联合国 A/54/213

大会

Distr.: General
10 August 1999
Chinese
Original: English/Arabic
Russian/Spanish

第五十四届会议

临时议程*项目 71

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/54/150。

一. 导言

1. 大会在 1998 年 12 月 4 日题为“从国际安全的角度来看信息和电信领域的发

展”的第 53/70 号决议第 2 段和第 3 段中请所有会员国向秘书长通报它们对下列问题的意见和评估:(a) 对信息安全问题的总体看法;(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) 应否订立国际原则,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五十四届会议提交报告。

2. 1999 年 3 月 19 日秘书长向各会员国发出一份普通照会,请它们按照大会的要求提出意见。收到的国家政府的答复见下文。

二. 收到的国家政府的答复

澳大利亚

[原件:英文]

[1999 年 6 月 2 日]

1. 澳大利亚主持经济合作与发展组织(经合组织)专家组的工作,该专家组负责编写经合组织信息系统安全问题的指导方针。澳大利亚还主持经合组织关于信息安全和隐私的工作队,该工作队除其它外负责监测信息安全的需要。澳大利亚参加国际标准化组织(标准化组织)关于信息技术安全标准的编写工作。澳大利亚在国内详细布置了政府信息安全的过程,澳大利亚标准协会同新西兰标准协会一起根据英国标准制订了信息安全管理的联合标准。目前澳大利亚的政府和工业界共同协作采取步骤,保护国家的信息基础设施。澳大利亚已进行立法,保护电信系统不受窃听、干扰和某种滥用。

2. 经合组织信息系统安全问题指导方针确定的和澳大利亚采用的信息安全目标是:“保护信息系统用户的利益免受信息系统不能使用、失密和不完整的损害。”

3. 随着技术的结合,可以扩大这项目标,把作为一种具体信息系统的电信系统包括在内。对信息系统的任何干扰和滥用都会影响它的使用性、保密性或完整性。不过在情况迅速变化时有可能编写仅针对技术的定义。

4. 澳大利亚不赞成联合国秘书处裁军事务部作为制订全球信息和电信系统安全问题国际原则的合适机构。电信和信息基础设施对贸易、经济发展、社会福利、执法和国家安全问题都有影响。其他论坛,如经合组织、国际标准化组织和国际电信联盟(电信联盟),已制订了关于这些问题的原则和指导方针,它们涉及的范围比大会第 53/70 号决议中提出的要广。此外,联合国亚洲和远东预防犯罪和罪犯待遇研究所(亚远预防犯罪所)和国际预防犯罪中心(预防犯罪中心)等国际机构正解决计算机犯罪问题。澳大利亚认为,联合国有关部门在计算机安全或滥用方面重复其他机构所做的工作没有任何好处。如果要汇编其他论坛所做工作的信息资源,澳大利亚将支持这样的建议。

白俄罗斯

[原件:英文]

[1999 年 5 月 25 日]

1. 白俄罗斯共和国完全支持大会 1998 年 12 月 4 日题为“从国际安全的角度来看信息和电信领域的发展”的第 53/70 号决议。大力运用新的信息技术和电信手段为加速世界文明的发展增添了最广泛的机遇。同时,正如大会在第 53/70 号决议中所述,“信息技术和手段可能会被用于不符合维护国际稳定与安全的宗旨,对各国的安全产生不利影响”。

2. 大会通过第 53/70 号决议是及时和相关的,因为它提请国际社会注意信息技术可能被用于战争并有必要防止新的信息技术和手段用于军事目的,那样这些技术就同大规模毁灭性武器不相上下了。还有,在大会通过第 53/70 号决议之后,就有可能具体考虑国际信息安全问题,包括未经授权干扰或滥用信息系统、电信系统和信息资源。最后,发展和商定国际信息安全的概念和国际法律原则是可取的办法,其目的在于增强全球信息系统和电信系统的安全并预防信息恐怖主义和犯罪行为。

文莱达鲁萨兰国

[原件:英文]

[1999 年 6 月 7 日]

关于大会 1998 年 12 月 4 日题为“从国际安全的角度来看信息和电信领域的发展”的第 53/70 号决议,

文莱达鲁萨兰国常驻联合国代表团谨转告文莱达鲁萨兰国国防部的以下意见:

