网络就绪指数2.0
CYBER READINESS INDEX 2.0

网络就绪度计划：基线和指数

A PLAN FOR CYBER READINESS: A BASELINE AND AN INDEX

〔美〕梅丽莎·海瑟薇 / 著　鲁传颖 / 译

信息安全与通信保密杂志社

序 言

网络就绪指数 2.0（CRI 2.0）——一项网络就绪计划，是建立在 2013 网络就绪指数 1.0 方法论基础上的基线和指数，力求使网络不安全造成的经济损失透明化，并鼓励各国将本国经济前景与国家安全重点放在一起。网络就绪指数 2.0 挑战了传统意义上认为网络安全主要是国家安全的论点。它展现了当网络安全（安全和韧性）可以带领经济增长和繁荣时，国家安全与互联网链接及信息通信技术的快速应用交织在一起。

网络就绪指数 2.0 由两个主要部分组成。第一，它客观地评估和衡量了各国对国家网络安全风险的就绪水平，以便向各国领导人通报为保护联系日益紧密的国家和潜在的国内生产总值增长所需采取的措施。第二，网络就绪指数 2.0 将网络就绪的核心组成部分记录为各国遵循的可操作蓝图，并因此定义了对一个国家来说什么是“网络就绪”。 这种全面的、比较的、基于经验的方法在七个基本要素中使用了超过 70 个独特的指标，以识别业务就绪的活动，并确定以下类别的改进领域：国家战略、事件响应、网络犯罪和执法、信息共享、研发投资、外交和贸易，以及防御和危机应对。由此产生的可操作的蓝图使一个国家能够更好地了解其互联网基础设施的依赖性和脆弱性，并评估其承诺和成熟度，以缩小其目前的网络安全态势和支持其数字未来所需的国家网络能力之间的差距。

网络就绪指数 2.0 是唯一公开可以获得的使用阿拉伯文、中文、英文、法文、俄文和西班牙文撰写的方法论，并且被各国政府、国际机构、智囊团、研究人员和公司视为一种平衡资源，用于评估和衡量国家、区域和地方各级的网络灾备情况。

通过公布每个国家的详细概况，CRI 2.0 方法论持续得到全球认可。自 2015 年该方法论发布以来，已为以下 9 个国家：美国、英国、日本、印度、荷兰、意大利、德国、法国和沙特阿拉伯出版了国家概况。这些概况吸引了各国对于网络就绪水平的关注，同时强调了通向网络就绪的独特方法。下面的段落就强调了其中的一些观察所得。

早在 20 世纪 90 年代初期，美国就已认识到在政府与产业界之间共享信息的重要性。然而，针对其网络环境受到威胁的数量和速度，迫切需要另一种方式来改变“老式的”人对人的信息交换。2015 年，美国开始了一个以实时自动方式分享网络威胁指标和防御措施的计划。自动指标共享（AIS）系统旨在自动地向以下组织机构提供信息：联邦部门和机构、私营企业、信息共享和分析中心（ISAC）。为了便于实现实时、自动的信息共享，美国国土安全部正在推进使用 STIX、TAXII 或 CybOX 协议——用于编码和传输高保真信息的标准语言、服务和消息交换。这些协议将有助于交换威胁评估和特性（详细的攻击模式）、恶意软件特性、操作事件管理、日志文件、指标共享、数字取证和广泛的网络态势感知。

英国于 2017 年初打开了国家网络安全中心（NCSC）的大门。NCSC 成为产业界和政府之间的桥梁。政府通讯总部（GCHQ）在 NCSC 中扮演着不可或缺的角色，对国家实施积极主动的网络防御态势至关重要。正因为如此，NCSC 开始在全国范围内实现边界网关协议（BGP）安全和域名系统（DNS）安全。此外，NCSC 是网络威胁情报的英国枢纽——了解对于国家及其企业和公民的威胁。它正在实施可控的安全服务方案、信息共享计划和其他举措，以迅速减少脆弱性，提高英国的整体网络安全水平。

日本正在利用即将举办的 2019 届世界橄榄球锦标赛与 2020 届奥运会和残奥会，建立网络安全体系并将其作为国家的优先发展事项，重新重视发展网络安全能力和应变能力。日本还预计，到 2020 年本国信息和通信技术部门体量将翻一番，同时宣布

其目标是在 2020 年成为世界上最先进的信息技术（IT）国家。政府正在努力创造合适的环境以期达成这一目标，并与即将举办的奥运会的最后期限相契合。事件就绪和网络安全战略国家中心（NISC）作为政策的中央协调机制，监测操控大量个人信息的政府相关组织，在危机时期，包括发生对关键基础设施的攻击时，提供指挥和控制。这也是日本 2020 年愿景的一个组成部分。

印度政府发展了一系列培训中心，以提高其在科学、技术、政策和法律交叉点上的能力和理解力。例如，在班加罗尔印度大学法学院关于网络法律和取证的高级研究、发展和培训中心，通过向司法官员、检察官、调查机构、网络安全人员、技术人员和其他人提供培训和教育，将法律转化为技术术语，反之亦然。目前，该中心由电子和信息技术部资助，它提供了一个独特的动手培训部分。此外，在印度政府和印度数据安全委员会（DSCI）以及国家软件和服务公司协会（NASSCOM）之间建立了一种公私伙伴关系，在孟买、班加罗尔、浦那和加尔各答成立了网络实验室。这些实验室旨在网络安全和取证方面对执法官员和行业合作伙伴进行训练。已经有超过 49,000 人通过 DSCI 网络实验室泛印度项目接受了训练。

荷兰在提升军事态势方面处于欧洲领先地位。它是最早将其军事网络任务和能力发展与北约《2010 里斯本网络防御宣言》以及随后的芝加哥、威尔士和华沙峰会宣言紧密结合起来的国家之一。尽管在其他领域存在军事缩编和广泛的预算削减，但是国防部在提升武装部队的网络作战能力方面仍积极投入。2014 年荷兰成立国防网络司令部，以领导业务和网络能力的发展，同时将进攻能力的开发和部署涵盖进来。荷兰是欧洲第一个对外承认需要具备进攻性网络能力的国家，它声称，网络行动应纳入军事任务，并成为任务指挥官工具箱中的又一工具。该国清楚地认识到，安全不仅是一个社会良好运作的前提，而且是其未来经济发展的保障。

意大利的邮政和通讯警务联手，与美国保密服务一道建立了欧洲电子犯罪特遣队（EECTF）。该机构专注于广泛的“基于计算机的犯罪活动”，包括身份盗窃、

网络入侵以及影响到金融部门和其他重要基础设施的与计算机有关的犯罪。总部设在罗马的欧洲 EECTF 监控计算机网络使用意大利邮政服务（Poste Italiane S.P.A.）的威胁软件，从欧洲执法当局、企业、安全解决方案提供商、情报机构和专家收集网络犯罪信息。此外，EECTF 积极共享有关网络犯罪的信息和警报，并建立了专门的工具，与其他成员组织交流专家意见、知识、最佳做法和共同的解决办法。这些成员组织包括国际执法机构（例如保加利亚警察、罗马尼亚警察和西班牙警察）、金融机构（例如美国运通、花旗银行和万事达卡支付公司）、国际组织（例如 ENISA、反钓鱼工作组 APWG、联合国区域间犯罪和司法研究所 UNICRI 以及数字犯罪财团）、信息安全厂商（例如卡巴斯基、赛门铁克和威瑞森）和学术界（例如博洛尼亚大学、萨勒诺大学和都柏林大学）。

德国正带领欧洲利用不同的市场激励机制来促进网络安全解决方案的生成。德国政府在以下三个领域提供与网络安全有关的企业研发奖励：计算机技术，意味着在数字化的世界中工作；ICT，意味着检测和解决网络安全事件；电子流动性，意味着价值链提议。此外，德国正积极努力，通过设立一个新的研究所——德国互联网协会来解决网络安全专业人员严重短缺的问题，并为包括爱因斯坦数字未来中心等其他举措提供支持（ECDF）。这将连接几个公共实体和大学，包括柏林工业大学、柏林自由大学、洪堡大学、柏林大学和柏林慈善医科大学，以及八所著名的研究机构和两所应用科学大学。

法国正努力将雷恩地区打造成法国和欧洲领先的网络枢纽。法国把政府机构集中在网络防御和情报方面，与大学项目和法国工业一道创造一个强大的网络安全和防御生态系统，产生下一代的技术解决方案，同时发展具备资质的人才队伍，孵化创业社区企业推动创新和数字经济。

沙特阿拉伯王国正处于成为网络就绪国家的筹备过程中。2017 年 7 月，沙尔曼国王颁布了一系列王室法令，其中最著名的是设立了国家安全主席。它是一股新的国

家安全力量，将集中安全事务的权力，包括网络安全、反恐和国内情报。该机构将包括之前内政部（MOI）的一部分部门，例如特别应急部队、技术事务、安全航空、民事和军事人员以及负责打击恐怖主义和处理其他安全问题的部门。此外，法令指出或许最早在 2018 年 1 月完成从内政部到总统对于国家网络安全中心（NCSC）的重新配置。NCSC 将成为王国中网络安全的重点。在接下来的几个月里，国家安全主席将有机会通过开发和制定国家网络安全框架与策略使沙特阿拉伯变得更为强大，同时通过确保相应的投资，以减少其当前的和长远的面临网络威胁的风险。

网络就绪指数 2.0 为回答什么是国家网络就绪制定了标准——直接帮助各国政府继续开展网络安全实践并制定政策。国家概况描述了各国在成为网络就绪过程中应用的独特方法，并有助于各国网络利益相关者深入了解每个国家网络计划的根源和目前的成熟程度。国家概况还可以通过跨文化交流的有效做法，促进更好的互动和合作。网络就绪指数 2.0 提供了一种全面的（也是易于使用的）的方法论来确定加强安全态势的基本要素，以防范网络不安全所造成的对国内生产总值的侵蚀。它可被作为一个工具，用来评估从所有政府和所有国家的角度出发，某一特定国家在成熟度曲线上的位置。当各种指标被放在一起考虑的时候，网络就绪指数 2.0 为各国政府评估和调整其经济与国家安全发展提供了一份蓝图。

梅丽莎 • 海瑟薇

2017 年 10 月 8 日

译者序

本书汇集了网络安全就绪度的方法论，在对世界20多个国家进行深入分析的基础上，作者选择最具代表性的美、日、法等八个国家撰写网络就绪度报告并进行重点论述，是一本以国家为单位来衡量网络安全状况的实用性研究著作。作者梅丽莎·海瑟薇在美国政府中长期从事网络安全工作，曾担任美国白宫国家安全委员会负责网络安全事务的主要官员，并成立了白宫网络安全办公室。其负责制定的《网络安全政策评估》是美国政府首次把网络安全提升到战略层面的一次尝试，得到了奥巴马总统的高度评价。

从政府部门离职后，海瑟薇活跃在学术界和企业界，分别兼任了哈佛肯尼迪学院贝尔弗科学与国际事务中心、哥伦比亚大学技术管理中心高级顾问，同时为公共和私人客户进行多学科和多视角的战略咨询与战略制定。海瑟薇先后为多国政府、全球组织、财富500强企业提供网络安全、企业风险管理和技术评估咨询。

网络就绪度是其致力于网络安全研究的一项重要成果，希望能够在对全球网络安全状况作出详细分析之后，给各国政府、学术界和产业界一个参照的对象。不同于其他指数类排名，本书汇集的报告是建立在各国政府官方政策文件，参与国际和地区网络安全事务的实践之上，因此，具有较强的参考价值。

同时也应当注意到，网络安全本身是一个复杂的领域，涉及政治、经济、安全、文化、社会等方方面面。就绪度按照国家战略、事件响应、电子犯罪与执法、信息共享、研发投资、外交与贸易、防御与危机应对七个方面进行评估，是否能够完整地反映出

实际情况也需要进一步的研究。此外，各个国家的国情不同，不同的决策体系、层次，甚至语言都给报告的研究带来了很大的困难。因此，我们也看到各个国家报告的完整性和详实度方面还存一定程度的差异。

当然，这些困难和挑战不仅体现了作者非凡的勇气和精湛的研究能力，也为我们研究全球网络安全提供了一个有益的参考。我们希望能够有越来越多的中国学者加入到全球网安全研究的队伍中，将目光瞄准更多的国家和地区，在深入研究的基础上，为全球网络安全的治理贡献中国智慧，提供中国方案。

本书在翻译过程中得到了海瑟薇女士的大力帮助，她还专门为本书作序，同时，也离不开信息安全与通信保密杂志社副总编辑唐莉、主编惠志斌的大力支持。本书的翻译有很多业界专家和学者的共同参与，具体分工如下：鲁传颖副研究员负责美国和日本报告，许蔓舒副教授负责印度报告，张腾军博士负责德国报告，张坤博士负责法国和沙特阿拉伯报告，韩小涵女士负责荷兰和意大利报告，王衍女士负责英国报告。

鲁传颖

2017 年 11 月 2 日

目　录

没有国家做好了网络准备

简介

在全球经济中，国民经济增长在很大程度上取决于信息通信技术（ICT）。同时，许多国家面临重大的经济损失，因为信通技术的安全问题削弱了这一增长。 到目前为止，没有任何方法来评估国家的成熟度和承诺，以保障其数字化未来和增长依赖的网络基础设施和服务。

网络准备就绪指数（CRI）1.0 版代表了一种检查此问题的新方法，旨在引发国际讨论，激发全球对解决网络不安全导致经济衰退问题的压力，从而促进经济增长。CRI 检查了接受 ICT 和互联网的 35 个国家，然后采用客观的方法来评估每个国家对 5 个基本要素的网络安全的成熟度和承诺。 评估网络安全进展的整体方法表明了包括政府监管和执法在内的凝聚战略的重要性，以及以市场为基础的激励措施和经济杠杆，将公共和私营部门的重视放在安全繁荣的数字化未来。

背景

近 50 年来，特别是近 25 年来，信通技术和互联网一直处于关键基础设施、服务、企业和社会技术转型的前沿。今天，各国正在为每一个家庭和企业提供无处不在的通信，并推行发展和现代化议程，将信息社会培育成数字时代。诸如电子政务、电子银行、电子卫生、电子学习、下一代电网、空中交通管制等基本服务的举措在大多数国家的经济议程中处于领先地位，正在追求这些举措来提高生产力和效率，提高员工技能，推动创新，实现 GDP 增长。一些估计提到，当 10% 的人口与互联网相连时，国内生产总值应增长 1% 至 2%。此外，拥抱互联网和信息通信技术的政府和企业认识到，

这将提高其长期竞争力和社会福祉，并可能贡献国内生产总值的 8%。最近的报道进一步表明，工业系统现代化（例如电力电网、石油和天然气管道、工厂运营等）的经济机会占未来十年全球经济的 46%。

国家不能忽视这种经济机会，特别是在当今经济停滞不前的情况下。然而，这种核心基础设施的可用性、完整性和韧性受到广泛的恶性网络活动的侵蚀，这是有害的。例如，据估计，20 国集团（G20）假冒和盗版的就业机会有 250 万人，政府和消费者每年亏损 1250 亿美元，其中包括税收亏损。美国估计，国际知识产权盗窃对美国经济的年影响为 3000 亿美元。这近似于 GDP 的 1%。此外，荷兰独立研究机构 Toegepast Natuurwetenschappelijk Onderzoek（TNO）的研究表明，网络犯罪使荷兰社会每年至少耗资 100 亿欧元，占国内生产总值的 1.5% 至 2%。这种损失几乎等于荷兰 2010 年的经济增长。英国和德国进行的其他估计显示出类似的损失。任何一个国家都不能容忍将其国内生产总值的一个百分点的损失用于减少非法网络活动。

衡量收益下降可能会迫使政府将其数字化议程和经济愿景与网络安全战略保持一致，并投资于两者的衍生价值。为经济损失带来透明度，可能会引发国家和全球在应对经济衰退方面的兴趣。因此，网络安全措施可以实现和维护 ICT 股息的承诺，并帮助各国实现互联网经济的全部潜力。

CRI 方法论

CRI 确定了网络安全，可用于保护以前 ICT 投资的价值和完整性以及实现互联网经济的 5 个基本要素。对每个国家是否处于成熟和对网络安全承诺的初步客观评估，可以通过迄今为止对这 5 个基本要素中的每一个采取了哪些步骤来衡量。为了更深入地分析 5 个基本要素中的每个内容，未来的研究可能会添加子索引，以进一步详细探讨每个国家对网络安全承诺的水平。

5 个基本要素是：

（1）制定和出版国家网络安全战略。

（2）该国家是否有运行的计算机应急小组（CERT）或计算机安全事故应急小组（CSIRT）。

（3）该国家是否表现出防止网络犯罪的承诺？

（4）该国家有信息共享机制吗？

（5）该国家针对网络安全基础和应用研究以及网络安全计划的投资是否广泛？

首先，国家是否制定了（并出版了）“国家网络安全战略”，描述了对该国的威胁，

并概述了必须采取的步骤、方案和举措来应对威胁。理想情况是，以经济方式说明战略问题；确定确保战略执行的主管当局——负责任的实体；在实施计划中包括具体的、可衡量的、可实现的、基于结果的和基于时间的目标；它将认识到在竞争环境中需要提供有限的资源（如政治意愿、金钱、时间和人力）来实现必要的经济成果。

为了更详细地探索这一领域，子索引可能会解决以下问题：

（1）该计划占 GDP 的百分比是多少？

（2）是否已经确定了影响和负责实施该计划的商业实体？

（3）是否已经确定了关键的服务（不是关键的基础设施）？

（4）是否为每个关键服务建立了服务协议（每周 24 小时 ×7 天）和中断报告要求的连续性？

其次，国家是否有运行的计算机应急响应小组（CERT）或计算机安全事故应急小组（CSIRT），以便在发生影响关键业务和信息基础设施的自然灾害或人为灾难的情况下，进行国家事件的反应？

为了更详细地探索这一领域，子索引可能会解决以下问题：

（1）是否有针对紧急情况和危机发布的事件应急计划？是否映射跨部门的依赖关系，解决运营和灾难恢复机制的连续性？是否已行使和更新？

（2）在关键服务和信息基础设施方面是否有强大的事件管理、韧性和恢复能力？

（3）是否建立了政府和监管机构国家联络点网络？

（4）建立关键行业国家联络点网络，对运营和恢复至关重要的服务和信息基础设施至关重要。

（5）是否建立了信息共享和警报系统？如果是这样，国家危机或响应中心是否会及时发出警报？

再次，国家是否表现出保护社会免遭网络犯罪的国际承诺？就CRI初始评级而言，使用了两项国际条约协议。第一项是欧洲委员会《网络犯罪公约》。第二项是上海合作组织《确保国际信息安全领域合作协议》。审评委只接受已经批准或加入这些条约的国家，因为只有这样，一个国家才有具体的义务和根据国际法维护其政治承诺的权利。根据这些条约，国家同意通过适当立法，促进国际合作，打击犯罪行为，促进国内和国际层面的侦查、调查和起诉。

为了更详细地探索这一领域，子索引可能会解决以下问题：

（1）是否有会计机制来确定国内生产总值受到网络犯罪影响的实际百分比 .

（2）是否对政府和关键基础设施网络进行一年一度的威胁评估？

（3）该国是否针对计算机系统、网络和计算机数据的机密性、完整性和可用性以及滥用此类系统、网络和数据的行为建立刑事犯罪行为立法？

（4）国家是否审查现行法律和监管治理机制？确定差距和重叠部门所在的地方，澄清并优先考虑哪些领域必须首先解决？（例如现行法律《旧电信法》和互联网时代的新要求）

表 1 网络就绪指数检测国家

网络就绪指数检查了着力发展信息通信技术和互联网的 35 个国家和地区，并比较了他们的成熟度和承诺，通过对每个国家在 5 个领域的网络安全的地位进行初步客观的评估来保护这些投资。		
阿根廷	印度	沙特
澳大利亚	印度尼西亚	新加坡
奥地利	以色列	南非
巴西	意大利	韩国
加拿大	日本	西班牙
中国	卢森堡	瑞士
丹麦	澳门	瑞典
芬兰	墨西哥	中国台湾地区
法国	荷兰	土耳其
德国	新西兰	英国
中国香港地区	挪威	美国
冰岛	俄罗斯	

选择标准

CRI 选择了国际电信联盟（ITU）信通技术发展指数和世界经济论坛（WEF）网络准备指数的前 20 个国家，以确定哪些国家正在接受信息和通信技术，并投资于可访问和负担得起的互联网服务，以促进经济增长。通过增加 20 国集团经济体的成员来进一步改进选择，因为它们代表的是：全球 GDP 的 90%，国际贸易的 80%，世界人口的 64%，化石燃料排放的 84%。 它也使巴西、俄罗斯、印度、中国和南非的经济增长最快。 最后，就世界银行的数据和国家按国内生产总值排名进行了磋商。前 20 名 GDP 贡献者为该指数增加了另外一个国家。 表 1 列出了包括在 CRI 中的 35 个国家和地区。

初步结果

首次应用 CRI 的初步结果表明：

（1）20 国集团预计，通过无处不在的通信和 ICT 采用率，国内生产总值增长率将至少达到 4%。

（2）一些国家在所有类别（例如澳大利亚、加拿大、荷兰、英国、美国）都采取行动领先指数，即使这些国家由于网络不安全而经历 GDP 下降。

（3）35 个国家和地区中有 27 个拥有网络安全战略，但很少有人正在衡量其进展情况，更少投资于该战略的成功结果。

（4）几乎所有国家都通过国家 CERT，或通过事件响应者论坛的事件响应能力。

（5）35 个国家和地区中有 20 个国家通过采取适当立法，促进国际合作和打击犯罪行为，通过促进国内和国际层面的侦查、调查和起诉，来保护社会免遭网络犯罪。

（6）很少有国家正在投资私人和公共信息共享交流，甚至更少有国家进行相关的研发举措。

结论

各国正在拥抱“万物互联”（IoE）的经济和社会潜力——人与事物、数据与事物之间的智能联系。国际电联和世界经济论坛正在衡量 ICT 为经济和社会带来的好处。同样重要的是，通过非法活动导致的国内生产总值（GDP）的流失正受到我们国家的关注（威胁到国家安全和经济繁荣）。采用安全框架并了解网络就绪度对于实现互联网经济和数字未来的全部潜力至关重要。

CRI 可以作为一个坚实的基础，以帮助提供这一紧迫和持续的要求。本报告适用于研究的 35 个国家和地区，也普遍适用于所有国家。它挑战了网络安全的传统思维，表明必须结束辩论。CRI 确定了可以抵御 GDP 侵蚀的更强有力的安全形势的基本要素。此外，审评委应引发国际上关于加强安全所需优先事项的讨论，鼓励政府采取行动，减少风险。

该指数将定期更新，评估各国的进展情况和不断变化的评估标准。

网络就绪指数 2.0
网络就绪度计划：基线和指数

《网络就绪指数 2.0》是对 2013 年 11 月发布的《网络就绪指数 1.0》的拓展与延伸。

引言

全球经济增长日益依赖于信息通信技术（ICT）的快速运用以及社会和网络的连通。的确，每个国家的数字议程都有望促进经济增长，提高效率，改进服务交付和性能，促进创新、提高生产力，从而推动管理的完善。然而这一核心基础建设的可用性、完整性和应变力正处于危险之中。联网系统和基础建设面对的威胁的数量、范围、速度和复杂度都在不断攀升。数据泄露、犯罪行为、服务中断和财产破坏屡见不鲜，已危及到网络经济。

目前没有一个国家做好了应对网络的准备。

全球的领导人明白，只有当网络的底层基础设施和设备安全稳妥时，日益密切的网络联系才能促进经济增长。因此，各国必须将本国的经济视野与国家安全重点相统一。

然而截至目前为止，针对数字前景与发展所依赖的网络基础设施和服务，尚没有一套可对比的全面经验之法，以评估国家在保护这些基础设施和服务方面的成熟度和投入。网络就绪指数 1.0[1] 提供了一种全新的评估方法，旨在引发国际讨论并激发全球范围内的行动，以解决网络安全问题造成的经济衰退。

在网络就绪指数 1.0 的基础上，网络就绪指数 2.0 考察了 125 个已经或即将实行的信息通信技术和网络，采用 7 个关键因素来客观评估各国的网络安全成熟度和承诺。凭借这种方法，一国可以更好地理解网络基础建设的复杂性及其导致的依赖性和安全

漏洞。[2] 具体来说，网络就绪指数 2.0 评估了各国对特定网络风险的准备情况，并且确定了各国领导人在哪些领域可以通过利用或更改法律、政策、标准、市场杠杆（例如激励机制和法规），落实其他计划以保护网络安全，维持经济价值，从而改变或完善自己国家当前的态势。

背景

大多数国家已经采取了基于信息通讯技术的经济战略，致力于向每个家庭和企业提供快速、可信、经济适用的通讯方式，从信息社会过渡到数字社会。[3] 网上政府、网上银行、远程医疗、远程教育、新一代电网以及交通基础设施自动化和其他关键服务等现代化举措，均位列大多数国家经济议程的首位。举例来说，中国的“互联网 +”行动计划，其目的在于鼓励电子商务、产业网络和网上银行的健康发展，同时促进新行业的发展以及业内企业的全球国际拓展。[4] 如同其他许多国家一样，中国将网络视为未来数字化服务发展的关键。无独有偶，印度总理莫迪表示要将印度打造成一个“数字化知识经济体”；利用印度享誉全球的信息技术（IT）实力，创造 IT、电信和电子设备市场的就业机会。此外，印度还力求成为健康、知识管理和金融市场的 ICT 解决方案的创新者。[5] 最后，欧盟委员会目前正致力于创建一套意义非凡的数字化服务统一市场，实现商品、服务、资本和业务的自由流通。数字单一市场战略成功落实后，预计每年将为全欧洲带来额外的 4150 亿欧元 GDP 增长。[6]

各国必须将本国的经济视野与安全重点相统一。

各国政府，特别是发展中国家，正在推进更为积极的 ICT 实施策略，向数以百万计的公民提供额外服务，更迅速地推进并深化经济发展。[7] 事实上，根据世界银行（World Bank）的预测，每 10% 的人口能够使用网络服务，就会带来 1% ~ 2% 的 GDP 增长。[8] 此外，最近的研究显示，政府和企业对接纳互联网和 ICT 的意识有所提高，有效提升其长期竞争力、改善其社会福利，间接带来高达 8% 的 GDP 增长。[9] 一些报告进一步显示，产业体系的现代化（例如电网、石油和天然气管道、制造业等）占全球经济的 46%，在未来十年内可能会增长至 50%。[10]

这是一个令全球各国都无法忽视的经济机遇。但是很少有人会考虑关键服务应变能力不足所导致的影响和经济成本、公民隐私暴露与侵犯、公司专有数据和国家机密遭到窃取、电子诈骗和电子犯罪的影响。所有这些都会动摇经济和国家安全。简言之，经济增长会受到网络安全问题的掣肘。[11]

经济增长会受到网络安全问题的掣肘。

举例来说，20 国集团（G20）经济体估算因假冒和盗版已经损失了 250 万份就业机会，网络犯罪给政府和消费者每年造成高达 1250 亿美元的损失（包括税收收入）。[12] 根据美国的预计，美国经济每年因知识产权盗用而遭受的损失高达 3000 亿美元，相当于美国 GDP 的 1%。[13] 荷兰、英国和德国的其他研究估计这些国家的 GDP 也会蒙受类似程度的损失。一个国家绝不可因为非法网络活动而损失哪怕是 1% 的 GDP。

应变能力强的网络化社会必须以安全为核心来促进现代化。

随着各国继续推进 ICT 和网络联系，如果安全和应变能力问题不能成为现代化战略的核心，信息披露、相关风险和经济损失将会呈井喷式增长。

衡量这些经济损失迫使各国领导人将国家安全议题与经济议题更好地统一起来，并且积极投资两大议题的衍生性价值。[14] 揭露网络安全问题造成的经济损失，可能会触发国内和国际关注，共同解决这一经济漏洞。CRI 2.0 建立了一个框架，指导各国以安全的方式推动经济增长，实现以 ICT 为基础，灵活应变、相互连通的社会。

1. 网络就绪指数 2.0——方法论

CRI 2.0 主要由两个部分组成：其一，CRI 2.0 通过客观评估各国对网络安全和应变能力的成熟度和投入，指导各国领导人要采取哪些步骤来保护联系日益紧密的国家和潜在的 GDP 增长；其二，CRI 确立了一国做好网络准备的意义，将网络就绪的核心部分转换为各国应遵循的可行蓝图。作为一套实用、独特和操作简便的工具，CRI2.0 方法论能有效评估一国当前网络安全状态和实现经济远景所需的网络安全性能之间的差距。该分析所制定和采用的蓝图涵盖了 70 多个独特的数据指标，包含以下七大因素：

（1）国家战略；

（2）事件响应；

（3）电子犯罪与执法；

（4）信息共享；

（5）研发投资；

（6）外交与贸易；

（7）防御与危机应对。

每个国家的事实评估都依赖于第一手资料，每个独特信息点都是以实证研究和文件为基础。根据对各国各个指标的评估，可以将网络就绪水平分为三个等级：信息不足、信息部分透明或信息充分。

CRI 2.0 方法论目前应用于评估 125 个国家和地区的网络安全就绪水平；评估各国在网络安全和应变能力基础设施及服务上的成熟度和投入（图 1 和表 1）。

信息不足：缺乏或尚未发现支持性信息或数据。然而，有可能存在相关数据，但目前尚未公开或属于机密。

信息部分透明: 有政策、活动和/或资金方面的支持性信息或数据，但是活动可能不成熟、不完善或处于早期阶段。虽然可以观察到该类举措，但可能较难评估其功能性。

信息充分：有充足的支持性信息或数据，通过该类信息和数据，可观察、评估活动的成熟度和功能性。[15]

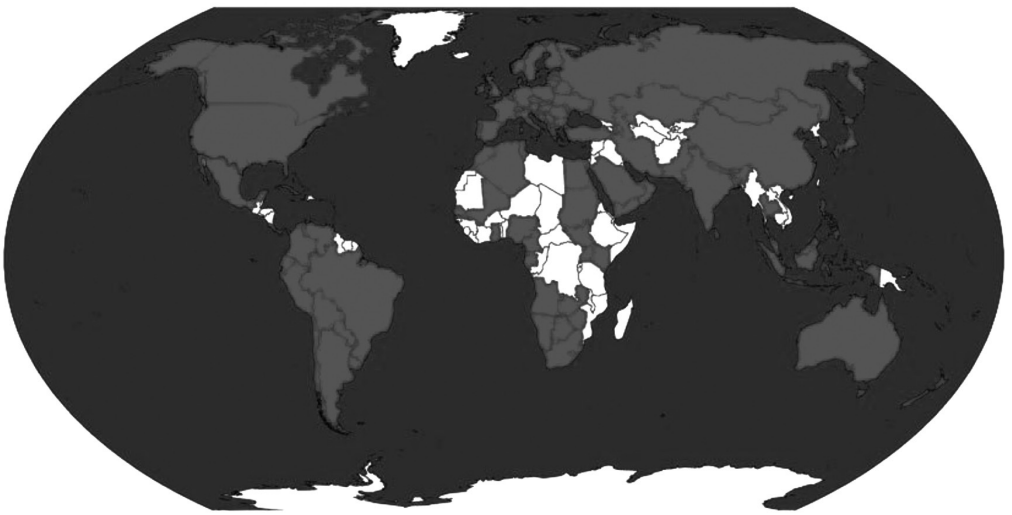


图 1　CRI 2.0 选择的国家和地区

表 1　CRI 2.0 选择的国家和地区

阿尔及利亚	哥伦比亚	以色列	荷兰	斯里兰卡
安道尔共和国	哥斯达黎加	意大利	新西兰	圣基茨和尼维斯
安哥拉	克罗地亚	日本	尼日利亚	圣文森特和格林纳丁斯
安提瓜和巴布达	古巴	哈萨克斯坦	挪威	苏丹
亚美尼亚	塞浦路斯	肯尼亚	阿曼	斯威士兰
阿根廷	捷克共和国	吉尔吉斯斯坦	巴基斯坦	瑞典
澳大利亚	丹麦	拉脱维亚	巴拉圭	瑞士
奥地利	吉布提	黎巴嫩	巴拿马	中国台湾地区
阿塞拜疆	厄瓜多尔	莱索托	秘鲁	马其顿共和国
巴林	埃及	立陶宛	菲律宾	泰国
孟加拉国	爱沙尼亚	卢森堡	波兰	特立尼达和多巴哥
巴巴多斯	芬兰	澳门	葡萄牙	突尼斯
白俄罗斯	法国	马来西亚	卡塔尔	土耳其
比利时	加蓬	马尔代夫	罗马尼亚	乌干达
不丹	冈比亚	马里	俄罗斯	乌克兰
玻利维亚	德国	马耳他	沙特阿拉伯	阿联酋
波黑	加纳	毛里求斯	塞内加尔	英国
博茨瓦纳	希腊	墨西哥	塞尔维亚	美利坚合众国
巴西	中国香港地区	摩尔多瓦	塞舌尔	乌拉圭
文莱	匈牙利	蒙古	新加坡	乌兹别克斯坦
保加利亚	冰岛	摩纳哥	斯洛伐克	委内瑞拉
喀麦隆	印度	黑山共和国	斯洛文尼亚	越南
加拿大	印度尼西亚	摩洛哥	南非	也门
智利	伊朗	纳米比亚	韩国	赞比亚
中国	爱尔兰	尼泊尔	西班牙	津巴布韦

选择的国家包括国际电信联盟（ITU）通信技术发展指数排名前 75 的国家和地区，用以强调连通性的重要性；还囊括了 G20 国家，因为它们代表了全球九成的 GDP、

八成的国际贸易、64% 的世界人口和 84% 的化石燃料排放。

为了具备区域代表性和全球包容性，其他国家是从以下组织中选取的：经济合作与发展组织（OECD）、非洲经济共同体（AEC）、拉丁美洲一体化协会（LAIA）、亚太经济合作组织（APEC）、中亚区域经济合作（CAREC）、海湾合作委员会（GCC）、南亚协会为地区合作运营联盟（SAARC）以及北美贸易联合会。这些区域经济组织的成员国不仅能体现通信技术发展指数，而且常常还能体现世界经济论坛（WEF）的网络就绪指数。这确保了每个选中的国家都采用信息通讯技术，并投资有一定普及度的、经济适用的网络服务，以促进经济增长。

鉴于海合会并不能代表整个中东地区，因此还选择了三个不属于海合会，但 GDP 排名最高的国家：伊朗、也门、黎巴嫩。[16]

