联合国 A/66/152

大会

Distr.: General
15 July 2011
Chinese
Original: English/Russian

第六十六届会议

临时议程* 项目 93

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/66/150。

11-41690 (C) 290711 030811

一. 导言

1. 大会在其第 65/41 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 [1] 的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 2011 年 3 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

澳大利亚

[原件：英文]
[2011 年 5 月 31 日]

澳大利亚欢迎有机会根据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 65/41 号决议提交本答复，表达我们的意见。

澳大利亚希望成为网络安全方面的世界领袖。我们认识到技术进步对全球数字经济和所有国家的安全所具有的重要性和裨益。澳大利亚力求利用自己的专门知识为所有国家创造最大程度的经济和安全收益。

随着技术越来越渗透进我们的生活之中，政府、企业和个人也就因各种目的和功能而越来越依赖于技术，如在线购买商品和服务、与别人交流、寻找信息和管理财务，甚至控制采矿和制造业中的设备等。要使因特网和数字经济带来的裨益最大化和增强全球网络安全，各国就必须一起努力，造就一个可靠、安全和有弹性的网络空间。澳大利亚努力成为主动参与者，为所有用户——国家、企业和个人——增强网络空间而发挥作用。

[1]

对信息安全问题的一般看法

澳大利亚认识到，网络安全属于国家最高安全优先事项。国际社会继续在经受网络犯罪规模不断扩大、复杂性不断增加和成功犯罪次数不断增多的情况。随着电子信息数量和价值的提高，罪犯和其他恶意行为者的努力也在增强；他们把因特网当作进行其活动的更为隐秘、便利和有利可图的途径。

在面对和管理这些风险时必须与包括隐私权在内的个人的公民自由权进行平衡，并需要促进效率和创新，以确保使澳大利亚实现数字经济的所有潜力。

澳大利亚及每一个国家的国家安全、经济繁荣和社会福祉都与各种信息和通信技术的可用性、完整性和保密性密不可分。据此，澳大利亚政府已投入大量资源，积极促进维护一个可靠、安全和有弹性的电子操作环境，以造福于所有用户。

尽管澳大利亚政府的网络安全政策主要侧重于澳大利亚信息和通信技术的可用性、完整性和保密性，但这一政策与其他相关政策和方案的网络安全政策是有协调的，例如网络安全着重于保护个人，特别是儿童，免受冒犯性内容、欺凌、为性剥削目的进行在线跟踪或诱骗等行为的侵扰。

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

为加强信息安全而作出的国内努力

澳大利亚认识到，要促进网络空间的国际合作就必须在国内模拟最佳做法。澳大利亚实施了一种以政府为主导的保护和加强网络安全的综合方法。在 2009 年，政府公布了首个网络安全战略，阐述了澳大利亚政府网络安全政策的总目标和具体目标，规定了澳大利亚政府为实现这些目标所要完成的各项战略优先事项。该战略还说明了澳大利亚政府在为实现这些战略优先事项而展开的全面工作中将要采取的各项关键行动和措施。

澳大利亚网络安全政策的目标是维护一个能支持澳大利亚国家安全并能使数字经济的裨益最大化的可靠、安全和有弹性的电子操作环境。该战略的关键举措包括建立两个相互支持的组织：一个新的国家计算机应急小组和网络安全作业中心。国家计算机应急小组成立于 2010 年，为所有澳大利亚人和澳大利亚企业提供了网络安全信息方面的一个单一联络点，并确保使澳大利亚的因特网用户能得到关于网络威胁、其系统脆弱性的信息，以及有关如何更好地保护其信息和通信技术的信息。国家计算机应急小组与操纵着对澳大利亚国家利益具有重大意义的系统的各关键基础设施和企业的业主和运营商保持密切工作关系。该小组向这些企业提供有针对性的网络安全威胁和脆弱性信息，以协助更好地保护他们的信息和通信技术基础设施。同样成立于 2010 年的作业中心向澳大利亚政府提供所有来源网络态势情况，并能以更强的能力促进对具有国家重要性的网络安全事件

作出业务反应。该中心确认和分析复杂的网络攻击，并协助应对发生于政府和关键私营部门系统和基础设施的网络事件。

该战略的一个关键优先事项是用信息、信心和实用工具教育和武装所有澳大利亚人，使他们上网时能保护自己。该战略的指导原则是共同责任原则，即所有用户在享受信息和通信技术裨益的同时，应采取合理步骤保护自己系统的安全，在交流和储存敏感信息时应谨慎小心，并有义务尊重其他用户的信息和系统。为使个人能在信息安全领域发挥积极作用，个人就必须知道和理解网络环境及其风险。为实现这一目标，澳大利亚现正开展一个提高认识方案，其中包括为澳大利亚家庭用户和小企业，包括为那些网络知识和技能有限的人建立了一个网络安全信息网站(见 www.staysmartonline.gov.au)，并与企业、消费者团体和社区组织合作开展了一个网络安全认识周。认识周帮助澳大利亚人了解网络安全风险，并教家庭和小企业用户用简单步骤保护其在线个人信息和财务信息。在 2010 年全国网络安全认识周期间，大约有 150 个政府机构、行业、社区和消费者组织合作在澳大利亚城市、区域和农村举办各种活动。在 2011 年，从 5 月 30 日至 6 月 4 日举行了认识周。

