国家网络安全战略制定指南

网络安全的战略参与

ITU

CCDCOE

The Commonwealth Cybercrime Initiative

CTO

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Deloitte.

Global Cyber Security Capacity Centre

GCSP

Microsoft

POTOMAC INSTITUTE FOR POLICY STUDIES

一些保留的权利

权利和许可

鸣谢

该指南是由来自政府间和国际组织、私营部门以及学术界和民间团体的十二家合作伙伴编写的。这些组织包括：英联邦秘书处（Comsec）、英联邦电信组织（CTU）、德勤、日内瓦安全政策中心（GCSP）、牛津大学全球网络安全能力中心、国际电信联盟（ITU）、微软、北约合作网络防御英才中心（NATO CCD COE）、Potomac政策研究所、兰德欧洲、世界银行和联合国贸易和发展会议（UNCTAD）。

小组人员包括Katalaina Sapolu（Comsec）、Shadrach Haruna（Comsec）、Martin Koyabe（CTO）、Fargani Tambeayuk（CTO）、Andrea Rigoni（德勤）、Carolin Weisser（GCSCC）、Marco Obiso（国际电联）、Kaja Ciglic（微软）、Kadri Kaska（NATO CCD COE）、Francesca Spidalieri和Melissa Hathaway（Potomac政策研究所）、Erik Silfversten（兰德欧洲）、David Satola和Sandra Sergeant（世界银行）以及Cecile Barayre（UNCTAD）。

欧盟网络和信息安全机构（ENISA）为此指南做出了突出贡献。

以下人员的贡献亦应得到认可：Grace Acayo、Rosheen Awotar-Mauree、Ben Baseley-Walker、Paul Cornish、Luc Dandurand、Michael Goldsmith、Kemal Huseinovic、Andraz Andy Kastelic、Maxim Kushtuev、Lena Lattion、Gustav Lindstrom、Damien Maddalena, Emily Munro、Lara Pace、Sarah Puello Alfonso、Valeria Risuglia, Taylor Roberts、Monica M. Ruiz、Irene Rubio、Ann Valjataga、Julienne Wright。

前言

很高兴代表相关合作伙伴介绍《国家网络安全战略指南》。该指南旨在为国家网络安全战略的制定、建立和实施提供一套统一的原则和良好做法。

在国际电联的推动下，来自公共和私营部门、学术界和民间团体的十二家合作伙伴一致同意分享他们的经验、知识和专长，编写一份指南，从参与组织收集现有的专业知识并提供补充出版物的参考资料，以便为获得可用资源提供便利。

在过去二十年里，全世界数十亿人得益于信息和通信技术的指数增长和迅速采用以及相关的经济和社会机遇。我们正在目睹一场深刻改变社会的数字革命。

网络安全是实现社会经济发展的一个根本要素。然而全世界只有七十六[1]个国家拥有公开的国家网络安全战略。因此，必须为制定战略加倍努力。正如标题所示，本指南的目的是激发战略思维并帮助各国领导人和决策者制定、编写和实施国家网络安全战略。

我相信，《国家网络安全战略指南》将成为所有负有网络安全责任的利益攸关方的有用工具。我本人要向合作伙伴表示感谢，感谢他们持续、宝贵的支持和承诺，使这个项目取得巨大成功，成为利益攸关多方成功合作的典范。

国际电联电信发展局主任
布哈伊马•萨努

[1] 来自国际电联2017年全球网络安全指数（GCI）

目录

序言

国家网络安全战略指南是构成成功网络安全战略的最全面概述之一，它是利益攸关多方与众不同、协作和公平努力的成果。这项工作利用了许多组织在国家网络安全战略和政策领域的知识、经验和专长。具体而言，这份指南是由来自公共和私营部门以及学术界和民间团体的十二家合作伙伴编写的。

聚集一堂的合作伙伴认识到，有必要加强整个国际社会在网络安全能力建设方面的合作与协调。这项工作的目标是支持各国领导人和决策者通过国家网络安全战略制定应对网络威胁的防御对策并从战略角度思考网络安全、网络准备、响应和复原力，在信息通信技术（ICT）使用中建立信任和安全。

网络安全是实现现代经济社会经济目标的基础要素。希望由此产生的《国家网络安全战略指南》能够成为以下所有利益攸关方的有用工具，其中包括负有网络安全责任的国家决策者、立法机构和监管机构。此外，该指南可能具有更广泛的适用性，因为其中的概念可用于区域或城市层面并通过调整用于行业。

1 文件概述

1.1 目的

编写本文件是为了指导各国领导人和决策机构如何制定国家网络安全战略并从战略角度思考网络安全、网络防备和恢复能力。

本指南旨在提供一个有用、灵活和用户友好的框架，以确定一个国家的社会经济愿景和当前安全态势的背景，并协助决策机构制定一项考虑到一个国家具体国情、文化和社会价值观的战略。该战略鼓励人们建设安全、恢复能力强、在信息通信技术方面得到加强且互联互通的社会。

《指南》是一种独特的资源，因为它提供了一个框架，该框架已由在该主题领域具有丰富经验的组织达成一致，并以此前在该领域开展的工作为基础。因此，它最全面地概述了迄今为止各国成功的国家网络安全战略。

1.2 范围

网络安全是一项复杂的挑战，包括多种不同的治理、政策、运营、技术和法律问题。本《指南》试图基于现有的和公认的模型、框架和其他参考资料来解决，组织和优先考虑这些领域中的许多问题。

《指南》侧重于保护网络空间的民用方面，因此，它强调了在起草、制定和管理“国家网络安全战略”过程中需要考虑的总体原则和优秀做法。

为此，《指南》明确区分了各国在国家网络安全战略周期中采用的“过程”（启动、清点和分析、生产、实施、审查）和“内容”（实际将出现在国家网络安全战略文件中的文本）。该指南不涉及一个国家的军队、防卫力量或情报机构发展防御性或攻击性网络能力等方面，尽管一些国家已在开发这种能力。

为了提供有关“什么”应纳入国家网络安全战略的指导和优秀做法，以及“如何”建立、实施和审查它，本指南涉及这两项要素。《指南》还概述了一个国家在网络方面进行防备所需的核心组件，强调了政府在制定国家战略和实施计划时应考虑的关键问题。

最后，本《指南》为决策机构提供了对现有方法和应用全面且高屋建瓴的概述，并提及了可为特定国家网络安全工作提供信息的其他补充资源。

1.3 指南的总体结构和用法

本《指南》主要是作为一种资源，帮助政府利益攸关方准备、起草和管理其国家网络安全战略。因此，内容的组织遵循战略发展的过程和顺序：

- 第2节 – 引言：概述了本《指南》的主题及相关定义；
- 第3节 – 战略制定周期：详细说明战略制定步骤及其在整个周期中的管理；
- 第4节 – 战略的总体原则：概述在制定战略期间需要考虑的贯穿各领域的基本考虑因素；
- 第5节 – 重点领域和优秀做法：确定战略制定过程中应考虑的关键要素和问题；以及
- 第6节 – 支撑性参考资料：提供相关文献的进一步说明，利益攸关方可以在其起草工作中进行研究。

第3节特别涉及与制定国家网络安全战略相关的过程和问题（如准备、起草、实施和长期可持续性），而第4节和第5节则更侧重于国家网络安全战略的内容，因为这两节突出了文档应包含的概念和要素。

1.4 目标受众

本《指南》首先针对负责制定国家网络安全战略的决策机构。次要受众是参与制定和实施战略的所有其他公共和私营利益攸关方，例如政府主管人员、监管机构、执法部门、ICT提供商、关键基础设施运营商、民间团体、学术界和研究机构。“指南”也可对在网络安全领域提供援助的国际发展界的不同利益攸关方有所裨益。

2 引言

在过去二十年中，全球数十亿人从信息通信技术的指数级增长和迅速普及相关的经济和社会机会中受益。

自创建以来，互联网已从信息交换平台发展成为现代商业、关键服务和基础设施、社交网络以及整个全球经济的支柱。因此，各国领导人已开始启动数字战略，并为可增加互联网连接并利用使用ICT带来好处的项目提供资金，以刺激经济增长，提高生产力和效率，改善服务提供和能力，提供对业务和信息的获取，实现电子学习，提高员工技能和促进优秀治理。各国不能忽视与连入网络并参与互联网经济相关的机会。

虽然我们社会对数字基础设施的依赖正在增加，但技术仍然具有内在的脆弱性。信息通信技术基础设施的保密性、完整性和可用性面临着快速发展的网络威胁的挑战，这些威胁包括电子欺诈、盗用知识产权和个人可识别信息、服务中断以及财产受损。作为经济增长和社会发展的催化剂，ICT和互联网的变革性力量正处于一个关键时刻，公民和国家对使用ICT的信任和信心正受到网络不安全的侵蚀。

为了充分发挥技术的潜力，各国必须将其国家经济愿景与国家安全优先事项保持一致。如果与信息通信技术基础设施和互联网应用的普及相关的安全风险未能与全面的国家网络安全战略和恢复计划保持适当平衡，那么各国将无法实现其所寻求的经济增长和国家安全目标。

作为回应，各国正在发展攻击和防御能力，以保护自己免受网络空间中的非法活动的影响，并在事件可能对其国家造成伤害之前预防事件发生。本文件将特别关注防御性响应，特别是以国家网络安全战略为形式的响应。

通过制定和实施国家网络安全战略，一国可以提高其数字基础设施的安全性，并最终促进实现其更广泛的社会经济愿望。国家领导人需要对数字环境所提供的机遇以及它对自己国家构成的风险保持战略性认识；他们还需要建立一个自己希望创造的数字化未来的清晰愿景。

2.1 什么是网络安全?

