联合国 A/67/167*

大会

Distr.: General
23 July 2012
Chinese
Original: English/Russian/Spanish

第六十七届会议

临时议程** 项目 90

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

* 由于技术原因于 2013 年 4 月 8 日重新印发。

** A/67/150。

12-43413 * (C) 080413 090413

一. 导言

1. 大会在其第 66/24 号决议执行段落第 3 段中邀请所有会员国在考虑到从国际安全的角度来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. 根据该要求，于 2012 年 2 月 16 日向会员国发出普通照会，请它们就该主题提供信息。下文第二节载有已收到的答复。以后收到的任何答复将作为本报告的增编印发。

二. 已收到的各国政府的答复

哥伦比亚

[原件：西班牙文]
[2012 年 5 月 21 日]

信息和通信技术的使用无疑给各国带来重大变化和效益。然而，这种技术进步也增加了世界各地利用技术进行的犯罪活动，这样就突出了采取紧急措施和控制的必要性，以保护国家免受这种新的威胁。

网络空间犯罪能力的提高和利用新技术对计算机构成的威胁是所有国家共同关心的问题，因为这些对包括民间社会在内的公共和私人领域的信息安全都产生重大影响，尤其显示出必须实施必要的安全协议和政策，以建立严格的控制，保护国家及其关键基础设施免于这些新威胁的影响。

在此背景下，哥伦比亚在 2005 年制定了 ISO 27001 标准，作为一个安全管理系统，涵盖了实施信息管理的所需的政策、组织结构、程序、过程和资源。其目的是实施 ISO 17799 中所包含的质量标准，诸如最佳做法准则和控制目标，而侧重点在于保密性、完整性和可用性，详情如下：

- 保密性：防止信息被未经授权的个人或程序所利用。
- 完整性：确保对组织有价值物品和事务的准确性和完整性。
- 可用性：确保经授权实体的需要时可获取并使用相关信息。

ISO 27001 的效益体现在以下方面：

(a) 建立一套井井有条的明确信息安全管理方法；

(b) 降低信息遗失或被盗的风险；

(c) 确保用户获取信息；

(d) 对信息所面临的风险和各项安全控制的持续审查；

(e) 进行外部和内部审计以识别信息安全系统潜在问题的能力；

(f) 保证遵守信息管理方面现行法规；

(g) 人们增强对信息安全问题的认识。

为努力增强信息安全的法律和业务框架，哥伦比亚共和国国会于 2009 年 1 月 5 日颁布 1273 号法令，修订“刑法”，除其他规定外，创立了受法律保护的新领域，即对信息和数据的保护，并确立对使用信息和通信技术系统的全面保护。

这项重要法令分为两个章节，对“数据和计算机系统的保密性、完整性和可用性的攻击”和“对电脑的攻击及其他罪行”。

第一章所述如下：

- 以不当方式进入计算机系统：任何人，未经授权或超过授权，在违背有合法权力予以禁止之人的意愿，进入或留在无论是否设有安全措施或保护的整个或部分计算机系统，则应处以四十八(48)至九十六(96)个月监禁，和 100 至 1000 倍目前法定最低月工资的罚款。

- 非法阻碍电脑系统或电信网络：任何人未经授权便阻止或妨碍计算机系统、其中所载计算机数据、或电信网络的正常运作或使用，则应处以四十八(48)至九十六(96)个月监禁，和 100 至 1000 倍目前法定最低月工资的罚款，条件是这一行为并未构成应处以更高刑罚的犯罪。

- 计算机数据的截取：任何人如未事先得到法院命令，在始发地、目的地或计算机系统内或在计算机系统电磁辐射传输中截取计算机数据，应处以三十六(36)至七十二(72)个月监禁。

- 电脑的损坏：任何人如未经授权，破坏、销毁、删除、损害、改变或者消除计算机数据，或数据处理系统或其部件或逻辑元件，应处以四十八(48)至九十六(96)个月监禁，和 100 至 1 000 倍目前法定最低月工资的罚款。

