联合国 A/58/373

大会

Distr.: General
17 September 2003
Chinese
Original: English/French/
Russian/Spanish

第五十八届会议

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

* A/58/150。

03-52339 (C) 101003 101003

一. 导言

1. 大会关于从国际安全的角度来看信息和电信领域的发展的第57/53号决议第3段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；(c) 旨在加强全球信息和电信系统安全的有关国际概念的内容。大会同一决议第4段请秘书长考虑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，并在一个由秘书长根据公平地域分配原则任命成员、将于2004年设立的政府专家组的协助下，以及在有能力提供此种协助的会员国的帮助下，进行研究，并将研究结果向大会第六十届会议提出报告。

2. 2003年2月18日发出的普通照会请所有会员国向秘书长通报它们对这个主题的看法和评估意见。迄今收到七份答复，其内容转录在下面第二节。进一步收到的答复将作为本报告增编印发。

二. 从会员国收到的答复

玻利维亚

[原件：西班牙文]
[2003年6月17日]

从国际安全的角度来看信息和电信领域的发展

1. 玻利维亚担心技术方面的进展将被用于同国际稳定与安全相抵触的目标，对国家的完整产生负面影响，危及国家本身在军事和民事领域的安全。

2. 玻利维亚强调必须防止信息技术资源被用于犯法或恐怖目的。

3. 为此，玻利维亚谨提出关于信息安全和未经许可干扰有关系统的基本准则如下。

信息的重要性

4. 在谈到信息时，我们直接或间接地指的是信息和电信系统（新的技术、新的应用——软件、新的装置--硬件、以及日益稳当、可靠和迅速地创建信息的新的形式），而主要的考虑就是这些系统的风险和安全。

5. 应当铭记，将信息集中起来的地点，往往可能是最安全的地点，但也是最易受侵犯的地点。

6. 鉴于电信的脆弱性质，因此尤应注意因特网和电话业务。因特网同信息系统直接有关。电话业务分为移动电话和有线电话两种。移动电话服务共同使用一个

传播空间，在这个空间内，无线电波正在传送，用户则处身于电话的通信和侦听活动中。

有关信息系统的犯罪或违法行为概述

7. 利用电脑和接收器附带地和意外地从事违法行为的形式和类别都大大增加。今天，大多数违法行为都是偶然发现的(欺诈、伪造和出售信息)。

8. 在管理信息系统方面，应当注意电脑病毒，这些都是意外或故意编写的程序，应予特别注意，而且必须实行严格的作业过程予以遏制。

9. 应予强调的是，当出现问题时，必须查明犯法行为的动机并立即提出解决办法。一些危险性最高的动机包括：个人利益、罗宾汉综合征、对某一组织的憎恶、精神失常和不诚实；一些危险性较低的动机包括为了组织的利益和游戏。

组织在安全方面的典型做法

10. 这些典型做法在目前的科学思维中发挥重要作用，关于调查的规则就是从这些典型做法引伸出来的。

11. 一些主要典型做法如下：审计系统的责任应由用户和内部审计部门负责；安全系统不考虑内部欺诈的可能性；在一个机构内发生事故的可能性很低；总会出现差错，因为没有一个系统是十全十美的；还有其他等等。

查明风险

12. 必须在一个组织的用户之中形成对信息所面临的风险的认识，使他们了解到安全是其工作的一部分。为此，必须确定安全系统的成本和质量，评估安装系统的风险，查明高风险的应用程序，以数量表示中止服务的影响，并制定所需的安全措施。

13. 在确定风险程度之后，必须拟订一份所应采取的预防措施以及在发生灾难时所应采取的措施清单，并指出每一项措施的优先顺序。

14. 应在机构、区域和国家各级考虑这些风险并以数量表示，说明是否有后备程序以及取回这些程序的可能性。

一个整体安全系统的考虑因素

15. 开发一个安全系统意味着“规划、组织、协调、指导和管制与维持并确保信息系统所涉资源的完整性有关的活动，以及保护某一机构、区域和国家的资产”。

16. 为此，必须界定行政方面的要素和安全政策，安排并分配责任，确立紧急程序，界定安全目标，对信息的风险和安全地位作出诊断，并最后拟订一项安全计划。

古巴

[原件：西班牙文]
[2003 年 5 月 28 日]

