联合国 A/68/156

大会

Distr.: General
16 July 2013
Chinese
Original: English/Russian/Spanish

第六十八届会议

暂定项目表 * 项目 94

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/68/50。

13-39734 (C) 120813 120813

一. 导言

1. 2012 年 12 月 3 日，大会通过了题为“从国际安全的角度来看信息和电信领域的发展”的第 67/27 号决议。在决议第 3 段中，大会邀请所有会员国在考虑到从国际安全角度看信息和电信领域的发展政府专家组的报告(A/65/201)所载评估意见和建议的情况下，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) 国家一级为加强信息安全和促进这一领域的国际合作所作的努力；

(c) 决议第 2 段所述概念的内容；

(d) 国际社会为加强全球一级的信息安全可能采取的措施。

2. 按照这项要求，2013 年 2 月 22 日向各会员国发出一份普通照会，请他们就此提供资料。所收到的答复载于下文第二节。以后再收到的其他答复将作为本报告增编印发。

二. 从各国政府收到的答复

古巴

[原件：西班牙文]
[2013 年 5 月 20 日]

利用电信出于恶意地公开或秘密破坏各国的法律和政治秩序，这种行为违反这一领域公认的国际准则，产生的影响可能会造成紧张局势并损害国际和平与安全。

古巴完全赞同第 67/27 号决议表达的关切，担忧信息技术和工具被用于可能会影响国际稳定与安全、危及国家的完整并损害各国的民事和军事领域的安全的目的。这项决议还正确地强调有必要防止为犯罪或恐怖主义目的使用信息资料和技术。

对此，古巴再次谴责历届美国政府将针对古巴的广播和电视战升级，违反了关于无线电领域的现行国际法规。这一攻势没有顾及到可能对国际和平与安全造成的破坏，而且制造了危险局势，例如不经古巴同意，用军用飞机向古巴共和国播放电视信号。

从飞机上发送信号违反了国际电信联盟(国际电联)无线电条例第 42.4 条规定，其禁止航空器电台在海上或海面上空进行广播。

2012 年，美国做了 192 次飞行，期间，除了从飞机上向古巴领土非法传送电视信号外，同时还进行了非法调频无线电传输。这些行为干扰了已在国际电联国际频率登记总表登记的古巴电视台。

位于美国境内的广播公司通过 30 个中、短波、调频电台和电视台对古巴每周平均非法播放 2 400 小时的电台和电视节目。其中若干电台所属的或所服务的组织与美国境内的知名反古巴恐怖分子有牵连；这些人播放煽动破坏、政治攻击和暗杀的节目以及其他典型的恐怖主义广播题材。

对古巴的非法电台和电视广播旨在促进非法移徙，鼓励和煽动暴力、蔑视宪法秩序和实施恐怖主义行为。古巴重申，使用信息明确地旨在颠覆其他国家的内部秩序、侵犯其主权及插手和干涉他国内部事务的行为是非法的。

对古巴的这些挑衅性广播违反了《国际无线电公约》所载的关于使用无线电电子光谱的国际准则，而美国政府是该《公约》缔约国。

古巴支持大会第 67/27 号决议，并将继续促进全球信息和通讯技术的和平发展，使之为全人类造福。

西班牙

［原件：西班牙文］
［2013 年 5 月 29 日］

1. 导言

信息安全是信息社会的重要方面。技术进步促使以多种格式处理和存储信息的能力持续快速增长；另一方面，通信领域可用的带宽大量增加，使人能够几乎实时传输和接收大量信息，而不需要特别复杂的基础设施。

这些技术进步使人能更便利地获得各种信息，但也方便了为非法目的使用或获取信息的作法，尤其是国家或跨国行动者之间将通信和信息系统用于敌对或犯罪目的，甚至用来实施恐怖行为或攻击。

近年来，犯罪组织、尤其是恐怖主义组织利用互联网的情况呈增长趋势；它们主要是利用互联网的两大优势，即其全球性和高度隐匿性。

因此，必须在社会和信息技术发展与国家和国际法规同期发展之间取得平衡；这些法规应当是适应新技术环境的最新现代法规，要能够应对需要保护信息的挑战，以防止非法使用而不限制个人权利和自由。

2. 滥用因特网进行恐怖主义活动

今天，由于恐怖组织使用互联网而产生的主要威胁如下：

(a) 利用互联网作为武器，即将其作为攻击重要基础设施的电脑系统或互联网基础设施本身的一种手段。这种类型的攻击在普通犯罪领域是比较常见的，但爱沙尼亚 2007 年受到的攻击表明，一国的信息基础设施也可能受到这类攻击的影响。与此类威胁直接相关的有，最近几年新出现的恶意软件大幅度增加，以及“僵尸”电脑网络被用于对计算机系统发起攻击。

