联合国 A/68/156/Add.1

大 会

Distr.: General
9 September 2013
Chinese
Original: Arabic/English

第六十八届会议

临时议程 * 项目 94

从国际安全角度看信息和电信领域的发展

从国际安全角度看信息和电信领域的发展

秘书长的报告

增编**

目录

* A/68/150。

** 本报告内的资料是在主要报告发布之后收到的。

13-47544 (C) 071013 091013

二. 从各国政府收到的答复

亚美尼亚

[原件：英文]
[2013 年 7 月 5 日]

亚美尼亚共和国 2009 年 6 月 25 日 NK-97 号总统令通过了信息安全概念文件。总统令指出，亚美尼亚共和国的国家安全在很大程度上取决于信息安全，包括信息、通信和电信系统等部分。概念文件还总体评估了亚美尼亚共和国的信息安全问题、当前面临的挑战和威胁及其根源和特点以及在不同公共生活领域解决这些问题的方法。

成立了一个政府间委员会，以协调与信息安全概念文件有关的方案的实施。

亚美尼亚共和国 2010 年 2 月 25 日的政府决定核准了“网络社会的形成”概念文件。成立了亚美尼亚共和国电子政务理事会，在“网络社会的形成”概念文件框架内界定了网络安全的一般范围。概念文件附件 4 列出了确保国家网络安全的各项工作。成立了一个国家委员会和一个专家组，以努力实现上述目标。

在国家层面采取了以下措施，以加强信息安全。

根据 2009 年 4 月 30 日第 479-N 号政府令，建立了一个特别通信站，以处理因特网安全问题，该通信站正在运行之中。该站确保上载因特网的政府机构公共信息的安全，并确保政府机构的信息系统与因特网的安全连通。

2012 年初，专家组制定了关于在亚美尼亚共和国建立网络安全系统的国家方案草案。方案草案目前正在亚美尼亚政府内进行讨论。

亚美尼亚共和国于 2006 年批准了 2006 年在布达佩斯开放供签署的《网络犯罪公约》，并于 2012 年批准了《关于在个人数据自动处理方面保护个人的公约》。亚美尼亚共和国国家安全局和警方是执行上述公约规定的主管政府机构。目前，政府间专家组正在开展活动，根据《公约》调整相关的本国法律。

亚美尼亚共和国在欧洲安全与合作组织(欧安组织)的框架内开展网络安全方面的积极合作。目前，亚美尼亚方面正在非正式工作组的框架内进行谈判，以制定一套网络安全建立信任措施。

亚美尼亚方面在其《2011-2013 年个别伙伴行动计划》中列入了网络防卫领域的一项行动，包括七项子行动，该计划正在与北约合作执行。

加拿大

[原件：英文]
[2013 年 9 月 3 日]

加拿大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所载评估意见和建议，谨向秘书长通报对下列问题的看法和评估意见。

1. 信息安全

加拿大对恶意网络活动带来的实际威胁上升感到关切，并认识到，应对恶意网络活动必须开展国家、区域和国际合作。

保持一个开放的网络空间符合加拿大的战略利益，因为这对加拿大的繁荣、安全以及民主和人权价值十分重要。加拿大公私部门的日常运作都有赖于安全、可靠和稳定的信息基础设施。基于计算机的系统及其因特网和网络连接成为许多加拿大关键基础设施的骨干，包括能源、金融、电信和制造行业以及政府信息系统。关键基础设施的平稳运行支撑着我们的方式生活和加拿大的经济、政治和社会福祉。

国家层面

早在 1996 年，加拿大政府就认识到，对加拿大关键基础设施的运作至关重要的系统可能受到网络攻击，政府有责任保护这些系统不受这种攻击。随后几年，政府采取了行动。在审查其评估和降低基础设施脆弱性的能力后，政府通过建立伙伴关系，开发和实施了保护加拿大关键基础设施的综合方法，并监测和分析了对联邦政府系统的网络攻击和威胁。2010 年，政府发布了国家重要基础设施战略和行动计划，并于今年早些时候发布了加拿大网络安全战略 2010-2015 年行动计划，其目的是确保政府系统的安全，建立伙伴关系，以确保联邦政府以外的重要网络系统的安全，并帮助加拿大人安全上网。

国际层面

2007 年以来，加拿大一直是美洲国家组织(美洲组织)网络安全方案的主要捐款国，该方案通过加强国家层面的规划和协调及区域合作，协助美洲各国预防、监测和应对网络威胁。加拿大通过反恐能力建设方案，帮助几个美洲组织成员国制定自己的国家网络安全战略，并加入美洲组织网络安全事件应对小组北半球安全网络。

自 2012 年以来，加拿大和欧洲安全与合作组织(欧安组织)的其他成员国努力制订建立信心和安全措施，以减少可能源于信息和通信技术使用的误解、升级和冲突风险。

加拿大还在一些论坛(包括八国集团、联合国毒品和犯罪问题办公室和美洲组织)积极参与打击网络犯罪的国际活动。加拿大还参加了最近联合国关于从国际安全角度看信息和电信领域发展的政府专家组(2012-2013 年)。

2. 国际概念

现有条约和习惯国际法适用于各国对信息和通信技术的使用，对于维护和平与稳定以及促进开放、安全、和平和无障碍的信息通信技术环境必不可少。与网络空间有关的现有国际法律包括《联合国宪章》、国际人权法和国际人道主义法。在最近的联合国政府专家组的报告中，加拿大高兴地看到，各国明确肯定，国际法作为负责任的国家行为的规范和原则基石，同样适用于网络空间。

加拿大还认为，在确保信息和通信技术安全性的同时，必须尊重人权和基本自由，包括持有看法而不受干涉的权利，以及表达自由、结社与集会和隐私得到尊重的权利。表达自由权载于《世界人权宣言》和《公民权利和政治权利国际公约》。这两项文书规定，人们在网下所享有的权利在网上同样应当得到保护，尤其是表达自由，这项权利不分国界，可以通过个人选择的任何媒介行使。