1. 自联合国大会第一委员会于 1998 年开始审议“从国际安全的角度来看信息和电信领域的发展”的专题以来，古巴一直支持这项决议。

2. 本项目列入大会议程的事实表明，国际社会认识到，如果信息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。

3. 2003 年在日内瓦和 2005 年在突尼斯分两个阶段筹备和举行的信息社会首脑会议探讨上述决议所涉的专题和国际社会优先注意与此决议密切有关的其他题目。

4. 为了公然或暗地破坏有关国家法律和政治秩序使用电信进行攻击，是不正当使用这种手段的形式表现，其影响可造成危害和平与国家安全的紧张局势和明显违反《联合国宪章》的原则和宗旨。

5. 第 57/53 号决议申明技术和信息手段的传播和使用与国际社会息息相关，广泛的国际合作可导致发挥其最大效用。

6. 决议序言部分第 8 段指出“关切这些技术和手段可能会被用于与维护国际稳定与安全宗旨不相符的目的，对各国基础设施的完整性可产生不利影响，损害其民用和军事领域的安全”。

7. 此外，决议执行部分第 3(b)段要求所有会员国通报它们对确定有关信息安全的各种基本概念的看法和评估意见，“尤其未经许可干扰或滥用信息和电信系统及信息资源”的意见。

8. 古巴认为“未经许可干扰”指这些系统的使用超出了国际商定的程序和准则的范围，特别是超出国际电信联盟的范围和违反有关国家条例。

9. 即使没有这样做的国家也应该采取一切必要措施，加强有关本国条例。

10. 鉴于相应技术的发展一日千里，为使其效用和效率与这种发展齐头并进，还必须定期审查这个领域的国际条例。

11. 信息和电信系统可用作武器，其设计和/或用途对一国的基础设施造成破坏。例如，使用外国软件或源自国内但是在境外策划构想的方式对国家网络进行袭击；通过无线电或电视播送的信号意图破坏其他国家依据宪法建立的社会秩序和体制；使其他国家的无线电广播遭受干扰、损坏或停顿的活动。

12. 古巴重申各国必须遵守现有的国际准则。必须按照国际合作协定征得有关国家的许可，才可接入其信息或电信系统，至于接入信息的形式和程度，应根据接入系统所在国的有关法律。

13. 对其他国家信息或电信信系统的侵袭可能危害国际和平与安全。遗憾的是，已有国家玩弄这种手段来推行敌对政策。

14. 20 年来，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。自 1985 年起和于 1990 年，美国政府非法建立一个无线电台和电视台，对古巴的无线电和电视广播不断进行干扰。政府和其他电台每周播放逾 2 220 小时旨在破坏古巴宪法秩序的节目。有 24 种频率专门用于这种广播。

15. 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。

16. 如古巴共和国外交部 2003 年 5 月 22 日发表的声明所指出那样，美国政府发动几十年来通过无线电台和电视侵袭古巴的新攻势。

17. 2003 年 5 月 20 日，由美国政府建立和操作旨在破坏古巴的无线电台,使用 4 个新频率，对古巴的广播进行干扰和造成影响。

18. 此举粗暴违反国际法和国际电信联盟所制定的准则及条例，之所以建立该国际组织，特别是其无线电广播条例，是促进全球电信的良好运作。

19. 2003 年 5 月 20 日下午 6 时至晚上 10 时，美国当局开动宣传机器，使用一架美国空军 EC－130 型飞机，为此目的向古巴播送电视信号，擅自使用古巴电视台合法分配到和已在上述国际组织登记的频道。

20. 这项行动违反国际法和各国在国际电信联盟的框架内商定的准则，特别是其禁止电视广播超越国界的第 23.3 号无线电广播条例。

21. 这种广播也违反国际电信联盟宪章的序言，因为所进行的活动没有善用电信手段来促进和平共处的关系、各国人民之间的国际合作和经济及社会发展。

22. 古巴拒绝和谴责美国当局纵容恐怖分子，何塞·巴苏尔托的活动和其向古巴播送电视信号的企图。尽管已通过外交途径正式通知当局已警告巴苏尔托先生向古巴广播被视为违反美国法律的行为，并会对他追究责任。5 月 20 日这名知名恐怖分子得以逍遥飞走；他之所以没有广播，不是怕明目张胆与他勾结的美国当局对他采取行动，而是其发射机发生故障而已。