澳大利亚政府承认，网络空间安全是一项共同责任，因此主动与因特网业协会合作，以拟订一个创新的因特网服务提供商网络安全自愿业务守则，并于 2010 年 12 月开始实施。该业务守则为澳大利亚因特网服务提供商提供了一个在网络安全问题方面向其顾客提供信息、教育和保护的一致性做法。澳大利亚在多边论坛上介绍了成功实施该业务守则的情况，并分享了在拟订该守则过程中得到的经验教训。在 2010 年 12 月举行的经济合作与发展组织(经合组织)信息安全工作队会议、亚洲-太平洋经济合作组织电信和信息工作组会议和亚太地区电信组织会议上都作了介绍。澳大利亚渴望通过双边能力建设活动和多边论坛与其他国家分享这一守则，以协助其他国家更好地与因特网服务提供商进行协作，并使因特网服务提供商在教育和保护终端用户时更为负责。

促进国际合作

澳大利亚将有关网络安全的国际合作列为高度优先事项。鉴于因特网的跨国性质，要实现有效的网络安全就需要开展协调的全球行动，因此，澳大利亚对国际参与采取了一种积极和多层面的方法。除其他方面外，这包括以双边方式和通过多边论坛与外国政府和组织进行联系，以帮助促进国际最佳做法、分享经验教训、建设能力，以及促进协调的全球方法来消除网络安全威胁。

澳大利亚在联合国的参与包括担任关于下列问题的各项决议的共同提案国：创造全球网络安全文化以及评估各国保护重要信息基础设施的努力，和从国际安全的角度来看信息和电信领域的发展。澳大利亚还响应大会第 64/211 号决议，就保护包括信息和通信技术在内的关键信息基础设施的最佳做法提出了自己的

意见，以促进改善全球网络安全。澳大利亚是国际电信联盟(国际电联)的成员，并向标准化和发展部门所属的研究小组作出贡献。澳大利亚向发展部门提供资金，以开展亚太区域的能力建设工作，包括网络安全举措。澳大利亚是经合组织信息安全和隐私问题工作队的积极贡献者及前任主席，目前是参与该工作队网络安全战略比较分析工作的志愿国。澳大利亚是拟订和执行《首尔-墨尔本关于亚太国家合作反垃圾邮件的协定》和作为在打击垃圾邮件方面的著名国际执法和合作网络的《伦敦行动计划》的当然领头国。

澳大利亚与其区域伙伴维持着协作关系，并致力于与他们一起工作。我们与本区域的其他国家在能力建设方面密切联系，以期实现一个可靠、有弹性和安全的网络空间。澳大利亚参与亚洲-太平洋经济合作组织电信和信息工作组的活动和东南亚国家联盟(东盟)区域论坛关于网络安全的工作。澳大利亚是亚洲-太平洋经济合作组织电信和信息工作组安全和繁荣问题指导小组的副召集国。澳大利亚目前正寻求担任东盟区域论坛工作计划下网络恐怖主义和跨国犯罪核心领域的共同牵头国。

在业务层面上，国家计算机应急小组与全球各国的国家计算机应急小组组织保持着密切的工作关系。在澳大利亚，该小组积极参与并促进在全球一级分享可靠和及时信息，包括威胁和脆弱性信息，以确保维持对态势的了解并对在线威胁作出一致和协调的全球应对。该小组积极促进能力建设举措，特别是在亚太地区，包括加入亚太计算机应急小组。该小组认识到信息安全不受地域限制，因此还通过加入事故对应和安全小组论坛和国际观察和警报网络与其他伙伴密切合作。

国际社会为加强全球一级的信息安全可能采取的措施

包括澳大利亚在内的所有国家都需继续寻找能加强信息安全的传统和创新措施。要迎接网络安全方面的全球性挑战就必须加强在多边论坛的努力，以改善可互操作网络的安全。这包括在联合国和国际电联内所作的努力，以及在类似亚洲-太平洋经济合作组织这样的区域论坛和具有更具体主题的国际小组(如事故对应和安全小组论坛和国际观察和警报网络)内所作的努力。