3. 可能采取的加强全球信息安全措施

加拿大正密切加强与国际伙伴，包括主要多边组织和私营部门协会的合作，以加强网络信息安全，这是加拿大经济繁荣和安全的支柱。加拿大还在一些主要合作伙伴以及网络安全领域的多边组织内加强合作和信息共享。

加拿大开发了一个新的进程，以协调国家对重大网络事件的反应，并动员其关键基础设施的所有者和经营者，制定和实施他们自己的网络安全战略。

其他国家对加强网络安全和防止网络犯罪也广泛关注。欧洲委员会的《网络犯罪公约》是专门针对网络犯罪的主要国际文书，加拿大于 2001 年签署了该公约。该文件也被称为《布达佩斯公约》，是制定全面的国家打击网络犯罪法律的指南，也是各国之间开展国际合作的框架。

德国

[原件：英文]
[2013 年 6 月 25 日]

对信息安全问题的一般看法

经济、行政和私人互动的数字化不仅是一个持续的过程，而且在加速。这不仅为工业化国家，也为发展中国家提供了前所未有的机遇。与此同时，对信息通信技术越来越多的依赖也产生了脆弱性和系统性弱点。所有行为体，从私人用户到企业和政府组织都形成了新的相互联系。网络攻击的趋势显然向更复杂的恶意活动发展，如针对高价值目标的严重持续性威胁或高度复杂的恶意软件。这些活

动以营利为目的，或意在于获取关键资产、系统和基础设施的控制信息，给政府、众多企业和组织，包括关键基础设施的服务提供商造成了严重后果。众所周知，高度复杂的恶意活动往往难以检测。确保现有技术安全的努力往往赶不及创新的速度。恶意工具和方法可以相对容易地获取，它们在监管不力的市场或黑市上就可买到，更加剧了风险。我们现有的信息技术环境无法仅仅通过传统的信息技术安全方法防范这些恶意活动。

高度专业的攻击者投入可观的技术和资金，来探寻信息通信技术系统的弱点，并为自己的目的利用这些弱点。难以可靠地确定源头以及由此产生的“假借旗号的攻击”机会，增加了国家和国际安全的风险，特别是由于误解和误判所造成的风险。意在收集信息的入侵最初看起来往往与那些以破坏为目的的攻击并无不同。这进一步增加了对外来攻击误解的可能性，可能导致国家在国际关系中违禁使用武力。

在哪些规范适用于网络空间问题上的普遍模糊性也增加了不可预见性。

事实证明，关键基础设施的程序控制系统，特别容易受到恶意的信息通信技术活动的攻击。全球范围内无法控制的附带损害的风险很高，包括可能造成实体破坏影响的工业控制系统的感染。对核心电信基础设施的单一网络攻击所造成的全球破坏可能比单一实体攻击更严重。

尽管各国信息通信技术的能力和安全程度各不相同，增强应变能力的具体步骤却往往被拖延，甚至完全被排除在计划之外，原因是网络安全风险是不确定的，如何有效地解决这些问题也不确定，并且数字攻击复杂而不断翻新，个体事件因其隐秘也不引人注意。

国家一级的努力

联邦信息安全办公室成立于 1991 年，是联邦政府最重要的中央信息技术安全服务提供者。联邦信息安全办公室以此职能发布了具有约束力的联邦行政部门最低信息技术安全标准，并且是负责报告信息技术事故的中央部门。此外，它还是一个中立的信息技术安全领域咨询和支持办公室。该办公室工作的主要成就包括：信息技术安全管理标准，作为事故处理和信息交换平台的联邦机构计算机应急小组(自 1994 年起)，成立于 2006 年的公民计算机应急小组，负责更广泛的社会上的信息技术安全工作以及宣传工作。此外，联邦信息安全办公室负责就信息技术产品和服务的恶意软件和安全漏洞发出警告，通知有关各方(包括信息技术供应商和公众)，并提出对策建议。

2005 年国家保护信息基础设施计划同时针对政府和业界，该计划之后，联邦政府又在 2011 年 2 月通过了网络安全战略。其核心是关键基础设施的保护。

2008 年以来，德国政府和德国关键基础设施运营商一直以公私伙伴关系形式进行合作。这个“保护重要基础设施实施方案”设有若干工作组，分别针对网络安全的不同方面，如关键服务的危机管理、演习和可用性。

联邦信息安全办公室下属国家信息技术情况中心负责跟踪国家和全球信息技术安全形势，以迅速探查和分析重大信息技术安全事故，并提出保护措施建议。一旦出现信息技术危机，该办公室将扩大能力，成为全国信息技术危机反应中心，集中处理信息技术危机的能力，总揽国家各个方面，包括政府网络和关键基础设施。

为执行 2011 年网络安全战略，负责网络安全问题的所有政府机关将相互并与联邦信息安全办公室领导和主持的国家网络应急中心内的私营部门开展密切的直接合作。

政策方面，国务秘书级的国家网络安全委员会负责处理关键的网络安全问题，并提出德国对这些问题的立场。这包括协调网络外交政策，包括外交、国防、经济和安全政策等各个方面。

此外，2012 年 10 月在国家一级推出了合作和信息交流平台：网络安全联盟促进了经济、学术和行政领域的合作伙伴之间的密切合作，特别是与具有特殊公共利益企业的合作。

保护重要基础设施实施计划在经过四年运行后目前正在进行更新。该计划将对更多的关键基础设施运营商开放，并将在关键基础设施行业内成立一些新的工作组。此外，将建立与新的网络安全联盟的合作。

网络空间中的国际互联意味着必须在国际一级采取协调行动。因此在欧洲联盟和国际组织内，德国极力主张加强网络安全，同时在网络空间保护社会和经济利益。

鉴于信息技术的全球连通，德国在其网络安全战略中主张制定广泛、无争议、具有政治约束力的网络空间国家行为规范。他们应为大部分国际社会所接受，并应包括建立信任和提高安全性的措施。