23. 根据国际电信联盟第 15.24 号无线电条例,美国的电视侵袭无疑是有害干扰，由使用甚高频的 13 频道(210 至 216 兆赫兹)的电视台严重骚扰已正式登记在这个频道广播的古巴电视服务。

24. 古巴当局已向美国政府的联邦电讯委员会报告此事，指出所有技术和法律准则均被粗暴违反。

25. 古巴还采取步骤告知国际电信联盟秘书长上述事实，并请他实行相应措施。

26. 古巴认为必须加强信息和电信的国际法律框架。还认为必须充分遵守管理国家之间的关系的国际法和《联合国宪章》在这个领域建立的国际秩序。实际上，已订有这方面的国际原则、条例和程序，应予遵守。

27. 应该致力制定无约束力的准则，并通过具有多边和法律约束力的国际协议或议定书形式的准则。

28. 两种方法都应当考虑到基本准则，例如关于未经许可干扰或滥用信息和电信系统的准则；与这些题目有关的主权问题；信息和电信手段各方面的和平使用；促进国际合作，以便在信息和通信技术对社会－经济发展的重大影响的基础上，挖掘发展中国家的信息和电信系统的发展潜力；预防、制止和杜绝将这些系统作敌对用途和本国采取措施，加大国家控制信息和电信系统的力度和打击有关犯罪行为。

29. 除前文所述以外，古巴认为应注意到以下几点，这与充分使用电信作为加强国际合作与安全的手段密切有关：

- 各国必须停止单方面使用胁迫措施，限制受影响的国家取得信息和通信技术以及接入信息交换的国际网络，这违反国际法。

- 任何国家取得电信技术或其他相关技术的证明和对它由此威胁国际和平与安全可施加惩罚的制度应是个多边制度，并以国际社会公认的标准为基础。

- 应该促进国际合作，调动必要资源帮助发展中国家加强和扩大其电信系统。

- 应该在国家和国际两级采取立法和其他相应措施，制止电信以及信息和通信技术的所有权和控制权过度集中在私人手中，以免对信息的必要多种来源造成不利影响，并用作破坏和平和煽动战争的宣传工具。

- 应该建立一个管理和监控因特网及其他国际信息和通信网的多边、政府间、民主和透明系统。该监控系统的政府间应有特点至关重要。

- 电信和其他国际通信监控系统应该是多边、透明、有明确责任和公共监督程序的系统，足以停止一些工业国家，尤其美国利用其全球监视系统侵犯许多国家的隐私、主权和安全。

- 应致力确保对文化多样性的尊重，消除在国际电信系统传播的信息中一切形式歧视或挑起仇恨的内容。

萨尔瓦多

[原件：西班牙文]
[2003 年 6 月 30 日]

萨尔瓦多政府根据第 57/53 号决议“从国际安全的角度来看信息和电信领域的发展”执行部分第 3 段提交的答复

1. 《萨尔瓦多共和国宪法》第 24 条禁止干涉和干扰电话通讯，这是萨尔瓦多在信息和电信安全方面现行的宪法框架。

2. 根据《刑法》第 184、185、186 和 302 条，扣押不是发给自己的书信、电脑硬件和其他私人文件或物品，或扣押个人或家庭性质的机密材料，以及利用技术手段进行监听或录音，截取或打断电报或电话通讯并对其进行干涉和干扰者，均应加以惩处。

3. 如果当事者正受到威胁，要求为被绑架或劫持的人缴纳赎金，或事关有组织的犯罪，而受害人或其代表出面要求或允许共和国总检察长对进行这种威胁或要求的对话或行为进行监听和录音，则这种行为不构成犯罪。

4. 由电力和电信监管总署负责按照设立该署的法律第 4 条和关于通讯保密的《电信法》第 29(b)条的规定，实行电信规范框架和行政制裁措施。

5. 2001 年和 2002 年，向立法大会提出了一份宪法修正案，以允许用电话干涉和（或）电话干扰作为协助打击有组织犯罪和贩毒的工具。这项提案至今尚未通过。

格鲁吉亚

[原件：英文]
[2003 年 6 月 20 日]