- 恶意软件的使用：任何人如未经授权，便生产、贩卖、收购、批发、销售或发送、或者携带出境，恶意软件或其他有害计算机程序，则应处以

四十八(48)至九十六(96)个月监禁，和 100 至 1 000 倍目前法定最低月工资的罚款。

- 侵入个人资料：任何人未经授权，便为自己或第三方的利益，获取、编制、提取、提供、销售、交流、发送、购买、拦截、披露、修改或使用个人秘码、载于文件、档案、数据库或类似媒介中的个人资料，应处以四十八(48)至九十六(96)个月监禁和 100 至 1 000 倍目前法定最低月工资的罚款。

- 为掌握个人资料伪造的网站：任何人带着犯罪意图在未经授权情况下，设计、开发、贩卖、销售、执行、编程或发送网页、链接或弹出窗口，则应处以四十八(48)至九十六(96)个月监禁，和 100 至 1 000 倍目前法定最低月工资的罚款，条件是这一行为并未构成应处以更高刑罚的犯罪。

第二章规定如下：

- 利用计算机或类似手段行窃：任何人绕过计算机安全措施，从事第 239 条关于操纵计算机系统、电子、远程信息处理或其他类似网络的行为，或借助既定认证和授权而假冒用户，则应处以刑法第 240 条规定的刑罚，即三(3)至八(8)年监禁。

- 未经同意的资产转移：任何人如为营利使用计算机或类似设备，未经同意作出损害第三方的资产转移，如这一行为并未构成应处以更高刑罚的犯罪，则应处以四十八(48)至一百二十(120)个月监禁，和 200 至 1500 倍目前法定最低月工资的罚款。任何人如编程、下载、拥有或提供计算机软件为上述目的作案，或欺诈，则应处以同样刑罚。

2009 年第 1273 号法令无疑是哥伦比亚在打击计算机犯罪方面所迈出非常重要的一步。但不同类型和模式的有组织犯罪，特别是网络犯罪的发展，已迫使哥伦比亚实施一项重点在于网络防御和网络安全的打击网络犯罪全面战略，为此在根据信息安全的概念所提出各项目标过程中要将机构间工作作为绝对第一要素。

在此框架内，哥伦比亚政府于 2011 年 7 月，推出了国家网络防御和网络安全政策，其基础为三个基本支柱：

- 为预防、协调和监测目的，采用适当的机构间框架，并为解决可能出现的任何威胁和风险提出建议。

- 提供信息安全方面的专门培训并扩大网络防御和网络安全领域的调查。

- 加强有关这些事项的立法和国际合作，加快哥伦比亚加入各种国际文书的进程。

为了全面实现上述战略方针，哥伦比亚拟定并成立了四个部门：

(a) 首先是跨部门委员会，负责提出信息化管理的战略前景和制定公共信息技术基础设施、网络安全和网络防御方面管理的政策指导原则；

(b) 第二个机构是哥伦比亚计算机应急小组，即网络安全和网络防御事项上的国家协调机构；

(c) 第三是武装部队联合网络指挥部，其任务是防止和打击任何影响到国家价值和利益的网络威胁或攻击；

(d) 最后，成立了网络警察中心，这一机构负责哥伦比亚的网络安全，提供信息、支持并防止网络犯罪。

这些机构将使哥伦比亚能够履行和实施国家网络防御和网络安全政策，并全面和有效地解决目前全世界迅猛增长的新型犯罪。

哥伦比亚不仅制定了网络防御和网络安全政策，而且也采取了一些重要的部门举措，以制定有效的信息安全政策。其中最重要政策内容如下：

举措	牵头机构	范围
政府在线战略的信息安全模型	政府在线计划——信息技术和通信部	这一安全模型是指构成政府在线目标基础的——套战略方针，如“个人信息的保护”，和“政府在线的信誉和信心”。模式中确定了政府机构信息安全的以下关键环节：(a) 提供信息和服务；(b) 信息和数据的完整性；及(c) 信息的保密性。
为执行国家网络安全战略，向政府提出的建议	电信监管委员会	在本文件中，电信监管委员会就国家网络安全战略向政府提出建议，并为政府和私营各级部门的协作与合作提出了合适工具；确定了防止网络犯罪的方式；按照国际标准，就实施和发展有关网络安全的法律框架提出建议；就建立系统，以解决网络安全事件，包括监