这 125 个国家和地区代表了全球的大部分国家，体现出 CRI 2.0 在国家选择标准上的多样性和代表性。

CRI 2.0 注重经济和安全的相互联系，为各国评估网络安全的成熟度奠定了坚实的基础，并且可作为一个框架，为政策战略、运营和机构计划、资源要求、法规和制定立法，以及运用多样市场杠杆提供信息。鉴于一国的 GDP 很有可能以不断发展的科技为主导，并与网络挂钩，所以 CRI 2.0 能够提升对一国可持续网络和 GDP 增长之间联系的认识。此外，CRI 2.0 还有助于人们理解网络问题引发的经济损失，掌握国家安全问题在一国数字和经济议程中的比例。通过这一方法，可实现基于分析的决议，判断如何应对问题并事先做好防范措施。

最后，CRI 2.0 向国际电信联盟（ITU）、世界经济论坛（WEF）、美洲国家组织（OAS）、美洲开发银行（IDB）、世界银行等国际实体提供了各自计划和国际讨论的框架与辅助手段。

以下是对 CRI 2.0 方法论中七大关键因素的详细描述。每个部分包含一个关键因素，采用至少 10 个支持指标进行评估。结合这些因素和指标，就构成了一国网络就绪水平的蓝图。此外，本文提供了国家实例，说明了网络就绪方面的创新性和多文化解决方案。虽然这些实例并不全面，但是侧重于独特的国家方案。

2. 国家战略

要说明一国的网络就绪水平情况，第一个也是最重要的因素，在于阐述和发布将国家经济远景与国家安全要务相统一的国家安全政策。互联网、宽带网络、手机应用、IT 服务、软件和硬件构成了数字经济和一国数字未来的基础。[17] 网络和信息通

讯技术已然成为家庭平台（如 FacebookTM、TwitterTM、InstagramTM、VKontakteTM 等）、商业引擎、关键服务和基础设施乃至全球经济的支柱。[18] 各个行业互相依赖又高度连通。举例而言，高级制造业采用工业控制系统和机器人，提高了生产力并降低了对人力干预的需要。现代农业将互联网协议设备（IP 设备）植入玉米内，以测定肥料要求并调整水供应。IP 设备还被安装在家畜身上，用于确定牲畜进食进草的地点，而且可以几乎不间断地评估牲畜的健康水平。电子商务——实现商品和服务的跨境自由流通，正在替代传统店面的角色。顾客在网上下单之后，不久品类繁多的商品就被直接送到家门口。如今，交通系统采用传感器、移动设备和自动服务亭来管理交通运营和交付票据。城市之间采用定位设备，追踪汽车的速度和位置，查证司机是否违反交通规则。医疗行业的现代化举措将公民的健康记录数字化，通过云计算在全球各地都能迅速查阅医疗记录。远程医学使用高速网络向医疗条件落后的区域提供医疗指导和服务。最后，财务系统每天交易数万亿美元的金额，商品市场贸易采用电子货币，网上银行正在代替对当地实体银行的需求。

网络基础设施面临的威胁日益增长。各国开始了解这些威胁，并罗列了基础设施保护、数据保护、国土安全保护等需求。全面的国家网络安全战略需描述国家经济领域的威胁，简要列出必要的步骤、计划和举措，以解决这些威胁，保护网络连接以及公民和公共组织及私人组织使用的信息通讯技术。[19] 应该借助网络和采用信息通讯技术所带来的经济潜力加固战略基础，其中包含有助于削减网络威胁造成的 GDP 损失的举措，以及提升全国整体安全和应变能力的举措。

健全的全国网络安全战略不仅仅是纸上谈兵，还必须能够付诸行动。如今，大多数战略反映的主要课题包括：罗列政府内部的组织权力和职权；树立公民的意识和教育；建立突发事件和危机管理的反应能力；拓展执法能力，应对网络犯罪率；促进公私合作关系，发展可信的信息交换和分享；以及引导资源用于研发和创新。许多战略首先从统计学开始，量化事件数量和基础设施感染率、命名威胁种类。这些数据为组织责任以及对各类任务和组织的资金投入的增加提供了充分的理由。然而，该类战略很少优先考虑最具风险的服务和基础设施，亦未将降低信息泄露和经济损失所必要的安全措施和资源要求统一起来。健全的全国网络安全战略必须说明经济领域的战略问题；确定并授权主管机关[20]执行策略；在开展计划中囊括具体的、可评估的、可实现的、基于结果和时间的目标；并且意识到必须在竞争激烈的环境中投入有限资源（例如政治意志、金钱、时间和人力），以取得必要的安全和经济成果。

至少 67 个国家和地区（其他国家尚在发展中）已经公布了网络安全战略，简要列出了旨在提升国家安全和应变能力的关键步骤。[21] 许多其他国家则具备国家战略（并非特定于网络安全），以指导并协调国家提升网络安全态势。但是，很少有国家将经济和国家安全议题明确联系起来并且特别强调网络安全的经济重要性。制定可执行战略的国家更是少之又少。因而，所有国家都有机会修改或制定其现有战略来反映网络安全的经济重要性。

完整的国家网络安全战略应包含以下因素：

声明：

● 公布国家网络安全战略，涵盖与信息通讯技术应用相关的经济机遇和风险。

组织：

● 指定主管机关并明确职权；

● 确定受国家网络安全战略实施影响和 / 或对国家网络安全战略实施负责的关键政府实体；

● 确定受国家网络安全战略实施影响和 / 或对国家网络安全战略实施负责的商业实体（确认商业领域的依赖关系）。

资源：

● 确定实施该战略所要求和分配的财政和人力资源；

● 确定实施该战略有望获得或损失（粗略估计）的 GDP 百分比。

落实：

● 确定保证关键网络基础设施和信息通讯技术实施所需要的机制；

● 确定通过实施战略、安全性和应变能力提高关键服务（并非关键的基础设施）水平；

● 确定服务协议连续性的国家标准（一周 7 天，一天 24 小时）以及每个关键服务、行业和基础设施的故障报告要求。

正如其他六个因素一样，这一关键因素的调查结果是对于瞬息万变的环境的简要概述。随着各国继续发展各自的网络安全战略，这一关键因素的更新将会反映这些变化，同时监控、追踪并评估值得注意的实质性发展。因此，CRI 2.0 将会继续提供附带全新实例的蓝图，为那些正在制定或修改其战略的国家提供信息。

3. 事件响应

第二个说明一国网络就绪水平的关键因素涉及确立并维护有效的全国事件响应能力。该项能力常常表现为一个或多个国家计算机安全事件响应小组（国家 CSIRT）

或计算机紧急响应小组（CERT），下文统称为计算机安全事件响应小组（CSIRT）。当发生与网络相关的自然或人为灾难、且影响到关键服务和信息基础设施时，该小组会负责管理事件响应。[22] 目前，全球已建立了 102 个国家计算机安全事件响应小组，还有四个小组尚在建立之中。[23] 计算机安全事件响应小组一般包含 IT 安全专家和来自学术界、私营企业和政府机关的从业者。这些事件响应小组不仅向涉及国家利益的网络事件提供具体技术能力，还加强了一国政府了解并打击网络威胁的能力。因此，一国要保护并维持对国家安全和经济发展至关重要的网络服务和基础设施，其整体战略中关键的一环就在于国家计算机安全事件响应小组的运作。[24]

关键信息的应变能力对于国家安全和经济增长而言至关重要。

不同于政府机构，国家计算机安全事件响应小组服务于诸多对象，从政府部门到公私实体，再到公民。成熟的国家计算机安全事件响应小组能够提供专门的响应服务，换句话说，它具备在事件发生时控制并缓解事件的应对能力。[25] 虽然国家计算机安全事件响应小组的具体组织形式可能有所不同，且并非每个国家都具有相同的需求和资源，但是这些专门的专业团队应该提供一系列积极应对、快速反应的功能，同时提供保护性、教育性和安全质量管理服务。这些服务包括但不限于：达成对国家面临的威胁的共识；发布网络漏洞和威胁的警报和通知；提升网络安全意识和最佳实践；确定、发现、控制、管理安全威胁，并为潜在事件做好准备；协调事件响应活动；分析计算机安全事件并提供反馈和吸取的教训（用于共享学习）；推进能够提高应变能力的活动；以及支持国家网络安全战略。

例如，新加坡的国家计算机安全事件响应小组（SingCERT）是由新加坡资讯通信发展管理局（IDA）与新加坡国立大学于 1997 年合作建立的。自创立之初，该小组就成为了新加坡网络安全局（CSA）的成员。SingCERT 被设计成事件响应的一站式中心，促进网络上安全相关事件的发现、解决和预防。SingCERT 提供技术协助并协调网络安全事件的响应，确认并追踪网络入侵趋势，及时发布威胁警告，并与其他安全机构进行协调，以解决计算机安全事件。[26]SingCERT 还积极组织和主持东南亚国家联盟（ASEAN）与亚太计算机紧急响应小组（APCERT）的演习活动。此外，新加坡主办过 7 次事件响应与安全小组论坛（FIRST）。

巴西的事件响应能力体现在设立了一个国家计算机安全事件响应小组 CERT.BR 和分布在四个州的 30 个区域计算机安全事件响应小组，全部隶属于巴西网络指导委员会。作为一个多方参与的无政府组织，该委员会是负责巴西网络防御和事件响应的

主要实体。[27] 巴西的 CERT.BR 负责事件响应、提高意识、网络威胁和入侵的数据收集以及协调各利益相关方，包括计算机安全事件响应小组、学术界以及私营企业。此外，巴西的计算机安全事件响应小组还包括了来自金融界、军方、政府和大学院校的团队。[28]

除国家计算机安全事件响应小组外，还建立了类似的区域实体，在具体地理区域推动并协调事件响应活动。比如 AfricaCERT，该非盈利组织涵盖了 11 个非洲国家，为非洲互联网的运营者进行合作和技术信息交流提供了论坛。

AfricaCERT 的主要目标包括但不限于：协调非洲各计算机安全事件响应小组的合作，处理计算机安全事件；协助在目前缺乏事件响应能力的国家建立计算机安全事件响应小组；开展并支持 ICT 安全领域的事件预防和教育推广项目；鼓励信息共享；以及推广网络安全的最佳实践。同样，亚太计算机紧急响应小组（APCERT）由区域内 28 个计算机紧急响应小组和其他可信赖的安全专家组成，旨在提高计算机安全事件相关的意识和能力，促进亚太地区的事件反应能力。[29]APCERT 的使命在于通过全球协作，追求一个“干净、安全和可信”的网络环境。为了有效交流网络威胁信息，APCERT 的组织框架依赖于联系人系统（POC）：在紧急情况发生时，每个国家选出一位 APCERT 成员作为联系人，以促进及时响应。[30] 同样地，伊斯兰合作组织——计算机紧急响应小组（OIC–CERT），包含了东南亚、南亚、中东、非洲、中亚的成员国，致力于推进成员国的计算机紧急响应小组和 OIC–CERT 之间的合作。

除了增强事件响应能力外，各国还参加了网络事件响应演习。这些演习帮助各国练习和培养有效危机管理技能以及验证一个 CSIRT 在压力下快速作出响应的能力。例如，2011 年 11 月，德国国会（执行部门）进行了为期一天的危机规划 / 准备演习。演习的目的是制定应对多方面袭击的政府响应程序，包括针对关键基础设施的“洪水攻击”（DDoS）；向银行系统植入恶意软件，危害 ATM 机和信用卡；以及向航空交通管制系统插入虚假交通信息。[31] 瑞典急难救助署（MSB）、邮政及电信总局（PTS）和国防电波局（FRA）还定期为相关高级管理人员提供合作性的首席信息安全官（CIAO）课程。课程的高潮在于顶层演习（Capstone Exercise），这种网络危机管理模拟涉及了决策流程中的政府和私营利益相关方，包括议会和负责瑞典关键服务的企业的首席执行官（CEO）。演习强调了关键政策和法律缺陷，同时对所有的参与方进行了网络安全教育。[32] 此外，2015 年 10 月，捷克共和国举行了一场事件响应演习，重头戏放在了对关键基础设施的威胁上，并且特别强调了核电厂的安全防护工作。[33] 一些国家还进行了针对已发生的网络事件的响应演习。举例来说，韩国总统朴槿惠下令韩国水力核

电公司（KHNP）的全体员工进行网络战争演习和培训，之前该公司多个站点发现了恶意软件。[34]

此外，国际演习不仅测试了事件响应操作能力，还模拟了各国间的合作。比如，美国每两年举行一次的“网络风暴”（Cyber Storm）演习，试图加强政府和私营企业的网络就绪水平。每次网络风暴演习都是基于之前真实事件所得到的教训，确保参与者有机会真实演练针对更复杂网络事件的响应。2016 年的网络风暴演习将涉及 16 个州、7 个国家和 14 个联邦机构。[35] 欧盟也在成员国和私营领域内举办两年一次的网络事件响应演习，取名为“网络欧洲”（Cyber Europe）。[36] 2014 年，几乎全部的欧盟成员国在持续 24 小时的网络欧洲演习中接受了将近 200 次真实的网络袭击，测试了自身的响应能力。各种袭击包括 DDoS、网站篡改、数据渗漏和针对关键基础设施的网络袭击。[37] 此外，欧洲防务局（EDA）和北大西洋公约组织（NATO）还联合举办了区域内广泛复杂的网络危机管理演习，目的在于加强成员国的网络事件响应能力，了解跨境依赖关系。[38] 美国和英国最近公布将测试大西洋两岸金融中心如何应对大规模网络袭击。演习于 2015 年 11 月举行，测试了国家的响应和跨大西洋的协作与交流。[39]

国家 CSIRT 也可发挥机制作用，建立国家的自信并培养协作。举例来说，中国、日本和韩国虽然历史上曾关系紧张，但是如今每年举办一次三边 CSIRT 会议，商讨网络事件响应机制。会议有助于树立信心，培养相互信任，促进了网络“热线”的形成，以针对重大网络事件进行沟通交流。[40]

网络事件响应能力、联合会议以及演习，这些都还只是能帮助国家积极准备重大网络事件以及减轻重大网络事件连锁反应的基本机制的一部分。CSIRT 能有效加强一国应对网络威胁的速度、恢复程度和应变能力，减少全国性大规模袭击和运动可能造成的整体经济和运营影响。要成功部署这些事件响应小组，关键前提之一就是要具备训练有素的工作人员以及可快速部署的高效工具。此举能有效促进事件响应小组在事件预防方面培养协作和协调的能力，实现快速应对事件，并促进国际和国内利益相关者之间的信息共享。

健全的国家事件响应能力应包括以下因素：

声明：

- 公布针对紧急事件和危机的事件响应计划；
- 确认并对应跨领域的依赖关系，以解决运营的连续性和灾难恢复机制；
- 有证据显示该计划定期实施并更新；

● 公布并宣传针对政府、关键基础设施和重要服务网络的全国网络威胁评估。

组织：

● 建立国家 CSIRT，管理事件响应并服务广大的全国选区（除政府和关键基础设施提供商以外，还需建立其他机构）；

● 确认与政府和监管机构接头的全国授权联络人网络；

● 确认与关键行业接头的全国授权联络人网络，所谓关键行业，是指对于关键服务和基础设施的运营和恢复都至关重要的行业；

● 建立信息警告和预警系统，全国危机或响应中心可使用该系统来及时有效地接收、解决和传播紧急信息。

资源：

● 确定国家 CSIRT 执行命令所需要和分配的财政和人力资源；

● 确定额外的资金以支持并定期检测信息警告和预警系统，以及通过全国网络安全演习评估该国应对网络事件和危机的应变能力。

落实：

● 具备在关键服务和基础设施的事件控制、管理、应变能力和恢复流程上的能力；

● 全国危机或响应中心具备及时解决和发布预警的能力；

● 有证据证明具备用于分析全国关注的趋势或计算机安全事件的持续研究方法，分享类似的行动方案和战略、技术和程序，以确定模式；

● 制定并落实系统和项目，通过全国网络安全演习定期测试并测量该国对网络事件和危机的应变能力。

这一关键因素的初步发现基于国家 CSIRT 资料，由卡耐基·梅隆大学[41]、欧洲网络与信息安全局（ENISA）[42]、FIRST[43] 和国际电信联盟提供。此外，还查阅了其他主要和次要资源，比如国家 CSIRT 的网站和相关新闻稿，以确定是否具备该类能力以及该类能力是否得到资金支持。由于各国开始意识到建立国家 CSIRT 的重要性，这一关键因素的更新将会监督、追踪和评估这些发展。

4. 电子犯罪与执法

一个国家安全防护能力的第三个关键因素体现在其对保护社会免受网络犯罪的投入。网络犯罪不仅仅是一个国内问题，也是一个国际问题，因此需要跨国的解决方案。各国必须做出保护社会免受电子犯罪的国际努力。这种能力最常见的形式是参与打击国际网络犯罪的国际论坛，以及建立国内法律和监管机制，应对网络犯罪。被指

定开展这些活动的相关法律和监管机构必须确定网络犯罪的定义，并赋予政府实体调查并有效制裁网络犯罪活动的机制、专业技术和资源。

欧洲委员会的《网络犯罪公约》和上海合作组织的《保障国际信息安全政府间合作协定》这两大国际协定展示了一国在保护社会免受网络犯罪方面的投入。欧洲委员会的《网络犯罪公约》自 2004 年 7 月 1 日起生效，一般被称为《布达佩斯公约》，其提供了一套可以协调多样的国家网络安全法律并且鼓励执法协作的机制。[44]《布达佩斯公约》具有一定的局限性，因为它允许签约国有选择性地执行公约中的条款，避免“影响其主权、安全、公共秩序或其他重要利益”。[45] 上海合作组织的《保障国际信息安全政府间合作协定》于 2009 年签署，有时被称为《叶卡捷琳堡协定》，拥有与《布达佩斯公约》执法方法相一致的准则。此外，该协定还寻求提升信息法律基础并建立各方在确保国际信息安全方面通力合作的实际机制。[46] 根据这些协定，各国同意适当立法，增进国际合作，通过促进国内和国际的监督、调查和检控，打击犯罪行为。CRI 2.0 相信已经批准或同意上述任何一个参与协定的国家会在打击网络犯罪方面取得不错的成绩，因为通过批准或同意该类协定，这些国家在国内法律下即具备具体责任和义务，以维持国际背景下应尽的努力。

除了上述国际机制之外，还有其他的国际性、多国性和区域方法来打击国际网络犯罪。举例来说，联合国大会通过了多个与网络犯罪相关的决议，比如 2001 年的《打击非法滥用信息技术》和 2003 年的《创建全球网络安全文化以及保护重要信息基础设施》。[47]

减少受感染网络设备的数量，是打击网络犯罪的一项重要投资。

值得注意的是，由 20 个国家组成的联合国政府专家工作组（GGE）同意就制裁 ICT 恐怖主义和犯罪行径进行合作，这可谓一个突破性时刻。这些国家的投入被编入 2015 年 6 月政府专家工作组报告《关于从国际安全的角度看信息与电信领域的发展》。[48] 亚太经合组织（APEC）还为成员国开展了关于网络犯罪的能力建设项目，以建立法律架构并培养调查网络犯罪的能力。在该项目中，APEC 成员国中的发达国家通过培训立法机关和调查人员来支持其他的成员国。[49]

CRI 2.0 利用这些国际性、跨国和区域方法来评估一国的网络就绪水平。此外，CRI 2.0 还包含了东南亚国家联盟（ASEAN）和国际电信联盟（ITU）等组织有关网络犯罪的国家信息。

虽然各国有意向在打击网路犯罪方面携手合作，并且网络安全协议的批准非常关键，但并不一定能够展示出打击网络犯罪的就绪水平。各国还必须积极建立国内网络

法律执法能力。例如，位于印度班加罗尔的印度国家法律大学的网络法律和取证研究、发展和培训高级中心通过向司法人员、检察官、调查机构、网络安全人员、技术人员和其他人员提供培训和教育，将法律转变为技术，同时将技术转变为法律。该中心由印度通信和信息技术部的电子和信息技术司资助，通过网络取证实验室提供了独特的实践培训要素，有助于促进复杂问题的快速理解。[50]

此外还有一个例子，国际刑警组织（INTERPOL）最近在新加坡创建了国际刑警组织全球创新中心（INTERPOL Global Complex for Innovation）。该机构使执法官员能够与行业开展合作，发展新的培训技巧并使用高级工具来解决网络犯罪，促进网络安全。[51] 举例来说，国际刑警组织创建了一套模拟游戏，教授执法官员黑暗网络和密码电子货币的交集和风险。黑暗网络催生了地下（非法）经济，出售个人身份信息（PII）、军事机密、武器设计、模块化恶意软件、“零日漏洞”、私人密钥和加密证书，以及许多其他类别非法获取的数据。国际刑警组织的第一次模拟与培训演习于 2015 年 7 月举行。[52]

经济增长会受到网络犯罪和诈骗的掣肘。

除了加强应对电子犯罪的能力和执法能力外，各国还必须清除网络基础设施中受到感染的部分，即僵尸网络。[53] 目前，全世界估计有十二分之五的电脑属于僵尸网络的一部分。美国联邦调查局（FBI）估计僵尸网络每一秒钟就会感染 18 个系统，造成全球预计 1100 亿美元的损失。[54] 一些国家已经采取行动来解决这一威胁并且取得了一定的成功。

比如加拿大政府的黑暗网络项目“网络活动预测性指标的高级分析学和暗区分析”，该项目由加拿大贝尔（Bell Canada）主导，集结了来自加拿大政府机关、学术机构和各行各业的专家，为网络威胁的“Clean Pipe”解决方案生成了一个商业案例。通过提供令人信服的证据，积极支持控制加拿大面临的来自网络的危险。该项目的发现结果为全国 Clean Pipes 战略制定了商业案例，影响了电信服务提供商的网络安全标准。[55] 再比如日本历时 5 年打造的网络清洁中心，2006 年至 2011 年间由日本 CERT 运营。[56] 该中心是 JP-CERT、各种安全提供商和网络服务提供商（ISP）跨学科合作的成果。它创造出针对僵尸网络恶意软件感染和利用的自动“防护网络”，提供了定制化的解决方案，解决具体计算机上的具体恶意软件。[57] 日本 Telecom-ISAC 继续努力，维持着网络清洁中心运作。[58] 最后还有澳大利亚的 iCode，该机构通过澳大利亚网络安全举措开展公私合作，旨在通过减少澳大利亚容易受到攻击

的计算机设备的数量，推进 ISP 的安全文化。iCode 鼓励所有的澳大利亚 ISP 加入 AISI，并向 AISI ISP 成员提供每日恶意软件感染和服务遭受攻击的数据。[59]

经济增长会受到网络犯罪和诈骗的掣肘。全球的网络犯罪规模已达约 4450 亿美元，对国民经济造成负面影响，损耗至少 1% 的 GDP，造成 200,000 人失业。[60] 打击网络犯罪并提高执法能力，是经济体做出的必要投资。各国通过批准各项协定、国际合作、能力培养、实施防僵尸网络项目以及其他各类举措以提升打击网络犯罪的执法能力，可缓解网络风险并促进未来经济发展。

保护社会免受网络犯罪的健全的国内和国际投入，需要做到以下关键几点：

声明：

● 通过批准国际网络犯罪协议或其他同等协议来打击网络犯罪，展现出国内和国际对保护社会免受网络犯罪的承诺；

● 展现出建立国内法律和政策机制的努力，以明确减少国内犯罪活动，推动协调各机制来解决国际和国内网络犯罪。

组织：

● 建立成熟的机构能力来打击网络犯罪，包括法官、检察官、律师、执法官员和其他调查人员的培训；

● 建立一个协调机构，主要任务和职权就是确保国内和国际上（即跨国合作）满足应对国际网络犯罪的全部要求。

资源：

● 确认打击网络犯罪所需要和分配的财政和人力资源；

● 建立会计机制，确定每年 GDP 受网络犯罪影响的比例（采用真实货币的实际损失），以评估国内系统性成本、收益的权衡，并据此分配资源。

落实：

● 有证据表明一国在审核并更新现行法律和监管治理机制方面做出努力，辨别哪里可能存在差距和部门重叠，阐明并优先考虑需要现代化的领域（诸如旧版电信法律等现行法律）；

● 针对损害电脑系统、网络和计算机数据的保密性、完整性和可用性的行为，以及滥用该系统、网络和数据的行为，包括国际版权侵权行为在内，国内法律要予以刑事制裁；

● 有证据证明一国能有效减少自身基础设施和网络中的感染情况（例如设立防僵尸网络和恶意软件修复举措）。

信息共享必须依托于所有利益相关者的信任和认可。

这一关键因素的初步发现是基于审查一国是否批准或同意加入《布达佩斯公约》或上海合作组织的《叶卡捷琳堡协定》，以及一国是否积极参与区域、多国或国际活动来打击网络犯罪。此外，目前来自该国的僵尸网络活动（指控节点和整体感染情况）被用于评估防僵尸网络举措的有效性。确定、评估和应对目标袭击等关键活动可能会对全球电信、贸易和商业造成巨大影响，要求不仅仅是传统的监督和保护机制。从全球范围来说，大多数政府和组织都建立了信息共享项目，以更好地了解国家行为体和非国家行为体造成的风险，并针对暴露于漏洞、后续感染和破坏行动的风险进行了管理。与国家 CSIRT 和 CERT 提供的部分服务相类似，正式的信息共享机制有助于促进事件响应的协作，促进实时分享威胁和情报信息，帮助提高了解为何行业会被设为目标，丢失了哪些信息以及采用了何种方法来保护信息资产。CRI 2.0 利用直接和间接资料来确定一国是否已经建立了法律和监管机制或其他降低风险的活动以及是否已经划拨资金来确保成功落实。这一关键因素的更新情况将监督、追踪并评估值得注意的实质性发展。

5. 信息共享

说明一国网络就绪水平的第四个因素是能否建立并维护信息共享机制，该机制能够交换具体可行的信息和 / 或政府和工业部门之间的信息。确定、评估和应对目标袭击等关键活动可能会对全球电信、贸易和商业造成巨大影响，要求不仅仅是传统的监督和保护机制。从全球范围来说，大多数政府和组织都建立了信息共享项目，以更好地了解国家行为体和非国家行为体造成的风险、管理与漏洞、后续感染和破坏行动的接触。

与国家 CSIRT 和 CERT 提供的部分服务相类似，正式的信息共享机制可以帮助促进事件响应的协作，促进实时分享威胁和情报信息，帮助提高了解为何行业会被设为目标，丢失了什么信息以及采用了什么方法来保护信息资产。针对解决网络威胁和帮助实体保护信息资产，出现了至少四类不同的信息共享模式：①政府驱动模式；②行业驱动模式；③非盈利合作驱动模式；④集合学术、政府和行业合作的混合驱动模式。每一个模式都面临着独特的挑战，比如平衡交换及时的、具体可行的网络安全信息的需求，同时保护数据的保密性，捍卫公民自由，管理互相竞争的财务和人力资源与利益。然而任何一个模式要想成功，都离不开两大因素：认可和信任，这就要求必须明确目标、角色、责任和结果。简而言之，当一方不情愿参加或采取守势时，模式就很

难取得成功。[61]

而且，利益相关方必须能够分享严重事件的宝贵信息，这就要求明确应该分享哪类信息、谁将获得这些信息以及自信息原持有者披露后，应采取哪些安全措施来保护这些信息。敏感信息交换的复杂度随着组织规模的壮大而相应增大，如果组织成员国是存在不同国家安全问题的主权国家，复杂度可能会大幅度增加。

许多国家已经制定了强大的国家信息共享项目，值得其他国家作为良好实践进行效仿。这些项目着重将类似的利益相关者集合成组，然后将这些组集合成一个国家性项目。比如荷兰就建立了一个政府发起的国家网络安全中心（NCSC），其前身是荷兰信息和通信技术安全小组（GOVCERT）。现在该中心已转变为成功的公私合作组织，负责荷兰国内的数字安全和信息共享。[62]其主要任务之一就是不断监测互联网上所有（潜在的）可疑信息，一旦发现任何确认的网络威胁，就通知政府机关和组织。NCSC 还直接连通荷兰的所有信息共享和分析中心，通过交通信号灯协议（TLP）实现信息共享，将信息分为四个等级：红、黄、绿和白。荷兰的信息共享项目是参照英国的国家基础设施协同中心（NISCC），向重要的国家基础设施业务交付信息安全设备。[63] 类似的还有日本的信息技术促进会（IPA），该机构作为制度权威，负责政府和关键行业间的信息共享，在与国内各大企业建立可靠关系并提供及时有效的情报方面，已经取得了可喜的成绩。此外，IPA 还与日本经济产业省、国家信息安全中心和日本网络救援建议团队（J-CART）密切合作，应对所有影响关键基础设施的重大网络事件。[64]

此外，美国的金融服务信息共享和分析中心（FS-ISAC）也是值得效仿的案例。该中心是一家由金融服务业开发的行业驱动机构，旨在促进发现、预防和应对网络事件和诈骗活动。该中心还与金融服务提供商、商业安全公司、联邦或全国性政府机构、州政府机构和当地政府机构、执法机关以及其他可信赖的实体建立了良好关系，向全球的成员企业提供可靠的、及时的网络威胁警报和其他关键信息。FS-ISAC 还采用了一种不同的交通信号灯协议（TLP）来确定哪些受众可以并应该接收具体信息。[65]FS-ISAC 在国际上不断推广威胁信息共享，拓展至英国和欧洲。跨行业间也存在其他 ISAC，但效果并不显著。

美国的国家网络执法师培训联盟（NCFTA）是一个非营利组织，其任务是促进私营行业、学术界和执法机关的协作，以确认、缓解和中和复杂的网络相关威胁。除了州执法机关、当地执法机关和行业代表以外，该非营利合作驱动的机构聚集了来自加拿大、澳大利亚、英国、印度、德国、荷兰、乌克兰和立陶宛的国际代表。NCFTA 与企业及时、顺畅地交换网络威胁情报，同时还与公共领域、私营领域、执法机关和学术界的主题专

家通力合作，缓解风险和诈骗行动造成的影响，收集起诉犯罪的必要证据。[66]

实时的、具体可行的信息是缓解网络威胁的关键。

最后，位于挪威约维克大学学院的网络和信息安全中心（CCIS）作为一个合作机构（学术界、政府和行业），代表了信息共享和网络安全协作的另一种声音。CCIS 推进网络和信息安全的全国性系统方法，提供信息共享计划来捍卫社会发现、预警和处理严重网络事件的能力。此外，它支持全国在网络和信息安全领域进行高质量研究，制定解决法案。

除了各国正在制定的各种信息共享项目以外，大多数政府的国防情报机构会收集宝贵的网络相关信息，一些国家已经开始撤销对该类情报的保密，将其分享给其他政府机构和关键行业。实际上，实时的态势感知常常是预防或缓解具体网络威胁的关键。作为信息共享举措的一部分，巴西等一些国家已经设计了机制，公开（取消保密）具体可行的信息，向其他实体（公共和私营）发出预警，提醒其可能遭受的攻击、具体威胁和策略以及潜在的防御解决方案。[67] 提升国家的防御姿态至关重要，一些国家乐意取消对部分情报的保密，以更好地确保安全。

一国的公私行业实体内部和之间能够交换及时、准确和具体可行的信息，这有助于降低遭受攻击和暴露于攻击的几率，也就降低了伴随性风险。随着信息共享的频率增加和质量提升，各实体应能够更快、更积极地解决网络基础设施面临的网络威胁。建立并维护具体可行的信息共享项目，可谓经济增长的基础投资。

一个有效的全国性、跨行业、具体可行的信息共享项目应当包括：

声明：

● 阐述并传播跨行业信息共享政策，实现政府和各行业间具体可行的情报或信息的交换交流。

组织：

● 确认机构结构，能将权威信息从政府来源处传送至政府机构和关键行业（政府到政府）；

● 确认机构结构，能确保存在用于运营性（接近实时）和取证用（事后）跨行业事件信息交换（双向）的机制（报告计划、技术等）；

● 建立学术驱动或非营利驱动的机制，用于漏洞、事件或解决方案的信息交换（替代模式，例如 NCFTA 或国家漏洞数据库）。[68]

资源：

● 确认政府驱动的权威信息交换或用于信息共享机制的其他机构结构所要求和

分配的财政和人力资源。

落实：

● 有证据证明，充分维护用于解决关键相互依赖关系的跨行业协作机制和跨利益相关者协作机制（包括事件态势感知以及跨行业事件管理和跨利益相关者事件管理）并测试其有效履行；

● 有证据证明，政府具备能力和流程以公开（取消保密）可用的网络情报信息并与其他政府和关键行业分享。[69]

该关键因素的初步调查结果基于对一国是否已建立信息共享和其他合作机制的审核。CRI 2.0 利用直接和间接资料来确定该机制是否存在并合理管理。这一关键因素的更新情况将监督、追踪并评估值得注意的实质性发展。

6. 研发投资

说明一国网络就绪水平的第五个因素在于为广泛的网络安全基础以及应用研究和 ICT 举措建立一套国家战略重点，并在上述几个方面进行投资。ICT 的发展给几乎每个经济行业都带来了变革，转变了企业、政府、教育和公民生活、工作和娱乐的方式。这些创新活动促进了经济发展，并且有助于改善应变能力，为坚定的安全态势设置条件。

网络创新中心加速了创意和技术向解决方案的转化。

政府和企业可以发挥其各自作用，可结合其研发预算推进新一代 ICT 和网络技术与解决方案。企业和政府正在大举迎接移动网络、云计算、大数据、量子计算和物联网，并且必须针对这些数字设备和技术的信任、安全和应变能力进行投资。通过投资网络研发和其他创新领域，国家、大学和企业能提升能力来弥补其网络安全与攻击者能力之间的差距。例如，欧盟的“地平线 2020”（Horizon 2020）计划预计投入 800 亿欧元用于研究和技术发展。鉴于欧盟的“文件开放查阅”基本政策，该计划旨在促进研究结果，加速创新，提升效率和透明度。“地平线 2020”计划共有三大部分。第一个领域主题为“卓越科学”，集中于基础科学和应用科学，计划在未来七年内资助新增 25,000 名博士候选人完成博士培训。第二个领域主题为“使能技术与工业技术领导力”，强调 ICT、纳米技术、高级材料和加工等。第三个领域是资助应对社会和经济问题（如健康、能源、交通和安全）的解决方案。这一投资的评估标准之一就是企业间的跨国合作和能满足泛欧需求的解决方案。[70]