1. 格鲁吉亚政府正在制订一项国家信息战略，以求发展电信领域和推广新技术，同时强调国家有关安全使用信息技术的政策。

2. 此外，格鲁吉亚政府还对格鲁吉亚加入全球信息社会问题采取政策，同时也认识到在信息安全领域现有的所有风险和挑战。

3. 格鲁吉亚政府认为，极其有必要参加旨在建立更加安全的国际信息社会的各项国际方案和合作项目，这是基于一项了解，即鉴于信息技术和系统的现实以及格鲁吉亚所属区域的特点，不可能单方面来处理信息安全问题。

俄罗斯联邦

[原文：俄文]
[2003 年 4 月 28 日]

与信息安全问题政府专家组的工作有关的问题

1. 大会结合国际安全问题，就信息和电信领域中的各项发展通过了 2001 年 11 月 29 日第 56/19 号和 2002 年 11 月 22 日第 57/53 号决议，根据这两项以协商一致方式通过的决议，定于 2004 年建立一个政府专家组。以这些规定为依据，将要求专家组进行以下工作：审查信息安全领域中现有的和潜在的威胁，并审议为消除这些威胁可以采取的合作措施；对旨在加强全球信息和电信系统安全的有关国际构想进行研究；向大会第六十届会议提交一份关于研究结果的报告。

2. 俄罗斯联邦认为，国际信息安全仍然具有重要意义，引起越来越多的讨论，现已成为各国的一个重要国家安全问题，并成为整个国际安全和战略稳定体系的一部分。信息和通信技术及方法的应用与在全世界各国实现军事和政治安全的努力直接有关，因此，应该本着全球、综合及不歧视的观点来审议这种应用，并争取尽量多的国家在公平地域分配原则的基础上参加审议。

3. 通过在联合国主持下审议这个问题，正是提供了这样一个方式。联合国是一个重要的国际组织，最充分地代表了所有国家的利益，并在裁军领域发挥着协调作用，从而将为建立一个平衡和有效的全球安全体系奠定基础。

4. 我们认为，在探讨各种各样与国际信息安全有关的问题和制定适当的建议方面，大会 1998 年 12 月 4 月第 53/70 号、1999 年 12 月 1 日第 54/49 号、2000 年 11 月 20 日第 55/28 号、2001 年 11 月 29 日第 56/19 号以及 2002 年 11 月 22 日第 57/53 号决议发挥了重要作用。这些决议是按照传统，以协商一致方式通过的，因此体现了整个国际社会的意见，并体现了各国就联合国秘书长的报告（A/54/213、A/55/140 和 Corr.1 及 Add.1、A/56/164 和 Add.1 以及 A/57/166 和 Add.1）所述信息安全问题得出的评估结论。

5. 联合国裁军研究所和联合国秘书处裁军事务部根据第 53/70 号决议提出的建议，于 1999 年 8 月在日内瓦组织了关于国际信息安全问题的研讨会。这个研讨会有来自 50 多个国家的代表参加，在确定应该以何种方式来处理当前与国际信息安全有关的问题方面发挥了重要作用。

6. 研讨会确认，信息安全是一个紧迫的问题，亟须将其列入国际议程。这个研讨会还提供了一个机会，用以确定各种方式来从本质上处理这个问题。当前没有任何公认的适当国际标准或工具，可用于从采取措施，以减少现有和潜在的全球信息安全威胁的角度出发，来处理信息安全问题。

7. 因此，有必要进行联合努力，争取尽量多的国家参与，以研究这个领域中的各种现有构想和方式，并分析当前与国际信息安全所涉各方面问题有关的国际法律规定。

8. 我们相信，通过建立信息安全问题政府专家组，将使国际范围内关于这个问题的多边讨论进入一个实质性的崭新阶段。这个专家组将为国际社会提供一个独特的机会，来检视各种各样有关的问题。

9. 俄罗斯联邦要在政府专家组的工作中发挥建设性作用，因此想提出一系列据我国认为可以列入专家组议程的问题。

10. 在审议国际信息安全问题时，首先必须遵守各项人类价值观，例如以公认的国际法标准和原则为基础，保证能够普遍、自由、公平和安全地在国际范围内交换信息。

11. 专家组应该考虑到根据关于国际信息安全的各项大会决议从各国收到的评估意见，并考虑可能交由其审议的其他材料。

12. 我们认为，该专家组可以侧重审议我们认为最主要的以下问题：

13. 第一，专家组应该商定一个适当的国际信息安全概念体系。在这个阶段，政府专家组所进行活动的主要目标可以是制定与信息网络、资源和系统、信息基础结构以及信息武器有关的基本定义，并确定对信息安全所构成威胁的特点、标志、特性描述和分类。