“国防部作为负责国家安全的部门赞成信息技术领域的信息安全是重要问题。对国防部来说,在传输中能够用于和可能威胁国家安全的任何形式的信息都被认为是重要信息。然而,鉴于国防部同信息技术的联系并且该问题也在我国其他部门的处理之中,国防部将同有关机构合作,满足该决议的要求。要保护和保证国际通信的安全,就应该把这项责任列入国际法院的管辖范围。”

古巴

[原件:西班牙文]

[1999 年 6 月 28 日]

对信息安全问题的总体看法

1. 信息技术广泛应用于人类活动的几乎所有领域,人称“社会的计算机化”,并且由于世界各国日益依靠信息系统,许多人称当今时代为“信息时代”。不过这也造成了新的安全问题,这些问题不仅需要每个国家而且需要整个国际社会非常认真地加以考虑。

2. 为非和平目的利用新的信息技术和电信技术可能对国际安全产生潜在的危险,因此,联合国是探讨有关应付这种潜在危险的方式和途径的合适论坛。

3. 另外,必须采取必要措施,为各国,特别是本身缺少充足资源发展这类技术的欠发达国家,的发展提供这些技术。

4. 另一方面,全球化在信息和电信领域已成为现实,距离已不再是信息交流的障碍;同时,便利信息交流的系统在安全方面却面临越来越大的危险。必须强调,全球化包含一种标准化,从而使干涉这些系统更加容易。

5. 我们不应忘记,我们谈论的技术起源于发达国家,其中美利坚合众国是世界上最大的霸权主义者,它在信息和电信领域尤其处于领先地位,这使它能够制订技术标准,从而利用信息和电信系统作为侵略的手段。

6. 相反,欠发达国家为了在新环境中生存没有其他选择,只有接受这些技术。这些国家大多数时候都没有充分意识到其中的危险,往往没有充分利用安全的安排、服务或机制。鉴于信息技术和电信技术广泛应用于人的发展的各个方面,这就造成信息系统非常易受伤害,可能造成破坏国际安全的状况。

7. 古巴很高兴有机会在大会审议这个项目,大会曾按照这项倡议以协商一致通过了第 53/70 号决议。古巴意识到该项目的重要性,将积极参加上述决议要求的评估工作。

信息安全基本概念的定义,包括未经授权干涉或滥用信息系统、电信系统和信息资源

8. 在我们生活的世界,信息和电信技术的应用正以前所未有的速度增加,令人遗憾的是,这也造成有些国家为了对其他国家实施侵略政策而把它们用于敌对目的。

9. 在这方面应指出的是,全球网络,特别是互联网,的发展和普及具有重大的影响。尽管这些网络的应用增加,但是信息和电信系统还是在完全合作的基础上运作。这点非常重要,因为互联网的自愿性质既是它的威力,又是它的最大缺陷。

10. 各国对信息网络的运作没有采用统一的立法,因而确保全球网络有效运作和增强安全的一套共同规则是自愿性的。

11. 然而,鉴于这些全球网络的联系是非强制性的,可以有理由认为,管理这类网络的任何行为规则都应是联系协议的一部分,而违反这些规则,不论现有的法律基础如何,都可能受到制裁。

12. 信息安全包括保护信息的机密(只有有权使用信息的人才能获得这些信息)、保护信息免受未经授权的修改(完整性)、保护信息系统随时提供服务(可用性)和防止未经授权的访问。

13. 在这种情况下,必须考虑一些基本的标准:

(a) 用户对他们自己的行为负责;换句话说,不论保护信息系统的手段多么软弱,未经授权访问计算机或未经授权使用网络是明显违反行为守则的行为;

(b) 使用这些技术的组织负责保证他们的雇员适当使用它们并为此制订安全政策、控制措施及程序。同样,每个国家应建立适当机制,确保设在其领土的组织遵守这些要求;

(c) 计算机服务和网络的提供者负责维护所操作系统的安全。他们还负责把他们的安全政策和任何政策变化通知用户;