相类似的，美国重视、协调通过国家信息技术和研发项目（NITRD）进行跨领域研究，每年拨付超过 40 亿美元的资金。2016—2020 年的首要研究领域包括：大数据、网络实体系统、网络安全和数据保密研发、高端计算和无线频谱共享。[71] 网络和信息技术研究和发展项目是计算机、网络和软件方面高级信息技术的主要政府资助活动。该项目试图加快高级信息基础的发展和部署，提升国防和国土安全，同时提高美国的生产力和经济竞争力。此外，美国国防高级研究计划局（DARPA）、美国情报高级研究计划署（IARPA）和美国国土安全高级研究计划署（HSARPA）也拨款用于网络研发。然而，如果把整个网络研发的预算加在一起，总额还不到美国 GDP 的 1%。根据美国当前和未来庞大的网络风险，1% 的 GDP 远不足以弥补网络安全问题的鸿沟。

其他政府资助的举措通过提供研发税收抵免来刺激网络安全创新。比如，以色列认识到要促进组织和企业的投资，常常需要政府的鼓励和投入，最近该国面向网络防御公司实行了重大税项减免政策，只要公司在位于贝尔谢巴的国家网络园区参加并举办活动，即可享受该政策。[72] 通过集合技术人才来促进独特的产、学、军生态系统，以色列正在建立一个经济和战略网络安全中心。贝尔谢巴的网络园区还有助于促进网络领域的公私合作，发挥卓越创新中心的作用，并且提供有效培训和雇佣渠道。

助学金和奖学金是促进高级网络安全教育、拓展知识、培训能力的又一市场机制。比如英国政府的“科学无国界”项目，为包括计算机科学和信息技术在内所有科学、技术、工程、数学（STEM）领域提供奖学金。类似的还有巴西国家科学技术发展委员会（CNPq），该机构隶属巴西科学、技术和创新部，设立了“科学启蒙奖学金”鼓励年轻学生的 ICT 教育。[73]

网络安全研发创新必须推进未来网络社会的信任、安全和应变能力。

网络安全创新中心，比如海牙安全三角洲（Hague Security Delta），培养了创新网络安全研发，促进私营企业、政府和研究机构的合作。该基金会由海牙市政府和荷兰经济部支持，是欧洲最大的安全网络，与美国、加拿大、新加坡和南非的主要安全网络建立了知识桥梁。其网络安全项目包括网络安全学院和网络事件体验实验室等。目前该项目包含了建立一个高级恶意软件检测平台，为通过定性扫描发现、报告和管理网络漏洞提供解决方案。[74]

美国硅谷、特拉维夫、波士顿、纽约和伦敦也出现了一些其他私营领域的“网络创新中心”。比如伦敦的网络创新中心 CyLon 或 Cyber London，是欧洲首个网络安全孵化器。CyLon 致力于在伦敦培养网络创新生态系统，帮助企业开发信息安全产品。[75]

这些多种多样的研发举措和网络创新中心促进了从创意和技术到解决方案的转变，促进了数字市场的发展，提高了底层网络和基础设施的安全和应变能力，同时改善了社会福利。

一国在推进网络研发、教育和能力建设方面的投入，包括以下因素：

声明：

● 政府公开表示会举全国之力积极发展网络安全基础研究和应用研究；

● 公开宣布鼓励机制（如研发税负减免），鼓励网络安全创新以及新发现、基本技术、技巧方法、流程和工具的传播；

● 公开宣布政府鼓励机制（如助学金、奖学金），鼓励网络安全教育、知识拓展和技能培养。

组织：

● 确定至少有一个实体来负责监管全国的网络安全研发举措，该实体同时扮演全国性、世界性协作联络人的角色；

● 建立获得机构支持的学位项目，专业为网络安全、信息安全或专注于数字环境安全和应变能力的类似高等技术领域；

● 建立一个实体，用以测定并报告政府或商业成功转化项目（从研究到产品或服务）的比例，专注于提升数字环境安全和应变能力的解决方案。

资源：

● 确定网络安全基础和应用研究及举措所需要和分配的财务与人力资源；

● 确认商业或政府转化增强技术和创新所需要和分配的财务与人力资源。

落实：

● 落实专用于发展、宣传和常规化彼此协作的安全技术标准的项目，并且该项目被国际认可的标准机构所接受，并得到巩固强化；

● 有证据证明国内政府努力支持、发展和维护网络安全研发，特别是研究或生产转化率（例如政府内实施的比例）和成功转化项目的商业采纳率；

● 有证据证明存在额外的商业努力（如网络创新中心）来支持、发展和维护网络安全研发，特别是研究或生产转化率（例如私营行业中实施的比例）和政府采用商业领域内成功转化项目的采纳率。

这一关键因素的初步调查结果，基于审核一国是否在广泛地资助网络安全举措之外，还针对研发、教育、知识拓展和能力培养领域进行了投资。CRI 2.0 利用直接和间接资料来确定现有政府鼓励机制以及专用于上述类似举措的资源的类别。这一关键

因素的更新情况将监督、追踪并评估值得注意的实质性发展。

7. 外交与贸易

说明一个国家安全防护能力的第六个关键因素，在于一国是否将参与网络问题作为外交政策的一部分。基本来说，网络外交试图寻求针对常见威胁的双方都接受的解决方案。网络问题存在于许多不同的国际关系领域中，包括人权、经济发展、贸易协议、武器控制和军民两用技术、安全、稳定与和平、冲突解决。虽然网络安全问题与几乎每一个话题都有所联系，并且大多数谈判者都精通具体的话题领域（贸易或武器控制），但这些专家常常不了解网络世界萌生出的新增机遇或风险。因此，设立主要负责有关网络问题的外交事务的专门办公室或专员，将是一国外交政策的重要部分。

鉴于经济复苏的缓慢节奏，许多国家通过贸易协议来追求新的国际经济政策，借此来促进经济增长，创造市场机遇。然而，这些经济举措变成了大家讨论国家安全问题的焦点。例如，《跨太平洋伙伴关系协议》（TPP）于 2015 年 10 月 5 日签署。协议旨在推动跨太平洋伙伴国家的贸易和投资，促进创新、经济发展并支持就业机会的创造和保留。相关方花了 5 年时间才达成这一协议，部分是因为网络问题。伙伴国家不能就数据保护和隐私要求、数据本地化要求（如知识产权保护）和内容限制等关键事务达成协议。

美国和欧盟正在协商达成与 TPP 类似的《跨大西洋贸易与投资伙伴协定》（TTIP）。该协议试图扩大市场准入，清除不必要的法规束缚，建立管理两大区域间复杂商业关系的规定，创造就业机会，推动 GDP 增长。[76] 谈判过程之所以如此缓慢，核心问题之一就是数据保护和隐私。

基本来说，网络外交试图寻求针对常见威胁的双方都接受的解决方案。

过去十年间，针对往来欧盟和美国或在欧盟和美国居住的人士的所有个人数据，欧洲和美国已经就数据转移和储存的共同保护标准达成一致意见。[77] 但是，爱德华·斯诺登（Edward Snowden）泄露的文件将美国政府情报部门对其他政府和公民信息的收集活动公诸于众，致使双边政府间的信任荡然无存。因此，许多欧洲国家要求建立国家层面的双边隐私标准、加密规则和法律框架，以便跟上突飞猛进的技术步伐，同时令国家为充分保护数据承担责任。此外，根据欧盟法院最近的一项裁决，欧盟和美国“安全港”（Safe Harbor）数据保护标准的长期协议被判无效。“安全港”行政决策允许美国公司遵守自律原则，依照欧洲数据保护法令和基本欧洲权利（如隐私），对欧洲用

户的数据提供“充分保护”。虽然双方在进行升级“安全港”的谈判，但是并没有设定完成升级的时间范围，更加大了《跨大西洋贸易与投资伙伴协定》的谈判复杂度。[78] 目前，美国驻欧盟商会估计安全港的失效会给欧盟带来最多 1.3% GDP 的损失。[79]

另一个区域自由贸易协议——《区域全面经济伙伴关系协定》（RCEP）正在东盟成员国、中国、印度、日本、韩国、澳大利亚和新西兰之间展开讨论。16 个 RCEP 国家占全球将近一半的人口，全球将近 30% 的 GDP，以及超过四分之一的全球出口量。RCEP 的目标是降低贸易壁垒，推动经济技术合作，保护知识产权，鼓励竞争，促进争端解决，扩大商品和服务出口商的市场准入。谈判过程中，一些国家试图引入保护数据的机制，出于国家安全目的维护数据主权。[80]

网络安全渗透于外交政策和贸易的方方面面。

此外还有聚焦技术方面的一整套安全领域的谈判。例如，拥有包括美国、英国、俄罗斯和大多数欧盟国家在内总共 41 个签约国的《关于常规武器和两用物品及技术出口控制的瓦森纳安排》（简称瓦森纳协定），最近同意限制网络“通信监控系统”和“入侵软件”的销售，这些系统和软件经过特殊设计或改造，可以逃避监控工具的检查或者可以突破防护措施。[81] 各国对于这些技术的军民两用持有不同的顾虑。比如，漏洞评估工具经常可以使用“零日漏洞”来发现网络漏洞。同样的技术可用作武器。因此，将这些技术纳入出口管控机制反映出了一个观点，那就是高级技术可能会突破国家的国防并构成国家安全风险。

其他的外交谈判和讨论试图建立共识或共同规则，以提高全球 ICT 环境的稳定性和安全。其中包括加强合作机制以应对 ICT 安全事件，解决 ICT 基础设施相关的请求（例如僵尸网络感染造成一国出现非法活动）。外交还被用于界定哪些类别的网络活动可以进行，哪些类别的网络活动必须禁止（比如负责任国家行为标准），一般被称为“网络行为规范”。举例来说，美国政府专家工作组最近强调了 ICT 环境的全球性质、信息安全领域现有和潜在的威胁以及解决这些威胁的可能合作措施。工作组发现遵守国际法律，特别是联合国宪章义务，为各国的 ICT 使用提供了一个关键框架。他们同意针对负责任国家行为的网络规范、法规或原则以及信任建立措施，建立一个框架。[82] 在信任建立措施中，政府专家工作组同意加强相关政府机构之间的合作机制，解决 ICT 安全事件，并且发展额外的技术、法律和外交机制，应对 ICT 基础设施相关的要求（例如建立 CSIRT 或其他官方组织来履行该职能）。前不久，美国总统巴拉克·奥巴马和中国国家主席习近平同意遵循美国政府专家工作组的建议，恪守联合国规定的在线行

为规范；特别是那些针对在和平时期使用网络袭击来破坏他国关键基础设施的规定。[83]

基于政府专家工作组的部分常见主题，巴西、俄罗斯、印度、中国和南非（金砖国家）的领导人达成一致意见，通力合作解决常见的 ICT 安全问题。他们还同意分享 ICT 使用安全方面的信息和最佳实践，协作打击网络犯罪，在成员国内部建立 POC 网络，利用现有的 CSIRT 建立金砖国家内部合作。他们还敦促国际社会重点关注信任建立措施、能力建设、不使用武力和防止 ICT 冲突。[84]2015 年 1 月，上海合作组织向联合国大会引入了修订版《信息安全国际行为准则》，试图确定各国在信息空间的权利和责任，推进建设性和响应性行为，推动合作来解决双边 ICT 威胁。[85] 上海合作组织根据 2012 年和 2013 年专家工作组的报告，修改了 2011 年行为准则的条款，以期拓宽在七十七国集团中的吸引力。

其他国际组织在追求具体目标时融入了经济、发展和安全的话题。比如国际电信联盟（ITU）在四场全球会议中就 ICT 和网络的政策、技术、管理环境展开定期国际讨论：信息社会世界峰会（WSIS）、国际电信世界大会（WCIT）、国际电信发展大会（WTDC）和国际电信标准化大会（WTSA）。[86] 此外，美洲国家组织和美洲开发银行联手成员国来系统性地解决网络安全问题，主要分三大领域：①同时具有社会包容性和环境可持续性的发展；② ICT 作为工具来实现创收、增加就业机会，访问商业网站和信息，实现在线学习并促进政府活动；③核心基础设施和公民服务的安全。[87]

毋庸置疑，网络安全问题正从广泛多样的外交领域中浮现出来。网络安全不仅仅是安全问题，还构成了贸易、外交和经济政策以及一国未来经济发展潜力的基础因素。一国要有效地在外交中参与网络事宜，关键在于建立一支训练有素的专业队伍，构建具体组织结构，拨付资金用于网络安全领域的国际讨论和谈判。例如，以色列和捷克共和国为重要城市（包括华盛顿特区和布鲁塞尔）的大使馆配备了网络专员。[88]

美国也对派往亚洲的外交人员进行了为期一周的网络意识培训。[89] 建立相关人员队伍对于一国实现未来外交政策、经济政策、贸易和经济增长目标来说日益重要。

健全的网络安全方面外交参与能力应包括以下因素：

声明：

- 确认将网络安全视为外交政策和国家安全中的重要组成部分（例如双边和多边官方讨论一般会涉及高层政治和军事领导人）；
- 确认将 ICT 和网络安全视为国际经济政策、谈判、商业贸易的重要组成部分。

组织：

● 在国家的驻外办公室或类似组织中设立一支训练有素的专业队伍，主要职责包括在国际上积极参与网络安全外交；

● 在驻外网络外交人员的数量和级别上保持一致性，一国公开表示积极参与网络安全外交，并将其视为全国性的顶级事务。

资源：

● 确定参与网络外交所要求和分配的财政和人力资源。

落实：

● 已经参与国际、跨国、区域或双边协议的制定、签署和执行，该协议旨在寻求解决常见问题、为双方都接受的解决方案；

● 有证据显示已采取行动来影响国际贸易和商业谈判，而国际贸易和商业谈判与 ICT 的使用或者网络基础设施、关键服务和技术的国际、区域或国内共享部分有关。

这一关键因素的初步调查结果，基于审核一国是否明确指定或设立了政府办公室或任命个人承担外交责任（包含网络问题的经济和安全部分）。CRI2.0 利用直接和间接资料来确定政府机构或个人是否参与并影响了网络安全相关的国际谈判，以及参与和影响的程度。这一关键因素的更新情况将监督、追踪并评估值得注意的实质性发展。

8. 防御与危机应对

网络就绪水平的第七个也是最后一个因素，在于一国国家武装部队或相关防御机构保卫国家免受网络空间中的威胁的能力。对这类能力感兴趣的国家正引导武装部队发展能力或专业知识，应对国家级关键网络冲突导致的网络威胁。[90]

各国之间的联系日益密切，在网络领域的互相依赖愈加明显，这反过来就会让他们更容易受到破坏性、毁灭性的网络活动的伤害。大多数国家在面对复杂网络袭击时的防御姿态都显得较弱。现代竞争和冲突的国际连通性促使网络对手跨过国家系统，目标直击一国的商业和非政府组织。比如 2012 年 8 月，沙特阿拉伯国家石油公司就经历了一场针对性袭击，袭击者使用恶意软件摧毁数据，造成将近 75% 的公司 IT 基础设施遭到破坏。[91] 公司高管表示这次袭击意图影响石油生产。

几个月之后的 2013 年 3 月，包含韩国第四大银行新韩银行在内的多家金融机构遭遇了恶意软件袭击，该软件与当初袭击沙特阿拉伯国家石油公司的软件相类似。银行的电子服务被迫中断，数据也遭到破坏。这一事件的经济损失预计超过 8000 亿美元。[92]

2014 年 12 月，“黑客”成功操控并破坏了一家德国钢铁厂的控制系统，造成高炉非正常停工，带来了巨大的损失。[93] 同年，索尼影业也沦为了网络袭击的受害者，

不仅多部未上映的动作电影遭到非法复制，而且公司邮件被窃取后遭到泄露，财务文件被曝光。数万名索尼员工的保密数据被复制，从数据到硬件，病毒软件破坏了将近八成的公司 IT 资产。[94]

各国必须做好准备，应对现有和未来的冲突，捍卫自身的网络利益。网络的速度和范围连通了社会的方方面面，人们很轻松就能获得军方级的网络武器，对许多人而言构成了不对称的优势。的确，恶意袭击者的种类多种多样，有政治激进主义者、罪犯、恐怖分子、国家和非国家组织，所有这些惨剧的导演都有着不同的动机。目前，60 多个国家已经培养了应对网络间谍和袭击的能力，同时还适当考虑获得或培养防御性或先发制人的攻击能力。[95] 此外，各国已经开始制定不同的战略和工具以升级国家级网络安全防御。大多数政府本能性地依赖提升已经能够在境外网络空间运行的安全机构（即防御组织或情报机构）的现有防御能力。其他政府试图将这些职能置于军事结构以外的安全组织中。[96]

比如，2010 年美国建立了一个专门的军事机构——美国网络司令部，应对针对军事基础设施的网络袭击。2015 年，该部门的任务有所拓展，当时美国国防部发布了第二项网络战略，以指引国防部网络军队的发展以及促进网络安全防御和网络威慑姿态（接受美国网战司令部命令和控制）。新战略强调需要“做好准备保卫美国国土和美国重要利益，应对后果严重的破坏性或毁灭性网络袭击”，以及建立、维护和使用可行的网络选择来控制冲突升级，塑造各阶段的作战环境。[97]

无独有偶，2014 年 12 月，俄罗斯公布了新的军事政策，突出强调俄罗斯出于防御和攻击目的以及“非核武威慑力”发展网络战备能力。[98] 俄罗斯的 2011 年国防部白皮书《关于俄罗斯信息空间武装部队活动的概念图》响应俄罗斯的国防政策，但明确包含了民众意见以及出于缓解局势的目的，需要让媒体了解不断变化的冲突情况。[99] 根据俄媒报道，俄罗斯政府计划 2016 年出台新的信息安全政策，旨在发展信息站和信息系统军队，起到战略威慑和阻止冲突的作用。[100]

韩国和巴西也建立了类似的军事组织，旨在确保攻击性、防御性和响应能力，同时确保在网络战中打胜仗。[101] 韩国已经在不断扩展自身的网络能力，据报道，韩国正在为其网络司令部培训 400 多支新队伍，总数将达到 1000 支队伍。[102]

此外，中国虽然没有公开发布任何网络或信息军事应用的正式战略政策，但出台了指导防御政策的“军事战略方针”。[103] 中国的 2013 年白皮书《中国武装力量的多样化运用》和 2014 年的《关于切实保障信息安全的意见》强调了发展防御性网络能力。这些文件强调人民解放军在网络领域秉承“人不犯我，我不犯人；人若犯我，我必犯人”

的原则。[104]

网络安全防御机构无需成为国家军队中的统一性机构。国家警察和情报势力可以承担起一国的网络防御能力，但武装力量还应当现代化，为更多传统的冲突做好网络准备。例如，冰岛已将网络响应集中划归到武装力量之外。过去冰岛的网络安全职责分散在内政部、邮政和电信管理局、数据保护局和冰岛警方中。然而，2015 年冰岛将所有的网络职能收归冰岛警察总署。[105] 冰岛 2015 年 6 月的全国网络战略还强调了北约同盟对于冰岛网络安全防御的不可或缺的作用。[106]

破坏性和毁灭性的网络活动需要可信的网络防护。

最后，以色列虽然目前没有设立正式的“网络司令部”，但其具备网络安全能力，分散在以色列国防军和以色列军情处。以色列军情处负责攻击性网络安全能力，而安全局负责保护。以色列的国内安全局“辛贝特”负责保护政府系统和关键国家基础设施，国家控制特别工作组则保护关键网络和私营行业免于“黑客”袭击和间谍活动。[107] 然而，情形可能会有所变化，因为 2015 年 6 月，以色列国防军总参谋长加迪·埃森科特（Gadi Eisenkot）宣布计划建立与海军和空军同等级的新国防军部队，负责所有的网络活动。如果国防部部长批准建立新部队，那么未来两年内将出现新的网络国防军。新的网络司令部一经设立，就会合并目前以色列国防军提供的防御能力和以色列秘密情报组织“8200 单位”（Unit 8200）和其他军情机构提供的攻击性防御和情报能力。[108] 这符合 2015 年 8 月发布的新的国防军五年计划“吉迪恩”（Gideon）。该计划特别号召增加举措来防御可能来自地区非政府和恐怖主义团体的网络袭击和其他非对称威胁。[109]

对于一国而言，必须具备网络防御能力才能确保国家和经济安全。各国越依赖网络和 ICT 系统，就越容易受到“低级”网络袭击和非对称活动的侵害。许多国家都面临着进退两难的局面：一方面，增强 ICT 对于发展来说至关重要；另一方面，国家间的联系越密切，产生的风险越大。不涉足网络经济已经不再是一个选择。各国必须做好在网络世界中自我防御的准备。如果一国无法实现自我防护，就没有做好应对网络的准备。

一国在设立并部署专门的国家防御单位，以履行网络防御能力或责任方面的投入，包括以下因素：

声明：

- 发布全国声明，指派一个组织负责全国网络防御，将该任务视为首要任务；
- 设定网络防御组织的政策，应对网络威胁；

● 阐述全国声明，引导网络防御组织培养应对主权领土内外威胁的能力。

组织：

● 在军队中建立全国性组织，主要负责国家的网络防御；

● 在军队以外建立全国性组织，主要负责国家的网络防御。

资源：

● 对于军队内部明确负责国家网络防御的组织，确认该组织所需要和分配的财务和人力资源；

● 对于军队外部明确负责国家网络防御的组织，确认该组织所需要和分配的财务和人力资源。

落实：

● 有证据表明进行了政府级演习，展示国家网络防御就绪水平；

● 有证据表明进行了涉及受影响商业实体的国家级演习，展示国家网络防御就绪水平；

● 有证据表明与国际伙伴进行了演习（如北约共同防御演习或亚太计算机紧急响应小组 APCERT 演习），展示信息交换和协助方面的合作；

● 确立网络空间的负责任政府行为标准，设定允许参与网络防御的门槛；

● 确立在发生重大网络事件时针对政府或具体行业的快速援助机制（同 CERT 或同等组织分离开）。

这一关键因素的初步调查结果，基于审核一国是否正式宣布建立防御力量，主要负责国家的网络防御。CRI 2.0 利用直接和间接资料来确定防御力量的运营成熟度。这一关键因素的更新情况将监督、追踪并评估值得注意的实质性发展。

结论

我们的网络系统和基础设施面临着越来越多的真实威胁，给国家和社会带来了危害。经济和国家安全议程必须共同努力，为网络安全问题增加透明度。展示这一重要联系，可能会激发国家和全球对解决这一经济蛀虫的兴趣。CRI 2.0 基于经验的全面、比较性方法提供了一个蓝图，针对数字前景和发展所依赖的国家网络基础设施和服务，评估任一国家保护这些基础设施和服务的成熟度和投入。

没有一个国家做好了应对网络的准备。

CRI 2.0 蓝图确定了七大关键因素中 70 多个独特的数据指标：国家战略、事件响应、

电子犯罪与执法、信息共享、研发投资、外交与贸易、防护与危机应对。这些指标和关键因素为一国采取能够抵御 GDP 损失的强大安全姿态提供了框架。

实际上，CRI 2.0 挑战了传统观念，将网络安全视为国家安全的重要部分。CRI 2.0 展示了国家安全与网络连通性及快速采用 ICT 之间的密切联系，当网络连通性与 ICT 采用处于安全状态时，密切联系在一起的，并且以安全方式迅速采用 ICT，即可以促进实现经济增长和繁荣。

如您需要了解更多信息或希望向 CRI 2.0 方法论提供数据，请联系：CyberReadinessIndex2.0@potomacinstitute.org

CRI 2.0 并非仅仅研究该问题，相反地，它还提出了一个框架，让一国可以评估其保护经济免受网络安全问题侵害的能力。CRI 2.0 将会定期更新，不断添加评估标准，在原来评估的基础上确保不丢失比较有效性。如此一来，针对一国数字前景未来和发展所依赖的网络基础设施和服务，CRI 2.0 将可以展示各国在保护这些基础设施和服务方面所做出的努力和完成的进度及发展情况。

没有一个国家能够承担得起网络安全问题及其带来的损失。CRI2.0 所提供的数据和方法论可以帮助国家领导人在一个深度网络化、竞争激烈、冲突丛生的世界中，做出规划，实现更安全、更具有应变能力的经济。

参考书目

1.《网络就绪报告 2.0》立足于《网络就绪报 1.0》，后者提供了一个方法论框架，通过五个关键因素对网络就绪水平进行评估。五大关键因素包括：国家网络战略、事件响应、电子犯罪与执法能力、信息共享以及网络研发。《网络就绪报告 1.0》对首批 35 个国家采用了该方法。更多关于《网络就绪报告 1.0》的信息，请参阅：梅丽莎·海瑟薇（Melissa Hathaway），《网络就绪报告 1.0》，海瑟薇全球战略有限公司（2013），http://belfercenter.ksg.harvard.edu/files/cyber-readiness-index-1point0.pdf。

2. 网络基础设施的复杂性，造成了关键服务交付（水、电、交通、通讯、健康等）的网络连接的互相依赖。更多关于网络基础设施复杂性的问题，参阅：梅丽莎·海瑟薇（Melissa Hathaway），《联系起来的选择：网络给主权决定带来了何种挑战》，《美国外交政策利益 36》第 5 期（2014 年 11 月）：301。

3. 全球寻求 ICT 基础的经济战略的实例，包括：欧洲的《数字单一市场》、印度的《数字印度》、中国的《互联网 +》以及国际电信联盟的《联接发展目标》（Connect 2020）。

4. 中国国务院，《互联网 +》，《国发 40》（2015）。美国国务院翻译。

5. 印度政府，《项目支柱》，《数字印度：支柱力量》（Power to Empower），http://www.

digitalindia.gov. in/content/programme-pillars。

6. 欧洲委员会，《数字单一市场：消除障碍，解锁在线机遇》，

http://ec.eu- ropa.eu/priorities/digital-single-market/。

7. 梅丽莎·海瑟薇（Melissa Hathaway）和弗朗切斯卡·斯比达力艾力（Francesca Spidalieri），《可持续安全发展：应变能力网络社会的框架》，《拉丁美洲和加勒比地区网络安全观察台》（未来一期为 2015 年 12 月美洲国家组织的出版物）。

8. 世界银行，《总览》，《信息和通讯技术项目》，最新修订 2014 年 10 月 2，http://worldbank.org/en/topic/ict/overview。

9. 大卫·迪恩（David Dean）等，《数码宣言：企业和国家如何能在数字经济中取胜》，《波士顿咨询公司报告》（2012 年 1 月）：2。

10. 彼得·伊万斯（Peter C. Evans）和马可·安农齐亚塔（Marco Annunziata），《工业互联网：推进思想和机器的极限》，通用电气（2012 年 11 月 26 日）：13。

11. 梅丽莎·海瑟薇（Melissa Hathaway），《网络就绪报告 2.0》和《从国家网络安全战略设计所学到的教训》，（于华盛顿特区的美洲国家组织－美洲开发银行关于网络安全政策的区域研讨会上发布，2014 年 10 月 23 日）。

12. 前沿经济学（Frontier Economics），《预测假冒和盗版造成的全球经济和社会影响：受商业行动委托，针对假冒和盗版的报告》，（伦敦，前沿经济学公司，2011 年）：47。

13. 美国国家亚洲研究局，《知识产权委员会报告：针对盗用美国知识产权的委员会报告》，美国国家亚洲研究局（2013 年 5 月）。

14. 梅丽莎·海瑟薇（Melissa Hathaway），《联系起来的选择：网络如何给主权决定带来了挑战》，《美国外交政策利益 36》第 5 期（2014 年 11 月）：301。

15. 哈维·波比路(Harvey Poppel)因20世纪70年代发明了哈维球(Harvey Balls)而闻名于世，当时他在博思艾伦汉密尔顿控股公司（Booz Allen Hamilton）担任顾问。

16. 基于 2013 年世界银行 GDP 排名。

17. 经济合作与发展组织（OECD），《2015 年 OECD 数字经济展望》（法国巴黎：OECD 出版社，2015 年），http://dx.doi.org/10.1787/9789264232440-en。

18. 梅丽莎·海瑟薇（Melissa Hathaway），《透明、信任和我们的网络》（在加拿大渥太华微软全球技术中心会议上发布，2015 年 10 月 20 日）。

19.ICT 基础设施建设包括含用户认购和家庭数据访问的固定和移动（音频和数据）市场，以及电信行业的投资和收益。

20. 主管机关指拥有法定权利、能力或权力来执行指定职能的任一个人或组织。

21. 国际电信同盟，《国家战略》，http:// www.itu.int/en/ITU-D/Cybersecurity/ Pages/National-Strategies.aspx。

22.CSIRT 和 CERT 指的是被指派应对计算机安全事件的 IT 安全专家团队。两个属于可互换，CSIRT 更为确切。

23. 国际电信同盟，《ICT 计划》，http:// www.itu.int/en/ITU-D/Cybersecurity/ Pages/Organizational-Structures.aspx。

24. 约翰·哈勒（John Haller），塞缪尔·梅林（Samuel Merrell）、马修·波特科维奇（Matthew Butkovic）和布兰德福特·威尔克（Bradford Willke），《国家网络安全的最佳实践：建立全国计算机安全事件管理能力》，版本 2.0（宾夕法尼亚州匹兹堡：卡耐基梅隆大学软件工程研究所，2011 年），http://resources.sei.cmu.edu/ library/asset-view.cfm?AssetID=9999。

25. 奥拉夫·科瑞德霍夫（Olaf Kruidhof），《国家和企业 CERT 的发展——信任是关键》，《计算机网络防御的最佳实践：事件发现和响应》，编辑：梅丽莎·海瑟薇（Melissa E. Hathaway），（阿姆斯特丹：北约和平与安全科学研究，IOS 出版社，2014 年 2 月）。

26. 新加坡紧急响应团队，《常见问答》，https://www. csa.gov.sg/singcert/about-us/faqs.

27.Ministério das Comunicações, “Portaria Interministerial N 147, de 31 de Maio de 1995,” http:// cgi.br/portarias/numero/147.

28. 巴西国家计算机安全事件响应小组（cert.br），《关于 CERT.br》 http:// www.cert.br/about/.

29.《文件》，亚太计算机紧急响应小组（APCERT），APCERT. org， 2015 年 10 月 13 日。http://www. apcert.org/documents/index.html。

30.《亚太计算机紧急响应小组（APCERT）运营框架》，APCERT，APCERT.org， 2015 年 10 月 13 日。http://www.apcert.org/ documents/pdf/OPFW（26Mar2013）.pdf。

31. 梅丽莎·海瑟薇（Melissa Hathaway），《计算机网络防御的最佳实践：事件发现和响应》，全球网络安全中心（2013 年 9 月）：12。

32. 英格瓦·海尔奎特（Ingvar Hellquist）（曾任上校，已卸任），资深顾问和拉斯·尼坎德尔（Lars Nicander），瑞典国防大学非对称威胁研究主任，《CATS 课程和网络演习》，（由梅丽莎·海瑟薇在瑞典斯德哥尔摩采访，2012 年 10 月 17 日）以及瑞典国防学院，《CATS 新闻》，非对称威胁研究的 CATS 中心（2013 年春）。

33. 杜桑·那拉提尔（Dusan Navratil），捷克共和国国防局局长和罗伯特·卡霍夫（Robert Kahofer），特别助理，《2015 年捷克网络 - 全国技术网络安全演习》，（由梅丽莎·海瑟薇在华盛顿特区采访，2015 年 10 月）。

34.《韩国表示核虫不足为惧》，TheRegister. co.uk，2014 年 12 月 30 日，http://www.theregister.co.uk/2014/12/30/south_ko- rea_says_nuclear_worm_is_nothing_to_ worry_about/ 以及《韩国水电与核电公司的电脑系统遭黑客袭击》，世界核新闻，2014 年 12 月 22 日，http://www. world-nuclear-news.org/C-Activists-hack- KHNPs-computer-systems-2212141.html。

35. 国土安全部，《网络风暴：保护网络空间》，http://www.dhs.gov/cyber-storm-securing-cyber-space。

36. 欧洲委员会，《欧盟的网络政策：建立开放、安全的网络空间》，《欧洲议会、欧洲委员会、欧洲经济和社会委员会以及地区委员会的联合通讯》，（2013 年 7 月）：7 和欧盟网络和信息安全局，《网络欧洲》，https://www.enisa.europa.eu/activities/Re- silience-and-CIIP/cyber-crisis-cooperation/ cce/cyber-europe。

37. 道格·准克沃特（Doug Drinkwater），《欧洲上千公司面临 200 次网络袭击》，SC 杂志，2014 年 10 月 31 日，欧洲网络与信息安全局（ENISA），《2014 年 ENISA 网络欧洲：媒体报

道》，https://www.enisa.europa.eu/activities/ Resilience-and-CIIP/cyber-crisis-co-operation/cce/cyber-europe/ce2014/ cyber-europe-2014-information/cyber-europe-2014-media-coverage。

38. 欧洲防务局，《在维也纳举行的复杂网络危机管理演习》，2015 年 9 月 16 日，https://www.eda.europa.eu/info-hub/ press-centre/latest-news/2015/09/16/ complex-cyber-crisis-management-ex- ercise-in-vienna 以及北约，《北约举办成立以来最大的一次网络防御演习》，2014 年 11 月 21 日，http://www.nato.int/cps/en/natohq/ news_114902.htm?selectedLocale=en。

39. 凯迪·波·威廉姆斯（Katie Bo Williams），《美国和英国本月即将测试金融行业的网络安全水平》，国会山庄报（The Hill），2015 年 11 月 2 日，http://thehill.com/policy/cybersecu-rity/258827-us-uk-to-test-finance-sec- tor-cybersecurity-this-month。

40. 国家互联网应急中心（CNCERT/CC），《针对网络安全应急响应的第二届中日韩三国 CSIRT 年会在韩国圆满结束》www.cert.org.cn/publish/englis h/55/2014/20140916145739295996084/20140916145739295996084_.html。

41. 卡耐基梅隆大学，《国家 CSIRT 列表》，CERT 部，http:// www.cert.org/incident-management/ national-csirts/national-csirts.cfm。

42. 欧洲网络与信息安全局（ENISA），《ENISAT-CERT 清单：欧洲 CERT 小组清单和活动》，ENISA 版本 2.16（2014 年 6 月），http://www.enisa.europa.eu/activities/cert/background/inv/files/ inventory-of-cert-activities-in-europe。

43. 事件响应和安全小组论坛（FIRST），《FIRST 成员》，http://www.first.org/members/teams。

44. 欧洲理事会，《网络犯罪大会》（2001 年 11 月 23 日）和上海合作组织，《信息安全领域的合作》，61 次全体会议（2009 年 6 月 16 日）。

45.Ibid.

