国　　际　　电　　信　　联　　盟

第22/1号课题

最后报告

ITU-D　　第1研究组　　第4研究期(2006-2010)

第22/1号课题:

保证信息和通信网络的安全:培育网络安全文化的最佳做法

ITU-D 研究组

2006 年世界电信发展大会（WTDC-06）根据第 2 号决议（2006 年，多哈），保留了两个研究组，并为它们确定了研究课题。WTDC-06 通过的第 1 号决议（2006 年，多哈）规定了研究组应遵循的工作程序。在 2006-2010 年期间，第 1 研究组受托开展电信发展战略和政策领域九个课题的研究工作。第 2 研究组受托开展电信业务及网络和信息通信技术应用的研发与管理领域十个课题的研究工作。

欲了解更多信息

请联系:

Souheil MARINE 先生/Christine SUND 女士
国际电联
电信发展局 (BDT)
Place des Nations
CH-1211 GENEVA 20
Switzerland
电话： +41 22 730 5323/ 5203
传真： +41 22 730 5484
电子邮件： souheil.marine@itu.int
christine.sund@itu.int

订阅国际电联出版物

敬请注意：我们不接受电话订购，因此请通过传真或电子邮件方式订购出版物。

ITU
Sales Service
Place des Nations
CH-1211 GENEVA 20
Switzerland
传真： +41 22 730 5194
电子邮件： sales@itu.int

国际电联电子书店：www.itu.int/publications

国 际 电 信 联 盟

第22/1号课题

最后报告

ITU-D 第1研究组 第4研究期 (2006-2010)

第22/1号课题:

保证信息和通信网络的安全:培育网络安全文化的最佳做法

免责声明

本报告是由来自不同主管部门和组织的众多志愿人员编写的。文中提到了某些公司或产品，但这并不意味着它们得到了国际电联的认可或推崇。文中表述的仅为作者的意见，与国际电联无关。

目录

页码

第22/1号课题

引言

本报告向各国主管部门概述介绍在国家层面处理网络安全问题所需的基本要素[1]并论及如何开展国家网络安全工作。鉴于各国现有应对能力各异且对网络安全的威胁不断变化，本报告并不能提供一个确保网络安全的良方，报告的框架只是介绍了一种可以灵活应用的方法，以帮助各国主管部门审议并改进现有的网络安全机制、政策和关系。尽管本报告的重心是网络安全，但我们注意到，保护有形网络也同样重要。我们也注意到网络安全的最佳做法，必须保护和尊重《世界人权宣言》和《日内瓦原则宣言》相关部分中有关隐私和言论自由的条款。[2]

本报告的主要组成部分有：

- 制定国家网络安全策略；
- 在各国政府和私营部门之间开展合作；
- 遏制网络犯罪；
- 创建国家级事件管理能力；并
- 宣传国家网络安全文化。

以上每一个主要组成部分均应是国家网络安全综合方案的一部分。这些组成部分的出现次序并不表示某项要素的重要性要高于其它要素。根据各国国情还可能有其它要素。

在本报告中，ITU-T X.1205建议书定义的**网络安全**，指的是可用于保护网络环境以及各组织和用户资产的工具、政策、安全概念、安全措施、指南、风险管理方法、行动、培训、最佳做法、保证和技术的一系列内容。组织的资产和用户资产包括网络环境中互相连接的计算设备、人员、基础设施、应用、业务、电信系统以及传输和/或存储的信息。网络安全致力于确保实现和维持各组织和用户的安全特性，不受网络环境中相关安全风险的威胁。一般的安全目标包括以下要素：

- 可用性
- 完整性，可能包括真实性和不可否认性
- 保密性

理解网络安全、关键基础设施（CI）、关键信息基础设施（CII）、关键信息基础设施保护（CIIP）和非关键基础设施之间的关系是重要的。图1说明了该种关系。

---

[1] 读者如感兴趣可查阅ISO 27001至27003的输出成果。

[2] 参见WSIS，《信息社会突尼斯议程》第42段。

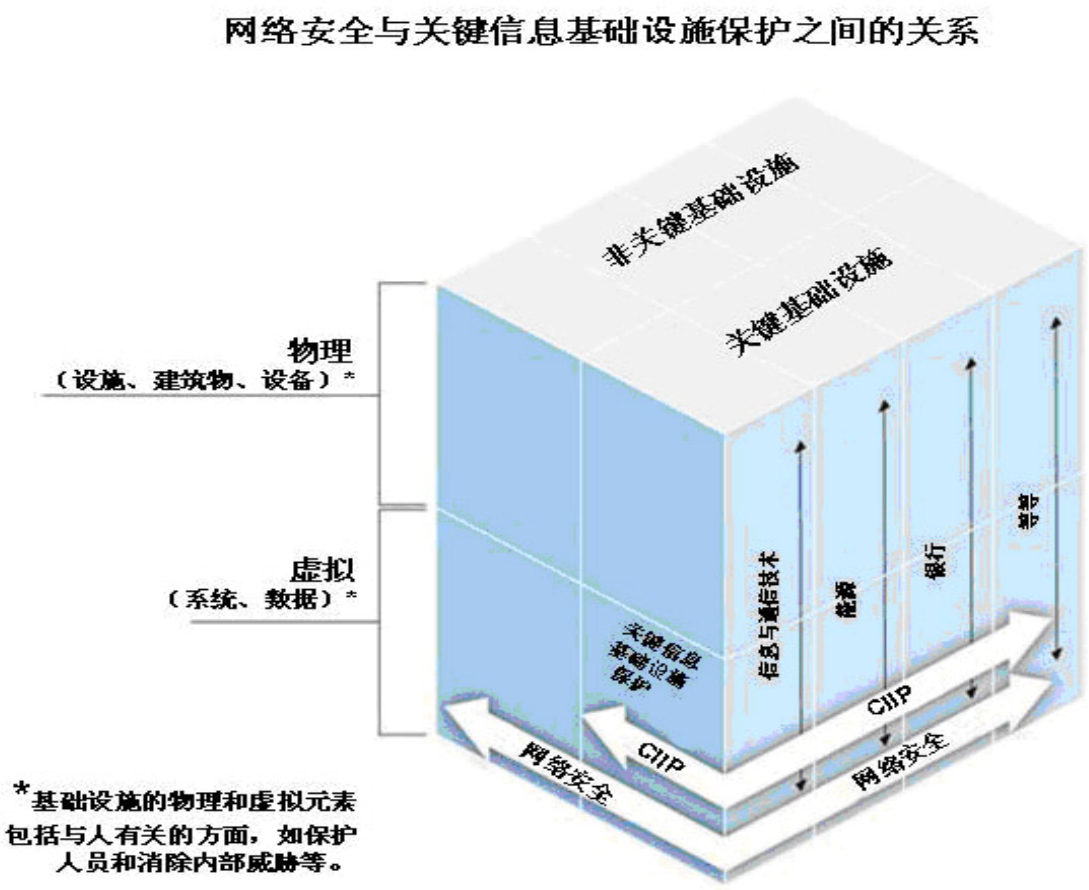
尽管定义可能略有不同，通常认为**关键基础设施**（CI）指那些受到中断或破坏即会削弱公共健康与安全、商业和国家安全或这些事项的多个组合的关键系统、业务和功能。CI既包括物理元素（如设施和建筑），也包括虚拟元素（如系统和数据）（见图1）。什么是“关键的”，各个国家可能理解不一，但通常包括信息通信技术（包括电信）（ICT）、能源、银行、运输、公共卫生、农业和食品、水、化学药品、航运等元素以及主要的政府服务部门。处于各个发展阶段的国家需要规划和制订保护其认为是“关键基础设施”（即关键基础设施保护，包括物理和虚拟保护）的政策，以确保获得合理程度的恢复能力和安全，支持国家使命和经济稳定。

这些经济部门都有自己的有形资产，例如银行建筑、发电厂、火车、医院和政府办公室。但是，国家经济的这些关键部门全部依赖于信息和通信技术。总体来看，这些部门及其有形资产如今都依赖于这种**关键信息基础设施**（CII）的可靠工作来提供服务并开展业务。因此，对CII的严重破坏会立即产生不利影响，其范围远远超出ICT行业，危及国家在多个行业实现其根本使命的能力。**对信息基础设施的关键保护**（CIIP）项目对CII的虚拟元素部分进行保护。

如图1所示，CIIP是CIP和网络安全的子集。网络安全通过加强各关键部门所依赖的关键信息基础设施的安全，并保障为用户的日常需要提供服务的网络和业务，来保护网络免受各种形式网络事件的影响。网络事件既会影响关键信息基础设施，也会影响非关键基础设施，并以多种恶意行为的形式表现出来 ，如通过僵尸网络开展拒绝服务攻击和散布垃圾信息和恶意软件（即病毒和蠕虫），以此影响网络运行能力。此外，网络事件也可能包括诸如“网页仿冒”、“网址嫁接”以及“身份盗窃”等非法行为。随着采用的工具和技术越来越随处可得，网络威胁持续增长，网络罪犯的技术能力和复杂程度不断增强。处于各种发展阶段的国家都经历了这些网络事件。

国家的网络安全策略包括提高对现有网络风险的认识、创建处理网络安全问题的国家架构、确立必要的、可用于处理已发生事件的关系。评估风险、实施缓解措施、控制结果也是一个国家网络安全计划的组成部分。良好的国家网络安全计划可通过有益于跨部门的持续规划，保护存储在信息系统中的信息，维持公众信心，维护国家安全、保障公众健康和安全，以此协助保护国家经济免受破坏。

图 1：关键信息基础设施保护与网络安全的概念关系



尽管在国家战略层面提高网络安全性十分重要，但信息社会世界峰会（WSIS）2003-2005年两阶段的相关成果，基于《日内瓦原则宣言》第35和36段及《突尼斯议程》第39段对C5行动方面进行的跟进，以及落实国际电联通过的信息社会世界峰会相关决议、行动和举措输出成果，均呼吁应在区域和国际战略上为其提供补充。例如：

a) 全权代表大会第71号决议（2006年，安塔利亚，修订版）《国际电联2008-2011年战略规划》的目标4；

b) 全权代表大会第130号决议（2006年，安塔利亚，修订版）《加强国际电联在树立使用信息通信技术的信心和提高安全性方面的作用》；

c) 2006年世界电信发展大会（WTDC-06）《多哈行动计划》的相关部分，其中包括将网络安全确定为电信发展局工作重点的“项目3：信息通信战略和信息通信技术（ICT）应用”。该项目的各项活动业已确定，特别是通过了名为“关于加强在网络安全、打击垃圾信息等领域合作的机制”的第45号决议（2006年，多哈）。第45号决议责成电信发展局主任召开会议讨论增强网络安全性的方法，其中包括，在相关成员国间增强网络安全性和打击垃圾信息的谅解备忘录，并将这些会议的研究成果上报2006年全权代表大会。电信发展局向2006年全权代表大会提交的报告可通过下述网站获取：http://www.itu.int/md/S06-PP-C-0024/en[3]。

d) ITU-T第17领导研究组有关网络安全的广泛工作和第13研究组的补充活动；

e) 最近世界电信标准化全会（2008年，约翰内斯堡）通过的第58号决议 – “重点鼓励发展中国家建立国家计算机事件响应组织（CIRT）”对ITU-D部门第22.1号课题下开展的工作表示认可；

f) 高级专家组（HLEG）针对秘书长于2007年5月17日发起的《全球网络安全议程》提交的报告总结了专家对此举措内包括的七项主要战略目标提出的建议，侧重于下述五个工作方面的相关建议：

- 法律措施
- 技术和程序措施
- 组织结构
- 能力建设
- 国际合作

在这些方面中“法律措施”着重如何以一种国际通用的方式处理ICT网络犯罪活动带来的法律挑战。“技术和程序措施”致力于采用关键措施，促进采用先进的方法提高网络空间的安全和风险管理，包括使用认证机制、协议和标准。“组织结构”的重点是防止、检测网络攻击对网络攻击做出响应并进行危机管理。“能力建设”致力于制定能力建设机制战略，以提高意识、传授技能并提高网络安全在国际政策议程中的地位。最后，“国际合作”的工作重点是为应对网络威胁，开展国际合作、对话与协调。[4、5]

g) 2009年世界电信政策论坛（WTPF）通过的关于“树立使用ICT的信心和提高安全性的协作战略”的4号意见最新草案[6]，特别注意请国际电联和请成员国的部分。

h) 电信发展局开展的项目3（电子应用）的活动包括向成员国中的发展中国家提供直接援助、通过项目和能力建设/国际电联国家网络安全/CIIP自我评估工具，国际电联僵尸网络问题缓解工具包和建立国家CIRT的工具包。

i) 2008年11月启动的保护在线儿童（COP）举措是国际行动的协作网络，与联合国其他机构和合作伙伴共同提供网上安全行为指导，以促进全球儿童和青少年的在线保护。COP举措的主要目标是：1) 确定对儿童和青少年而言，网络空间的主要风险和漏洞；2) 通过多种渠道形成对这些风险和问题的认识；3) 制定切实可行的工具，帮助各国政府、组织和教育机构尽量减少风险，4) 分享知识和经验，同时促进国际战略伙伴关系，以确定和落实具体措施。

---

[3] 根据过去四年的经验阿拉伯国家更加坚信，各成员国通过签订谅解备忘录（MoU）加强网络安全和打击垃圾信息是满足全球和/或区域需求的最佳方案。

[4] 来自阿拉伯国家的专家支持HLEG主席报告中的所有建议。

[5] HLEG主席报告详情见：http://www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf

[6] WTPF 4号意见草案全文见：http://www.itu.int/osg/csd/wtpf/wtpf2009/documents/opinion4.pdf

j) 国际电联和国际打击网络威胁多边伙伴关系（IMPACT）已在国际电联全球网络安全议程框架下建立协作，目的是将来自政府、私营部门公司和学术界的主要利益攸关方和合作伙伴联系起来共同向国际电联成员国提供专业知识、设施和资源，以有效地应对网络威胁。国际电联 – IMPACT协作的主要目标是：1) 制定跟踪、预警和事件响应全球框架；2) 确立适当的国家和区域组织结构和政策，如国家计算机事件响应组（CIRT）；3) 促进跨部门的人力和机构能力建设；以及4) 促进全球利益攸关多方的国际合作。

第一部分

制定国家网络安全战略并寻求达成共识

制订与实施国家网络安全规划需要全面的战略，该战略包括对国家现行做法进行广泛的初步审议，并考虑所有利益攸关方（政府机构、私营部门和公民）在此过程中所扮演的角色。

出于国家安全和经济发展的原因，政府需能实现、促进和保证其对关键信息基础设施的保护。如今，信息基础设施跨越了一个国家的不同工业部门，也超越了国界的限制。关键信息基础设施的无所不在创造了无数的机遇与经济优势。

伴随着这些好处，代价高昂的相互依赖与风险也接踵而来。国际电联电信发展局（BDT）委托进行的研究对这些代价做了如下归纳[7]：

> 在信息业务的整个价值网络中，包括软件销售商、网络运营商、互联网业务供应商和用户，均受到恶意软件和垃圾信息的影响。这些影响包括但不限于：预防措施成本、纠错成本、宽带和设备的直接成本以及拥塞的机会成本。垃圾信息和恶意软件还创造了合法和非法的新的收入流，从而使情况变得更加复杂了。它们推动了合法的业务模式（例如，防病毒、防垃圾信息产品、基础设施和带宽），也推动了违法的业务模式（出租僵尸网络、委托进行基于垃圾信息的销售、基于垃圾信息的炒股诈骗等）。因此，它们对利益攸关方产生了混合的、有时是相互冲突的激励因素，从而导致对这个问题的一致响应复杂化。

多年来，很多国家一直将公用交换电话网（PSTN）视为关键基础设施并为其提供相应保护。许多国家的PSTN基础设施资源大部分归商业公司所有，它们相互或与政府合作对网络加以保护。然而，在互连互通的有线和无线网络中基于数字的信息和通信技术（ICT）迅速崛起，急剧改变了网络安全的性质和要求，从而导致传统的基于PSTN的安全政策和程序已不足以满足对此类安全的新要求。