(d) 系统卖主和供应商负责提供装有适当安全控制部件的可靠系统。卖主或供应商必须在系统上市前评价每个系统的安全控制状况。每件产品必须说明其中的安全性能。系统卖主和供应商有义务修理他们出售或免费分发的系统中有关部件的故障;

(e) 用户、服务供应商和软件及硬件卖主负责在安全方面合作。如果发现一个网址被侵入,希望每个网址都通知其他网址并相互帮助采取对付破坏安全行为的措施。这类帮助可以包括跟踪连接点、查明破坏行为和法律援助。

14. 侵入信息网络的个人主要企图:

(a) 获得、篡改或销毁信息。这无疑是大多数入侵者的主要目的;

(b) 侵入他人计算机和仿佛受权用户那样使用它们;

(c) 获得进一步入侵的分离点。可能完全为了从这些系统发起新的进攻而侵入系统;

(d) 拒绝提供服务,即让需要信息和有权使用信息的人得不到信息;

(e) 获得知名度,这对万维网服务机非常有用。

15. 滥用信息系统、电信系统和信息资源,特别是某些国家利用这些系统和资源执行干涉他国事务的政策,就是侵犯了受影响国家的主权和独立并可能形成严重威胁国际安全的紧张局势的焦点。

16. 各国都在不断努力实现为国家利益服务的政治目的,根据既定的国际准则,这除其它外包含滥用无线电台和电视台,以破坏被当作敌国的他国宪法次序。

17. 例如,古巴就是受到上段提及的政策影响的国家。古巴几十年来一直受到美国无线电台和电视台的侵袭,这就可以说明问题的严重程度,这是世界上军事、经济和政治最强国推行顽固侵略政策的一部分,它公开宣布的目的就是推翻古巴政府。

18. 在这方面,例如到 1999 年 4 月为止,共有 17 个设在美利坚合众国领土的电台向古巴广播煽动性信息。

19. 每天中波、短波和调频无线电台广播 288.5 至 306.5 小时;每周 2084.5 小时;如果加上每周发射的电视讯号,那共达 2089 小时。

20. 在多数情况下,这类信息煽动古巴公民进行民事骚乱和参与破坏和恐怖主义行动。

21. 古巴一贯赞成在平等和尊重国家主权和独立的基础上解决国家间的分歧并在许多场合公开表明这个观点。这个立场仍然没有改变。

宜制订国际原则,加强全球信息系统和电信系统的安全并协助打击信息恐怖主义和犯罪行为

22. 毫无疑问,新信息技术的发展要求同时努力确保国际法在这方面的逐步发展,包括阐明可加强信息系统安全的适当法律框架。

23. 这项任务并不简单,因为我们考虑到还存在不少问题,它们都需要详细说明普遍接受的定义,随后才可编写有助于实现安全领域目标的新原则。

24. 全球网络的性质超越每个国家的管辖范围;在许多情况下,国家根本不可能再依靠地理边界管辖。还有,除了其他因素外,国家的不均等发展造成很难以制订可普遍适用于分享这些技术的所有国家的统一国际规则。

25. 不过,我们不必从头开始,因为各国为了跟上最近技术进步的步伐,已在许多多边论坛上商定和通过了公认的原则和国际法律文书。这些原则和文书非常有益于巩固或发展新的国际原则,加强全球信息系统和电信系统的安全并协助打击信息恐怖主义和犯罪行为。

26. 要举几个这类协议的例子,古巴认为可考虑以下文书:

(a) 大会 1947 年 11 月 3 日第 110(II)号决议,其中谴斥.....意图煽动或鼓励任何威胁和平,破坏和平,或侵略行为的宣传;

(b) 1982 年在内罗毕通过的《国际电信公约》和联合国教育、科学及文化组织(教科文组织)和国际电信联盟(电信联盟)通过的有关国际法律文书;

(c) 大会通过的各国利用人造地球卫星进行国际直接电视广播所应遵守的原则,其中规定,进行这类活动时应遵守国际法并有利于从维护国际和平与安全角度增进国家和人民之间的相互了解和加强他们的友好关系与合作;