“网络安全”有着多种国内和国际定义。在本文件中，“网络安全”一词用于描述用以保护涉及政府、私营组织和公民联网基础设施中资产的可用性、完整性和保密性的各种工具、政策、指导原则、风险管理方式、行动、培训、最佳做法、保证和技术；这些资产包括联网的计算设备、人员、基础设施、应用、服务、电信系统以及在网络环境中的信息。[2]

2.2 国家网络安全战略的益处和制定过程

国家网络安全战略可以采取多种形式，可根据具体国家的目标和网络就绪水平进行不同程度的细节处理。因此，对于国家网络安全战略的构成没有既定且协商一致的定义。

根据该领域内的现有研究成果，本文件鼓励利益攸关方将国家网络安全战略视为:

- 表达一个国家应对网络安全的愿景、高级目标、原则和优先事项;
- 概述承担改善国家网络安全任务的利益攸关方及其各自的职责；以及
- 描述一个国家为保护其国家网络基础设施并在此过程中提高其安全性和恢复能力而采取的步骤、计划和举措。

制定愿景、目标和优先事项可使各国政府能够在整个国家数字生态系统中，而不是在特定部门、某项具体目标或应对特定风险时全面审视网络安全 - 它使其具有战略性。国家网络安全战略的优先级因国家而异，因此，虽然一个国家的重点可能是解决与基础设施相关的关键风险，但对其他国家而言，它可能是保护知识产权，增强对在线环境的信任，或提高公众的网络安全意识；或这些问题的组合。

[2] 定义改编自https://www.bcmpedia.org/wiki/Cyber_Security

有必要寻找投资和资源并随后确定其优先顺序对于成功管理像网络安全这样包含广泛的区域内的风险至关重要。

国家网络安全战略还提供了将网络安全优先事项与其他信息通信技术相关目标相结合的机会。网络安全对于实现现代经济的社会经济目标至关重要，战略应反映如何支持这些目标。这可以通过参考寻求实施国家数字或发展议程的现有政策或通过评估如何将网络安全纳入其中来实现。

最后，国家网络安全战略的制定过程应将政府的愿景转化为有助于实现其目标的连贯和可实施的政策。这不仅包括应该采取的步骤、计划和举措，还包括为这些工作分配的资源以及如何使用这些资源。同样，该过程应确定将用于帮助确保在设定的预算和时限内实现预期结果的指标。

3 国家网络安全战略的周期

本节概述了战略制定的各个阶段，包括：

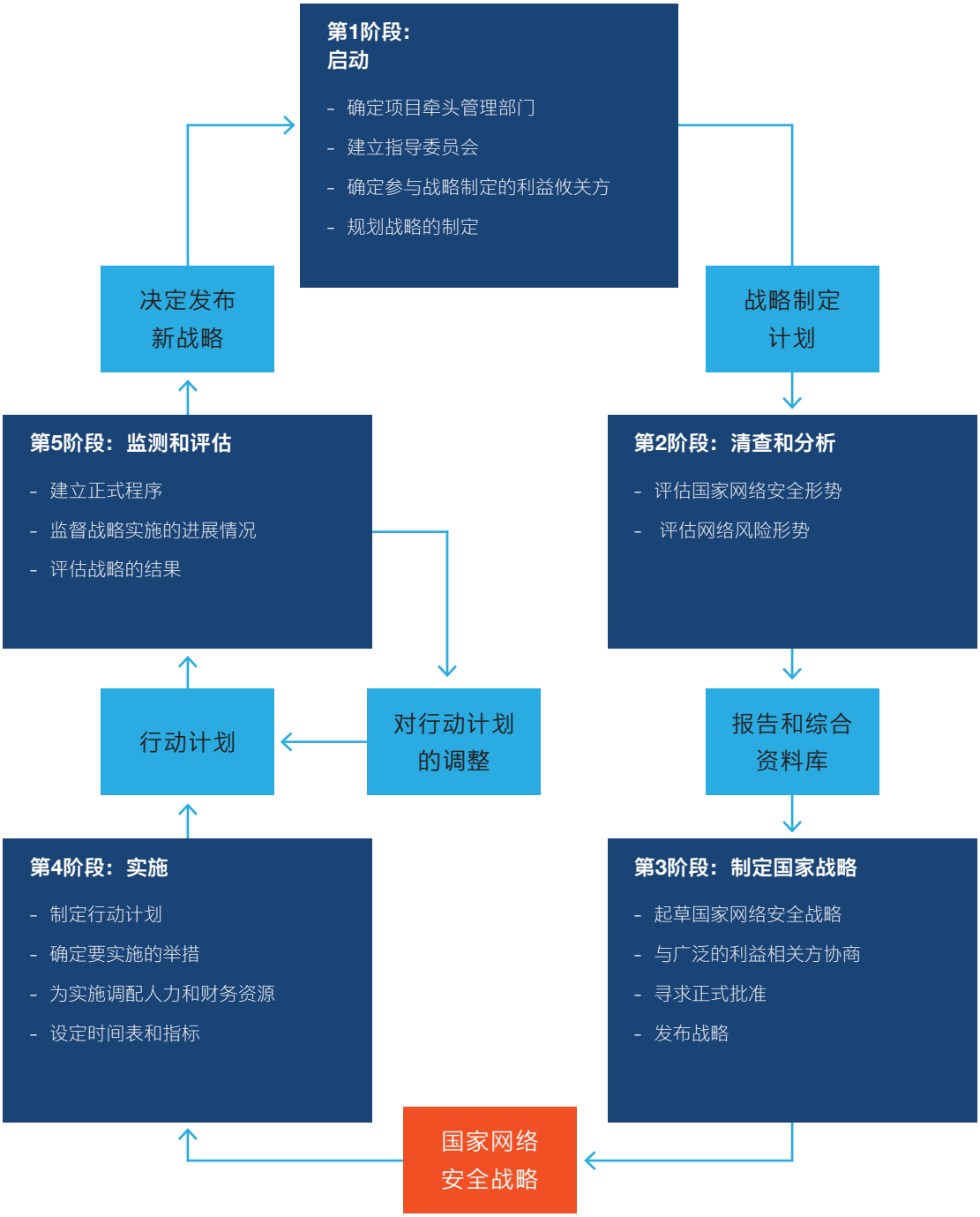
- 第一阶段 – 启动
- 第二阶段 – 清查和分析
- 第三阶段 – 制定
- 第四阶段 – 实施
- 第五阶段 – 监督和评估

本节还介绍了应该参与制定战略的关键实体，并强调了可能有助于该进程的其他相关利益攸关方。

本节最终旨在让读者了解一个国家为了起草国家战略所采取的步骤，以及根据国家的具体需求和要求实施国家战略的可能机制，并纳入总体原则（第4节）和优秀做法（见第5节）。

如图1所示，该周期指导本文件的用户重点关注国家层面的网络安全战略考量。

图1 - 国家网络安全战略的周期



3.1 第一阶段：启动

根据本文件第4和第5节，国家网络安全战略的启动阶段为其高效制定奠定了基础。预计这一阶段将侧重于应该参与战略制定的关键利益攸关方的流程、时间表和确定。这一阶段的成果是形成制定战略的计划。在国家治理过程中已有规划时，该计划可能需要得到该国领导层[3]的批准。

3.1.1 确定项目牵头管理部门

根据明确领导关系、职责和资源分配的原则（第4.8节），战略制定过程应由一个单独且有权能的机构负责协调。领导层应指定一个已有或新设立的公共实体，如部委、机构或部门，领导战略的制定工作。该实体在本文件中称为项目牵头管理部门，也应指定负责领导战略制定过程的个人。

项目牵头管理部门在整个制定过程中应保持中立。为此，建议将该实体与负责实施该战略的实体区别开来。应采用这种或其他机制来克服任何固有的偏见，并有助于避免政府内部对资源的争夺。

3.1.2 成立指导委员会

领导层还应设立指导委员会，与项目牵头管理部门合作制定战略。它应有权提供指导，并在质量保证中发挥作用。此外，它还应根据明确领导关系、职责和资源分配的原则保证这一过程的透明度和包容性（第4.8节）。应从一开始就明确界定指导委员会的职责、设立和成员构成。

由于指导委员会可能需要研究敏感文件，因此其构成应该相应地做出安排。同样重要的是，其成员资格反映了给予该机构的各种职责，例如通过任命的资历深浅。

3.1.3 确定参与战略制定的利益攸关方

在这一步骤中，项目牵头管理部门应确定参与制定战略的初始利益攸关方。它还应阐明不同利益攸关方的职责并简要说明他们在整个过程中将如何协作以管理期望。

[3] 负责国家层面决策过程的个人或实体。

在整个过程中，项目牵头管理部门可能需要与其他利益相关方联系，以确保利用所有相关知识和专业技能。这将包含包容性原则（第4.3节），该原则强调了与政府、私营部门和民间团体等一系列利益攸关方开展合作的重要性。例如，项目牵头管理部门可以考虑将ICT公司、关键基础设施运营商、学术专家和致力于提高网络安全意识和就绪水平的非政府组织等包括在内。

这种合作机制可以采取咨询委员会的形式，该委员会将有助于向指导委员会举荐成员并就各个阶段提供咨询意见。

3.1.4 规划战略的制定

在启动阶段的最后一步，主要项目牵头管理部门应制定一项制定国家网络安全战略的计划。一旦起草了该计划，应根据国家治理程序，酌情将其提交指导委员会和领导层批准。

在起草计划时，项目牵头管理部门还应考虑国家网络安全战略是采取立法还是政策的形式，因为不同的选择可能会影响需要遵循的正式程序以及通过战略的时间表。

战略制定计划应确定主要步骤和活动、主要利益攸关方、时间表和资源要求。它应规定期望相关利益攸关方如何以及何时参与制定进程，提供输入意见和反馈。

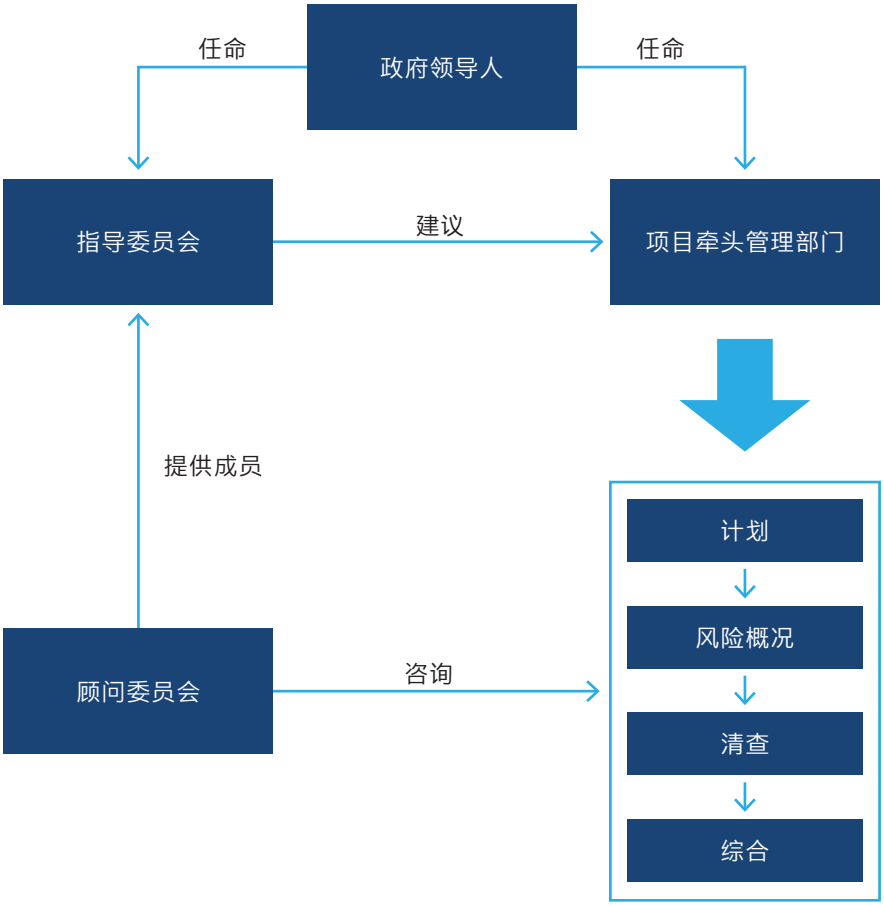
它还应确定所需的人力和财政资源，以及可以采购这些资源的渠道。例如，可以从政府间组织、私营部门、学术界或发展机构征求所需的专业知识。同样，可以通过在现有预算中重新分配专用资金流或通过第三方（例如国际组织）提供的新资金来解决资金需求。

应特别注意确保国家网络安全战略的整个周期（包括其制定、实施和改进）的长期融资。有关实施资源分配的更多详细信息，请参阅“为实施分配人力和财务资源”（第3.4.3节），有关长期资金的更多详情，请参阅“分配专用预算和资源”（第5.1.5节）。