(b) 以互联网为手段开展其他活动，主要有以下：

- 通信活动。犯罪组织以互联网取代固定电话或移动电话等其他手段进行通信。互联网安全和匿名通信最常用工具包括电子邮件、即时讯息程序和论坛。
- 散布与恐怖活动有关的宣传和材料。目前有数以千计涉及恐怖活动或煽动暴力的网站，随着 Web 2.0 和社交网络现象的出现，这种趋势愈演愈烈。如何防止恐怖组织利用因特网是一个非常复杂的问题，因为这些网站很容易迁移。这是一个跨国现象，因为承载和管理网页的服务器可能在若干国家，而且可能不是在有关恐怖组织开展行动的国家；若这些国家之间没有双边协定，则会造成法律真空。
- 招募活动。有时互联网被用来作为开展招募活动的手段，特别是通过论坛和即时讯息程序。
- 筹资。互联网还为恐怖组织开展获取资金的活动提供了机会。特别值得注意的是，恐怖组织可通过互联网参与开展欺诈、敲诈勒索和洗钱活动，以此为手段获取资金。
- 传播培训手册。恐怖组织通过互联网传播恐怖主义技术、制造爆炸物和武器操作手册。
- 收集信息实施攻击。互联网是一个非常重要的信息来源，经常被恐怖组织用来获取有关其活动目标的资料，无论是个人、组织还是基础设施。

3. 国家一级为打击恐怖组织利用互联网采取的措施

3.1. 立法措施

在各国采取的措施中，西班牙近年来、特别是在 2007 年开展了大量工作，在其法律系统中增加了关于信息安全以及自由行使《世界人权宣言》和《西班牙宪法》所赋自由和权利的一系列法律。制定的广泛法律法规既包括纯粹国内内容，又包括欧洲联盟指令；为实现上述目标，这些法律法规实施了新的信息安全标准，认为要在维护信息保密性的同时实现适度保护，大多数情况下最重要的是保持信息的完整性和可用性。需要指出的有：

- 规管个人资料自动处理的 1992 年 10 月 29 日第 5/1992 号组织法，其主要想法是建立预防机制，防止信息处理造成侵犯隐私，及其各项衍生规定。

- 保护个人资料的 1999 年 12 月 13 日第 15/1999 号组织法，目的是在处理个人资料中保障和保护公众自由和自然人的基本权利，特别是其荣誉与个人和家庭隐私，及其各项衍生规定。

- 关于电子签名的 1999 年 9 月 17 日第 14/1999 号皇家法令，以促进企业、公民和公共行政活动中迅速引进新的电子通信安全技术，将 1999 年 12 月 13 日欧洲议会和欧洲委员会第 1999/93/CE 号指令纳入西班牙法律法规，该指令制定了关于电子签名的欧盟框架。关于电子签名的 2003 年 12 月 19 日第 59/2003 号法，根据实施皇家法令后积累的经验纳入修改内容，更新了这项框架。

- 规管国家情报中心的 2002 年 5 月 6 日第 11/2002 号法以及后来规管国家情报中心的 2004 年 3 月 12 日第 421/2004 号皇家法令，规定国家情报中心负责协调使用数字媒体和程序的各种行政机构的行动，保障这一领域的信息技术安全，并确保遵守关于保护机密信息的法规等等。

- 关于信息社会和电子商务的 2002 年 7 月 11 日第 34/2002 号法，将关于信息社会服务某些方面、特别是内部市场电子商务的 2000 年 6 月 8 日第 2000/31/CE 号指令(电子商务指令)纳入西班牙法律。该法还纳入了欧洲议会和理事会关于保护消费者权益方面中止行为的 1998 年 5 月 19 日 98/27/CE 指令的部分内容，规定可依其规定，对违反该法规定的行为采取中止行动。

- 2003 年 11 月 3 日第 32/2003 号一般电信法，规管网络运营和提供电信服务。

- 关于电子签名的 2003 年 12 月 19 日第 59/2003 号法，如上所述。

- 关于公民电子获得公共服务的 2007 年 6 月 22 日第 11/2007 号法，规管公民与公共行政之间通过使用电子、计算机及通信技术和媒体进行交流。

- 规管警方从脱氧核糖核酸(DNA)获得的身份查验数据库的 2007 年 10 月 8 日第 10/2007 号组织法，建立统一收集国家安全部门储藏身份查验数据文件的数据库，这些数据是在刑事调查、尸体鉴定程序或失踪人员调查中通过 DNA 分析取得的。

