联合国 A/57/166/Add.1

大会

Distr.: General
29 August 2002
Chinese
Original: English/Spanish

第五十七届会议
临时议程*项目 62
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

* A/57/150。

** 其中所载为提出主要报告后收到的资料。

各国政府的答复

[原件：西班牙文]
[2002 年 7 月 15 日]

古巴

对信息安全问题的总的看法

1. 近几十年来全世界科技方面的发展突飞猛进。信息学和通信方面的进展无疑是一种影响到各种人类活动的技术革命。信息学和通信两方面的进展相辅相成，扩大了两者的潜力使其达到难以想象的高度。

2. 具有高度运算能力的高速个人计算机的引进、加快信息传送速度的新设备的使用和通信卫星的激增只不过是所取得的成就的几个例子而已。

3. 当前的全球化进程是所谓的技术革命所造成的一种实际结果。人与人间的距离在缩短，通讯和信息的流通都是在第一时间进行的。工业程序急剧改变，信息工具在迅速重新设计生产程序，将效率提高到前所未有的水平。

4. 这些变化不但影响到平民，也影响到军事工业。如今信息学已成为现代武器和武器系统的一个重要组成部分。过去的十年，我们目睹各种武装冲突动用尖端武器，这些武器由于应用最新信息学的成果等原因而具有前所未有的破坏力，并可极其准确地击中其目标。

5. 信息工具展示了它们的潜力。例如，软件的应用方式不一而足，包括受传染或可能传播病毒的高度破坏性程序不断加剧的扩散，可能由于信息网的增长和接入这些网络的程度而在较短的时间内在世界任何地方造成无可弥补的损害。

6. 这些技术造成一种依赖，从而必须共同设法确保所有这些手段得到适当的利用。

7. 本项目列入大会议程的事实表明，国际社会认识到，如果这种技术不是用于和平目的，就可能对国际和平与安全构成威胁。

8. 此外，一些为了公然或暗地破坏有关国家法律和政治秩序的目的怀敌意使用电信的情况是使用这种手段的另一种负面形式，其可能的影响是制造紧张局势和违反《联合国宪章》的原则和宗旨造成有损于国际和平与安全的情况。

9. 大会第 56/19 号决议提供了机会，从国际安全的角度来分析信息和电信的各个方面，包括加强和扩大这方面的现有国际法的可能性。

与信息安全有关的基本概念，包括擅自干预或不当使用信息和电信系统和信息资源的定义

10. 对一些基本概念讨论如下。

1. 准则和程序的标准化

11. 由于进入互联网以及使用卫星及其他通信工具的自愿性质，缺乏所有使用者的共同道德守则的事实对于通过这种手段传送信息的安全构成威胁。

12. 机密性、完整性和可获得性等要求可确保网络的有效使用。这些方面的要求可保证每一项信息都只供获准的使用者查阅、不得改动并可在需要时随时取阅。

13. 如果这些规定没有得到遵守，安全就会受到减损。信息工具的每个制造厂商都必须保证不容许其软件或硬件遭到非法修改或是产生能够损害信息系统任何因素的信息武器。总的说来，这些原则适用于任何服务的提供或是产品的制造或信息和通信技术系统。

14. 如果信息系统的每个制造厂商都对生产程序、技术和系统进行较有效地控制，并为同一目的确保其后这种系统和技术的操作和使用过程的后续行动，就可能做到这一点。同样地，必须建立合作机制，以便供应厂商和使用者就所发现的违规情事互通消息，并确定生产者对于解决与他们出售的产品有关的安全问题所负的责任。

15. 必须订立最低标准以便在安全的环境中发展技术。还必须对技术予以核证，因为这种做法有助于标准化机制。在这方面，古巴准备同任何有关国家合作，提供它这方面的一些经验。

2. 擅自干预信息或通信系统

16. 必须加强国际法规防止对这些系统的侵袭。各国无法单独处理这个问题。在信息网和通信系统普遍化的情况下人们的互相依赖达到一种程度，已不可能由一个国家独力担负这项任务。