举措	牵头机构	范围
		测、分析和对策提出建议；并就树立国家网络安全文化提出指导原则，以提高哥伦比亚保护关键信息基础设施的水平。
哥伦比亚互联网服务供应商的计算机安全协调中心	哥伦比亚信息技术及通信协会	哥伦比亚计算机安全协调中心与其附属机构的安全中心(哥伦比亚最大的互联网服务提供商)直接联系。它能够协调关于处理和解决的要求并提出关于计算机安全问题的报告。

无论国家信息安全的能力如何，必须指出的是，哥伦比亚认为，应在国际层面上采取一系列措施，加强信息安全。

- 加强联合国会员国之间的沟通渠道，以协调打击影响到信息和数据的跨国犯罪活动的斗争。
- 制定国际和区域文书，重点在于就威胁到每个国家网络安全和网络防御的可惩罚行为提出法律定义。
- 制定并编纂协议，以解决计算机事故，以期提出全球信息安全政策。
- 加强"黑客"集团方面的预防和立法活动，尤其在高等院校，以减少青少年参与这类组织的可能性，因为这些组织威胁到国家数字基础设施的正常发展。
- 实现立法规范化，重点在于信息安全方面的预防、援助和后续行动活动。
- 综合并实施技术，侧重点在于采用信息安全管理方面最佳做法。这里必须注意制定出尖端技术的投资计划，以及政府对技术开发项目的支持。
- 提供机会就此事项通用标准交流信息和知识。

哥伦比亚共和国关于信息安全的立法

法/决议	主题
第 527(1999)号法令(电子商务)	确定和管理数据信息、电子商务和数码签字的存取和使用，设立了鉴定机构，并载有其他规定。

法/决议	主题
第 599(2000)号法令	颁布“刑法”，其中维持“违法破坏通信”刑事罪行的框架，确立了版权合法权利，并包括一些间接涉及计算机犯罪的行为，如报价、销售、或购买能够拦截个人之间的私人通信的设备。此法界定了侵入计算机系统的不法行为(第 195 条)，即在违背有合法权力予以禁止之人的意愿情况下，以不当方式进入设有安全措施保护的计算机系统，或留在这一系统内，可处以罚款。
第 962(2005)号法令	颁布规定，精简国家机构和实体以及履行公共职能或提供公共服务之个人的行政程序。此法规定了鼓励公众成员使用综合技术，减少行政手续的等候时间和成本。
第 1150(2007)号法令	推出提高第 80 号法令(1993 年)效率和透明度的措施并颁布了关于公共采购的其他一般规定。专门确立了公共行政部门颁布行政法案和文件的可能性，并以电子形式发出通知，为此，法令提出建立电子化公共采购制度的可能性。
第 1273(2009)号法令	修订“刑法”，除其他规定，建立了新的受法律保护的利益，即“对信息和数据的保护”，并确定使用信息和通信技术的全面保护系统。
第 1341(2009)号法令	界定了信息社会和信息和通信技术框架的原则和概念，建立国家无线电通信局并包含其他规定。
电信监管委员会第 2258(2009)号决议	涉及到网络和电信服务提供商的网络安全问题。该决议修订通信监督管理委员会第 1732(2007)号决议第 22 和第 23 条和第 1740(2007)号决议 1.8 和 2.4 条。本法规提出的要求是，网络和/或提供互联网接入的电信服务提供商，必须采用安全模式，按照其网络的具体特点和要求，推动提高其网络访问的安全，根据国际电信联盟提出的安全框架，坚持数据保密性、数据完整性和网络元素可用性、信息、服务和应用，以及认证、访问和不可抵赖性措施等项原则。决议还确定网络和电信服务提供商必须满足关于通信和信息安全的不可侵犯性的要求。
第 052(2007)号通知(哥伦比亚金融监管局)	确定通过为客户和用户的产品和服务的媒体和分销渠道，处理信息的最低安全和质量要求。

