



## 第五十六届会议

暂定项目表\* 项目 81

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

章次	页次
一. 导言.....	2
二. 各国政府的答复.....	2
玻利维亚.....	2
墨西哥.....	2
菲律宾.....	3
瑞典**.....	5

\* A/56/50。

\*\* 代表属于欧洲联盟的联合国会员国。

## 一. 引言

1. 大会在其 2000 年 11 月 20 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 55/28 号决议中，请所有会员国继续向秘书长通报它们对下列问题的看法和评估意见：(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；和(c)旨在加强全球信息和电信系统安全的各种概念的内容；并请秘书长根据收到的会员国的答复，向大会第五十六届会议提交报告。

2. 2001 年 3 月 19 日，秘书长向会员国发出一份普通照会，请它们应大会所请提供看法。本报告第二节所载为截至 2001 年 7 月 3 日为止从各国政府收到的答复；任何其他答复将在收到后作为增编印发。

## 二. 各国政府的答复

### 玻利维亚

[原件：西班牙文]

[2001 年 6 月 14 日]

根据从玻利维亚外交部收到的资料，玻利维亚武装部队目前没有适当的电子设备，今后也没有打算购置或生产这种设备。

### 墨西哥

[原件：西班牙文]

[2001 年 5 月 16 日]

1. 墨西哥认为，应该加大努力鼓励将科学和技术进展及信息技术应用于民用用途。墨西哥支持大会题为“从国际安全的角度来看信息和电信领域的发展”的 1998 年 12 月 4 日第 53/70 号和 1999 年 12 月 1 日第 54/49 号决议。

2. 当前引起关切的安全问题，大多集中在一些国家的国防所赖以运作的信息系统可能受到伤害的问题，以及信息技术和电信可能受到恐怖份子利用或者被用来进行威胁的危险。

3. 在这方面，国际合作与国际法，是确保为应付信息安全问题而采取的措施不致从任何方面限制信息和通讯自由的唯一途径。

4. 这无疑是一个非常重要的议题。不过，大会其他委员会中的事态发展和讨论情况也应该铭记在心，因为它们对于界定和明确在考虑信息安全问题时可以采用的概念能做出宝贵的贡献。

5. 对于有关信息安全的各种基本国际标准或概念的定义问题，墨西哥认为，未经许可的干扰的概念可能会引起不恰当的混淆，因为它令人觉得与某些国家以值得怀疑的人道主义或其他动机为由来个别地或联合起来干预他国事务的行动有点相似。

6. 因此，对于任何涉及到信息系统的个人或机构的活动，最好将那个概念改成“不许可的进入”，或者简单地用“非法进入”。

7. 关于发展国际原则来增进世界信息和电信系统安全的必要性，应该强调的是，这种原则的目的不仅是要增进这种系统的安全，而且要以法律保障来给予更有效的保护。

8. 同时，还应该更严密地审查大会以及其他国际组织——例如联合国教育、科学及文化组织（教科文组织）——多年来先后通过的处理国际安全、国际恐怖主义和信息等问题的国际文书中的有关规定，以便确定在这个领域的现有有关原则并加以评估。

9. 在这方面，墨西哥赞同大会关于消除国际恐怖主义的措施的 1996 年 12 月 17 日第 51/210 号决议，特别是其中第 3 (c) 段所提到的要注意恐怖主义份子利用电子或有线通信系统实施犯罪行为的风险，必须寻求符合本国法律的办法来促进合作，防止这种犯罪行为。

10. 在 2000 年 4 月 10 日至 17 日在维也纳举行的第十次联合国预防犯罪和罪犯待遇大会期间，秘书处编写了一份题为“与计算机网络有关的犯罪”的文件 (A/CONF.187/10)，其中指出，为了有效地对抗和防止计算机犯罪，必须在各个级别采取协调一致的国际措施。