(d) 《关于禁止发展、生产、储存和使用化学武器及销毁此种武器的公约》,公约附件中规定,保护也能用于阐明上述原则的有用参考资料的机密信息。

27. 最后,古巴认为,联合国在分析该问题时应发挥领导作用,除其它外,作为这种作用的一部分,联合国应承认每个国家都有权采用安全保护系统保护它的信息系统和电信系统,并建议会员国通过有关法律,制裁编写和散发计算机病毒和其他有害程序的行为。此外,可以在联合国的框架内签署有法律约束力的多边协定,禁止侵入信息系统和电信系统的行为。还可考虑签署有关协定,保证为和平目的利用所发展的新技术和各国均可使用新技术。

阿曼

[原件:阿拉伯文]

[1999 年 6 月 22 日]

1. 苏丹国电信局不负责向用户提供信息,仅提供便利进入信息系统的网络和技术。

2. 电信局作为网络和技术的提供者对信息安全问题有总的看法。可以说,未经授权者有可能利用电信局提供的技术获取信息,从而会产生消极影响。

3. 电信局作为电信服务提供者通常不负责用户信息的安全,用户必须自己采取必要的保障措施来满足其信息的安全要求。然而,电信局可以通过某些服务,如互联网,限制公用域信息的存取。

4. 关于信息安全的基本概念,苏丹国实施的条例,特别是版权条例,都规定信息具有物质和道德的价值,从而向它提供法律保护。通过这项原则可以确定信息安全的基本概念。其中最重要的内容如下:

(a) 非法截取信息和数据;

(b) 非法进入计算机系统;

(c) 刺探和窃听数据和信息;

(d) 侵犯他人的隐私权或保密权;

(e) 提供无论何种数据或电子储存的文件;

(f) 销毁、篡改和转移数据;

(g) 收集和盗用信息;

(h) 泄漏信息和数据;

(i) 以篡改或伪造手段侵入计算机程序;

(j) 违反知识产权非法复制程序;

(k) 偷窃和使用网络地址;

(l) 在收件者收到函件前,修改、增加或删除传输中的原函件信息;

(m) 引进病毒和搞乱网络内容;

(n) 实际(具体)破坏设备和建筑物。

5. 可增强信息系统安全的方法有以下各点:

(a) 对有关人员进行危险存在和预防危险的安全教育;

(b) 存取管制;即向受权存取某种信息的人员发放各种许可证;

(c) 在真正用户间利用数字标识进行通讯联系;

(d) 硬件和软件都加密;

(e) 采用防火墙防止输入已被搞乱的信息;

(f) 采用抗病毒措施。

6. 苏丹国希望制订加强全球信息系统安全的国际原则,尤其因为它引进了互联网服务,从而面临信息安全方面的各种危险。

卡塔尔

[原件:英文]

[1999 年 6 月 10 日]

卡塔尔国有关当局已对大会 1998 年 12 月 4 日第 53/70 号决议第 2 段和第 3 段提出以下意见和评价:

(a) 对信息安全问题的总体看法。通过交流专门知识、了解未经授权的干涉的种种危险以及这种干涉对安全和财政事务的影响,就能从总体上认识信息安全的问题;

(b) 信息安全基本概念的定义。正如下文表 1 和表 2 所示,加强安全的基本概念就是为确保信息交流方式和途径的可靠性而不得不采取的步骤以及意外产生的各种挑战,下表中除这方面的新挑战之外,列出了各个阶段确保信息安全的必要步骤;

(c) 增强通信安全的原则。发展传递信息的手段就能增强信息的安全,考虑到所涉及的高昂财政费用,以下各点对增强通信安全最为重要:

㈠ 利用经专门设计能交流某些信息的非常规通信程序书;

㈡ 采用专用编码系统,其中不使用大批量生产的程序;

㈢ 改用不同的计时和编码程序。

表 1

网络安全措施

安全步骤		
威胁	安全措施	功能
非法截取、阅读或修改数据	加密(数据加密标准、RSA 算法)	把数据编码,防止有人捣乱
合法用户获得他或她未经授权获得的数据	存取控制软件	指定和管理用户的特定权利
用户为了舞弊不如实说明他或她的身份	证实身份	其技术包括加密软件和专用卡,以核实送件者和收件者的身份
未经授权的用户从一个网络进入另一个网络	防火墙	筛选并防止某些通信业务进入网络或服务器
黑客利用服务器操作系统的漏洞获得并搞乱数据	操作系统工具	弥补操作系统中已知的漏洞