古巴

［原文：西班牙文］
2012 年 5 月 21 日

敌意地利用电信来公开地或秘密地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 66/24 号决议表达的关切，担忧信息技术和媒体被用于不符合国际稳定与安全的目的，危及国家的完整，并损害各国的民事和军事领域的安全。这项决议并正确地强调有必要防止为犯罪或恐怖主义目的使用而信息资料和技术性。

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攻势升级，违反了约束无线电领域的现行国际法规。这一攻势非但没有考虑到可能对国际和平与安全造成的破坏，而是制造了危险局势，例如不经古巴同意，用军用飞机向古巴播放电视信号。

2011 年间，美国采用 30 个频道，对古巴每周平均非法播放了 2 193 小时的节目。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无线电恐怖主义题材。

对古巴进行的这些挑衅性广播违反了下列国际准则：

- 《国际电信联盟公约》序言所述的基本原则。美国政府对古巴播放电视节目的内容是颠覆、破坏和误导性的，违背了这些原则。
- 《国际电信联盟公约》CS 197 和 CS 198 条款规定，所有电台，无论用于何种目的，其设立和操作均不得对其他会员国的无线电通讯或服务造成有害干扰。
- 2007 年 11 月举行的世界无线电通信大会第九届全会通过的协议，其中第 6.1 段(g)分段规定：“航空器上运营的任何广播站，如系专门向他国政府领土播放而未经该国政府许可，则构成违反《无线电规章》”。
- 国际电信联盟《无线电规章》第 8 条第 8.3 款规定，其他国家政府在设定本国频率时，应考虑到已经设定和登记了的并得到国际承认的频率，以避免有害干扰。
- 国际电信联盟《无线电规章》第 42 条第 4.2 款，该条禁止在海面或其上空的航空器站进行任何无线电广播业务。

- 《无线电规章》委员会在 2004 年 12 月第 35 次会议上作出裁定，指出采用 213 兆赫的广播对古巴节目造成有害干扰，并要求美国政府采取适当措施取消转播。自 2006 年 9 月以来，《无线电规章》委员会还一直要求美国政府采取措施，消除在 509 兆赫上的干扰，但至今没有任何答复。2009 年 3 月 20 日，该委员会第 50 次会议的决定(RRB09-1/5 号文件)概要再次重申，这些广播是非法的，并要求美国采取一切必要措施，消除这两宗干扰古巴电视节目的情况。

- 《无线电规章》国际电信联盟第 23 条第 23.3 款限制国家境外的电视播放。2009 年 1 月美国政府问责局(美国官方机构)发表的报告承认，美国政府对古巴的广播和电视节目构成违反国际法和国内法的行为。

2007 年在日内瓦举行的世界无线电通信大会通过了结论文件，认定美国在航空器上对古巴的无线电播放违反了《无线电规章》。全体会议通过的结论明文规定：“航空器上运营的任何广播站，如系专门向他国政府领土播放而未经该国政府许可，则构成违反《无线电规章》”。

这些结论是世界无线电通信大会全会通过的，对国际电信联盟的工作具有法律效力。因此，世界无线电通信大会通过了 1990 年由当时的国际频率登记委员会所作的声明，即对航空气球上对古巴领土播放电视节目违反了《规章》的规定。

国际电信联盟《无线电规章》委员会 2010 年 7 月举行的第 54 次会议通过如下决定：

> 经仔细审议主任的报告以及古巴当局的来文(RRB10-2/3(Add.1)号文件)，委员会很遗憾古巴无线电广播电台继续受到美国播放的干扰，并决定维持对此问题的决定。
>
> 委员会还注意到“办公室以委员会执行秘书处资格”提出的请求，即将古巴短波和超短波无线电台受到干扰的问题提交下一届全体会议。委员会承认各国政府有向全体会议提交任何问题的主权权利，确认《无线电规章》参加 2010 年全体会议的两名代表可在下一届全体会议上提出一切必要的资料和评价。

最近，2012 年 2 月，世界无线电通信大会责成国际电信联盟无线电通讯局局长在定于 2015 年举行的下届会议上追踪了解并报告美国通过其无线电-电子侵犯行为对古巴电台和电视台广播的干扰。