ICT引发诸多变数，因此开发、拥有、提供、管理、服务和使用信息系统和网络的政府、企业、其它组织和个人用户之间开展合作应引起更多重视。虽然政府一如既往地在网络安全方面发挥领导作用，但亦有必要确保包括基础设施运营商和销售商在内的其它相关利益攸关方被囊括在整个规划和决策过程中。通过共同合作，政府和私营部门可以有效发挥各自的专长并管控CII风险。这种整合增加了信任并可确保以恰当和最有效的方式制订和应用政策与技术。在国际层面，保护关键信息基础设施和提高网络安全则要求国与国之间并与国际合作伙伴进行合作和协调。

I.A 本部分涉及的目标概览

I.A.1 在国家政策层面树立有关网络安全问题和国家行动与国际合作必要性的意识，

I.A.2 制定提高网络安全以降低网络和物理破坏风险和效应的国家战略，

I.A.3 在国际层面参与促进事件的预防、筹备、响应和恢复等国家行动。

---

[7] 参见ITU-D文件1/144（2008年5月6日）研究草案“网络安全性的经济方面：恶意软件和垃圾信息”。

I.B 实现上述目标的具体步骤

以上是各国的共同目标；然而实现这些目标的具体步骤因各国特定需求和环境不一而有所差别。在很多国家，国家政府将采取下列步骤。

I.B.1 敦促各国政府中的领导人，有必要通过开展政策讨论，采取国家行动来解决国家网络基础设施所面临的威胁和弱点问题。

1) 一国欲提高网络安全并确保本国关键信息基础设施的安全，第一步便是将网络安全定为国策。一般而言，国家的网络安全政策声明 1) 承认CII对国家的重要性，2) 确定其面临的风险（通常为一项全方位灾害防治方案[8]，3) 确立网络安全政策目标，并 4) 全面确定该方案如何实施，包括与相关利益攸关方合作。

一旦全面的网络安全政策已明确定义，可通过国家战略的方式将其广为周知。该战略描述各方的角色和责任，设定优先级别并确定实施的时限和步骤。此外，政策和战略也可将国家的精力集中于其它的国际网络安全活动中去。为制订一个全面的网络安全政策，有必要加强关键决策者对这些事项的意识。决策者应当理解，实现各方一致认可的网络安全目标需要较长的时间。

2) 国家网络安全框架不应是一成不变的政策。相反，该框架和政策应灵活，并可响应动态的风险环境。该框架应建立政策目标。通过建立明确的政策目标，政府机构和非政府组织可共同工作，以最有效的方式达成设定的目标。

3) 应通过与所有相关参与方的代表合作磋商制定国家政策，这些参与方包括政府机构、私营部门、学术界及相关协会等。该政策应在国家层面（最好由政府首脑）颁布。

I.B.2 指定一名牵头人和牵头机构负责整体的国家行动；确定在政府内部的部门建立计算机安全事件响应组织（CSIRT）[9]，承担国家层面的责任[10]；针对国家战略各个方面指定牵头机构。

1) 启动网络安全举措需要在初期指定某个人领导国家网络安全方面的活动，该牵头人应为政府负责政策层面工作的代表，了解网络安全问题且能够指导和协调政府机构的力量并能有效与私营部门互动。牵头人的理想人选应活跃于政坛并能够接触到政府首脑。这样的高层权威对于保证各实体协同工作而言必不可少，目前这些实体之间可能互动。这有助于逐渐形成一个制度基础，而后国家网络安全技术带头人和组织在其上添砖加瓦。

2) 一旦国家推出网络安全举措，启动这一举措的个人或机构便可卸下这一职责。

3) 必须确定负责制定和实施国家安全政策其它方面的机构。

I.B.3 在政府机构和私营部门内部指定称职的专家和决策者，划分他们的职责。

1) 有效的国家行动需要在所有参与方中树立“网络安全文化”意识。开发、拥有、提供、管理、服务和使用信息系统和网络的个人和组织，无论是否隶属于政府，必须了解各自应发挥的作用以及需要采取的行动。资深的决策者和私营部门领导人必须为各自机构确定目标和重点工作。资深技术专家必须提供行动方针和框架。

I.B.4 为参与方及参与方之间确立合作安排。

---

[8] 全方位灾害或多方位灾害风险管理方案包括考虑所有潜在的自然和技术灾害；这包括自然和人为的（意外的或有意的）紧急情况和灾害。

[9] CSIRT指一组IT安全专家，其主要职责是响应计算机安全事件。该团队提供处理这些事件的必要服务并协助其委托人从破坏事件中恢复（《如何一步一步建立计算机安全事件响应团队》可参见http://www.enisa.europa.eu/act/cert）。CSIRTS有时也称为“计算机紧急响应组织”（CERT）。CSIRTS和CERT执行的是同样的功能。CSIRT中“计算机”一词在本报告中的含义包括路由器、服务器、IP移动设备和相关应用等。

[10] 本报告中，一个在国家层面指定的CSIRT称为“CIRT”。

1) 国家政府应确立官方和非官方的合作安排，允许并提倡私营部门和政府间的交流和信息共享。应由广泛的机构在技术或运营层面实施网络安全。这些工作还应加以协调，其中包括建立信息共享的机制。

I.B.5 在国家层面建立政府和私营部门实体的合作机制。

1) 制定政策以及编制和实施国家计划应采用公开和透明的形式。这些工作必须考虑各参与方的意见和利益。

I.B.6 为本地参与方指定国际对口单位，鼓励国际范围内处理网络安全问题的行动，包括信息共享和协助工作，同时考虑到实施WTDC-06第45号决议的项目的结果。

1) 加强国家网络安全的工作可借助于参加区域或国际论坛，这些论坛常以会议和讲习班的形式提供教育和培训。此类论坛将普及对问题的意识，邀请专家发言并允许各国介绍各自的观点、经验和计划。参与和/或加入目标一致的区域以及国际组织将有助于此类工作的开展。这也是第45号决议项目的目标之一。

2) 参与多边组织现有计划和活动,寻求改进和加强全球网络安全是另一种加强国际合作的方式。多边组织如国际电信联盟(信息社会世界峰会行动方面C5)，经济合作与发展组织（OECD），美洲国家组织（OAS）和亚太经济合作组织（APEC）等。此外，还有各国政府可以交流网络安全信息的其它会议，如国际子午线会议（Meridian Conference）等。

3) 此外，还应参与私营部门领导的活动，如“反网络钓鱼工作组”以及其它类似的国际活动。

I.B.7 为确定网络安全保护工作及其工作重点，建立综合风险管理流程。

1) 只有在了解风险的基础上，政府、基础设施所有者和运营商（包括为其提供支持的销售商）方可在公共机构 – 私营企业 – 民间开展合作，确定并突出需要保护的关键功能和要素。一旦确定之后，便可区分重点的关键信息基础设施功能，并按照重要性及其具体情况进行排序。应当牢记，“关键性”有赖于具体情况，某些情况下的关键功能在另一情况下可能并非关键。在各国确定和划分关键功能时，不能忘记关键性将随技术、基础设施和程序的改进而变化。

2) 保护CII和网络空间殊非易事。CII和网络空间的保护及其中包含的关键功能涉及到应用一系列风险管理做法（即评估威胁、弱点和结果，确定控制和缓解措施，实施控制措施并测量措施的有效性），使得运营商可以管理风险并确保其关键业务的恢复能力。鉴于其提供业务的实时性，每个信息基础设施提供商通常都备有复杂的风险管理方法和措施。但是，信息基础设施的互连、相互依赖和技术复杂程度限制了轻易评估整体风险或就绪的能力。结果，调节公共-私营部门的协作可以很好地评估共享的依赖和基础设施风险（自然灾害、技术故障、恐怖攻击等）。

I.B.8 评估和定期复评现有网络安全工作的状态并制定项目的优先程度。

1) 国家网络安全战略应包括一项国家评估调查，将其用作已取得进展的自我评估或作为培训或支持评估工作的一部分。通过采用一种通用的自我评估工具，各国可确定其国家框架的优势和潜在差距，并根据预定的目标建立对其进行调整的流程（电信发展局已制定自我评估工具 – 国际电联国家网络安全/CIIP自我评估工具，配合本最佳做法文件）。

I.B.9 确定培训要求及如何实现这些要求。

1) 通过将本报告推荐的最佳做法与本国目前网络安全保障工作进行对比（即进行差异分析），一个国家可发现其网络安全项目尚需改进的方面。解决方案可以从技术（例如新设备或软件）、法律（例如起草新法律或法规，纠正不当网络行为）或从组织方面着手。通过差异分析还可能发现需要加强能力建设（培训）的地方。

第二部分

建立国家政府和私营部门的合作关系

保护重要信息基础设施和网络空间是一项共同的责任，只有拥有和运行大量基础设施的各级政府和私营部门开展合作才能完成。当然，政府在所有国家决定上必须拥有最终决定权。必须认识到，尽管世界信息安全系统已大体变成了一个具有互操作性的互连整体，这一网络的结构会因国家的不同而大相径庭。因此，这些系统的所有者和运营商之间的合作，将提高这一安全系统的有效性和可持续性。

确保基础设施具有恢复能力是政府和私营部门的长久利益所在，政府私营部门合作伙伴关系对于加强网络安全至关重要，因为没有任何一个实体能够单枪匹马保护整个基础设施。鉴于在很多国家，私营部门拥有并运行着大量网络基础设施，因此建议政府和私营部门各司其职，开展富有成效的合作。成功的公共 – 私营部门合作需要三大要素：1) 清晰的价值定位；2) 明确划定的作用与职责和 3) 信任。

价值定位

成功的伙伴关系取决于向政府和私营部门合作伙伴阐明合作会使双方受益。政府通常能够在自己力所不及的领域，得益于基础设施厂家和运营商的能力，例如：

- 拥有和管理多个国家众多部门的大部分关键基础设施；
- 对资产、网络、系统、设施、功能及其它能力的了解；
- 事件响应技能与经验；
- 快速瞄准需求的产品、服务和技术的创新和提供能力；以及
- 设计、部署、运行、管理和维护全球互联网。

在评估私营部门的价值定位时，与政府合作加强CIIP和网络安全的优势是显而易见的。政府可以通过多种方式给这一合作关系带来价值，其中包括：

- 就重要基础设施面临的威胁，向所有者和运营商提供及时、分析性、准确、综合及实用的信息；
- 使私营部门从一开始就参与CIP举措和政策的制定工作；
- 利用公共平台和其它直接交流方式向公司领导层说明，投资于超出其具体商业战略范围的安全措施，对商业和国家安全的益处；
- 营造一种鼓励和支持公司自愿采取广泛认可且稳妥可靠的安全做法，并根据需要在超出其狭隘商业利益需求的高度，更新和加强其安全工作和做法；
- 与私营部门共同确定工作重点，并对它们提供保护和/或修复；
- 向强化未来CI保护工作所需的研究提供支持；
- 通过举行练习、专题研讨会、培训班和计算机建模活动，为从事跨部门的相互依赖性研究寻求资援，形成支持商业持续性规划的指导性决定；并且
- 实现时间敏感性信息的共享以及在发生事件期间，向重点基础设施提供修复与恢复支持。

作用与职责

政府与私营部门同心协力，便可就各自承担的网络安全作用与职责达成共识。政府可以协调和领导保护工作。例如，政府的延续需要确保其网络及物理基础设施的安全可用，这是向其重要职责和服务提供支持的必要条件。此外，政府可以在发生灾难时发挥关键的协调作用，也可以在私营部门面对事件资源不足的情况下提供帮助。政府可以推动和鼓励私营部门采取提高安全性的主动行动，包括制定及时交流有关威胁的分析性实用信息所需的政策和规范，并激励私营部门在超出其商业利益需求的高度强化安全性。最后，政府还可以赞助和资助研究与开发工作，以改进安全程序和工具。

信任

信任是政府与私营部门成功合作的关键，也是建立、发展和维持政府与私营部门合作关系的必需。政府与私营部门之间的有力合作和信息交流，可增进对情况的了解，加强就战略问题的合作，有助于网络风险管理和对响应与恢复工作的支持。通过更好的信息交流与分析，政府和私营部门将能更有效地发现威胁和弱点，并交流缓解和预防风险的策略和资源。

以下是政府在与私营部门进行合作时需要考虑的总体目标。

II.A 本部分涉及的目标概览

II.A.1 建立政府-私营部门合作关系，为有效管理网络风险并保护网络空间作出努力。

II.A.2 提供一种机制，为达成共识汇集多种视角、权益和知识，并共同推进强化国家网络安全的工作。

II.B 实现上述目标的具体步骤

II.B.1 从最初就将私营部门观点纳入安全政策和相关工作的制定和实施之中。

1) 在许多国家中，私营部门掌握和运行着许多国家依赖的最关键的基础设施和网络要素。创建和支持网络空间的技术随着私营部门的创新而日新月异。因此，仅靠政府不足以保证网络空间的安全。对私营部门观点的了解以及关键基础设施的主要所有者和运营者的参与，对于政府旨在制定和实施网络安全政策和风险管理框架的网络安全工作至关重要。私营部门可以通过参加政府 – 私营部门工作组向政府通报情况，政府则可以征求行业对网络安全政策和战略制定的意见，并通过信息共享机制与私营部门机构协调行动。政府应保证私营部门从一开始便参与举措和政策的制定、实施和维持工作。

2) 政府和私营部门应联手通过一项风险管理办法，使政府和私营部门能够确定网络基础设施、分析威胁、评估弱点、估计后果并制定缓解办法。

3) 政府和私营部门应联合开展有关网络风险管理的研发（R&D）活动。私营部门和政府公开其R&D重点和举措，可以确保资源的有效分配和使用，R&D举措的及时制定，以及最终产品和服务为强化国家网络安全而及时地依序推出。

II.B.2 促进不同关键基础设施行业的私营部门团体的发展，以便同政府携手解决共同面临的安全问题。

1) 不同关键基础设施部门成立的商业协会等团体，有助于满足共同的网络安全需求。这些团体可能侧重解决战略和/或运作问题，以及涉及整个私营部门的安全管理问题，其中可能包括风险管理、认知、政策的制定与执行等一系列问题。这些私营部门团体可以提供一种与政府合作的制度化程序，并能作为就网络安全等敏感问题开展对话的论坛。

2) 很多国家的不同关键基础设施部门都成立了这类团体，使各部门代表能够聚集一堂，就安全威胁、薄弱环节与事件影响交流信息。通常，这类团体还能够实时地向成员发出提示和报警，促进对关键基础设施造成事件影响的意外事件的缓解、应对和恢复工作。

3) 这些团体应考虑采取措施，使成员（如政府和私营部门）间的合作和信息交流能够在一个可信任的论坛进行。这些措施中可能包括以下内容：向成员提供匿名保护；访问跨部门和政府信息；使用针对敏感威胁、薄弱环节和分析的产品；以及获得有关应急响应协调、运作方式和练习等主题的专业技能。然而在为促进合作而考虑这些做法的同时，还必须在其中加入专用和商业敏感信息的保护方式。

II.B.3 让私营部门团体与政府聚首于可信任的论坛，研究解决共同面临的网络安全挑战。

1) 在政府和私营部门之间建立互信并实现成功合作需要若干条件。建议在政府和私营部门之间达成一项指导合作和交流的书面协议。参与方需要有共同的愿景和宗旨。由强有力的个人或机构领导确定工作重点、分配资源并作出维持政府私营部门合作关系所必需的承诺。还需要确定接触规则，指导个人和机构在合作关系中的行为。

2) 参与方必须能够看到实实在在的可衡量的成果。为个人和机构的合作做出价值定位和明确的阐述，是发展和维持公共 – 私营部门合作关系的关键。

II.B.4 鼓励相互依存行业的团体开展合作。

1) 一类基础设施发生的事件可能产生连带影响，致使其它类基础设施发生相似事件。例如，电力短缺可能干扰电话和互联网业务。此外，虽然各行各业都制定了各自的应急计划，但他们必须考虑到事件可能对其它部门产生的影响。跨基础设施的信息交流有助于对贯穿多个部门的全国性意外事件采取应对措施。