网络空间的建立信任和安全措施

网络空间是一项公益物和一个公共空间。因此，我们必须从基础设施的复原力以及系统及其数据的完整性和故障安全性的角度来考虑网络空间的安全。既然是公共空间，各国就必须促进网络空间的安全，特别是防范犯罪和恶意活动的安全性，保护那些选择使用真实性验证工具的人免遭身份盗窃，确保网络和数据的完整性和保密性。

网络空间是全球性的。要确保网络安全、执行权利和保护关键信息基础设施，国家就必须在国家一级并与国际伙伴合作作出重大努力。在国家层面上，德国经济、学术和行政机构的大量计算机应急小组显然有相互开展合作的文化。在这方面，联邦计算机应急小组是这些小组的有效协调人。在欧洲和国际层面，联邦计算机应急小组与一系列其他政府计算机应急小组密切合作，其中，事件应对小组和安全小组论坛网络是全球计算机应急小组在网络空间相互连通的最重要的论坛。

在此背景下，德国准备就一整套涉及网络空间之内国与国的行为规范展开工作，特别包括信任、透明度和安全建设措施，并希望得到尽可能多国家的签署。因此，德国积极参加了 2012/13 年度政府专家组，专家组负责“继续研究信息安全领域的现有威胁和潜在威胁及为对付这些威胁可以采取的合作措施，包括国家在信息空间中负责任行为的规范、规则或原则和建立信任措施……”(大会第 66/24 号决议)。

德国在 2011 年 5 月 9 日至 10 日举行的欧洲安全与合作组织(欧安组织)网络安全会议上就这样一个关于国际规范的行为守则概述了如下可能的要点：

(a) 确认关于数据和网络可用性、保密性、竞争性、完整性和真实性、隐私和知识产权保护的一般性原则；

(b) 尊重保护关键基础设施的义务；

(c) 加强针对建立信任、减少风险措施、透明度和稳定的合作，具体做法是：

- 交流与国际网络空间监管有关的国家战略、最佳做法和国家看法；
- 交流对与网络空间使用有关的国际法律规范的国家看法；
- 设立和通报联络点；
- 设立预警机制和加强各国计算机应急小组之间的合作；
- 将危机通信链升级，以包含网络事件并支持拟订可促进建立稳健和安全的全球网络基础设施的技术建议；
- 在打击恐怖主义的责任中包含交流对付非国家行为者的做法，并加强有关合作；
- 支持发展中国家的网络安全能力建设，为大型活动的网络安全支助工作拟订自愿措施。

按照这一思路，德国于 2012 年 7 月向联合国政府专家组提交了一份立场文件。我们非常欢迎专家们关于网络空间负责任的国家行为和建立信任措施的规

范、规则或原则的建议，以及专家们对在网络安全方面采取多利益攸关方做法的重视。

2011 年和 2012 年，德国支持了联合国裁军研究所(裁研所)和汉堡大学和平研究及安全政策研究所开展的国际网络安全以及建立信任和安全措施项目。2011 年 12 月举行的第一届柏林网络会议，为国际网络安全方面的风险、战略和建立信任问题上的国际讨论提供了一个平台。2012 年 9 月举行的第二届柏林网络会议重点讨论了因特网与人权问题。一个主要的结论是，安全、自由和在线隐私是相辅相成的概念。德国还支持了 2012 年 11 月 8 日和 9 日在日内瓦举行的 2012 年裁研所网络安全会议，会议重点讨论了确保网络稳定性的建立信任措施。

此外，我们认为有必要就下列方面展开辩论：在确定网络攻击源头方面进行国际合作，因为网络攻击的源头通常很难追踪；国家在得到有关从其领土上发动的网络攻击的通报之后，仍不采取行动结束这类攻击而应对这类攻击承担的责任；国家在不促成网络空间的无法无天状态方面所应承担的责任，例如在知情的情况下容忍在其领土上储存非法收集的个人数据。

2013 年 6 月 27 日和 28 日举行的第三届柏林网络会议是由联邦外交部与波茨坦大学密切合作举行的，主题是“保护网络空间的自由和稳定：国际法的作用和相关性”，会议致力于对网络运行不逾越武装袭击的门槛从而不引致武装冲突法的适用问题进行国际法律评估。按照现有国际准则和原则，国家对在其控制范围内影响信息和通信技术的安全和稳定的行动负有责任。每一个国家都应该考虑如何最大限度地减少或制止源于其控制范围内在其网络上运行的恶意网络活动。按照国际习惯法下的现有国家责任规范，国家对与其有关的国际不法网络活动负有责任，这些活动包括网络空间中任何遵从该国指令或在其指示或控制下行事的国家支持的代理人的国际不法活动。各国应采取一切必要措施，确保其领土不被其他国家或非国家行为体用于非法利用信息和通信技术损害其他国家及其利益。这些必要的措施应包括履行国际责任所需的适当的国家立法和监管框架。国际不法网络活动可以三种主要方式涉及各国：(1) 作为可能具有破坏性影响的恶意网络活动的源头国；(2) 作为信息和通信技术基础设施被恶意网络活动利用的过境国；(3) 作为恶意网络活动造成的损害的目标国。在所有这些情况下，各国都有义务尽其职责，这既可以是实质性的，也可以是程序性的，其范围可从预防(即潜在危害发生前的阶段)到遏制(即实际、持续的破坏性网络活动的开始阶段)到后续活动(即恶意网络活动实施后的阶段)。