图2显示了不同利益攸关方和委员会之间可能的工作配合和职责分工。

第55页提供了更多的参考资料。

图 2 – 利益攸关方



3.2 第二阶段：清点和分析

此阶段的目的是收集数据，以评估国家网络安全形势以及当前和未来的网络风险形势局，为国家网络安全战略的起草和制定提供信息。本项工作的结果应该是一份报告，概述将提交指导委员会的战略性国家网络安全态势和风险形势。

在开始实际形成战略文本之前，项目牵头管理部门应仔细分析和评估在评估阶段收集的信息，以确保找出网络安全能力方面存在的任何差距，并提出弥补这些差距的方案。分析应该评估现有政策、监管和运作环境在多大程度上符合战略的既定目标，并强调它们的不足之处。

同样，它也应用于确定具体的关键问题，例如教育和培训差距。

最后，分析应该形成对战略所有相关和预期结果的评估，以及所选手段的潜在影响和结果。

第55页提供了更多的参考资料。

3.2.1 评估国家网络安全形势

为使国家网络安全战略有效，它需要反映该国的网络安全态势。为此，应对该国现有的网络安全优势和劣势进行分析，并与政府、私营部门和民间团体的相关利益攸关方合作，查阅相关材料和文件。这一步应该采用综合方法和定制优先事项的原则（见第4.2节）。

作为这项工作的一部分，项目牵头管理部门应确定对社会和经济正常运作至关重要的资产和服务，并清点与网络安全相关的现有国家法律、法规、政策、计划和能力。项目牵头管理部门还应确定现有的软监管机制（例如公私伙伴关系），并评估为应对网络安全挑战而开发的能力，例如国家计算机应急响应小组（CERT）。此外，应确定并查点具有网络安全职能的现有公共机构（如监管机构或数据保护机构）的职能和职责。

此外，应收集能够说明该国网络安全状况的相关数据。这可能包括：有关现有国家网络安全计划、国际举措、私营部门项目，信息通信技术和网络教育及技能发展计划，网络研发举措的信息；有关互联网普及率和感染率、ICT普及、技术发展的数据；以及对未来ICT和网络安全趋势和威胁的见解。

私营部门、研究机构和其他利益相关方团体提供的相关信息也应包括在本分析中。对发展中国家而言，与发展伙伴制定协作举措，以协调技术援助和投资也至关重要。

最后，项目牵头管理部门还应调查区域和国际层面的类似信息，并审查针对具体行业的战略和举措。

3.2.2 评估网络风险形势

根据上一步收集的信息，主要项目牵头管理部门应评估该国因数字依赖而面临的风险。这可以通过确定国家公共和私人数字资产，它们的相互依赖性、脆弱性和威胁以及预测网络事件的可能性和潜在影响来实现。

这项工作包含风险管理和恢复能力原则（第4.6节），该原则认识到风险管理对于充分实现数字环境对社会经济发展的益处至关重要。此外，这种初始风险评估可以为未来更具体的风险评估奠定基础（有关风险管理和恢复原则以及如何进行风险评估的更多信息，请参见第5.2节）。

3.3 第三阶段：形成国家网络安全战略

这一阶段的目的是通过一系列公共磋商和工作组与公共部门、私营部门和民间团体的主要利益攸关方合作，形成战略案文。由项目牵头管理部门协调的这一更广泛的利益攸关方将负责确定战略的总体愿景和范围，设定高级别目标，评估当前形势（详见第二阶段），按目标对社会、公民和经济的影响程度确定目标的优先次序，并确保必要的财政资源。作为该阶段的一部分，应考虑所有跨部门原则（第4节），并应考虑本指南中详述的优秀做法要素（第5节）。

3.3.1 起草国家网络安全战略

评估和分析阶段完成后，项目牵头管理部门应与指导委员会合作，启动该战略的起草工作。可以创建专门的工作组，专注于特定主题，或起草战略的不同部分。工作组应遵循启动阶段确定的流程，并根据需要进行调整。

战略应规定该国整体的网络安全工作方向；明确清晰的愿景和范围；确定在特定时间范围内完成的目标；并根据对社会、经济和基础设施的影响确定这些因素的优先级别。此外，它应确定可能的行动方针；为实施工作提供激励措施；并推动所需资源的分配以支持所有活动。该战略还可能包括在清查和分析阶段得出的一些调查结果。

与规划战略制定的步骤类似，实际文件需要提出明确的治理框架（第5.1节），该框架定义了主要利益攸关方的职责和职能。这包括确定负责管理和评估战略的实体，以及负责其整体管理和实施的实体，例如某个中央机构或国家网络安全委员会。

该战略还需要确定或确认负责在该国启动和制定网络安全政策和法规的不同实体的职责范围。此外，它还应确定负责收集威胁和薄弱环节信息、应对网络事件（例如国家CERT）、强化就绪水平和开展危机管理的实体的职责和任务。它还应确保明确所有这些实体之间以及与中央机构如何配合。

3.3.2 与广泛的利益攸关方进行磋商

如上所述，吸引利益攸关方对于战略的成功至关重要。为了确保最终战略以共同愿景为基础，文件草案应在不仅限于参与战略制定过程的人员的广泛利益攸关方群体中传播。这可以通过各种活动实现，包括在线磋商、评审讲习班和其他工作组。预计此过程获得的反馈和意见将用于战略的最终定稿。

3.3.3 寻求正式批准

在战略制定的最后一步，项目牵头管理部门应确保领导层正式采纳该战略。这种官方采纳程序将因国家而异，并以法律框架中如何界定战略为基础。例如，它可以通过议会程序或政府法令获得通过。

此外，至关重要的是，该战略不仅得到了最高层政府的批准，而且这一承诺在其实施阶段仍会延续。有关官员应承担责任，并在政治资本和资源方面得到支持。

3.3.4 发布战略

该战略应该是一份公开文件，应随时提供。将其广泛公开将确保公众了解政府的网络安全优先事项和目标，并支持任何提高网络安全意识的工作努力。如果该战略附有行动计划，后者还应表明与民间团体和私营部门进一步接洽和合作的其他机会。

第55页提供了更多的参考资料。

3.4 第四阶段：实施

实施阶段是整个国家网络安全战略周期中最重要的因素。在充分的人力和财务资源的支持下，结构合理的实施方法对于战略的成功至关重要，需要作为其制定的一部分加以考虑。实施阶段通常以行动计划为中心，该计划指导所设想的各种活动。

3.4.1 制定行动计划

与战略的制定一样，其实施不是单一机构的唯一职责。相反，它需要政府内一系列不同利益攸关方的参与和协调以及民间团体和私营部门的支持。根据明确领导关系、职责和资源分配原则（第4.8节）制定的行动计划可以支持战略的有效实施。

制定行动计划几乎与计划本身一样重要。由项目牵头管理部门精心策划的这一过程应作为一种机制，汇集相关利益攸关方，就目标和结果达成一致，并协调工作和集中资源。

3.4.2 确定要实施的举措

国家网络安全战略强调了政府的目标以及他们希望在所确定的不同重点领域取得的成果。在行动计划中，项目牵头管理部门应-与相关利益攸关方协调-确定每个重点领域内有助于实现这些目标的具体举措。例子包括组织网络安全演习、为关键基础设施建立安全基线、或设置事件报告框架等。

实施这些举措所需的时间表和工作应根据其重要性确定优先次序，以确保适当利用有限的资源。为此，可以考虑第二阶段（清查和分析）的成果和结果，特别是关于"评估网络风险形势"（第3.2.2节）。

3.4.3 为实施分配人力和财务资源

一旦确定了优先举措，主要项目牵头管理部门应确定具体的政府实体作为每项举措的承办人。反过来，这些政府实体将负责并负责实施分配给它们的每项具体举措，并作为实施过程的一部分，期望与其他相关利益攸关方协调其工作。

为了确保这些实体能够实现预期的结果，主管项目牵头管理部门应评估是否已经给予他们实施所需的适当（法律或其他）授权。项目牵头管理部门还应与具体举措的承办人合作，以了解完成工作所需的资源。该评估应包括人力资源，专业知识和资金需求。然后，项目牵头管理部门应与承办人合作，帮助他们根据该国的行政财务结构寻求和获得所需资源。

3.4.4 设置时限和指标

行动计划的最后一个关键要素是制定具体指标和关键绩效指标，以评估所采取的每项举措，例如该国是否开展了关于信息共享重要性的宣传活动，是否与基础设施部门一道组织和实施了网络安全演习，或通过了安全基准法。还应设定具体的实施时间表。

指标和关键绩效指标应由项目牵头管理部门与各承办人合作制定。应鼓励后者界定和维护一套更详细的指标，以便在完成期间和之后评估各项举措的效率和有效性。

第55页提供了更多的参考资料。

3.5 第五阶段：监督和评估

在此阶段，主管当局应设计一个正式程序来监督和评估该战略。在监督阶段，政府应确保根据其行动计划实施该战略。在评估阶段，政府及其主管当局应根据不断变化的风险环境评估该战略是否仍然具有相关性，是否仍然反映了政府的目标以及需要做出哪些调整。

3.5.1 建立正式流程

为确保有效监督和评估战略的实施，政府必须确定一个独立的实体，负责监督和评估实施进度和效率。理想情况下，该实体应参与制定适当的监督和评估指标，以实施战略及相关行动计划和举措，以上工作应在形成和启动阶段进行。

监督和衡量战略实施计划的绩效和成功执行应是一个国家所实施治理机制的一部分。对实施计划的持续评估（即哪些进展顺利，哪些进展不顺利）有助于为战略提供信息。关于战略实施的良好治理机制还应明确界定确保成功执行的问责和责任。通过近期、中期和长期目标建立指标或关键绩效指标（KPI）有助于加强治理和管理机制。关键绩效指标或指标应：

- **具体** - 针对特定待改进领域。
- **可衡量** - 量化或至少建议进展指标。
- **可实现** - 说明在可用资源的情况下，可以实际获得哪些结果。
- **负责任** - 指定谁承担工作
- **与时间相关** - 指定何时可以实现结果。

建立基线指标将有助于更好地监督行动并突出可改进的领域。此外，预算的分配应与预期结果的规模和复杂程度相匹配。

3.5.2 监督战略实施进展情况

负责监督“战略”执行进度的实体应根据战略整个周期内商定的时间表予以实施。这种监督活动的结果（例如，报告）应当指出已商定时间表的任何偏差以及任何延误的原因，例如优先事项的改变、资金或资源短缺等。此外，负责实施战略不同部分的部门还应定期向项目牵头管理部门报告最新情况。

这种方法将确保就所承诺的责任对相关利益攸关方进行问责；它还将确保尽早确定在实施方面面临的任何问题。反过来，这将使政府能够根据实施过程中吸取的经验教训纠正这种情况或相应调整其计划。

3.5.3 评估战略的结果

除了评估商定指标的进展之外，还必须定期评估结果并将其与设定目标进行比对。这对于了解战略目标是否正在实现或是否应考虑采取不同行动至关重要。作为此过程的一部分，还需要定期重新评估更广泛的风险环境，以了解是否有任何外部变化正在影响战略的结果。实际上，这个过程可以作为对国家风险评估概况的轻微修订。