14. 第二，专家组应该检查对国际信息安全产生影响的各种因素。这是一个错综复杂的领域，国际社会必须采取一种全盘兼顾方式，把民用领域和军事领域内的恐怖主义、犯罪或军事威胁都考虑在内。

15. 在逐渐形成的全球信息社会中，信息和通信技术相互关联，并且不受国界限制。因此，在全球信息社会中，国际信息安全同以下问题之间有着不可分的联系：查明内部或外部性质的威胁源头；国家主权问题；与尊重人权和自由有关的问题，特别是与尊重个人生活不受干涉的权利有关的问题。这些问题和相关问题可以为政府专家组内的讨论提供一个基础。

16. 可以在下个阶段确定可共同接受的措施，用以防止把信息技术及方法用于恐怖主义目的和其他犯罪目的，并确定限制使用信息武器的措施，特别是禁止使用这些武器袭击别国关键基础结构的措施。这个阶段的目标看来将包括：检视有多大可能性来制定相互通知程序以及防范未经批准使信息技术产生跨界影响的程序；建立一个国际监测系统，用以跟踪监测可能在信息领域出现的威胁，并建立监督国际信息安全安排执行情况的机制和解决与信息安全有关的冲突局势的机制；为信息和电信技术及方法（包括那些与软件有关的技术及方法）的国际认证制度制订管理条件，以保证信息安全。

17. 应考虑到在执法机构之间进行国际合作的可能渠道，以防范和制止信息空间的犯罪，特别是查明网络袭击的来源。应该考虑在各国有关信息安全的国家法律之间进行协调的问题，以便对信息安全犯罪进行统一分类以及为属于犯罪的行动规定应承担的责任。

18. 还建议专家组考虑向受到网络袭击的国家提供国际援助的可能性，以减轻这些国家的正常运作受到干扰所产生的影响，特别是在其关键的国家基础结构受到袭击时提供援助。

19. 在较长的期间内，也许应该努力制订一份可共同接受的多边国际法文件，以加强国际法律安全安排。这份文件将规定，各国和其他国际法主体必须为其在信息空间进行的活动——或在其管辖的领土上进行的这类活动——承担国际责任。

20. 俄罗斯联邦认为，可以规定，参加者有义务不在信息空间从事旨在对他国信息网络、系统、资源和程序或基础结构造成损害的活动，也不从事旨在干扰他国政治、经济和社会制度，或在心理上操纵该国居民，以破坏其社会和国家稳定的活动，从而把这种义务作为一个世界性的国际信息安全制度的基础。

塞内加尔

[原件：法文]
[2003 年 6 月 9 日]

1. 有关电传信息安全的措施特别是在交换有关武器贩运的情报时发挥作用。这些情报必须保密。

2. 因此，必须采取如下一些保密措施：

3. 通过安装特制的技术装置来保证材料、软件和数据处理的安全；

4. 通过具体和专门的规定来保证情报交流程序的安全。

乌克兰

[原件：俄文]
[2003 年 5 月 27 日]

1. 对信息安全的问题的一般评估

1. 全球化的国际进程，各种新的信息技术的采用以及信息社会的出现，所有这些都突出了信息安全作为国家安全的一个因素的重要性。

2. 国家信息基础设施的发展和各种新的信息技术的发明和采用给信息社会带来了某些特定的危险。这些威胁中，最为严重的是蓄意威胁，造成这些威胁的原因可能是相关的个人在精神、知识或物质利益方面，存在着客观或主观差异，在

追求理想的方式和方法方面也存在差异。因此，这在有些情况下可能引起冲突局势。

3. 对信息社会造成的主要威胁包括：

- 对信息的操纵（错误信息、掩盖或歪曲信息）；
- 违反现有的信息交流方式，擅自存取信息资源，或对存取信息资源无理限制，或者非法搜集或使用信息；
- 摧毁国家信息空间或者为反对国家之目的使用这一空间；
- 信息恐怖主义，如传播计算机病毒，致使程序或装置发生故障，在技术设施或场所安装射频装置截获信息，非法使用信息和电信系统及信息资源，兜售不实信息等。