注:DES:数据加密标准。

RSA:里韦斯特、沙米尔和阿德勒曼(研制者的姓)。

表 2

安全挑战

变化	挑战
当今网络	安全受到威胁的原因
包括多得多的便携式计算机	便携式计算机容易被盗
有更多的无线连接	无线连接更易受窃听
分散在更大的区域	遥控场址更难保护
同更多种平台连接	用户忘记密码或写下几个密码
越来越多地同互联网这样的公用网络相互连接	黑客悄悄跟踪公用网络
更多采用 UNIX 计算机系统	UNIX 操作系统特别易受损害

俄罗斯联邦

[原件:俄文]

[1999 年 6 月 9 日]

一般性评论

1. 现阶段世界科学和技术进步的特征之一是全球信息革命--最新信息技术和全球电讯手段的迅速发展和普遍运用。信息革命影响到国家重大活动的所有领域,它正为发展国际合作开辟新的机会,并建立了一个全球信息领域,使信息逐渐成为一个国家财富及其战略资源中一个极其宝贵的部分。

2. 与此同时,日益明显的是,在这一进程出现积极方面的同时,也存在着一种现实的危险:信息领域的发展可以被用于从事与维护国际稳定与安全目标以及遵守各国主权平等、和平解决争端和冲突、不使用武力、不干涉内部事务和尊重人权和自由等原则不相符的目的。

3. 使用最新信息技术来强化国家军事潜力的做法会改变全球和区域的力量平衡,导致传统和新出现的力量和势力中心之间出现紧张状况。

4. 国际领域内正出现一个全新的对抗领域,存在着信息和通讯领域科技发展可能导致军备竞赛升级的危险。在此情况下,各国的国家安全以及区域和全球的总体国际集体安全体系都受到影响。

5. 我们指的是“信息武器”的出现。视一个社会信息技术的水平以及其重要结构的脆弱程度而定,这种武器的使用可以产生与大规模毁灭性武器相类似的破坏性后果。很显然,这种武器可能会被恐怖分子、极端分子或犯罪团伙以及违法个人使用。

6. 因此,信息武器的普遍性、保密性或非人格性以及它跨越国界广泛使用的可能性及其经济合算性和总体效率,使它成为施加影响的一种及其危险的手段,当今的国际法几乎没有办法规范这一武器的发展和使用。

7. 在这方面,显然需要在国际上对全世界民用和军用信息技术的发展订立法律规范,并制定出针对能够符合国际安全需要的信息安全的协调国际政策。

拟议措施

8. 国际社会在这方面所作的进一步努力可以依据大会 1998 年 12 月 4 日协商一致通过的题为“从国际安全的角度来看信息和电信领域的发展”的大会第 53/70。关于这一议题的决议草案是由俄罗斯联邦提出的。

9. 大会必须通过关于信息安全问题的决议,以减轻利用信息来从事恐怖主义、犯罪或军事活动的危险。

10. 必须继续联合审议信息安全领域的状况,以明确现有的所有立场和看法,并在倡导信息安全概念的共同努力中将它们考虑进去。

11. 随着共同办法和趋向的确定,应开始制定国际原则(例如一种制度、一套国家行为守则)方面的工作,以加强国际信息安全。首先,这些原则的形式应是多边宣言;其后应将这些原则纳入一项多边国际法律文书。此外还应在日内瓦裁军谈判会议的框架内开展这方面的工作。

12. 与此同时,国际社会应将上述原则作为一个整体来审议和通过,也就是说,要考虑到军事、恐怖主义或犯罪性质的威胁,并且着眼于把这些原则适用于军事和民用领域。

对国际信息安全的主要威胁

13. 对国际信息安全的主要威胁是:

(a) 建立和使用影响或破坏另一国信息资源和信息的手段;

(b) 蓄意使用信息来影响另一国的要害结构;

(c) 使用信息技术破坏一国的政治和社会制度;从心理上控制一国的居民,以破坏社会的稳定;