据此，大会肯定了其前次会议通过的结论，指出美国政府利用飞行器广播反古巴的电台和电视台节目是非法的。

美国政府对古巴的敌对态度，在其近 50 年来的经济、商业和金融禁运中显露无遗，这一禁运也影响到信息和电信领域：

- 禁运严重打击了古巴的信息和电信领域。2010 年至 2011 年，经计算，这方面的损失共达 7 396 394 美元。

- 古巴仍然无法获得许多网站提供的服务，一旦链接被确认来自古巴.cu 域名的互联网地址，就会遭到拒绝。

- 美国还明知故犯而且虚伪地继续污蔑古巴阻止其公民进入全球网络；而事实正相反，由于美国实施的封锁法，古巴不能连接到古巴群岛周围的光纤电缆，因而被迫支付昂贵的卫星服务。

- 2010 年 10 月 6 日，Twitter 网络运营公司承认对禁止从古巴发送手机短信一事承担全部责任。同样，它在今年 4 月份承认，古巴被限制使用一些特定的 Twitter 工具，理由是试图从一个被禁止的国家进入 Twitter。

- 2011 年 2 月起，信宇金融公司(Syniverse)停止向古巴 ETECSA 通信公司支付手机漫游费，理由是，该公司的银行不能与古巴进行交易，这也就是说，ETECSA 公司不仅无法收到 260 万美元的漫游费，还面临着意想不到的困难。

联合国大会从国际安全的角度对于信息和电信领域发展的讨论具有现实意义和重要性。美国政府对古巴的这种行动说明了对这一问题的讨论很有必要，而且迫切需要采取措施制止这种行动。

古巴支持大会第 66/24 号决议，并将为全球信息和通讯技术的和平发展继续作出贡献，使之为全人类造福。

巴拿马

[原文：西班牙文]
2012 年 7 月 10 日

二十一世纪的经济日益地以服务部门为基础，这在第一世界经济体中尤其明显。电子商业仅仅是这一经济部门的最新表现方式，它在世界各地便利了商业交易，并减少了提供货物和服务的费用和时间。电子治理是国家政府的电子商业形式，它允许国家政府通过各种(网络的或者是移动的)技术来快速有效地满足公民的大量需要。

由于在支持电子商业和施政方面广泛地采用信息和通信技术，必须尽力确保这些技术满足国家的服务对象及公民对于机密性、正确性和易用性方面的基本需求。但是，目前开展的许多工作都注重于从技术上解决全球性的问题，也就是说从不同的角度解决问题。

我们认为，国家如果希望推动电子商业和治理，首要的任务就应该是根据其他国家先前采纳并得到广泛接受的国际标准，制定法律框架，与此同时也针对利用这方面资源来活动的罪犯和恐怖主义者设置杜绝的条件。只有在法律和技术上采取了防范措施的国家才有希望因自己为电子商业和治理创造有利条件而从中获得经济利益。

同时，应当继续努力，制定能够在明确的和现实的时间范围内实施的网络安全战略，从而对于不同的国家利益发生碰撞的情况形成保护国家网络安全的技术和政策。这些战略不仅应能加强国际和平，而且还应当力图维护各国的国家安全和稳定。

巴拿马在国家范围采取了以下措施来加强信息安全并推进国际合作：

(a) 根据 2011 年 9 月 26 日第 709 号行政命令建立了计算机安全事件行动小组；

(b) 修改了实体法(《刑事法》)，纳入了涉及到网络犯罪的新的刑事罪行项目，随后并提交国会通过(第 337 号法案)；

(c) 对《刑事程序法》进行研讨和修改，使之与新纳入《刑事法》的罪行相吻合；

(d) 建立一个由政府革新和国家公共安全署领导的工作组，研讨因特网服务提供商在信息安全领域中的责任。此外，还论及通过中美洲地区国家管制人员在区域范围(中美洲电信技术委员会/国际电信联盟)落实该工作组研讨的结果；