欧洲安全与合作组织的网络安全

欧洲安全与合作组织讨论网络安全问题已经有好几年了。2010 年在阿斯塔纳举行的欧安组织首脑会议上，欧安组织 56 个与会国的国家元首和政府首脑强调，

“在面临新兴的国际威胁时，必须实现目的和行动更大程度的统一”。《阿斯塔纳纪念性宣言》把网络威胁称为新出现的跨国威胁之一。

德国积极参与了 2011 年在维也纳举行的欧安组织关于“全面应对网络安全：探索欧安组织未来作用”的会议。会议讨论了有关欧安组织后续活动的具体建议。2012 年 5 月，常设理事会第 1039 号决定(PC.DEC/1039)设立了一个非正式工作组，负责制定一套建立信任措施草案，以加强国家间合作，提高透明度、可预见性和稳定性，并降低可能源于信息和通信技术的使用的误解、升级和冲突风险。2012 年 6 月，德国向工作组提交了一份非文件，其中载有德国对欧安组织框架内第一组建立信任措施的建议。德国感到遗憾的是，无法就第一组建立信任措施的通过在 2012 年 12 月的都柏林部长理事会上达成共识，但欢迎工作组在 2013 年恢复工作。

德国将继续支持欧安组织就探索欧安组织在网络安全领域的未来作用展开讨论。

网络安全的军事层面

由于军队在所有指挥层级也都越来越依赖信息技术以掌控日益复杂的情况，对信息的保护及处理信息的手段已成为首要任务。

但是，在军方的考虑中，信息安全面临的挑战不仅来自知道如何操纵武器实际摧毁信息基础设施的潜在对手，而且还来自不负责任的用户、技术故障、罪犯或单纯的意外事件。

因此，需要作出的努力包括提高每一个用户的认识，确保信息技术供应链的可靠性，采取对应性防御措施以抵御网络攻击，以及建立一个具有整体弹性的信息技术构架。

总之，需要进行全面风险管理，采取措施加强国家和全球层面的信息安全。

德国联邦国防军在国防军所有部门建立了有弹性的指挥和控制架构、安全技术和程序，以及信息技术安全组织，包括一个独立的计算机应急小组，在出现关键性信息技术运作故障时可进行干预。使个人能力和技术能力适应日益严重的威胁是一项永久性任务。

德国联邦国防军与德国联邦内政部密切协作作出努力，大力支持加强北大西洋公约组织(北约)和欧洲联盟的信息安全，并为此目的制定政策并更好地协调能力。此外，德国联邦国防军与一些国家就政策层面和工作层面的信息安全问题进行定期交流。

德国联邦国防军欢迎提出倡议，并与德国联邦政府其他部门就国际行动进行合作，以进一步保护全世界信息网络的可用性，例如拟订网络空间的自愿国际行为守则。

北约的网络防御

北约将网络安全定为新出现的关键性安全挑战之一。在 2010 年 11 月在里斯本举行的北约首脑会议上，各国国家元首和政府首脑通过的战略概念文件指出：“网络攻击可达到威胁国家和欧洲-大西洋繁荣、安全和稳定的程度”。

按照首脑会议宣言的要求，北约国防部长于 2011 年 6 月通过了北约网络防卫政策和网络防卫行动计划。从那时起，北约一直在持续实施该行动计划。

该政策侧重于保护北约的网络和与北约网络相连或为北约核心任务处理北约信息的成员国国家网络(包括拟订共同原则和标准，以确保在所有成员国内实现最低限度的网络防御)。为减少来自网络空间的全球性风险，北约打算与伙伴国、类似联合国和欧洲联盟这样的有关国际机构、私营部门和学术界合作。

德国欢迎北约就网络安全作出承诺，并积极支持有关讨论。

伊朗伊斯兰共和国

[原文：英文]
[2013 年 6 月 7 日]

1. 伊朗伊斯兰共和国认为，信息和电信技术和手段的使用为所有国家和整个人类带来了很多机会。如今，信息和电信是现代社会的重要组成部分，是促进国家富强和繁荣的非常重要的资源。伊朗认为，应在国家和国际层面尽一切努力，为所有国家尽可能广泛使用信息和电信技术和手段提供基础，并确保这些技术和手段仍然是所有社会的主要驱动力。

2. 毫无疑问，实现这样一个崇高的目标在很大程度上取决于，是否能够确保充分尊重所有国家在信息和电信领域的主权权利，包括不受任何限制或歧视地开发、购置、使用、进口和出口以及获得信息和电信技术和手段及相关服务。事实上，确保信息的持续可用性、可靠性、完整性和安全性，并建立一个安全和可靠的信息和电信环境符合所有国家的利益，因此非常必要。不可否认，采取任何措施拒绝或限制向发展中国家转让先进信息和电信技术实际知识、技术和手段，以及提供信息和电信服务，会对其整体发展产生不利影响，因此，应避免采取这些措施。

3. 与此同时，信息通信技术和手段有可能被用于非法用途，包括对国家的社会、文化、经济、政治和安全基础设施和利益产生不利影响的用途。一方面，社会对信息可用性和电信基础设施的依赖日益增长，另一方面，一些人，特别是犯罪分

子和恐怖主义分子，将信息和电信技术和手段用于非法用途，包括国家恐怖主义，这显示现有的脆弱性以及信息和电信产生的任何可能威胁的广泛影响。因此，重要的是在国家一级采取一切适当的基础设施、法律和技术措施，加强信息和电信技术和手段的安全性，防止其用于非法用途。

4. 然而，由于信息和电信技术和手段的复杂性和独特性，包括空间无边界、动态、匿名、速度和快速的技术进步，以及信息和电信基础网络之间日益增加的互联互通，似乎不可能仅仅通过采取国家措施确保信息和电信的安全。出于这个原因，并考虑到在很多国家发生的将这些技术和手段用于非法目的不断增多的情况，所有国家都应该在国家一级采取行动，在国际上开展合作。