46. 上海合作组织，《信息安全领域的合作》，61 次全体会议（2009 年 6 月 16 日）.https://ccdcoe. org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf。

47. 法官斯坦·希尼尔伯格（Stein Schjolberg）和阿曼达·哈巴德（Amanda M. Hubbard），《协调统一国家应对网络犯罪的法律途径》，国际电信联盟（2005 年 7 月 1 日）:6。

48. 二十个国家签署了政府专家工作组报告，包括：白俄罗斯、巴西、中国、哥伦比亚、埃及、爱沙尼亚、法国、德国、加纳、以色列、日本、肯尼亚、马来西亚、墨西哥、巴基斯坦、韩国、俄罗斯、西班牙、英国和美国。参见：联合国，《在国际安全背景下信息和电信领域发展的政府专家组报告》，A/65/201 和 A/68/98 （2015 年 6 月 26 日）。

49. 埃内斯托·萨瓦那（Ernesto U. Savona），《犯罪和技术：法规、执法和研究的新前沿》（荷兰多德雷赫特：施普林格出版公司， 2004）:50。

50. 网络法律和取证研究、发展和培训高级中心，《学术项目》印度国立法学院，https://www.nls.ac.in/index.php?option=com_ content&view=article&id=502&Itemid=32。

51. 国际刑警组织，《国际刑警组织亟待创新的全球复杂事宜》，访问日期：2015 年 9 月 17 日，

http://www.interpol. int/About-INTERPOL/The-INTER- POL-Global-Complex-for-Innovation。

52. 马丹·奥贝罗（Madan M. Obero），《黑暗网络和密码电子货币》（在印度班加罗尔的《网络 360：协作会议》上发布，2015 年 9 月 30 日）。

53. 僵尸程序指一类恶意软件，可以使用你的计算机发送垃圾软件，制作钓鱼网站，或者通过监控你的按键盗取你的身份。受感染的计算机会被第三方所操控，用于发动网络袭击。更多信息请参阅：梅丽莎·海瑟薇（Melissa Hathaway）和约翰·萨维奇，《网络空间的管理：网络服务提供商的职责》，网络对话 2012（2012 年 3 月）。

54. 阿拉斯戴尔·史蒂文森（Alastair Stevenson），《美国 FBI 警告称僵尸网络每秒钟感染 18 个系统》，V3.cok. uk，2014 年 7 月 16 日，http://www.v3.co.uk/ v3-uk/news/2355596/botnets-infecting- 18-systems-per-second-warns-fbi。

55. 加拿大贝尔公司等，《黑色空间项目》，安全电信咨询委员会（2011）:13，https://citizenlab.org/cybernorms2012/ cybersecurityfindings.pdf。

56. 伊藤友里惠，《网络清洁中心》，（经网络就绪报告团队远程采访，华盛顿特区，2015 年 11 月 10 日）。

57. 日本内务省和经济产业省，《什么是网络清洁中心》，网络清洁中心，https:// www.telecom-isac.jp/ccc/en_index.html 以及迈克尔·罗沙维奥（Michael M. Losavio），J. 伊戈尔·舒特（J. Eagle Shutt）和的博拉·基林（Deborah Wilson Keeling），《改变游戏规则：网络安全提升后的社会和司法模型》，出自塔雷克·萨达为（Tarek Saadawi）、路易斯·乔丹（Louis H Jordan Jr.）和韦森特·布德罗（Vincent Boudreau），《网络基础设施保护卷 2》（美国陆军军事学院战略研究，2013 年）:101。

58.Telecom-ISAC Japan，《主席致辞》，2011 年 5 月 12 日，https://www. telecom-isac.jp/english/index.html。

59. 澳大利亚网络安全计划（AISI），《澳大利亚网络安全计划总览》，http://www.acma.gov.au/Industry/Internet/e-Security/ Australian-Internet-Security-Initiative/australian-internet-security-initiative。

60. 麦咖啡杀毒软件（McAfee），《McAfee 和战略与国际研究中心：打击网络犯罪可给全球经济带来积极影响》，2014 年 6 月 9 日，http://www.mcafee.com/us/about/ news/2014/q2/20140609-01.aspx 以及美国国家亚洲研究局《知识产权委员会报告：针对盗用美国知识产权的委员会报告》，美国国家亚洲研究局（2013 年 5 月）。

61. 梅丽莎·海瑟薇（Melissa Hathaway），《为何成功合作对于推进网络安全来说至关重要》，新新互联网， 2010 年 5 月 7 日。

62. 荷兰公共安全与司法部，《国家网络安全中心（NCSC）》，https://www.ncsc.nl/english。

63.2007 年 2 月，英国国家基础设施安全协调中心与国家安全建议中心合并，成立国家基础设施保护中心（CPNI）。了解更多关于 CPNI 的信息，请访问：国家基础设施保护中心，http://www.cpni.gov.uk。

64. 日本的信息技术促进会（IPA）、日本 IT 安全中心，《日本网络安全信息共享合作计划

（J-CSIP）年度活动报告 -2012 财年》，（2013 年 4 月）。

65. 金融服务信息共享和分析中心，《金融服务信息共享和分析中心总览》，2015 年 9 月 17 日访问，https://www.fsisac.com/sites/default/files/ FS-ISAC_Overview_2011_05_09.pdf。

66. 国家网络刑事鉴定及培训联盟，《成为国家网络刑事鉴定及培训联盟的伙伴》https://www.ncfta.net/ become-ncft-partner.aspx。

67. 拉斐尔·曼达里诺（Raphael Mandarino），《MT2: 公私合作》，国家安全局、巴西信息安全和通信部、总统办公室，（在第一届国际刑警组织安全会议上发布，香港，2010 年 9 月 15-17 日）。

68. 美国国家标准与技术局（NIST），《全国漏洞数据库》，https://nvd.nist.gov。

69. 英国和巴西目前实行机制，对情报予以解密（取消保密）并与关键行业分享，比美国的情况要好很多。

70. 欧洲委员会，《ICT 研究和创新》，《地平线 2020: 欧盟研究和创新框架计划》，http://ec.eu-ropa.eu/programmes/horizon2020/ en/area/ict-research-innovation。

71. 了解更多网络和信息技术研究和发展项目及其研究领域，请参阅：www.nitrd.gov/Index.aspx 和网络和信息技术研究和发展项目，《网络和信息技术研究和发展项目》，《2016 财年总统预算附录》（2015 年 2 月），https://www.whitehouse. gov/sites/default/files/microsites/ostp/ fy2016nitrdsupplement-final.pdf。

72. 以色列驻纽约大使馆，《内阁批准国家网络园的税务减免待遇》，以色列驻纽约大使馆，2014 年 6 月 7 日，http://embas-sies.gov.il/wellington/NewsAndEvents/ Pages/Cabinet-approves-tax-break-for- National-Cyber-Park-6-Jul-2014.aspx。

73.CiênciaSemFronteiras，《常见问答》，http://www.cienciasemfronteiras.gov.br/web/csf-eng/faqEGTI_2013-2105_v1-3，提升高等教育人员素质的协调组织（CAPES），《提升高等教育人员素质的协调组织（CAPES）》，http://www.iie.org/Programs/CAPES，和巴西国家科学技术发展委员会（CNPq），《ProgramasInstitucionais de IniciaçãoCientífica e Tecnológica》，http://www.cnpq.br/web/guest/piict。

74.《网络安全》，海牙安全三角洲，https://www.thehaguese- curitydelta.com/cyber-security。

75. 扎克·库特勒（Zach Cutler），《全球五个正在发展的网络安全中心》，企业家，2015 年 9 月 3 日，http:// www.entrepreneur.com/article/250024。

76. 欧洲委员会，《关于＜跨大西洋贸易与投资伙伴协定＞（TTIP）》，贸易，http://ec.europa.eu/trade/ policy/in-focus/ttip/about-ttip/。

77.《欢迎来到美国 - 欧洲安全港》，http://www.export.gov/ safeharbor/eu/eg_main_018365.asp。

78. 欧盟法院，《欧盟法院宣布欧盟委员会建立美国安全港的决定无效》，新闻发布会 117/15（2015 年 10 月 6 日），http://curia.europa.eu/jcms/upload/docs/applica- tion/pdf/2015-10/cp150117en.pdf。

79. 美国驻欧盟商会，《欧盟法院对施伦斯案件的决定会阻碍环大西洋地区的商业来往，损害欧洲经济，破坏数字单一市场》，新闻发布会，2015 年 10 月 6 日，http://www.amchameu. eu/

sites/default/files/press_releases/ press_-_ecj_decision_on_schrems_will_ disrupt_transatlantic_business.pdf。

80. 梅丽莎·海瑟薇(Melissa Hathaway),《联系起来的选择: 网络如何给主权决定带来了挑战》，302 和亚伦·苏克玛（Arun Mohan Sukmar），《亚洲的新游戏》，《印度教徒报》，2015 年 8 月 15 日，访问时间：2015 年 9 月 16 日，http:// www.thehindu.com/opinion/op-ed/arun-mohan-sukumar-column-the-new- great-game-in-asia/article7575755.ece。

81.《关于常规武器和两用物品及技术出口控制的瓦森纳安排》，最近更新时间：2015 年 9 月 16 日，http://www.wassenaar.org/index.html。

82. 联合国，《在国际安全背景下信息和电信领域发展的政府专家组报告》，A/65/201 和 A/68/98（2015 年 6 月 26 日）。

83. 白宫新闻秘书办公室，《情况说明书：习近平主席访美》，2015 年 9 月 25 日，https://www.whitehouse.gov/the-press-of-fice/2015/09/25/fact-sheet-president- xi-jinpings-state-visit-united-states。

84. 多伦多大学，《2015 年金砖国家领导人第七次会晤乌法宣言》，金砖国家信息中心，2015 年 7 月 9 日，http://www.brics.utoronto.ca/ docs/150709-ufa-declaration_en.html。

85. 联合国大会，《2015 年 1 月 9 日中国、哈萨克斯坦、吉尔吉斯斯坦、俄罗斯、塔吉克斯坦和乌兹别克斯坦常驻代表致联合国秘书长的一封信》，《在国际安全的背景下发展信息和电信 领 域》，A/69/723（2015 年 1 月 13 日），http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/ PDF/N1501402.pdf?OpenElement。

86. 梅丽莎·海瑟薇（Melissa Hathaway），《全球网络管理委员会的讨论文件》，（文件于 2014 年 5 月 27 日在瑞典斯德哥尔摩发布）。

87. 美洲开发银行，《美洲开发银行和美洲国家组织携手推进拉美和加勒比地区的网络安全》，2014 年 10 月 22 日，http://www.iadb.org/en/news/ news-releases/2014-10-22/cybersecurity-workshop-for-latin-america，10957.html。

88. 杜桑·那拉提尔（Dusan Navratil），捷克共和国国防局局长和罗伯特·卡霍夫（Robert Kahofer），特别助理，《2015 年捷克网络 - 全国技术网络安全演习》， （由梅丽莎·海瑟薇在华盛顿特区采访，2015 年 10 月）。以及罗文·阿扎尔（Rueuven Azar），使团副团长和艾维塔尔·马塔尼亚（Eviatar Matania），国家网络局局长（由梅丽莎·海瑟薇在美国马里兰州罗克维尔采访，2015 年 6 月 2 日）。

89. 克莱格·霍尔（Craig L. Hall），美国驻印度加尔各答大使馆，（由梅丽莎·海瑟薇在印度加尔各答采访，2015 年 9 月 23 日）。

90. 不同的网络战会有不同的网络冲突。网络战是完全技术层面的，但原则上可完全在网络中进行。一般而言，网络战是网络冲突的一部分。“网络冲突指的是那些攻击性和破坏性的国家重大冲突，而决定冲突结果的重大事件，离不开位于决定性进程中关键点的网络（指网络技术）机制”。克里斯·戴姆恰克（Chris Demchak），《应变能力、破坏和“网络威斯特法利亚”（Cyber Westphalia）：网络冲突世界中的国家安全选择》，出自《保卫网络空间：国家安全新领域》，尼古拉斯·彭斯（Nicholas Burns）和乔纳森·普莱斯（Jonathon Price）编辑，（华盛顿特区：阿

斯彭研究所，2012 年）。

91. 克里斯托弗·布朗克（Christopher Bronk），《针对沙特阿拉伯国家石油公司的网络袭击》，《生存》（Survival）杂志第 55 期（2013 年 4-5 月） 81-96。

92. 梅丽莎·海瑟薇（Melissa Hathaway）和约翰·斯图尔特（John Stuart），《网络四特色：把控我们的网络未来》，《乔治城国际事务杂志》，（2014 年 7 月 25 日）。

93. 罗伯特·李（Robert M. Lee）、迈克尔·安森特（Michael J. Assante）和蒂姆·康威（Tim Conway），《德国钢铁厂网络袭击》，《工业控制系统》（2014 年 12 月 30 日）。

94.《索尼影业遭黑客攻击事件真相》，《趋势科技》，2014 年 12 月 22 日，http://blog.trendmicro.com/reali- ty-sony-pictures-breach/，肖恩·菲茨杰拉德（Sean FitzGerald），《关于索尼影业泄密风波的一切》，《秃鹫》，2014 年 12 月 22 日，http://www.vulture.com/2014/12/everything-sony-leaks-scan- dal.html#，以及《索尼黑客事件爆出，员工医疗、薪酬数据或将泄露》，Krebson Security 安全博客，2014 年 12 月 2 日，http://krebsonsecurity.com/2014/12/sony-breach-may-have-ex- posed-employee-healthcare-salary-data/。

95. 珍妮弗·德弗莱斯（Jennifer Valentino-Devries）和丹尼·亚德龙（Danny Yadron），《世界网络力量目录》，《华尔街日报》，2015 年 10 月 11 日，http://www.wsj.com/ articles/cataloging-the-worlds-cyber- forces-1444610710 and United Nations，联合国大会，《在国际安全的背景下发展信息和电信领域：致秘书长的报告》，（2015 年 7 月 22 日）http://www.un.org/ga/search/view_doc.asp?symbol=A/70/172。

96. 詹姆斯·路易斯（James Lewis）和卡崔娜·蒂姆林（Katrina Timlin），《2011 年网络安全和网络战：对国家政策和组织进行初步评估》，联合国裁军研究所（UNIDIR），联合国裁军研究所资源和战略和国际研究中心（2011）:3。

97. 国防部，《国防部网络战略》，（2015 年 4 月）：7-8。

98. 俄罗斯总统，《俄罗斯联邦的军事政策》，俄罗斯政府（2014）汤姆斯·摩尔（Thomas Moore）翻译，https:// www.scribd.com/doc/251695098/ Russia-s-2014-Military-Doctrine。

99. 俄罗斯国防部，《俄罗斯武装力量在信息领域内活动的概念图》（2011 年），美国国务院翻译。

100.《新的信息安全政策指出网络不稳定带来的危险，》《俄罗斯新闻》，2015 年 9 月 10 日，http://en.news-4-u.ru/the-new-doctrine-of-information-se- curity-pointed-out-the-danger-of-de- stabilization-via-the-internet.html。

101. 巴西国防部最近也通过设立三军网络司令部（ComDCiber），引导巴西武装部队提高国家的网络防御。虽然三军网络司令部包含三军，但军队会起到带头作用。三军网络司令部是基于之前在巴西利亚设立的巴西网络防御中心（NU CDCiber）。参见 eeInigo Guevara，《巴西设立网络司令部》，《简氏防务周刊》，2014 年 11 月 4 日，以及迭戈·坎巴罗（Diego Rafael Canabarro）和斯奥勾·伯恩（Thiago Borne），《巴西和网络战的迷雾》，国家数字管理中心（2013）:5. 关于韩国的网络能力，请参阅：韩国，《国防白皮书》，（2014），57，http://www.mnd.go.kr/ user/mnd_eng/upload/pblictn/PBLICT- NEBOOK_201506161156164570.pdf。

102. 扎卡里·凯克（Zachary Keck），《韩国寻求攻击性网络能力》，《外交家》，2014 年 10 月 11 日，http:// thediplomat.com/2014/10/south-ko- rea-seeks-offensive-cyber-

capabilites/。

103. 了解中国的网络政策，请参阅 :Amy Chang，《战国》，新美国安全中心，（2014 年 12 月）。

104. 国务院新闻办公室，《中国武装力量的多样化运用》白皮书，2013 年 4 月，http://eng.mod.gov.cn/Database/ WhitePapers/ 和习近平，中央军委，《关于切实保障信息安全的意见》，由 Amy Chang 在《战国》一书中部分翻译，新美国安全中心，（2014 年 12 月）：20。

105. 北欧理事会会长，《冰岛网络责任》，（由梅丽莎·海瑟薇与北欧理事会会长及负责国家计算机应急小组的北欧理事会各国使团进行会晤，瑞典斯德哥尔摩，2014 年 11 月 19 日。

106. 内政部，《2015-2016 年冰岛国家网络安全战略：行动计划》，冰岛内政部部长（2015 年 6 月），http://eng.innanrikisraduneyti.is/media/ frettir-2015/Icelandic_National_Cyber_Security_Summary_loka.pdf。

107. 雅各布·卡兹（Yaakov Katz），《安全和防御》，《耶路撒冷邮报》，2010 年 10 月 8 日，出自詹姆斯·路易斯（James Lewis）和卡崔娜·蒂姆林（Katrina Timlin），《2011 年网络安全和网络战：对国家政策和组织进行初步评估》，联合国裁军研究所（UNIDIR），联合国裁军研究所资源和战略和国际研究中心（2011）:14 和《关注技术出口，以色列建立网络司令部》，路透社，2011 年 5 月 18 日，http://www.reu- ters.com/article/2011/05/18/us-israel-se- curity-cyber-idUSTRE74H27H20110518。

108. 米奇·金斯伯格（Mitch Ginsburg），《军方要建立统一的网络部队》，《以色列时代报》，2015 年 6 月 16 日。

109. 迈克尔·赫索格（Michael Herzog），《以色列国防公布新战略》，华盛顿研究所：政策观察 2479 （2015 年 8 月 28 日），http://www.washing- toninstitute.org/policy-analysis/view/ new-idf-strategy-goes-public。

作者简介

梅丽莎·海瑟薇（Melissa Hathaway）是网络政策和网络安全领域的权威专家。她是资深研究员和波托马克政策研究所校务委员会成员，同时还在哈佛肯尼迪学院的贝尔弗尔科学与国际事务研究中心担任资深顾问。她曾效力于两届政府，为奥巴马总统制定《网络政策评估报告》，并为小布什总统主导过国家网络安全综合计划。她曾制定一套独特的方法论，用来评估和测量面对特定网络安全风险的准备程度，被称为“网络就绪报告”。她就影响公司和国家的网络安全事务定期发表论文。她的大多数文章可在以下网站上找到：http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html。

克里斯·德姆查克（Chris Demchak）是波托马克政策研究所《网络就绪报告》项目的课题专家。她的研究领域包括数字应变能力、网络冲突以及网络空间的结构和

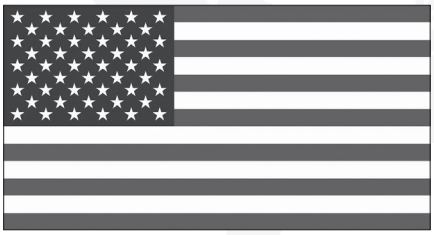
风险。她曾设计一款数字化的组织模型 Atrium，帮助大企业应对、解决系统中的突发问题。她还著有《破坏和应变能力之战：网络冲突、权力和国家安全》。

强森·科本（Jason Kerben）是波托马克政策研究所“网络就绪报告”项目的课题专家。他曾在多个部门和机构中担任信息安全和网络安全方面的资深顾问。他尤其专注于影响组织任务的法律和监管制度。他开发了一些方法论来评估和管理网络安全风险，为大量具体网络安全活动（包括管理信息和通讯技术的国际规则、身份和访问管理、持续诊断和缓解措施以及网络保险）提供建议。

詹妮弗·麦卡阿德（Jennifer McArdle）是波托马克政策研究所革命性科学思想中心的研究员，在位于罗得岛州纽波特的沙尔瓦瑞金纳大学担任助理教授。她的学术研究集中在网络冲突、升级管理和军事创新方面。她目前在伦敦国王学院战争研究院攻读博士。

弗朗西斯卡·斯比达利艾里斯（Francesca Spidalieriis）是波托马克政策研究所“网络就绪报告”项目的课题专家。她同时在沙尔瓦·瑞金纳大学佩尔中心担任网络领导力资深研究员。她的学术研究和发表刊物主要集中在网络领导力发展、网络风险管理、网络教育和意识以及网络安全人力发展。她最近发表了一篇题为《美国在网络安全方面的状态》的报告，将《网络就绪报告 1.0》应用于美国各州。

美国网络就绪度报告



国家人口	3.2142 亿
人口增长率	0.8%
按市价计算的 GDP（当前美元）	17.947 万亿美元
GDP 增长率	2.4%
引入互联网的年份	1969
国家网络安全战略	2003 年、2008 年
互联网域名	.com,.gov, .org, .edu, .mil, .net, .us
固定宽带用户渗透率	30.4%
移动宽带用户渗透率	97.9%
移动手机用户渗透率	98.4%

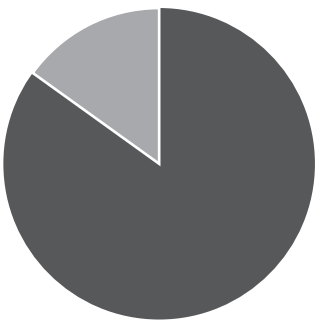
ICT 发展与网络联接指数排名

国际电信联盟（ITU） 通信技术发展指数排名	15	世界经济论坛（WEF） 网络就绪指数	7

来源：世界银行（2015）、ITU（2015）、NRI（2015）、互联网社会

概述

1969 年 10 月 29 日，在美国政府资助、国防部研究计划署（ARPA）主导的一个研究项目中，实现了首次互联网传输。该项目旨在改善科学家与计算机之间的交互，并组建一张覆盖全国的网络，使人们即使相隔很远，也可以随时随地进行交互。阿帕网（ARPANET）采用分组交换技术，为美国总统、军方以及国家安全机构提供了一种可靠的新型通信、指挥和控制系统。[1] 如今，ICT 及互联网服务已成为美国经济增长的主要引擎，ICT 驱动的货物出口及服务出口分别占总出口额的 9% 和 24.3%。[2] 美国互联网渗透率高达 87% 以上，是高度数字化的国家。然而，政府也发现，城市和农村地区存在巨大的“数字鸿沟”。消除这一鸿沟，为更多民众提供能负担得起的高速宽带是提升生产力、增加经济机会的关键。[3]2010 年，联邦通信委员会（FCC）向政府提交了“连接美国”国家宽带计划，计划在 2020 年之前为一亿家庭提供负担得起的高速互联网。[4]



美国互联网渗透率：87.4%

然而，距离该计划推出已经 6 年过去了，美国宽带渗透率并未达到预期目标。随着数字产品的不断增加以及物联网（IoT）的快速渗透（两者都需要更大带宽支持），FCC 决定通过提高无线频谱的利用率，重点提升美国的 ICT 水平。[5]2016 年，FCC 改变了策略，决定将更多政府所有的频谱拿出来拍卖，以缓解无线网络的频谱需求。FCC 目前正计划大幅扩充可用频谱资源，彻底改变美国无线基础设施的架构，为 5G 无线服务和应用的发展打下基础。[6]

美国政府对 ICT 行业的态度基本上是任其自由发展，对很多其他行业也持相同态度，这样做有助于避免潜在的利益冲突问题。关于美国数字经济议程，目前只有商务部长对该议程四大重点（促进自由、开放网络的建设；推进网络诚信；确保宽带入网；

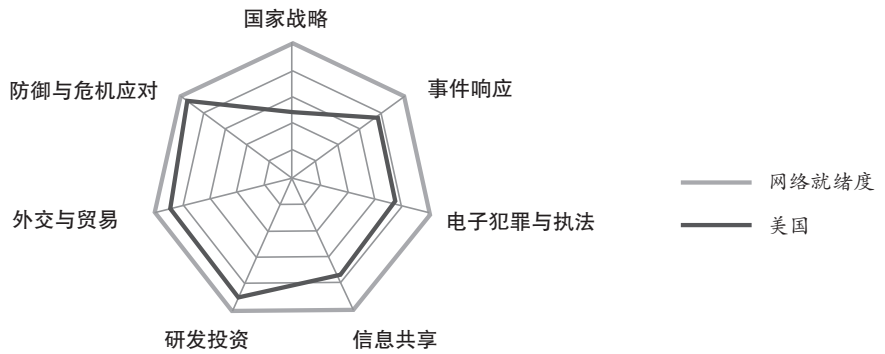
鼓励创新）的公开描述，还没有出台详细的官方文件。[7] 但我们可以从以下三个政策举措中看出美国数字经济议程背后的一些逻辑。首先，商务部发布了《网络经济中的商业数据隐私与创新》（又名“绿皮书”），强调在减少数字商务壁垒的同时，应加强数据隐私及知识产权保护，增强网络安全，确保信息跨境流动自由。[8] 其次是白宫发布的《大数据：抓住机遇、保存价值》报告（又名“Podesta 报告”）。该报告主要讨论了新兴技术、IoT、数据聚合对经济、政府和社会的变革作用，并指出政府也应重视其中的个人隐私问题。[9] 第三，美国政府发起跨大西洋贸易投资协定（TTIP）及跨太平洋合作伙伴协定（TPP），试图通过贸易维持经济健康发展。这两大协定都提倡货物、服务、数据及资本的自由流动，以助推经济发展，同时将 ICT 置于谈判国经济发展战略的重要位置。美国贸易代表办公室（USTR）指出，美国希望达成以下几方面的目标：打击非公平贸易行为、消除数字贸易壁垒、遏制贸易保护主义抬头、实施数据或隐私保护、打击商业机密盗窃行为、加强网络安全合作，确保全球经济持续健康发展。在 TPP 谈判过程中，USTR 发布了“数字 24 条”（Digital 2 Dozen），称维持互联网的自由度和开放性有助于推动数字经济跨境贸易。[10] 上述三大举措大致描绘了美国数字议程的概貌。

奥巴马在上任之初即认识到“网络威胁是美国目前面临的最严重的经济和国家安全挑战。”据估计，美国每年由于网络攻击造成的经济和知识产权损失高达 3000 亿美元（超过 GDP 的 1%），企业平均损失 1500 万美元。[11] 此外，消费者对网络安全的担忧也对数字经济的前景带来了越来越大的影响。近期研究表明，美国有一半的网民出于隐私和安全考虑，决定不进行在线金融交易或是开展电子商务，或在社交网站发帖。[12]

为什么会这样？有三起前所未有的重大国家安全事件引发了民众对网络安全的关注。这损害了美国在技术方面长期保持的领先和中立形象，对美国 ICT 巨头也产生了负面影响，进而严重阻碍美国数字经济发展。事件一：2010 年，美国陆军士兵 Chelsea Manning 涉嫌向“维基解密”网站提供海量机密情报，包括军事和外交文件，将美国外交政策公诸于众，严重影响美国的公开立场。事件二：2013 年，爱德华·斯诺登将美国国家安全局（NSA）秘密监听项目的细节披露，引发了全世界对该项目意图的质疑，美国因此陷入严重的信任危机。事件三：美国联邦人士管理局（OPM）遭到黑客攻击，导致 2400 万政府工作人员个人信息泄露，包括敏感信息，其中不乏美国现任及未来政策制定者。在这三起事件及很多其他重大安全事件发生后，奥巴马在 2015 年的讲话中表示：“恶意网络攻击行为……对美国国家安全、外交政策和经济造成不同寻常的严重威胁。”[13]

从政策和舆论来看，美国政府有意加强美国的网络安全态势，但后续网络安全战略和政策的执行是否能落到实处仍是个未知数。相比经济领域的战略重点，网络安全问题在政府的工作中往往没那么紧急和重要。此外，还有很多其他一系列不和谐因素导致政府无法聚焦网络安全问题。例如，基础设施落后，急需升级，将安全和风险抵御能力嵌入各个环节；互联的企业越来越频繁地遭遇知识产权被窃，甚至导致数字服务被迫中断；美国政府及其盟友的关系以及美国政府与业界（硅谷、西雅图、波士顿等）的关系不断恶化；专业安全人才匮乏；立法滞后，跟不上互联网的发展速度；多个政府部门之间的网络安全职责存在重叠；没有明确的主导部门等。

本报告采用网络就绪度指数 2.0（CRI 2.0）为框架，评估了美国应对网络安全风险的准备度，并制定了一份行动蓝图，帮助美国进一步了解其互联网基础设施之间的依赖性及脆弱性。基于对美国当前网络安全形势的分析，本报告还探讨了美国需要发展哪些能力，才能确保数字化顺利推进。



美国网络就绪度评估（2016）

本报告采用 CRI 2.0 方法论，从七大维度（国家战略、事件响应、电子犯罪与执法、信息共享、研发投资、外交与贸易、防护与危机应对）对美国的网络安全工作及能力进行了全面评估。

国家战略

美国出台了一系列国家网络安全政策和法规。[14] 1998 年，美国总统签发《关键基础设施保护》总统令（PDD–63），商务部发布《绿皮书》[15]，首次提出网络空间安全和经济政策框架。2003 年，PDD–63 进行了修订并纳入《国家网络安全战略》及国土安全《基础设施识别、优先级排序和保护》总统令（HSPD 7）。两者都重点推出

了减少网络空间安全威胁的计划。[16] 同年，美国国土安全部成立，负责协调各政府部门的网络安全事件应对工作。2008 年，国家网络安全综合计划（CNCI）随第 54 号国家安全总统令及第 23 号国土安全总统令（NSPD–54/HSPD–23）发布。CNCI 旨在实现三大目标：设立第一道防线，应对当前最迫切的安全威胁；制定应对安全威胁的策略；加强未来网络安全环境建设。[17] 此外，CNCI 还列举了一系列政府出资项目，为推动国家安全工作有效开展奠定了基础。

2009 年，白宫公布了《网络空间政策评估：保障可信赖的和可迅速恢复的信息和通信基础设施》报告，以强化 CNCI 计划。该报告列出了短期内的重点工作，包括：明确各政府部门的网络安全职责和分工，制订网络事件应对计划，发起国民网络安全意识提升项目，制定研发框架，任命一名国家安全协调员，直接向总统汇报。[18]《网络空间政策评估》报告给出了 25 条执行建议，包括如何降低网络安全风险、提升网络空间的风险应对能力。

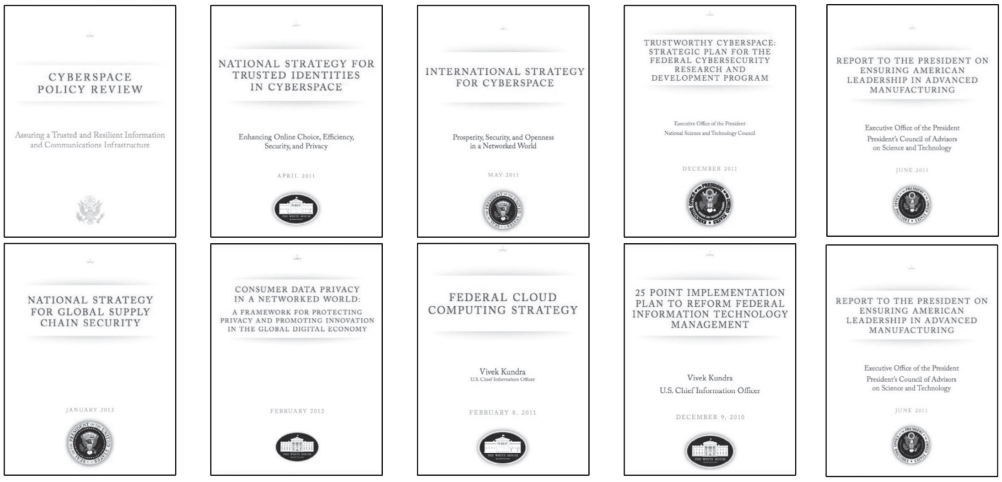
美国出台了一系列国家网络安全政策和法规。

随后，美国政府又持续发布了多项网络安全计划和举措，但重点有所不同。几年后，美国政府再次发布《网络空间政策评估报告》，重新确定了五大领域的战略重点，与国际网络空间战略以及斯诺登泄密事件相呼应。这五大重点包括：保护关键基础设施，保护联邦网络安全，提升事件通知及响应能力，开展国际合作，打造未来网络安全环境。这些战略也被纳入了各项国家政策中。例如，2013 年 2 月，第 13636 号行政令“提升关键基础设施网络安全”要求国土安全部识别处于高风险状态的关键基础设施。此类基础设施一旦发生网络安全事故，就会对某个区域，甚至全国带来巨大的公共卫生安全、经济安全和安全风险。[19] 该政策还从关键服务、基础设施、企业的角度，识别了数十个面临安全风险的实体，他们亟需提升自身的安全状况。同时期发布的第 21 条“关键基础设施的安全和韧性”总统政策令对政府部门的网络安全职能进行了澄清，以加强关键基础设施安全和韧性。[20]2016 年 7 月，第 41 条“美国网络事件协调”总统令颁布了联邦政府网络安全事件应对原则，包括政府部门和私营行业发生的网络安全事件。[21] 然而，这些政策文件本质上都没识别能够主导网络安全管理的政府部门，而是卷入多个政府部门，任命多位官员负责政策制定和危机响应。

OPM 信息泄露事件发生后，美国政府再次转移了工作重心，开始重点关注联邦政府的网络安全。白宫专门发布了相关指南，指导政府部门开展以下网络安全工作：重点识别并保护重要信息及资产，及时发现并快速应对网络事件，确保网络安全事件

发生后能迅速恢复并及时总结和利用经验教训，招聘并保留高素质网络安全人才，为联邦政府所用，促进现有和新兴技术的高效获取和部署。[22]

该指南正式纳入 2015 年发布的《网络安全战略与执行计划》（CSIP）中，重点保障政府的网络及数据库安全。该计划旨在制定强大的机制，并通过一系列举措，在指定时间内，快速提升联邦政府应对网络安全的能力。[23] 尽管该计划列出了 18 个月内需要执行的 50 多条行动计划，但没有明确监督机制，因此，很多列出的计划都未能落地。于是，2016 年 2 月，白宫发又发布了另一项“网络安全国家行动计划”（CNAP），明确了两大网络安全提升计划：第一，淘汰现有信息技术系统，升级联邦政府网络软硬件，提升安全性和韧性。第二，通过立法，强制要求联邦政府部门采用持续诊断与缓解（CDM）工具以及其他管理服务，以降低联邦政府面临的网络安全风险。