(e) 建立一个由检察官办公室领导的电子证据处理程序工作组，国家政府革新署参加工作组的工作；

(f) 向美洲国家组织提出获得技术援助的正式请求，以制定美洲网络安全战略；

(g) 参加 4 月份在巴拿马进行的、由美洲组织计算机应急小组协助举办的事件处理高级培训班；

(h) 评估联合国毒品和犯罪问题办公室关于设置一项建设巴拿马杜绝网络犯罪能力的方案；

(i) 经常出席美洲司法部长/部长/总检察长会议和美洲反恐怖主义委员会；

(j) 外交部长卡洛斯·阿罗塞梅纳在 2012 年 1 月 31 日的普通照会中正式请巴拿马驻布鲁塞尔的大使代表我国加入《网络犯罪公约》。

关于可以在国际社会采取可能的措施，以加强全球范围的信息安全问题，我们认为应当审议以下的建议：

(a) 设置一项共同的法律框架，以此使各国能够根据国际上接受的程序，快捷地相互提供法律援助，据此开展合作；

(b) 制定国家和区域网络安全战略；

(c) 通过国家计算机事件行动工作队推动国家之间经常的信息交流，来鼓励信息的流通，尤其是涉及到司法追究犯罪和恐怖主义行为的信息；

(d) 开展使公众了解有关适用于每一国家的本地和国际规则的宣传方案。

卡塔尔

[原件：英文]

[2012 年 5 月 18 日]

卡塔尔国在一个既考虑信息安全资产又考虑利用这一资产的个人安全的整体方针下在信息安全领域作出国家努力。此项战略与卡塔尔 2030 年远景相呼应，后者着重指出人类、社会和经济发展是关键支柱，并将国际电信联盟全球网络安全议程、八国集团重要信息基础设施保护原则等国际努力视为驱动力。

卡塔尔国家网络安全方案(作为一项信息安全高级研究中心举措设立的计算机应急小组)是一个由最高信息和通信技术委员会主持、得到政府资助的组织。目前，该组织成为卡塔尔网络安全议程中的一块重要基石，其中包括重要信息基础设施保护和政府信息和通信技术任务保证部门。

卡塔尔计算机应急小组与政府各机构、公私营部门组织和卡塔尔公民合作，确保在线威胁得到监控、风险得到抑制。计算机应急小组确立了调查威胁的做法，包括最新数字取证法、恶意程序分析、威胁监控系统能力、以及通过情景培训方案加强安全防备和安全对策的渠道。以下是该应急小组职能简介：

防范威胁情报

安全操作中心。在安全分析方面将利用内部研制的工具(威胁监控系统)主动提请政府机构和关键组织注意与清除工具有关的威胁。

威胁监控系统。该系统是一个内部工具，将从一些来源收集到的威胁情报信息进行汇总和分析，以发现感染病毒的电脑或地方网站，并减轻影响。

恶意程序分析实验室

成立该实验室的目的是在全国范围建立衡量、分析恶意程序威胁及提供防护以免遭受这一威胁的能力。目前，该实验室提供一份详细报告，说明恶意程序在感染病毒机器中的表现形式，目标系统的种类，国内恶意程序来源，命令和控制服务器与因特网的任何链接。该实验室还有助于测量收集到的每套恶意程序的杀

伤力，以便通过恶意程序的总量评估与具体恶意程序威胁有关的风险，并利用市场现有的一切杀毒引擎查杀恶意程序。

公共事件处理

卡塔尔计算机应急小组旨在通过向民众和关键部门提供必要支持，尽可能减少卡塔尔国受病毒感染的机器数目。为了实现这一目标并提供正确指导，卡塔尔扩大了事件回应服务，通过公共事件处理门户网将家用非对称数字用户线路因特网用户涵盖在内。计算机应急小组提供各种措施、准则和基本软件工具，扫描和查杀家用非对称数字用户线路机器中的病毒。

网络安全培训

计算机应急小组为政府各组织和其他海湾合作委员会国家的信息技术专业人员举办与网络安全有关的培训和讲座。

网络安全认识

应急小组以公司雇员为重点，建立有关网络安全问题的人类知识基础，并确定最佳做法。

该小组努力保护重要基础设施，因为一些行业部门如金融、能源及信息和通信技术，对维持卡塔尔经济以及卡塔尔人口和政府的需要至关重要。为此，该小组力求保护作为这些关键部门基础的信息系统，做法如下：