5. 伊朗伊斯兰共和国注意到在联合国和其他国际组织内正在进行的与信息和电信问题有关的工作，但认为，从国际安全的角度审议信息和电信领域发展，最适宜的国际机制是在联合国内启动一个进程，并且所有国家平等参与这一进程。伊朗坚信这一进程的主要目的应该是，对于增强信息和电信的安全性的重要性，以及对信息和电信技术和手段的威胁的性质、范围和严重程度，建立国家之间的共同理解，并寻找防止这些威胁的方法和手段。此种进程可能会导致通过一个行动方案，其中设立各会员国应采取的必要措施，并以每五年召开国际会议的形式进行，以产生从声明到行为守则的各种政治成果。然而，这一进程的最终目标应该是为加强和确保全球信息和电信的安全性以及防止将信息技术和电信技术和手段用于非法目的，逐步建立坚实的国际法律基础。

6. 伊朗伊斯兰共和国认为，从国际安全角度审议有关信息和电信领域发展的问题应在以下原则和内容基础上进行：

(a) 作为一项一般原则，国际法是适用的，因此，应适用于各国对信息和电信技术和手段的使用。出于这个原因，在使用这些技术和手段时，各国必须遵守联合国的宗旨和原则及其《宪章》规定的义务，特别是有关通过和平手段解决国际争端的第二条第三款，有关禁止以与联合国宗旨不符的任何方式使用或威胁使用武力的第二条第四款，以及有关禁止干预和干涉国家内政的第二条第七款；

(b) 各国在信息和电信领域的主权权利应不受任何影响，包括不受任何限制或歧视地开发、购置、使用、进口和出口以及获得信息和电信实际知识、技术和手段及相关服务。因此，各国一定不要采取任何措施，拒绝或限制向发展中国转让先进信息和电信实际知识、技术和手段，以及提供信息和电信服务；

(c) 确保在国家一级信息和电信的安全性完全是各个国家的责任。然而，由于信息和电信是全球性的，应鼓励各国进行合作，防止恶意使用信息和电信技术和手段造成的威胁；

(d) 表达自由的权利应该充分予以尊重。与此同时，在任何情况下，均不应在行使这一权利时违背联合国宗旨和原则、保障国家安全、公共秩序、公共健康或道德和行为准则的国家法律和原则；

(e) 各国对其利用明显属于它们的信息和电信技术和手段从事国际不法活动的行为负责；

(f) 为所有国家的利益建立一个安全可靠的信息和电信环境应是主要的指导原则，因此，各国应避免在任何情况下，为敌对、限制或其他非法目的使用信息和电信技术和手段，包括开发和使用信息武器，破坏或动摇其他国家的政治、经济或社会系统或削弱他们的文化、道德、伦理或宗教价值观，违反国际法，包括宪法和国际电信联盟的规则或目标国家的本国法律进行跨界信息传播；

(g) 各国应在国家和国际层面提高认识，即需要通过负责任地使用相关的技术和手段，保护和改善信息和电信的安全，目的是营造一个信息与通信安全的国际共同文化。

日本

[原文：英文]
[2013 年 8 月 12 日]

对信息安全问题的一般看法

日本认为，网络空间是公共和私营部门社会经济活动的一项基本基础设施。网络空间通过确保信息的自由流动和表达自由促进经济增长、就业和发展，以及民主和保护人权。网络空间的使用对于人们生活必不可少，并已遍及全球。

与此同时，为充分享受网络空间的“积极一面”的裨益，对保护隐私和知识产权以及确保网络空间安全的需求不断增长。此外，网络攻击已在世界各地发生，并已成为全球跨国威胁。这些攻击可能是世界各地不同实体以不同方法进行的。一个国家不可能仅靠自己来解决不断增加的网络犯罪和网络攻击，国际社会，包括相关国家和利益攸关方的合作对于应对这些挑战必不可少。

基于这些观点，日本正在努力构建一个安全和可靠的网络空间，主要侧重确保信息的自由流动和表达自由，同时对在保护隐私和安全保证之间取得平衡给予应有的重视。

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

在国家一级加强信息安全的努力

最近，与网络空间有关的风险已经变得更为严重，维护网络安全已经成为一个与我们的国家安全和危机管理、社会和经济繁荣以及日本人民的安全与和平有关的重要议程。

在这方面，日本在2013年6月制订了一项网络安全战略，覆盖2013年至2015年三年期间。日本将根据这一战略采取行动，改善政府机构和重要基础设施的信息安全，并加强对网络攻击采取对策的能力。

具体而言，日本已经将以下措施纳入这一战略：与公私合作伙伴一起促进有关网络攻击的信息共享；不仅为政府和行业，也为日本人民提高信息安全素养；提高网络安全意识；通过国际合作加强对网络攻击采取对策的能力；提高我们在制订与网络安全有关的国际规则方面的贡献。

在国家一级促进国际合作的努力

在制订使用网络空间的国际规范方面，我们必须尽快开始制订现实和可行的行为规范，以不具法律约束力的形式来解决当前的问题，应对迅速发展的网络技术。日本将在国际论坛上继续积极参与这些努力。

在建立信任措施方面，日本正在积极与有关国家进行双边协商和区域对话，包括与东盟区域论坛，目的是“提高透明度”和“促进信息共享”。此外，为努力不在网络空间中造成安全漏洞，日本正在向亚洲、大洋洲和非洲的发展中国家提供能力建设援助，如组建和加强计算机应急小组。日本还在通过加强与其他国家的国家计算机应急小组的协调，在国际上推动信息共享。日本认为，这些努力有助于与有关国家建立信任。

第67/27号决议第2段所述概念的内容

日本认为，现有的国际法，包括《联合国宪章》和国际人道主义法，适用于网络空间的使用。然而，由于信息和通信网络技术的独特特点，需要进一步考虑如何适用个别规则和原则。

考虑到国际法在国际社会确保法律稳定性和可预见性中发挥的重要作用，我们认为，确定和阐明现行国际法如何适用于网络空间，将对有关网络空间的特定国际规范的制订起到补充作用，并有助于建立一个稳定的网络空间。