II.B.5 制定政府和私营部门事件管理合作方案。

1) 快速定位、信息交流和恢复措施通常能够减少网络事件造成的损失。需要在国家一级建立公共 – 私营部门合作关系，以开展分析、发出报警并协调应对措施。

2) 政府和行业应该共同制定战略、运作和认知协调框架，以改进事件管理。这一框架应具有一个正式的信息交流结构，其中包括负责与政策相关的问题和运作信息交流的牵头人，还包括有关交流和上报事件情况、保护和发布敏感的（政府和私营部门）专用信息以及信息通报和传播机制的政策和程序。私营部门的信息通常包括公司专用信息，一旦外泄就可能造成市场份额萎缩、负面宣传或其它消极影响。同样，政府信息也可能是保密或敏感的，不得对外公布。必须采取政策和技术措施，在保护信息和公众的知情权之间找到平衡。政府可以通过强化信息交流政策和私营部门关系以及持续的政策评估，不断提高互信。网络练习通过试用危机确实出现期间部署的机制，也能够考验政府和私营部门在网络事件响应及恢复工作中的沟通与协调。

第三部分

遏制网络犯罪

通过制定刑法、程序和政策并对其进行现代化更新，以防止、遏制、响应并起诉网络犯罪，可大大改善网络安全。

III.A 本部分涉及的目标概览

III.A.1 颁布实施有关网络安全和网络犯罪的一套综合性法律。

各国均需要打击网络犯罪的国内立法、电子刑侦程序并为他国提供援助。这些法律有的通过国家法典专门加以规定，而有些则不然。为简化起见，本报告认为各国均应出台网络犯罪基本法，另加一套相关程序和相互支撑的法律文本。当然具体采用什么结构最适合该国的国情由各国自行决定。

III.B 实现上述目标的具体步骤

III.B.1 评估现有法律体系的正确性。各国应审查其现有刑法典，包括相关程序，判断其可否解决目前（和将来）出现的问题。我们建议采取以下步骤：

1) 建议酌情制定必要的相关法律，特别注意但又不局限于地区性举措。这些法律应涉及破坏或毁坏计算机数据；支持调查的程序机制以及追查电子邮件来源的能力等；也包括可能的国际法律合作（如取证等）。

2) 一国应考虑其法律是否依赖过时的技术。例如，某个法律可能只涉及侦听话音传输。这样的法律也许需要进行修订，以纳入数据传输的条文。

3) 一国的网络犯罪法的评审工作应由感兴趣的所有相关部委和立法机构（即便他们与刑事司法毫无关联）进行，确保可借鉴的意见无一遗漏。信息技术官员应当注意到一些情况，如网络犯罪法未必囊括日渐盛行但该国立法者尚未普遍认知的新技术。

4) 此外，建议当地私营部门、国际私营部门设在当地的子公司、当地非政府间组织、学术界、公认的专家和公民团体也应对一个国家的现有刑法进行评估。

5) 一个国家可以就上述问题向他国寻求建议。

III.B.2 起草并通过应对网络犯罪的实体法、程序法、相互援助法和政策。

1) 建议各国积极参与酌情制定必要法律的活动，特别注意但又不局限于包括欧洲理事会制定的《网络犯罪公约》在内的地区性举措。建议各国参与区域性和国际合作，以打击网络犯罪，加强网络安全，并制定包括打击垃圾信息、恶意软件和僵尸网络等在内的网络安全完善机制。

2) 一个国家的网络犯罪法律草案应由所有的政府机构和立法机构进行评估。这样的草案应提交公众评议，以便处理任何可能的、在草案中未涵盖的技术、侵害或其他相关问题。

3) 网络犯罪法不仅能够应对传统的网络犯罪，例如计算机犯罪和计算机侵入，也应保护和其它犯罪有关的电子证据。

4) 对用于民事和商务的数据保护法，不应作为导致无理妨碍各国交换刑事犯罪证据的补充和解释。

5) 决定聘用顾问起草法律的国家，应审查顾问资质并在起草过程中监督其工作。未根据一国法律接受专门培训的人可能无法悉数收录必要条款，特别是程序和相互间的法律援助部分。而且没有公诉经验的人士不可能全面考虑证实案件过程中的实际情况。有些顾问有资格协助起草电子商务法，但对刑法却不在行。

6) 就《公约》未涉及的内容，可向其它国家征求意见。例如，各国可要求互联网服务提供商将经过其系统的数据保留一段时间（通常为六个月）；或要求将具有一定影响的计算机事件报告政府部门；或要求用户经过身份认证方可使用网吧。

7) 如果时间允许，一国可向其它国家和多边国际组织征求关于网络犯罪法草案（或修正案）的意见。如上文所述，这种意见可私下征求，且多个国家根据其经验提出意见将十分有益。

8) 一国应尽早（根据本国程序）向对该主题感兴趣并经认可的相关各方征求意见：当地私营部门、跨国私营部门的当地子公司、当地非政府间组织、学术界、无隶属关系但对此感兴趣的自由公民等。

III.B.3 建立或指定国家网络犯罪部门。

1) 各国无论发展水平如何，至少应具备基本的网络犯罪侦查能力。例如，即便在欠发达国家手机用户也呈爆炸式增长，而手机可用于欺诈、转账、共同谋划犯罪、向电子网络发送病毒，制造爆炸案等。

2) 各国应选定或培训一个或多个有能力开展国家网络犯罪调查的网络犯罪调查机构。有时该选定哪家（含多家）执法机构是显而易见的事。而有时候多家执法机构相互争抢，可能导致上级部门很难做出决定。即便一国目前没有具备必要技能的人，有个别警官对电子技术很有兴趣、愿意掌握更多知识从而在这条路上走得更远也不足为奇。

3) 网络犯罪侦查部门（包括只有少量刑侦员的情况）需要支持。他们需要相对先进的设备、合理可靠的网络连接和不断培训。这种支持可来自于国家政府、国际组织或其它国家以及私营部门的捐赠。

4) 在可能的情况下，建议这些部门至少具备基本的计算机取证能力。这需要软件工具和更多培训。（如果不可能具备取证能力，各国应事先准备接受关键证据可能丢失这一事实，甚至关键案件也不例外。）在某些情况下，其他国家和相关组织可就特殊案件提供取证协助。另外，其它国家和组织也可能提供网络取证方面的培训。例如，美国卡耐基 – 梅隆大学计算机应急组织协调中心（http://www.cert.org）通过在线方式或CD-ROM提供免费或低价的网络取证培训。

5) 网络犯罪部门一经建立，应将该部门的设立和职责告知该国其它执法部门和检察机关。如果地方执法部门在调查涉及电子证据的恶性案件，但不知道国内有网络犯罪部门能够搜索到目标计算机或提供其它协助，则在该国首都成立这样的部门根本无济于事。不幸的是，一国执法部门不知道本国有网络犯罪部门的现象在全世界司空见惯。

6) 网络犯罪部门或可能组建的部门应在最大范围内与国际合作伙伴建立联系。在最初阶段，可向其它国家和国际执法机构就建立该部门征求有关意见。在随后的阶段，其它国家、国际执法机构、相关多边组织和私营部门会提供各类培训，甚至设备和软件。建立这种联系还有另外一个原因：随着全球联网程度越来越高，向外国执法部门寻求帮助十分关键。

7) 网络犯罪部门还应与国内各相关和感兴趣的部门建立联系，例如国内非政府间组织、计算机安全事件响应组织、私营部门实体和学术界，以确保他们知晓该部门的存在及其能力，与其进行合作并知道如何报告可能的网络犯罪。

III.B.4 发展与国家网络安全基础设施的其它部门及私营部门的合作关系。

1) 政府部门、国家网络安全基础设施的其它部门和私营部门之间的合作关系十分重要，理由如下：

a) 上述小组之间交流信息（例如，告知有关方面正在探讨新法律或开发一项新技术）

b) 交换意见（例如，“如果我们在新法中如此规定，您觉得是否涉及隐私问题？”或“如果出于合法的公共安全方面的原因追查电子邮件的话，对某项技术应做何改动？”）

c) 相互培训，尽管多数情况下由私营部门向政府提供培训

d) 相互提供有关威胁或薄弱环节的警告

e) 从而便于来自不同部门的人员可深入了解对方，在紧急情况下可以相互信任。

2) 建立这种关系的第一步是由一人或多人制定一份人员和机构名单，注明该国相关部门的这些人员与机构的特定计算机技能和职责。这些人员的联系方式也在名单中列出。也许列非正式的名单最好，从而避免大家为了登入名单的资格而争执不休。

3) 每个国家都可能设立无数对网络安全有所关注的相关部门，包括立法机构、部委、非政府间组织、计算机安全事件响应组织、学术界、私营部门和个人。其中有些是纯粹的国内部门，而有些则隶属于大型的外国实体。

III.B.5 促使检察官、法官和立法人员就网络犯罪问题达成谅解。

1) 要正确解决网络犯罪问题，检察官和法官了解诸如计算机、软件、网络以及电子证据的重要性日渐凸显等领域的问题。同样，立法者也应了解这些问题并知晓其本国法律是否足以应付网络犯罪。培训是该问题的一个解决办法。

2) 如要求进行基本的技术培训，渠道很多，这要根据各国资源因地制宜：

a) 具有技术能力的国内服务机构或部委，例如执法机构或信息技术部；

b) 外国政府；

c) 相关跨国组织；

d) 本地私营部门；

e) 国际私营部门，特别是（但不是必须）其在本地从事业务经营；

f) 相关学术界；

g) 国内外计算安全事件响应组织；和

h) 国内外相关非政府间组织。

3) 应通过培训使资深决策者和高级政府官员了解电子网络面临的威胁（例如国内银行系统如何遭袭）和电子网络带来的威胁（例如利用互联网找寻易受侵害的儿童进行性交易）。上述组织应举办涉及电子网络这些方面的相关培训。

4) 最好针对检察官和法官举办起诉网络犯罪或其它涉及电子证据的犯罪、使用电子证据、争取国际合作的方式等方面的培训。这些培训可由以下机构举办：

a) 具有适当职权的国内服务机构或部委，例如公诉员办公室或司法部；

b) 外国政府；

c) 相关跨国组织；

d) 相关学术界；

e) 相关国内外非政府间组织，及其

f) 相关个人。

5) 一国可能需要法案起草方面的培训。上段列出的组织可以提供此类培训。本地和国际私营部门，特别是（但不是唯一的）设立了本地公司的国际私营部门，可能具有这方面的技术专长。不过私营部门实体更有可能在电子商务法方面有所帮助，而不是网络犯罪、刑事诉讼程序和国际司法协助法。

6) 对于上述各类培训，培训机构可能亲赴请求培训的国家开展工作，或提供（电子或纸质）培训模块，供请求国的培训师使用。在第III.B.3.4节所述的CERT-CC培训等个别情况下，往往提供免费培训或仅收取最低费用。

7) 在有些国家，提高全国对网络犯罪的意识关键在于争取高级官员（甚至是一位大权在握的高级官员），尤其是预算控制官员的支持。如果众所周知某位部长对网络安全十分关注，则他/她所在的部委（甚至包括政府其它部门）也许会更多地支持想有所作为的一线工作人员。

III.B.6 参与全天候（24/7）的网络犯罪联络网。

1) 1997年，在工业化国家八国集团（G8）的高技术犯罪分组在G8司法和内政部长的指导下启动了全天候（24/7）的网络犯罪联络网，以便在涉及电子证据的紧急调查方面加强国际协助。很多网络犯罪调查员均感到学习如何向他国寻求迅捷的援助十分困难。另外，很多调查员认为十多年前订立的司法协助条约对诸如午夜对某国金融系统发动计算机入侵等瞬间得手的案件毫无助益。截至2008年初，这一网络已通达将近50个国家。欢迎具备以下必要能力的国家加入该网络。

2) 加入网络之前，各国必须指定一个全天候开放的联络点，这也是该联络网被称之为“24/7网络”的原因所在。联络点可以是可直接对话的个人或可通过办公室与其联络的个人。他/她必须具备三个方面的知识： 1) 技术，这样才能避免冗长的技术答疑，毫不迟延地传达请求； 2) 本国法律，和 3) 基于哪部国内法为其他国家提供协助。如果联络点本人不具备上述三种知识，则必要时（不一定等到下一个工作日）必须即刻联系本国政府内的其他有权且有能力提供帮助的人。

3) 通信必须（至少在最初的时候）从A国的全天候联络点发至B国的全天候联络点，以确保连续性和安全性。这意味着联络点不应向本国其它部门透露联络方式，而应代表本国发出请求的部门（例如省级警察局）首先进行国际联络。如果两国基本确立合作关系，则联络点可顺势退出调查，由A国相关省级警察组织与B国直接联系。

4) 加入该网络并不表示各国保证一直向另一方提供协助，或联络网替代了两国间正常的司法协助。联络网仅能保证请求国会即刻引起有关责任部门的关注，即使在深夜也不例外。在提供最初的协助之后，各国可要求（也可以放弃）使用较迟缓的相互协助渠道。

5) 二十四小时待命并不表示办公室要日夜有人员监守、开启一定数目的计算机工作站且网络调查员时刻等待电话或电子邮件。很多国家没有设立这样的办公室。更为普遍的情形是，一国指派一位执法人员（也可能是多人轮班）随时通过电话联络，或许睡觉时手机也不离身。

6) 申请加入的国家应联系G8高科技犯罪分组主席（其成员不仅限于G8成员国，目前将近50个国家已经加入）申请国必须填写一张简表。[11]这一过程不需签署备忘录或条约等正式的国际协议。24/7网络时常为联络点举办培训和联网会议，必要时还提供参会的差旅费补贴。

7) 加入网络的单位有责任将它的存在及其有能力协助联系他国告知国内其它感兴趣的执法部门或网络犯罪部门。

[11] 该表应传真给美国司法部计算机犯罪与知识产权处24/7网络协调员（美国华盛顿特区），号码：+1 202-514-6113。还可通过电子邮件发至richard.green@usdoj.gov。

第四部分

创建国家层面的事件管理能力：监控、警告、响应和恢复

政府有必要成立或指定一个国内组织，作为保障网络空间安全和保护关键信息基础设施的牵头人，它的使命包括监控、警告、响应和恢复，并促成政府实体、私营部门、业界、学术界和国际社会之间的协作。

政府在国际层面保障网络安全时主要发挥针对发生的网络事件的筹备、侦测、管理和响应作用。实施事件管理机制需要考虑资金来源、人力资源、培训、技术能力、政府和私营部门关系及法律要求。各级政府之间以及与私营部门、学术界和国际组织的协作对有效协调管理事件的能力与专长，提高有关潜在事件和补救措施的意识而言非常必要。政府在确保协调这些实体的过程中扮演着重要的角色。

IV.A 本部分涉及的目标概览

建立国家事件管理能力需要开展一系列密切相关的活动，这些活动包括：

IV.A.1 建立一个协调统一的国家网络空间安全响应系统，以便负责网络事件的防范、预测、侦测、响应和恢复。

IV.A.2 设立管理网络事件的联络点，汇集政府（包括执法部门）的关键要害部门和基础设施运营商和销售商的必要部门，以降低风险和事件的严重程度。

IV.A.3 参与监控、警告和事件响应的信息共享机制。

IV.A.4 制定、测试并演习紧急响应计划、程序和协议，以便确保政府和非政府合作伙伴可以在危机中建立信任并有效协调。

IV.B 实现上述目标的具体步骤

发展国家事件管理能力是一项长期的工作，首先要建立国家计算机事件响应组织（N-SIRT）[12、13]。

IV.B.1 确认或建设国家计算机安全事件响应组织（CIRT）的能力。

1) 对重大网络事件的有效响应可以控制对信息系统的危害，确保采用有效的响应方式，缩短恢复时间和成本。CIRT应与公共和私营部门合作，而且需要这样的组织（特别在影响到国家的事件中）担任政府内部的牵头人，协调网络事件的防卫和响应工作。在这些情况下，N-CSIRT必须与相关部门并肩而战，但不扮演指导或控制的角色。