评估以及相关建议应汇总到项目牵头管理部门的报告中，并包括更新行动计划的相关方法，并确保报告保持最新并对不断变化的政策和风险格局做出响应。

最后，在战略周期内形成的报告也应根据启动阶段确定的时间表，为国家网络安全战略的全面审查奠定基础。这项总体审查不仅应考虑所取得的进展和外部环境的变化，还应重新评估政府自身的优先事项和目标。

第55页提供了更多的参考资料。

4 总体原则

本节介绍了九条相互渗透的原则，它们将共同助力制定一个前瞻性的全面国家网络安全战略。

这些原则适用于本文件确定的各关键焦点领域。在国家战略制定进程的各个阶段，无论是国家战略文件的起草还是实施过程中均应加以考虑。

这些原则的顺序是按叙事逻辑而非重要性排列。

4.1 愿景

上述战略应为整个政府和社会勾勒出一个明确的愿景。

国家网络安全战略确定的愿景若有助于所有利益攸关方了解哪些问题已到了关键时刻、战略因何不可或缺（背景）、哪些任务必须完成（目标）、战略的关切点所在及其影响（范围），则其获得成功的机率更高。

愿景越明确，则领导人和主要利益攸关方更容易确保实施方法的全面性、一致性和连贯性。此外，明确的愿景亦有助于在相应利益攸关方之间开展协调、合作与实施。考虑到数字环境不断变化的特性，应在足够高的层面确定愿景。

战略目标和实施的时间表应与愿景相吻合。

其它参考内容见第56页。

4.2 全面的方法和定制的工作重点

战略的制定应基于对整体数字环境的全面了解与分析，且需要根据国情量身定制并确定工作的重点。

网络安全不仅是一项技术挑战而且具有复杂的多面性，其涉及的内容已超越经济与社会的繁荣，延伸至执法、国家与国际安全、国际关系、贸易谈判和可持续发展等领域。

至关重要的是要了解网络安全的各个方面，以及它们之间可能存在的互补或竞争互关系。在此理解之上对具体国情加以分析，则可根据战略的目标和时间表确定工作重点。确定工作重点将使我们能够制定具体的目标和时间表并分配必要的资源。

各国国家网络安全战略的重点不尽相同。部分网络安全议题分别涉及同一件或不同战略文件（例如，国家安全与国防数字化问题既可在国家安全也可在国际战略中处理）。

其它参考内容见第56页。

4.3 包容性

国家网络安全战略应在所有相关利益攸关方的积极参与下制定，满足其需求并确定他们的责任。

数字环境对政府、企业和个人均很关键。这些群体面临着网络安全风险且根据各自职责的不同，均在某种程度上承担着管理网络的责任。尽管确定并请全体相关利益攸关方参与并非易事，但这是制定与成功实施国家网络安全战略的基础。这将有助于了解利益攸关方的需求，他们的独有的知识与专业技能，推动为实现此战略的目标开展合作。

为促进实现包容性，该战略应为一份公开文件。

其它参考内容见第56和57页。

4.4 经济与社会繁荣

国家网络安全战略应促进经济和社会繁荣，使ICT为可持续发展和社会包容性做出尽可能多的贡献。

数字环境的潜力可加速经济发展和社会进步，提升重要的社会价值，增强公共服务的交付水平和能力，推动国际贸易并促进实现优秀治理。

对通过数字环境来满足社会需求的愈发依赖，增加了人们对网络安全的关注度。但网络安全自身并非目标；国家网络安全战略应与更广泛的社会经济目标保持一致，以建立必要的信任与信心，帮助人们实现这些目标并保护国家免受网络威胁。

其它参考内容见第57页。

4.5 基本人权

国家网络安全战略应遵重并与基本人权价值保持一致。

此项战略应认识到这样一个事实，即网上人权必须在网络空间得到保护。战略应尊重得到普遍认可的基本权利，其中包括但不限于联合国的《世界人权宣言》和《公民及政治权利国际公约》以及相关多边和区域立法框架中规定的权利。

言论自由、交流隐私和个人数据保护应得到关注。国家网络安全战略特别应避免产生专制、实施无正当理由或非法的监视、进行通信监听或处理私人数据。

为平衡国家与个人的需求，国家网络安全战略应酌情确保在具体调查或法律案件的调查过程中进行的监督、通信监听和数据采集已取得相关国家机构的授权，且可实现有效监督、程序保障和救助的，公开、准确、全面、非歧视性的立法框架是其实施的基础。

其它参考内容见第57和58页。

4.6 风险管理与复原力

国家网络安全战略应支持有效管理网络安全风险并促使社会经济活动具有复原力。

尽管数字环境为利益攸关方提供了经济和社会机遇，但亦使他们暴露于网络安全风险之下。例如，在机构使用ICT来促进创新、获得生产力并提升竞争力或是政府部署网上业务的过程中，可能会出现网络安全事件，造成财务损失、

声望损害、运营中断以及创新受挫等问题。与其它类型的风险一样，网络安全风险无法根除，但却可以管控并尽量减少。

为应对这些挑战，国家网络安全战略应鼓励相关实体确定网络安全投资的重点并以主动的方式对风险进行管理。根据实体的风险偏好不同，在考虑到数字环境变化特性的基础上，需在安全措施与潜在利益之间达成平衡。国家网络安全战略亦应认识到持续管理风险的必要性并在相互依赖的实体之间推行一种统一的方法。

对风险管理的关注亦将使利益攸关方为潜在的安全事件做好准备，确保本国的经济和社会活动具有复原力。有鉴于此，国家网络安全战略应鼓励采取包括事件与危机管理在内的，确保业务连续性的措施并制定恢复计划。

其它参考内容见第58页。

4.7 适当的政策工具

国家网络安全战略应在各国具体国情的基础上，使用最恰当的可用政策工具实现各项目标。

只有所涉全体利益攸关方均做出行为改变，政府的网络安全目标方能实现。大多数情况下，政府握有可取得相应成果的不同杠杆和政策工具。这其中包括立法、监管、标准化、激励和信息共享计划与机制、教育计划、最佳做法共享、预期行为标准的制定以及建立社区之间的互信。不同方式各有优劣，成本不一且结果各异。

最佳结果可通过为各独立目标选择最适当的政策工具并平衡不同工具的使用来实现。

其它参考内容见第59页。

4.8 明确领导权、职责和资源的分配

国家网络安全战略应在政府最高层面制定，接下来由政府负责指定相关职责，并为其划拨充分的人力和财务资源。

应在政府最高层推广和保持网络的安全性。此外，为确保问责且相关工作取得进展，需确定各独立工作方面的联络人。另外，工作所涉各方应明确了解自己的职责。国家网络安全战略还应为实施工作分配必要的人力、财力和物力资源。此项原则不仅要指导战略制定流程，还要指导战略行动计划的制定。

其它参考内容见第59页。

4.9 值得信任的环境

国家网络安全战略应有助于建设一个公民与企业均可依赖的数字环境。

建立对国家数字生态系统的信任，使用户的权益得到保护且数据的安全性得以保障，对充分发挥使用ICT所释放的社会、政治和经济机遇至关重要。该战略必须在国家层面为政策、流程和行动提供支撑，以确保得到ICT支持并为公众所用的关键业务（包括电子政务、电子商务和数字金融交易等）的安全。此类行动不仅需要向普通民众反复灌输信任原则，同时亦需在为公民提供ICT相关服务的公共和私营组织内部反复提及。

其它参考内容见第59页。

5 国家网络安全战略的优秀做法

网络安全影响到社会经济发展的许多领域但亦受到国家背景下多项因素的影响。

因此，本节介绍了一系列优秀做法要素，这些要素不仅使战略全面有效，亦可实现针对国家背景的量身定制。

上述优秀做法要素已划分为几组明确的重点领域 – 有效地形成了国家网络安全战略的总主题。尽管本文将重点领域和要素均列为优秀做法示例，但尤为重要的是将后者放在国家背景下审视，因为有些要素可能与相关国家的具体国情不符。各国应确定并遵循相应的优秀做法要素，这些要素应可支持依据本国战略（第4节）确定之愿景制定的目标和工作重点。下述独立要素或重点领域的顺序与重要性和优先级无关。

5.1 重点领域1 – 治理

此重点领域介绍了有待审议纳入国家网络安全战略案文的优秀做法要素，供研究国家网络安全治理结构使用。此战略应明确声明政府在网络安全方面的目标和雄心，并概要介绍保障其落实所需确定的职能与责任。

为此，国家网络安全战略应确定并赋予权能机构执行此项战略的权利；为落实此战略建立一项机制，以确定受此影响或应对此负责的政府实体并将他们纳入进来；承诺将具体、可衡量、可实现、基于结果和时间的目标纳入战略实施计划；认识到为取得期望的成果提供资源承诺（例如政治愿望、资金、时间和人力）的必要性。

5.1.1 确保提供最高水平的支持

国家网络安全战略获得政府最高层的正式批准。批准有两个重要目的。首先，增加了获得充分资源且协调工作取得成功的可能性。其次，它向更广泛的国家生态系统发出了相关国家认为网络安全有多重要的信号。

5.1.2 建立有权能的网络安全机构

国家网络安全战略应确定一个专门的国家网络安全权能机构– 一个获得提升并深深扎根于政府最高层的领导者（无论是个人还是实体）–为战略的落实提供指导，协调相关行动并实施监督。

此国家网络安全权能机构应作为管理实体，制定并明确相关职能、责任、程序、决策权以及为确保有效落实战略必须执行的任务。这其中包括确定监督战略落实的利益攸关方，并为各部委或政府部门、机构或负责此战略具体事宜及随后行动计划的个人确定绩效目标。此方法可能需要更多的政策或法律架构，为执行者履行使命赋能。

鉴于网络安全与诸多不同的领域存在交叉关系，因此重要的是确保国家权能机构具备吸纳和指导相关利益攸关方的能力。

5.1.3 确保政府内部的合作

国家网络安全战略应建立一个机制来确定并纳入受战略落实影响或负责战略实施的政府实体。政府内部的承诺、协调与协作是这些政府机构必须履行的核心职能，可确保治理结构（即规则）和资源能够取得国家网络安全战略期望取得的成果。

有效的沟通与协调能够确保所部委和各政府机构相互了解对方的权利、使命和任务。然而，承诺旨在保持政策在一段时间内的连贯性，保障战略许诺得以实施。例如，协调机制将定期召开由与行动计划相关的所有利益相关方参加的会议，共同对计划进行审议。为解决特定问题创建的政府内部任务组可作为合作机制的范例。承诺方面的示例为：国家内外政策议程应保持一致，以确保不会因某部委对同一政策问题持有不同观点，而破坏另一部委的信誉。

5.1.4 确保跨部门合作

国家网络安全战略应认识到，政府在确保网络安全方面对私营部门和其它国家级利益攸关方的依赖（及相反）。为此，该战略应阐明政府邀请这些利益攸关方参与的方式并对他们的职能与责任做出规定。例如，国家网络安全战略应为关键行业创建一个国家负责人联系网，这对关键服务和基础设施恢复运营至关重要。

5.1.5 划拨专门预算和资源

国家网络安全战略应为战略的落实、维护和修订划拨专门且与之相适应的资源。充足、连贯且持续的资金为建立有效的国家网络安全态势奠定了基础。资源的确定应从以下角度着眼：资金（即专门预算）、人力、材料、关系与合作伙伴关系、持续的政治承诺以及成功实施所需的领导力。为战略目标和任务确定资源不应是一次性的举措。资源既可根据任务或目标划拨，也可按政府实体分配。