- 确定国家防护战略、最佳做法、框架和工具，以及提高利益攸关方的认识
- 直接协助关键基础设施拥有者和操作者，改进监督控制和数据采集网络保障措施
- 了解行业部门问题和跨部门依赖性，以及实施针对具体部门的防护战略
- 与国际保护信息基础设施组织合作，确定跨国解决方案
- 衡量本国的国际保护信息基础设施组织的成熟性，评价进展情况

此外，最高信息和通信技术委员会网络安全方案继续与立法机构合作起草法律和标准，以不断改进应对当前新出现的威胁的国家信息和通信技术保障措施。

最高委员会建议通过国际社会采用/拟订下列可能的措施：

- 5 年内在所有国家建立在区域一级协调统一的国际法律框架
- 3 年内在目前尚未成立计算机事件应对小组的所有国家成立这一小组
- 5 年内拟订与国际合作原则相符的国家网络安全战略，包括重要信息基础设施保护措施

- 以各种利益攸关方(例如，政府、学术界、私营部门和学校)的能力建设和提高认识为目标，制定网络安全课程
- 强调必须为儿童和青年提供网上安全意识方案。

土耳其

[原件：英文]

[2012 年 5 月 31 日]

信息和通信技术迅速渗入日常生活和业务流程。对个人、机构或政府至关重要的各种数据以数字方式得到储存并在网络空间传输。尽管好处多多，但技术也带来一定风险，比如不能维护数字存储数据的机密性和完整性，并存在信息系统可利用性问题。信息和通信系统的脆弱性——产生于设计、配置和操作错误，技术能力不足以及雇员和用户缺乏培训或安全意识——为这些风险的产生提供了合适的环境。

为了规避风险或减少风险，修补脆弱性，在国家和机构一级为建立网络安全作出努力的重要性与日俱增。在这方面，建立公私营机构行政人员、雇员和用户的技术和行政能力以及提高他们的安全意识被认为是这些努力的重要部分。

土耳其政府高级行政人员深切了解加强国家信息安全的必要性。此外，土耳其信息和通信管理局特别侧重于研究网络空间的最佳做法和新产生的威胁，组办国家网络安全活动，加强应对紧急情况的机构和技术能力，对电子通信操作员定期进行审计，以确保有充分的政策、程序、方案和监控手段来妥善处理电子通信安全事件。

为了加强全球信息和通信系统安全，研究有关全球威胁、信息系统的具体脆弱性、信息机制方面的最佳做法的国际概念以及与其他国际组织分享专家知识，具有实际意义。

举行就网络空间信息和通信安全事件采取合作和取证方法的多方会议，以及交流有关恶意软件数据库信息，可证明是加强全球信息安全的有益工具。

乌克兰

[原件：俄文]

[2012 年 5 月 31 日]

对信息安全问题的一般看法

信息和通信技术被迅速引入生活的各个领域以及信息联系趋于全球化，导致全世界范围的非法活动转移到网络空间。如今，没有国境之分的计算机犯罪(亦称网络犯罪)不仅威胁到个人的权利和自由，也威胁到民族利益和国家安全。

近年来，国家重要基础设施遭计算机攻击事件明显上升，通过扭曲重要信息、扰乱工厂的生产流程、干扰公用事业和能源供应及运输系统，对国家造成危害。

个别国家国家机关和机构的信息系统是黑客发动攻击以阻碍其活动的目标，2011 年对这些国家的网络犯罪评估表明，网络攻击对社会构成重大威胁，其后果难以预料。

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

一些发达国家为对付这些威胁建立了由一个单一协调机构领导的国家打击网络犯罪系统。通过这一方法可以有效集合相关政府和非政府实体的实力和资源，打击和化解网络安全威胁。

这是为审查对下列各项采用的方法提供指导时的主要考虑之一：评估新的威胁和挑战，包括在信息安全领域，举办关于建立一个单一的全国打击网络犯罪系统的国家高级别活动，起草网络安全法案，以及与外国情报机构和执法机构建立和加强合作。