- 关于电子通信和公共通信网络的数据保存的 2007 年 10 月 18 日第 25/2007 号法，对在这一领域进行的调查有积极影响。

- 2007 年 12 月 21 日第 1720/2007 号皇家法令，批准了 12 月 13 日保护个人数据的第 15/1999 号组织法的实施条例。
- 2007 年 12 月 28 日第 56/2007 号法，涉及到推动信息社会的措施。
- 对下列有关恐怖组织因特网活动的网络犯罪的刑事定罪：
  - 电脑破坏，刑法第 264 条
  - 威胁，刑法第 169 条及以下
  - 宣扬称颂恐怖主义，刑法第 578 条

3.2. 其他措施

- 成立打击犯罪集团使用互联网的专门执法小组。
- 参加欧洲刑警组织开发的“检查网络”项目。
- 国家情报中心的国家密码学中心每天都大力促进打击网络攻击的工作。特别是其计算机应急小组有能力应对信息安全事故。2007 年初作为西班牙一个政府机构设立的计算机应急小组参加主要国际论坛，交流关于网络安全的目标、想法和信息。
- 设立保护关键性基础设施国家中心。
- 国防部在网络防御领域正采取各种措施。特别是，国防参谋长参与北大西洋公约组织(北约)在爱沙尼亚塔林的网络防御英才中心，西班牙自该中心成立以来一直予以资助并提供了两名专家。国王陛下最近访问了中心，在访问期间国王陛下强调了西班牙致力于国际网络安全倡议，这表明中心在国际打击网络恐怖主义的努力中的作用日益重要。
- 北约在网络防御活动方面非常活跃，制定了一个构想，通过了一项政策，并任命了一个联盟的网络防御管理机构。
- 欧洲安全与合作组织(欧安组织)设立了一个建立信任措施非正式工作组，以便降低因采用信息和通信技术产生的冲突风险。该工作组的目标是通过为使用信息和通信技术制定政治和军事建立信任措施，减少网络攻击的可能性，同时通过国际合作加强共同安全，且提高清晰度和透明度，并减少因误解可能导致冲突升级的风险。
- 国家安全计划制定了使用电子媒体的国家安全政策，其植根于可以充分保护信息的基本原则和最低要求，各政府部门都参与其工作。其法律依据是根据第 11/2007 号法令第 42 条将于近期出台的一项皇家法令。西班牙的安全战略提出了该国的主要安全威胁和风险，并制定应对措施，

同时明确规定网络空间是必须采取行动的领域之一。这种分析为制定应对策略、建设能力和实施行政改革奠定了基础。

第 2012 号国防指令列出了西班牙必须应对的全球威胁，指明网络攻击是主要风险之一，只能通过各方力量的联合方可避免，就西班牙而言，联合力量将以北约和欧洲联盟为基础，但还需要得到对监测这些事务有直接利害关系的其他国家和国家集团的支持。

该指令还要求在国家网络安全战略有关原则框架内参与促进全面的网络安全管理。

2012 年通过的国防政策指令也把新出现的网络空间作为国际关系的一种新领域，而且提出一项防御优先事项，即加强信息和情报收集系统以支持指挥和控制系统等操作，目的是降低网络攻击的风险。

2011 年 1 月，国防参谋部负责人发布了军事网络防御构想，这为规划、发展和利用所需军事能力以确保军事行动期间有效利用网络空间提供了指导。

4. 国际社会可为加强全球信息安全采取的措施

对信息系统的依赖程度增加和关键基础设施的连通性加大使得网络空间安全对现代国家的运作至关重要。出于这个原因，网络安全应成为国家安全规划的一个内在组成部分。

目前，没有一个应对网络安全威胁的国际法律框架的保障。因此，在与网络安全有关的事项中在不损害国家主权的情况下，有必要制定这一领域的多边合作协定，类似于《国际海上人命安全公约》等，各国家承诺统一法律以便对网络犯罪进行追查，尽量避免由于隐匿性、缺少立法和经济利益使因特网成为犯罪和恐怖主义的理想温床。

私营部门、特别是互联网服务提供商，必须参与打击网络犯罪的努力。私营部门的合作是必不可少的，因为大多数互联网服务由私营部门掌握。私营部门长期以来一直面临互联网上存在的威胁，并积累了非常宝贵的知识和经验。