此外，政府亦可考虑为网络安全制定由网络安全治理机构管理的中央预算。无论是将分散的资金整合至统一集成的项目，还是创建统一的政府内部预算，均应分阶段对总体项目进行管理和跟踪，从而确保战略的成功实施。

5.1.6 制定实施计划

国家网络安全战略应伴有或附有实施计划，在该计划内对如何实现战略目标加以详细阐述。有效的实施计划确定了各项任务和目标的负责实体，一段时间内执行计划所需的资源（近期、中期、长期），使用的流程以及预计的会取得的成果（有关实施启动的第3.4节）。

其它参考内容见第60和61页。

5.2 重点领域2 – 国家网络安全的风险管理

此重点领域介绍了通过风险管理处理网络安全问题的优秀做法。正如风险管理和复原力原则（第4.2节）规定的那样，鉴于网络风险无法根除，因此应采用风险管理的方法。其实，确保国家能够很好的了解其面临的风险，方能使该国最为有效地管理风险。从风险评估角度看，相关方法应侧重确定网络之间的相互依存性并考虑到跨境依存带来的风险。风险管理方法应考虑包括从开发到采购，从运营到更换在内的整个生命周期。

此外，重要的是应注意到由于网络安全威胁变幻莫测，因此必须定期审核所有风险管理方法。有鉴于此，国家网络安全战略应做出风险管理活动的监督和评估规划，以确保其不断改进。

5.2.1 定义风险管理的方法

国家网络安全战略应针对风险管理制定连贯一致的方法，并要求所有政府实体和国内的关键基础设施运营商采用。此方法应能辨别社会与经济稳妥运营所必须的关键资产和业务、受到的威胁及与之相关的风险。

上述方法应以建立一个国家风险登记库为目标，同时确保该登记库所记载的风险得以安全保存并可以安全的方式发出通报，从而使政府能够对风险及处理风险的方法实施监督。此外，该方法还应根据风险出现概率的计算结果及其产生的影响，制定确定优先级的方式。另外还应进一步规定各主要行业实体在评估、验收和处理国家级网络安全风险方面的职责。

5.2.2 确定管理网络安全风险的通用方法

国家网络安全战略应为管理网络安全风险确定一种通用的方法。这将确保效率以及所有组织之间的统一，并促进相互依存的系统之间交流风险信息。基于国际标准的方法可降低成本并更好地与私营部门互动，因此安全战略应向这种方式倾斜。

上述方法应为风险管理方方面面的职能与责任分配提供指导，例如威胁评估、资产估值、缓解措施的实施与维护，以及剩余风险的承担。此方法应包括一项认证计划，用于为评估提供帮助并最终提升一致性。

至关重要的是，在基础设施或服务采购方面，风险管理方法应通过安全的架构与设计，进一步为尽量降低风险提供指导，同时认识到将安全融入产品设计流程、程序或服务，方能最好地实现安全性（通过设计实现安全）。

5.2.3 确定行业网络安全的风险特征

国家网络安全战略应呼吁将行业风险特征应用于网络安全。行业风险特征是对所面临威胁类型开展的定量分析。风险属性的目标是，通过为不同类型的威胁及其产生危险的变量指配数值来降低对风险认识的主观性。此战略应为该国认为对本国社会和经济至关重要的行业推荐风险属性。

行业风险特征的使用是独立机构开展更具体风险评估的基础，不仅国内各行业内部和行业之间形成了统一标准，同时减少了机构进行风险评估所需的资源。为确保时效性，应定期更新行业风险特征。

5.2.4 制定网络安全政策

国家网络安全战略应鼓励为政府机构和关键基础设施运营商等重要国家实体制定网络安全政策。依据恰当制定政策工具原则（第4.7节）采用的此类政策，将涵盖治理、运营和技术要求，并对利益攸关方的职能与责任做出说明，同时就解决这些问题的具体方法提供指导或提出要求。

例如，战略有可能包含以下方面的政策：保障采购或开发领域的网络安全、制定信息共享计划、协调安全漏洞的披露、制定维护的最低标准、规定具体的安全基线、制定一致性认证计划以及强制要求上报网络事件。

采取在国家层面进行协调的方法将实现更为有效且高效的网络安全管理，因为这不仅能够统一各类做法亦可促进协调与互操作。

其它参考内容见第61页。

5.3 重点领域3 – 就绪程度和复原力

此重点领域概要介绍了一批优秀做法，这些做法支持国家建立并保持可有效防止、检测、缓解并应对重大网络安全事件的能力，同时可以提升国家的整体网络复原力。

5.3.1 建立网络事件响应能力

国家网络安全战略应呼吁建设适当的国家事件响应能力，以应对运营网络安全方面的挑战。通常，此项能力的建设是指成立计算机应急响应团队（Certs）、计算机安全事件响应团队（Csirts）或负责全国事务的计算机事件响应团队（Cirts）。

尽管CERT/CSIRT/CIRT的具体组织形式可能不同（例如，由国家、政府和行业出面），且并非每个国家都有相同的需求和资源，但这些专业化的专门团队应同时履行前瞻性的和应对性的职能，并提供攻击预防和教育服务。因而这些实体能够提升国家的快速响应和遭受网络攻击后恢复的能力，同时增强其在威胁下的复原力，降低重大网络攻击可能给国内经济和运营造成的影响。

国家网络安全战略亦应确定并开发合作机制以及国家与行业事件响应团队（如果该国存在这种团队）和国际对等实体之间的沟通程序。

5.3.2 为网络安全危机管理制定应急计划

国家网络安全战略应呼吁针对网络安全紧急情况和危机制定国家应急计划。此项计划应为国家总体应急计划的组成部分或与之相匹配。此外，还应考虑为关键信息基础设施制定具体的计划。

此项国家网络安全应急计划既应考虑到国家风险评估的结果，亦应顾及可能会给关键基础设施持续运营造成影响的跨行业依存关系，以及各种灾害恢复机制。除此之外，计划应概要介绍国家事件响应机制；同时根据网络安全事件给关键资产和业务造成的影响重点阐述其分类方式。

5.3.3 促进信息共享

国家网络安全战略应呼吁建立信息共享机制，使公共和私营部门能够相互交流（可采取行动的）情报及威胁信息。

共享正式与非正式信息的计划能够促进对事件做出响应和并恢复过程中开展有效地协调，进行统一、准确和恰当的沟通；推动受影响的各方与其它利益攸关方迅速共享威胁和状况信息；帮助人们加强对攻击方式和受攻击行业的了解；传播可用于防止和缓解受影响资产遭受破坏的方法；并最终减少漏洞与暴露及其伴随风险。

国家网络安全战略应确定一个或多个制度架构（即权能机构），负责在包括公共和私营部门在内的国家网络安全社团内传递精确且可采取行动的信息。

信息共享应为双向流程。如果政府愿意分享其持有的信息，则其采取的行动将向私营部门实体证实，政府确是威胁信息共享方面的合作伙伴，且这些行动将有助于响应者将精力集中于根本性威胁并为应对这些威胁做好更加充分的准备。

5.3.4 开展网络安全演习

国家网络安全战略应组织并协调开展国内外网络安全和事件响应演习。这些演习可采用不同形式（如仿真或实时演习）并以技术和决策者为对象。

网络安全演习和其它危机规划机制能够帮助各国发展制度建设能力，从而可以有效地对事件做出响应，测试危机管理程序和沟通机制，验证Certs/Csirts/Cirts在压力下做出响应的操作能力并帮助人们了解各种跨行业的依存关系。

与此类似，国际网络安全演习有助于强化各国的网络事件响应能力，了解跨境的依存关系，建立国家之间的信任与信赖，以及提升各国的复原能力和备灾的总体水平。

其它参考内容见第62和63页。

5.4 重点领域4 – 关键基础设施业务和基本业务

此重点领域研究与保护关键基础设施（Cis），特别是关键信息基础设施（Ciis）有关的优秀做法。尽管这两条术语并没有得到普遍认可的定义，且政府需根据本国的风险评估考虑需在术语中纳入哪些实体和业务，但本导则对这两条术语的定义如下：

- 关键基础设施（CI）用于描述对具体国家的社会经济运行和安全至关重要的资产；和
- 关键信息基础设施（CII）是指服务于国家关键基础设施主要功能的IT和ICT系统。

此外，亦可用基本业务的概念指代那些对维护关键社会或经济活动必不可少的业务。

无论如何，虽不全面但下文列出了几个业务实例：能源（电力、石油和天然气）、交通（航空、铁路、水利和公路）、金融和银行（信贷机构、交易所及核心交易对手）、医疗卫生（医疗卫生机构，包括医院和私人诊所）、饮用水的供给和分配、数字和通信（固定和移动电话服务以及互联网基础设施的提供，如互联网交换点（Ixps）和域名服务等）。

5.4.1 为保护关键基础设施和服务制定风险管理方法

国家网络安全战略应依据风险管理与复原力的原则（第4.6节），从风险管理的角度保护Cis和Ciis。详细的风险评估应为确定国家Cis和Ciis以及关键业务提供指导，这些设施和业务的中断可能会给卫生、安全、保障或公民的经济福祉造成严重影响，也可能会影响政府或经济的有效运行。

此外，在确定和确立项目实施优先级以及Cis和Ciis的保护政策方面，亦应采取基于风险的方法。为促进私营部门的参与，也可考虑采用基于国际标准的风险管理方法。

5.4.2 采用责任清晰的治理模式

国家网络安全战略应从高层阐述保护CI和CII的不同利益攸关方的治理结构、职能和责任。正如明确领导权、职责和资源分配的原则（第4.8节）中规定的那样，有效且高效的CI 保护方案要求利益攸关方明确界定职能和责任，并建立协调机制来管理持续存在的问题。

Cis 和Ciis通常不归政府所有或控制且CI和CII的保护工作通常已超出任何单一政府机构的能力和职责范围。因此，任命一个保障CI和CII （网络）安全的总协调方，如跨机构委员会，可为保护关键基础设施提供极大帮助。

CI和CII保护的治理模式应涵盖：确定负责特定垂直行业政府实体，Cis和Ciis运营商的义务与问责以及公共和私人机构之间的沟通渠道和合作机制，其目的是确保关键服务和基础设施的运营与恢复。

5.4.3 确定最低限度的网络安全基线

国家网络安全战略应突出现有或拟议的新立法和监管框架，概述CI和CII运营商等的最低限度网络安全基线。在制定这些基线时，应考虑国际公认的标准和最佳做法，以确保达到更好的安全效果并提高效率。

安全基线应注重结果，阐明组织应达到的目标（例如“控制对关键资源的逻辑访问”）而不是应如何落实安全（例如“利用双因素认证”），这反过来又可让政府和行业受益于持续的安全改进。此外，这些基于成果的开发方法为具体行业的实施或起草“做法”指导方案留下了空间，这使企业可以灵活地定期更新指导方案，以适应不断变化的技术和威胁环境。

5.4.4 广泛利用一系列市场杠杆

国家网络安全战略应广泛考虑一系列政策，确保能够切实激励所有组织和个人，使他们能够依据全面的方法和定制工作重点（第4.2节）的原则，履行各自的网络安全责任，化解面临的风险。