2) 要求CIRT提供相应的服务和支持，防范并响应关系到安全的问题，并担任网络安全事件报告、协调和通信的唯一联络点。CIRT的使命应包括就关键信息基础设施进行分析、警告、信息共享、弥补弱点、减轻影响并协助国家恢复工作。具体而言，CIRT应在国家层面履行几项职能，包括但不限于：

---

12 参见WTSA第58号决议。在某些国家CIRT被称为国家计算机安全事件响应组织（NCSIRT）或国家安全事件响应组织（N-SIRT）。

13 ITU-T将根据第58号决议开展工作取得的成果，可能会对这些最佳做法中的第四部分产生影响。

- 侦测并识别反常行为；
- 分析网络威胁和弱点并发布网络威胁警报；
- 分析综合他方（包括厂商和技术专家）发布的事件和弱点信息，为利益攸关方提供评估报告；
- 建立可靠的通信机制并促使利益攸关方加强联系，以共享信息并应对网络安全问题；
- 提供早期告警信息，包括与弥补弱点并减少潜在问题有关的信息；
- 制定减轻影响和响应战略，促成对事件协调一致的响应；
- 共享有关事件及其响应的数据和信息；
- 跟踪和监控信息，确定发展态势和长期补救措施；
- 公布保护一般性网络安全的最佳做法和事件响应和防范的指导意见。

IV.B.2 在政府内部建立民间和政府机构之间的协调机制。

1) CIRT主要作用在告知利益攸关方有关信息，包括目前弱点和威胁的信息。必须参与响应活动的利益攸关方就是相关政府机构。

2) 与这些实体进行有效协调可以采取多种形式，例如维护一个用于信息交换的网站；通过邮件列表提供新闻快讯和趋势分析报告等信息；发行出版物，内含警告、小窍门和网络安全的全面信息，例如新技术、弱点、威胁和后果。

IV.B.3 与业界建立合作关系，就国家网络事件进行筹备、侦测、响应和恢复。

- 政府和CIRT必须与私营部门合作。很多国家的私营部门拥有相当多的关键信息基础设施和信息技术资产，政府必须与私营部门联手才能实现有效管理事件的总目标。
- 与私营部门建立互信合作关系后，政府能够深入了解私营部门所有并运营的关键基础设施。公共 – 私营部门 – 民间的合作关系可管理与网络威胁、弱点和后果有关的风险，并通过信息共享、多国和双边承诺增强对局势的认识。
- 鼓励私营部门与政府间信息共享的做法，实现运作信息的实时共享。
- 鼓励合作关系可通过以下方式实现：向政府和私营部门宣传优势；制定并实施保障敏感性专有数据的计划；建立公共和私营部门之间网络风险管理和事件管理工作组；共享事件响应/管理最佳做法以及培训资料；共同划分政府和私营部门在事件管理方面的职责，以设置前后一致的、可预测的操作规则。

IV.B.4 在政府机构、业界和国际合作伙伴内部设联络点，旨在推动与CIRT进行磋商、合作和信息交流。

1) 指定适当的联络点并形成旨在进行磋商、合作和信息交流的合作关系是确立协调有效的国内和国际事件响应机制的基础。这些关系可有助于对潜在的网络事件的早期预警，便于事件响应实体和其它利益攸关方交流有关发展趋势、威胁和响应的信息。

2) 随时更新与利益攸关方的联络点和通信渠道，有助于积极及时地交流趋势和威胁的有关信息并加快响应速度。尽可能根据各部门的职能建立联系且避免单线联系十分重要，这样即便在曾经联系的个人离职的情况下也能够保证通信渠道畅通无阻。建立关系往往始自个人之间的相互信任，但其后应发展为机构间的正式安排。

IV.B.5 参与国际合作和信息共享活动。

1) 政府应当鼓励与各组织、供应商和其它相关主题专家开展合作，以便（1）促使事件响应成为一项全球性准则，（2）推动并支持CIRT加入现有的全球和区域性大会和论坛，从而能够开展能力建设，在区域基础上完善事件响应技术，并（3）在为建立国家CIRT和与CIRT机构进行有效沟通搜集材料方面开展协作。

IV.B.6 开发保护政府机构的网络资源的工具和程序。

1) 有效的事件管理还需要制定和实施政策、程序、方法和安全控制手段以及开发使用保护政府网络资产、系统、网络和功能的工具。对于一个CIRT而言，这些包括标准操作程序（SOP）、内部和外部操作指导方针、利益攸关方协调的安全政策、部署CIRT操作的安全信息网络以及安全通信。作为事件响应的牵头人，CIRT应相互协调，并支持与其他事件响应实体的合作。政府还应对新老员工不断提供事件响应方面的培训。

IV.B.7 通过CIRT开发协调政府运作应对并恢复大规模网络攻击的能力。

1) 如果某个事件上升为具有全国影响的事件，就有必要设立中心联络点来协调其它政府实体及诸如私营部门等其它利益攸关方团体。制定计划和程序来确保CIRT已做好准备应对一场可能的事件是重要的。

IV.B.8 促进可靠的信息披露做法以保护网络基础设施的运作和完整性

1) 硬件和软件等信息技术产品中的漏洞可能会被发现。是否公开披露应视情况而定，从而避免漏洞信息被滥用。在披露此类漏洞前应给予供应商充分的时间。

第五部分

宣传国家网络安全文化

鉴于个人电脑功能日渐强大、技术日渐融合、ICT日益广泛的应用以及跨国界连接不断增加，开发、拥有、提供、管理、服务和使用信息网络的参与者必须了解网络安全问题，并各尽其责地采取行动，以保护网络。政府必须在培育网络安全文化和支持其他参与者行动的过程中发挥领导作用。

V.A 本部分涉及的目标概览

V.A.1 根据联合国大会（UNGA）第57/239号决议“培育全球网络安全文化”[14]和第58/199号决议“培育全球网络安全文化和保护关键信息基础设施”[15]，推动建设国家安全文化。

1) 推动国家网络安全文化不仅涉及政府在确保信息基础设施安全操作和使用（包括政府操作的系统）时发挥的作用，而且扩展到私营部门，包括公司、民间团体和个人。同样这一部分涵盖政府和私营部门的用户培训、加强安全以及隐私、垃圾信息和恶意软件等其它重要问题。

2) 经济合作与发展组织（OECD）的研究表明，在国家层面，推动创建安全文化的主要因素在于电子政务应用软件和服务以及对国家关键基础设施的保护。因此主管部门纷纷采用电子政务应用软件和服务，改进其内部操作并为私营部门和个人提供更好的服务。不应单单从技术角度解决信息系统和网络的安全问题，而应包括风险防范、风险管理和用户意识等措施。OECD发现电子政府活动产生的积极影响在于从公共管理部门扩大到私营部门和个人。电子政务举措其实对安全文化的传播起到了增效作用。

3) 各国通过开展合作活动，最好是通过某种类型的协议，在落实网络安全举措时应采用跨学科和多个利益攸关方的方法。此外，有些国家正在建立落实国家政策的高级管理结构。同时对提高意识和教育举措给予重视，共享最佳做法、参与者之间的相互协作以及采纳国际标准也十分重要。

4) 国际合作对于培育安全文化极为重要，有利于互动和交流的区域性组织的作用同样不可小觑。

V.B 实现上述目标的具体步骤

V.B.1 就政府负责操作的系统实施网络安全计划。

1) 政府欲保障自己操作的系统，首要步骤便是制定和落实一项国家安全计划。筹备该计划的过程包括风险管理、安全设计和实施。应对计划及其落实步骤定期进行复评，掌握进度并找出计划及其落实步骤中需要改进的地方。计划还应包括事件管理的内容，包括响应、监控、警告和恢复，以及信息共享网络等。安全计划还应当涵盖V.B.2呼吁采取对政府系统用户的培训行动以及政府、私营部门和民间团体就安全培训和举措开展合作等内容。用户意识和责任是培训所应解决的主要问题。

---

[14] http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf

[15] http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf

V.B.2 实施面向系统和网络用户的安全意识计划和举措。

1) 一个有效的国家网络安全意识计划应在公众和关键部门中普及网络安全意识，保持与政府网络安全专家的联系以分享网络安全举措的信息并推动在网络安全事项上的协作。当制定意识计划时，需要考虑三项功能：1) 与利益攸关方的联系及其介入，以在私营部门、政府和学术界之间建立和维持信任关系，增强网络安全意识并有效确保网络空间的安全；2) 进行协调，以确保在政府体系内就网络安全事件进行协作；3) 通信和联络，主要是进行内部（在负责该计划的政府机构内部）和外部（其它政府机构、业界、教育机构、家用计算机用户和普通大众）联络。

V.B.3 鼓励在企业中发展安全文化。

1) 与企业构筑安全文化伙伴关系可通过一系列创新型的方法实现。很多项政府举措曾专门用于提高中小企业（SME）的意识。政府与企业协会的对话或政府 – 私营部门 – 民间协作能够协助主管部门设计和实施教育和培训举措。这些举措包括：（离线和在线）公布信息，例如小册子、指南、手册、政策和概念样本等；建立面向SME的网站；提供（在线）培训；提供在线自我评估工具；开发将电子签名与SME业务和应用软件集成的软件工具；为安全系统的形成提供财力、税收支撑或其它激励措施；或采取积极措施，增强网络安全。

V.B.4 支持将影响扩大至民间团体，特别关注儿童、青年、残疾人和个人用户的需求。

1) 一些国家的政府已经与企业开展合作，提高公民对日渐猖獗的威胁和应对措施的意识。有些国家举办特别活动，例如信息安全日或信息安全周，其中计划采取向包括普通民众在内的更多人推广宣传信息安全的行动。大部分举措旨在通过包括教师、教授和父母在内的学校体系或直接散发学习资料教育儿童和学生。使用的各类学习资料花样繁多，从网站、游戏、在线工具、明信片、教科书到考试文凭等。这些举措包括为儿童的父母开办培训课程，告知他们安全风险问题；为教师提供学习资料；为孩子提供上网游戏工具并传播信息安全的教育信息，寓教于乐；编制教材和开发游戏；设立有关安全上网冲浪的考试、文凭以及测验。

2) 政府和私营部门可以共同吸取制定安全计划和培训用户方面的教训；学习他人的成功经验和创新成果；努力提高国内信息基础设施的安全。

V.B.5 推动综合性国家意识普及项目，让各参与方（企业、员工和大众）在保障网络空间安全方面各尽其责。

1) 由于部分用户、系统管理员、技术开发商、采购员、审计员、首席信息官和企业董事会网络安全意识匮乏，导致很多信息系统极易受到攻击，所以即便基础设施本身不存在这些弱点，也会蒙受巨大风险。例如，系统管理员的安全意识通常是企业安全计划中很弱的一环。倡导私营部门培训员工，并对员工实行广泛认可的安全认证，将有助于弥补这些弱点。政府在国家发展和意识普及活动中进行协调，构建安全文化，将建立与私营部门的互信关系。维护网络安全是共同的责任。门户网站和各网站可作为一种有益的机制来推动国家意识计划，使政府机构、企业和个人消费者可以获取信息并采取措施，各尽其责地保护其网络空间。

V.B.6 加强科学和技术（S&T）以及研究和开发（R&D）活动。

1) 就政府支持科技研发活动而言，有些工作可以专门针对信息基础设施的安全。通过确定网络R&D的重点工作，各国可以协助开发安全性能强的产品并应对难以克服的技术挑战。由学术机构进行的R&D，可以让学生参与网络安全举措。

V.B.7 审查现有的隐私制度并使之与在线环境保持同步。

1) 审查时应考虑各国以及OECD等国际组织所采用的隐私机制。OECD于1980年9月23日通过的《保护隐私和个人数据的跨国界流通的指导原则》将继续作为国际社会达成共识的有关个人信息收集和管理的一般性指导原则。通过确立核心原则，指导原则在协助政府、企业和消费者保护隐私和个人数据以及避免数据跨国界流通（以在线和非在线形式）方面不必要限制等领域发挥主要作用。

V.B.8 提高网络风险和可用解决方案意识。

1) 解决技术问题需要政府、企业、民间团体和个人用户共同制定和实施有关措施，将技术（即标准）、程序（如自愿性指导原则或强制性规定）和人员（即最佳做法）等各个部分融为一体。

2) 威胁的一个例子即垃圾信息，相关联的威胁则如恶意软件。包括ITU-T第17研究组第4号课题在内的一些组织，正在研究有关垃圾信息的问题。附件A列出了此问题的高层概述。

3) 身份管理是技术工具应对各种网络安全需要的一个例子。包括ITU-T第17研究组第10号课题在内的一些组织，正在研究有关身份管理的问题。附件B列出了此问题的高层概述。

附录 1

缩略语列表

APECTEL	亚太经济合作组织电信和信息工作组
CAN-SPAM	未经请求的色情及行营销信息攻击控制法（2003年）（美国）
CCIPS	（美国司法部）计算机犯罪与知识产权处
CERT	计算机应急响应组
CERT-CC	（美国卡耐基 – 梅隆大学）计算机应急组织协调中心
CII	关键信息基础设施
CIIP	关键信息基础设施保护
CIRT	计算机事件响应组
COE	欧洲理事会
CPNI	国家基础设施保护中心（英国）
CSIRT	计算机安全事件响应组织
CVE	一般弱点和暴露的问题列表（美国）
DHS	国土安全部（美国）
DOJ	司法部（美国）
EU	欧盟
FAR	联邦采购条例（美国）
FCC	联邦通信委员会（美国）
FIRST	事件响应安全组织论坛
G8	8国集团
ICT	信息和通信技术
IMPACT	国际打击网络威胁多边伙伴关系
ISAC	信息共享和分析中心（种类繁多，例如IT-ISAC；美国）
IT-ISAC	信息技术信息共享和分析中心
ITAA	美国信息技术协会
LAP	伦敦行动计划
MSCM	移动业务商用信息
NIAC	ITAA国家信息保障理事会
NIATEC	（美国爱达荷大学）国际信息保障培训和教育中心
NIST	国家标准和技术研究院（美国）

NRIC	网络可靠性和互操作性理事会（美国FCC）
NSTAC	国家安全和电信顾问委员会（美国DHS）
NVD	国家弱点数据库（美国）
OECD	经济合作和发展组织
OVAL	开放式弱点评估语言
PSTN	公用交换电信网
R&D	研究和开发
S&T	科学和技术
SME	中小型企业
SMS	短信业务
SOP	标准操作程序
TCPA	电话消费者保护法（美国）
UNGA	联合国大会

附录 2

网络安全合作实施战略和有效措施

下文简要介绍的方法采用一种项目方式，旨在促使各国把发展强大的网络安全系统作为一项重点国策。这种方式分为三个项目阶段，将一国从最初的能力测评推进到项目实施和评估阶段。这种分步实施的方法如下文所示：

网络安全合作实施战略和有效措施

阶段 1 – 测评、评估和推荐合作交流项目计划。

- **测评：**首要一步是一国对其安全项目的当前状态进行评估。专家组通过使用标准化的测评工具进行此类测评。
- **评估：**测评阶段收集的信息有利于了解该国当前网络安全项目的优势和不足，并确定应着重开展哪些工作。
- **推荐：**通过评估获得的信息成为计划的基础，以满足国家需要。