计算机应急小组可在网络安全中发挥关键作用。建设专业化队伍和对成员正在进行的培训是各国政府应采取的首要步骤，以确保网络安全。还须建立专事调查互联网犯罪的执法单位。

因为网络安全是一个全球性挑战，因此，须开展国际合作改善网络安全，还应加强政策和业务水平。各国计算机应急小组之间应该不断沟通，以促进在很短的响应时间内共享攻击信息。在经验教训以及最佳国家和国际做法方面也应共享。

其他措施包括：

- 从小就培训公民，使他们认识到需要注意所用的信息系统的安全性。许多类型的网络犯罪利用(或甚至是依赖)很多网民不采取适当预防措施使其计算机和账户尽可能安全和坚不可摧这一情况。因此，用户教育必不可少。更深刻地认识这个问题可减少犯罪分子为开展活动用于实施网络犯罪、特别是“僵尸电脑网络”方面活动的电脑数量。

- 根据各国法律，强化国际司法和警务合作，以便能够针对互联网的分散性和链接记录的不持久性，快速高效地追查刑事罪行。

- 组织跨国论坛、研讨会和会议以提高专家的知识，分享各类攻击的知识和网络攻击的新趋势，评估脆弱性和潜在攻击的影响，分享经验教训和最佳做法，并促进对警察进行网络犯罪调查方面的标准化培训。

- 协调欧洲委员会和北约等专事特定网络安全领域的组织的努力，以避免不必要的重复工作。

- 与私营部门和民间社会合作，制作指南和记录良好做法，以提高网络安全。

总之，国际社会应采取保护信息所需的措施，从统一的战略远景出发，并在可能情况下建立统一导向，为所有国家树立共同的标准和准则，制定平衡和全面的具体保护措施，并协调有关各国和各国际组织的政策和行动。

乌克兰

[原件：俄文]
[2013 年 5 月 31 日]

1. 信息安全问题总体评估

信息安全、电信安全和网络犯罪应对等领域是乌克兰国家安全的核心内容。反之，确保乌克兰的国家安全有助于在一个全球化的世界中加强国际安全。

世界各地都在实现全球化、建立信息社会和采用新的信息技术，这些使得作为国家安全组成部分的信息安全更加重要。信息安全的定义是国家在信息领域的利益在多大程度上可以免遭外部和内部威胁的侵袭。

相应地，下列内容都属于信息安全方面所面临的国际威胁范畴：

- 非法使用信息资源；

- 自动化系统内，包括国家关键基础设施管理中使用的那些系统内未获授权的破坏性活动；

- 以侵犯基本人权和自由方式或为了实施恐怖、极端或其他犯罪行为，包括侵略行为而使用网络空间、开展相关活动、或使用信息技术和资源；

- 广泛地或在特定国家使用信息基础设施传播煽动敌意和仇恨的信息；
- 传播违反现行国家法律、道德规范和原则的信息；
- 使用网络空间破坏社会稳定，破坏另一国家的社会、经济、政治和社会制度或传播旨在歪曲文化、道德和美学价值的错误信息；
- 防止尖端技术的获取，促进在信息技术领域的依赖性，以便获得优势和控制外国网络空间。

应着重指出下列与全球化有关的问题领域：针对大众或个体的信息和心理操控；利用信息和电信技术限制消费者获得服务；以及网络犯罪。

乌克兰专家指出，下列因素可能导致上述威胁的可能性加大：

- 信息资源和网络空间服务的大多数用户的计算机知识薄弱；
- 缺少共同的信息安全国际概念框架；
- 国家立法在建立和更新(恢复)信息基础设施的信息保护措施方面采取不同方法；
- 不同国家在计算机化和信息安全方面水平差异很大；
- 将具有潜在破坏性资源连接到信息和电信系统的危险；
- 网络空间未经授权活动来源可能无法查明的事实。

2. 国家为加强信息安全，支持信息安全方面的国际合作所做的努力

乌克兰负责信息安全及其组成部分的主要政府机构包括内务部、安全局和国家特别通信和信息保护局。这些机构正在积极参与管理信息安全的各个方面，其中特别关注控制论构成部分(网络安全)的监管和法律框架。

乌克兰正在执行下列与信息安全有关问题的社会关系法律规定。

根据《乌克兰宪法》第十七条的规定，信息安全与保护国家主权和领土完整、维持经济安全一样，是一项至关重要的国家职能。

根据乌克兰信息法第三条的规定，确保乌克兰信息安全是国家信息政策的主要领域之一。

在乌克兰整个安全系统内，信息安全占有特殊位置，因为信息关系和进程是社会和国家内所有进程的组成部分。在此方面，信息安全被定义为信息空间(信息环境)的状态，其中包括信息技术、信息资源和相关方之间的信息关系，信息安全确保信息空间的演变和使用造福于个人、社会和国家。