澳大利亚支持拟订关于网络空间负责任行为的国际原则，包括商定一套广泛的网络空间规范行为原则，以促进在网络方面进行更好的国际合作并加深信任，最终拟定商定的国际网络空间规范。澳大利亚作为国际社会的一员将继续支持通过双边和多边论坛在这一问题上取得进展，以帮助实现一个更安全、更具有弹性和更可靠的网络环境。

国际社会为加强全球一级的信息安全可作出的具体努力包括：

(a) 拟订全球标准，包括商定一套广泛的网络空间规范行为原则，以促进进行更好的国际合作并加深信任；

(b) 扩大国际法律体系打击网络犯罪的能力，包括法律框架的一致性(例如，使更多的国家加入《欧洲委员会网络犯罪问题公约》，澳大利亚预计将在 2011 年底前达到其要求)，和加强执法合作，以使各国能有效制定国内法；

(c) 发展和推广对态势认识、战略预警和事件应对方面的最佳做法，包括发展各国的国家计算机应急小组，以在各国间开展和协调这类活动；

(d) 由经验丰富和机构健全的国家采取提高认识举措和开展能力建设活动，以协助发展中国家实现一个可造福于所有人的可靠、安全和有弹性的网络空间；

(e) 采用更为一致的方法与行业结成伙伴关系，以拟订网络空间的行为导则，如澳大利亚因特网行业业务守则。

有关国际概念

现行国际法为预防来自各种行为者的信息安全威胁提供了一个保护框架。各种现行国际法原则可适用于网络空间的使用，包括各国主权平等原则和禁止使用武力和禁止侵略行为，以及国际人道主义法。需要在各国间、国际和区域论坛继续进行讨论，以更确切地确定这些原则对来源于网络领域的威胁的适用范围和适用性。

格鲁吉亚

[原件：英文]
[2011 年 6 月 1 日]

就格鲁吉亚而言，信息安全问题在 2008 年 8 月之后得到了特别重视，因为当时俄罗斯联邦对格鲁吉亚展开了猛烈的分布式拒绝服务攻击。

根据对这些事件的评估并鉴于近期正在迅速大规模发展电子政务项目和服务，因此信息安全成了国家安全概念中的一个重要方面。为改善对信息安全的监管，格鲁吉亚政府近年来一直在采取一些重大举措。

2010 年，格鲁吉亚司法部成立一个法律实体——数据交换机构，直接负责拟订和执行政府部门的信息安全政策。在成立数据交换机构之后，格鲁吉亚政府发展了可协调实现电子政务和信息安全的机构机制。

数据交换机构在法律及其《章程》规定的职能框架内与格鲁吉亚司法部合作，执行和引入符合 ISO 27000 国际标准的信息安全政策。该机构还协调执行和引入国家和企业部门信息安全所需的机制或标准，特别是开展具有各种意义的活动。在这些活动中，最重要的一项活动就是每年举行的格鲁吉亚信息技术创新会议；该会议的议程总是与信息和网络安全有关，并得到该机构授权可拟订和执行有关提高公众对信息和网络安全问题认识的政策。

就日常的网络安全问题而言，数据交换机构负责建立计算机应急小组及其运作；目前该小组在该机构之下发挥职能，管理格鲁吉亚网络空间的信息安全事件。该机构还监测格鲁吉亚政府网络的运作以保障其安全。

该机构在信息和通信技术方面的职能还包括提高专业教育水平(以培训信息安全专才)、起草建议、监测安全和发放数据签名证书。在专业教育方面，该机构计划在国际捐助方(如欧洲联盟和世界银行)的帮助下开展一些特别项目。这些项目将确保使专业教育达到适当水准。至于数字签名安全，该机构将在民事登记局开始发放公民电子身份证(印有数字签名)时履行这一职能。

除了作为信息安全牵头和协调机构的数据交换机构所开展的活动外，还应强调格鲁吉亚政府目前所采取的其他举措，而数据交换机构也积极参与了这些举措：

(a) 在格鲁吉亚国家安全委员会之下成立了负责网络安全战略和行动计划的专家工作组(将在下阶段作出具体定义)；

(b) 正在拟订一些立法倡议，包括行政法和国家保密法，计划在 2011 年提交议会。应特别提及数据交换机构现正拟订的关于“信息安全”的法案，计划在 2011 年提交议会审议；

(c) 2010 年,格鲁吉亚司法部和格鲁吉亚财政部在该机构的帮助下拟订了信息安全内部条例(政策和导则)，现正开始实施。计划在政府其他机构采取类似举措。

德国

[原件：英文]
[2011 年 6 月 6 日]