11. 在各国国内一级，对这种犯罪的调查需要专家、专门知识和适当的程序。应该敦促各国考虑是否可能建立一些机制，使它们能够在司法程序需要得到有关计算机系统和网络的准确资料作为证据的时候，能够及时得到这种资料。

12. 在国际一级，为了提高对计算机犯罪进行调查的效率，必须在国家司法机构和有关法律部门的协调支持下，及时采取行动。

## 菲律宾

[原件：英文]

[2001 年 5 月 22 日]

### 1. 对信息安全问题的一般看法：

1. 信息安全领域的各种问题从复杂性和范围来说，非常庞大而且没有界限，所以信息安全成了一个严重的全球性问题。在今天这个信息时代出现的各种

问题所引起的威胁蔓延的很快。每一种技术进展和革新，也都带来可能被利用来损害人类美好前景的新机会。

2. 信息安全的问题，也会造成与大规模毁灭性武器一样的威胁。它威胁到人类生存的一切方面。没有一个国家或者国家集团能够单独应付这个问题。因此，它是一个全球共同关切的问题，迫切需要所有国家——无论是技术上先进还是落后的国家——做出协调一致的回应。

## 2. 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

3. 下列基本概念可以定义如下：

(a) **未经许可干扰或未经批准侵入**。(一) 非政府干扰行为；或(二) 政府批准的但是超出了已确立的国际信息安全制度或协议范围的干扰；

(b) **许可的干扰**。政府着手进行的为国际条约所许可或在已确立的国际信息安全制度或协议界限以内的“干扰”；

(c) **未经批准使用信息**。(一) 未事先取得来源允许使用非法或合法获得的公共和私人信息；(二) 政府实体为个人、非政府利益使用非法或合法获得的重要公共及私人信息；(三) 政府在任何已确立的国际信息安全制度或协议或其他有关条约和国际法框架以外使用非法或合法获得的重要公共和私人信息；

(d) **滥用信息和电信系统**。(一) 怀着恶性意图使用信息和电信资源，包括有关的基础设施；(二) 所有未经批准的对信息的使用；

(e) **信息资源**。指未经处理和经过处理的数据（即统计资料、事实、数字、记录等等）、软件程序、技术性电脑硬件和设备（即个人电脑、膝上型电脑、扫描仪和其他新的和先进的技术形式）、信息技术和其他有关设施（即传输塔、碟型卫星天线、控制塔/楼）、信息技术专家和专业人员（即计算机程序员、系统分析员等等），包括信息电脑网络和系统（因特网）；

(f) **信息武器**。战略上发展或创建的信息资源，以供用于信息战争或造成破坏、混淆或令对方处于劣势，和任何其他具有恶性意图的形式；

(g) **信息战争**。(一) 旨在通过执行措施来利用、损毁、破坏、动摇或损害敌方的信息及其功能以取得信息优势的行动；(二) 为保护己方的信息资源和电信系统而采取的行动；(三) 利用己方的信息资源和电信系统以实现其目标和利益的行动，例如电脑战（国防和军事领域的信息战争）或“因特网战争”（在更大的社会范围内的信息战争）；

(h) **信息恐怖主义**。在信息安全范围内的恐怖主义行为；

(i) **电脑犯罪或信息犯罪**。(一) 涉及到信息安全内容的犯罪行为；(二) 针对信息资源实施的具有恶性意图的行为（例如技术破坏行为、非法技术侵入和非法修改数据和程序）；(三) 一切未经许可的干扰和未经批准的侵入；

(j) **电脑/技术罪犯**。(一) 实施触犯已确立的国际信息安全制度或协议行为的人；(二) 其犯罪行为涉及或在很大程度上依赖于信息安全的使用的人；(三) 被发现多次实施损害信息资源的行为的人（未成年的涉嫌人应豁免于被当作技术罪犯判罪）；

(k) **信息殖民化**。(一) 一国针对另一国，为了在信息领域取得支配和控制地位，而阻止后者取得最新信息技术，和造成其他国家在信息领域形成技术依赖性状况的行为；(二) 在信息方面进行扩张，对另一国的国内信息和电信基础设施取得垄断地位，造成依赖和控制的情况的行为；