与社会发展利益相关联的国家安全优先事项决定了信息安全的主要目标。这些目标如下：

- 确保乌克兰的国家信息主权，因为信息流动变得日益全球化，其他国家竞相争取在信息领域占据上风；
- 营造一个支持个人和整个社会的文化、道德和智力发展的信息环境；
- 将乌克兰的信息资源维持在足以保证个人、社会和国家能可持续运转和发展的水平；
- 保护自然人和法人以及国家的信息免受外部和内部信息的威胁，其中包括应对计算机犯罪的措施；
- 确保乌克兰信息利益攸关方权利的有效性，并切实得到执行，以建立和利用国家信息资源、信息技术和信息基础设施。

为加强信息安全，正在落实监管和法律框架以及专业培训系统，而且负责信息安全的国家机构也互相协调开展的各项活动。这一协调包括与乌克兰计算机应急小组(计算机应急小组)、以及国际认可组织，事故对应和安全小组论坛合作。

根据乌克兰法律，计算机应急小组是国家特别通信和信息保护局的一部分，负责协调各类所有权结构的企业、机构和组织的工作，以防止、分析和应对信息和电信系统中针对国家信息资源的未经许可行动所致后果。

此外，计算机应急小组与有关的外国和国际机构及组织合作，以及该小组对于外国对口单位(是事故对应和安全小组论坛的正式成员，是国际电信联盟打击网络威胁国际多边伙伴关系的成员)的义务鼓励国际信息安全方面的合作。

根据乌克兰批准《网络犯罪公约》的法令进行修正的法案，由内务部授权建立和监督 24 小时联络点网络，以便为计算机系统和数据犯罪调查提供紧急援助；起诉被控犯有此类罪行的个人；并收集电子证据。

管理反网络犯罪司 24 小时网络犯罪反应网的相关部门隶属于内务部，并负责开展相关活动和业务，其中包括以下内容：

- 打击分布式阻断服务的攻击；
- 打击使用付款卡或付款卡账户数据施行的刑事犯罪；
- 打击未经许可干预“客户银行”远程银行服务的操作；
- 打击传播非法网络内容(侵犯版权)；
- 打击网上传播色情，包括儿童色情；
- 打击电信罪行；

- 打击未经许可进入卫星数据传输网络方面的犯罪活动；
- 打击因特网上财务和其他形式的欺诈行为；
- 打击刑事犯罪和其他电子商务罪行；
- 管理 24 小时联络点网络应对行动。

目前正在努力更新国家信息安全法律，以建立符合国际规范的监管和法律框架。

乌克兰现正在根据 2010 年 12 月 10 日关于 2010 年 11 月 17 日乌克兰国家安全和防卫理事会关于 2011 年乌克兰国家安全面临的挑战和威胁决定的 1119 号总统令起草关于网络安全的法律草案。

根据现行法规和法案，以下国家政策领域需要得到更多关注：

(1) 2012 年 12 月 10 日关于 2010 年 11 月 17 日乌克兰国家安全和防卫理事会关于2011年乌克兰国家安全面临的挑战和威胁决定的1119号总统令(第4段)；2012 年 6 月 8 日关于 2012 年 5 月 25 日国家安全和防卫理事会关于加强乌克兰反恐活动决定的 388 号总统令(第 1 段)；2012 年 6 月 8 日关于 2012 年 6 月 8 日国家安全和防卫理事会关于更新的国家安全战略理事会决定的 389 号总统令(第 3.1.1、3.3 和 4.3 段)；以及 2012 年 6 月 8 日关于 2012 年 6 月 8 日国家安全防卫理事会关于修订乌克兰军事原则决定的 390 号总统令(第 7 和第 19 分段)，其中包括以下目标：

- 建立国家网络安全系统；
- 建立统一的全国打击网络犯罪系统；
- 起草和核准作为网络袭击保护重点的国家安全和防范关键场所的清单；
- 起草国家网络安全法草案并提交给议会；
- 将网络安全列为国际稳定和乌克兰国家安全面临的主要威胁之一；
- 作为一项战略目标和主要的国家安全政策目标，核准编写信息和通信技术使用国家标准和技术条例，并与欧洲联盟成员国的相关标准相一致；
- 提出“网络恐怖主义”一词的定义；
- 在乌克兰建立有效机制，以应对全球化世界中使用信息技术所带来的最新的国家安全威胁(在某些情况下可能威胁到国家利益的现象和趋势)，特别是“网络威胁”；
- 对以核工业设施、化学工业设施及其他潜在有害场所为目标的网络袭击进行分析，这种向乌克兰展示军事力量的方式可能导致军事冲突；