近年来网络空间的安全态势发生了根本性变化。一方面，我们可以看到技术驱动的创新过程正在发挥作用：越来越多的业务流程管理实现了电子化和相互连通，有时直接或间接连上了因特网。信息技术系统的复杂性不断加深。创新周期越来越短。另一方面，有组织犯罪和其他非国家行为者正在不停地攻击信息技术网络、数据库和网站。在某些情况下，这类攻击产生的影响尚未得到实事求是的评估。

正是出于这个原因，联邦政府在 2011 年 2 月通过了一个新的网络安全战略。该战略的核心就是保护关键基础设施。所有涉及网络安全问题的政府机关都要密切合作，并通过新设立的网络应对中心与其他机关和私营部门直接联系，以期快速侦测和分析重大信息技术事故，提出有关保护性措施的建议。至于政策，新成立的国家部长一级的网络安全委员会负责处理关键的网络安全问题和形成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。在网络空间的国际相互连通意味着必须在国际一级采取协调行动。因此，德国将在欧盟和国际组织大力倡导加强网络安全。

鉴于信息技术的全球连通性，德国在其网络安全战略中倡导拟订广泛、无争议、具有政治约束力的网络空间国家行为规范。这些规范应得到国际社会大部分成员的接受，并应包括能建立信任和增强安全的措施。

网络空间的信任和安全建设措施

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弹性及系统和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，特别是针对犯罪和恶意活动的安全性，保护那些选择使用真实性工具的人免遭身份盗窃，确保数据和网络的完整性和保密性。

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。

在此背景下，德国准备就一整套涉及网络空间内国家对国家行为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的国家的签署。

德国最近在 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)关于网络安全的会议上就这样一个关于国际规范的行为守则作了如下概述：

(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) 加强旨在建立信任、减少风险措施、透明度和稳定的合作，具体做法是：

- 交流与国际监管网络空间有关的国家战略、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故，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(如奥林匹克运动会)的网络安全支助工作拟订自愿措施。

此外，我们认为有必要就下列方面展开辩论：

在确定网络攻击的归属方面进行国际合作，因为网络攻击的归属通常很难追踪；国家对于从其领土上发动的网络攻击在得到有关这类攻击的通报之后仍不采取行动结束这类攻击所应承担的责任；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以非法手段收集的个人数据。

网络安全的军事层面

由于军队在所有指挥层级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上的信息安全。

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)和欧盟的信息安全，并为此目的制定政策和建设能力。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兴的关键性安全挑战之一。2010 年 11 月在里斯本举行的北约首脑会议上经国家元首和政府首脑通过的《战略概念》指出：“网络攻击可达到一个威胁国家和欧洲-大西洋繁荣、安全和稳定的门槛”。

国家元首和政府首脑在《首脑会议宣言》中给北约理事会规定了如下任务：“尽量利用现有的国际结构并根据对我们目前政策的审查结果，在 2011 年 6 月底前完成拟订北约深入的网络防御政策，并为执行这项政策起草一份行动计划”。

作为新政策的第一步，北约国防部长于 2011 年 3 月通过了一个网络防御概念。

该概念侧重于保护北约的网络和与北约网络相连或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。

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。在 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》把网络威胁称为这些新兴的国际威胁中的一个威胁。

德国积极参与了 2011 年 5 月 9 日至 10 日在维也纳举行的欧安组织全面应对网络安全：探索欧安组织未来作用的会议。在会议期间，讨论了有关欧安组织后续活动的具体建议。

德国将继续支持欧安组织展开讨论，以探索欧安组织在网络安全领域的未来作用。

希腊

[原件：英文]
[2011 年 6 月 6 日]

对信息安全问题的讨论比以往任何时候都更为广泛。现正考虑对目前网络和系统全球化所带来的威胁采取何种反制措施。在国家和国际上研究并采取了维护信息自由流动的措施。

目前的国际和多国概念得到追踪和研究。需要就风险评估进行国际指导。网络防御问题也应得到讨论。在全球分享信息方面应维护国家在信息安全上的主权权利。

应认识到，所有会员国都应继续向秘书长通报其对相关问题的看法和评估。在这方面，要注意以下几点：

(a) 所有信息安全相关问题都应置于高度优先地位；

(b) 跨越国家和国际边界研究和实行维护信息自由流动和规定必要程度的保密性、完整性、可用性的方法；

(c) 应在国家和国际一级起草和商定有关建设和分享能力的网络连通性概念。应推行网络连通性风险评估并提供相关国际指导。此外，由于各国一个非常严重的关切问题就是需要采取网络防御措施，因此就需要提供一致性的国际指导，以促进合作、效率和经济效益。最后但并非最不重要的是，不能忽视对国家维护其主权和维持其信息基地的要求，起草的每一个概念都应考虑到这一点；