(d) 国家采取行动操纵和控制信息领域,阻止获取最新信息技术,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;

(e) 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结构;

(f) 国家制定和采行各种计划或理论,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;

(g) 利用信息技术和手段来危害信息领域的人权和自由;

(h) 违背国际法原则和准则以及具体国家国内立法,无节制地跨界散播信息;

(i) 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,以及损害传统的文化、道德、伦理和审美价值;

(j) 信息扩展以及垄断另一国国家信息和电信基础结构,包括在国际信息领域对其运作设定条件。

建立国际信息安全制度的主要任务和目标

14. 有必要建立国际法律基础,以便:

(a) 确定信息战的主要特征及其分类;

(b) 确定信息武器的主要特征及其分类,以及可视为信息武器的方法和手段;

(c) 限制信息武器的流动;

(d) 禁止发展、传播或使用特别危险的信息武器;

(e) 防止信息战争的威胁;

(f) 禁止将信息技术和手段用于敌对目的,尤其是针对商定类别的设施;

(g) 确认针对要害结构使用信息武器的后果相当于使用大规模毁灭性武器;

(h) 建立以个人、社会和国家利益平衡为基础的公平和安全国际信息交换的条件;

(i) 防止为恐怖主义或其他犯罪目的威胁使用信息技术和手段;

(j) 防止威胁使用信息技术和手段来影响社会意识,以此破坏社会和国家的稳定;

(k) 制定相互通知和防止未经许可而使用信息影响他国的程序;

(l) 建立机制来解决信息安全领域的冲突;

(m) 建立国际制度来确定查验信息技术和手段(包括软件和硬件),以保障它们的信息安全;

(n) 制定执法机构之间的国际合作制度,以防止信息领域的犯罪活动;

(o) 建立机制来监测国际信息安全制度条件的遵守情况;

(p) 协调国家立法,以确保信息安全。

与国际信息安全有关的基本概念

15. 与国际信息安全有关的基本概念包括:

(a) 信息领域。有关建立、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的活动领域;

(b) 信息资源。信息基础结构(硬件以及建立、处理、储存和传递信息的系统),包括数据文件和数据库以及信息和信息流动;

(c) 信息战。国家之间在信息领域进行对抗,破坏信息系统、程序和资源以及要害结构,损害另一国的政治和社会制度,以及对一国居民进行大规模的心理控制,危害社会的稳定;

(d) 信息武器。为破坏另一国的信息资源、程序和系统而使用的办法和手段;利用信息来破坏一国的国防、行政、政治、社会、经济或者其他重要系统,以及对一国居民进行大规模控制,以破坏社会和国家的稳定;

(e) 信息安全。在信息领域保护个人、社会和国家的基本利益,包括信息和电信基础结构以及信息本身的特征,例如完整性、客观性、可获性和保密性;

(f) 对信息安全的威胁。危害个人、社会和国家在信息领域的基本利益的因素;

(g) 国际信息安全。排除危害国际稳定行为并制止在信息领域威胁国家和国际社会安全的国际关系;

(h) 信息和电信系统及信息资源非法利用。未经有关授权或以违反有关规则、立法或国际法准则的方式使用电信和信息系统及资源;

(i) 未经批准而对信息和电信系统及信息资源进行的干扰。干扰信息的搜集、处理、积累、储存、搜寻、传播或使用,以此破坏信息系统的正常运作,或侵害信息资源的完整性、保密性或可获性;

(j) 要害结构。一国的设施、系统和机构,蓄意对信息资源施加影响,其后果可能直接影响国家安全(运输、能源供应、信贷和财政、通讯、国家行政机关、国防系统、执法机构、战略信息资源、科学设施和科技发展、构成高度技术与环境风险的设施以及负责消除自然灾害或其他紧急情况后果的机构);

(k) 国际信息恐怖主义。在国际信息领域使用电信或信息系统及资源或对这些系统或资源施加影响,以达到恐怖主义目的;

(l) 国际信息犯罪。在国际信息领域使用电信或信息系统及资源或对这些系统系统或资源施加影响,以达到非法目的。

沙特阿拉伯

[原件:阿拉伯文]

[1999 年 5 月 27 日]