(2) 内阁法规和法案：2012 年 8 月 22 日核准乌克兰-北大西洋公约组织(北约)合作 2012 年年度国家方案的第 720-P 号令、2012 年 6 月 15 日国家安全和防卫理事会上述决定下的第 24066/1/1-12 号指令，在 2012 年 6 月 8 日第 388 号总统令下加以执行，该法令也规定了网络安全法案；

(3) 乌克兰议会正在审议关于修正若干国家网络安全法案的法律草案。这些法律草案尤其规定了国家法律中如何使用“国家网络安全”、“关键基础设施场所”、“关键信息基础设施场所”以及“网络空间”等概念，还规定了国家安全面临的主要网络威胁定义、国家政策的主要领域和负责国家安全的各实体在这一领域的职责。

3. 通过国际框架，加强全球信息和电信系统安全

乌克兰制定了保护信息和电信系统中信息的法规和法律框架，其保护结构的原则和方法符合国际标准化组织关于信息技术安全评价的 15408 普遍标准。

鉴于计算机犯罪已超越国界，成为一种国际现象，乌克兰正在与外国执法机构进行合作。

此外，乌克兰正在通过与欧洲安全合作组织、欧洲委员会议会、欧洲委员会以及北约和平伙伴关系的项目和方案以及根据双边协定致力于确保国际信息安全。

4. 国际社会为加强信息安全可能在全球层面采取的措施

由于计算机犯罪的跨国性质，现在需要拟订一套国际原则，以加强信息和电信网络安全和总体的国际安全政策，以及加强信息安全威胁发现、评估和预测的方法、手段和资源。

全球信息安全的一个主要领域就是拟订和通过国际法律文书，消除不够精确的信息安全术语。其中重要的一个方面是确定网络空间的国际法律地位，并在法规和法律文书中体现各国“在这一空间国家机构的管辖权(与国家领空和领水相当)，以及网络战争、网络侵略等问题的进一步管理。

制定标准方面的另一个主要问题是对网络犯罪提出统一定义并对相关罪行进行明确分类。

国际社会在加强全球信息安全方面可以采取的其他措施包括协调统一的信息保护条例和法律框架；为评估信息安全系统和资源的实效商定标准和办法；信息安全证书的相互承认；以及在解决研究、技术和法律信息安全问题方面加强合作。与此同时，国家执法机构间在预防、制止和惩处计算机犯罪方面加强合作也是合作成功的关键。

大不列颠及北爱尔兰联合王国

［原文：英文］
［2013 年 5 月 16 日］

大不列颠及北爱尔兰联合王国欣见对题为“从国际安全角度来看信息和电信领域的发展”的大会第 67/27 号决议作出回应的机会。

对信息安全问题的一般看法

联合王国将在本呈件中使用其优选术语“网络安全”及相关概念，指代在维护网络空间的信息保密性、可用性和完整性方面作出的努力。“信息安全”一词常被商业和标准组织用来指代相同事物，联合王国也接受该专有名词的上述具体含义。“信息安全”一词的使用可能会造成混淆，因为该词被一些国家和组织用作一种理论的组成部分，即将信息本身视为需要对其采取保护措施的威胁。联合王国不认同“信息安全”一词在上述背景下使用时的含义，因为这种理论可能被用作借口，试图进一步控制言论自由，违背《世界人权宣言》和《公民权利和政治权利国际公约》的商定原则。

网络空间是充满重大机会的领域，但也具有实际和潜在威胁。现在有 20 多亿人通过英特网连接到网络空间，而且随着移动技术使发展中国家能以更低成本利用英特网的巨大效益，这一数字必将进一步增长。英特网提供经济增长引擎、开放接受教育的机会、加强人类交流和了解、突破文化和地理障碍、促进在线提供服务并通过使政府以崭新和具有活力的方式对其公民负责来加强民主。例如：

- 以英特网为基础的活动已占联合王国国内生产总值的 8%。确保企业和客户对网络空间的商业活动感到安全对经济增长至关重要。
- 2011 年，联合王国推出了电子请愿书服务，使任何人都可以就政府负责的任何问题发起或签署请愿书。所有收集到 100 000 个或更多签名的请愿书可列入议会辩论议题。在其推出的第一年，发起了 15 600 多份请愿书，其中 10 份通过了 100 000 个签名的门槛值。这 10 份请愿书都已经或计划在议会进行辩论。