17. 必须遵守现有的国际准则。必须征得有关国家的许可才可接入其信息或通信系统，接入的形式和程度应由该国决定。

18. 对其他国家信息或通信系统的侵袭可能危害国际和平与安全。已有国家使用这种策略来推行敌对政策。

19. 古巴受到美利坚合众国政府发动或在其唆使或默许下发动的这种侵袭。为表明情况有多么严重，我们要指出古巴几十年来一直受到美国的无线电和电视侵袭，其目的显然是为了扰乱古巴的国内秩序和推翻古巴政府。

20. 例如大体说来，2001 年 1 月至 2002 年 3 月期间，平均有 15 家无线电台和电视台从美国境内传播偏颇的不实消息。

21. 在这段期间，这些无线电台和电视台每天利用中波、短波和调频频带广播 312 至 319 小时。这意味着平均为周 2 257 小时。如果计入电视信号，则总数达每周 2 288 小时。

22. 从 1990 年以来，美国政府每年为这种无线电和电视侵袭投资 2 000 万美元以上，仅仅本财政年度就为数大约 2 400 万美元。

23. 这些消息多煽动非暴力反抗以及破坏和恐怖行为。最近美国政府的一个无线电节目甚至在古巴引起一次企图制造内乱的事件，这次事件还牵涉到一个第三国的外交使团，触发原来可能危及古巴同该国的外交关系的紧张局势。

3. 滥用信息和电信系统

24. 这些系统的使用超出了国际商定的程序和规范范围，并违反有关国家条例。尚未加强国家条例的国家应采取一切必要的措施加强其条例。

25. 鉴于相应技术的发展速度快，为了确保其效果和效率跟得上这种发展，必须定期审查这个领域的国际条例。

26. 目前几乎没有任何社会领域或任何人类活动能够摆脱信息和电信系统的影响。这意味着，滥用这种工具会造成无可估量的冲击。

4. 信息和电信系统是两用技术

27. 这个领域的历史发展有一个独特之处，那就是新技术既可作民用，又可作军用。换句话说，当前许多作广泛民事用途的技术源自军事部门，反之亦然。

28. 因此，国际社会在这个领域的工作应从两个方面着手：预防、制止和杜绝将信息和电信系统作敌对用途，并加强国际合作以利用这种系统。

29. 除其他外，需要对下列与信息和电信系统有关的要点进行分析：

(a) 制止未经许可获得这些系统的程序的设计和普遍应用；

(b) 利用这种工具的透明度；

(c) 策划具体措施，以保护与大规模毁灭性武器及其他先进武器有关的信息系统；

(d) 采取措施防范未经许可进入核电力站、电力站或对一国具有重要战略意义的其他设施；

(e) 国家之间就涉及受其控制或在其管辖下的个人或法律实体的非法活动交换情报，基本上是为了制止非法行为；

(f) 加强国际合作，以促进技术转让，并培训或巩固有关国家能力；

(g) 禁止在外层空间装置工具充作军事用途；

(h) 除其他之外，采取措施，制止利用信息和电信系统作这种用途，以加强在国际关系中不干涉他国内政的基本原则。

5. 信息武器

30. 信息和电信系统可作为一种武器，若其设计和(或)用途对一国的基础设施造成破坏。例如：利用国外软件或源自国内但在国外策划或构想的方式对国家网络进行袭击；利用未经许可的方式或未征得受攻击国的同意进行无线电广播或电视广播；为破坏社会稳定、推翻政府或改变国家的政治和社会秩序而对人的行为施加影响。

6. 信息和电信系统对恐怖主义的用途

31. 必须对形形色色的恐怖主义予以打击和抵制，不分根源或行为人。这些技术难免被用于从事恐怖主义行为。由于这些技术分布广泛、易于取得，并鉴于技术使用费低，影响力大，所以对恐怖分子具有吸引力。