(l) **技术先进国家**。(一) 其经济超过 50% 连线的国家；(二) 可以一般地指发达国家。

### 3. 第 55/28 号决议第 2 段所述旨在加强全球信息和电信系统安全的各项概念的内容

4. 关于建立一个国际信息安全制度的提议，在现阶段至为重要。这种提议应确保违反所述信息安全协议的国家受到责任追究。也应该在技术先进国家与先进国家之间形成一种平衡。这个制度应该考虑到那些已经在针对处于劣势的国家进行其自己形式的“干扰”的技术先进国家。最后，这个制度应该认真地将“执法”看作是增强国际信息安全的一个极其重要的因素。在实际作业上，可以创立一个国际中心来协调不同国家的执法部门，以追查涉嫌人，和帮助这些国家在其国内开展执法行动。

### 瑞典\*

[原件：英文]

[2001 年 6 月 26 日]

1. 在联合国大会第五十五届会议上，欧洲联盟（欧盟）成员国支持就大会题为“从国际安全的角度来看信息和电信领域的发展”的第 55/28 号决议达成的协商一致意见。该决议第 3 段请联合国会员国向秘书长通报它们的看法和评估意见，欧盟成员国希望提供以下的共同答复。

\* 代表属于欧洲联盟的联合国会员国。

## 1. 对信息安全问题的一般看法

2. 信息和电信技术，大大便利了信息的自由流动，为世界各地的个人、工商企业和政府带来了巨大好处。它促进了民主与言论自由以及公民社会的发展。欧盟认为重要的是，要促进和确保信息和电信技术领域的进一步发展，同时也要增强信息自由的原则。欧盟认识到，各种信息和电信系统、基于信息的基础设施的完整性，及个人、企业、教育或医疗机构和私营部门的组织以及政府的各种信息资源，都有受到未经许可的干扰或滥用的潜在威胁。

3. 信息和网络安全，就是要保障发信人和收信人的身份，保护信息以免受到未经许可的修改，防止未经许可取得信息，以及提供可靠的设备、服务和信息供应。

4. 信息安全的范围，也包括对与军事能力和国家安全的其他方面有关的信息的保护。对重要信息资源及信息和电信系统保护得不够，国际安全就可能受到威胁。

## 2. 旨在加强全球信息和电信系统安全的有关国际概念的可能内容

5. 作为一个起点，欧盟希望强调，为了有效地对付信息安全方面的各种复杂新问题，国际合作固然至为重要，但是首要的一点是，每个国家既有权利、也有责任保护它自己的信息和基于信息的系统。

6. 欧盟认为，现存的危险具有跨国性质，而让人能够对信息和电信系统实施攻击的技术很容易得到。所有经济体都要依赖信息的自由流动和信息技术的和平使用。任何旨在控制潜在的犯罪和恐怖主义攻击、包括防范国际安全上的危险，都应该考虑到对信息资源和基于信息的系统的保护。

7. 目前已经在开展一些多边努力，在信息安全领域进行国际合作，例如：欧洲委员会、2000年4月10日至17日第十次联合国预防犯罪和罪犯待遇大会，（见A/CONF.187/15）、联合国预防犯罪和刑事司法委员会、经济及社会理事会的信息学工作组、联合国信息和通信技术工作队、经济合作与发展组织、国际电信联盟、8国集团高技术犯罪问题小组和美洲国家组织。

8. 因此，欧盟认为，联合国会员国应该监注这些论坛和其他论坛正在做的工作，以便在适当时候，评价在这个领域可以采取哪些种类的实质性行动来作出有益的贡献。在大会的范围内，欧盟不认为第一委员会应该是讨论信息安全问题的主要论坛。由于这个问题主要涉及到裁军和国际安全以外的议题，所以欧盟认为，对于这个问题的至少某些方面，由其他委员会来讨论更为适当。