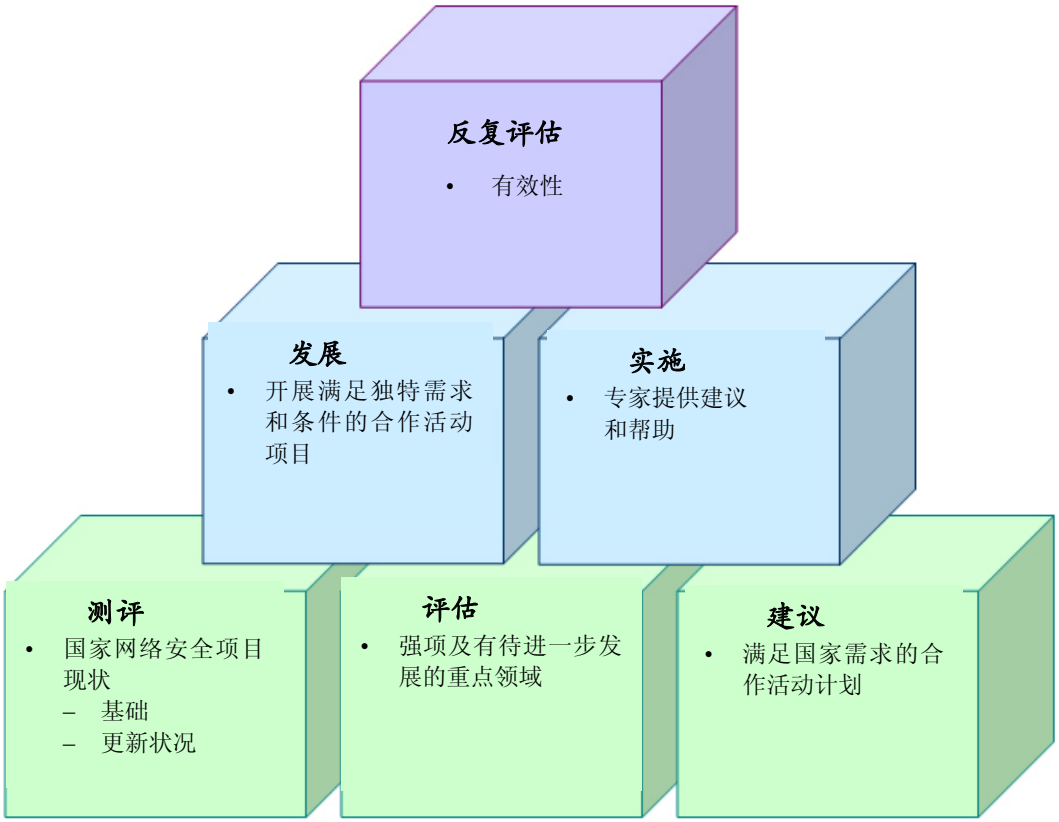
阶段 2 – 制定和实施合作项目。

- **制定合作项目：**国家专家和国内外的同行会面，根据特定国家的特殊需求和环境设计、确定和调整各项活动。这些活动可以包括一系列的合作交流以及确定长期的重点需求。
- **实施项目：**国内或国际专家落实项目并提供具体建议。

阶段 3 – 评估合作项目、确定成功与否并收尾。

- **评估合作项目：**网络安全合作项目将由内部或国际专家对其有效性定期进行重新评估。尚不完善的领域将成为进一步合作交流的主题，并且是这一持续进程的新起点。在一国与其他国家合作的情况下，如果该国的项目经评估被视为有效，则这种合作将逐步终止。

图 1：网络安全能力建设的项目方法



有效措施

下文介绍了评定该领域的效果以及向上级官员报告进展的方法。该方法构成一种逻辑链，即将基本输入（针对国家和/或地区的耗时耗钱和耗力的项目）和最后预期的结果（强化网络安全）相关联。该链如下表所示：

评定类别：	效果要素：
基本输入：	**国家项目：** • 时间 • 资金 • 人力
基本工作程序：	**工作（包括可能的合作交流）：** • 制定国家战略 • 制定法律法规 • 事件管理 • 政府 – 行业伙伴关系 • 网络安全文化
基本输出：	**数量：** • 会议或合作交流 • 与高级政策和技术官员的联络
中期结果：	**国家行动：** • 新的网络犯罪法律和法规 • 执法行动 • 建立 CSIRT • 政府 – 行业意识普及项目 • 事件相应问询 • 参与国际组织的网络安全活动 • 遵守国际公约和指导原则
最终结果：	由于国家法律和政策框架、事件响应以及意识提高工作，网络安全风险得以降低。
最后成果：	增强了国家网络安全和全球的安全。

附件A

个案研究：垃圾信息

国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X系列

增补6

（09/2009年）

X系列：数据网、开放系统通信和安全性

ITU-T X.1240系列 –
关于打击垃圾信息及相关威胁的增补

注意！

预出版的建议书

本预出版的建议书是近期获批但未编辑的建议书版本。编辑后出版的版本将取代本版本。因此，预出版版本和最终出版版本之间将存在差异。

前言

国际电信联盟（ITU）是从事电信与信息通信技术（ICT）领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准ITU-T建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

ITU-T X系列建议书增补6

ITU-T X.1240系列 – 关于打击垃圾信息及相关威胁的增补

摘要

ITU-T X系列建议书增补6指出，为了有效打击垃圾信息，政府需要使用各种方法，包括有效的法律、技术工具以及消费者和企业培训。本文件审议了正在处理垃圾信息问题的各国际论坛。本增补提供了一些关于美国和日本如何处理垃圾信息问题的信息，作为用于说明目的的个案研究。

来源

ITU-T第17研究组（2009-2012年）于2009年9月25日通过了ITU-T X系列建议书增补6。

目录

ITU-T X系列建议书增补6

ITU-T X.1240系列 – 关于打击垃圾信息及相关威胁的增补

1 范围

本增补的主题是垃圾信息及相关威胁。本增补的目标读者为新近接触垃圾信息概念并希望了解一些基本信息的国家管理者。

本增补着眼于需要用于有效打击垃圾信息的各种工具，并对一些国际论坛在该领域内正在进行的工作做出了说明。此外，本增补介绍了美国和日本打击垃圾信息的做法，作为用于说明目的的个案研究。

2 参考

无。

3 定义

本增补定义了下列术语。

3.1 网络钓鱼：企图哄骗人们进入错误网站，从而盗取个人私密信息。

3.2 垃圾信息：尽管对垃圾信息并没有统一的定义，但该术语通常用来形容通过电子邮件或移动消息服务（SMS、MMS）发送的未要求的大量电子通信内容。

4 缩写词和首字母缩略语

本增补使用了下列缩写词：

ADSP	作者域发送惯例
APEC TEL	亚太经济合作组织电信和信息工作组
CAN-SPAM	未经请求的色情及行营销信息攻击控制法（2003年）（美国）
CNSA	垃圾信息管制机构联系网络（欧盟）
DKIM	域密钥识别邮件
FCC	联邦通信委员会（美国）
FTC	联邦贸易委员会（美国）
ISP	互联网服务提供商
JEAG	日本反邮件滥用组织（日本）
LAP	伦敦行动计划
MAAWG	反信息滥用工作组
MMS	多媒体消息服务

MSCM 移动业务商用信息

OECD 经济合作和发展组织

OP25B 出局端口25阻止

SMS 短信业务

SPF 发件人策略框架

5 惯例

无。

6 背景

6.1 垃圾信息：垃圾信息曾是包含商业广告的令人备感头痛的通信形式，现在已演化成更严重的网络安全问题的催化剂。例如，垃圾信息可以成为一种载体，便于行骗、四处散播恶意软件（如病毒和间谍软件）并在诱使消费者透露保密信息之后进行身份盗窃（如网络钓鱼）。发信者可以以极低的成本从世界上任一角落将信息发至世界上任何一个人，因此垃圾信息已升级为亟待通过国际合作加以解决的国际问题。

6.2 网络钓鱼：网络钓鱼利用的是互联网电子邮件系统的一个基本特点，即任何人都可不须经过任何形式的认证即可向另一人发送电子邮件。[16] 网络钓鱼企图哄骗人们进入错误网页，从而盗取个人私密信息。网络钓鱼之所以存在主要是由于人们时常会收到来自常用网站的电子邮件，根本意识不到该邮件并非来自合法网站。由于电子邮件没有认证可言，不经仔细审查信息，难以断定该信息是否合法。要进行这种认真的审核需要对万维网使用的潜在机制了如指掌。

网络钓鱼存在的另一个原因是，多数人难以证明其将访问的网站是否合法。有时，我们在进入敏感信息之前不会认真看网页的URL，有时我们根本不知道正确的URL如何。

用来“钓取”敏感信息的万维网服务器往往本身就是恶意软件的牺牲者，由此更难捕捉到钓鱼者。

6.3 恶意软件：在所有人不知情的情况下或未经所有人允许便运行于设备的恶意软件也是一个棘手问题。

7 有效处理垃圾信息及相关威胁的国家作法

7.1 国家战略与垃圾信息：就国家战略而言，各国应制定并保持一套有效的法律、执法机关和工具及技术工具和最佳做法，开展消费者和企业培训，以便有效治理垃圾信息问题。

7.2 法律和监管基础与垃圾信息：就法律基础和监管框架而言，对垃圾信息有管辖权的机关必须具备必要的权力，以便调查国内实施的或对本国造成影响的与垃圾信息有关的违法行为，并采取相应行动。对垃圾信息有管辖权的机关还应当建立与国外权力机关合作的机制。请国外权力机关给予协助的请求应当根据共同利益的领域并在产生重大危害的情况下重点安排。

---

[16] 互联网电子邮件系统设计于上个世纪70年代，当时只有极少数的研究人员和政府官员可以上网，无须认证发送电子邮件人员的身份，因此也没有在系统上设计这一功能。尽管电子邮件系统至此有所发展，这种根本的缺陷由来已久。

7.3 政府/业界合作与提升国家对垃圾信息及相关威胁的认识：所有感兴趣的人士，包括执法机关、企业、行业团体和消费者团体应在打击涉及垃圾信息的违法行为中相互合作。政府执法机关应与行业和消费者团体携手，教育用户并促进信息共享。政府执法机关应与私营部门合作，推动开发打击垃圾信息的技术工具，包括便于查找和识别垃圾信息发送者的工具。

网络钓鱼通常是一种可以防止的犯罪。政府应与私营部门合力改善保护公民免受网络钓鱼的手段，并对消费者和企业进行安全认证方法的培训。

政府亦可发挥作用，教育大众必须使用防病毒软件和应用最新操作系统补丁及可信赖的计算技术来检查恶意软件情况。

8 国际（多边）打击垃圾信息举措

目前有若干打击垃圾信息举措的多边论坛：

8.1 伦敦行动计划

美国联邦贸易委员会（FTC）和英国公平贸易办公室于2004年在伦敦主办了国际垃圾信息执法大会，会上形成了《国际垃圾信息执法合作的伦敦行动计划》（LAP）。截至2008年7月，超过25个国家的政府机构和私营部门代表已经签署了该计划。LAP鼓励感兴趣的各方，包括垃圾信息执法机构和私营部门利益相关方，考虑申请加入该组织。

LAP的宗旨是推动国际垃圾信息执法方面的合作，解决与垃圾信息有关的问题，例如在线欺诈、网络钓鱼和散播病毒。通过一份篇幅不长的文件，LAP设定了增进国际针对非法垃圾信息的执法和教育合作的基本工作计划，以建立这些实体之间的关系。该文件不具有约束力，仅要求参与者尽最大努力不断推进工作计划。http://londonactionplan.org/

自成立以来，LAP一直举办年度研讨会，特别是与欧洲垃圾信息管制机构联系网络（CNSA）一起举办的研讨会。2007年10月，LAP和CNSA与反信息滥用工作组（MAAWG）会议在弗吉尼亚州的阿灵顿市同期同地举办了年度联合研讨会，从而推动了与私营部门加强执法合作。2008年10月，LAP和CNSA的年度联合研讨会与Eco第六届德国反垃圾信息峰会在德国威斯巴登市同期同地举行。

8.2 OECD垃圾信息工具箱和理事会有关打击垃圾信息的执法合作建议书

2006年4月，OECD垃圾信息任务组发布了反垃圾信息“工具箱”，其中包括相关建议书，以协助政策制定者、监管机构和企业制定垃圾信息解决方案的有关政策，重新树立对互联网和电子邮件的信心。工具箱包含反垃圾信息规则、业界推动的解决方案、反垃圾信息技术、教育和意识普及以及全球合作/扩展等八个部分。认识到国际合作对于打击垃圾信息十分关键，OECD成员国政府还批准了“打击垃圾信息执法行动中跨国合作建议书”，其中敦促各国确保本国法律允许执法部门快速有效地与其他国家共享信息。参见：http://www.oecd-antispam.org/sommaire.php3

8.3 APEC TEL垃圾信息研讨会

2006年4月，APEC TEL举办了“垃圾信息和相关威胁”研讨会，三十位演讲者和专题讨论小组成员汇集一堂讨论垃圾信息问题并为TEL制定了共同的行动议程，其中包含如下议题：

1) 建立和实施国家反垃圾信息监管机制，包括执法和行为准则；
2) 行业在打击垃圾信息中扮演的角色，包括政府 – 行业共同合作；
3) 垃圾信息的技术应对方案；

4) 跨国界合作和执法，并以欧洲理事会的《网络犯罪公约》和OECD理事会的《加强合作建议书》作为推进合作的主要工具；和

5) 有必要举办针对性的用户培训和意识普及活动。

TEL就未来采取的具体步骤达成共识，包括：

1) 鼓励共享法规和政策的相关信息，利用OECD垃圾信息工具箱等资源；

2) 制定一份APEC反垃圾信息部门联系人名单，有效利用OECD和ITU的同类资源；

3) 鼓励经济体加入伦敦行动计划或首尔 – 墨尔本协议等自发性合作论坛；

4) 与OECD就信息共享和指导性举措开展合作；及

5) 支持发展中经济体的能力建设，更好地解决垃圾信息问题。

9 对一些打击垃圾信息的活动的个案研究

本节介绍了一些国家打击垃圾信息的活动。

9.1 美国

9.1.1 美国法律规定对商业性电子邮件发送者的要求（“CAN-SPAM法”）

2003年，美国颁布了《未经要求的色情及营销信息攻击控制法》（简称“CAN-SPAM法”），其中规定了对商业性电子邮件发送者的要求、详细列出了垃圾信息发送者和以垃圾信息推销产品的公司如违反法律将受到的惩罚，并赋予消费者要求发件人终止不当行为的权利。

CAN-SPAM法的主要条款包括：

- **禁止虚假或误导性的标题信息**。邮件的“发件人”、“收件人”和路由信息（包括起始域名和电子邮件）必须准确无误，并能由此识别最先发送该邮件的人。
- **禁止欺骗性的主题**。主题栏不得误导收件人对邮件信息或主题的理解。
- **要求邮件为收件人提供“停止接收”的选择**。发件人必须提供回复邮件的地址或其它给予互联网的应答机制，收件人能够借以要求发件人以后不再向其邮件地址发送信息，发件人必须尊重这一要求。发件人可以提供选择“菜单”，供收件人选择停止接收某类信息，但发件人必须提供一种可以阻断来自该发件人的所有商业信息的选择。选择停止接收的机制必须能够在商业性邮件发出后至少30天内即可处理“停止接收”的要求。自收到“停止接收”的要求起，按法律规定发件人有10个工作日的时间以终止继续向要求人发送邮件。不得协助另一实体或由另一实体代替原发件人继续向该邮件地址发送邮件。最后，不得出售或转让（包括以邮件列表的形式）已选择“停止接收”的收件人的电子邮件，转让电子邮件以确保另一实体遵守法律规定的情况除外。
- **要求商业性邮件包含广告识别信息以及发件人有效的邮寄地址**。发件人的信息必须包含清晰显眼的通知，说明该信息为一则广告或招揽性文字且收件人可以选择停止从发件人接收此类商业性邮件。信息还必须提供发件人的有效邮寄地址。

联邦贸易委员会（FTC）被授权使用其民事法执法权推行CAN-SPAM法，并对每项违法行为最高处以11 000美元的罚金。自1997年FTC针对未经要求的商业电子邮件（或“垃圾信息”）首次开始执法行动以来，通过94次执法行动（其中有31次是CAN-SPAM法所针对的违法者），FTC对欺骗性和不道德的垃圾信息行为进行了积极的追剿。