(d) 国际社会为加强全球一级信息安全而可能采取的措施如下：

㈠ 详细阐明并商定有关国际概念；

㈡ 为统一的通用基础设施提出一个涵盖基本立法事项的指导计划，以为所有函件和短信的电子处理提供必要的信息安全，提供多种通信方式；

㈢ 应统一多国联盟和小国家集团遵循的概念，并扩大至全球一级施行。对任何设计好的复杂措施进行工程分析远不及就威胁的具体性质及其对人类的不利影响达成一致意见更为重要，因为对手也可能会利用这种分析结果；

㈣ 在进行上述所有工作的同时，应认识到，国家主权是任何全球化努力的基本参照物。应起草一个包含各种能反映所需的一体化程度假设情况的国际概念，以为国家信息交流网关提供定义，并作为在国家、多国和国际一级作出的所有努力的指南。

哈萨克斯坦

[原件：俄文]
[2011 年 6 月 7 日]

为确保信息和通信技术的网络安全，哈萨克斯坦共和国于 2010 年成立了计算机应急小组。

在这方面，从哈萨克斯坦网用户处收到的在哈萨克斯坦网域或由哈萨克斯坦服务器提供服务的网站所发现的任何有关病毒、安全代码、软件机器人系统或非法要求(色情、暴力、侵犯版权等)的信息将送交计算机应急小组进行分析。

荷兰

[原件：英文]
[2011 年 6 月 6 日]

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，支持保护一个能尊重人权的开放、自由的因特网。安全和可靠的信息和通信技术对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。

信息和通信技术提供了机会，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，以及使用信息和通信技术的用户的个人责任。

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

荷兰正在国内和国际上作出努力，以建立一个安全的数字环境。在国家一级，荷兰政府于 2011 年 2 月提出了一个题为“通过合作得到加强”的国家网络安全战略。作为该战略的组成部分，政府将成立国家网络安全委员会，以确保在公共部门、私营部门和学术研究机构之间采取协作方法。政府还将设立国家网络安全中心，以确定趋势和威胁，并帮助管理事故和危机。中心的一个主要任务是根据来自公共和私营方面的信息进行网络威胁分析。中心将包括现有的政府计算机应急小组。

在国际上，荷兰积极协助欧盟、北约、因特网治理论坛、国际电联和其他伙伴关系作出努力。荷兰促进在各网络安全中心(包括国家计算机应急小组组织)之间进行实务合作，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，荷兰意图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。

国际社会为加强全球一级的信息安全可能采取的措施

荷兰认识到，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。

荷兰认为，很有必要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，就必须在所有利益攸关方和各组织之间就知识和信息进行密集的国际交流。在施行现行国际法律框架方面的一致性是值得国际重视的另一个重要问题。

美利坚合众国

［原件：英文］
［2011 年 6 月 7 日］

一. 导言

信息和通信技术对于所有会员国的发展都至关重要。这些技术连接在一起创建了网络空间，有助于实现在 2003 年和 2005 年举行的信息社会世界首脑会议所设想的关于信息社会的共同愿景。信息和通信技术有益于日常生活的基本功能、商业及商品和服务的提供、研究、创新、创业，以及信息在个人、组织和政府之间的自由流动。这些技术是一项强大的新工具，促成电子政务，促进经济发展，便利提供人道主义援助，并使关键的民用、公共安全和国家安全基础设施发挥作用。此外，网络通信在减少国际了解和合作障碍方面所能发挥的潜在作用再怎样强调都不为过分。

尽管对信息和通信技术的依赖日益加深，但与这种依赖性相连的风险也在增加。各种天然和人为的事件和活动威胁着国家关键基础设施、全球网络的可靠运作，威胁着运行于或储存在这些设施和网络中的信息的完整性。人为威胁的数量、复杂性和严重程度都在加大。有一些是来自国家方面的，但许多来自非国家行为者，涉及犯罪或恐怖活动。动机各异，从盗窃钱财或信息、扰乱竞争对手，到民族主义和将国家冲突的传统形式延伸到网络空间，不一而足。这些威胁行为者将个人、公司、国家关键基础设施和政府都当成目标，对各个国家和全球相连的整个国际社会的福祉和安全造成了严重后果。

不管各国政府为保护其信息网络在国内采取何种国家措施，就减少信息和通信技术风险的战略进行国际协作对于确保所有国家的安全而言都必不可少。各国政府必须有信心，相信支持其国家安全和经济繁荣的网络是安全和有弹性的。实现可靠的信息和通信技术基础设施将确保所有国家都实现信息革命的潜力。