国际社会为加强全球一级的信息安全可能采取的措施

使用网络空间的国际规范

对于安全、经济和社会领域的网络攻击或网络间谍活动，现在还没有进行监管的国际规范。此外，网络空间方面具有法律约束力的规范的有效性在这一阶段仍不明确。在这个时候，难以确定网络空间的未来概况，因为网络技术的发展速度相当快。此外，就具有法律约束力的规范达成共识将需要很长的时间。因此，在规范的法律性质方面，日本认为重要的是开始讨论设立不具有约束力的一般行为规范。

建立信任措施

由于国家之间建立信任工作的累积会对国际规范的制订产生积极影响，国际社会必须继续促进这些工作。在促进建立信任措施方面，确保透明度和信息共享是必要的，但是，各国所采取的措施级别不同，因为每个国家有权力决定此种级别，因此，有必要通过在联合国主持下的框架和区域框架等全球框架鼓励信息共享。

荷兰

[原文：英文]
[2013 年 8 月 7 日]

荷兰十分高兴有机会提出对第 67/27 号决议的回应。

对信息安全问题的一般看法

荷兰支持安全和可靠的信息和通信技术，支持保护尊重人权的开放、自由的因特网。这对于我们的繁荣和福祉至关重要，是实现可持续经济增长的催化剂。

网络空间提供了多种机会，但也使我们的社会变得更为脆弱。威胁的跨国界性质使得国际合作必不可少。许多措施只有在得到国际共同执行或协调的情况下才能有效。在这方面，荷兰极为重视公共部门与私营部门的伙伴关系，通过建立信任措施架设桥梁，并提高所有信息和通信技术使用者对个人责任的认识。

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

荷兰正在为建立一个安全的数字环境在国家一级和国际上作出努力。在国家一级，荷兰政府在实施一个称为“合作产生力量”的国家网络安全战略。荷兰将在 2013 年更新这一战略，预计将 2013 年下半年公布。经修订的战略将涉及有关网络空间的全面观点，同时考虑到经济机会、开放、自由和安全。

荷兰的国家网络安全委员会确保在公共部门、私营部门和学术研究机构之间采取协作方法，并在网络安全领域为高级别决策者提出咨询意见。荷兰还有一个国家网络安全中心，该中心确定趋势和威胁，并帮助管理事故和危机。中心有三项任务：根据来自公共和私营部门的信息进行网络威胁分析；对网络威胁和事件作出反应；信通技术危机情况下的业务协调。该中心包括现有政府计算机应急小组。在过去一年中，该中心扩大了能力，并与重要信息分享和分析中心建立了紧密的关系。国家网络安全中心举行的国际年度会议使来自政府、私营公司、执法部门的专家和技术专家汇集在一起，交流最佳做法。荷兰已实施一套实质性措施，以提高网络安全，并非常愿意与第三国分享它使用的模式。

在核保安部门使用的公私合作伙伴关系的一个例子是荷兰政府举行的技术会议，核工业可以在此种会议上表明其在信息安全领域的需求。此种信息被政府用于改善“基于设计的威胁”。关键词是“现实”和“相称”。

在国际上，荷兰积极协助欧洲联盟、北大西洋公约组织、欧洲安全与合作组织、因特网治理论坛和其他伙伴关系作出努力。荷兰对欧洲联盟委员会和外交与安全政策高级代表联合信函持积极看法，该信函呼吁为欧洲联盟创建一个公开、自由和安全的网络空间，欧洲理事会已表示赞同该信函的观点。欧洲联盟正在与国际伙伴和机构、私营部门和民间社会一起应对这一挑战。荷兰完全支持欧洲联盟的目标，即确保互联网安全，同时推动互联网的开放和自由，以鼓励制订建立信任措施和行为规范，并在网络空间适用现有的国际法。我们坚信，安全和使用权利是保障互联网持续发展的关键因素。为此，欧盟已将核心价值，即人的尊严、自由、民主、平等、法治和尊重基本权利，作为其指导原则。荷兰赞同这些核心价值，并把它们视为任何网络安全战略的基础。荷兰同意，为促进建立强大的和有复原力的网络空间，公共部门和私营部门都需要发展自己的能力和高效地协同工作。

荷兰促进在各网络安全中心(包括计算机应急小组组织)之间进行实务合作，并加强国际观察和警报网络。网络犯罪迅速增多，这就需要进行有效执法，以维持对数字社会的信心。关于执法工作，荷兰鼓励来自其他欧洲国家及欧洲以外国家的执法机构进行更多的跨界调查。荷兰是《欧洲委员会网络犯罪问题公约》的缔约方，并鼓励其他国家加入该公约。

关于核信息的安全性，荷兰在欧洲核保安监管者协会内部分享包括网络安全在内的核安全的政策方针和最佳做法的信息。荷兰积极参加国际原子能机构的技术会议，这些会议旨在分享网络和信息安全的信息。

荷兰认为，自由、透明度和安全是相互配合和相互加强的。这是荷兰创建自由在线联盟的原因，该联盟目前有 21 个成员国政府。自由在线联盟致力于促进互联网自由，并强调数字权利的重要性。为此，志同道合的政府联盟在多利益攸关方进程中与民间社会和私营部门协调他们的努力和工作，以支持个人在网上行使他们的人权和基本自由的能力。为促进实现进一步保持互联网对所有人都是开放和自由的目标，联盟成员建立了数字捍卫者伙伴关系，这是一个支持创新解决方案的基金，目的是保护处于危险中的博客和网上行动者，并在互联网不自由或无法使用的国家提供紧急网络服务。荷兰对该基金的捐款在 2012 年 10 月 1 日至 2014 年 12 月 31 日期间达 100 万欧元。