4. 负面信息影响的一个直接后果就是错误信息，造成国家信息环境及其信息资源的失真和（或）摧毁，并使得重要的国家、工业、金融、学术或一般文化体系无法运作，结果丧失对信息的国家主权。

5. 因此，对信息社会各种问题的审议表明，除了一般问题之外，存在的问题还有维护信息资源的基本范围和质量，拟定使用这些资源及适当信息技术的战略，建立足够的信息基础设施，维护信息和电信系统的信息安全以及同影响到个人、社会和整个国家的负面信息活动进行斗争的必要性。

6. 国家信息资源保护水平不足，可能会造成工业和信息技术的贸易亏损，从而带来巨大的经济损失，也会由于通信、监测和管理系统可能瘫痪，不能正常运行，并由于有关国家机密的信息泄漏等情况发生，给国家安全整体带来严重损失。

7. 信息安全依赖在每一阶段采取措施，保护信息。信息安全的目标是确保系统的完整性，保护并保证信息的准确性和完整性，并在此类信息遭到篡改或摧毁时，将后果控制在最低程度。

8. 现代世界的一个特点是，在社会和国家活动的不同领域使用局域和全球信息系统，以便加快信息交流，更快地获得各种信息资源。

9. 这种系统的广泛使用，特别是在与国家管理相关的活动领域使用，造成了各种真实的可能性，使国家信息资源和控制系统被擅自存取，被用来传播非法信息，使得这些资源和系统的完整性及其信息的可存取性遭到破坏。

10. 政治、经济、军事、金融和国家活动的其他方面的稳定运转不仅依赖电信和信息系统运行的效率，而且也依赖其可靠性。如果正在建立信息空间，那么，为国家管理提供服务的信息和电信系统的可靠性和保护问题便格外重要，而且具有现实意义。对信息系统的存取可以使宝贵的信息得到利用，然而，如果信息系统

的工作遭到阻塞，那么就可能使经济的重要部门乃至整个领域全部瘫痪，或部分瘫痪，使信息资源遭到损害，被法律禁止的信息得以传播。

11. 确保信息和电信系统内所载信息的安全对于保证信息安全、国家和民族主权以及稳定的社会发展来说，是一个主要的因素，也是一个先决条件。

12. 在信息和电信系统发展的现阶段，对于系统所载信息的主要威胁包括：

- 重要的信息和电信系统有秩序的运作被扰乱；
- 意外或蓄意行为，造成信息的保密性、完整和可存取性被破坏；
- 对信息系统进行干扰（传播计算机病毒、安装制造障碍的程序和装置、在技术设施和场地使用截获装置、截获信息和解码、兜售假信息、射频干扰关键密码字系统、扰乱通信和指挥系统的线路等等）。

13. 应当建立复杂的信息保护系统，包括使用密码和技术保护措施，再加上一系列组织和技术手段，唯有如此才能确保信息和电信系统，特别是政府管理部门的这些系统得到可靠的保护，使之免遭罪犯破坏。

14. 应当特别注意计算机网络与国际信息网络连接问题。

15. 乌克兰要想充分进入国际社会，就必须扩大同诸如因特网等全球信息交流网络的合作。这些系统提供了现代信息和电信服务方面的广泛选择，其中许多系统都做出宣传，说可以提供信息保护。

16. 与此同时，此类系统中广泛使用了各种装置，但是，如果得不到以前的编程代码，则很难甚至不可能了解这些装置的特性，因此对信息、金融交易和电子付款的安全构成威胁。已经发生无数事例，银行在使用进口信息技术方面考虑欠妥，使得专家利用这种技术仅用十分钟就可渗入系统。

17. 必须注意，未经充分准备将服务器和局域网络同全球网络连接，可能会出现危险。任何局域计算机网络与因特网连接，如果没有适当的保护措施，都会很容易遭到黑客的攻击。

18. 各国间在交流信息方面采用新途径和新方式，越来越多的人喜欢利用因特网以新的形式进行企业活动（电子商业），并逐渐采用电子控制系统，与此同时，计算机技术得到广泛应用，电子形式的信息也更为广泛。其结果是，信息连接的内容越来越依赖于对这些信息提供的保护程度，而这些内容又成为社会上不良分子及其同伙注意的目标。现有的各种保护系统和机制互不兼容，真正有可能发生擅自闯入、使用、阻塞或消除以电子形式创造、处理、传送或储存的信息。