这项任务并不容易。国际社会面临的挑战是，要维护一个既能促进效率、创新、经济繁荣和自由贸易同时又能促进安全、安保、公民自由权利和隐私权的环境。这项任务的困难因信息和通信技术的独特属性而难上加难：所有人都可利用、网络通常由私营部门而不是由政府拥有和营运。与传统武器不同的是，破坏性的信息技术工具是隐形的，无法看见的。对这类工具的使用可穿越许多国家，很难

确定其起始点、身份和肇事者的赞助方。非国家行为者正不断发展能力，使国家或非国家行为者越来越有可能利用代理人参与网络空间的破坏活动。这些属性使传统战略，如类似用于军控的措施，失去控制或遏制威胁行为者的效力；因此，需要采用创造性的新方法来减少风险。尽管任务艰巨，但会员国仍须团结在共同目标之下，通过保障信息技术的安全和完整性来维护和加强信息技术可以作出的贡献。

会员国的任务有两个方面：国内的和国际的。确保国家信息基础设施的安全是政府在国内与有关民间社会利益攸关方协调下必须领头担负的责任。同时，国内的努力应得到在为解决对网络化信息系统的各种威胁的跨国性质而制定的战略方面的国际协作的支持。这些努力应包括关于事故管理、减少和应对、跨国犯罪调查和起诉方面的合作；关于改善网络基础设施稳健性的技术建议；以及确认国际共享的行为规范，同时采取旨在加强稳定和减少误解风险的建立信任措施。

二. 威胁、风险、脆弱性

针对构成网络空间的系统网络和在网络空间中运行的信息的威胁是 21 世纪严重的全球挑战之一。国家和非国家行为者可通过信息和通信技术把普通公民、商业、关键工业基础设施和政府当作目标。信息和通信技术、因特网及其他基础设施的会集创造了前所未有的可使电信、电力、油管和炼油厂、金融网络和其他关键基础设施瘫痪的机会。

信息技术的独特特点便利将其用于破坏活动，严重挑战力求减少风险的各国政府。与传统军事技术不同，构成网络空间的网络不是由政府垄断的，在许多情况下是由私营部门拥有和运营的。信息技术本身是广泛可用的技术，不具有固有的民用或军用性质，如何使用这类技术完全取决于使用者的动机。

所有人都可免费获得可用于破坏的软件工具，至少可获得基础工具。只要掌握必要技能，任何人都可以开发更为复杂的方法。此外，这些工具变化迅速，可利用新发现的脆弱性。这类工具在传统意义上是看不见的，相当隐秘，可能带有易于模仿的隐性“签名”。由于因特网的性质，恶意代码在到达其目标之前可越过许多国家的领土，从而使确认其始发点的工作变得极为繁重、费时，往往需要大量跨国合作。即使发现了始发点，肇事者或赞助者的身份仍可能无迹可寻。因此，恶意行为者可以而且几乎正从地球任何地方进行秘密运作，并在很大程度上可逃脱惩罚。

身份的模糊性因网络入侵动机的模糊性而变得更为复杂。有组织的犯罪分子和其他个人或团体可能为促进自身的利益而采取行动，但也有可能被国家和非国家行为者招募作为代理人。缺乏及时的高可信属性和哄骗的可能性可能对政府造成不确定性和混乱，从而加大在重大网络事故中危机不稳定性、误导反应和丧失升级控制的潜在可能。

对网络空间的可靠运作构成威胁的主要行为者包括：

(a) **犯罪分子**。很多恶意工具起源于有组织的犯罪分子和黑客所作的创业努力。犯罪活动的复杂性和范围日益加大，突显了网络空间恶意活动在影响国家竞争力、导致普遍减弱对因特网用于商业和贸易的信心，甚至致使民用基础设施瘫痪方面所具有的潜力。这些活动的数量和范围都在不断加大。

(b) **国家**。有越来越多的传闻性公开报道，说国家正在发展和利用将国家冲突传统形式延伸至、利用或通过网络空间的能力。但是，有关在普遍认为是国家赞助的事件背后的来源或意图的确凿证据仍然无处可寻。通常的情况是，只能从涉及某一事件的目标、效果和其他旁证来推断肇事者的身份和动机。

(c) **恐怖分子**。恐怖分子目前尚不具有破坏信息网络或通过使用信息和通信技术实施具有物理效应的作业的能力，但不能排除今后出现这种能力的可能性。大多数专家认为，恐怖分子目前依赖信息和通信技术来招募人员、进行组织活动和筹集资金。因恐怖分子利用因特网而产生的具体威胁可能包括利用因特网来组织和展开具体的动能恐怖攻击。

(d) **代理人**。让人越来越感到关切的是出于金钱利益或民族主义或其他政治动机而代表其他人，不管是国家还是非国家行为者，从事在线恶意活动的个人或团体。据报告，“软件机器人大师”可向出价最高的人提供各种恶意服务。信息技术的独特属性向这类行为者提供了高度的匿名性，有效地掩盖了与赞助者的任何关系，使赞助者可作出听起来可信的否认。