CAN-SPAM同时授权司法部（DOJ）执行有关刑事判决的权力。CAN-SPAM法规定了严厉的刑事处罚措施，包括垃圾信息发送者的刑期。其它联邦和州级部门可依其司法管辖权执行法律，提供互联网接入的公司也可以起诉违法者。

9.1.2 禁止向无线设备发送商业性电子邮件的条例

美国还通过了多项条例，保护消费者的无线设备免于收到未经要求而自行发送的商业性信息（垃圾信息）。这些条例禁止向手机等无线设备发送商业性电子邮件信息，包括电子邮件和某些文本信息，但规定了一些特殊情况。这些条例仅适用于符合《未经要求的色情及营销信息攻击控制法》（简称“CAN-SPAM法”）中“商业性”定义的信息，以及主要目的在于商业广告或促销商业性产品或业务的信息。非商业性信息，例如公共机构候选人员或更新现有客户账户的信息不适用这些条例。

移动业务商业性信息（MSCM）可以包括向移动业务提供商提供的电子邮件地址发送的、最终送达用户无线设备的任何商业性信息。除非收件人个人事先明确授权发件人（即所谓的“选择接收”要求），否则禁止发送MSCM。在发件人知道该信息将发送至移动设备的情况下，如地址中包含至少于30天前纳入FCC列表的域名，则不得向该地址发送任何商业性信息。为协助商业性信息发送者识别属于无线用户的地址，条例要求无线业务提供商向联邦通信委员会（FCC）提供相关的邮件域名信息。仅向手机号码发送的短信息（SMS）不在这些法规的保护范围之内，但自动拨号呼叫受其它法律管辖。

根据FCC的条例，FCC可对无照垃圾信息发送者每次违规行为处以11 000美元以下的罚款，而对公共传播牌照持有者处以130 000美元以下的罚款。除罚款外，对于违反《通信法》或该法授权FCC发布的任何法规的行为，FCC可命令垃圾信息发送者停止其行为。另据《通信法》规定，违反该法条款的任何人（除交纳罚款外）将由司法部追究其刑事责任，并可能被处以1年以下的有期徒刑（累犯可处两年以下有期徒刑）。到目前，FCC还未就此类商业信息启动任何执法程序。

9.1.3 限制网络钓鱼的方法

正如上文所述，垃圾信息制造者和网络钓鱼者利用的一个基本条件是人们对发件人的无知。互联网工程任务组（IETF）已发布两项标准–域密钥识别邮件（DKIM）[b-IETF RFC 4871]和作者域发送惯例（ADSP）[b-IETF RFC 5617]可提高收件人确定发件人的能力。厂商已开始向客户提供实施成果。该标准至少免费实施一次[17]。反网络钓鱼工作组（APWG）可以提供帮助。这是一个行业协会，其工作重点是消除因日益猖獗的网络钓鱼和电子邮件欺骗所造成的身份盗窃和欺诈问题。该机构提供了一个可讨论网络钓鱼问题、尝试和评估潜在技术解决方案并访问网络钓鱼事件中央数据库的论坛http://www.antiphishing.org/index.html。

这份标准能够实现“白名单认证”或证明是否真是您的银行或朋友或同事在与您联系（举例而言）的能力。该标准本身就能对一些形式的网络钓鱼（并非所有）造成限制。

9.2 日本

9.2.1 执法

日本有两项通过限制电子邮件发送来抑制垃圾邮件的法律。主要内容如下。

- 下列原则对通过电子邮件发送广告信息的情况适用。（许可式）
  - 禁止未经收件人同意使用电子邮件发送广告信息的情况适用。
  - 要求发件人机构向收件人发送广告邮件时必须持有收件人同意的证据。
  - 广告邮件需提供有关如何停止发送广告邮件的程序的信息、寄件人的姓名等。
  - 如收件人使用正确的程序通知该机构不希望收到广告邮件，则该机构就不能再向其发送任何广告邮件。
- 禁止在发送电子邮件时使用伪造的发件人信息，如，电子邮件地址、IP地址和域名。
- 禁止向计算机程序自动生成的虚构收件人地址发送电子邮件。

---

17 “免费”在此指有能力按照专利持有者规定的条件在免交使用费的情况下实施该功能。

9.2.2 反垃圾邮件措施促进委员会

各有关方面，如互联网服务提供商（ISP）、广告商、发送广告邮件的应用服务提供商（ASP）、安全厂商、消费者组织、主管部门等在2008年成立了反垃圾邮件措施促进委员会。委员会于2008年11月通过了“根除垃圾邮件宣言”。

9.2.3 网络清洁中心（CCC）

网络清洁中心（CCC）是由日本政府、ISP相关组织和主要ISP密切合作创建的，负责查找感染僵尸的电脑。该中心的工作程序如下。

– CCC管理着大型蜜罐系统（honey pot system），接收来自恶意软件（通常为僵尸）感染的电脑的感染活动。蜜罐系统收集感染电脑的IP地址和恶意软件（僵尸）的程序代码。

– 将IP地址清单及其被探测到的日期/时间发送给每个ISP。ISP确定这些IP地址的用户，并通知他们电脑可能被恶意软件感染的情况。ISP还向其发送有关CCC的信息（链接到网页）和杀毒软件。

– CCC对收集到的程序代码进行分析。如该程序代码是尚未确定的代码，则将制作并发布可以查杀这个新的恶意程序代码的新的杀毒软件。

这项活动有助于遏制日本的僵尸感染。由于大多数垃圾邮件都来自被僵尸感染的电脑，也有助于减少日本的垃圾邮件发送。

9.2.4 出局端口25阻止（OP25B）

当ISP用户发送和接收电子邮件信息时，他们使用了由ISP提供的电子邮件服务。因此用户将电子邮件发送至ISP的邮件服务器，ISP的邮件服务器再将邮件传递到目的地电子邮件服务器。ISP用户通常不是将电子邮件直接发送到目的地电子邮件服务器。由于僵尸或病毒感染的电脑将垃圾邮件直接发送到目的地地址的电子邮件服务器，此类电子邮件不经过ISP的邮件服务器。如能够阻止用户电脑使用简单邮件传输协议（SMTP）（目标端口号为25的TCP）绕过ISP网络的通信，则就可以屏蔽掉许多垃圾邮件。因此，日本政府、ISP及相关机构密切合作对下列问题进行了研究。

– 引入出局端口25阻止（OP25B）[b-MAAWG MP25]的TCP后对用户的影响。

– 根据日本现行法律拦截具体通信的限制。

经研究，许多ISP在下列活动中应用了OP25B。JEAG（日本反电邮滥用组织）在其中发挥了重要作用，它出版了一项建议书，敦促ISP引入OP25B。

– 虽然对日本ISP而言，OP25B的引入并不是强制性的，但52家ISP（几乎包括所有主要ISP）都已于2009年7月前引入了OP25B。

– 已引入OP25B的许多ISP在TCP端口587提供SMTP AUTH，作为一种替代的通信方式，以防止服务质量的下降。用户可以将来自与OP25B兼容的其他ISP的邮件提交此类ISP的邮件服务器。

9.2.5 发件人身份验证技术

发件人身份验证技术是检测电子邮件源地址欺骗的技术。JEAG出版了一份建议书介绍这些技术，总务省发出一份题为“ISP在接收端引入发件人身份验证的重要法律问题”的文件。目前，几乎所有主要的移动通信运营商和一些互联网服务提供商都引入了发件人策略框架（SPF）[b-IETF RFC 4408]，这是发件人身份验证技术的一种，用户可利用验证结果进行过滤。2009年8月，已公布的SPF针对域名“jp”的记录是35.99%。另外一些ISP已开始引入DKIM[b-IETF RFC 4871]作为进一步的发件人身份验证手段。

9.2.6 移动通信运营商之间有关垃圾邮件发送者信息的交流

在日本，几乎所有蜂窝电话都有处理一般电子邮件信息的能力。由于许多垃圾邮件是由移动蜂窝电话发送的，日本所有移动通信运营商通过以下步骤交流有关垃圾邮件发送者的信息。

– 根据“移动电话不当使用防治法（Mobile Phone’s Improper Use Prevention Act）”对任何欲签订移动电话合同的个人的身份进行检查。

– 如移动通信运营商发现一个蜂窝电话用户违反“特定电子邮件传送管理法（Act on Regulation of Transmission of Specified Electronic Mail）”发送垃圾邮件，则将该用户信息提供给其他所有移动通信运营商。

因此，如一用户用蜂窝电话发送垃圾邮件信息，那么该用户在日本将很难成为移动电话的合同用户。

一个相关的非营利组织通过设置传感器，对垃圾邮信息进行收集和分析。它向日本的发送源ISP提供垃圾邮件发送者的有关资料，并与国外一些机构进行此类信息交流。

参考资料

[b-IETF RFC 4871] IETF RFC 4871（2007年），域密钥识别邮件（DKIM）签名。（*Domainkeys Identified Mail*）

http://www.ietf.org/rfc/rfc4871.txt

[b-IETF RFC 5617] IETF RFC 5617（2007年），域密钥识别邮件（DKIM）作者域发送惯例（ADSP）（*Author Domain Signing Practices*）

http://www.ietf.org/rfc/rfc5617.txt

[b-MAAWG MP25] MAAWG建议书（2005年），管理住宅或动态IP空间端口25 – 采用的好处和无谓的风险。（*Managing Port 25 for Residential or Dynamic IP Space Benefits of Adoption and Risks of Inaction*）

http://www.maawg.org/port25

[b-IETF RFC 4408] IETF RFC 4408（2007年），在电子邮件中授权域名使用的发件人策略框架（SPF）（*Sender Policy Framework (SPF) fo Authorizing Use of Domains in E*-Mail）版本1。

http://www.ietf.org/rfc/rfc4408.txt

[b-contr-spam] 《未经要求的色情及营销信息攻击控制法（2003年）》（美国法规）。该法案记录在以下法律中： 15 U.S.C. §§ 7701-7713；18 U.S.C. § 1037；28 U.S.C. § 994；47 U.S.C. § 227。

http://www.gpsaccess.gov/uscode/index.html

[b-ITU-T cyb] 反信息滥用工作组大会报告：

http://www.itu.int/ITU-D/cyb/cybersecurity/spam.html 。

附件B

身份管理

国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X系列

增补 7

（02/2009年）

X系列：数据网、开放系统通信和安全性

关于网络安全中身份管理概述的增补

注意！

预出版的建议书

本预出版的建议书是近期获批但未编辑的建议书版本。编辑后出版的版本将取代本版本。因此，预出版版本和最终出版版本之间将存在差异。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准ITU-T建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

X系列建议书增补7 – ITU-T X.1250 – 系列

关于网络安全中身份管理概述的增补

摘要

传统的公用电路交换电信网（PSTN）安全已经历了几十年的运行考验，但涉及多个服务提供商的分布式公用分组交换网（如，互联网和下一代网络（NGN））却不能同日而语。这类网络使用共同的传输平台控制流量和用户流量，加上IP流量可以匿名发送，并且可能产生单向流量，使得这类网络容易受到不良使用。所有电子服务（如电子企业、电子商务、电子卫生、电子政务等电子服务）都可能受到攻击。确定使用者、网络设备和服务提供商就能对其认证，给予适当接入权并予以审计，这样至少可使该问题得到部分解决。由于身份管理为用户、服务提供商和网络设备身份提供更高的保障和信任，因此可通过减少安全风险改善网络安全。这一网络安全问题是服务提供商在业务和技术层面及政府在国家层面作为国家网络安全计划一部分需考虑的问题。

引言

身份管理（IdM）是一种管理、控制用于代表实体（如服务提供商、最终用户组织、人、网络设备、软件应用和服务）通信过程中的信息的方式。一个实体可能具备多重身份属性以便按不同安全要求获得多样服务，而这些服务可能设在多个地方。

IdM是网络安全的关键组成部分，因为它提供了在各实体之间建立并保持可信赖的通信和网络的能力。它不仅支持对实体身份的认证，还可以在一定范围内授权接入特权（而不是百分百的接入）并随着实体角色的变化而轻而易举地改变接入等级。IdM通过检测并审计实体的接入活动使机构确保其安全政策得到适当落实。IdM可向组织内外实体提供接入，而不损失安全或暴露敏感信息。简而言之，一个良好的IdM解决方案可以提供支持身份认证、提供和管理的能力，并审计实体的活动。

IdM是管理安全和实现信息社会最终用户所期待的移动式、随需网络接入和电子服务的关键因素。除其它防御机制（如防火墙、入侵检测系统、防病毒）外，IdM在保护信息和通信网络及服务免受欺诈和身份盗窃等网络犯罪中发挥至关重要的作用。这将提高使用者对电子交易安全性和可靠性的信心，从而推进IP网络在电子服务中的使用。

在实施IdM系统过程中，必须解决基本的隐私问题，即开发方法保证身份信息准确，并防止身份信息用于除收集以外的目的。

1 范围

身份管理已经成为网络安全的关键组成部分，通过验证身份信息的有效性提供更高的保障，从而改善网络的安全性。本增补概要介绍了这种新服务。

本增补中所用的涉及IdM的“身份”一词并非指其纯粹含义。特别是它不构成任何肯定的验证。

2 参考

无

3 定义

定义见其他X.1250系列建议书。

4 缩略语

IdM – 身份管理

IP – 网际协议

PSTN – 公用交换电话网

5 惯例

无

6 IdM对于全球网络基础设施保护和安全跨国协调的重要性

IdM能力及其在不同国家、区域和国际网络中的实施和使用将加强全球网络基础设施的安全保障。IdM最佳做法及实施对于提供身份信息保障和保护全球网络基础设施的完整性及可用性是十分重要且必不可少的。

IdM能力可通过辨别授权使用专项服务的用户支持国家和国际应急通信业务。

此外，IdM能力可用来防止、检测国家和国际网络安全事件，并支持协调对这些事件做出的响应。在某些情况下，IdM可帮助主管机构和实体协调其跟踪和定位这类事件发源地的工作。

7 身份管理促成两实体间的可信任通信

IdM的一个重要功能是支持对用户、网络或服务的认证。在涉及两个实体的认证过程中，一个实体向另一实体表明身份。根据第二个实体的安全要求，第二个实体可能需要验证这些表明方可充分信任第一个实体并授予特权。该过程是双向的。

认证信任分许多级别，从低或无，弱（如用户名和密码）到强（如公钥基础设施（ITU-T X.509））。进行风险评估可以确定适用的认证等级。某个实体可能需要比另一实体更高的认证等级，比如说，因为这一实体掌握着关键信息源。

8 身份数据的保护、维护、撤销和控制

IdM的其它重要功能包括保护、维护和控制可信赖的身份数据。

法律或政策可要求保护个人可识别的信息，防止身份信息用于信息收集以外的目的。确保身份信息继续有效是另外一个备受关注的问题。使用身份信息的服务若想得到持续发展，身份信息必须得到正确维护，使其准确、及时、一致。

必要时，身份数据属性管理应支持核对身份数据是否已经撤销的能力。

在很多情况下，实体将要求控制其自我数据和私密信息的使用。

9 身份数据的可信任来源的“发现”

IdM还包含可信任身份数据“发现”的概念。在一个高度分布式、多提供商环境（如互联网和下一代网络）中，提供身份信任和某个实体的相关表明所必需的身份数据可能放在网络的任何地方。各实体可能在不同地方拥有不同身份提供方给予的多重数字身份。在认证过程中，当两个实体中的一个处于移动状态时，另一实体可能需要定位并与相关身份提供方建立信任关系，从而完成认证移动实体的过程。发现可信任信息来源的概念与目前的移动蜂窝电话所使用的程序异曲同工。

10 电子政务（e-Government）

实施IdM为实体带来的好处包括减少风险、加强信任、提高功能性并可能降低成本。当实体为政府时，这些优势同样适用。对于电子政务，其主要目标依然是降低成本并向政府所属公民和企业伙伴提供更加高效而有效的服务。

与其它服务提供商相同，政府面临着如何有效和高效利用网络世界中的身份的问题。为实现电子政务，政府必须对其打算提供的电子服务进行风险分析并实施适当的保护措施。很多电子政务业务（例如电子医疗）的敏感特性需要政府进行强有力的认证。