19. 对国家信息资源的干扰是目前全世界都在关注的话题。1990 年代初之前，至关重要的问题是保护国家免遭外国间谍渗透，近年来，国民生活的所有方面都广泛的采用了信息技术，因此，与所谓的计算机犯罪进行斗争变得更加紧迫。能够

证明这一点的是，目前，国际上已经承认计算机犯罪是知识犯罪的一种新的形式。此外，实施这种罪行不仅有组织犯罪集团，而且还有恐怖主义组织和个体罪犯。

20. 对罪犯特别有吸引力的是国家机关、执法部门、海关和税务、金融和信用机构、军事单位等使用的信息系统。在乌克兰，执法部门不止一次地发现非法行为，其中涉及在国际支付系统中使用塑料卡，进行虚假的电子付款，以期非法获得货币，或者通过因特网干扰计算机网络的活动。

2. 信息安全基本概念的定义，包括未经授权干扰或非法使用信息或电信系统或信息资源

21. 信息和电信技术的深入发展使得确保信息安全问题愈发严重，其中包括未经授权干扰或非法使用信息和电信系统问题以及保护信息资源问题。

22. 在这方面，必须将“信息安全”理解为对国家信息空间的某种保护，使国家能够获得国家利益，并使个人、社会和国家的各种权利能够得到遵行。

23. 鉴于上述各种非法活动给社会带来相当大的危险，并鉴于信息和电信系统有效运转的重要性，《乌克兰刑法》对与利用使用计算机和计算机系统或网络相关的各种罪行做了规定，并对实施此种犯罪规定了相应的刑罚，特别是：

- 非法干扰计算机或计算机系统或网络运行，造成计算机化信息或此种信息的载体失真或毁坏，或通过软件或其他技术装置散播计算机病毒，意在非法渗透计算机或计算机系统或网络；
- 盗窃、挪用或勒索计算机化信息或以欺骗或滥用职权等手段获得此种信息；
- 负责自动计算机或计算机系统或网络的人违反操作规则，非法拷贝计算机化信息，或严重扰乱计算机或计算机系统或网络的运行，造成计算机化信息或其保护手段的失真或毁坏。

24. 总之，可将“计算机犯罪”界定为信息技术操作过程中一种非法行为，违反了信息技术系统操作的既定程序或存取程序，或损害了信息的完整性、保密性或可存取性，损害了公民的权利和自由。

3. 旨在加强全球信息和电信系统安全的国际概念的内容

25. 二十一世纪将作为全球信息社会诞生和发展的时期载入史册，它将以信息技术进程来巩固或扩展物质进程，并帮助大大提高劳动生产率，改善社会福祉。许多国家已经在为国家和全球基础结构建立组织和技术基础。联合国在《世界人权宣言》中阐述了保障获得基本通信和信息手段的权利的问题。

26. 一些国际组织（国际电信联盟、国际标准化组织/国际电工委员会、欧洲电信标准研究所）和许多国家标准化组织对 1990 年代后半期发达国家在寻找有效

办法处理信息技术传播问题方面的经验作了汇编。这些经验表明需要建立多层次（国家和区域各级）的信息技术基础结构，随后将它们并入全球信息基础设施。

27. 欧洲在全球信息基础设施中的参与不仅显示了国家信息基础设施在欧洲区域内的建立，而且也意味着要协助在具体国家建立此种基础设施以促进全欧洲每个国家的共同利益。欧洲人所说的不是“欧洲信息基础设施”，而喜欢采用“欧洲信息社会”一词。欧洲信息社会的组成部分是它的网络、基本服务和其他服务。可以通过采用欧洲宽带高速公路来加强现有的欧洲网络，这将把欧洲的所有电信、电缆和卫星服务连成一个单一的整体。欧洲国家支持使用跨欧洲基本服务，包括电子邮件服务以及文件和视像传送。

28. 欧洲国家还十分重视世界技术革命下一阶段的社会方面问题。欧洲委员会已通过了关于制定建设信息社会方面国家政策的决议和文件。在各方看来，这不是为了赶时髦，而且是实现发展的一项必要条件。如果对此不予接受，那将导致丧失动力，造成从领先的经济和技术地位后退。