国家在应对这类威胁时所面临的挑战很艰巨。信息和通信技术的属性意味着，这些威胁行为者的每一个行动可能只能从其效果中才能看到。因此，无法及时得到肇事者的高可信身份属性(如果有的话)，是否能成功往往依赖高度的跨国合作。代理人的作用越来越大使分析属性的程序进一步复杂化，因为受害方不仅必须确认肇事者，而且还必须确认赞助者，这就使得这一挑战在今后变得更为麻烦。

要迎接这类挑战，各国政府就需要在国内组织和领头作出努力，为通信和信息基础设施发展和部署具有弹性的分层防御，而不管威胁的来源在何方。同时，这些威胁的复杂跨国性使国际协作成为必要，以便在全球基础上实施解决各种风险的战略。

三. 行为原则、规则和规范

A. 国家在保证网络安全方面的责任

过去 10 年中，会员国已经认识到本国有责任在国内采取系统性步骤，保护自己免受网络安全威胁，并确认有必要进行国际合作。联合国大会有 5 项决议提请注意各国政府可采取用于减少其安全风险的基本防御措施。虽然这些决议的目

的是为了提高认识，但同时也为了网络安全而推动一些涉及个人和国家行为的有用规范：

(a) 大会在关于打击非法滥用信息技术的第 55/63(2000)号决议中强调，需要有现代化的有效国家法律来充分起诉网络犯罪并促进及时进行跨国调查合作；

(b) 大会在第 56/121 号决议中特别提及国际和区域组织在打击高技术犯罪方面的工作，包括欧洲委员会在拟订《网络犯罪问题公约》方面的工作：

联合国和其他组织一直在该领域展开密集活动。关注非法滥用因特网问题的联合国主要组织包括联合国毒品和犯罪问题办公室、预防犯罪和刑事司法委员会、联合国预防犯罪和刑事司法大会、国际电信联盟和其他组织；

(c) 大会在第 57/239 号决议中确认需要创造全球网络安全文化，认识到政府有责任领导社会所有组成部分了解各自在网络安全方面的作用和责任，并强调指出信息社会所有参与者都必须解决的互补性要素；

(d) 大会在第 58/199 号决议中特别强调会员国在为创造全球网络安全文化和保护关键信息基础设施所作努力时应考虑的行动。可将这些行动视作政府应采用的一整套规范，这些规范为促进国际协作减少风险提供了基本基础或前提；

(e) 大会在第 64/211 号决议中邀请所有会员国利用所附的自我评估工具详细评估本国至今在上述领域及其他领域所作的努力，并分享那些可协助其他会员国作出努力的成功措施和最佳做法。

B. 在敌对行动情况下可适用的规范

尽管信息和通信技术的属性独特，但仍可以现行的国际法原则作为适当框架来确定和分析应用于制约敌对行动情况下网络空间使用的规则和规范。在这方面可考虑两个不同但相关的法律体系：*诉诸战争权和战时法*。前面一个体系提供的框架可用于考虑在网络空间发生的事件是否上升为可触发一国采用自卫权的武力使用水平。后一个体系提供的框架可用于确定应用于制约武装冲突情况下网络空间使用的规则。

诉诸战争法。制约使用武力和自卫的法律框架的大部分内容来源于《联合国宪章》的三项规定：

(a) 《宪章》第二条第四款规定：“各会员国在其国际关系上不得使用威胁或武力……，侵害任何…国家之领土完整或政治独立”；

(b) 《宪章》第三十九条将安全理事会定为仲裁者，负责断定是否发生了威胁和平、破坏和平的情况或侵略行为，并要安全理事会提出建议或作出决定，以根据《宪章》第四十一条和第四十二条采取适当的对应措施；

(c) 《宪章》第五十一条认可并加强了如下原则：“联合国任何会员国受武力攻击时，在安全理事会采取必要办法，以维持国际和平及安全以前，本宪章不得认为禁止行使单独或集体自卫之自然权利。”

要就一项在网络空间发生的破坏活动是否构成可触发自卫权的武装攻击达成一个明确的法律结论可能会很困难。例如，当威胁行为者和动机不明、作用的结果也未直接造成大量死亡或实际破坏时，有可能会对是否发生了武装攻击作出不同的结论。但是，这种模糊不清和出现分歧的可能性并不意味着需要拟订一个专用于网络空间的新的法律框架。相反，它们只反映出在施行《宪章》时所出现的挑战，而这类挑战在许多情况下早已存在。然而，在某些情况下，在网络空间发生的一项破坏活动可能构成武装攻击。在这种情况下，应适用以下既定原则：