11 与IdM相关的监管考虑

政府主管部门和区域组织须考虑很多与IdM实施相关的潜在监管问题，如隐私和数据保护、国家安全和应急准备以及运营商之间的强制结付。政府不仅利用身份管理技术，更应强制要求其他实体使用这类技术，以达到国家政策和安全目标的广泛实现。

参考资料

很多论坛都在围绕IdM问题开展工作。这些论坛包括：

ARK（加州数字图书馆档案资源密钥）：http://www.cdlib.org/inside/diglib/ark/

ETSI/3GPP：http://www.3gpp.org/SA3-Security?page=type_urls

ETSI TISPAN：http://www.etsi.org/tispan/

欧盟eID路线图：
http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf

欧洲公民卡：http://europa.eu.int/idabc/servlets/Doc?id=19132

FIDIS（欧盟信息社会未来身份）：http://www.fidis.net/

FIRST（事件响应论坛和安全组织）：http://www.first.org/

Guide（欧盟面向欧洲的政府用户身份）：http://www.ist-world.org/ProjectDetails.aspx?ProjectId=4ddb2e61c84343f0acd370607e5a8499&SourceDatabaseId=7cff9226e582440894200b751bab883f

Handle：http://www.handle.net/

Higgins：http://www.eclipse.org/higgins/index.php

IDSP（美洲国家标准学会预防身份盗窃和身份管理标准委员会（IDSP））：
http://www.ansi.org/standards_activities/standards_boards_panels/idsp/overview.aspx?menuid=3

IGF（ORACLE身份治理框架）：http://www.oracle.com/technology/tech/standards/idm/igf/index.html

ITRC（身份盗窃资源中心）：http://www.idtheftcenter.org/

互联网工程任务组：http://sec.ietf.org/

ITU-T第17 研究组（安全）身份管理焦点组：www.itu.int/ITU-T/studygroups/com17/fgidm/index.html

ITU-T第17研究组(安全)第10号课题：

http://www.itu.int/ITU-T/studygroups/com17/index.asp

ITU-T第13研究组（下一代网络）第13号课题：http://www.itu.int/ITU-T/studygroups/com13/index.asp

自由联盟项目：http://www.projectliberty.org/

简化身份：http://lid.netmesh.org/wiki/Main_Page

MODINIS-IDM企业集团：http://www.egov-goodpractice.org和
https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium

国家身份卡方案：http://www.homeoffice.gov.uk/passports-and-immigration/id-cards/；
http://en.wikipedia.org/wiki/Identity_document

OASIS（结构信息标准推进组织）：http://www.oasis-open.org/home/index.php

OECD（经济合作和发展组织）数字身份管理研讨会，2007年5月8-9日，挪威Trondheim：
http://www.oecd.org/sti/security-privacy/idm.

OMA（开放移动联盟）：http://www.openmobilealliance.org/

开放集团：http://www.opengroup.org

OSIS（开放源代码身份系统）：http://osis.idcommons.net/wiki/Main_Page

PAMPAS（欧盟先进移动隐私和安全先驱（PAMPAS））：http://www.pampas.eu.org/

PERMIS（欧盟信息社会标准化举措（ISIS））PrivilEge和角色管理基础设施标准验证）：http://www.permis.org/

Prime（欧盟针对欧洲的隐私和身份管理）：https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium

W3C（世界万维网企业集团）：http://www.w3.org/

Yadis：http://yadis.org/wiki/Main_Pagehttp://yadis.org/wiki/Main_Page

附件C

链接和参考文件

此参考资料单将定期更新，以便考虑到《国际电联全球安全议程》的输出文件和落实第45号决议（WTDC-06）项目的输出成果、ITU-T第17研究组（ITU-T安全问题牵头研究组）开展的工作、相关WTSA决议、有关网络安全的WSIS C5行动方面的后续工作以及诸如2006年全权代表大会第130号、131号和149号决议等各相关决议方面的工作。

第一部分：就国家网络安全战略寻求并达成共识

I.C.1 提高意识（I.B.1，I.B.2）

国际层面

- 联合国大会有关“打击违法滥用信息技术”的第55/63号决议：
  http://www.un.org/Depts/dhl/resguide/r55.htm
- 联合国大会有关“打击违法滥用信息技术”的第56/121号决议：
  http://www.un.org/Depts/dhl/resguide/r56.htm
- 联合国大会有关“培育全球网络安全文化”的第57/239号决议：
  http://www.un.org/Depts/dhl/resguide/r57.htm
- 联合国大会有关“培育全球网络安全文化和保护关键信息基础设施”的第58/199号决议：
  http://www.un.org/Depts/dhl/resguide/r58.htm
- 联合国信息社会世界高峰会议（WSIS）《日内瓦原则宣言》和《行动计划》及《突尼斯承诺》和《信息社会行动计划》：
  http://www.itu.int/WSIS/index.html
- 经济合作与发展组织（OECD）信息系统和网络安全导则：建设安全文化（2005年）：
  http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html
- 国际关键信息基础设施保护2006年手册（卷1）：
  http://www.isn.ethz.ch/pubs/ph/details.cfm?id=250
- 国际电联网络安全相关资料库：http://www.itu.int/cybersecurity/
- 国际电联全球网络安全议程： http://www.itu.int/cybersecurity/gca/
- 国际电联网络安全门户网站： http://www.itu.int/cybersecurity/gateway/
- 国际电联发展部门网络安全网页： http://www.itu.int/ITU-D/cyb/
- 国际电联保护在线儿童举措及相关指导方针：http://www.itu.int/cop/

I.C.2 国际、区域和国家战略（I.B.2、I.B.3、I.B.4、I.B.5和I.B.7）

国际层面

- 国际电联国家网络安全/关键信息基础设施保护（CIIP）自我评估工具包：
  http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
- 国际电联和ETH苏黎世 – CIIP总体国家框架：
  http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

- 国际电联电信发展部门第22/1课题研究组：保障信息和通信网络的安全：培育网络安全文化的最佳做法： http://www.itu.int/ITU-D/study_groups/SGP_2006-2010/documents/DEFQUEST-SG1/DEFQUEST-Q22-1-E.pdf
- 国际电联全球网络安全议程：http://www.itu.int/cybersecurity/gca/
- 国际电联发展中国家网络安全指南（2009年修订版）：http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf
- 国际电联WTDC第45号决议：关于加强在网络安全、打击垃圾邮件等领域合作的机制（2006年，多哈）；http://www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf
- 国际电联电信标准化部门第17研究组，第4号课题概览-已批准的与电信安全有关的 ITU-T建议书目录：http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D0000090003MSWE.doc
- 国际电联电信标准化部门第17研究组第4号课题-《安全手册》：http://www.itu.int/pub/T-HDB-SEC.03-2006/en/
- 国际电联电信发展局有关网络安全的经济方面的研究：恶意软件和垃圾信息：http://www.itu.int/ITU-D/cyb/presentations/2008/bauer-financial-aspects-spam-malware-april-2008.pdf
- 经济合作与发展组织（OECD）信息系统和网络安全指导原则：迈向安全文化：http://www.oecd.org/document/42/0,3343,en_21571361_36139259_15582250_1_1_1_1,00.html
- OECD协同国家网上安全政策实施计划：http://www.oecd.org/dataoecd/23/11/31670189.pdf
- 世界银行报告“网络安全：保护网络的新模式”：http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2006/12/12/000020953_20061212113151/Rendered/PDF/381170CyberSec1uly0250200601PUBLIC1.pdf
- 美国信息技术协会（ITAA）关于信息安全的白皮书：http://www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf

区域层面

- APEC电信和信息工作组 – APEC网络安全战略（2002年）：http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf
- CITEL蓝皮书：美洲国家电信政策（2005年）第8.4-8.5条：http://www.citel.oas.org/publications/azul-fin-r1c1_i.pdf
- 欧盟理事会的决议：安全的信息社会战略– 对话、伙伴关系和授权（2007年）：http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf
- 《有关网络安全的多哈宣言》（2008年）：http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-regional-cybersecurity-forum-output-20-feb-08.pdf
- 欧盟关于“安全的信息社会战略”的通报（2006年）：http://ec.europa.eu/information_society/doc/com2006251.pdf
- 欧盟更安全的互联网项目：http://europa.eu.int/information_society/activities/sip/index_en.htm
- 欧洲网络和信息安全局（ENISA）委托的研究“安全经济学和内部市场”（2008年）：http://www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm
- 美洲国家组织：打击网络安全威胁的美洲国家战略 （2004年）：http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

国家层面

- 澳大利亚关键基础设施保护建模和分析项目（CIPMA）：http://www.csiro.au/partnerships/CIPMA.html
- 危机和风险网络（CRN）国际CIIP手册：国家保护政策目录和分析：http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250
- 德国关于信息基础设施保护的国家规划：http://www.en.bmi.bund.de/cln_028/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure__Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.pdf
- 日本关于信息安全的国家战略（暂译）：http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf
- OECD 11个成员国的实施战略：http://www.oecd.org/document/63/0,2340,en_21571361_36139259_36306559_1_1_1_1,00.html
- 新西兰数字战略： http://www.digitalstrategy.govt.nz
- 新加坡信息通信安全总规划2：http://www.ida.gov.sg/doc/News%20and%20Events/News_and_Events_Level2/20080417090044/MR17Apr08MP2.pdf
- 新加坡保护网络空间的战略：http://www.ida.gov.sg/News%20and%20Events/20050717164621.aspx?getPagetype=21
- 英国国家基础设施保护中心（CPNI）：http://www.cpni.gov.uk/
- 美国保障网络安全的国家战略：http://www.whitehouse.gov/pcipb/

I.C.3 评估和项目开发（I.B.5、I.B.7和I.B.8）

- “信息与相关技术控制目标（COBIT）”4.1：http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981（免费提供摘要；下载全文需注册）
- 信息技术基础设施图书馆（ITIL）安全管理：http://www.itil-itsm-world.com/（需付费）
- 国际标准化组织/国际电工委员会（ISO/IEC）27000系列，“信息技术-安全技术-信息安全管理系统”：http://www.iso27001security.com/index.html
- ISO/IEC 13335，“信息技术-安全技术-信息通信技术安全管理-第1部分：信息和通信技术安全管理的概念与模式”：http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39066（需付费）
- ISO/IEC 17799，2005年“信息技术-安全技术-信息安全管理操作规则”：http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612（需付费）
- ISO/IEC 21827，“系统安全工程-性能成熟模型”（SSE-CMM®）：http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34731（需付费）
- 国际电联电信发展局有关网络安全的经济方面的研究：恶意软件和垃圾信息：http://www.itu.int/ITU-D/cyb/presentations/2008/bauer-financial-aspects-spam-malware-april-2008.pdf

- 国际电联WTSA第50号决议：网络安全（2008年，约翰内斯堡，修订版）：http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf
- 国际电联WTSA第52号决议：抵制和打击垃圾信息（2008年，约翰内斯堡，修订版）：http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf
- 国际电联WTSA第58号决议：重点鼓励发展中国家建立国家计算机事件响应组（2008年，约翰内斯堡）：http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.58-2008-PDF-E.pdf
- NIST特刊（SP）800-12，“计算机安全绪论：NIST手册”（1996年2月）：http://csrc.nist.gov/publications/nistpubs/800-12/
- NIST特刊800-30，“信息技术系统风险管理指南”（2002年7月）：http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- NIST 特刊800-53，“联邦信息系统推荐的安全控制措施”（2007年12月）：http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
- NIST特刊800-53A草案，“联邦信息系统安全控制的评估指南”（2007年12月）：http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-53-A
- NIST特刊800-50，“建立信息技术安全意识和技术项目”（2003年10月）：http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
- NIST特刊800-30，信息技术系统风险管理指南，（2002年7月）：http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- 可操作的关键威胁、资产和弱点评估SM（OCTAVESM）：http://www.cert.org/octave/

I.C.4 国际援助联系人（I.B.6）

- 反网络钓鱼工作组（APWG）：http://www.antiphishing.org
- 事件响应安全组织论坛（FIRST）：http://www.first.org
- 电气与电子工程师学会：http://www.ieee.org
- 互联网工程任务组：http://www.ietf.org
- 反信息滥用工作组：http://www.maawg.org
- 世界信息技术服务联盟：http://www.witsa.org
- 万维网联盟：http://www.w3c.org

第二部分：建立国家政府 – 行业的合作关系

II.C.1 政府 – 行业合作关系的结构

国际层面

- 网络安全行业联盟：http://www.csialliance.org/about_csia/index.html
- OECD 反垃圾信息工具包 – 反垃圾信息的合作性伙伴关系：http://www.oecd-antispam.org/article.php3?id_article=243
- 反垃圾信息联盟：http://stopspamalliance.org/

区域层面

- 中东：第14届海湾阿拉伯国家合作委员会电子政务和电子服务论坛：
http://www.zawya.com/Story.cfm/sidZAWYA20080529073202/SecMain/pagHomepage/chnAll%20Regional%20News/obj2A17E941-F5E0-11D4-867D00D0B74A0D7C/

国家层面

- 澳大利亚企业-政府伙伴关系：关键基础设施保护信托信息分享网络：
http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/CIPPrograms_CriticalInfrastructureProtectionModellingandAnalysis(CIPMA)
- 美国信息交流和分析中心（ISAC）和协调协会
  - 金融服务ISAC：http://www.fsisac.com/
  - 电气部门ISAC：http://www.esisac.com/
  - 信息技术ISAC：http://www.it-isac.org
  - 电信ISAC：http://www.ncs.gov/ncc/
  - 网络可靠性和互操作性协会（NRIC）：http://www.nric.org/
  - 国家安全和电信咨询委员会（NSTAC）：http://www.ncs.gov/nstac/nstac.html
- 美国行业-政府间的标准合作：美国国家标准学会-国土安全标准小组：
http://www.ansi.org/standards_activities/standards_boards_panels/hssp/overview.aspx?_menuid=3
- 美国信息技术协会信息安全白皮书：
http://www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf
- 美国IT行业协调委员会（SCC）：http://www.it-scc.org
- 美国国家网络安全伙伴关系：http://www.cyberpartnership.org/
- 美国国家信息保障协会（NIAC）关于部门合作关系模式工作组的报告：
http://itaa.org/eweb/upload/NIAC_SectorPartModelWorkingGrp_July05.pdf
- 美国国家基础设施保护计划：http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm
- 美国针对行业的计划：http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm
- 美国针对IT行业的计划：http://www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf
- 美国国家电信与信息主管部门：http://www.ntia.doc.gov/

II.C.2 网络安全信息共享

国际层面

- 反信息滥用工作组：http://www.maawg.org

国家层面

- 美国国家标准与技术研究所（NIST），计算机安全与研究中心：http://csrc.nist.gov/
- 美国计算机紧急应变小组（US-CERT）国家网络报警系统：http://www.us-cert.gov/cas/

II.C.3 认识的提高与对外宣传：政府和企业用工具

国际层面

- 建立安全意识项目：http://www.gideonrasmussen.com/article-01.html
- 互联网安全中心企业安全资料和出版物：http://www.cisecurity.org/resources.html
- 企业的安全意识战略：http://articles.techrepublic.com.com/5100-10878_11-5193710.html
- 小企业网络安全常识指南：http://www.uschamber.com/publications/reports/0409_hs_cybersecurity.htm
- EDUCAUSE政府和行业安全意识资料库：http://www.educause.edu/Security%20Task%20Force/CybersecurityAwarenessResource/BrowseSecurityAwarenessResourc/8770?time=1215527945
- ENISA 信息安全意识举措（可提供多种语言版本）：http://www.enisa.europa.eu/Pages/05_01.htm
- 国际刑警组织IT安全和犯罪预防方法（防止企业中的犯罪）：http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp
- 国际刑警组织IT违法公司名录：http://www.interpol.int/Public/TechnologyCrime/CrimePrev/companyChecklist.asp
- 公告板安全意识海报：http://www.noticebored.com/html/posters.html
- OECD反垃圾信息工具包–教育和意识：http://www.oecd-antispam.org/article.php3?id_article=242
- SANS安全政策资料库：http://www.sans.org/resources/policies/
- 安全意识工具箱 – 信息战争网站：http://www.iwar.org.uk/comsec/resources/sa-tools/
- 美国国家网络安全伙伴关系 – 小企业和小企业资料中心的意识：http://www.cyberpartnership.org/init-aware.html