与许多国家一样，联合王国在能源、财政和运输等许多重要国家服务领域都依赖网络空间。这些服务的严重故障，无论是意外还是蓄意入侵所致，都会造成严重混乱、经济损失或人员伤亡。

构成威胁的情形复杂多变。联合王国政府及企业和个人系统每天都面临入侵企图。入侵动机包括政治和产业间谍活动、网络犯罪、破坏/控制网络或拒绝提供服务。威胁行为体包括国家、国家代理人、非国家行为体、有组织犯罪团伙以及个体投机分子。网络空间的相互关联性意味着对一个系统的破坏活动可能对其他系统造成意想不到和难以预测的影响。由于难以明确地确定网络事件的具体源

头、犯罪人可能伪装成他人、对网络空间中可接受的国家行为的理解不成熟、某些国家的网络基础设施缺乏复原力以及没有统一的国际办法来发现、追踪和起诉网络犯罪分子，应对上述威胁的工作困难重重。

所有社会成员在打击上述威胁方面都应发挥作用并承担义务。各国政府应在国际性努力中，率先改善对可接受国家行为的理解，并打击网络犯罪，但鉴于大多数网络空间基础设施是私营公司所拥有和经营，这些公司参与相关辩论至关重要。联合王国认为，改善网络安全绝不能牺牲网络空间带来的经济和社会效益。尤其必须确保不能滥用提高网络安全的努力来进一步限制国际协定给予的言论自由。在这方面，民间社会组织的作用尤其重要。

在国家一级为加强信息安全和促进这一领域的国际合作所作的努力

本国办法

联合王国 2010 年发布的国家安全战略将网络攻击确定为 4 种“1 级”威胁之一，其他 3 种威胁包括国际军事危机、重大事故或自然灾害以及恐怖攻击。2011 年 11 月，联合王国发布了最新的网络安全战略，其中提出了“从充满活力、具有复原能力和安全的网络空间中获取巨大经济和社会价值，在自由、公平、透明和法治等核心价值观指导下，采取行动促进繁荣、国家安全及强大社会”的愿景。提出了支持实现本战略的 4 个目标：

- 打击网络犯罪，成为世界上网络空间商业活动最安全地方之一；
- 提高应对网络攻击的能力并更好地保护我们在网络空间的利益；
- 帮助建设开放、稳定和充满活力，而且可供联合王国公众安全使用并支持开放社会的网络空间；
- 建设支持实现我们所有网络安全目标所需的跨领域知识、技能和能力。

为支持实现这些目标，联合王国政府划拨了 6.5 亿英镑的追加支出，用于旨在改变应对网络威胁对策的四年期方案。

联合王国已投资于建设崭新和独特的能力，以保护其核心网络及服务，并深化理解其所面临的威胁。知识的增多转而能帮助联合王国更好地对网络防御工作进行优先排序，并提供指导。在联合王国国防部的主导下，联合王国已建立三军种股，负责制定新的战术、技术和计划，以建设应对复杂威胁的军事能力。政府与破坏性网络活动受害者密切合作，这项工作的成果使政府能够向产业界提供咨询意见，以改进产业界网络安全措施。就其自身的网络而言，政府正在制订新的服务共享安全模式，包括更复杂的员工验证、更好的合规检查以及更强的网络复原力。

联合王国政府已投资于加强执法和检察能力，以预防、阻止和调查网络犯罪并将责任人绳之以法。中央警察网络犯罪股的规模已扩大两倍，已组建 3 个区域网络治安组，并为主流警官设计了关于打击网络犯罪的培训。严重有组织犯罪监察局将在 2013 年晚些时候与中央警察网络犯罪股合并，组建全国犯罪监察局国家网络犯罪股，这向改进联合王国打击网络犯罪的执法能力迈进了一步。

联合王国的产业已成为猖獗的知识产权盗窃等网络犯罪的最大受害者。联合王国政府与产业界和学术界携手提高对应对网络威胁必要性的认识，2012 年，政府为产业界首席执行官编写了指导文件，阐明高级管理人员应如何制定战略以保护其最宝贵的信息资产。联合王国政府还成功地完成了一项信息共享试点举措，为各组织提供可信任的环境，使其能够分享关于当前威胁和事件管理的资料。这涵盖了国防、财政、药品、能源和电信等部门的约 160 家公司。

联合王国政府与产业界合作，一直积极提高产业界及公众对所面临威胁的认识，促使其采取通常仅需的简单步骤来保护自己，并对提高网络产品和服务安全性提出要求。这些举措包括：“安全在线周”(与欧洲联盟和加拿大共同推出)；国家反欺诈局推出的关于在线欺诈行为的专项运动；2012 年“细节决定成败”运动。