该计划还提倡任命一位白宫信息安全官（CISO），统筹联邦各机构的网络安全工作及政府计算机系统升级工作。然而，这些计划的实施需要大量资金支持，美国国会尚未通过总统的提议，很有可能要等到下一届政府上台。[24]

为支持经济和创新目标，美国还需制定明确的网络安全战略。目前，针对 ICT 转型和 IoT 普及伴随的机会和风险的讨论还很少。尽管已任命专人统筹联邦政府的网络安全工作，但在实际操作中，美国政府仍有多人在统筹、监督和管理网络安全工作，包括白宫网络安全协调员、联邦首席信息官、美国贸易代表、总统科学顾问以及总统国家经济委员会、国家安全委员会和内阁的多位成员。

事件响应

1998 年，美国首次意识到需要建设国家网络事件响应能力，因此发布了关于保护国家关键基础设施的第 63 号总统令（PDD–63），建立国家基础设施保护中心（NIPC）。NIPC 隶属于联邦调查局，负责推动并协调联邦政府进行事件响应，规避攻击，调查威胁并监控整改行动。 2003 年，NIPC 的职责转移至美国国土安全部。目前，该职责由国家网络安全和通信综合中心（NCCIC）承担。NCCIC 负责统筹美国联邦政府、州政府、地方政府以及区域、国际和私营行业之间的网络事件响应工作。NCCIC 负责与私营行业、民间团体、执法机构、情报机构、国防机构以及跨国组织共同提升意识，协调网络安全事件响应、规避和恢复活动，致力于保护联邦公民机构的安全。[25]

2000 年早期，美国国会在美国总务署设立了联邦计算机事件响应中心（FedCIRC），统筹各联邦机构之间的协调和信息共享。[26]FedCIRC 是美国第一个政府计算机应急响应小组（CERT）。2003 年国土安全部成立后，FedCIRC 的职责转移至国土安全部，并改名为美国计算机应急响应小组（US–CERT），职责也日益扩充。目前，NCCIC 负责统筹网络信息共享，主动管理国家网络威胁。

NCCIC 负责协调网络信息共享，主动管理国家网络风险。

US–CERT 目前隶属于 NCCIC，与私营行业关键基础设施所有者和运营者、学术界、联邦机构、信息共享与分析中心、州和地方合作伙伴、国内和国际组织合作，收集网络事件信息，对网络事件进行分类，并积极应对网络事件；为信息系统运营者提供技术援助；及时发布当前和潜在安全威胁及与漏洞相关的实用信息。此外，US–CERT 还负责运营国家网络空间安全保护系统（NCPS），向非国家安全联邦部门和机构提供入侵侦测和防御服务。

根据国土安全部 2008 年发布的全国响应框架（NRF）（后于 2013 年刷新），美国 2010 年起草了《国家网络事件响应计划》（NCIRP），但 NCIRP 并未涵盖网络事件。NRF 明确了美国应对自然灾害和其他灾难性事件的流程以及政府高层应如何构建可持续政府。因此，NCIRP 旨在构建组织角色、职责和行动框架，做好准备应对国家层面的网络事件并协调恢复工作。[27]NCIRP 还将不同的政策和理论整合成针对网络空间的订制化战略方案，为运作实施、规划和准备活动提供支持，并指导短期恢复工作。然而，NCIRP 设计的初衷是尽量减少私营行业的参与度。现在，六年过去了，NCIRP 还只是初稿。美国 2015 年发布的《网络安全法》要求国土安全部将 NRF 与 NCIRP 对齐，

并评估输出风险指引计划的可行性，以更好地应对影响关键基础设施的网络事件。[28]

2016 年 7 月发布的第 41 号总统令《美国网络安全事件协同方案》确定了联邦政府在应对网络事件时应遵循的原则，不论网络事件是涉及政府机构还是私营行业实体。[29] 此外，该方案从三个方面明确了各联邦机构在应对威胁和帮助受害者恢复的过程中需承担的职责。首先，面对来源不明的威胁或攻击，由联邦调查局牵头的国家网络情报联合特遣部队（NCIJTF）应立即采取响应行动。其次，国土安全部下属的国家网络安全和通信综合中心（NCCIC）负责协调资源，帮助受害者尽快恢复，并通过网络找出攻击者。再次，国家情报总监管辖的网络威胁情报整合中心（CTIIC）是联邦主导机构，负责提供情报和其他活动支持，并协调资源确定打击和遏制威胁的策略。尽管明确各机构在帮助受害人过程中的职责非常重要，但仅明确职责还远远不够，因为这还无法有效应对不断增长的网络安全事件和求助需求。

在打击现实世界威胁活动的同时，美国还定期在国内和国际上开展网络安全应急演习，这不仅测试了事件响应操作能力，还模拟了各国之间的合作。例如，国土安全部每两年举行一次“网络风暴”实战演习，试图加强政府和私营企业的网络就绪水平。[30]2016 年的“网络风暴”演习覆盖了 16 个州、11 个国家和 14 个联邦机构。此外，美国能源部主导地方、州和国家层面的网络就绪演习，如北美电力可靠性协会的电网安全演练（GridEx）。2015 年 11 月开展的 GridEx 是电力行业最大的危机应对演习，超过 350 个政府和行业组织以及 4,500 名人员参与了演习，为测试和制订国家响应计划献计献策。[31] 此外，美国财政部还与金融事业部协调委员会一起举办网络安全相关的研讨会和演习，模拟网络安全事件，并识别公共和私营行业合作应对网络安全事件过程中面临的关键挑战。自 9・11 恐怖袭击事件后，美国财政部已联合众多金融机构在多个地区开展网络安全演习。欧洲防务局（EDA）和北大西洋公约组织（NATO）联合举办了区域内的网络危机管理演习，目的在于加强成员国的网络事件响应能力，了解跨境依赖关系。美国也参与了这些演习。[32]

美国还定期在国内和国际上开展网络安全应急演习，不仅测试了事件响应操作能力，还模拟了各国之间的合作。

美国国家情报总监办公室（ODNI）向国会提交了年度《美国情报界全球威胁评估报告》，[33] 指出过去四年间网络威胁是美国面临的最严峻的威胁。国家情报委员会（NIC）通常会在美国大选后发布《全球趋势报告》，总结不安全网络带来的威胁。美国国防部、国土安全部、美国计算机应急响应小组（US-CERT）、国家网络感知系统（NCAS）等其他政府部门和机构也发布了很多面向特定行业的深度评估报告。

电子犯罪和执法

美国政府认识到网络犯罪的严重程度及其对公共和私营行业的影响，并采取了一系列措施来应对这类网络威胁。

自 2006 年加入欧盟理事会《网络犯罪公约》后，美国开始推动实体法和程序法在网络犯罪方面进行国际协调。

网络犯罪是指利用互联网上自由流通的商品、服务、数据和资金来实施犯罪。为打击这类犯罪活动，2006 年美国加入欧盟理事会《网络犯罪公约》（也称《布达佩斯公约》），成为第 16 个成员。自 2007 年《布达佩斯公约》生效以来，美国通过七国集团的全天候联络人国际网络创建了一个非正式的数据保存和信息共享渠道，并通过建设捐助伙伴关系向发展中国家提供援助，推动实体法和程序法在网络犯罪方面进行国际协调。[34] 美国执法机构也与众多伙伴国家合作抓捕并引渡在美国或第三方国家被起诉的网络犯罪分子。

2009 年，美国发布《网络空间政策评估报告》，指出 80 多部法律需要更新，以适应互联网和数字时代的要求。其中，至少有 20 部法律是实现政府任务和满足私营行业信息和安全需要的关键。自 2009 年以来，每期国会都会引入数十个网络安全法律提案，但只有少部分能获得两党的支持，最终成为法律。比较典型的例子有 2015 年的《网络安全法》，后被纳入《2016 年度综合拨款法案》。《网络安全法》确定了政府与自愿加入该计划的企业之间的网络威胁信息共享流程。[35] 该法律中的部分内容旨在强化美国司法部与联邦贸易委员会 2014 年联合发布的一项政策。这项政策规定在不违反反垄断法的情况下，竞争对手之间可以共享网络安全信息，[36] 但这并不能完全消除反垄断（市场共谋）方面的担忧。因此，《网络安全法》针对特定类型的网络安全信息共享设立了责任保护条款。美国还需修订很多法律，让执法机构和广泛的安全团体能更好地保护美国并与其他国家合作以减少犯罪活动。

2016 年 6 月，来自民主党和共和党的两位极具影响力的参议员宣布组建两党“参议员网络核心小组”。这为全面应对网络安全问题提供了一个良好的平台，让参议员和参议院的其他人员实时了解主要的网络安全政策和法律事务。该核心小组将重点关注网络犯罪对国家安全和经济的影响，以及如何防止犯罪分子利用技术逃脱法律制裁。[37] 早在 2011 年，众议院也组建了类似的小组，不过只涉及共和党。共和党领导人组建了任务小组，来审视各委员会职责范围内的网络安全问题。该小组认为至少有 16 部法律需要改革，并提出了一系列综合建议。[38]

早在 2008 年，美国前总统布什签署《国家网络安全综合计划》，认为美国司法部和联邦调查局应“主导美国网络犯罪的调查和起诉工作”。由联邦调查局主导的国家网络情报联合特遣部队（NCIJTF）作为统一接口，负责协调网络威胁的调查工作。NCIJTF 作为跨机构特遣部队，推动美国情报机构和联邦执法机构开展协作并联合开展行动，共同打击利用关键基础设施控制系统漏洞的网络恐怖分子、窃取知识产权和商业秘密的恶意国家、窃取钱财或身份信息以获取经济利益的犯罪分子、网络敲诈勒索行为、非法攻击企业和政府服务机构的黑客活动分子以及偷窃和实施破坏的内部人士。2016 年 2 月，美国司法部（包括联邦调查局）增加了 23% 的网络安全活动经费，以提升自身能力，更好地发现、打击和抓捕恶意网络攻击者。[39]

联邦调查局也设立了专门的网络部（CyD），参与 NCIJTF 的工作，并协调在美国的 56 个办事处经过特别训练的网络小组。每个办事处都配有特工人员和分析师，负责调查计算机入侵、知识产权和个人信息窃取、儿童色情和剥削以及网络欺诈等犯罪行为。根据调查结果，美国有力地打击了网络僵尸行动，起诉国际犯罪团伙，并积极分析恶意软件的最新趋势。网络部通过众多机制与国际伙伴合作，例如：推出网络和法务专员方案；在网络部总部成立国际网络犯罪协调机构；在位于匹兹堡的美国国家网络执法师培训联盟（NCFTA）推出国际实习计划；开展双边或多边调查并在国际刑警组织和欧洲刑警组织的国际网络中心担任相关职位。

美国特勤局负责调查电子和金融犯罪，并在国内和国际上建立打击电子犯罪特别行动组，重点负责识别和定位网络入侵、银行诈骗、数据泄密和其他计算机相关的国际网络犯罪分子。特勤局的网络情报科直接帮助逮捕了跨国网络罪犯，这些罪犯分子盗窃数亿个信用卡号码，给金融和零售机构带来约 6 亿美元的损失。[40] 此外，特勤局还负责运营国家计算机取证机构，该机构向执法官员、检察官和法官提供网络培训和信息，打击网络犯罪。[41]

非传统的执法政府机构也加入了打击网络犯罪的行列。例如，2013 年，美国联邦通信委员会发起了一项自愿计划，修复僵尸网络。这项计划参考了澳大利亚的自愿原则，从参与度上看取得了不同程度的成功。该计划旨在提高互联网服务提供商对《阻碍指南》（遵从守则面临哪些阻碍）”的认识，并鼓励大家使用该指南，在策划和评估僵尸网络补救工作中参考该指南和《僵尸网络评估指南》[42]。该计划包括试点研究来收集应对僵尸网络活动的趋势和经验教训，并收集僵尸网络修复工作衡量指标的相关信息。[43] 美国目前仍是全球计算机感染僵尸网络数量最多的国家，有着全球最多的直接控制僵尸网络感染的服务器。[44] 大量的计算机被感染，催生了大量的非法活动。

这不禁让人怀疑美国致力于打击网络犯罪的承诺，美国曾承诺其不会成为犯罪活动的发源地，且不会将这些犯罪活动演变成跨国犯罪。.

美国积极参与国际执法工作。美国联邦调查局网络部在伦敦、堪培拉、渥太华、海牙、布加勒斯特、基辅和塔林设立了长期网络法务专员岗位（ALAT）；在东京、斯德哥尔摩、特拉维夫、布拉格和巴西利亚设立了临时 ALAT 岗位。此外，网络部还会向布鲁塞尔、索非亚、巴黎、首尔、柏林及法兰克福、罗马和贝尔格莱德等地派遣长期网络 ALAT。[45] 网络 ALAT 被派往国外执法机构或情报机构，推动信息共享，促进美国与其他国家之间的调查合作，并改善与外国合作伙伴的关系。未来几年，网络部还将继续推动协作并建立广泛的合作伙伴关系。

此外，美国国务院与司法部和国土安全部合作，打击跨国网络犯罪。例如，美国国务院建立打击跨国有组织犯罪奖励计划，向提供有用信息的犯罪举报人提供奖励，帮助执法机构逮捕或起诉刑事组织的嫌疑成员和领导人。[46]

虽然目前很多项目都致力于培养精通网络法律和网络犯罪相关的律师，但众多美国政府官员认为具备专业知识起诉网络犯罪的执法专业人员仍然匮乏。

美国联邦调查局网络部在伦敦、堪培拉、渥太华、海牙、布加勒斯特、基辅和塔林设立了长期网络法务专员岗位（ALAT）。

一些能力建设方案和工作停滞不前。近期提交的《加大州和地方政府打击网络犯罪力度》法案如果获得通过，将授权国家计算机取证机构培养州和地方执法人员、检察官和法官，帮助他们更好地调查网络电子犯罪，利用计算机和移动终端进行取证，应对网络入侵调查。然而，该法案尚未获得两党的支持，在本届国会可能也不会有什么进展。目前，很多能力建设计划未获得授权和资金支持，新法律尚未出台或更新，能力建设工作将停滞不前。[47]

信息共享

直到 20 世纪 90 年代后期，美国政府才意识到信息共享的重要性，随后将其纳入《关键基础设施保护》总统令（PDD–63）。根据这一政策指令，为保护关键基础设施，必须进行信息共享，并成立信息共享与分析中心（ISAC）。PDD–63 要求所有关键基础设施领域进行特定信息共享，了解该领域的漏洞和面临的威胁。拥有 ISAC 的基础设施领域还可受益于中心提供的运作服务。例如，金融服务信息共享和分析中心（FS–ISAC）可协助金融领域探测、预防并应对网络安全事件和诈骗活动。[48]FS–ISAC 还与金融服务提供商、商业安全公司、联邦及全国性政府机构、州政府机构和地方政

府机构、执法机关及其他可信赖组织建立密切联系，为全球企业成员提供可靠及时的网络威胁预警和其他关键信息。FS–ISAC 还根据不同的交通信号灯协议（TLP）为受众提供定制化信息。2012 至 2013 年间，美国几大银行遭到网络攻击。通过向银行业提供实时共享信息，FS–ISAC 帮助这些公司预测并防御网络攻击。目前，FS–ISAC 正向英国和欧洲拓展其威胁信息共享机制。

过去 20 年来，美国政府始终关注信息共享，在多项政策中反复强调这一点。最近，政府还发布了两项总统行政命令：2013 年 2 月签发第 13636 号行政命令——《增强关键基础设施网络安全》；2015 年 2 月签发第 13691 号行政命令（EO 13691）——《加强私营部门网络安全信息共享》。这些文件要求政府与私营部门加强网络安全威胁信息共享，提高及时性和质量，促进行业内外进行更密切的协作并分析信息。EO 13691 鼓励私营部门通过信息共享和分析组织（ISAO）进行协作，使 ISAO 成为私营部门之间、私营部门与政府共享关键网络安全信息的枢纽。[49] 该行政命令还要求国土安全部与信息共享组织达成协议，加强 ISAO 与联邦政府的协作、简化机制，从而使 NCCIC 与 ISAO 达成信息共享协议。EO 13691 还授权国土安全部与其他联邦部门审批信息共享分类协议，拉通私营部门企业，确保它们获得不同类别的网络安全威胁信息。该命令还提出一系列志愿标准和隐私保护方针，如《公平信息处理条例》，以加强隐私保护和公民自由保障。

国土安全部持续通过 NCICC 与私营部门增进合作，制定更高效的手段，为私营部门个人授予安全许可，应对信息共享过程中面临的挑战：缺乏及时、可操作的可信信息；信息共享平台运作成本过高；很多信息仍为机密或由非政府部门独有；对《信息自由法》的担忧（尤其在处理敏感私有信息和网络安全漏洞时）；隐私保护与公民自由问题；企业需承担法律责任；以及进一步努力面临的困难。

2015 年年末，美国发布《网络安全法》，为自愿与联邦政府和其他公司分享或获取网络威胁信息的组织提供有限法律保护。《网络安全法》为国土安全部规定了下列职责：①了解所有组织分享的网络威胁指标和防御措施；②明确联邦政府了解自动实时共享的指标。在《网络安全信息共享法案》（CISA）指导下，国土安全部开发了指标自动共享（AIS）系统，可快速获取私营部门和政府组织共享的网络威胁指标。国土安全部还鼓励企业与 NCCIC 合作，升级网络设备，实现网络威胁指标自动共享。AIS 项目的目标是，自动向情报组织提供信息，包括联邦部门和机构、私营企业以及 ISAC。然而，目前要实现全面自动共享仍面临挑战。为推动 AIS 系统的广泛应用、满足其需求，美国政府将要求采用国土安全部制定的 STIX、TAXII 或 CybOXIn 协议。

这些协议要求在编码和传播高保真信息时使用规范语言、服务以及信息交换。最近，司法部和国土安全部发布了具体指导方针，协助私营部门组织与联邦政府共享网络威胁指标和防御措施。[50]

国土安全部还努力打造可信环境，促进与私营部门共享网络威胁信息，例如正式签署合作研发协议（CRA–DA）。该协议是网络信息共享与合作计划（CISCP）的一部分。此外，国家网络情报联合特遣部队（NCIJTF）与其他联邦网络中心和部门携手，利用联邦调查局（FBI）的网络保护系统，改善管理网络威胁报告的流程，通知已成为恶意网络活动攻击目标和受害者的企业。借此行动，截至 2015 年 7 月，网络中心制作了 10,000 多份网络威胁报告，发布了 2,000 多次通知[51]。2015 年 2 月，奥巴马总统指导成立了网络威胁情报整合中心（CTIIC），旨在提高政府组织对外国恶意网络威胁的实时态势感知能力。作为国家网络威胁情报中心，CTIIC 是连接各相关政府部门的枢纽，对国家面临的直接网络威胁进行全面情报分析。

国家网络执法师培训联盟（NCFTA）代表着信息共享的另一种模式。NCFTA 是非盈利性组织，负责推动私营行业、学术界及执法机关进行协作，识别、降低、化解复杂的网络威胁。[52] 作为非营利性合作驱动机构，除美国州及地方执法机关和行业代表以外，NCFTA 成员还包括加拿大、澳大利亚、英国、印度、德国、荷兰、乌克兰和立陶宛等国的国际代表。NCFTA 与企业及时、顺畅地交换网络威胁情报，同时还与公共领域、私营领域、执法机关和学术界的主题专家通力合作，缓解网络威胁和诈骗行动造成的影响，收集起诉罪犯的必要证据。

区域层面上，政府在马萨诸塞州波士顿建立了高级网络安全中心（ACSC），关注信息共享计划。与 NCFTA 一样，ACSC 也是非盈利性组织，旨在促进行业、高校与政府组织携手合作，应对最高级网络威胁。该中心每两周举行一次会议，分享主要威胁指标，交流对新兴恶意软件活动的洞察。ACSC 还开展自动信息共享，以便成员互相交流威胁与应对信息，与本地高校和企业共同参与下一代网络安全研发。

国家网络执法师培训联盟推动私营行业、学术界及执法机关进行协作、共享信息。

值得注意的是，其他领域也制定了独特的信息共享模式。首先，FS–ISAC 成立了特殊利益委员会——威胁情报委员会（TIC）。该委员会仅为成员提供平台，共享与网络威胁相关的高度敏感信息。此外，美国八大银行成立了网络防御工作组，联合各自人才、提升防御姿态。工作组的目标是共享更多威胁信息，全方位应对网络攻击，开展作战演习、解决大型银行面临的问题。各行业也主导建立了威胁情报交流组织，如网络威

胁联盟，旨在提高认知，保护组织和客户免遭高级网络威胁。

研发投资

现代互联网起源于美国国防部的一项试验，旨在关联国防部出资的所有研究机构。美国不断利用原始投资打造 ICT 环境。1991 年，在两大事件的影响和指导下，国防部的研发试验应运而生。其中一大事件是美国国家科学院发布了名为《危机四伏的计算机》的报告。报告称，“随着计算机系统的普及和发展，与物理过程的互联性不断增强，但落后的系统设计、系统故障和系统攻击或使社会安全面临威胁。一旦系统设计和使用存在疏忽，系统便可能中断，从而对社会造成危害。”[53] 因此，报告指出，政府必须制订全面可行的计划，切实保护网络基础设施安全。同年，政府还推出了网络和信息技术研究开发计划（NITRD），作为美国信息技术研发（如计算、网络和软件技术等）的主要公共平台。该计划通过协调各部门的研究项目，助力美国保持在网络和信息技术领域的领导者地位，满足联邦政府对先进网络和信息技术的需求，加速先进网络和信息技术的开发和部署。[54]

网络和信息技术研究开发计划（NITRD）通过协调各部门的研发项目，助力美国保持在网络和信息技术领域的领导者地位。

美国科学和技术政策办公室（OSTP）主要负责为总统制定科技政策和编制预算提供建议。网络安全和信息保障研发（CSIA R&D）高级指导小组成立于 2008 年，其主要职责是支撑 CNCI 计划落地。CNCI 的目标之一是开发领先技术，在网络安全方面取得跨越式进展。CNCI 的另一举措是评估各研究项目，确定是否存在重复劳动，以及政府出资的项目是否有益于解决国家面临的关键难题。[55]CNCI 计划是政府的初步尝试之一，旨在对所有保密和公开的研发项目进行分类，并制定相应战略，重新平衡网络安全研发项目，对齐政府当前的工作重点和未来需求。

最近，NITRD 发布《2016 年联邦网络安全研究和发展战略计划》，明确阐述了政府的短期、中期和长期网络安全研发目标。其中短期目标旨在实现科技进步，通过有效的风险管理，引导组织深入了解网络空间的漏洞和威胁，并利用有效的控制工具，识别、评估和应对风险，从而打击对手的非对称优势。中期目标旨在通过建立可持续、安全的系统和运作流程，打击对手的非对称优势。长期目标则侧重于通过实现科技进步，提高对手的成本和风险，减少非法所得，从而阻击恶意网络活动。为此，政府必须具备新的取证能力，快速识别入侵者，并采取行动，保护无辜民众的言论自由和匿名性。

美国联邦政府的研发活动主要由三大机构负责：国防高等研究计划署（DARPA）、

国土安全部高等研究计划署（HS-ARPA）和情报高等研究计划署（I-ARPA）。DARPA 资金充足，推出了一系列聚焦近期需求的研究计划。2011—2013 年间，DARPA 发布了“网络快速通道”（CFT）项目，旨在通过开展低成本、快捷的项目改善网络安全、终端和系统，并为上百个小型网络安全项目提供资金。[56]CFT 鼓励项目执行者识别软件和硬件漏洞，制订解决方案，再由 DARPA 对这些解决方案进行分类，以解决安全问题。面向公众发布解决方案的分类后，许多初创企业应运而生。此外，CFT 项目还鼓励黑客社区申请资金支持。最近，DARPA 资助了一个为期多年的网络超级挑战赛，旨在开发解决方案，实现手动修复补丁和网络防御自动化。DARPA 项目负责人称，“我们希望开发一种自动化系统，能够自主识别未知漏洞、进行漏洞分析，并决定何时安装补丁、如何管理修复过程等，从而大大降低网络修复周期（从一年减少至几分钟或几秒）”。[57] 目前，DARPA 还推出了许多类似项目，包括主动网络防御项目，旨在帮助组织建立同步、实时能力，识别、定义、分析、规避网络威胁与漏洞[58]，以及网络战项目——X 计划，助力国防部建立平台（类似视频游戏），采用类似运动战的方式规划、实施和评估网络战争。[59] 此外，DAPRA 最近还启动了一项名为“攻击检测（Rapid Attack Detection）、隔离（Isolation）、鉴定系统”（RADICS）的计划，旨在开发自动化的电网防御系统，检测电网攻击，隔离关键电力设备，加速恢复电力供应。该系统适用于所有电网。[60]

国土安全部（DHS）自 2003 年起开始资助网络安全项目。2011 年，DHS 将网络安全提上议程，并成立专门部门，聚焦 HS-ARPA 关注的话题。DHS 旨在为网络安全研发项目提供资金，从而将创新想法转变为用于关键基础设施建设的短期解决方案。DHS 项目还为金融服务和能源部门开发了许多身份认证管理、数据隐私、安全协议、与取证相关的可信技术。[61]

I-ARPA 资助的网络安全研究项目包括：网络事件预测、网络参与者行为和文化分析、威胁情报、威胁建模、网络事件编码、网络事件检测等。其中，“网络攻击自动非常规传感器环境（CAUSE）”项目是一项多年计划，目的是在于开发和测试新型自动化技术，大大提高网络攻击的预测和检测能力。[62] 其他项目包括资助技术研发，确保开发安全代码、可信的集成电路及其他计算机网络运行和技术项目。

目前，美国还有几大机构致力于基础和应用网络安全研发。例如，美国国家科学基金会（NSF）推出了“安全与可靠网络空间”（SaTC）计划，拨款 300 万美元用于资助大、中、小型项目；[63] 以及网络服务奖学金项目，为毕业后从事联邦、州、地方或部落政府网络安全工作的学生提供奖学金。[64] 此外，NSA 和 DHS 还共同赞助

了信息安全教育、研究、网络运作和最近成立的网络防御等国家学术卓越中心，以推动信息安全高等教育，消除网络安全技能方面的巨大鸿沟。[65] 美国共有 180 多家机构通过了学术卓越中心认证。在这些机构接受教育的学生可通过国防部信息安全教育奖学金项目和联邦网络服务奖学金项目申请奖学金和补贴。此外，美国国家标准与技术研究院（NIST）还联合政府、学术界和私营企业，共同启动了“国家网络安全教育计划”（NICE），主要聚焦网络安全教育、培训和劳动力发展，提高网络安全专业人才的数量。[66]

尽管政府不断在研发方面加大投入力度，但私营部门仍是美国大多数网络安全创新和投资的主体。亚特兰大、奥斯汀、波士顿、纽约、西雅图和硅谷等地的创新和网络安全中心吸引了大量网络安全风险资本投资，包括防病毒、防垃圾和反黑客软件应用研发。值得注意的是，2013 年，美国 ICT 行业的研发投资高达 1330 亿美元，占总研发投资（3230 亿美元）的 41%。[67] 同年，ICT 行业经济总量占美国 GDP 的 4.6%，同比增长 1%。由于美国经济高度依赖 ICT 行业（包括网络安全研发），因此美国政府非常重视建立和深化与行业的合作伙伴关系。[68] 例如，近期，国防部成立了国防创新试验小组（DIUx），以更加开放的态度接受非常规技术理念和人才，并计划在硅谷和波士顿设立办事处。[69]

亚特兰大、奥斯汀、波士顿、纽约、西雅图和硅谷等地的创新和网络安全中心吸引了大量网络安全风险资本投资。

外交与贸易

2008 年后，国际网络安全开始成为美国联邦政府的头等大事。国家网络安全综合计划（CNCI）包含至少三项国际交往举措，例如，制订长期网络威慑战略和计划、供应链风险管理计划，以及与私营部门的互动计划，以维护基础设施安全，评估竞争环境的长期战略性基础设施和经济需求。[70] 尽管这些举措未面向公众发布，但关键利益相关人之间的合作和互动进一步突出了网络问题在美国外交和贸易方面的重要意义。

2009 年，美国总统奥巴马发布了《美国网络空间政策评估》报告，重申了“在全球化形势下保护美国繁荣和安全”的重要性。2009《美国网络空间政策评估》报告评估了美国的国际交往战略和国际网络安全政策框架建议。2011 年，美国政府发布了网络空间国际战略，总结了国际网络空间行为规范的指导原则，以制定全球通用的统一标准，确保网络稳定性和可靠性，实现多利益相关人共同治理，支持网络安全尽职调查。该战略提出了 7 大主要目标：①制定国际安全标准，建立创新、开放的市场，提振经济；②加强安全性、可靠性和防御能力，维护美国网络基础设施安全；③加强

合作和法治，加大执法力度；④加强军事力量，应对 21 世纪的安全挑战；⑤建立有效、包容的体制，深化网络治理合作；⑥促进安全能力和繁荣建设，助力国际发展；⑦确保基本自由和隐私，提升互联网自由度。[71]

美国政府还得到了来自区域和国际社会的承诺，致力于共同实现国际网络稳定。

2011 年，国防部成立了网络问题协调员办公室（S/CCI），主要负责以下事务：协调国防部的全球网络问题外交互动；作为白宫和联邦政府网络安全机构在国防部的接口人为国防部长和副部长提供网络问题方面的建议；作为公私部门的网络问题接口人协调国防部地方和职能部门的网络安全工作。新成立的办公室还将与负责协调国际通信和信息政策的国防部经济商务司合作，共同解决网络相关问题，包括安全和经济问题、言论自由以及网络信息自由流动等。[72]

2015 年，美国国会通过了一项新的立法，要求国防部展开一系列行动，支撑政府实现网络空间国际战略目标。随后，国防部向国会提交了一份报告，强调国防部在网络安全方面做出的努力，如人员培训，以及提高人们对网络安全空间经济和安全问题的了解。[73] 来自 120 多个使馆的 500 多名外交官员参加了跨部门区域研讨会，接受了互联网和电信政策培训，以妥善应对本地和区域层面的网络问题。[74] 此外，报告还强调了美国政府在这方面的贡献，通过制定和采纳国际网络空间行为准则，采取相应措施，增强国内外对网络安全的信心。

国际层面，美国积极与国际合作伙伴开展网络合作，如巴西、印度、日本、英国以及海湾合作委员会等。2015 年，美国政府与中国主席习近平签订协议，共同打击国家主导的网络间谍活动，防止将知识产权用于非法商业目的。为进一步发展国际网络能力，国防部还资助了一系列网络能力建设举措，包括计算机网络安全应急小组（CSIRT）发展项目；即将发布的中非国家网络安全和网络犯罪培训项目等，并作为网络技术全球论坛（GFCE）的创始国之一开展了许多其他项目。

此外，美国政府还得到了来自区域和国际社会的承诺，致力于共同实现国际网络稳定。2015 年 6 月，联合国政府专家小组（UNGGE）发布一份报告，介绍了各国在 ICT 方面达成的共识，并倡导制定各国网络行为准则、规定或原则，提出信心建立措施。2015 年 G20 安塔利亚峰会公报重申了报告中的许多理念。[75] 公报指出，《联合国宪章》适用于所有使用 ICT 技术的国家行为，各国在使用 ICT 技术的过程中必须遵循负责任的国家行为准则，即 2015 年发布的联合国决议：“国际安全背景下的信息和电信发展。”[76] 公报还指出，“任何国家不得开展或支持通过 ICT 技术窃取知识产权，

包括商业秘密或其他商业机密，从而为企业或商业部门提供竞争优势。”G20 国家达成一致，“各国应确保安全使用 ICT 技术，尊重和保护自由原则，禁止非法、任意干涉数字通信隐私”。2016 年 5 月，G7 领导人重申了这一原则，并签订了一项新协议，承诺共同提高能源行业的网络安全性。[77]

美国还是欧洲安全与合作组织（OSCE）成员，签订了两项网络安全和 ICT 使用信心建立措施协议[78]，包括制定具体的信心建立措施，加强跨国合作、透明度、可预见性和安全性，降低使用 ICT 技术造成的误解和争端风险；进一步制定信心建立措施，降低使用 ICT 技术造成的冲突风险。[79]

贸易谈判和大多数安全条约均面临网络安全问题。但美国政府谈判人员通常都是某一话题或区域的专家，因此无需考虑其他方面的因素。例如，美国最近签署了《关于常规武器和两用物品及技术出口控制的瓦森纳安排》的新增条款。作为武器控制的主要谈判机构，美国国防部主张控制网络通信监控系统的销售，以避免对手选取关键通信或字元数据和提取元数据（如批量采集）。美国的这一立场或受斯诺登事件影响。第二项需要限制出口的技术是入侵软件或渗透测试工具。这类工具通常使用零日漏洞检测网络漏洞。这种技术同样可用于制作武器。因此，对这些技术进行出口管制表明美国认为先进技术可以削弱国防力量，为国家安全带来风险。美国商业部门并未参与整个谈判过程，甚至根本不知道这次谈判。谈判结束后，商业部提出，其中一些条款可能产生某些意料之外的后果，影响 ICT 行业产品的销售，甚至威胁美国的商业利益。美国私营部门官员和一些国会成员对政府表示十分失望，认为政府理应邀请非政府部门加入谈判，从而减少签订网络安全条款带来的不必要麻烦。目前，美国正着手撤销这一条款。

网络安全还是许多经济贸易谈判的重要话题。

网络安全还是许多经济贸易谈判的重要话题，因为国家政策可能阻碍商品、服务、数据和资本的自由流动。作为美国的主要贸易谈判机构，美国贸易代表办公室（USTR）旨在确保谈判的技术和国籍中立，消除贸易壁垒或贸易保护主义。2013 年，美国和欧盟就《跨大西洋贸易与投资伙伴关系协定》（TTIP）展开谈判。[80] 此次谈判的目的在于刺激增长、创造就业、提高全球企业竞争力、扩大出口。 此次谈判要求美国和欧洲制定统一的数据和隐私保护政策，消除欧洲对安全监测活动的担忧。此外，此次 TTIP 谈判还签订了一项重要协议，即《欧盟—美国隐私护盾协议》。该协议允许欧美之间进行数据传输和存储，并承诺建立统一的数据保护标准。最重要的是，该协议要求美国公司保护欧洲公民的个人数据，消除欧洲民众对数据滥用的担忧。2016 年初，