国际社会为加强全球一级的信息安全可能采取的措施

荷兰的出发点是，建立一个能促进创新、刺激经济增长和保障基本自由的开放的因特网。荷兰强调，必须就旨在实现安全使用网络空间的国家行为标准的拟订工作继续进行对话。荷兰愿意对这一对话作出积极贡献。荷兰赞赏地注意到欧洲委员会、欧盟、 欧安组织和联合国政府专家组等不同的国际和区域行为者/利益攸关方在网络安全领域建立信任措施方面所作的重要工作。

在核保安峰会进程中，信息安全发挥核心作用。华盛顿核保安峰会《工作计划》和《首尔公报》称，核保安峰会国家旨在 “防止非国家行为体获取恶意使用此类材料所需信息或技术，并防止破坏核设施的基于信息技术的控制系统。”作为核保安峰会的主席，荷兰支持所有有助于实现这一目标的工作。

在核保安峰会进程中，荷兰支持大不列颠及北爱尔兰联合王国牵头执行和分享在核部门的信息安全领域中的最佳做法。这是通过以下途径进行的：制订和加强有关此类信息的有效管理和安全的国家措施、安排和能力；加强有关国家安全文化；与国家科学、工业和学术界联系，进一步提高认识，形成和传播最佳做法，增加专业标准，并借鉴国际原子能机构的经验并与其合作，支持其他主要国际组织和伙伴国促进共同实现这些目标。荷兰十分重视包容各方的因特网治理模式，让私营部门和知识机构参与这一对话，并愿意与其他国家分享经验和最佳做法。

要使网络空间更为安全和可靠，并充分获得网络在发展和将世界各国社会紧密联系在一起方面的充分潜力，就必须在所有利益攸关方和组织之间就知识和信息进行密集的国际交流。因此，荷兰欢迎在伦敦和布达佩斯举行的网络会议，以及即将在首尔举行的会议。

最后，荷兰认为，国家行为规范的制订并不需要重编国际法，而是需要确保在适用现行国际法律框架方面的一致性。我们鼓励继续对话和思考，以在网络空间适用现有规则和国际法律的实际效果方面达成共识。

阿曼

[原件：阿拉伯文]
[2013 年 6 月 26 日]

交通和通信部谨转递以下涉及大会关于从国际安全的角度来看信息和电信领域发展的第 67/27 号决议的资料：

1. 对信息安全问题的一般看法

信息技术和电信领域发生的快速发展伴随着越来越大的风险。黑客正在使用日益先进的技术在全球获取信息。国家和机构面临的最严峻挑战是信息和通信技术用户之间的信息安全文化缺乏或不够，缺乏合格人员，世界各国监管电子通信的立法不同。各国必须联合起来共同合作，打击信息安全威胁，加强应急准备，提高全球对这个问题的认识，并分享相关的信息与专长。

2. 在国家一级为加强信息安全和促进这一领域的国际合作做出的努力

- 电信管理局成立于 2002 年，信息技术管理局成立于 2006 年，以监管电信和信息技术部门；

- 颁布了相关立法，即第 69/2008 号皇家法令发布的《电子交易法》和第 30/2002 号皇家法令发布的《电信监管法》；
- 国际电信联盟和打击网络威胁国际多边伙伴关系最近在阿曼设立了第一个阿拉伯区域网络安全中心；
- 为了应对技术风险和威胁，信息技术局在 2010 年 4 月设立了一个国家计算机应急小组；
- 通过信息技术管理局，阿曼加入了许多相关区域和国际机构，包括伊斯兰会议组织计算机应急小组、海湾合作委员会计算机应急小组和事故应对和安全小组论坛。许多阿曼机构已获得 ISO 认证；
- 主管机构不断更新其战略；
- 政府当局可以利用一系列信息安全技术和方案；
- 为保障政府网络设立了一个中心；
- 为保障政府网站设立了托管服务；
- 为加强信息安全提供技术支持；
- 采用了一系列信息安全政策与标准；
- 举办了一系列信息安全培训课程；
- 组织了各种提高认识运动；
- 开展了评估信息应急准备方案；
- 举行了一些相关的区域和全球讲习班与会议；
- 在地方一级开展了提高认识活动；
- 社会各部门都参与了促进信息安全工作；
- 促进信息安全的阿曼国家计算机应急小组大使方案于 2012 年 1 月启动；
- 创建了一个加强儿童在线安全的网站(cop.cert.gov.om)；
- 对学校、大学、网吧和青年经常光顾的其他地方进行了提高认识访问；
- 为提高学生和教员的认识举办了讲习班；
- 中心在公共活动中发挥了积极作用，帮助尽可能多的青年人，并向他们通报安全风险和对策；
- 中心举办了“训练教练员”方案，使年轻国民获得有关资格；

- 开设了第一个中东信息安全行动中心。

3. 概念的内容

- 阿曼不断监测并审查这些国际概念，以便跟上加强全球信息和电信系统安全的努力。
- 必须考虑到各国的具体情况及其电子交易立法。
- 利益攸关方必须遵守每个国家都力求维护的特定价值观和原则。

4. 国际社会为加强全球一级的信息安全可能采取的措施

- 根据 2013 年 3 月在阿曼举行的网络防御会议的建议，建立一个联合国主持下的国际组织，监管电子交易和信息及国家间网络安全；
- 促进国家间合作，以期为信息和通信技术部门提供保障。大多数国家很大程度上依靠这个部门的努力促进发展。这种合作必须在一个国际组织的主持下进行；
- 持续开展国家间协调，加强信息安全并分享先进经验；
- 协调应对信息安全事件，为每一个国家指定协调中心；
- 参与政策和条例制订并分享最佳做法；
- 分享专长和知识并进行互访；
- 为信息安全人员举办座谈会和讲习班；
- 组织联合国际方案，以提高认识和传播全球安全文化；
- 扶植学术协作并制订相关方案与课程；
- 鼓励和扶植这个领域的联合研究和开发方案。

土耳其

[原件：英文]
[2013 年 6 月 10 日]