确定市场能够和应当推行的措施与风险环境要求之间的差距，是决定何时以及如何利用现有的一系列激励和抑制措施来改善安全的关键一步。为鼓励Cis和 Ciis全面采用网络安全标准和做法，国家网络安全战略应表明政府将考虑一系列可供其使用的政策选项和市场杠杆。

5.4.5 建立公私合作伙伴关系

国家网络安全战略应鼓励建立正式的公私合作伙伴关系，以强化Cis和 Ciis的安全。公私合作伙伴关系是有效保护关键基础设施及管理短期和长期安全风险的基石。它们对增进行业和政府之间的信任至关重要。

然而，建立可持续的伙伴关系需要所有参与的利益攸关方清楚地了解合作伙伴关系的目标和集体努力带来的共同安全利益。其中部分领域包括：就共同的网络安全基线达成一致、创建有效的协调结构、信息共享流程和协议，建立信任、确定并交流改善安全的设想、方法和最佳做法并加强国际协调。

其它参考内容见第63和64页。

5.5 重点领域5 – 能力与能力建设及提高认识

技术和政策考虑可能会主导网络安全讨论，但却忽略了人类基本要素这一核心。此重点领域负责应对推进网络安全能力建设以及提高政府实体、公民、企业和其他组织在认知方面面临的挑战——这对支持国家的数字经济至关重要。

本节考虑的优秀做法包括：推出专门的网络安全课程和认识提高方案，拓展培训计划和劳动力培养方案，采用国际认证计划以及促进创新和研发集团的建设。

5.5.1 开发网络安全课程

国家网络安全战略应促进学校课程的开发，目的是加速网络安全技能的提高并在整个正规教育体系内树立相关意识。此类开发应包括开发专用的网络安全中小学课程，整合高等教育所有计算机科学和IT教案中的网络安全课程，并设立专门的网络安全学位和得到政府支持的学徒制度。

此外，学校课程应促进增强网络安全意识，激发人们对网络安全就业机遇的兴趣。为深入推动此领域的工作，政府还应考虑制定各种激励计划，如建立私人教育项目奖学金和提供相关领域的学徒补贴。

5.5.2 激励实施技能拓展和劳动力培训

国家网络安全战略应为公共和私营部门的专家和普通人士制定网络安全培训和技能发展计划。这项工作的内容或可包括根据行业和政府确定的需求提供高管和业务人员培训，提供正式实习和见习机会，以及开展安全专业人员的（国家和国际）认证。技术培训应辅之以侧重风险管理的举措。

该战略还应推出旨在完善网络安全职业道路（特别针对公共部门）的举措，并通过激励措施增加合格网络安全专业人员的供给。此类举措应与学术界、私营部门和民间团体合作创建。为解决网络安全专家中依然存在的性别差距问题，在为确保未来的包容性而发展各项技能以及开展的各项培训中，均应考虑采取性别均衡的方法，激励、鼓励和促进妇女更多地参与其中。

5.5.3 实施协调一致的提高网络安全认识方案

国家网络安全战略应在国家层面将协调网络安全的工作和活动责任指派给相关权能机构，以确保精简资源并建立问责制。该机构应与相关利益攸关方协作制定并实施网络安全意识方案，同时侧重于传播有关网络安全风险和威胁的信息及应对这些风险和威胁的最佳做法。

提高网络安全意识的方案或可包括：以公众、儿童、遭受数字挑战者为对象的认识提高活动，以消费者为中心的教育方案和针对公共和私营部门高管的增强意识举措。

5.5.4 促进网络安全的创新与研发

国家网络安全战略应营造一种环境，促进各行各业和各利益攸关方团体开展网络安全方面的基础和应用研究。这些举措包括，确保国家的研究工作能为国家实现网络安全战略目标提供支持；在公共研究机构内开展以网络安全为重点的研发项目；有效传播新发现、基线技术、技能、流程和工具等。此外，作为该战略的一部分，各国还应寻求在涉及网络安全的科学领域与国际研究界建立联系，这不仅包括计算机科学、电气工程、应用数学和密码学等技术领域，亦涵盖社会和政治科学、商业和管理研究以及心理学等非技术领域。

该战略应审视捐赠、采购、税收抵免、竞争和其他鼓励网络安全解决方案、产品和服务进行创新的举措中的激励机制。

其它参考内容见第64和65页。

5.6 重点领域6 – 立法和监管

此重点领域的内容涵盖根据包容性原则和信任环境原则（分别见第4.3节和第4.9节）制定法律和监管框架，其目标是保护社会免受网络犯罪的侵害并促进建立一个安全可靠的网络环境。此框架的内容可能包括：界定何为非法网络活动的立法；从法律上认可个人权利和公民自由；建立遵约机制；建设执行该框架的能力；实现关键实体的制度化；并就打击网络犯罪开展国际合作。

5.6.1 网络犯罪立法

国家网络安全战略应促进国内法律框架的发展，明确界定应禁止哪些网络活动并以减少网络犯罪为目标。通常，这种能力以网络犯罪立法的形式体现，其实现方式是颁布特定的新法律或对现有法律做出修正（例如刑法、银行、电信和其他行业的监管法律）。

该战略还应鼓励创建一个进程来监督立法和治理机制的实施与审查，找出差距和机构设置的重叠，明确需要实现现代化的领域并将其列为工作重点（例如老电信法等现有法律）。

5.6.2 承认并捍卫个人权利和自由

国家网络安全战略应根据基本人权原则（第4.5节）保障基本的正当程序权（在刑事调查和起诉的情况下）和数据保护权，包括保护个人数据隐私（可能通过建立数据保护和隐私框架来实现）和言论自由。

5.6.3 创建合规机制

国家网络安全战略应推动建立国内的合规机制（执行和激励机制）。应根据上述法律框架出台合规机制，预防、打击并减轻针对ICT系统和基础设施机密性、完整性和可用性的攻击以及给计算机数据造成威胁的活动。这些机制应包括实施数字调查、合法通信监听和使用电子证据等特殊手段。

5.6.4 推动执法能力建设

国家网络安全战略应鼓励发展网络执法能力，包括对参与打击网络犯罪的一系列利益攸关方（如法官、检察官、律师、执法官员、法医专家和其他调查人员）进行培训和教育。执法部门应接受专门培训，从而能够解释并应用国内网络犯罪方面的法律（即将法律转化为技术概念，或将技术概念转化为法律）；有效发现、阻止、调查和起诉网络犯罪；与工业界和国际执法实体（如国际刑警组织、欧洲刑警组织）有效协作，打击网络犯罪并促进网络安全。此要素应虑及有关能力和能力建设以及提高认识的，重点领域5（第5.5节）中的内容。

5.6.5 建立组织间流程

国家网络安全战略应对在网络犯罪立法得到遵守方面拥有主要权力的国内机构、保护关键基础设施的机构、以及负责确保所有国际网络犯罪方面的要求得到满足（例如确保国家法律符合国际条约规定的义务）且跨越不同司法领域（例如跨境合作）的机构（另见第5．1. 3节和第5. 1. 4节；和第5. 6. 6节）加以确认，并承认他们的职责范围。

在一些法律制度中，可能需要通过立法来建立诸如国家Certs / Cirts / Csirts等参与网络安全事务的机构，或澄清某机构在协调国家网络政策方面的权威。

5.6.6 支持开展打击网络犯罪的国际合作

国家网络安全战略应表明，在可能的情况下，该战略将根据总体国家议程，通过批准打击网络犯罪的国际网络犯罪协定或同等协定及促进国际网络犯罪得到处理的协调机制，致力于在全球范围内保护社会免遭网络犯罪侵害。此方式可能要求国家法律与国际条约义务及双边协定保持一致，例如，通过建立双边法律协助制度允许开展跨境调查和起诉、处理数字证据及引渡。

本要素应虑及有关国际合作的重点领域7（第5.7节）中的内容。

其它参考内容见第65和66页。

5.7 重点领域7 – 国际合作

此重点领域强调了除本国以外，该战略应涵盖的区域和国际层面网络安全要素。网络安全在国际关系的诸多不同领域正发挥着越来越大的作用，这些领域包括人权、经济发展、贸易、商业、军备控制、安全、稳定、和平及冲突的解决。

因此，该战略应认识到网络安全无国界的属性，并强调不仅有必要与国家利益攸关方合作，还需与国际利益攸关方合作。公共和私营国际利益攸关方的参与是促进开展建设性对话、建立信任与合作机制、找到双方均认可的解决方案以应对共同挑战和打造全球网络安全文化的关键所在。

依据全面的方法和定制工作重点的原则（第4.2节）推动开展区域和国际合作，应与国家的政治、社会、文化和经济布局及外交政策的优先事项相协调。

5.7.1 承认网络安全作为外交政策优先事项的重要性

国家网络安全战略应表达出对网络安全国际合作的承诺，并承认网络问题是该国外交政策的组成部分。为此，重要的是鼓励发展并使用侧重于解决网络问题的能力和技能（网络外交），作为传统外交方法和进程的补充。该战略可能还包括建立特定的组织结构，并设立一些专门办公室或培训部分以通过外交手段解决网络问题为主要职责的人员。

更具体而言，该战略应清晰阐明政府的重点工作领域和国际合作的长期目标，包括哪些利益攸关方（例如公共、私营、区域、全球利益攸关方）将参与合作。相关内容可能包括支持建立国际网络安全规范和建立信任的措施，承诺进行网络安全能力建设，参与国际网络安全标准的制定以及参加现有的区域和国际条约。

上述做法可能亦需加强不同政府参与方（例如国家元首和内阁首脑、外交部、信息通信技术部、工业和贸易部、司法部、国防部等）之间地协调，从而使国内参与机构在国际网络安全舞台谈判桌上阐明的政策立场与其他政府机构协调一致。

5.7.2 参与国际讨论

国家网络安全战略应确定相关国家希望加入的具体国际论坛和合作机制，以便针对与网络相关的问题有效施地加外交影响。这些论坛和机制可能包括区域或全球组织、政府间的论坛、公共和/或私营部门联盟，以及涵盖网络安全问题的现有传统合作与协作机制。

随着相关国家开始参与国际讨论，有可能需要政府发展更多侧重于网络问题的能力和技能，并提高总体网络安全能力。因此，重要的是有效确定这些工作的优先次序，同时为其分配充足的资源（人员和资金），以确保这些努力取得具体成果。

5.7.3 促进网络空间的正式和非正式合作

国家网络安全战略应阐明相关国家有意做出采用承诺的，可运行的国际合作机制。相关国家或希望参与国际社会采取的正式和非正式行动，推进在制定政策和立法、执法、事件响应、信息与威胁情报共享等领域的合作。例如，参与这些举措可为相关当局就潜在威胁和脆弱性开展更好的合作与信息交流提供支持。

5.7.4 协调国内外的网络安全工作

国家网络安全战略应考虑现有的区域和国际战略网络安全举措并促进他们保持协调一致。这将使相关国家能够利用现有的最佳做法，并为网络安全方法的统一与融合做出贡献。

为此，该战略应通过使国家法律框架和政策与国际承诺保持一致，以及实现国家网络安全保障方法与国际为此付出的努力相统一的方式，表明该国致力于确保其国内外政策议程的统一性。