欧盟委员会和美国商务部就该协议达成一致意见，为 TTIP 的成功谈判奠定了基础，但 TTIP 能否最终审批通过仍是未知数。

ICT 和网络安全问题也是《跨太平洋贸易伙伴关系协定》（TPP）谈判所面临的主要问题。此次谈判主要聚焦知识产权保护和数据主权能否改变云服务的交付和数据中心的位置。许多国家希望在该协议条款中新增国家安全例外条款。在 TPP 谈判期间，USTR 发布了《数字贸易 24 条》报告，即通过建立自由、开放的互联网空间，推动数字经济发展。[81]TPP 谈判国家接受了美国提出的许多条款，包括知识产权保护和执行。其中许多条款要求 TPP 国家开展大规模政策改革。一些国家担心条款中的知识产权和其他贸易规定可能会侵犯公民的隐私权和言论自由。目前，TPP 已在理论上达成一致，但仍需通过美国国会的最终审核。TPP 协定能否真正造福美国经济仍是未知数，因此美国国会可能不会签署该协定。

此外，许多传统国际关系中也存在网络问题，包括人权、经济发展、贸易协定、武器和两用技术控制、安全、稳定，以及和平与冲突决议等。尽管美国不断加大国际网络合作，但政府换届带来的结构转变（如没有关于美国国际战略或治理的法律）和连续性问题或影响美国国际交往的重心和注意力。美国国会还举办了几次听证会，重新定义政府的国际网络关系战略和法定制度。按照听证会要求，政府需明确美国的网络震慑政策和数字战争行动，以及国防部网络协调人的地位是否应由参议院确认。

防御与危机应对

二十多年来，美国不断进行网络防御和网络攻击。早在 1994 年，参谋长联席会议副主席就要求进行“信息战联合作战能力评估”[82]。1995 年，国防部开展了一场名为“Evident Surprise”的军事演习，召集各行政部门领导进行讨论，并就信息战政策和跨部门合作达成一致。[83]1997 年 6 月，国防部启动了“Eligible Receiver”无预警演习，旨在检验国防部在面对信息基础设施攻击时的规划和应急能力[84]。这次演习暴露了国防部信息系统的重大漏洞和应对攻击的不足。

1998 年，一系列名为“Solar Sunrise”的攻击活动席卷美国国防部，再次暴露了此前军事演习和研究中出现的不足和差距。为此，国防部成立了计算机网络防御联合特遣部队（JTF–CND），于 1999 年 6 月开始全面运作[85]。2000 年秋，国防部条例规定，将 JTF–CND 更名为计算机网络作战联合特遣部队（JTF–CNO）。2002 年 10 月，新《统一指挥计划》（修订版第二版）再次对 JTF–CNO 进行了调整，将其并入美国战略司令部（USSTRATCOM）。2004 年，战略司令部指挥官批准了《全球信息栅格网络行

动联合作战概念》，扩大了 JTF–CNO 的任务范围。

通过 20 多年的不断尝试，明确网络防御、网络作战和计算机网络攻击的职责和组织架构，国防部成立了美国网战司令部（USCYBERCOM），于 2010 年 10 月开始全面运作。网战司令部将网络攻击与防御相结合，与美国最大的情报机构国家安全局（NSA）接受统一领导。NSA 拥有计算机和新兴 ICT 基础设施与架构相关的专业知识。但两大组织的任务、权力及资源各有不同。同时，美国军队的各个分支都需组织网络部队培训，不局限于现有资源，而是接受网战司令部的作战指挥，持续保护自身网络安全。国防部的网络机构——国防信息系统局（DISA）负责人也需向网战司令部汇报工作。技术层面，网战司令部是战略司令部的二级联合司令部。网战司令部的主要监管对象是外国国家或非国家行为者。目前政府正审核一项治理举措，决定是否让网战司令部进行独立指挥。根据一系列制度决策，国防部决定任命一位高级指挥官负责网络安全，确保拉通所有网络防御、攻击以及网络维护部门，共同在网络空间执行战略安全任务。[86]

在商议和制定网络战略的同时，美国已开始将这些组织投入运作。2011 年，国防部发布网络空间作战计划声明。网络空间作战防御战略部（DSOC）制定了五项战略举措：①将网络空间视为作战领域；②关注新的防御作战概念，保护国防部网络和系统；③与美国政府和私营部门合作，制定全方位网络安全战略；④深化与美国同盟国和国际合作伙伴的关系，加强网络安全协作；⑤利用国家网络人才和技术。[87] 但公众认为，这五项举措表明国防部的网络资产仍主要关注保护其自身网络。

美国网战司令部必须做好准备，为政府机构和民政部门提供技术和任务支持。

2015 年，国防部发布了另一项网络战略，扩大了网战司令部的职责。网战司令部不仅需要负责保护美国军队的网络，还应协助其他政府机构（尤其是国土安全部）和民政部门开展工作。根据“民事当局防务支援”任务要求，国防部需为民政部门提供人员、技术及资产支持，包括技术援助、任务支持以及为国家网络紧急情况做好准备工作。战略指出，美国军队必须按照《武装冲突法》进行网络作战，确保在诉诸武力前优先使用其他综合国力手段。截至 2015 年，美国爆发武装冲突的主要原因包括生命和重大财产损失，以及对美国外交政策和经济造成严重影响（新的主要触发事件）。新战略还指出，政府必须切实保护美国国土和重大利益不受破坏性网络攻击，避免造成严重后果（目前还包括重大经济影响）。[88] 根据战略规定，国防部有权“保护国家及其利益”，“在网络防御和执法举措无法规避潜在网络风险的情况下，总统或国防部长可指挥美国军队进行网络作战，应对目前网络空间遭受的攻击或潜在危机，保护国土安全和国家利益”[89]。

随着职责的不断扩大，网战司令部计划建立多支队伍，分别为军队、国内政府机构和主要基础设施企业提供支持。2016 年，网战司令部指挥官 Admiral Rogers 在美国国会听证会上简要介绍了各队伍的建设进展。网络任务部队（CMF）目前共有“123 支队伍，计划建设 133 支。其中 27 支队伍已开始全面运作，68 支已具备初步作战能力。作战任务分队（CMT）按照战斗命令支持作战任务；国家任务分队（NMT）负责保护国家关键基础设施免遭恶意网络活动攻击，以免造成重大后果；网络保护分队（CPT）则负责保护国防部信息网络和地方计算机网络防御服务提供商（CNDSP）的安全。”[90]

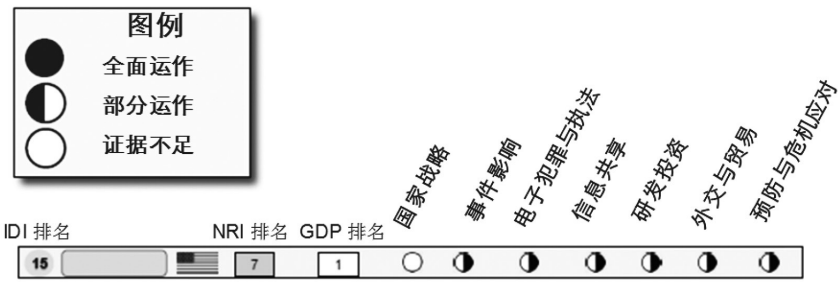
为完成作战任务，政府在 2016 财年为网战司令部拨款 4.66 亿美元作为预算。[91]CMT 部队拟招募 6,187 名成员，目前已有 4,990 名，并计划于 2018 年开始全面运作。[92] 未来几年，网战司令部有望继续增加预算。

美国在网络领域活跃于国际舞台。作为北大西洋公约组织（NATO）的创始国之一，美国积极参与公约组织和所有同盟国的演习，包括“网络联合”演习。[93] 此外，网战司令部还进行了“网络军旗”演习，召集国防部网络与信息技术人才在真实环境中磨练技能。[94] 网战司令部还通过支持国土安全部的项目，增强美国防御行业玩家的网络准备度，开展防御工业基地项目、培训项目，以及“网络爱国者”“网络盾牌”和“网络风暴”等演习，提高网络响应能力和美国民众的网络知识。[95]

CRI 2.0 概要

CRI 2.0 评估结果显示，美国的网络防御准备度正不断提高，并已开始运作 CRI 七大评估要素中的大多数领域。

分析结果反映了美国当前不断变化的格局。美国持续制定并刷新其经济（数字）议程、国家网络安全战略、政策及各项举措，寻求国家经济愿景与安全重点工作之间的平衡。国家概况的变化反映出国家在各个方面发生的变化，有利于监测、跟踪并评估美国社会所取得的显著进步。



CRI 2.0 利用全面、可比较、基于经验制定的方法论，帮助国家领导人在网络化、竞争激烈、冲突丛生的世界中做出规划，打造安全、有活力的数字世界。

如需了解更多 CRI 2.0 的相关信息，请参阅：
http://www.potomacinstitute.org/academic-centers/cyber-readiness-index。

注释

1.Charles M. Herzfeld, A Life at FullSpeed: A Journey of Struggleand Discovery. (Arlington: Potomac Institute Press, 2014) 116

2.World Bank, "ICT Service Exports (% of Service Exports, BoP)," 2015, http://data.worldbank.org/indicator/BX.GSR.CCIS.ZS, and World Bank, "ICT Goods Exports (% of Total Goods Exports)," 2015, http://data.worldbank.org/indicator/TX.VAL.ICTG.ZS.UN.

3.White House, "Mapping the Digital Divide," Council of Economic Advisers Issue Brief (July 2015), https://www.whitehouse.gov/sites/default/files/wh_digital_divide_issue_brief.pdf.

4.Federal Communications Commission, "Connecting America: The National Broadband Plan," (Washington, DC, 2010), https://transition.fcc.gov/na-tional-broadband-plan/national-broad-band-plan.pdf, and OECD, "OECD Digital Economy Outlook 2015," (Paris: OECD Publishing, 2015): 23.

5.Federal Communications Commission, "Broadcast Incentive Auction," January 8, 2016, https://www.fcc.gov/about-fcc/fcc-initiatives/incentive-auctions.

6.Federal Communications Commission, "Fact Sheet: Spectrum Proposal to Identify, Open up Vast Amounts of New High-Band Spectrum for Next Generation (5G) Wireless Broadband," July 2016, https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0623/DOC-339990A1.pdf.

7.Alan B. Davidson, "The Commerce Department's Digital Economy Agenda," US Department of Commerce, November 9, 2015, https://www.commerce.gov/news/blog/2015/11/commerce-de-partments-digital-economy-agenda.

8.US Department of Commerce, Commercial Data Privacy and Innovation in the Internet Economy, Internet Policy Task Force (June 2011), https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

9.White House, Big Data: Seizing Opportunities and Preserving Values, May 2014, https://www.whitehouse.gov/sites/default/files/docs/big_data_pri-vacy_report_may_1_2014.pdf.

10.Office of the US Trade Representative, The Digital 2 Dozen, https://ustr.gov/sites/default/files/Digital-2-Dozen-Final.pdf.

11.The IP Commission Report, “The Re- port of the Commission on the Theft of American Intellectual Property,” TheNational Bureau of Asian Research, (May 2013), http://www.ipcommission.org/report/ip_commission_report_052213.pdf, and “Sen. Warner, Gardner Announce Launch of Bipartisan ‘Senate Cybersecurity Caucus’,” June 14, 2016, http://www.warner.senate.gov/public/index.cfm/pressreleases?ID=6232F6A3-DC2D-444C-AEE5-C891511D4286.

12.Rafi Goldberg, “Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities,” National Telecommunications & Information Administration, May 13, 2016, https://www.ntia.doc.gov/blog/2016/lack-trust-inter-net-privacy-and-security-may-deter-eco-nomic-and-other-online-activities.

13.White House, “Notice – Cyber-Enabled Activities Emergency Continuation,” March 29, 2015, https://www.white-house.gov/the-press-office/2016/03/29/notice-cyber-enabled-activi-ties-emergency-continuation.

14.White House, “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,” (2009), https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

15.White House, “Presidential Decision Directive/NSC 63,” May 22, 1998, http://fas.org/irp/offdocs/pdd/pdd-63.htm, and US Department of Commerce, “Cybersecurity, Innovation, and the Internet Economy,” Internet Policy Task Force (June 2011).

16.White House, “The National Strategy to Secure Cyberspace,” (February 2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, and White House, “Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritiza- tion, and Protection,” December 17, 2003, https://www.dhs.gov/home-land-security-presidential-directive-7.

17.White House, “The Comprehensive National Cybersecurity Initiative,” (2008), https://www.white-house.gov/issues/foreign-policy/cybersecurity/national-initiative.

18.White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.

19.White House, “Executive Order 13636– Improving Critical Infrastructure Cy- bersecurity,” February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improv-ing-critical-infrastructure-cybersecurity

20.White House, “Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience,” February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-criti-cal-infrastructure-security-and-resil.

21.White House, “Presidential Policy Directive 41 – United States Cyber

Incident Coordination," July 26, 2016, https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-di-rective-united-states-cyber-incident.

22.White House, Office of the President and Office of Management and Budget, "Memorandum for Heads of Executive Departments and Agencies - Cyber- security Strategy and Implementation Plan (CSIP) for Federal Civilian Government," October 30, 2015, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

23.Ibid.

24.White House, "Fact Sheet: Cybersecurity National Action Plan," February 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

25.US-CERT, "National Cybersecurity and Communications Integration Center," https://www.us-cert.gov/nccic.

26.US-CERT, "About Us," https://www.us-cert.gov/about-us.

27.US Department of Homeland Security, "National Cyber Incident Response Plan," September 2010, http://www.federalnewsradio.com/pdfs/NCIRP_In-terim_Version_September_2010.pdf.

28.US Congress, "Consolidated Appropriations Act, 2016," http://docs.house.gov/billsthisweek/20151214/CPRT-114-HPRT-RU00-SAHR2029-AMNT1final.pdf. The Cybersecurity Act of 2015 was signed into law by President Obama on December 18, 2015 (Public Law No: 114-113). The new law established a process for the government to sharecyber threat information with businesses that voluntarily agree to participate in the program. It contained componentsfrom the following legislation of the 114th Congress: H.R. 1560 -"Protecting Cyber Networks Act;" H.R. 1731 -"National Cybersecurity Protection Advancement Act of 2015;" and S. 754 -"Cybersecurity Information Sharing Act of 2015."

29.White House, "Presidential Policy Directive 41 - United States Cyber Incident Coordination."

30.US Department of Homeland Security, "Cyber Storm," https://www.dhs.gov/cyber-storm.

31.US House of Representatives, "Testimony of Patricia A. Hoffman before the Committee on Transportation and Infrastructure," April 14, 2016, http://transportation.house.gov/upload-edfiles/2016-04-14-hoffman.pdf.

32.European Defense Agency, "Complex Cyber Crisis Management Exercisein Vienna," September 16, 2015, https://www.eda.europa.eu/info-hub/press-centre/latest-news/2015/09/16/complex-cyber-crisis-management-ex-ercise-in-vienna, and NATO, "Largest Ever NATO Cyber Defence Exercise Gets Underway," November 21, 2014, http://www.nato.int/cps/en/natohq/news_114902.htm?selectedLocale=en.

33.James Clapper, Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, February 9, 2016, https://www.dni.gov/files/documents/SSCI_Unclassi-fied_2016_ATA_SFR%20_FINAL.pdf.

34.US Department of State, “G7 Foreign Ministers’ Meeting,” April 15, 2015, http://www.state.gov/s/cyberissues/releasesandremarks/240955.htm.

35.US Congress, S. 754 “Cybersecurity Information Sharing Act of 2015,” part of the “Consolidated Appropriations Act, 2016,” https://www.congress.gov/bill/114th-congress/senate-bill/754.

36.US Department of Justice and Federal Trade Commission, “Antitrust Policy Statement on Sharing of Cybersecurity Information,” April 2014, https://www.ftc.gov/system/files/documents/public_statements/297681/140410ftc-dojcyberthreatstmt.pdf.

37.“Sen. Warner, Gardner Announce Launch of Bipartisan ‘Senate Cybersecurity Caucus’,” June 14, 2016, http://www.warner.senate.gov/public/index.cfm/pressreleases?ID=6232F6A3-DC2D-444C-AEE5-C891511D4286.

38.US House of Representatives, “Recommendations of the House Republican Cybersecurity Task Force,” October 5, 2011, http://thornberry.house.gov/uploaded-files/cstf_final_recommendations.pdf.

39.White House, “Fact Sheet: Cybersecurity National Action Plan,” February 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

40.US Department of Homeland Security, “Statement of Director Mark Sullivan, United States Secret Service, before the House Committee on Homeland Security, Subcommittee on Counterintelligence and Intelligence,” September 13, 2011, https://www.dhs.gov/news/2011/09/13/statement-re-cord-usss-house-homeland-security-sub-committee-counterterrorism-and.

41.“National Computer Forensic Institute,” https://www.ncfi.usss.gov/ncfi/.

42.The Communications Security, Reli- ability and Interoperability Council, “Final Report: U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs) - Barrier and Metric Considerations,” (March 2013), https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Re-port_March_%202013.pdf.

43.“Microsoft Security Intelligent Report,” Microsoft, (2010), https://www.micro-soft.com/security/sir/default.aspx.

44.“Global Botnet Threat Activity Map,” Trend Micro, http://www.trendmicro.com/us/security-intelligence/current-threat-ac-tivity/global-botnet-map/index.html.

45.US Department of Justice, “Letter from Pete J. Kadzik, Assistant Attorney general, to Senator Tom Carper, Ranking Member of the Senate Homeland Security Committee,” March 4, 2016, 5-6.

46.US Department of State, “Transnational Organized Crime Rewards Program,” http://www.state.gov/j/inl/tocrewards/.

47.US Congress, “H.R. 3490 - 1114th Congress: Strengthening State and Local Cyber Crime Fighting Act,” https://www.congress.gov/bill/114th-congress/house-bill/3490.

48.Financial Services-Information Sharing and Analysis Center, “Overview of the FS-ISAC,” https://www.fsisac.com/sites/default/files/FS-ISAC_Overview_2011_05_09.pdf.

49.White House, “Executive Order 13691- Promoting Private Sector Cybersecurity Information Sharing,” February 13, 2015, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sec-tor-cybersecurity-information-shari.

50.US Department of Homeland Security and US Department of Justice, “Guidance to Assist Non-Federal Entitiesto Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015,” February 16, 2016, https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Shar-ing_Guidance_(Sec%20105(a)).pdf.

51.White House, “Fact Sheet: Administration Cybersecurity Efforts 2015,” July 9, 2015, https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015

52.National Cyber-Forensics & Training Alliance, https://www.ncfta.net.

53.National Research Council, “Chapter 2,” in: Computer at Risk: Safe Computing in the Information Age, (Washington, DC: The National Academies Press, 1991), http://www.nap.edu/read/1581/chapter/2.

54.Networking and Information Technology Research and Development, “Aboutthe NITRD Program,” https://www.nitrd.gov/about/about_nitrd.aspx.

55.White House, “The Comprehensive National Cybersecurity Initiative,” (2008), https://www.white-house.gov/issues/foreign-policy/cybersecurity/national-initiative.

56.White House, “Federal Cybersecurity Research and Development Strategic Plan,” (February 2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Feder-al_Cybersecurity_Research_and_De-velopment_Stratgeic_Plan.pdf.

57.DARPA, “Cyber Fast Track (CFT),” November 13, 2015, http://open-catalog.darpa.mil/CFT.html.

58.Cheryl Pellerin, “Bug-Hunting Computers to Compete in DARPA Cyber Grand Challenge,” US Department of Defense, July 18, 2016, http://www.defense.gov/News/Article/Article/848549/bug-hunting-computers-to-compete-in-darpa-cyber-grand-challenge.

59.DARPA, “Active Cyber Defense (ACD),” http://www.darpa.mil/program/active-cyber-defense.

60.DARPA, “Plan X,” http://www.darpa.mil/program/plan-x.

61.DARPA, “DARPA Exploring Ways to Protect Nation’s Electrical Grid from Cyber Attack,” December 14, 2015, http://www.darpa.mil/news-events/2015-12-14.

62.US Department of Homeland Security, “Science and Technology - Cyber Security Division,” https://www.dhs.gov/science-and-technology/cyber-security-division.

63.Office of the Director of National Intelligence, “Cyber-attack Automated Unconventional Sensor Environment (CAUSE),” https://www.iarpa.gov/index.php/research-programs/cause.

64.National Science Foundation, “Se- cure and Trustworthy Cyberspace (SaTC),” https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709.

65.National Science Foundation, “CyberCorps Scholarship for Service,” https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504991.

66.National IA Education and Training Pro- grams, “About CAE Program,” https://www.iad.gov/NIETP/aboutCAE.cfm.

67.National Initiative for Cybersecurity Education, “About NICE,” http://csrc.nist.gov/nice/about/index.html.

68.Brandon Shackelford and John Jankowski, “Information and Communications Technology Industries Account for $133 Billion of Business R&D Performance in the United States,” National Science Foundation InfoBriefs (April 13, 2016).

69.Zach Cutler, “5 Growing Cyber Security Epicenters Around the World,” Entrepreneur, September 3, 2015, https://www.entrepreneur.com/article/250024, and Cheryl Pellerin, “Carter SeeksTech-sector Partnership for Innovation,” DoD News, April 23, 2015, http://www.defense.gov/News-Article-View/Article/604513/carter-seeks-tech-sec-tor-partnerships-for-innovation.

70.US Department of Defense, “DoD Directive 5105.85, Defense Innovation Unit Experimental (DIUx),” July 5, 2016, http://www.dtic.mil/whs/directives/corres/pdf/510585p.pdf.

71.White House, “The Comprehensive National Cybersecurity Initiative,” (2008). https://www.white-house.gov/issues/foreign-policy/cybersecurity/national-initiative.

72.White House, “International Strategy for Cyberspace,” (2011), https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strat-egy_for_cyberspace.pdf.

73.US Department of State, “Office of the Coordinator for Cyber Issues,” http://www.state.gov/s/cyberissues/.

74.US Department of State, “International Cyberspace Policy Review,” March 2016, http://www.state.gov/documents/organization/255732.pdf.

75.“Testimony of Christopher Painter, Coordinator for Cyber Issues, US Department of State, Before the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy,” May 14, 2015, http://www.foreign.

senate.gov/imo/me-dia/doc/051415_Painter_Testimony.pdf.

76.“G20 Leaders’ Communiqué,” (November 2015): 6, http://www.mofa.go.jp/files/000111117.pdf.

77.UN General Assembly, “Developments in the filed of information telecommunications in the context of international security,” December 4, 2015.

78.Government of Japan, “G7 Japan 2016 Ise-Shima,” May 2016, http://www.japan.go.jp/g7/summit/documents/.

79.Office of the US Trade Representative, “T-TIP Issue-by-Issue Information Center,” https://ustr.gov/trade-agreements/free-trade-agreements/transatlantic-trade-and-investment-partnership-t-tip/t-tip.

80.OSCE, “Permanent Council Decision No. 1106,” December 3, 2013, http://www.osce.org/pc/109168.

81.OSCE, “Permanent Council Decision No. 1202,” March 10, 2016, http://www.osce.org/pc/227281.

82.Office of the US Trade Representative, “The Digital 2 Dozen,” https://ustr.gov/sites/default/files/Digital-2-Dozen-Final.pdf.

83.Leslie Lewis et al., Joint Warfighting Capabilities (JWCA) Integration, National Defense Research Institute, (1998), http://www.rand.org/pubs/monograph_reports/2007/MR872.pdf.

84.Secretary of Defense William S. Cohen, “Annual Report to the President and the Congress,” (1998): Chapter 8, http://history.defense.gov/Portals/70/Documents/annual_reports/1998_DoD_AR.pdf?ver=2014-06-24-153404-623.

85.“Eligible Receiver,” Global Security, http://www.globalsecurity.org/military/ops/eligible-receiver.htm.

86.RAND Corporation, “Ensuring Military Capability: Continuity of Operations,” Chapter 6, https://www.rand.org/content/dam/rand/pubs/monograph_re-ports/MR1251/MR1251.Chap6.pdf.

87.US Senate Armed Services Committee, “Statement of Admiral Michael S. Rogers Commander U.S. Cyber Command Before the Senate Armed Services Committee,” April 5, 2016, http://www.armed-services.senate.gov/imo/media/doc/Rogers_04-05-16.pdf.

88.US Department of Defense, “Strategy for Operating in Cyberspace, (July 2011),http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-050.pdf.

89.US Department of Defense, “The Department of Defense Cyber Strategy,” (April 2015): 7-8, http://www.defense.gov/Portals/1/features/2015/0415_cy-ber-strategy/Final_2015_DoD_CY-BER_STRATEGY_for_web.pdf.

90.Ibid.

91.US Senate Armed Services Committee, “Statement of Admiral Michael S. Rogers

Commander U.S. Cyber Command Before the Senate Armed Services Committee."

92.Steven Aftergood, "Pentagon's Cyber Mission Force Takes Shape," FAS, September 10, 2015, https://fas.org/blogs/secrecy/2015/09/dod-cmf/.

93."Experts put to the test during NATO's largest annual cyber defence exercise," North Atlantic Treaty Organization, November 20, 2015, http://www.nato.int/cps/en/natohq/news_124868.htm.

94."Air Force competes in second 'Cyber Flag,'" Air Force News Agency, December 4, 2012, http://www.defencetalk.com/air-force-competes-in-second-cyber-flag-45800/.

95.US Department of Homeland Security, "Cyber Storm II: National Cyber Exercise,"https://www.dhs.gov/cyber-storm-ii.

英国网络就绪度报告

国家人口	6460 万
人口增长率	0.8%
按市价计算的 GDP（当前美元）	2.988 万亿美元
GDP 增长率	2.3%
引入互联网的年份	1991 年
国家网络安全战略	2011 年
互联网域名	.uk,.co.uk,.org.uk,.scot
固定宽带用户渗透率	37.4%
移动宽带用户渗透率	123.6%
移动手机用户渗透率	98.7%

ICT 发展与网络联接指数排名

国际电信联盟（ITU） 通信技术发展指数排名	4	世界经济论坛（WEF） 网络就绪指数	4

来源：世界银行（2015）、ITU（2015）、NRI（2015）、互联网社会

概述

英国的商业互联网，作为美国公司（Oracle）和英国政府的英国电信公司合作的项目，建立于1991年。次年，英国第一家商业物联网服务商Pipex引进了拨号上网服务，为150家客户网点提供上网服务。

自20世纪90年代初期，互联网链接得到了成倍扩张，促使互联网—政府、互联网—商业、互联网—银行得到了长足发展。今天，英国已经是欧洲国家中互联网普及率最高的国家之一，拥有90%互联网普及率（见图1）——高于欧洲平均水平79%[1]。在2015年，超过78%的英国人，几乎每日都上网，超过74%的人口在路上会使用。因而WIFI热点迅速增长，现在已经有数百个热点遍布于全国，包括公共场所、咖啡店、旅馆等。在2010年到2015年，手机宽带的订阅量翻倍，从24%上升到了66%[2]。

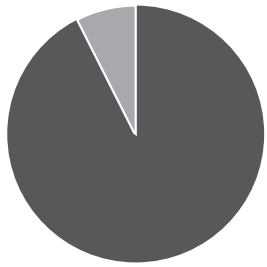


图1 英国互联网渗透率：91.6%

2013年，英国发布了国家数字化战略《信息经济战略》，旨在向商业区和服务不足的地区提供高速宽带服务[3]。到最后，英国宽带局（BDUK）——英国文化、媒体和体育部的一部分，则执行像超级链接城市项目（SCCP），支持在大多数成熟的宽带增长业务。另外，该数字化战略还注重包括英国内外的通信互通性和标准。英国还在规范P2P技术不断增长的市场影响上采取主动性的姿态，尤其是受到影响的金融领域[4]。

像很多其他发达国家一样，网络安全对英国是一个主要的挑战。2010年，英国政府意识到网络安全在经济和国家安全层面是“一级风险”[5]，进而立誓要把英国打造成“居住和工作都是最安全上网的地方”[6]。在2011年，前英国外交部部长William Hague发起了保卫网络空间自由和民主价值观的愿景计划，这形成了未来网络空间的国家间行为准则协议的基础，同时也为新一届英国政府制定了关键性安全首要任务。

在2011年慕尼黑安全会议上演讲中，他讨论了所有的步骤，英国政府已经对国内外网络威胁采取对抗行动，并立誓与“私营部门合作，确保安全且有弹性的关键基

础设施，而且确保最强技能基础，抓住网络空间经济机会，提升公众对网络安全威胁的意识。[7]”尽管从那时起，这些目标雄心壮志，但是英国政府负责的不同研究却发现，知识产权的窃取在增加，甚至每年越来越多的英国组织，在从事网络犯罪。而严重形式和安全分支机构的影响力也在继续上升，据估计，在大组织的个人分支会花费，在60万英镑到115万英镑（像2015年）（大概在74 1363美元到142万美元）[8]。

由于网络不安全因素，2015年合并的《国家安全战略和战略防御与安全评估》（SDSR）重申了国家以及脆弱性和潜在的经济损失[9]。2016年，英国国家犯罪局（NCA）报告说，网络犯罪已经超过了其他形式的犯罪，对于增强司法和商业合作打击这一威胁的需求，感到压力山大[10]。结果，2015年SDSR和后续报告称，鉴于网络威胁的数量和精细程度增加，英国政府正在计划于2016年发布一个新的国家网络安全战略，而且最近建立的国家网络安全中心（NCSC）作为“产业和政府的桥梁”，“为私有和公共类似部分提供单独联系点”[11]。

随之形成的是第二个“国家网络安全项目”，未来5年，英国政府计划差不多双倍投资于网络安全，最高到19亿英镑（约23.5亿美元）。政府通信总部（GCHQ）将在这项战略的交付上以及与产业和学术的合作上，被公认为新中心最成功的“关键”部门。NCSC将会在GCHQ扮演面向公众的部分，将会在网络安全问题上对各种体量的商业和各个部门提供权威性建议，帮助他们更好地理解网络威胁和削弱影响[12]。

网络就绪指数2.0受到雇佣，评估英国网络风险准备水平。这些分析为英国提供一个可执行的蓝图，以便更好的理解，它的网络基础设施的依赖与薄弱，进而评估它在减小，现在网络安全现状和为支撑数字化未来的国家网络安全能力，这个鸿沟上的承诺能力和成熟度。所有关于英国网络安全相关的努力和在7个基本元素（国家战略、突发时间反馈、互联网犯罪和执法、信息共享、研究和发展投资、外交与贸易、防御和风险反馈）上的能力评估如图2所示。

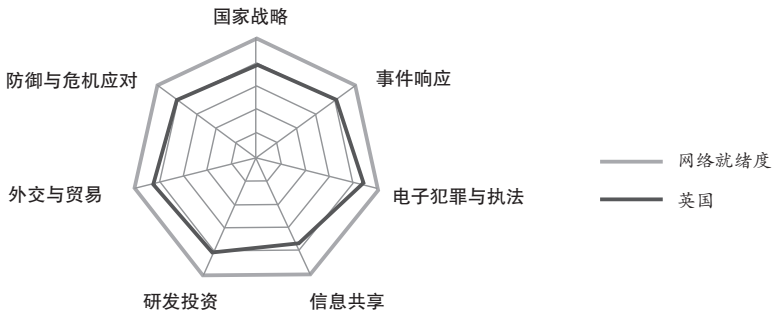


图2 英国网络就绪评估（2016）

国家战略

2009 年英国发布了第一个国家的《网络安全战略》[13]，在 2011 年该战略进行了升级[14]。前英国外交部部长 William Hague 在 2011 年 2 月的慕尼黑安全会议上概述了关键因素。他声称，“有的惊人链接能力的互联网，已经大规模且增长式创造了很多机会，激发了经济潜能，更新获取信息，而且需要民主政府更加透明。”然而，他也承认说，“源于我们对网络空间的异常依赖，其中有一个黑暗面，”而且确认说，“英国准备参与其中”打击国家内外的网络威胁[15]。

2011 年的战略包括，英国所面临的一个详细的网络威胁，和排名前五大风险的网络攻击和网络犯罪。伴随性的执行方案，以关键目标为基础，包括通过建立起一个新的网络行动防御组，和把网络安全嵌到英国主流国防计划和行动中，以驻守英国网络能力。自从第二个战略发布，英国政府已经投入了 8.6 亿英镑（约 10.6 亿美元）去加速获得新技术和执行能力，以实现 2011 年版本中提到的“充满活力、弹性和安全的网络空间”[16]。战略还设计了在内阁办公室的国家网络安全项目，以此作为强有力政府的责任，确保战略的实行。

另外，英国国家网络安全战略与英国国家数字化战略（2013 年的信息经济战略）协同运行。两者都承认尽管 ICT 是经济增长的重要引擎，但是网络安全必须支撑信息经济，以便于实现这样的经济增长。正如英国数字化战略中所说的，没有网络安全商业，消费者就不会带着信任和自信去使用互联网和其他数字化技术。[17]”

在未来 5 年，英国政府计划投资上限到 19 亿英镑（约 23.5 亿美元）以在网络攻击方面进行保护，而且伴随着后续的五年计划，计划在 2016 年年底发布第二个五年的国家《网络安全战略》。最终，一个新建立的总部在伦敦的国家网络安全中心（NCSC），和在 GCHQ 所在切尔滕纳姆的卫星办公室，一起致力于确保公众、公众和私营部分的组织、以及英国关键国家基础设施的上网安全。 NCSC 有 4 个主要目标：（1）理解网络安全环境，分享知识，而且用专业知识去定位和处理系统化的博弱项；（2）在效率机制上的对英国公众和私营部分组织提供指导，以提高他们网络安全和执行演习，降低网络风险；（3）通过提到政府和执法活动的合作，回应国家网络安全的突发事件；（4）提高国家网络安全能力[18]。到 2017 年，NCSC 计划建立一个超过 700 专业人员的专职部门，这个部分在伦敦新总部和 GCHQ 分化出来，将会包括为市中心、伦敦白厅、情报部门和安全服务，能源、电信，以及其他关键国家基础设施的专业团队[19]。