对信息安全问题的一般看法

随着越来越多地使用信息技术，信息安全成为全球化世界的一个必要条件。信息安全和网络安全是必须与有关各方合作管理的事项。在土耳其，网络安全局这个协调有关各方并跟踪相关研究的中央机制是内阁关于强制执行、管理和协调国家网络安全研究的决定设立的。2012 年 10 月 20 日第 28447 号《土耳其政府公报》公布了这项决定。

2012 年 12 月 20 日，国家网络安全局第一次会议核准了 2013-2014 年国家网络安全战略和行动计划。

战略和行动计划的目标如下：

- 建立一个基础设施来实现各政府组织通过信息技术提供的服务、流程和数据；
- 确保由政府或私营部门运行的重大基础设施所使用的信息系统的安全；
- 确定战略网络安全行动，以尽量减轻网络攻击的影响并缩短攻击后恢复时间；
- 构建一个基础设施来协助司法当局和执法机构调查网络犯罪。

行动计划的主要领域如下：

1. 条例；
2. 协助司法程序的研究；
3. 建立一个国家计算机应急小组；
4. 加强国家网络安全基础设施；
5. 培训人力资源，提高其对网络安全的认识；
6. 发展国家网络安全技术；
7. 扩大国家网络安全机制的范围。

行动计划由在上述主要领域执行的 29 个行动方针组成。

在国家一级为加强信息安全和促进这一领域的国际合作做出的努力

《电子通信法》(第 5809 号)授权成立的土耳其国家监管机构，即信息和通信技术管理局（信通技术管理局）开展了一系列活动，促进满足国家和国际信息安全需求的努力。

在这方面，管理局的网络安全领域活动见下文。

1. 监管和检查

《电子通信安全规章》及以此规章为依据的相关公报规定了对授权营运人的若干要求。有关研究旨在直接在营运人活动中提高国家网络安全水平，并间接促进国际网络安全。

另一方面，《电子签字法》(第 5070 号)和《土耳其贸易法》(第 6112 号)范围内也有关于电子签字和登记电子邮件的管理局条例。这些条例有助于促进文件和电子邮件交流过程安全可靠的努力。

2. 网络安全演习

信通技术管理局组织了网络安全演习，以进一步发展技术和行政能力，提高认识，并创造国际合作机会。

2.1 2011 年国家网络安全演习

2011 年国家网络安全演习于 2011 年 1 月 25 日至 28 日举行，有 41 个公共、私人和非政府组织参加，包括金融、信通技术、教育、国防和保健部门以及司法执法单位和各部委的代表。6 个上述组织的代表以观察员身份参加了演习。

2.2 2012 年网络保护演习

2012 年 5 月在信通技术管理局协调下举行了这次演习，在电子通信部门运行的 12 个因特网接入服务提供者参加了演习。这些参加者和第三代(3G)移动因特网服务提供者在该部门中的市场份额最大。在这次演习中，对参加者主要实施了分布式拒绝服务攻击，对防御这些攻击的安全措施的适当性进行了评估。

2.3 2013 年国家网络安全演习

信通技术管理局与土耳其科学和技术研究理事会在交通、海洋事务和通信部的主持下，共同组织了 2013 年国家网络安全演习，于 2012 年 12 月 24 日至 2013 年 1 月 11 日举行，有 61 个公共、私人和非政府组织参加。尽管大多数参加者是政府组织，私人和非政府组织也参加了演习。此外，国际电信联盟(国际电联)——打击网络威胁国际多边伙伴关系主席以及作为网络安全国际合作平台的事故应对和安全小组论坛的一名委员会成员作为发言者出席了演习闭幕式。

3. 预防网络威胁项目

预防网络威胁项目(Siber Tehditleri Önleme Projesi-STOP)涉及为建立一个发现网络威胁的蜜罐系统而开发必要的机制，安装和改进一个网络攻击报告系统，制作关于网络威胁的元数据。该项目所需活动按照短期国家网络安全行动计划所预期的最后期限即将完成。在该项目的国际合作范围内，信息和通信技术管理局成为国际电联——打击网络威胁国际多边伙伴关系的成员。该伙伴关系在国际电联的领导下工作。

4. 防止垃圾邮件项目

2009 年在信通技术管理局的协调下开展了这个项目，因特网服务提供者和托管服务提供者做出了努力。项目旨在防止对网络安全构成威胁的垃圾邮件，并占

用网络资源。在项目结束时，传播垃圾邮件的因特网提供者数目减少了 99%；全球网络安全公司编写的报告反映了这一改善。

5. 建立一个国内因特网交换点

互联网服务提供者从一个远程点在两个端点之间不必要地循环互联网流量的路由做法，会由于不必要的传输延迟和安全关切的增加而导致服务质量下降。

在这方面，通过建立一个有效的因特网交换点，以及运营者有能力在更具吸引力的情况下交换流量，不可取的路由做法及其引起的安全关切可以大大减少。因此，信通技术管理局与有关各方(国内因特网服务提供者和国际内容提供者)一道开展各种活动，重点是建立一个有效的国内因特网交换点。

加强全球信息安全的措施

建立一个国家计算机应急小组

今天，有必要成立一个网络事件应对组织，在国家一级开展有效工作，查明新出现的网络威胁，采取必要措施减少或抑制潜在网络事件的影响，并共享信息。为此，2013 年 2 月，交通、海洋事务和通信部将设立和运作土耳其国家计算机应急小组的任务下放到通信主管单位。为设立每周 7 天、每天 24 小时防御网络威胁的国家计算机应急小组发起了各种活动。2013 年 5 月开始运作的计算机应急小组(USOM)将努力与其他国家的计算机应急小组及国际组织密切合作。

由于信通技术的迅速发展和传播，对信息安全的威胁超越国界。因此，国际组织和各国政府必须促进信息安全相关问题合作，并尽快开展这种合作。