(a) 对迫在眉睫或实际发生的武装攻击应用自卫权，不管攻击者是国家行为者还是非国家行为者；

(b) 自卫时的武力使用必须限于为解决迫在眉睫或实际发生的武装攻击所必需的，并必须与所面临的威胁相对称；

(c) 各国需采取一切必要措施，确保其领土不被其他国家或非国家行为者用于针对另外国家及其利益的武装活动的目的，包括策划、威胁、实施或为武装攻击提供物资支持。

战时法。武装冲突法规定了适用于进行武装冲突的规则，即战时法，包括在武装冲突情况下信息技术工具的使用。特别是，武装冲突法的下列关键原则在判断武装冲突时网络攻击的合法性方面发挥重要作用：

(a) 区分原则要求将攻击局限于合理的军事目标，民用物体不应成为攻击对象；

(b) 对胡乱攻击的禁止包括禁止实施采用无法合理指向特定军事目标的作战手段或方法的攻击；

(c) 对称性原则禁止实施预期可能造成平民生命附带损失、平民受伤害或民用物体受破坏并在程度上超过所预期的具体和直接军事优势的攻击。

这些原则禁止攻击纯粹的民用基础设施，因为干扰或摧毁这些设施并不会带来有意义的军事优势。此外，在攻击一个军事目标之前必须评估附带损害的潜在性。换句话说，对信息技术攻击也必须做目标设定分析，就像传统上为使用动能(常规和战略)武器的攻击所作的分析一样。

虽然上述原则已确立并适用于网络空间的情况，但在网络空间活动的情况下解释这些法律体系确实会出现新的独特挑战，需要在各国间进行协商与合作。这并非不寻常。当新技术得到开发时，它们经常给现行法律体系的应用带来挑战。

C. 代理人的使用

信息和通信技术的独特属性给各国带来了新的挑战，使用代理人从事破坏行动就是其中一个例子。通过代理人采取行动极大地提高了国家参与攻击而又可听起来可信地进行否认的能力。虽然现行国际法有关于使用雇佣军的规定，但是在网络空间使用代理人的做法引起了具有广泛影响的新的重大问题。各国需要共同努力，制订解决该问题的有效方法。

D. 允许信息自由流动的责任

有关言论自由和信息自由流动的权利载于《世界人权宣言》和《公民及政治权利国际公约》；这些权利普遍规定，除受某些限制外，每个人都有言论自由的权利，包括不受干扰地保持看法的自由，以及通过任何媒介和超越国界寻找、接收和传授信息的自由。这些原则已在众多的国际论坛上得到确认，包括大会、国际电信联盟和信息社会世界首脑会议等。

E. 打击恐怖主义的责任

现在至少有 16 项安全理事会决议呼吁各国打击恐怖主义。这些义务全面适用于恐怖分子或恐怖主义协助者利用网络空间招募人员、筹资、转移资金、购买武器或策划攻击的情况。所有国家都有义务在尊重其他国家主权及本国在允许信息自由流动方面的责任的情况下，分享有关在线恐怖主义融资、招募人员、策划和协助活动的信息，并采取应对行动。

四. 透明性、稳定和减少风险及合作措施

正如上文所概述的，会员国面临着管理一个高度多样化和复杂的威胁环境的挑战。过去 10 年中，国际上展开了打击网络犯罪威胁的广泛努力。美洲国家组织、亚洲-太平洋经济合作组织、西非国家经济共同体、非洲联盟和欧洲委员会等展开了调查和起诉网络犯罪方面的培训工作。通过《网络犯罪问题公约》及通过受害国之间的双边努力，在调查和起诉网络犯罪方面实现了广泛的国际合作；在应对犯罪活动对信息和通信技术的威胁时，国际合作仍然是最有效的方法。

受到跨国关切的其他领域亦须得到类似的关注。这些领域包括因对与国家在网络空间的行为有关的国际规范缺乏共同理解而出现误解的风险，这将影响出现重大网络事件时的危机管理工作。这就需要拟订措施，以加强合作和建立信任，减少风险或加强透明性和稳定：

透明性措施

- 交流国家网络安全战略和最佳做法(已获得的经验教训)
- 交流国家对关于使用网络空间的国际规范的看法
- 交流专门负责网络安全的国家组织结构和联络点

稳定和减少风险措施

- 建立或更新通信链及相关协议，以纳入网络事件
- 加强合作以应对有组织的非国家行为者(罪犯、恐怖分子、代理人)
- 建立程序，以允许在国家计算机安全事件应对小组之间进行日常信息交流

合作措施

- 支持在较不发达国家进行网络安全方面的能力建设。