突发事件反馈

英国第一个国家 CERT 建立于 2014 年，回应 2011 年国家网络安全战略。

网络突发事件的汇报和反馈机制，直到 2014 年都是非常碎片化的。没有一个单独的国家计算机紧急应急团队，但是反而有两个主要专注于不同组织的政府团队：（1）一个是建立在国家基础设置保护中心之下的计算机安全突发应急团队（CSIRT — UK），这个团队服务于这部分的公司；（2）一个 GovGertUK，为政府和广大公共部门组织提供反馈服务。为了配合 2009 年国家网络安全战略，英国政府还建立了一个网络安全行动中心（CSOC），负责监控网络空间和协调突发事件反馈。[20] 另外，英国还有其他 20 个公共和私人的 CERT 和一个国防部专用的 CERT 负责 MOD 网络。

在 2014 年，英国建立了一个网络评估中心和第一个英国国家 CERT（CERT — UK），以配合 2011 年的国家网络安全战略。CERT — UK 致力于 4 个主要责任：处理国家网络安全突发事件管理；为处理网络安全突发事件的关键基础设施公司提供支持；促进在产业、学界和公共领域对网络安全情况的意识；提供单独的国际接触点，用于在国家 CERT 上的协调与合作。其他的 CERT 是不能再拆分的，但是 CERT — UK 变成一个主要的国家实体，负责增加英国网络准备和管理国家网络安全突发事件的弹性和能力。

这些包括：协助更加高效的国内反馈和信息分享合作（包括一个网上汇报架构来记录网络安全突发事件）；再跨境突发事件反馈上，为国际合作者们，提供一个链接点；参与国内与政府部门和产业合作者的演习（比如说“白色噪音”演习），与北约进行多国家网络安全演习，与其他国家的 CERT 合作建立信任，增强对网络威胁的理解。

而且，CPNI 和国家信息技术管理局（CESG，GCHQ 的一个信息安全分支）开展了一个领航员项目和后续的设计两个网络突发事件反应（CIR）方案——一个小政府运行一个 CIR，而一个大的政府运行一个大的 CIR，去帮助关键基础设施公司获取认证的量身定制的网络突发事件反馈服务，而且提供他们可提供该服务的公司名单。这种方法使得组织化的网络攻击犯罪（包括国家和多国家产业，CNI，以及更公众和中央政府），找到合适的突发反馈和量身定做的线性服务，与此同时允许 GCHQ 和 CPNI 关注那些最具挑战国家安全的攻击。另一个最近的项目由 CESG 落地——“认证的网络安全咨询服务”方案——认证咨询服务公司为政府和产业提供安全架构，风险评估，和风险管理服务 [21]。

英国政府正在与 GREST 工作——一个非营利、代表技术信息安全产业的信赖

体——来评估网络安全方案提供者的质量，和批准运营者和网络突发事件反馈的产品，渗透测试、袭击刺激，和其他相关项目。比如说，网络基础项目，就是 CESG 发布的，为组织机构提供基本网络安全标准，和帮助他们更好的应对网络袭击。目前超过 1 000 家公司已经获得了网络基本认证的资格。作为这个项目的一部分，CESG 和 CPNI 已经发布了非常成功的产业指导，这些产业聚焦组织机构可以提高网络架构，和减轻或阻止大部分的网络袭击的实际操作步骤[22]。已经实施的指导文件发布在 2012 年，又在 2015 年重新发布，名字是《迈向网络安全的 10 个步骤》，而且还有一套最好的实施方案，发布于 2015 年，叫做《小企业：你需要知道的网络安全》[23]，它为商业提供了帮助他们提高降低网络风险的技术指导。另一项计划包括给小型企业的凭单方案，到达 5 000 英镑（6 178 美元）中型企业获得专业建议，以增强他们网络安全的能力，保护新型商业的（创新）想法，以及保护知识产权。

另外，内政部正在和领头的通信公司，提供增强网络安全的服务，来规范关键基础设施，特别是在金融、电力、通信以及交通领域。这些服务会给予英国政府更高的监督，理解这些领域所面临的具体的网络威胁，包括在互联网传输过程中的威胁，以及其他方式发生的。在这些方式上，这个项目有助于形成一个更加主动和防御性的态势。

英国已经和合作产业开展了几个国家网络安全演习，政府机构和关键基础设施建设的具体执行部门进行危机反馈计划实践。比如说 2013 年 11 月，英格兰银行开展了“行走鲨鱼 2 网络安全演习”——这是一项整体银行系统应对刺激性网络袭击，评估其反馈的压力测试演习，它作为英国金融政策委员会推荐的工作，去评估和提高网络弹性[24]。英国政府与美国非常活跃合作，去组织演习，这些演习测试着他们对金融突发事件反馈能力，而且评估和强化着跨太平洋合作和沟通机制。另外，英国常规性的参与多变国家的网络安全演习，比如说欧盟（EU）组织的，北约（NATO）组织的，欧洲防御局（EDA）组织的，美国国土安全部组织的（比如说，网络风暴），这些演习以理解跨境依赖和强化国家间的网络突发事件反馈能力[25]。

新国家网络安全中心将会负责国家网络突发事件反馈以及保护关键基础设施。

除提高网络威胁意识和与商业团体和公共领域，教育他们如何在互联网上处于安全，新的国家网络安全中心还准备去成为一个有能力的权威，为国家网络安全突发反馈和确保英国反抗网络袭击的关键性国家基础设施的弹性负责。作为努力的一部分，CERT — UK 的功能被放进到 NCSC，这将和已经被 CESG，CPNI 和网络评估中心发展的能力一起去简化现有的设置和扩大英国网络能力。

互联网犯罪和法律执行

英国网络安全战略 2011–2016 年度报告重申说，2011 国家网络安全项目的承诺“处理网络犯罪，使得英国成为全球网络空间最安全做生意的地方”[26]。在 2011 年到 2016 年之间，英国政府项网络犯罪防止计划和三个其他与网络有关的项目，集资 8 亿英镑（约 10.6 亿美元）。

一些显著的努力正在进行，用于处理这些总体目标包括在国家网络局建立新的国家网络犯罪部，负责在国家层面上，协调最严重的网络犯罪威胁，支持与专业性合作伙伴的专业能力，以及地区组织犯罪部 (ROCUs) 的每一个网络部建立。NCCU 接受国家网络安全项目的自主，与 ROCUs、都市警察网络犯罪部（MPCCU）和产业、政府、国家法执行机构紧密地展开工作，以对迅速变化的威胁进行反馈，并降低整体的网络犯罪[27]。

尽管在 2011 年，英国在网络犯罪方面签署了欧盟委员会网络犯罪公约，但是实际上，直到英国 2011 年敦伦网络空间会议（这是一个多国参与的网络会议）前才批准。2012 年，英国外交与联邦事务部，投资了 10 万英镑（约 123 560 美元）去执行在英国的布达佩斯公约[28]。这项资金支持，致力于加强与网络犯罪相关的强化法律途径；培训法律执行机构和司法机关，而且提供公共和私营合作以及国际合作。根据英国网络安全战略 2011–2016 年度报告，英国政府的检察机关（CPS）也向不同的受众提供海外培训，包括向在具体牵扯到互联网犯罪和电子证据相关话题的警察、检察官和法官[29]。

在英国主要应用的网络犯罪法是《1990 计算机滥用法案》，根据该法案，未经允许的上网或篡改电脑资料是违法行为。在 2015 年，《严重犯罪法案》对《计算机滥用法案》做了修订，根据修订，对未经授权的行为造成严重破坏的新罪行，实施了“欧盟信息系统攻击指令”，并明确了执法机构的保留规定[30]。

而且，NCA 创立了一个新的国家网络犯罪部，把之前互联网犯罪部在严重组织犯罪局（SOCA）和都市警察中心互联网犯罪部的工作合并。新的工作组执行 NCA4 个操作上的命令（边境，组织的犯罪，经济犯罪，儿童剥削和上网保护（CEOP）），这些命令是由专家、情报和指导提供支持的。这个新工作组扮演着国家执行部门，处理国家级别最严重的网络犯罪，对主要的国家突发事件做部分回应。

信息共享

网络安全信息分享合作（CiSP）是一个私营—公共合作关系，他们分享网络威胁

和脆弱性信息。

网络安全信息分享合作（CiSP），作为 CERT — UK 的一部分，在 2013 年落地。它是一个联合性、合作性的倡议，在产业和政府间分享网络威胁和脆弱性信息，以此增强整体情况认知，进而减少网络突发事件对英国商业的影响[31]。它由国家往楼安全项目出资建立，将各个体量的不同部门的组织聚集到一起。CiSP 跟随英国国家网络安全战略的目标，仅仅 3 年时间，就成倍增长，2016 年 5 月，已经有 2 220 个组织和 6 150 个员工。

合作的价值已经在国际上被认可，而且 CiSP 很快变成了其他国家的标准，比如已经成为建立政府—产业信息共享合作关系的荷兰。CiSP 的组织成员来自不同领域和组织，包括 CESG、执法部门和国际合作者，他们可以在一个安全且动态的环境里，实时交换网络威胁信息，同时在一个共享信息的保密工作框架内执行任务。另外，CiSP 的成员还会定期从一个“分裂细胞”中接受网络威胁信息，建议和警示，这个“分裂细胞”是一个产业和政府结合的分析团队，该团队从多方获取数据资源，进行检测、分析和收集网络威胁信息，来帮助组织各个层面的网络熟悉度[32]。CiSP 还参与了国家层面的网络安全演习，包括 2013 年的行走鲨鱼 2 行动。

CERT — UK 和 CiSP 的办公地点在一起，对于每天与关键国家基础设施公司处理网络突发事件，提供一个国际维度讨论。另外的信息交换机制已经在全国建立起来，包括非营利的研究中心和会员组织。

2015 年的《国家安全战略和战略防御与安全评估》明确要求 GCHQ 将网络威胁“知识与英国产业和同盟国”分享[33]。

最后，在英国，新的国家网络安全中心将会服务于信息安全的权威性来源，而且将会为在公众和私有领域之间分享最好的安全实践，扮演一个枢纽作用[34]。NGSC 将会运作 CiSP 和它的网络平台，因此使得更多的组织机构可以彼此以及和 NCSC 去分享重要信息。NCSC 计划用从突发事件和情报搜集来的，以及其他的合作者们分享的知识，去提供最好的事件建议和指导，去解决系统性的脆弱，增强英国整体的网络安全。

研究和发展投资

2011 年的英国国家网络安全战略和 2014 年《网络安全战略报告—进步计划》都提到了英国政府对网络安全研究和发展的承诺[35]。而且，2014 年国家创新计划，名为“我们的增长计划：科学与创新”，英国政府建立了为英国实现“世界上做科学和商业最

好的地方”的长期政策[36]。

英国在网络研究和发展的投资，被几个不同的政府机构所监视着，包括 GCHQ，新商务、能源和产业改革部（前商业、创新、技能部），文化、媒体、体育部、内阁办公室，和能源与物理科学研究会（EPSRC）。作为一部分承诺，在 2015 年 EPSRC 提供了 5 百万英镑（约 620 万美元）自主安全信息技术中心（SCIT）——英国的网络安全研究知识和创新中心。英国政府还捐助额外的 19 亿英镑（约 23.5 亿美元）支持到 2020 年的网络安全研究和创新[37]。这套投资设定与新的 GCHQ 网络加速器一并开始，作为“两个世界领先创新中心发展的一步”[38]。 这项新的计划旨在确定出“那些发现创新技术去解决真实存在的网络安全问题的公司，和那些拥有可以应用于网络安全背景产品的公司”[39]。 文化、媒体和体育部已经承若在未来 5 年投入 5 000 万英镑（约 6 180 万美元）建立两个创新加速器中心[40]。第一个网络加速器中心将建立在切尔滕纳姆（GCHQ 的所在地），而且将预计在 2017 年早些时候开放。被选拔为加速器中心一部分的公司也将会对接 GCHQ 公司员工以及技术，以便去了解他们面临的网络威胁的种类，以及提高能力，发展想法，改进前沿产品，以对抗现有的和不断出现的网络威胁。第二个创新中心将在 2017 年晚些时候在伦敦开放。两个加速器中心将都由“ Telef ó nica Open Future”的一部分英国 Wyra 运作， Telef ó nica Open Future 公司为帮助创业公司发展创新和增长的想法提供多年的帮助[41]。

英国面临着对有能力保护关键基础设施和数字化财产专业人士的严重短缺。预计在英国，少于 0.6% 的计算机科学毕业生在网络安全领域谋求职业发展，而且英国会计办公室已经警告，这会花 20 年的时间才能填补训练这个网络安全从业者的鸿沟[42]。英国内阁办公室，商业、能源、产业改革部，国家网络安全项目，和 GCHQ 正在一起领导和支持一些活动，来提高不同教育层面网络安全的技能。比如说，英国网络安全挑战——英国政府、产业和学术届支持的一个非盈利组织，运作了一个比赛，以吸引和激发未开发的网络安全才能，组织网络影帝，发住人们发展新技能，探索网络安全相关的职业机会[43]。“网络第一”，这是最近的一 GCHQ 的计划，旨在识别和训练不同背景的青年才俊支持 GCHQ 和英国网络安全任务。被选上的人会获得资助攻读网络相关的本科学位，在暑假实习期间练习网络技能，毕业后在国家安全部门工作[44]。

2016 年英国政府发布了一个名为“网络安全：未来学校和未来教育的项目与资源”报告，以寻求教师更好的将网络安全整合进教学指导。另外，GCHQ 提供为具体的 GCHQ 认证的网络安全方面的硕士学位提供标准。目前，10 所英国大学已经达到

了 GCHQ 认证的网络安全领域上的硕士学位的严格标准，而且其他英国大学也提供硕士和博士水平的网络安全项目，包括伯明翰大学、布里斯托尔大学、剑桥大学、英国帝国理工、兰开斯特大学。11 所英国其他的大学也获得了网络安全研究和努力方面高级标准的“优异学术中心”的地位。这些学术中心和像谷歌、火狐等私营公司展开合作，发展网络安全前沿的解决方案，处理像隐私保护这类问题，而且也和其他国家发展合作，促进网络安全研究和发展[45]。

2010 年，英国政府建立了弹射项目——该项目是一个世界领先的工作中心，用来增强英国创新以及把英国商业、科学家和工程师聚合到一起从事最近阶段的研究和发展，帮助提高未来经济增长[46]。这个项目已经在初期投资了 2 亿英镑（约 2.47 亿美元），而且旨在为英国的创新和增长提供新的动力。它的目的在于链接英国研究和学术共同体，解决关键问题，将高潜力的思想转化成为新的产品和服务，以在广泛的商业规模上销售。第一个弹射中心，正在将英国的创新转化成实际的努力，通过聚焦专家，获得前沿设备和专业设备发展和测试想法，将概念转化成产品和服务。

而且英国还参与了欧盟的“地平线 2020”计划，该计划的原则之一，就是通过开创新的研究与发展工作，增强私营和公共领域的合作，以创造 ICT 领域的增长[47]。另外，伦敦的“网络创新枢纽“伦敦网络，是欧洲第一个网络安全加速器和恒温箱空间，该枢纽被发展以激发网络创新和帮助商业，发展信息安全相关的产品[48]。

NCSC 像在处理关键国家网络安全问题上发挥领导作用，通过聚合政府、产业和学术来增强 ICTs 的优势，通过对根产生的分析来理解系统性的脆弱性，与关键的股东合作，激励市场更好的处理网络威胁。

英国发布了“伦敦过程”——将不同国家聚集在一起，处理网络空间中可接受行为规范。

外交和贸易

在网络空间的国际规则促进和发展上，以及在参与国际间网络安全、网络犯罪、经济增长和发展和互联网治理方面的参与上，英国已经成为一个先锋力量。2011 年，前英国外交部部长 William Hague 召开了网络空间的伦敦回忆，这是第一个内政部聚集参加的系列会议，由世界上诸多国家举办，此后称为“伦敦过程”。

这些潜在的专题性的对话设立的目标是，将更多国家带到一起，去处理网络空间可接受行为的更好链接规则的需要，以及做出一个承诺去合作，来保护潜在互联网安

全。 在 2011 年慕尼黑安全会议上，Hague 部长强调关键的原则应该是“巩固关于未来使用网络空间的国际规则”[49]。 这些原则包括与国家和国际法相匹配的网络空间原则；每一个人在网络空间接触技能、技术、自信、机会的权利；对表达、意见、隐私和知识产权自由的保护；对不同语言、文化和思想的尊重；对集中打击网络犯罪的需求；对一个能确保在工作网、服务和内容的投资公平回报的竞争环境[50]。

这些基础性的因素，与一个多种利益相关者方案一起，成为了联合国治理专家组（UN GGE）达成许多网络相关协议的基础，而这方面，英国在最近一些年扮演着活跃的角色。2015 年 7 月，UNGGE 重新确认了在 2013 年国际法上的结论，尤其是将 UN 宪章应用到网络空间[51]。他们也同意在新的报告所说的，关于国际法可能应用到网络空间、自信建立渠道做推荐、国际合作，和能力建设[52]。在报告中提出的网络空间，自主性、负责人国家行为未建立的规则，最终在 2015 年 12 月，被采用到联合国安理会，晚些时候被 G — 20 合法化。

英国还是欧盟安全组织与合作（OSCE）的成员，而且已经积极参与一些讨论，这些讨论是网络安全和 ICT 应用方面，CBM 另外的主要两个协议——OSCE 决议 1106，在 2013 年落地，概述了 11 个具体的 CBMs，旨在增强国家间合作、透明性、预测性、稳定性和降低错误解读的风险，升级和源于 ICTs 使用的冲突[53]。OSCE 决议 1202 在 2016 年 3 月达成一致，重新确认了原有的 11 个 CBMs，而且增加了 5 个尤其是未降低源于使用 ICT 使用冲突风险的机制[54]。这些机制集中在包括保护沟通渠道的需求，来降低错误解读和升级的风险；发展共享风险的管理过程，以防跨过破坏 ICT 关键基础设施的泛滥；拓展方法交换最好的实践；提升国家和跨过 CIT 关键基础设施的安全，包括在区域和次区域的整合；鼓励对于影响在 ICT 使用中影响安全的脆弱性的汇报。

2016 年 2 月，有些著名的双边合作包括英国对以色列网络安全贸易，这些增强了两国之间的商业和学术合作，包括在突发事件管理上 CERT 对 CERT 的研究。2015 年，印度—英国网络对话，和印度总理莫迪访问英国，以增强现有的在网络问题上的合作。两国重新确认了他们在打击网络犯罪，和升级国家负责任的主动性规则，而且将国际法应用于网络空间[55]。另外，自 2013 年开始，英国和中国举办过一个成功的 1.5 轨对话，帮助明确和激发在两国政策、利益重合上的合作，与此同时也澄清一些在一些认知分歧上无法达成一致的内容[56]。

英国政府已经发展出了产业导向的标准，来促进英国作为“互联网贸易和商业最安全的地方”，而且也去帮助“英国商业促进在国内外市场的产品和服务”[57]。比如说，

2014 年由 CESG 主持的“网络要点项目”，就已经帮助各个领域和各个体量的组织发展网络安全标准，以此保护他们不受最常见的网络威胁。这个项目的要求和标准在学术、私营和公共组织的应用上是相似的[58]。

2015 年 12 月，英国起草了非正式的欧盟网络和信息安全指导协议（NIS），以提高欧洲网络安全能力和合作。这个指导协议在 2016 年 5 月被欧盟正式采用，并在 2016 年 8 月实施[59]。尽管英国要离开欧盟，但英国可能仍然和这个协议，以及其他欧盟数据保护和数据隐私规定绑定，至少是在英国正式退出欧盟之前。现在英国与其他欧盟成员进行贸易的公司，将在 2018 年，遵守新的欧盟数据保护规定（GDPR）。

自从 NIS 和 GDPR 规定落地以来，很多总部在英国的国际生意也受到影响，而且甚至考虑离开英国，去其他欧洲国家。这可能会迫使英国与欧盟协商独立的数据隐私和安全协议，或者采用与欧盟规定一致的国家法律来继续和欧盟市场的贸易来往[60]。

防御与危机反馈

2015 合并的“国家安全战略和战略防御和安全评估”，清晰地把 GCHQ 定位和国家责任一起地主要政府机构“去发展能力，侦查和分析网络风险，抢先攻击，以及跟踪这些责任。[61]”在同一个文件中，国防部强调他们的意图是发展一个“联合网络组”，合并网络能力抵抗 MOD’的军事防御系统（最开始），与此同时，正如所需要的，也协助整个国家的防御。英国政府已经对主要在国家财产和利益的网络攻击，开始运用非网络惩罚性的反馈，正如被要求的那样，这些原来假定和 GCHQ 和军事能力相关，而且甚至已经被讨论考虑“活跃网络防御”的可能性了，而这些都是和把英国建立成“网络空间最受保护的国家”的目标是一致的[62]。

伴随着 NCSC，英国政府已经投入了 4 000 万英镑（约 49 万美元），在 GCHQ 的指导下，开设一个网络安全运行中心（CSOC），去更好的分享关键网络情报，与关键部门和英国其他部分取证[63]。这项行动是政府发展和利用“国家的艺术”防御性网络安全策略的一部分，为的是提高英国抵御风险的能力，防御工作网和系统，而且去发展网络空间的主权能力。CSOC 计划将向英国军队提供支持，整体上，增强英国网络安全姿态（比如政府部门、产业和国际伙伴的合作）。

与其一致的，作为北约建立成员，英国定期参与北约的网络演习、计划和行动。它也在其他小区域和同盟的欧盟内外的其他国家，进行双边网络相关防御演习。尽管

这些演习结果关系到英国更大的系统性的网络防御整体效果，公众是不知道的，但是GCHQ 和英国 MOD 会常规性的和其他一小部分欧盟国家组织在一起，考虑更先进的网络防御能力。

CRI 2.0 底线

根据 CRI2.0 评估，英国正在网络准备上的道路上，而且现在已经实现了在 7 个 CRI 基本元素的部分运行。

在动态和变化的英国准备和能力的方法上，上述分析发现代表了一种投射。随着英国继续发展和更新它的经济（数字化议程）和国家的网络安全战略、政策和倡议，反应出一个更加平衡的方法，与国家经济远景和国安安全优先匹配，更新了的国家图景，将会反映出这些变化，而且监视、跟踪和评估实质性的和显著的进步。

CRI2.0 提供一个综合、对比和建立在经验基础上的方法论，在一个神秘性、竞争性和容易冲突的网络世界，帮助国家领导人们谋划通向未来更加安全和弹性的数字化未来。

更多详情，请参见 http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

注释

1.World Bank, “Internet users (per 100 people),” 2014, http://data.worldbank.org/indicator/IT.NET.USER.P2.

2.UK Office for National Statistics, “Internet Access - Households and Individuals: 2015,” August 6, 2015, http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2015-08-06.

3.UK Department for Business, Innovation and Skills, “Information Economy Strategy,” June 14, 2013, https://www.gov.uk/government/publications/information-economy-strategy.

4.OECD, “OECD Digital Economy Outlook 2015,” July 15, 2015, http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm.

5.UK Government, “Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, (2010): 47, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf.

6.UK Parliament, “Final Annual Report on the 2011-2016 UK Cyber Security Strategy,” April 14, 2016, http://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Lords/2016-04-14/HLWS652/.

7.UK Government, “Foreign Secretary William Hague’s Speech at the Munich Security Conference: Security and freedom in the cyber age – seeking the rules of the road,” February 4, 2011, https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road.

8.UK Government, “PwC 2015 Information Security Breaches Study on UK Corporations,” (2015), https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf.

9.UK Government, “National Security Strategy and Strategic Defence and Security Review,” (2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.

10.National Crime Agency, “Cyber Crime Assessment 2016,” http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file.

11.UK Government, “Prospectus: Introducing the National Cyber Security Centre,” May 25, 2016, https://www.gov.uk/government/publications/national-cyber-security-centre-prospectus.

12.“National Cyber Security Centre HQ operational,” SC Magazine UK, October 3, 2016, http://www.scmagazineuk.com/ncsc-will-be-based-in-the-nova-office-and-shopping-complex-near-victoria-station-in-london/article/526405/

13.UK Cabinet Office, “Cyber Security Strategy of the United Kingdom,” (June 2009), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf.

14.UK Cabinet Office and National Security and Intelligence, “Cyber Security Strategy,” November 25, 2011.

15.UK Government, “Foreign Secretary William Hague’s Speech at the Munich Security Conference: Security and freedom in the cyber age – seeking the rules of the road.”

16.UK Government, “UK Cyber Security Strategy: statement on the final annual report,” April 14, 2016, https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-the-final-annual-report.

17.UK Government, “Information Economy Strategy,” (June 2013).

18.UK Government, “Prospectus: Introducing the National Cyber Security Centre,” (March 2016): 4.

19.“National Cyber Security Centre HQ operational,” SC Magazine UK.

20.UK Cabinet Office, “Cyber Security Strategy of the United Kingdom,” 5.

21.Rene Millman, “GCHQ information security arm CESG awards six firms Certified

Cyber Security Consultancy status," Public Technology, February 15, 2016, https://www.publictechnology.net/articles/news/gchq-information-security-arm-cesg-awards-six-firms-certified-cyber-security.

22.GCHQ, "Re-Launch of '10 Steps to Cyber Security'," January 16, 2015, https://www.gchq.gov.uk/news-article/re-launch-10-steps-cyber-security.

23.UK Government, "Small Businesses: What You Need to Know about Cyber Security," March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf.

24.UK Government, "Government and regulators meet to combat cyber threats to essential services," February 5, 2014, https://www.gov.uk/government/news/government-and-regulators-meet-to-combat-cyber-threats-to-essential-services.

25.European Defense Agency, "Complex Cyber Crisis Management Exercise in Vienna," September 16, 2015, https://www.eda.europa.eu/info-hub/press-centre/latest-news/2015/09/16/complex-cyber-crisis-management-exercise-in-vienna, and NATO, "Largest ever NATO cyber defence exercise gets underway," November 21, 2014, http://www.nato.int/cps/en/natohq/news_114902.htm?selectedLocale=en.

26.UK Cabinet Office, "The UK Cyber Security Strategy 2011-2016: Annual Report," (2016): 5, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.

27.National Crime Agency, "National Cyber Crime Unit," http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit.

28."UK gives £100K to implement Convention on Cybercrime," Information Age, March 2, 2012, http://www.information-age.com/technology/security/2089928/uk-gives-£100k-to-implement-convention-on-cybercrime.

29.UK Cabinet Office, "UK Cyber Security Strategy 2011-2016: Annual Report," (2016): 13. The

30.UK Government, "Serious Crime Act 2015," March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415953/Factsheet_-_Computer_Misuse_-_Act.pdf.

31.CERT-UK, "Cybersecurity Information Sharing Partnership (CiSP)," https://www.cert.gov.uk/cisp/.

32.CERT-UK, "Fusion Cell," https://www.cert.gov.uk/cisp/.

33.UK Government, "National Security Strategy and Strategic Defence and Security Review," (2015): 40.

34.John Leyden, "National Cyber Security Centre to shift UK to 'active' defence," The Register, September 16, 2016, http://www.theregister.co.uk/2016/09/16/uk_gov_active_cyber_defence/.

35.UK Cabinet Office, “The UK Cyber Security Strategy Report on Progress and Forward Plans,” (2014): 23.

36.UK Department for Business, Innovation & Skills, “Our Plan for Growth: Science and Innovation,” (2014): 5, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/387780/PU1719_HMT_Science_.pdf.

37.EPSRC, “EPSRC and Innovate UK Announce £5 Million Investment in UK Cybersecurity Research and Innovation,” March 19, 2015, https://www.epsrc.ac.uk/newsevents/news/csit1/, and David Crozier, “CSIT Labs Is Launched: An Incubator Programme Designed to Engineer Viable Ventures in Cyber Security,” CSIT Labs, November 24, 2015, https://www.csitlabs.com/2015/11/24/csit-labs-is-launched-an-incubator-programme-designed-to-engineer-viable-ventures-in-cyber-security/.

38.GCHQ Cyber Accelerator, “Developing the UK’s Cyber Security Ecosystem Through the Acceleration of Innovative Cyber Security Start-ups,” https://wayra.co.uk/gchq/.

39.Ibid.

40.Dan Worth, “Government, GCHQ and O2 team up to created cyber security startup labs,” V3, September 23, 2016, http://www.v3.co.uk/v3-uk/news/2471833/government-gchq-and-o2-team-up-to-create-cyber-security-startup-labs.

41.Matt Burgess, “GCHQ launches cyber security accelerator with Wayra,” Wired, September 26, 2016, http://www.wired.co.uk/article/gchq-wayra-cyber-startup-accelerator.

42.Sean Coughlan, “Cyber-attacks increase leads to jobs boom”, March 26, 2014, BBC News, http://www.bbc.com/news/business-26647795.

43.CESG, “Cyber Security Challenge,” October 17, 2015, https://cybersecuritychallenge.org.uk/education/insights-camps/.

44.GCHQ, “Investing in Cyber,” June 3, 2016, https://www.gchq.gov.uk/features/investing-cyber.

45.UK Cabinet Office, “The UK Cyber Security Strategy Report on Progress and Forward Plans,” (2014): 23.

46.Catapult, “About us,” https://www.catapult.org.uk/about-us-text.

47.UK Government, “Innovate UK: Emerging and Enabling Technologies,” April 7, 2016, https://www.gov.uk/government/collections/innovate-uk-emerging-and-enabling-technologies, and “Horizon 2020: What It Is and How to Apply for Funding,” November 3, 2015, https://www.gov.uk/guidance/horizon-2020-what-it-is-and-how-to-apply-for-funding.

48.“CyLon,” https://cylonlab.com.

49.UK Government, “Foreign Secretary William Hague’s Speech at the Munich Security Conference: Security and freedom in the cyber age – seeking the rules of the

road," February 4, 2011, https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road.

50.Ibid.

51.US Department of State, "Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues," Press Release, June 7, 2013, http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm.

52.NATO CCDCOE, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," August 31, 2015, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html.

53.OSCE, "Permanent Council Decision No. 1106," December 3, 2013, http://www.osce.org/pc/109168.

54.OSCE, "Permanent Council Decision No. 1202," March 10, 2016, http://www.osce.org/pc/227281.

55.UK Cabinet Office, "The UK Cyber Security Strategy 2011-2016: Annual Report," (2016): 15.

56.International Institute for Strategic Studies, "Sino-UK Track 1.5 Dialogue on Cyber Security," October 15, 2014, https://www.iiss.org/en/about%20us/press%20room/press%20releases/press%20releases/archive/2014-dd03/october-a29d/sino-uk-track-15-dialogue-on-cyber-security-1496.

57.UK National Audit Office, "The UK Cyber Security Strategy: Landscape Review," (February 2013): 25, http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf.

58.UK Government, "Cyber Essentials scheme: Overview," April 7, 2014, https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

59.European Council, "EU-wide cybersecurity rules adopted by the Council," May 17, 2016, http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/.

60.Mark Rasch, "Brexit's Potential Impact on Information Security," Security Current, June 27, 2016, http://www.securitycurrent.com/en/ciso_journal/ac_ciso_journal/brexits-potential-impact-on-information-security.

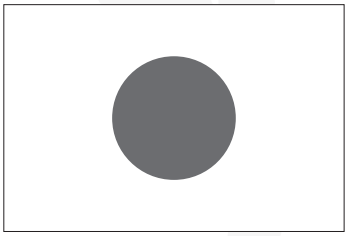
61.UK Government, "National Security Strategy and Strategic Defence and Security Review."

62.UK Government, "Chancellor's speech to GCHQ on cyber security," November 17, 2015, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

63.This new agency replaces an earlier, Cabinet-led, multi-agency version defined by the 2011 U.K. Cyber Security Strategy and set up in 2012. The new Cyber Security

Operation Centre is intended to have a more effective relationship between the computer intelligence expertise at GCHQ and the audiences it is supposed to serve. For more on the new CSOC, see: U.K. Government, "Defence Secretary announces £40 million Cyber Security Operations Centre," April 1, 2016, https://www.gov.uk/government/news/defence-secretary-announces-40m-cyber-security-operations-centre.