32. 除其他外，可能还有些行动与下列情况相似和同样危险：机场自动系统受干扰；商业航班导航系统受干扰、电力站控制系统、供水和公路遭破坏；通信网络遭破坏。

33. 在国际安全范围内评价信息和电信方面的进展难免涉及与恐怖主义有关的问题。处理此事的直接框架可能是联合国正在进行的关于国际打击恐怖主义的倡议，这些谈判是为了制定国际规范和条例以及其他相关的多边倡议。

34. 古巴准备分析这些看法和可能提出的其他任何基本看法。它相信，作为保证国际和平与安全的最高组织，联合国是讨论这些问题的理想机构。

35. 从事信息和电信系统工作的国际机构也应参加这方面的辩论。关于详细制定国际原则以加强全球信息和电信系统的安全并帮助打击信息领域的恐怖主义和犯罪的适当性

36. 显然需要加强信息和电信领域的国际法。这些国际法不会从虚无中产生；现存的有关国际原则、条例和程序须予考虑。国家经验也应予考虑。

37. 必须努力制定不具约束力的准则，并通过规范。它们可以多边和具有法律约束力的议定书或国际协定的形式出现。

38. 这两种方法必须正视上述基本看法及可能提出的其他看法，特别是未经许可干预或滥用信息系统和信息资源；与这些问题有关的主权方面；信息和电信工具

各方面的和平使用；预防、制止和杜绝利用这些系统作敌对用途；执行国家措施对信息和电信系统实行更大的国家管制，并制止有关犯罪行为。

[原件：西班牙文]
[2002 年 6 月 24 日]

巴拿马

1. 巴拿马共和国确认，在信息和电信领域重要的技术发展将会改变所谓的“网络战场”，对国际和平构成新的威胁。技术不仅影响到武装冲突，而且在消除武装冲突方面也起着作用（情报、目标、武器的质量和数量）。

2. 利用新信息和电信技术进行袭击比常规轰炸会造成更大的破坏。现今，金融信息、石油及天然气在管道的流动以及巴拿马运河上的航运均受电脑控制。除其他外，电脑还控制水存量和水库、空中交通和紧急服务。因此根据关于信息安全（包括未经许可干预或滥用信息和电信系统及信息资源）的基本概念的定义，为了应付这种新的暴力形式，必须设立一些保护系统。但这种保护系统（如防火墙）需要大量财政资源和人力资源，许多国家都难以获得这些资源。

3. 因此，加强全球信息和电信系统安全需要设立一个安全系统，使各国能够交换情报，以监测和制止那些利用通信技术策划犯罪活动的个人或网络的活动或通讯。对技术先进国家来说，这意味着必须作出承诺和承担义务，以向技术落后国家提供、转让或帮助它们建立这种能力。同样地，技术先进国家必须保证它们不会利用其技术优势对其余技术落后国家进行商业或工业谍报活动。

4. 因特网和新的信息和电信技术可起破坏作用。但若适当地加以利用，则可成为保护人类安全的必要工具，有助于国际安全。

[原件：阿拉伯文]
[2002 年 8 月 28 日]

阿拉伯叙利亚共和国

阿拉伯叙利亚共和国对在国际安全范围内远程信息领域的发展作了如下答复

- 应当解除阻止联合国发展中会员国拥有和进口远程信息技术的禁令。
- 联合国应在立法方面积极发挥具体作用，消除科技先进国与发展中国家之间的数字鸿沟。
- 应当订立制止国家、组织和个人非法进入及使用其他国家的远程信息系统的法律，应根据这些法规对违反者提起公诉。
- 应当执行国际电信联盟关于保护分配给联合国各会员国的无线电频率以防止其他国家或任何其他方面进行干扰或非法干预的决议。

- 必须订立关于在数据库和信息网络（因特网）散发有关民族历史、文明和文化的资料的国际标准和规定，禁止以散发错误资料的方式提供虚假情报，并主张采取适当措施，包括对违反者采取行动的手段。

- 应当设立一个受到国际支持的国际当局，其任务是向国家提出理由和证据，要求在远程信息系统的安全事项上进行合作。除其他外，这一国际当局还负责向这些国家提供物质和技术支助，使它们能够通过远程信息系统安全领域的技术合作履行其义务，以及训练其本国专业技术人员。