现有国际努力可视为该战略一部分，这些知名实例包括但不限于：联合国国际安全背景下信息通信领域发展问题政府专家组（UN GGE）开展的工作、欧洲安全与合作组织（OSCE）树立信心措施（CBM）及网络空间适用国际标准部门采取的行动、七国集团高科技犯罪分工作组开展的工作、欧洲委员会的《布达佩斯网络犯罪公约》、非洲联盟的《网络安全公约》、上海合作组织成员国政府在确保国际信息安全领域开展合作的协定、《阿拉伯国家打击信息技术犯罪公约》、《西非经共体打击网络犯罪指令》，以及北约网络防御合作高级培训中心（NATO CCD COE）对1.0和2.0版《塔林手册》提供的支持。

其它参考内容见第65和66页。

6 参考材料

在本《指南》的编写过程中，对现有指南和最佳做法进行了梳理。

这项工作有利于确定已有效、可支持各国制定各自国家网络安全战略的现有材料。以下清单提供了上述材料的完整目录，包括网页链接。

英联邦打击网络犯罪举措（CCI）（2017年），《刑事事项法律互助哈拉雷协议》

卡耐基梅隆大学（2003年），《计算机安全事件响应团队（CSIRT）手册》

英联邦（2018年），《英联邦网络宣言》

英联邦电信组织（CTO）（2015年），《英联邦制定国家网络安全战略的方式》

欧洲委员会（2001年），《布达佩斯网络犯罪公约》

欧洲联盟理事会（2017年），《网络外交工具箱》

欧洲网络与信息安全局（ENISA）（2014年），《国家网络安全战略评估框架》

ENISA（2011年），《计算机应急响应团队（CERT）运营差距与重叠》

ENISA（2011年），《事件管理良好做法指南》

ENISA（2015年），《确定关键信息基础设施资产与服务的方法》

ENISA（2016年），《国家网络安全战略良好做法指南－制定与落实国家网络安全战略》

ENISA（2012年），《国家网络安全战略：发展与执行实用指南》

ENISA（2012年），《国家网络安全战略，制定加强网络空间安全的国家努力路线》

ENISA（2016年），《国家网络安全战略：培训工具》

ENISA（2016年），《关键信息基础设施的保护－盘点、分析和建议》

ENISA（2016年），《事件响应与网络危机合作战略》

牛津大学全球网络安全能力建设中心（2016年），《国家网络安全能力成熟度模型》

国际电联（2017年），《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》

国际电联（2017年），《全球网络安全指数》

国际电联（2011年），《国家网络安全战略指南》

国际电联（2010年），《了解网络犯罪：现象、挑战及法律对策》

国际电联（2009），《发展中国家网络安全指南》

微软（2013年），《制定国家网络安全战略》

微软（2014年），《关键基础设施保护：概念和连续性》

微软（2014年），《关键连接：保护基础设施》

微软（2014年），《网络安全需求等级》

微软（2018年），《设立有效的国家网络安全机构》

微软（2018年），《网络安全政策框架》

微软（2015年），《网络安全信息共享框架》

微软（2017年），《网络安全风险管理：安全基线》

北约合作网络防御中心（NATO CCD COE）（2012年），《国家网络安全框架手册》

NATO CCD COE（2013年），《国家网络安全战略指南》

美国国家标准与技术研究院（NIST）（2014年），《改进关键信息基础设施网络安全框架》

美洲国家组织（OAS）（2015年），《建立国家计算机安全事件响应小组（CRIST）的最佳做法》

OAS（2004年），《美洲全面网络安全战略：多层面和多学科方式构建网络安全文化》

OAS（2015年），《网络安全意识宣传活动工具包》

OAS（2015年），《美洲网络安全和关键基础设施报告》

经合组织（2015年），《为促进经济社会繁荣管理数字安全风险的建议配套文件》

经合组织（2012年），《处于转折阶段的网络政策制定》

经合组织（2015年），《理事会关于为促进经济社会繁荣管理数字安全风险的建议》

经合组织（2013年），《理事会关于保护个人信息跨国传送及隐私权指导纲领的建议》（《隐私权指导纲领》）

经合组织（2008年），《理事会关于保护关键信息基础设施的建议》

经合组织（2007年），《关于制定关键信息基础设施保护的政策报告》

波托马克政策研究所（2015年），《网络就绪指数2.0 – 网络就绪计划：基线和指数》

联合国（2015年），可持续发展目标

联合国（1976年），《经济、社会及文化权利国际公约》、《公民权利和政治权利国际公约》、《公民权利和政治权利国际公约任择议定书》、第2200号决议（XXI）

联合国（2014年），《数字时代的隐私权》（第A/RES/68/167号决议）

联合国（1948年），《世界人权宣言》

贸发会议（2014年），《信息通信技术政策审查框架》

贸发会议，《制定电子商务立法》

贸发会议（2016年），《数据保护条例与国际数据流动》

UNHR（1976年），《公民权利和政治权利国际公约》

世界银行等（2017年），《打击网络犯罪：面向新兴经济体的工具和能力建设》

针对单个原则和良好做法的参考文献细分目录如下。

国家网络安全战略周期

分议题	参考文献
启动	ENISA（2016年），国家网络安全战略：培训工具 NATO CCD COE（2013年）：《国家网络安全战略指南》，第1.3节
清点工作与分析	ENISA（2016年），国家网络安全战略：培训工具 NATO CCD COE（2013年）：《国家网络安全战略指南》，第2.1、2.2、3.2.1、3.3.1节 NATO CCD COE（2012年）：《国家网络安全框架手册》，第3.4、4节
国家战略的制定	ENISA（2016年），国家网络安全战略：培训工具
落实	ENISA（2016年），国家网络安全战略：培训工具
监测与评估	ENISA（2016年），国家网络安全战略：培训工具 NATO CCD COE（2013年）：《国家网络安全战略指南》，第3.9节 NATO CCD COE（2012年）：《国家网络安全框架手册》，第2.4节

总体原则

分议题	参考文献
愿景	微软（2013年），《制定国家网络安全战略》，第4页 NATO CCD COE（2013年）：《国家网络安全战略指南》，第1.3.1节 经合组织（2015年），《为促进经济社会繁荣管理数字安全风险的建议》 波托马克政策研究所（2015年），《网络就绪指数2.0–网络就绪计划：基线和指数》，第1-3页
综合方法与针对具体情况的优先事项	ENISA（2016年），《国家网络安全战略良好做法指南–制定与落实国家网络安全战略》 牛津大学全球网络安全能力建设中心（2016年），《国家网络安全能力成熟度模型》（CMM），维度1.1，第14页 微软（2013年），《制定国家网络安全战略》，第5页
包容性	CCI（2013年），《核对清单》，第2页 CTO（2015年），《英联邦制定国家网络安全战略的方式》，第4.5和4.6.6节 ENISA（2015年），《确定关键信息基础设施资产与服务的方法》，第3章 ENISA（2016年），《国家网络安全战略评估框架》，3.2 ENISA（2016年），《国家网络安全战略，制定加强网络空间安全的国家努力路线》，第9页 牛津大学全球网络安全能力建设中心（2016年），《国家网络安全能力成熟度模型》（CMM），维度1.1，第14页 国际电联（2011年），《国家网络安全战略指南》，第5.3章 NATO CCD COE（2013年）：《国家网络安全战略指南》，第1.1.3节 NATO CCD COE（2012年）：《国家网络安全框架手册》，第3.4、3.5、4.3节

分议题	参考文献
包容性（续）	OAS（2015年），《网络安全意识宣传活动工具包》，第20页 OAS（2015年），《美洲网络安全和关键基础设施报告》，第2页 经合组织（2015年），《理事会关于为促进经济社会繁荣管理数字安全风险的建议》，第14-15页 经合组织（2013年），《理事会关于保护个人信息跨国传送及隐私权指导纲领的建议》（《隐私权指导纲领》）；《经修订的经合组织隐私权指导补充说明备忘录》，第31页 波托马克政策研究所（2015年），《网络就绪指数2.0–网络就绪计划：基线和指数》，第3-6页 贸发会议（2016年），《数据保护条例与国际数据流动：对贸易和发展的影响》 贸发会议（2014年），《信息通信技术政策审查框架》
经济与社会繁荣	微软（2014年），《网络安全需求等级》第1章 NATO CCD COE（2012年）：《国家网络安全框架手册》，第1.5.1、2.2.1节 波托马克政策研究所（2015年），《网络就绪指数2.0–网络就绪计划：基线和指数》，第1-3页
基本人权	CCI（2013年），《核对清单》，2.6.5 CTO（2015年），《英联邦制定国家网络安全战略的方式》，原则4 ENISA（2014年），《国家网络安全战略评估框架》，3.1.1目标 联合国（1976年），《经济、社会及文化权利国际公约》、《公民权利和政治权利国际公约》、《公民权利和政治权利国际公约任择议定书》

分议题	参考文献
基本人权（续）	国际电联（2011年），《国家网络安全战略指南》，第7.4章 微软（2013年），《制定国家网络安全战略》，第5页 NATO CCD COE（2013年）：《国家网络安全战略指南》，第1.3.1、1.3.3节 NATO CCD COE（2012年）：《国家网络安全框架手册》第1.5.4、1.5.5、5.2.6节 经合组织（2015年），《为促进经济社会繁荣管理数字安全风险的建议配套文件》，原则9和原则3 贸发会议（2016年），《数据保护条例与国际数据流动：对贸易和发展的影响》 联合国（1948年），《世界人权宣言》 联合国（1976年），《经济、社会及文化权利国际公约》、《公民权利和政治权利国际公约》、《公民权利和政治权利国际公约任择议定书》 联合国（2014年），《数字时代的隐私权》
风险管理和复原力	ENISA（2016年），《国家网络安全战略良好做法指南–制定与落实国家网络安全战略》 牛津大学全球网络安全能力建设中心（2016年），《国家网络安全能力成熟度模型》（CMM），维度1.3，第15页 微软（2013年），《制定国家网络安全战略》，第6页 微软（2017年），《网络安全风险管理：安全基线》 经合组织（2015年），《为促进经济社会繁荣管理数字安全风险的建议》与配套文件
适当的政策工具	ENISA（2016年），《国家网络安全战略良好做法指南–制定与落实国家网络安全战略》 NATO CCD COE（2013年）：《国家网络安全战略指南》，第3.1节 NATO CCD COE（2012年）：《国家网络安全框架手册》，第1.4节

分议题	参考文献
明确的领导力、作用和资源分配	ENISA （2016年），《NCSS良好做法指南–制定和落实国家网络安全战略》 NATO CCD COE（2012年）：《国家网络安全框架手册》，第4节 微软（2018年）：《设立有效的国家网络安全机构》 波托马克政策研究所（2015年），《网络就绪指数2.0–网络就绪计划：基线和指数》，第1-7节
可信的环境	牛津大学全球网络安全能力建设中心（2016年），《国家网络安全能力成熟度模型》（CMM），维度2.2，第25页 NATO CCD COE（2013年），《国家网络安全战略指南》，第1.3.1节 波托马克政策研究所（2015年），《网络就绪指数2.0》，第4、6节