2011 年 6 月，乌克兰安全局与 11 个国家(加拿大、塞浦路斯、法国、德国、拉脱维亚、立陶宛、荷兰、罗马尼亚、瑞典、联合王国和美国)的机构合作，制止了一伙黑客的犯罪活动。这伙人通过因特网用恶意软件传播病毒，从外国银行机构盗取了 7 200 万美元。

2011 年 10 月，乌克兰安全局在乌克兰雅尔塔组织了由乌克兰和北大西洋公约组织专家出席的网络防御年度圆桌会议。会议结果更加坚定了乌克兰关于有必要在公私营部门的参与下及利用其他国家的经验，进一步发展信息安全系统的立场。

在安全局倡议下，独立国家联合体特勤局、安全和执法机构主管第三十二次会议将讨论关于设立一个单独的网络安全委员会的问题。

第 2 段(大会第 66/24 号决议)所述概念的内容

乌克兰立法将对国家安全，包括信息安全构成的主要威胁界定如下：

- 限制公民的言论自由和获取信息的自由。
- 网络犯罪和网络恐怖主义。
- 暴露国家机密或任何其他受法律保护的机密信息，或暴露属于国家财产，或用来满足国家需要及社会和国家利益的保密资料。
- 企图操纵民意，包括传播误导性、不完整或带有偏见的信息。

国际社会为加强全球一级的信息安全可能采取的措施

国际社会可用来加强信息安全的主要途径是，为个别国家确保本国信息安全和在这方面建立有效合作创造有利环境。

为建立有效打击信息安全领域的现有威胁和潜在威胁的机制，国际社会应采取下列措施：

- 推行促进网络防御合作的协商机制，便于就起草这一领域的立法和条列交流经验。
- 建立系统，以交流网络空间监测信息，及早通报网络攻击事件及交流网络攻击技术层面的信息，同时追查攻击源头以及采取有效的反措施。
- 加强合作，消除网络攻击的有害影响，分享经验，拟订遏制网络攻击的技术解决方案和组织建议。
- 拟订制定标准术语和《因特网行为守则》等规则的国际法律文书。

由于需要应对这些威胁，伙伴情报机构和执法机构应在下列领域共同作出努力：

- 建立机制，使各情报机构能够针对有组织犯罪团伙，包括恐怖主义团体未经许可干扰国家因特网基础设施或政府部门或企业信息系统的信息资源的活动迅速分享信息。
- 分享有关下列各项罪行的信息：为伪造银行卡等目的未经许可闯入金融机构的计算机系统，或为了偷取机密资料或阻挠业务，未经许可干扰银行计算机系统的运行。
- 在开展业务时进行合作，追查利用国家因特网基础设施进行网络犯罪的人，并记录他们的非法活动。
- 在调查利用计算机技术进行犯罪时，交流审查软件和硬件(网络法证)方面的经验和现行做法，分享计算机设备的审查方法和技巧，以便记录犯罪活动。
- 为情报机构工作人员提供联合培训方案，为情报专家提供实习生方案。
- 参加关于打击网络犯罪的讲座、研讨会和会议。

可采用的一种合作形式是，为确保及早发现威胁而建立监测国家因特网基础设施资源系统，以及建立确认化解这些威胁的最佳工具的系统。

可将建立国家计算机事件应对中心及促使他们彼此间密切合作作为一个可能的协调机制，以便对国家机构、电信服务提供者和国家信息和通信技术基础设施其他行为者开展的防止非法使用计算机和信息技术网络安全活动进行协调。

这些国家中心的重要任务包括以下方面：

- 在相关数据库信息中收集、分析和汇编有关现有的网络安全威胁的信息。
- 监测和查明其运作违反了关于使用国家因特网基础设施的条列的网络机制和资源。
- 拟订建议，使因特网用户能够保护个人、社会和国家在信息领域的利益，并建议向用户提供咨询服务和技术支持。
- 接获有关黑客攻击的紧急报告，为制止攻击提供紧急援助，立即向因特网用户和其他信息系统(地方系统和公司系统)用户发出关于网络安全威胁的通知。
- 与其他国家同类中心合作和交流信息。