在日益依赖电子信息系统的每个国家,许多政府和私营机构在信息技术中都取得了进展。然而,与这些进展相对应,国际势力为扰乱、损害和干挠这些信息系统以达到破坏和恐怖主义目的而从事的活动数量也伴随增加。这导致经济、社会和安全受到破坏。必须制定国际原则和法律来对付威胁和危害信息安全的现象,打击和取缔此类国际行为。有关国际组织必须将那些犯下此种罪行的人绳之以法,予以惩处。

大不列颠和北爱尔兰联合王国

[原件:英文]

[1999 年 5 月 30 日]

一般性评论

1. 以信息为基础的各种系统在全球相互联接,其程度之广,使许多国家,甚至所有国家的关键基础机构的重要部分面临着可能受到犯罪分子和恐怖分子电子袭击的威胁。电子袭击的危险在目前也许不太大,但随着公共和私营部门都日益依赖日益相互联接的计算机系统,此一危险将会加大。此外,由于各个系统是在国际上相互联接的,因而这是一种跨界的威胁。所以,犯罪分子和恐怖分子为了邪恶目的企图渗入我们各系统,这给联合国所有会员构成了一个挑战。因此,大不列颠及北爱尔兰联合王国欢迎采取步骤,探讨我们可以以哪些双边和多边手段来保护以信息为基础的关键基础机构免遭此种攻击。

国内行动

2. 为此,1999 年 1 月,女王陛下政府宣布采取步骤尽量减小联合王国重要国家基础设施遭受电子袭击的危险。国内措施包括:

(a) 确保政府内所有关键系统得以确定,而且这些系统的保护受到有效的管理与监督;

(b) 与私营部门协作制定与所面临危险程度相称的措施,确保关键国家基础设施内的重要系统得到适当标准的保护;

(c) 通过实施现有推广最佳做法的行动,在私营部门更广泛地提高对信息安全的认识和信息安全标准。

国际行动

3. 与此同时,跨界联接意味着对其他国家境内系统的攻击可能会给联合王国本国的关键国家基础设施产生波及影响;以第三国为行动基地的恐怖分子和犯罪分子可能会企图攻击联合王国境内的系统。因此,联合王国认识到必须开展国际合作来对付邪恶攻击的威胁,并正在考虑加深与其国际伙伴就这些问题进行的对话。其中包括八国集团高技术犯罪问题小组关于相互法律援助的工作,以及欧洲委员会关于网络犯罪问题公约的工作。

4. 联合王国认为,联合国应监测这些论坛和其他论坛的工作,以在适当时候评价它在这一领域可以采取何种有助益的实质行动。这可包括制定国际原则来加强全球各系统的安全,帮助打击信息恐怖主义和犯罪行为。

美利坚合众国

[原件:英文]

[1999 年 5 月 20 日]

对信息安全问题和基本概念定义的一般看法

1. 美利坚合众国认为,信息安全是一个广泛而复杂的问题,它包含众多因素,影响到个人、团体和政府的许多不同活动。尽管这个普遍议题包括涉及国际和平与安全的方面(第一委员会的工作),它也包括与全球通讯技术有关的方面以及与经济合作和贸易、国际产权、执法、反恐怖合作及第二或第六委员会所审议其他问题相联系的非技术性问题。政府的各种行动和方案绝不是唯一的适当重点,因为信息安全也涉及个人、团体、企业和私营部门其他组织的重大关切。

国际安全方面

2. 在武装冲突期间,各国采用了与信息安全相关的各种技术。无线射频干扰和电磁对抗是两个明显的例子;这些技术有着很长的历史。今后,军事力量必须保护其自身的数据网和其他与计算机有关的系统。此外,会员国需要有能力在自然灾害或灾难性紧急情况导致主要通讯设施或公共和私营部门其他数据网络丧失功能情况下使基本信息系统恢复运作。信息安全还延伸到军事能力和国家安全其他方面有关信息的保护。