国家网络安全战略良好做法

分议题	参考文献
重点领域 1 – 治理	CCI（2013年），《核对清单》 CTO（2015年），《英联邦制定国家网络安全战略的方式》，第4.4.1、4.4.4、4.4.5、4.4.8、4.4.9、4.4.20、4.4.21、4.4.34、4.5节 ENISA（2016年），《国家网络安全战略良好做法指南–制定与落实国家网络安全战略》，第3.1、3.2、3.4、3.5、3.17节 ENISA （2016年），《国家网络安全战略评估框架》，第2.2.1、3.1.1、3.1.2、3.1.3节 ENISA （2016年），《国家网络安全战略：确定加强网络空间安全的国家努力路线》第4、6节 牛津大学全球网络安全能力建设中心（2016年），《国家网络安全能力成熟度模型》（CMM），维度1.1、1.5、1.6，第14-15页 国际电联（2011年），《国家网络安全战略指南》，第5.2.1、5.3、7.2、7.3、11.1、11.2、20、20.2节 微软（2013年），《制定国家网络安全战略》，“实现网络安全的原则方法–确立明确的优先事项和安全基线” 微软（2018年），《设立有效的国家网络安全机构》 NATO CCD COE（2013年），《国家网络安全战略指南》，第1.1、3.3、3.8节 NATO CCD COE（2012年），《国家网络安全框架手册》，第1.4.2、2.1.1、2.1.3、2.2、2.3、2.4、3.1、3.5、4、5.3.1节 经合组织（2012年），《处于转折阶段的网络政策制定》，附件四 经合组织（2013年），《理事会关于保护个人信息跨国传送及隐私权指导纲领的建议》（《隐私权指导纲领》） 经合组织（2015年），《理事会关于为促进经济社会繁荣管理数字安全风险的建议》，2-A，配套文件

分议题	参考文献
重点领域 1 – 治理（续）	经合组织（2008年），《理事会关于保护关键信息基础设施的建议》 波托马克政策研究所（2015年），《网络就绪指数2.0》，第1节
重点领域 2 – 国家网络安全中的风险管理	CTO（2015年），《英联邦制定国家网络安全战略的方式》，第4.4.6、4.4.15、4.4.24、4.4.25、4.4.26、4.4.27节 ENISA（2016年），《国家网络安全战略良好做法指南–制定与落实国家网络安全战略》，第3.3节 牛津大学全球网络安全能力建设中心（2016年），《国家网络安全能力成熟度模型》（CMM），维度1.3，第14页 国际电联（2011年），《国家网络安全战略指南》，第10.1.2节 微软（2017年），《网络安全风险管理：安全基线》 微软（2013年），《制定国家网络安全战略》，“确立风险管理办法”–章 NATO CCD COE（2013年），《国家网络安全战略指南》，第3.5节 NATO CCD COE（2012年），《国家网络安全框架手册》，第2.1.2、5.3.2节 NIST（2015年），《改进关键信息基础设施网络安全框架》 OAS（2018年），《国家网络风险管理》 经合组织（2008年），《理事会关于保护关键信息基础设施的建议》 经合组织（2015年），《理事会关于为促进经济社会繁荣管理数字安全风险的建议》 波托马克政策研究所（2015年），《网络就绪指数2.0》，第1节
重点领域 3 – 就绪与复原力	卡耐基梅隆大学（2003年），《计算机安全事件响应团队（CSIRT）手册》 CCI（2013年），《核对清单》

分议题	参考文献
重点领域 3 – 就绪与复原力（续）	CTO（2015年），《英联邦制定国家网络安全战略的方式》，第4.4.3、4.4.20、4.4.21、4.4.22、4.4.27、4.4.31节 ENISA（2016年），《国家网络安全战略良好做法指南–制定与落实国家网络安全战略》，第3.6、3.7、3.10、3.14、4.1、4.5、4.8节 ENISA（2016年），《事件响应与网络危机合作战略》 ENISA （2011年），《CERT运作差距与工作重叠》 ENISA（2011年），《事件管理良好做法指南》 牛津大学全球网络安全能力建设中心（2016年），《国家网络安全能力成熟度模型》（CMM），维度1.2，第14页 国际电联（2011年），《国家网络安全战略指南》，第11.3、17.3节 微软（2017年），《网络安全风险管理：安全基线》 微软（2015年），《网络安全信息共享框架》 微软（2013年），《制定国家网络安全战略》，“事件响应能力建设”–节 NATO CCD COE（2013年）：《国家网络安全战略指南》，第3.5节 NATO CCD COE（2012年）：《国家网络安全框架手册》，第3.2、4.2.2节 OAS（2016年），《建立国家计算机安全事件响应小组（CRIST）的最佳做法》，第35页 OAS（2004年），《美洲全面网络安全战略：多层面和多学科方式构建网络安全文化》，第3-4页 经合组织（2015年），《理事会关于为促进经济社会繁荣管理数字安全风险的建议》，第2-B节 波托马克政策研究所（2015年），《网络就绪指数2.0》，第2、4节

分议题	参考文献
重点领域 4 – 关键基础设施服务/基础服务	CTO（2015年），《英联邦制定国家网络安全战略的方式》，第4.4.12、4.4.13、4.4.20、4.4.25、4.4.26、4.4.28、4.4.32节 牛津大学全球网络安全能力建设中心（2016年），《国家网络安全能力成熟度模型》（CMM），维度1.3、1.4，第14页；维度5.2，第49页 ENISA（2016年），《国家网络安全战略良好做法指南–制定与落实国家网络安全战略》，第3.6节 ENISA（2015年），《确定关键信息基础设施资产与服务的方法》 ENISA（2016年），《国家网络安全战略评估框架》，第4.2节 国际电联（2011年），《国家网络安全战略指南》，第5.1.1、5.3.3、11.4节 微软（2017年），《网络安全风险管理：安全基线》 微软（2014年），《关键基础设施保护：概念和连续性》，所有章节 微软（2014年），《关键连接：保护基础设施》，所有章节 NATO CCD COE（2013年）：《国家网络安全战略指南》，第3.4、3.5节 NATO CCD COE（2012年），《国家网络安全框架手册》，第4.5.4节 OAS（2015年），《美洲网络安全和关键基础设施报告》 经合组织（2015年），《理事会关于为促进经济社会繁荣管理数字安全风险的建议》 经合组织（2008年），《理事会关于保护关键信息基础设施的建议》：第一部分、第二部分 波托马克政策研究所（2015年），《网络就绪指数2.0》，第2、4节

分议题	参考文献
重点领域 5 – 能力、能力建设与提高认识	CCI（2013年），《核对清单》 CCI（2005年、2017年），英联邦联络人框架 CCI（2011年），《刑事事项法律互助哈拉雷协议》 CTO（2015年），《英联邦制定国家网络安全战略的方式》，第4.4.11、4.4.17、4.4.20、4.4.34、4.4.12、4.4.14、4.4.16、4.4.23节 ENISA（2016年），《国家网络安全战略良好做法指南–制定与落实国家网络安全战略》，第3.12、3.8、3.11、3.13、4.3、4.6、4.7、4.14节 ENISA（2016年），《事件响应与网络危机合作战略》，第2.1节 ENISA（2011年），《CERT运作差距与工作重叠》，第6、16、19、21、27、29、31、32、50、57页 ENISA（2010年），《事件管理良好做法指南》，第 19、23、26、32、46、56、58、64、69页 牛津大学全球网络安全能力建设中心（2016年），《国家网络安全能力成熟度模型》（CMM），维度1.5，第15页；维度2.1、2.2、2.3，第25页；维度3-1、3-2、3-3，第32页；维度5.6，第49页 国际电联（2011年），《国家网络安全战略指南》，第5.3.7、5.3.8、12.4、12.1、12.3、18节 微软（2013年），《制定国家网络安全战略》，“推动研究和技术投资、公众意识、工作人员培训与教育”一节 NATO CCD COE（2013年），《国家网络安全战略指南》，第3.5节 NATO CCD COE（2012年），《国家网络安全框架手册》，第4.5.5、4.6.3节 OAS（2015年），《网络安全意识宣传活动工具包》，所有章节

分议题	参考文献
重点领域 5 – 能力、能力建设与提高认识（续）	经合组织（2015年），《理事会关于为促进经济社会繁荣管理数字安全风险的建议》，第2-B节 波托马克政策研究所（2015年），《网络就绪指数2.0》，第2、5节 贸发会议（2015年），电子商务和法律改革方案
重点领域 6 – 立法与监管	CCI（2013年），《核对清单》 CTO（2015年），《英联邦制定国家网络安全战略的方式》，第4.4.5、4.4.6、4.4.7、4.4.8、4.4.9、4.4.18、4.4.19、4.4.20节 欧洲委员会（2001年），《布达佩斯网络犯罪公约》，第15条 ENISA（2016年），《国家网络安全战略良好做法指南–制定与落实国家网络安全战略》，第3.15、3.184.9、4.12节 牛津大学全球网络安全能力建设中心（2016年），《国家网络安全能力成熟度模型》（CMM），维度4.1、4.2、4.3，第39-40页；维度5.7，第50页 UNHR（1976），《公民权利和政治权利国际公约》，第19条 国际电联（2011年），《国家网络安全战略指南》，第5.3.4、5.3.5, 9、11.5、12.2、15节 国际电联（2010年），国际电联网络犯罪立法工具包 NATO CCD COE（2013年），《国家网络安全战略指南》，第3.2节 NATO CCD COE（2012年），《国家网络安全框架手册》，第5节 OAS: 波托马克政策研究所（2015年），《网络就绪指数2.0》，第3节 联合国（2015年），可持续发展目标16.3 贸发会议，全球网络法跟踪系统 世界银行等，《打击网络犯罪：面向新兴经济体的工具和能力建设》

分议题	参考文献
重点领域 7 – 国际合作	CTO（2015年），《英联邦制定国家网络安全战略的方式》，第4.4.20、4.4.21节 ENISA（2016年），《国家网络安全战略良好做法指南–制定与落实国家网络安全战略》，第3.16和4.10节 ENISA（2016年），《国家网络安全战略指南》，第3.16节 牛津大学全球网络安全能力建设中心（2016年），《国家网络安全能力成熟度模型》（CMM），维度4.3，第40页 国际电联（2011年），《国家网络安全战略指南》，第5.3.9、10.2.2、13、19节 微软（2013年），《制定国家网络安全战略》，“建立国际参与架构”–节 NATO CCD COE（2013年），《国家网络安全战略指南》，第1.3、3.2.1、3.3.2节 NATO CCD COE（2012年），《国家网络安全框架手册》，第4.7、5.4.2、5.4.3节 经合组织（2008年），《理事会关于保护关键信息基础设施的建议》，第4、5章 经合组织（2015年），《为促进经济社会繁荣管理数字安全风险的建议》，第13、48、58页 波托马克政策研究所（2015年），《网络就绪指数2.0》，第4、6节

7 缩略语

缩略语	定义
CCI	英联邦打击网络犯罪举措
CERT	计算机应急响应团队
CBM	建立信任措施
CII	关键信息基础设施
CTO	英联邦电信组织
ENISA	欧洲网络与信息安全局
ICT	信息通信技术
ITU	国际电信联盟
NATO CCD COE	北约合作网络防御中心
NIST	美国国家标准与技术研究院
OAS	美洲国家组织
OECD	经济合作与发展组织
UN	联合国
UNCTAD	联合国贸易和发展会议

ISBN: 978-92-61-27795-6