联合王国正投资于技能和研究，以便在今后能够跟上此问题的发展速度。在网络安全领域开展研究的联合王国首批 8 家大学被授予了“网络安全研究学术英才中心”地位。正在为年轻学生编制互动学习材料，已推出一项技术实习计划，以便在中学和大学学生中确定并培养才能。为确保网络安全领域的工作人员接受适当的教育和培训，专业人员信息保障认证制度将帮助政府和产业界征聘具有适当水平的适当技能的网络安全专业人员，并安排适当的工作。

国际办法

联合王国一直处于国际性努力的前沿，致力于提高网络空间的透明度、可预测性和稳定性。2011 年 11 月，联合王国主办了首次网络空间国际大会，汇集了来自 60 多个国家以及商业和民间社会组织的代表，讨论扩大网络空间经济和社会效益的途径、打击网络犯罪合作、安全可靠地使用英特网以及国际安全。2012 年在布达佩斯举行的大会进一步推动了上述活动产生的动力，而目前正在规划将在首尔举行的 2013 年大会。

联合王国是“从国际安全角度来看信息和电信领域发展的政府专家小组”积极成员，也是欧安组织“在网络空间建立信任措施非正式工作组”活跃成员。

2012 年 10 月，联合王国宣布了建立全球网络安全能力建设中心的倡议，该倡议每年获资 200 万英镑，其中包括各种多边和双边举措。该中心将就如何建立更安全和更具复原力的国家基础设施为其他国家提供独立咨询意见和专门知识，并成为在这个重要问题上开展世界级研究和国际协作的协调中心。

为进一步开展打击国际网络犯罪的国际努力，联合王国继续推动反网络犯罪公约及其各项原则，将其作为该领域最有效的工具。重大有组织犯罪监察局继续与国际伙伴合作，牵头就全球执法问题与因特网指定名称号码管理公司进行交涉。

旨在加强全球信息和电信系统安全的有关国际概念

最重要的概念是遵守关于国家间关系的国际法及现行行为准则。联合王国坚定认为，这些原则同样适用于网络空间，如果各国毫不含糊地申明其在网络空间的活动将遵守这些法律和规范，就将为建设更加和平、可预测和安全的网络空间奠定基础。

在这方面，网络空间具有特殊挑战，例如难以明确地确定活动源头、评估活动意图以及非国家行为体的作用。联合王国欢迎国际社会讨论如何在这方面遵守有关国家行为的国际法和规范。

联合王国不认为缔结全面多边条约、行为守则或类似文书的努力可积极推动在可预见的未来加强网络安全。在整个网络空间以“网速”转变的情况下，任何具有约束力的协定的复杂性和综合性意味该协定无法实现成效或获取广泛支持，除非在行为规范和建立信任措施方面开展了许多年(可能需要几十年)的艰苦工作，从而在签署方之间建立了必要的理解和信任，并确保他们能够可靠地遵守自己的承诺。在其他议题上缔结这类协定的经验表明，有意义和有效的协定只能是建立共同理解和共同方法的外交努力的结果，而非这种外交努力的起点。联合王国认为，国际社会的努力应侧重于建立对国际法律和规范的共识，而非就具有约束力的文书展开谈判，因为这种谈判只会导致片面和过早地在网络安全领域实施一种设想的方法，而该领域目前在支持此方法方面尚未达到水到渠成的程度。

国际社会为加强全球一级的信息安全可采取的措施

网络空间不分国界的性质使各国迫切需要加强双边、区域和多边合作，以制定应对共同威胁的共同响应方法。联合王国认为，在现阶段可作出最重要贡献的措施包括：

(a) 各国之间继续进行讨论，根据现行国际法原则和国际习惯规范，制定一项可为人接受的国家行为的规范框架；

(b) 在网络空间采取建立信任措施，目的是提高国家行为的透明度和可预测性，从而减少误解或事件意外升级的风险；

(c) 各国建立计算机应急小组，作为事件处理和信息共享中心，并通报主要联系点和建立可靠的危机沟通机制；

(d) 制定联合演习，测试事件联合处理及沟通程序；

(e) 制定统一的法律方法来打击网络犯罪；

(f) 加强与商业和民间社会代表的对话，确保在这个很大程度上由私营部门拥有和经营的领域采取协调一致和重点有序的方法；

(g) 建立了更成熟网络安全能力的国家承诺支持其他国家的能力建设。