准则以及具体国家国内立法，无节制的跨界散布信息

信息领域的全球化使作为国家安全正常范围的地域、国家和行政界限或管辖范围的传统概念变得含糊。因此，有必要明确界定威胁可能出现在哪里，是在国内还是国外。例如，可以将对另一国的敌对军事信息行动伪装成“当地”罪犯的行动。换言之，以前可以确保在国内有合法的信息交流制度的国家在新的情况下可能对从国外向其境内输送可能非法或有破坏性的信息束手无策，这种信息包括色情产品、假情报、带有种族歧视或不容忍的信息、旨在煽动社会、民族或宗教仇恨的信息、颠覆性质的信息或来源于国际犯罪和恐怖主义团伙或为其利益服务的信息。

11. 操纵信息流动、信息误导和掩藏信息，以此破坏社会的心理和精神环境，以损害传统的文化、道德、伦理和审美价值

由于信息环境和信息活动的性质，它们可以极大地改变社会中大量群体的公众认识和行为。一种特别的危险是，操纵这种影响形式，施加这种心理压力可以引起个人或社会团体不符合现实的感觉。不稳定、紧张的政治局势会增加这种操纵的效力。将大量假情报输入信息系统或在这种局势中掩藏真情报使人无法对事件和促成因素作出客观的评估。公众舆论特别容易受这种影响。

这种行动有现代信息结构所拥有的力量做后盾，可以导致摧毁一个社会的心理环境及其文化和其他价值观念，制造文化战。社会道德败坏然后又为泯灭该国自我意识、摧毁其抵制可能的侵略的意志创造条件。