经济、贸易和技术因素

3. 信息安全包括需要保护商业性质的科学研究以及生产技术和其他类型产权数据(如销售计划和客户服务信息)。

4. 信息安全还要求执行国际知识产权协议(如视听材料以及计算机软件),以保护它不被非法拷贝和出售。隐私权的保护是信息安全的又一方面,即确保通过公共

国际网络或私人数据网传递的个人和商业信息的安全。

5. 在技术方面,国际电信联盟的条例和国家主管部门的活动确保电子信号的相互兼容、电磁波谱的适当使用以及国际网络的广泛可靠性。这些职能同样适用于提供诸如声频和数据传递等广泛服务的卫星以及用于航空和航海和搜寻与救护服务所需的定位数据和其他信息。此外,设计和安全标准为包括计算机在内各种电子设备的产商和用户提供了重要保证。所有这些管理和行政职能都可通过信息安全的广泛概念来确定。

执法和反恐怖合作

6. 对以信息为基础的技术的广泛依赖导致出现了空前的全球联接和相互依赖,致使公共和私营部门全国性和国际性活动的许多方面在理论上可能会遭受犯罪分子和恐怖分子非法使用的危险。

7. 虽然各国依赖信息技术的程度各有不同,但依靠此类通讯的活动的范围--经济、商业、工业、教育、法律--意味着所有国家都可能由于此种通讯被利用来从事犯罪目的而受到危害。此外,这一依赖性可能会加剧,因为此类技术对于政府的稳定运作以及对于保持各国间相互联系的重要全球商业和通讯系统的维护而言,日益重要。

8. 因此,美国把滥用信息技术来从事犯罪活动视作对所有各国利益的一种挑战,并赞成其他国家表示的关切,即我们应努力推动采取适当的单边和多边办法来确保我们依赖信息技术的资源的完整性。

9. 同样,美国认为非法侵入或企图破坏或更改其国家信息系统任何部分的任何行为都是对其重要国家基础设施的潜在危险,因而是对其国家利益的威胁。美国认识到此一威胁的潜在严重性,因而在国家一级发起了长期的公共和私营部门方案,目的是保护其重要的国家基础设施。然而。美国也认识到,随着许多此类基本基础设施在全球范围的日益相互依赖,它保护本国信息系统的国家努力的成功最终将部分取决于其国界以外与其相联的系统的安全程度。

10. 因此,美利坚合众国认为,所有国家都必须采取必要的国家步骤,确保其国内信息系统的完整性,同时确保依照法律最严厉地惩处那些在其国界内企图破坏信息系统的犯罪分子或国际恐怖分子。每个国家都有义务采取行动,确保本国的信息系统是可靠的,而且尽可能保证它们不会被犯罪分子滥用或者不提供服务,此外在信息系统中断的情况下能够使这些系统迅速恢复运作。

11. 美国的刑法禁止干扰美国的信息基础设施。美国敦促所有国家审查其国内法规,确保它们适当规定对滥用信息系统来从事犯罪和恐怖主义目的的行为进行起诉。美国意识到有必要多次修改其与计算机有关的法规,以改进法规,使之能对付新的问题。

制定国际原则的必要性

12. 正如前面已经指出的那样,信息安全是一个广泛而复杂的问题。它带有许多以极其复杂的方式彼此相联系的许多层面。鉴于明显需要分析信息安全的所有方面,并对它们彼此联系的方式有一个彻底的理解,针对信息安全所有方面制定范围过广的原则还为时过早。国际社会需要在采取进一步行动之前进行大量有系统的思考。为此,各会员国应征求我们各自政府和社会中众多专家的意见与看法。

13. 然而,业已很明显的是,必须开展国际合作,以有效对付信息恐怖主义和犯罪活动所导致的新的复杂问题。目前在处理国际合作问题方面正在不断开展若干多边努力。欧洲委员会正在研讨一项关于网络犯罪问题的公约草案;八国集团高技术犯罪问题小组正在审议有关相互法律援助和有关高技术犯罪问题方面的措施;美洲国家组织也设立了一个小组来研究这些领域;联合国亚洲和远东预防犯罪和罪犯待遇研究所正在联合国范围内审查有关的问题。

14. 所有这些正在开展的所有努力都有其作用,当然应允许其发展并产生结果。如果大会所制定的战略或所规定的活动可能会阻碍或干扰国际社会业已开展的工作,那将是非常不明智的。