国家层面

- 美国联邦贸易委员会：http://www.ftc.gov/infosecurity
- NIST 800-50安全意识和培训计划：http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

第三部分：遏制网络犯罪/法律基础和执法情况

国际层面

- 欧洲理事会：《网络犯罪公约》（2001年）：http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp
- G-8高科技犯罪原则：http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html
- 国际电联与国家法律方法统一、国际法律协调和执法相关的背景材料http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
- 国际电联/InfoDev ICT规则工具包：http://www.ictregulationtoolkit.org/
- 国际电联关于认识网络犯罪的出版物：发展中国家指南：http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html
- 国际电联网络犯罪立法工具包：http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html
- 国际警察组织信息技术犯罪资料库：http://www.interpol.com/Public/TechnologyCrime/

- OECD反垃圾信息监管方法：http://www.oecd-antispam.org/article.php3?id_article=1
- OECD反垃圾信息工具包：http://www.oecd-antispam.org/article.php3?id_article=265
- 联合国大会关于“打击违法滥用信息技术”的第55/63号决议：http://www.un.org/Depts/dhl/resguide/r55.htm
- 联合国大会关于“打击违法滥用信息技术”的第56/121号决议：http://www.un.org/Depts/dhl/resguide/r56.htm
- 联合国区域间犯罪和司法研究所（UNICRI）善用知识并建立新的伙伴关系打击网络犯罪资料库：http://www.unicri.it/
- 联合国国际贸易法委员会（UNCITRAL）电子签名示范法：http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html
- 联合国毒品和犯罪办公室资料库：http://www.unodc.org/

区域层面

- 亚太经济合作组织与网络犯罪有关的文件及领导人和部长声明：http://www.apectelwg.org/
- 网络犯罪大会《开罗宣言》：http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_EN.pdf
- 有关计算机和计算机相关犯罪的共同体示范法：http://www.thecommonwealth.org/Internal/38061/documents/
- 欧洲理事会：《网络犯罪公约》（2001年）：http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp
- 美洲国家组织：美洲国家网络犯罪合作门户：http://www.oas.org/juridico/english/cyber.htm

国家层面

- CERT/CC：联邦调查局如何调查计算机犯罪：http://www.cert.org/tech_tips/FBI_investigates_crime.html
- 网络犯罪法律（Cybercrimelaw）：全世界网络犯罪立法调查：http://www.cybercrimelaw.net/index.html
- 欧洲理事会：各国网络犯罪立法调查：http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/Legprofiles.asp#TopOfPage
- 微软：“亚太地区立法分析：现有和待批准的网络安全和网络犯罪法律”：http://www.itu.int/ITU-D/cyb/cybersecurity/docs/microsoft_asia_pacific_legislative_analysis.pdf
- OECD成员国有关反垃圾信息的法律：http://www.oecd-antispam.org/countrylaws.php3
- 联合国“西亚经济和社会委员会（ESCWA）成员国的网络立法模式”：http://www.escwa.un.org/information/publications/edit/upload/ictd-07-8-e.pdf
- 美国司法部（USDOJ）计算机犯罪与知识产权处网站：http://www.cybercrime.gov
- 美国司法部（USDOJ）计算机犯罪起诉手册（第1章 – 计算机诈骗和滥用法案）：http://www.cybercrime.gov/ccmanual/
- 美国特勤局 – 掌握电子证据的最佳做法：http://www.forwardedge2.com/pdf/bestPractices.pdf

第四部分：创建国家层面的事件管理能力：监控、警告、响应和恢复

IV.C.1 国家响应计划和国家级CSIRT

国际层面

- 卡耐基-梅隆大学/CERT协调中心 （CERT/CC）：http://www.cert.org/csirts/
- CERT/CC：建立CSIRT的行动清单：http://www.cert.org/csirts/action_list.html
- CERT/CC：创建一个CSIRT：启动程序：http://www.cert.org/csirts/Creating-A-CSIRT.html
- 针对CSIRT确定事件管理程序：进展中的工作：http://www.cert.org/archive/pdf/04tr015.pdf
- CERT/CC：CSIRT常见问题：http://www.cert.org/csirts/csirt_faq.html
- CERT/CC：CSIRT手册：http://www.cert.org/archive/pdf/csirt-handbook.pdf
- CERT/CC：事件管理能力衡量标准版本0.1：http://www.cert.org/archive/pdf/07tr008.pdf
- CERT/CC：CSIRT的组织模式：http://www.cert.org/archive/pdf/03hb001.pdf
- CERT/CC：CSIRT的业务：http://www.cert.org/csirts/services.html
- CERT/CC：为贵机构的CSIRT招募人员 – 需要哪些基本技能?：http://www.cert.org/csirts/csirt-staffing.html
- CERT/CC：CSIRT的惯例情况：http://www.cert.org/archive/pdf/03tr001.pdf
- CERT/CC：建立国家CSIRT的步骤：http://www.cert.org/archive/pdf/NationalCSIRTs.pdf
- CERT/CC虚拟培训环境 （VTE）：http://www.vte.cert.org/
- ENISA：CSIRT建立指南：http://www.enisa.europa.eu/pages/05_01.htm
- 国际电联 – IMPACT合作及相关资源：http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html
- GOVCERT.nl：方框中的CSIRT – 有关设立CSIRT的信息：http://www.govcert.nl/render.html?it=69
- 英国CPNI：警告、建议和报告点 （WARP）工具箱：http://www.warp.gov.uk/

区域层面

- 亚太CERT：http://www.apcert.org/index.html
- 欧洲CSIRT网络资料库：http://www.ecsirt.net/
- 欧洲政府CERTs（EGC）集团：http://www.egc-group.org/

国家层面

- 澳大利亚：AusCERT：http://www.auscert.org.au
- 奥地利：CERT.at：http://www.cert.at
- 巴西：CERT.br：http://www.cert.br/
- 智利：CLCERT：http://www.clcert.cl/
- 中国：CNCERT/CC：http://www.cert.org.cn/

- 芬兰：CERT-FI：http://www.cert.fi
- 匈牙利：CERT-Hungary：http://www.cert-hungary.hu
- 印度：CERT-In：http://www.cert-in.org.in
- 意大利：CERT-IT：http://security.dico.unimi.it/
- 日本：JPCERT/CC：http://www.jpcert.or.jp/
- 韩国：KrCERT/CC：http://www.krcert.or.kr/
- 马拉西亚：MyCERT：http://www.cybersecurity.org.my
- 荷兰：http://www.csirt.dk/
- 波兰：CERT POLSKA：http://www.cert.pl/
- 斯洛文尼亚：SI-CERT：http://www.arnes.si/en/si-cert/
- 新加坡：SingCERT：http://www.singcert.org.sg/
- 瑞典：SITIC：http://www.sitic.se
- 瑞士：MELANI：http://www.melani.admin.ch
- 泰国：ThaiCERT：http://www.thaicert.nectec.or.th/
- 突尼斯：CERT-TCC：http://www.ansi.tn/en/about_cert-tcc.htm
- 卡塔尔：http://www.qcert.org
- 阿拉伯联合酋长国：http://aecert.ae/
- 美国国家响应计划：http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml
- 美国CERT：http://www.us-cert.gov/
- 以及其他国家的CERT/CSIRT网站

IV.C.2 合作和信息共享

国际层面

- CERT/CC：安全弱点和修复：http://www.cert.org/nav/index_red.html
- 事件处理工具（CHIHT）交换所：http://chiht.dfn-cert.de/
- 事件响应和安全组织论坛 （FIRST）资料库：http://www.first.org/
- ISP安全支持服务资料库：http://www.donelan.com/ispsupport.html
- 国际电联网络安全网关：与观察、警告和事件响应有关的背景材料：http://www.itu.int/cybersecurity/gateway/watch_warning.html
- 小企业和个人IT安全报警系统：http://www.itsafe.gov.uk/
- OECD：反垃圾信息工具箱：http://www.oecd-antispam.org/article.php3?id_article=265

区域层面

- 跨欧洲研究和教育网络协会（TERENA）：http://www.terena.org/

国家层面

- 荷兰：荷兰国家报警服务：http://www.waarschuwingsdienst.nl/render.html?cid=106
- 英国CPNI：警告、建议和报告点（WARP）工具箱：http://www.warp.gov.uk/
- 美国IT-ISAC：https：//www.it-isac.org/

- 美国IT行业协调委员会（ISCC）：信息技术：针对关键基础设施和重要资源部门的特别计划：http://www.it-scc.org/documents/itscc/Information_Technology_SSP_2007.pdf
- 美国国家标准与技术研究所 （NIST）：http://csrc.nist.gov/

IV.C.3 有关脆弱性的信息/工具和技术

- 内置安全 – 旨在协助创建安全系统的软件保障和安全信息汇编：https://buildsecurityin.us-cert.gov/daisy/bsi/home.html
- 共同的脆弱性和弱点问题一览表（CVE）：http://www.cve.mitre.org/about/
- 开放式脆弱性评估语言（OVAL）：http://oval.mitre.org/
- 美国国家软件脆弱性数据库（NVD）：http://nvd.nist.gov/nvd.cfm

第五部分：推动国家网络安全文化的发展

V.C.1 政府系统和网络（V.B.1、V.B.2和V.B.7）

国际层面

- WSIS《行动计划》C5行动方面：http://www.itu.int/wsis/implementation/index.html
- 国际电联全球网络安全议程：http://www.itu.int/osg/csd/cybersecurity/gca/
- 国际电联WSIS反垃圾信息主题会议：http://www.itu.int/osg/spu/spam/meeting7-9-04/index.html
- WSIS C5行动方面第一次会议，主席的报告：http://www.itu.int/osg/spu/cybersecurity/2006/chairmansreport.pdf
- WSIS C5行动方面第二次会议，《行动计划》：http://www.itu.int/wsis/docs/geneva/official/poa.html
- 第二次会议议程，附演讲链接：http://www.itu.int/osg/csd/cybersecurity/WSIS/meetingAgenda.html
- WSIS C5行动方面第三次会议的报告：http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf
- 第三次会议议程，附演讲链接：http://www.itu.int/osg/csd/cybersecurity/WSIS/agenda-3_new.html
- 微软：针对世界政策制定机构的计算机保密、互联网安全和安全信息：http://www.microsoft.com/mscorp/twc/policymakers_us.mspx
- OECD安全文化门户，附带资料库：http://ww.oecd.org/sti/cultureofsecurity
- OECD“信息系统和网络安全指导原则：迈向安全文化”（2002年）：http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html
- OECD“保护隐私和个人数据的跨国界流通的指导原则”（1980年）：http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html
- OECD报告“促进OECD国家信息系统和网络的安全文化”（2005年）：http://www.oecd.org/dataoecd/16/27/35884541.pdf
- 《世界银行信息技术手册》 – 信息安全和政府政策：http://www.infodev-security.net/handbook/part4.pdf
- 联合国大会第57/239号决议附件a和b：http://www.un.org/Depts/dhl/resguide/r57.html

区域层面

- ENISA：“信息安全意识举措：当前做法和成功的衡量标准”（2007年）：http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf
- ENISA：“用户指南：如何提高信息安全意识”（2006年）：http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_a_users_guide_how_to_raise_IS awareness.pdf
- 欧洲互联网安全信息来源（InSafe）：http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- 美洲国家组织：打击网络安全威胁的美洲国家战略：建立网络安全文化的多维度和多学科方法（特别是附录）（2004年）：http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

国家层面

- 巴西：Antispam.br资源：http://antispam.br/
- 巴西：巴西互联网指导委员会《互联网安全指南》 – CGI.br：http://cartilha.cert.br/
- OECD促进安全文化的举措（按国别）：http://www.oecd.org/document/63/0,3343,en_21571361_36139259_36306559_1_1_1_1,00.html
- 美国CERT网站：http://www.us-cert.gov/
- 美国国土安全部（DHS）国家关键基础设施保护研发计划：http://www.dhs.gov/xres/programs/gc_1159207732327.shtm
- 美国联邦机构安全惯例：http://csrc.nist.gov/fasp/
- 美国联邦采购条例（FAR），第1、2、7、11和39部分：http://www.acqnet.gov/FAR/
- 美国联邦网络安全和信息保障研发计划：http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf
- 美国信息安全和隐私保护顾问委员会：http://csrc.nist.gov/ispab/
- 美国国土安全总统指令/HSPD-7，“关键基础设施的识别、优先安排和保护”：http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html
- 美国多国信息共享和分析中心：http://www.msisac.org/
- 美国保障网络空间安全的国家战略：http://www.whitehouse.gov/pcipb/
- 总统信息技术顾问委员会关于网络安全研究重点的报告：http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

V.C.2 企业和私营部门组织（V.B.3.、V.B.5.和V.B.7.）

- 巴西互联网安全运动：http://www.internetsegura.org/
- 思科安全中心（最佳做法部分）：http://tools.cisco.com/security/center/home.x
- 微软可信的计算：http://www.microsoft.com/mscorp/twc/default.mspx
- NIATEC授课材料：http://niatec.info/index.aspx?page=105
- 《世界银行信息技术手册》 – 组织安全：http://www.infodev-security.net/handbook/part3.pdf
- 美国CERT工作场所布告和须知：http://www.uscert.gov/reading_room/distributable.html
- 美国国土安全部/行业“网络风暴”演习：http://www.dhs.gov/xnews/releases/pr_1158340980371.shtm

V.C.3 个人和民间团体（V.B.4.、V.B.6和V.B.7.）

- 巴西：巴西SaferNet：http://www.safernet.org.br/site/
- 保证网上安全（SUSI – 更安全地使用互联网业务）：http://www.besafeonline.org/
- CASEScontact安全提示：http://casescontact.org/tips_list.php
- 儿童网（Childnet）儿童国际资料库：http://www.childnet-int.org
- 网络和平举措：http://www.cyberpeaceinitiative.org/
- 网络提示在线（CyberTipline）：青少年学习如何保证网上安全：http://tcs.cybertipline.com/
- 儿童和父母互联网安全区资料库：http://www.internetsafetyzone.co.uk/
- 国际刑警组织IT犯罪专用核对清单：
  http://www.interpol.int/Public/TechnologyCrime/CrimePrev/privateChecklist.asp
- 国际电联保护在线儿童及相关指南：http://www.itu.int/cop/
- 聪明上网（GetNetWise）家庭工具：http://kids.getnetwise.org/tools/
- 在线安全保障组织– 防范欺诈技巧：http://onguardonline.gov/index.html
- 保障安全（MakeItSecure）–互联网常见危险信息： http://www.makeitsecure.org/en/index.html
- 马拉西亚电子安全举措：http://www.esecurity.org.my/
- NetSmartz：父母和监护人资料库：http://www.netsmartz.org/netparents.html
- 新西兰网络安全：http://ww.netsafe.org.nz
- 安全在线（SafeLine）非法内容举报热线：http://www.safeline.gr/
- 安全漫画：http://www.securitycartoon.com/
- 保证上网安全组织：http://www.staysafeonline.info/
- 在线安全组织（WiredSafety.org）：http://www.wiredsafety.org/
- 《世界银行信息技术手册》 – 个人安全：
  http://www.infodev-security.net/handbook/part2.pdf
- 英国儿童性剥削在线保护中心资料库：http://www.ceop.gov.uk/
- 英国网上安全在线：http://www.getsafeonline.org/
- 美国针对非技术用户的CERT：http://www.us-cert.gov/nav/nt01/

针对终端用户的其他国际性、区域性和国家性提高意识举措。

瑞士印刷
2010年，日内瓦
图片鸣谢：国际电联图片库