29. 涉及最新数据传送技术方面活动的世界法律管制趋势证明，有必要制定统一的办法，为参与国际信息交换的所有各方确立立法和标准化工具。美洲法学家协会认为，目前已经存在设立一个赛博空间立法多国委员会的现实需要。设立一个“赛博法院”是建议由这个未来委员会审议的问题清单上最重要的项目之一。目前，信息安全立法的主要问题是必须对现行法律规则进行调整，使之适应信息技术的进步。

30. 今天，不可能想像会有一个没有计算机网络的信息空间。正是这一技术促使产生了许多类型商业的出现和发展：电子帐户卡、银行间业务清算、证券交易服务、经纪服务等等。

31. 预期到 2005 年，欧洲联盟有一半以上人口将使用因特网。因此，欧洲联盟各国正努力建立人们对通过因特网开展商业和金融业务的信心，并且加快向电子商务的过渡。

32. 1999 年 5 月 7 日，欧洲议会就 INFOPOL 98 的草案达成协议，授权主管机构合法地从事网络监测。这事实上是欧洲委员会关于合法截获与新技术有关电信内容的决议的草案。这份文件要求让从事实时监测的机构能够利用所有电信网络，包括因特网和卫星电话系统。联合王国政府已开始实施一个项目，建立一个截获该国境内所有电子信息传输的中心。

33. 中国政府目前正通过发放调制解调器使用许可证的办法，控制对网络的使用，而且所有因特网信息都须通过为数有限的国家操作者传送。

34. 不妨提请注意下列信息安全方面的问题：

- 对知识产权的侵犯；

- 对人们正常社会生活产生有害影响的信息的传播，包括与儿童使用因特网有关的问题；
- 从事非法商业活动；
- 未经许可获取保密资料；
- 在信息交换过程中侵犯个人权利与合法利益；
- 传播低品位广告。

35. 此外还有另一个与因特网有关的危险——个人保密资料有可能在未经本人许可情况下遭盗用。这种资料有可能通过分析此人使用因特网的情况加以掌握。

36. 因特网是一个非常具体的通信手段，但由于它具有跨界性质，因而很难从法律上加以管制。所有因特网使用者均受其本国法律的约束。但是，非法的内容虽储存于所在国境内的服务机内，却可显示于他国境内。缔结国际协议对于规范因特网所涉及的法律关系来说，固然必不可少，但是国际协议的通过则又由于国家立法对一种或另一种犯罪采取种种不同的对待方法而变得很复杂；例如，在“淫秽色情”概念上就存在不同的解释。今天，与因特网有关的立法举措的普遍趋势是确定主机服务提供者须对其计算机内所载的信息内容承担责任。由于从技术角度讲，这是一个非常复杂的问题，因而一些国家的立法规定，在确定服务提供者的责任时必须以提供者知悉非法信息的内容为条件。

37. 刑警组织的成员包括 178 个国家的执法机构。它报告说，它将在美国 Atomic Tangerine 公司的网址上公布关于网络犯罪的资料。刑警组织提供有关骇客以及威胁电子商业公司安全的犯罪类型的情况。Atomic Tangerine 公司则必须把属于 Atomic Tangerine 公司而且专门为监测因特网而设计的网络雷达预警系统所获取的信息传送给刑警组织。

38. 匿名通信是最重要的问题之一，因为它使得确定非法信息所属人身份以及对其进行起诉的工作复杂化，有时甚至使这项工作不可能完成。因此，许多国家的专家建议在法律上禁止匿名通信，但是同时允许用假名进行通信，因为必要时就可以确定此种通信的行为人。

39. 1998 年 12 月 21 日，欧洲联盟理事会通过了欧洲议会提议的一项关于加强因特网安全的行动计划。这项计划实施了四年（从 1999 年 1 月 1 日至 2002 年 12 月 31 日）。它的总预算为 2 500 万欧元。该计划建议根据各产品的因特网基准，设定各种因特网质量标准。这些规定将纳入国家立法以及因特网服务提供者的自订规则中。1999 年 3 月，欧洲联盟委员会在讨论了关于电信、媒体和信息技术部门彼此趋同的报告所载各项内容之后，通过了一份报告，其中得出以下基本结论：对因特网的法律规范必须是透明、明确和平衡的。