日本网络就绪度报告



国家人口	1.27 亿
人口增长率	— 0.1%
GDP 市值（美元）	4.123 万亿美元
GDP 增长率	0.5%
互联网引入年份	1986 年
国家网络安全战略	2013 年发布，2015 年更新
互联网域名	.jp
固定宽带订阅用户（每 100 人）	29.3
移动宽带订阅用户（每 100 人）	121.4
手机订阅用户（每 100 人）	120.2

日本信息通信技术（ICT）的发展程度与连通性排名

国际电信联盟（ITU）ICT 发展指数（IDI）	11	世界经济论坛网络就绪指数（NRI）	10

资料来源：世界银行（2015）、国际电信联盟（2015）、世界经济论坛网络就绪指数（2015）和互联网协会。

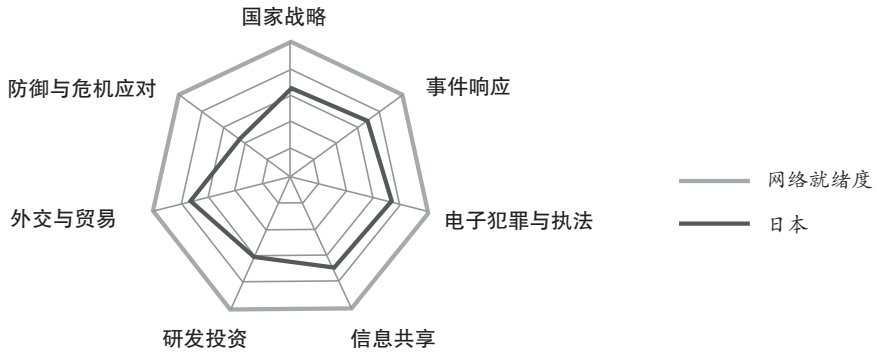
概述

当日本在 20 世纪 80 年代中期首次引入互联网时，最初是作为一项科学学术实验。之后用了近十年的时间，全国各地的家庭和办公室才接入互联网。当今日本是一个高度互联和数字依赖的国家，其国民是全球信息通信技术（ICT）中最为活跃的用户，互联网渗透率高达 90%以上。随着固定线路通信订阅用户的下降，互联的关键驱动因素则是移动通信和移动宽带订阅用户。为缓解移动设备使用量增加面临的瓶颈，日本政府计划在 2017 年之前将分配给天气和业余无线电的频谱进行共享，从而使无线通信的带宽翻倍。

日本政府多年来一直在苦苦挣扎，作为世界第三大经济体，企图摆脱长期的经济停滞。目前，ICT 产业占日本国内生产总值（GDP）的 9%，这比前几年还要低，实际上日本在全球 ICT 市场的份额从 2014 年开始衰退。此外，相比其他亚太地区的稳步增长，日本 ICT 出口大幅降低，从 2012 年的 5%降至 2014 年的 3.3%。日本政府认为 ICT 是促进未来经济增长的一种重要手段。预计到 2020 年，日本 ICT 产业规模将实现翻番，而其中大部分增长要归功于物联网（IoT）。日本政府还宣布了到 2020 年成为世界最先进的信息技术国家的目标，并通过促进开放的数据和研发、世界级的 ICT 基础设施以及更强大的网络安全态势，努力为 ICT 发展营造良好环境 。[1]

然而，网络安全对日本而言并不是一个新问题，安倍首相正在利用日本即将举办的国际会议，如 2016 年七国集团部长级会议、2020 年东京奥运会和残奥会，将网络挑战变成驱动日本安全和韧性能力议程的机会。事实上，安倍首相利用这些会议活动，将网络安全作为国家的一个优先事项，使得发展网络安全能力和韧性尤为紧迫。通过将这些努力与新兴的物联网市场接轨，安倍还将确保日本在更广泛的 ICT 经济市场中占据优势地位。

我们使用网络就绪指数（CRI）2.0 来评估日本的网络风险防护就绪水平。这项分析为日本提供了一个可操作的蓝图，以更好地了解其互联网基础设施的依赖和漏洞，并评估其关于缩小当前网络安全态势与支持其数字化未来所需的国家网络能力之间的差距的承诺和成熟度。基于 CRI 2.0 的七个基本要素，即国家战略、事件响应、电子犯罪和执法、信息共享、研发投资、外交与贸易，以及防护与危机应对，以下是对日本网络安全相关工作和能力的一个综合评估：



国家战略

日本政府自 2006 年发布第一版《信息安全国家战略》[2] 开始，不断修订其国家网络安全战略。2009 年发布了第二版《信息安全国家战略》[3]，2013 年信息安全政策委员会（现为网络安全战略总部）发布其首个国家《网络安全战略》。2015 年 9 月，日本内阁批准了日本《网络安全战略》第二版，这表明了高层领导对网络安全问题的重视程度[4]。2014 年 11 月发布的《网络安全基本法》规定，日本网络安全政策必须遵循以下原则：信息自由流动、尊重公民权利、促进利益相关方模式和开展合作，这些内容均体现在 2015 年发布的战略中。

日本在 2013 年发布首个国家《网络安全战略》，2015 年修订出台第二版。

对比 2013 年战略，新的网络安全战略强调 ICT 带来的机会与风险。日本政府将 ICT 视为通过创新激励经济增长的潜在来源，尤其是随着物联网的发展，同时 ICT 也带来了风险和不安全因素。在很多方面，2015 年网络安全战略所强调的商业契机、创新和物联网，符合日本的 ICT 战略政策议程，即日本“数字议程”，该议程基以多项部级政策为基础，包括日本 ICT 增长战略、日本振兴战略以及成为世界最先进的信息技术国家的宣言。

在 2015 年战略中，日本政府将关键信息基础设施（CII）列为重点优先领域，证实应采取多利益相关方模式确保关键信息基础设施的安全。关键信息基础设施主要行业包括电力、水务、信息通信服务和金融服务等。

2015 年战略指定网络安全战略总部为战略执行权威部门。经过对信息安全政策委员会进行重组，网络安全战略总部成立于 2014 年，是国家网络安全指挥与控制机构，

有权向其他政府机构提供建议。网络安全战略总部由日本内阁官房长官菅义伟领导，成员包括外交部长、国防部长、经济和贸易部长、内政部长，国家公安委员会主席以及由首相指派的其他成员和专家。

最后，暨 2015 年国家网络安全战略之后，日本国家事件就绪和网络安全战略中心（NISC）在 2016 年 8 月发布了《安全物联网系统整体框架》。虽然国家战略已阐明了通过物联网的创新和安全促进经济可持续发展的重要性，但新的框架表明，即使对于包括制造商在内的非关键基础设施，日本也将采取安全措施，并以全球多利益相关方模式来保障物联网安全 。[5]

事件响应

自 20 世纪 90 年代中期以来，日本成立了多个事件响应组织，应对网络紧急情况和危机，最早是在 1996 年成立了国家计算机应急响应小组协调中心（JPCERT / CC）[6]。

随着 2014 年新《网络安全基本法》的通过，原国家信息安全中心的地位得到提升，从 2016 年 3 月起更名为“国家事件就绪和网络安全战略中心（NISC）”，目前作为新的网络安全战略总部（原信息安全委员会）秘书处[7]。《网络安全基本法》规定，NISC 职责包括政策协调、对处理大量个人信息的政府相关组织进行监督，以及当发生对关键基础设施的攻击等危机时进行指挥和控制。

2014 年《网络安全基本法》正式确立了国家事件就绪和网络安全战略中心。

2015 年日本国家网络安全战略强调了多利益相关方模式，这种模式也反映在 JPCERT / CC 的组织架构上，JPCERT / CC 是一家在 2003 年注册的、独立的、非营利性组织，为政府部门和私营机构提供服务。除了与其他 CSIRT、相关政府机构、网络服务提供商、安全供应商和行业协会协调事件响应之外，JPCERT / CC 还通过复杂的通报程序收集网络事件相关信息，并定期发布事件威胁监控报告和事件处理报告。事件处理报告包括各类业务协调案件的日常更新、其他研究、技术文档以及新闻稿[8]。

此外，JPCERT / CC 帮助成立了亚太计算机应急响应小组（APCERT）并担任其秘书处，该小组为与更为宽泛的亚太地区其他 CERT 机构组织开展年度国际网络演练起到了积极作用[9]。JPCERT / CC 还参与了日中韩年度 CERT 会议，讨论网络事件响应机制。日中韩三个国家历史上出现过紧张的局势，会议有助于增进国家间的信心和信任，成果包括建立“网络热线”，就重大的网络事件进行沟通[10]。为筹办 2020 年东京奥运会，日本还组织各有关部门和国家警察局开展网络演练 。[11]

日本正于经济产业省（METI）下设立一个新的运行机构——工业网络安全促进局（ICPA），以保护日本关键基础设施免受网络攻击。新机构将着重依靠“白帽子黑客”来提升关键行业的应急能力，包括电力、天然气、石油、化工和核设施。工业网络安全促进局拟于 2017 年开放，政府希望该机构能够全面运营并为 2020 年奥运会期间国家安全保卫工作做好准备。此外，日本政府近日宣布成立“网络攻击机构”，培训其员工可以防止、减轻和应对关键基础设施网络攻击[12]。该机构预计于 2017 年初投入运营，将成为日本首个专门针对防止电气系统网络事件和敏感发电站设计泄漏的培训中心。该培训机构将作为日本信息技术促进局（IPA）的一部分，目标是在 2020 年东京奥运会和残奥会期间防止潜在的大规模停电事件。

总体来看，日本采取了专项行动解决政府间协调面临的挑战，同时努力使影响事件响应能力的政府行动统一起来。

网络犯罪与执法

日本于 2001 年签署并批准了《欧洲委员会网络犯罪公约》（一般称为《布达佩斯公约》），此后建立了一系列网络犯罪相关立法、国际合作努力和打击网络犯罪的程序。除了承认网络犯罪国际法外，日本还对其刑法进行修改，加入网络犯罪相关行为，并通过了另外几部法律，包括《未经授权计算机访问法》《电讯法》《著作权法》《儿童色情法》《保密信息法》和《电子签名法》[13]。目前，日本正在审议《个人资料保护法》以确保其适用于对个人大数据的使用。近年来，日本执法部门成功地查明、逮捕并起诉了从日本企业非法窃取客户个人资料和商业秘密的本地网络犯罪分子。

日本在 2014 年成立了首个独立的数据保护机构，即个人信息保护委员会（PIPC），并在 2015 年进行改组，使其负责保护所有日本公民的个人身份信息。在设立这一机构之前，16 个不同的部门对政府监管的各个行业实施隐私保护。随着日本开始为所有公民建立国家数字身份从而可以快速准确地查验和核实身份，隐私保护的重要性日益凸显。在 2011 年地震和海啸之后，东京能源公司 Tepco 加快了智能电表部署计划。该公司计划截至 2018 年将智能电表部署到 80% 的客户。此外，日本的 Suica 地铁智能卡等近场通信技术正在被更为广泛地用于非接触式支付，银行也将无线技术用于信用卡和借记卡。

另外，日本于 2006 年创建网络清理中心，旨在提供恶意软件修复和反僵尸网络解决方案[14]。该中心是 JPCERT / CC、安全供应商和互联网服务提供商（ISP）之间跨学科合作的一个成果，并建立了一个针对僵尸网络恶意软件感染和使用的自动“保

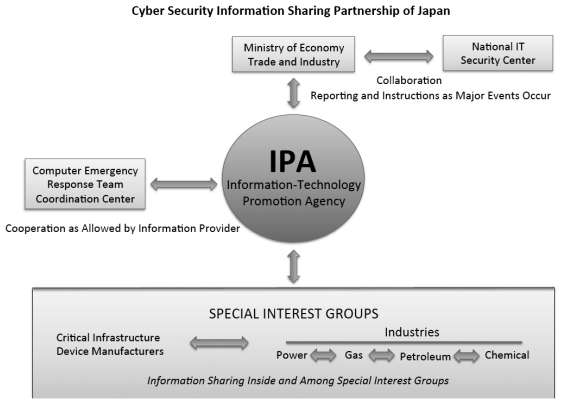
护网”。它还针对个人计算机上的特定恶意软件提供定制化的解决方案。该中心于2011 年解散，其职能转移到日本电信 –ISAC。2013 年，日本遭受攻击，20,000 多个不同的 IP 地址受影响，这表明有必要进一步加强对僵尸网络的整治能力。

信息共享

为了建立协调关系、加强信息共享安排，日本正在采取措施推动建立并扩展公共和私营部门的信息共享网络。这些措施包括基于行政机构和其他组织实体的网络相关知识和经验，提升信息共享和分析功能，例如多个信息共享与分析中心（ISAC）。现在，要求各政府机构都与国家事件就绪和网络安全战略中心密切协调配合，从而与其管辖范围内的组织和业务运营商共享信息，并提供必要的建议。这不仅符合 2015 年新版国家网络安全战略的要求，也与《关键信息基础设施保护基本政策》第三版保持一致，后者再次强调了所有网络空间利益相关方，包括关键信息基础设施运营商、企业和个人，开展协作和信息共享的重要性 。[15]

2014 年《网络安全基本法》正式确立了国家事件就绪和网络安全战略中心。

信息技术促进局（IPA）隶属经济产业省（METI），是推动政府与重点行业之间信息共享的权威机构，并与国内各大公司建立了信任关系 [16]。IPA 负责运营日本网络安全信息共享伙伴关系（J–CSIP），由公私合作，为影响关键基础设施的网络安全事件提供持续性的信息共享平台以及全网范围的响应 [17]。成员包括将与政府协作阻止网络攻击的公司和行业组织。此外，IPA 与 METI、NISC、JPCERT / CC 和网络救援咨询小组（J–CRAT）密切合作，对影响关键基础设施的所有重大网络事件做出响应。



信息技术促进局组织架构图（2016 年）（http://www.ipa.go.jp）

根据 2015 年国家网络安全战略，日本政府拟加强和扩大信息收集与分析功能和活动，从而能够更快、更有效地预见和检测网络空间的威胁。政府计划成立一个极为专业的检测、分析和危机响应小组，从而能够立即发现并响应网络攻击。政府还将为 2020 年奥运会加快成立一个专门的 CERT 作为核心机构，负责为与这一重要的国际事件和其他相关业务的安全管理和运营有重要关联的利益相关方提供信息共享。

研发投资

2011 年发布的《信息安全研究与发展战略》[18] 再次强调了日本政府自 2005 年以来，在研发与技术开发大挑战项目的大纲下，对公共和私人 ICT 技术研发工作的支持。大挑战项目寻求整合长期和短期研发技术项目，重点围绕日本 ICT 安全环境的变化，例如具有创新性的 ICT 技术（如云计算）、复杂和多样化的威胁（如高级可持续威胁 APT）以及面对自然灾害建立韧性 ICT 系统。尽管该项目取得了一定的进展，但 2006 年至 2010 年期间，政府的信息安全预算下降了 47%，从 912.2 亿日元（约合 8100 万美元）降到 48.6 亿日元（约合 4300 万美元）。与其他国家不断增长的研发预算相比，2011 年政府研发战略认为这是一个“令人警醒”的趋势。2013 年，日本国家信息安全中心（现为国家“网络安全事件就绪与网络安全战略中心”）发布的一份报告指出，该国缺少 8 万名信息安全工程师，而目前网络安全从业人员缺乏对抗在线攻击的有效技能[19]。

为筹备 2020 年奥运会，日本总务省要求为网络安全培训提供额外资金。

为筹办七国集团峰会和 2020 年奥运会，日本总务省申请拨款约 200 亿日元（约合 1.78 亿美元），从 2016 财年开始共四年时间用来支持奥运会相关事宜[20]。这笔资金可用于地方政府、学校和企业的培训。总务省将对与奥运会相关的网络攻击演习进行监督。

此外，2013 年网络安全战略强调，将降低税收作为企业激励措施，推动中小企业增加信息安全投入。同样地，2015 年网络安全战略强调了创新对经济的重要性。根据 2014 年的数据，小企业在研发支出上获得 12%的抵免，而大企业获得 8% ~ 10%的抵免。对于专注研发的企业，可以提供更多的税收优惠[21]。这些税收优惠并不仅限于网络安全和 ICT，目前尚不清楚日本对于商业网络研发是否有其他特别的激励措施。

最后，日本在二月份举办了每年一届的全国网络安全宣传活动，目前还推出了其他两项活动来提高网络安全意识：被称为“夏威夷”的密码保护运动，以及被称为“攻壳机动队”的信息运动，该活动通过海报和漫画进行宣传。

外交与贸易

过去十年来，日本一直积极从事与网络安全和 ICT 组件相关的外交和贸易谈判。事实上，日本外交部的《外交蓝皮书》将网络安全列为最为影响国家外交政策的因素之一[22]。为了应对日益加剧的网络安全困扰，外交部近期新成立了网络安全政策司，有 15 个编制，致力于推动网络空间法治建设[23]。外交部计划通过该司就网络空间治理规则相关外交和法律工作，与其他有类似想法的国家进行协调，并支持发展中国家的能力建设举措。

外交部近期新成立了网络安全政策司，致力于推动网络空间法治建设。

日本还定期参加各种涉及网络安全和 ICT 的国际和双边会议。2016 年 2 月，日本签署了跨太平洋伙伴关系协定（TPP），该协定覆盖网络安全、电子商务和加密义务等。目前，日本正在参与区域全面经济合作组织（RCEP）的谈判，其中包括许多与网络有关的提案，如版权、禁止互联网转播广播等。

作为《关于常规武器和两用物品及技术出口控制的瓦森纳安排》缔约国，日本同意限制互联网监控软件以及经特别修改能够规避监控工具或抵制对抗措施的入侵软件的销售。此外，日本积极派员出席日本—东盟信息安全政策会议、日美网络对话、日美互联网经济政策合作对话以及日美防务工作组。最值得注意的是，日本积极参加联合国政府专家组（UN GGE）工作，参与制定全球规范，特别是对《联合国政府专家组关于从国际安全角度看信息和电信领域发展的报告》做出了贡献[24]。2012 年，日本外交部承认国际法适用于网络空间，并且于 2016 年 5 月在日本举办的七国集团（G7）峰会期间再度重申。

防御与危机应对

2013 年和 2015 年发布的日本国家安全战略均强调了网络防御的重要性。2012 年，国防部（MoD）宣布计划成立网络防御部队（CDU），预算 1.42 亿美元、编制 100 人[25]。该部队随后于 2014 年成立。网络防御部队的主要目标是保护信息系统，收集恶意软件以及病毒的有关数据，并确定响应机制。此外，当发生网络攻击和武装攻击联合攻击时，国防部和自卫队（SDF）负责对事件进行响应和处置。日本计划通过与美国密切合作，联合开展网络演练，来扩充这些能力。鉴于安倍政府为修改《宪法》

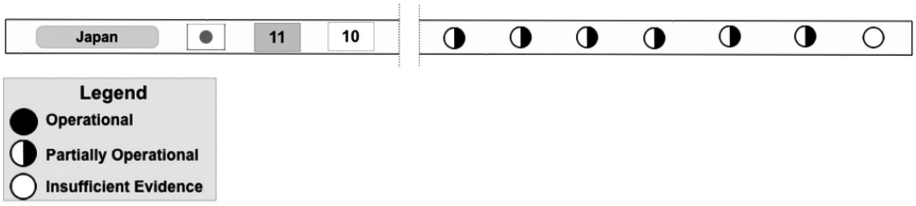
2014 年，日本国防部专门成立网络防御部队，以提升日本国家网络安全态势。

第 9 条关于解禁集体自卫权做出的努力，随着行政部门职能的成熟，自卫队和网络防御部队有可能会扩大其能力范围，为更广义的国家网络安全态势做出贡献。

CRI 2.0 基线

根据 CRI 2.0 评估，日本正走在做好网络就绪的道路上，CRI 的 7 个基本要素目前均为部分运行。

本报告的分析结果反映了日本网络建设动态变化概要。随着日本继续发展，提出新的经济（数字议程）以及国家网络安全战略、政策与倡议，体现日本国家经济愿景和国家安全优先事项相一致的更平衡方法，本报告也将随之更新以反映这些变化并对实质性和显著的改进之处进行关注、跟踪和评估。



注释

1.1 OECD, OECD Digital Economy Outlook 2015, (OECD Publishing: Paris): 21, http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-digital-economy-outlook-2015_9789264232440-en#page1.

2.Japan Information Security Policy Council, "The First National Strategy on Information Security," February 2, 2006, http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

3.Japan National Information Security Policy Council, "The Second National Strategy on Information Security," February 3, 2009, http://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf.

4.Government of Japan, Provisional Translation, "Cybersecurity Strategy," September 4, 2015, http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.

5.Mihoko Matsubara, "Assessing Japan's Internet of Things (IoT) Security Strategy for Tokyo 2020," PaloAlto Networks, September 19, 2016, http://researchcenter.paloaltonetworks.com/2016/09/cso-assessing-japans-internet-of-things-iot-security-strategy-for-tokyo-2020/.

6.JPCERT, "Activities: Incident Response and Analysis," https://www.jpcert.or.jp/english/pr/.

7.Information Security Policy Council, "The Basic Policy of Critical Information

Infrastructure Protection," May 9, 2014, http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf, and Japan National Center of Incident Response and Strategy for Cyber Security, http://www.nisc.go.jp/eng/index.html.

8.JPCERT, "Incident Handling Quarterly Report," https://www.jpcert.or.jp/english/ir/report.html.

9.APCERT, "APCERT Embarks on Cyber Attacks Beyond Traditional Sources," http://www.apcert.org/documents/pdf/APCERTDrill2015PressRelease_Final.pdf.

10.CNCERT/CC, "2nd China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response was held in Korea," www.cert.org.cn/publish/english/55/2014/20140916145739295996084/20140916145739295996084_.html.

11.Tim Kelly and Nobuhiro Kubo, "Japan holds first broad cybersecurity drill, frets over Olympics risks," Reuters, March 18, 2014, http://www.reuters.com/article/us-japan-cybercrime-idUSBREA2G10920140318.

12.Nicky Cappella, "Japanese government plans cyber attack institute," The Stack, August 24, 2016, https://thestack.com/security/2016/08/24/japanese-government-plans-cyber-attack-institute/.

13.Japan National Police Agency, White Paper on Police 2014, https://www.npa.go.jp/hakusyo/h26/english/Contents_WHITE_PAPER_on_POLICE2014.htm, and National Center for Incident readiness and Strategy for Cybersecurity, "Related laws and regulations," http://www.nisc.go.jp/law/index.html.

14.Ministry of Internal Affairs and Communications and Ministry of Economy, Trade, and Industry, "What is Cyber Clean Center", https://www.telecom-isac.jp/ccc/en_index.html.

15.Information Security Policy Council, "The Basic Policy of Critical Information Infrastructure Protection," 2014.

16.Information-Technology Promotion Agency, "About IPA," https://www.ipa.go.jp/english/about/index.html.

17.Information-Technology Promotion Agency, "Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) Annual Activity Report FY2012," (April 2013).

18.Japan Information Security Policy Council, "Information Security Research and Development Strategy," (July 8, 2011).

19.Government of Japan, "Cybersecurity Strategy,"

20.Doug Drinkwater, "Japan to train thousands on cybersecurity pre 2020," SC Magazine, July 22, 2015, http://www.scmagazineuk.com/japan-to-train-thousands-on-cyber-security-ahead-of-2020-olympics/article/427765/.

21."2014 Global Survey of R&D Tax Incentives," Deloitte (2014): 26, https://

www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-global-rd-survey-aug-2014.pdf

22.Japanese Ministry of Foreign Affairs, “Diplomatic Bluebook,” http://www.mofa.go.jp/policy/other/bluebook/.

23.“Foreign Ministry sets up division to push rule of law in cyberspace,” Japan Economic Newswire, July 12, 2016.

24.UNODA, Developments in the Field of Information and Telecommunications in the Context of International Security, https://www.un.org/disarmament/topics/informationsecurity/.

25.Japan Ministry of Defense, “Defense Programs and Budget of Japan: Overview of FY2014 Budget Request,” http://www.mod.go.jp/e/d_budget/pdf/251009.pdf.

印度网络就绪度报告

国家人口	13.11 亿
人口增长率	1.2%
按市价计算的 GDP（当前美元）	2.095 万亿美元
GDP 增长率	7.6%
接入互联网的年份	1986 年（进入）, 1995 年（公众接入）
国家网络安全战略	2013
互联网域名	.in
互联网用户数（每 100 人）	26
固定宽带用户数（每 100 人）	1.3
移动宽带用户数（每 100 人）	5.5
移动手机用户数（每 100 人）	79

信通技术（ICT）发展与网络联接指数排名

国际电信联盟（ITU）信通技术发展指数（IDI）排名	131	世界经济论坛的网络就绪指数（NRI）排名	89

来源：世界银行（2015）、国际电信联盟 ITU（2015）、世界经济论坛的网络就绪指数 NRI（2015）、互联网社会。

概述

在 20 世纪 70 年代，印度电子部（DoE）开始与联合国开发计划署（UNDP）制定战略，将计算机带入印度——这一行动，对于印度社会的信息化和促进经济至关重要。1985 年，国家科学技术中心成立，负责建立了印度第一家互联网服务提供商（ISP），教育研究网络（ERNET）——主要针对学术和研究机构的互联网平台。ERNET 引入“in”扩展名并为印度学术机构提供第一次国际连接[1]。当时接入互联网的三大主要倡议之一就是要连接印度的社会、学界和政府。最初为政府所有的印度计算机维修公司（CMC）在 1977 年转为公共有限公司，由此启动了印度第一个公共网络——INDONET 网络，并于 1986 年开始运营。INDONET 的目标是在国内创建互联基础设施和文化，并最先向公共和私营实体提供电子邮件、文件传输服务、应用程序和数据网络[2]。最终，基于卫星网络的国家信息中心网络（NICNET）将中央政府与州政府和地方管理员连接起来，在人口普查、医疗服务、选举结果、国家政策和其他政府服务方面启用双向信息共享。[3]

1995 年互联网开始普及到印度公众，由此中央政府将互联网作为支持经济增长、创造就业、更高效的政府运作和提高公共服务访问的催化剂。然而，今天印度的互联网普及率仍是亚太地区中最低的，只有 26% 的人口连接到互联网，远落后于中国和巴西等其他大型发展中国家[4]。印度有近十亿人还没有连接互联网，是世界上最大的离线人口国家[5]。但是，2016 年非官方统计数据表明，印度的互联网普及率正在提高[6]。

政府继续推动数字化，向所有的印度人民提供电子政府服务。但是，由于离线人口规模巨大，这些目标仍然难以实现。例如，2006 年印度政府启动了国家电子政务计划（NeGP），启动了 31 项以公众服务为中心的任务模式项目（MMPs），包括养老金、缴纳所得税、银行和保险服务等。虽然许多项目在全国范围得到实施，但 NeGP 最终没有达到预期目标[7]。在过去的十年里，印度持续推动发展这些倡议，在塑造未来的计划中先前的挫折和教训发挥了重要作用。其中，Aadhaar 生物识别方案是一个较为成功的电子政务项目，这是世界上最大的国家身份证号码计划，由印度身份证主管部门（UIDAI）领导[8]。这个生物工具是一个由 12 位数字唯一标识的文件，包含人口和其他生物特征数据的细节，能够向印度居民及时有效地提高福利和服务，现在超过 80% 的人口在使用这一工具[9]。虽然这个计划允许更多的公民访问电子政务服务，但批评人士担心这个大型信息库可能被政府监管所滥用，或是受到犯罪分子的破坏，非法利用这些信息。

把印度变成一个“数字授权社会和知识经济”是当前政府的主要目标之一。总理纳伦德拉·莫迪在2015年的数字战略中提出“数字印度”构想——这项全面经济计划以创造就业为优先任务，通过创新和健壮的通信互联基础设施来实现[10]。由于意识到连通性支撑着经济增长，该计划提出提高电信服务的措施，包括加快宽带部署至少达到50%（目前约为7%），普及移动互联网的接入率，在印度农村地区增加30%（目前约为45%）。如果成功实施，该计划可以产生双重效应：①吸引外国直接投资；②增加高科技出口，进而产生额外9%的GDP增长率（约1800亿美元）[11]。此外，“数字印度”构想鼓励信通技术为医疗部门、知识管理和金融服务等产业创新提供解决方案。该计划有许多其他相关项目，如“印度制造”“技能印度”“创业印度”和“印度站起来”等，旨在进一步鼓励年轻一代和IT行业创新，开发创新的解决方案，促进印度第二大进口产品电子设备的国内生产[12]。印度的这个“数字革命”正是要充分实现信通技术的经济效益。“数字印度”的实施由电子和信息技术部（Ministry of Electronics and Information Technology，MeitY）协调，前身为电子和信息技术部门（Department of Electronics and Information Technology，DeITY）。行动计划包括核心ICT基础设施的建立、拓展和现代化，明确提出特定的里程碑和目标，预计在2018年中完成。

上述这些计划继续将印度定位于ICT全球市场的领导者。2016年，印度ICT行业贡献了1430亿美元的收入，1080亿美元的出口，大约370万人的就业机会。[13]电子商务是印度增长最快的市场，由于公司采用基于本地的电子商务、创新移动平台和在线支付解决方案，自2015年以来电子商务增长了20%（约170亿美元）[14]。由此，一些印度IT服务公司，如Wipro和Infosys逐渐成为世界市场中的全球竞争者，而其他如Flipkart公司（网上购物）、Quikr（在线市场）和Nauki.com（招聘网站）正在成为国内电子商务快速发展空间中的主要参与者[15]。

尽管印度的数字战略拥有产生更大数字红利的潜力，并且已经相当成功地吸引到ICT领域的外国直接投资，但政府尚未使网络安全与经济活动同等优先。网络安全对印度不是一个新问题，政府现在认识到网络安全还可将网络挑战转化为机遇，推动印度ICT的安全和韧性。在启动“数字印度”时，莫迪把网络风险比作“不流血战争的全球威胁”，宣称“印度要在应对全球网络威胁中扮演重要角色”，而且他的国家“可以提供创新和可靠的解决方案……确保整个世界生活在和平之中”[16]。

虽然国家统计数据并不容易获得，但印度连续高居两项国家排名，一是在网络攻击起源国排名中名列第三，仅次于美国和中国；二是在网络犯罪和恶意软件的攻击目

标排名中位居首位。对黑客而言，像印度这样的国家是一个很有吸引力的目标。因为他们经历了 ICT 应用、电子商务活动、网上银行和金融交易的快速增长，但连通性的提高并没有伴随更高的安全意识[17]。印度最高法院委托的一项研究表明，2013 年由恶意软件、身份盗窃和网络钓鱼等网络犯罪造成的损失超过 40 亿美元[18]。2015 年，印度国家安全顾问多瓦尔（Ajit Kumar Doval）将网络安全列为印度面临的主要国内安全挑战之一[19]。

尽管印度提出加强网络安全的相关举措，包括最早从 2008 年的《信息技术（IT）法案》，最近专门成立国家网络安全协调中心（National Cyber Security Coordination Centre，NCCC），到“数字印度”承诺努力建设安全的网络空间[20]，印度的基础设施保障和韧性、法律和监管措施，以及更广泛的经济改革都还没有跟上莫迪总理数字革命的设想。而这些又因印度缺乏一个专业的网络安全劳动力和在线离线人口在数字、教育、收入、性别上的持久差异而被放大。此外，印度 2013 年“国家网络安全政策”缺乏一个实施计划，政府目前大多数政策可以说是“零打碎敲”[21]。批评人士还指出，最近一系列网络间谍攻击表明印度缺乏一个具有弹性的网络和一个协调的安全响应机制[22]。最后，高层的国家安全官员注意到在授权保护印度关键信息基础设施的各机构之间缺少一个综合的途径[23]。总之，在国家级网络风险防范方面，印度仍有很大差距。

印度面临着许多挑战，在前进路上很难将网络安全确定为优先事项。事实上，印度的主要目标是保护法律、秩序和安全。过去和持续的挑战一直主导着国家安全议程，包括当前感知到的与分离主义、宗派主义、恐怖主义和军事有关的威胁[24]。改善国家的网络安全态势需要投入足够的资源，以及提升其对未来印度国家和经济安全的重要性。

网络就绪度指数 2.0 评估了印度应对网络安全风险的准备水平。这种分析为印度提供一个可行的蓝图，以便更好地理解其对互联网基础设施的依赖性及脆弱性，评估其是否拥有足够的责任和成熟度，来弥合当前网络安全态势和支撑数字未来的国家网络能力之间的差距。

对国家网络安全相关努力和能力的全面评估主要基于网络就绪度指数 2.0 中的七个基本要素，包括国家战略、事件响应、电子犯罪和执法、信息共享、研发投资、外交和贸易，防御和危机应对。

国家战略

2010 年，印度政府的国家安全委员会、国家安全顾问委员会（NSAB）和其他高

层办公室遭到一系列引人注目的计算机入侵事件。通过应对这些事件，政府创建了网络防御和准备部际工作组，由印度的技术情报机构——国家技术研究组织（NTRO）主持相关工作[25]。这也是印度在网络防御方面最早采取的多利益相关方措施。

网络防御和准备部际工作组帮助制定印度的网络政策和未来组织。2013 年，电子和信息技术部门（the Department of Electronics and Information Technology, DeITY）升格为电子和信息技术部（Ministry of Electronics and Information Technology，MeitY），并在 2016 年发布第一份“国家网络安全政策”。该网络安全战略指出，互联网普及已经成为支持印度经济增长和社会发展、提升就业机会、提高生活水平的催化剂。并强调印度政府在推动 ICT 应用所发挥的作用，包括公共服务（如政府—公民的服务、公民身份和公共分配系统）、医疗（如远程医疗、远程咨询和移动服务）、教育（如：在线学习和虚拟教室）、金融服务（如移动银行和支付网关）等领域。文件总结了 ICT 普及率的提高带给印度的好处，但也警告不安全网络空间存在的固有风险有能力“减损国家资源”和“破坏公众对国家及其基础设施的信心”[26]。该文件清楚表达了印度的前景目标是“为公民、企业和政府建立一个安全有弹性的网络”[27]。确保网络空间弹性和信任的目标还包括：加强监管框架确保安全的网络安全生态系统；加强和创建国家和行业水平获取网络威胁信息的 24 x7 机制；建立 24 x7 国家关键信息基础设施保护中心（NCIIPC）；到 2018 年创建拥有 5 万人的网络安全劳动力。文件提出了 15 个其他目标和相关行动领域，比如创建安全的网络安全生态系统；开发确保安全的框架；鼓励开放标准；促进关键信息基础设施的保护和弹性；创建网络安全意识。在许多方面，文件显得雄心勃勃，因为它提出了明确的目标和行动项目，但没有提供实施计划或者实现这些目标的行动指南。

该战略呼吁成立中央国家机构，负责协调印度所有与网络安全相关的事项。然而，尽管成立国家安全委员会秘书处（National Security Council Secretariat，NSCS）作为中央网络安全协调机构，负责协调网络安全和互联网治理，但是在电信部门内，通信和信息技术部是负责国家级网络安全政策实施的机构[28]。

2015 年印度设立并配备了国家网络安全协调员职位。利用机构的知识优势，该职位由前 MeitY 的印度计算机应急小组（CERT）前主管担任。协调员定位在总理办公室，也是新成立的国家网络协调中心（National Cyber Coordination Center，NCCC）主任，隶属于 MeitY 之下。NCCC 的任务是协调公共和私营部门，包括情报机构、执法、互联网服务提供商和行业，共同缓解网络威胁的影响，促进网络威胁情报共享并评估可能流入网络的恶意信息。财政部已经为其运行拨款 1.3 亿美元，但 NCCC 仍然处于

能力建设和人员组建当中，从技术的角度来看，目前还不清楚它将如何开展所指定的活动和任务 。[29]

结合国家经济发展远景和国家安全需求，印度更新了国家网络安全战略。虽然印度政府尚未对外公布该战略，但阐述了网络安全的九项核心原则：①促进和平与稳定；②多利益相关方的方法；③支持投资联合国政府专家组（UN GGE）；④能力建设和研发；⑤计算机应急小组之间的技术合作和标准制定；⑥促进经济增长；⑦执法人员之间的合作；⑧支持网上自由；⑨数据和隐私保护 。[30]

此外，印度政府已认识到信息通信技术的运用带来的益处和威胁。2013 年的“国家网络安全政策”和 2015 年“数字印度”都积极阐述了作为印度经济增长的主要推动力，互联网连接和信息通信技术发展的重要性。但是，“数字印度”旨在提高在公民服务中 ICT 的渗透和应用，而国家网络安全战略则完全专注于确保印度信息基础设施和建设网络安全意识。因此，直到数字印度和网络安全战略达成协调一致，印度才可能实现支撑其数字未来所需的经济承诺和国家安全保障。

事件响应

2008 年 IT 修正案（70A 条款）提出设立“国家节点代理”的政府机构，用于关键信息基础设施保护，修正案（70B 条款）将这个角色分配给印度计算机应急小组（CERT-In），负责“保护印度网络空间。”[31]

然而直到 2014 年，当印度的工业控制系统到处发现有恶意软件[32]，当时的 DeITY （现在的电子和信息技术部，MeitY）正式宣布成立国家关键信息基础设施保护中心（NCIIPC）作为负责关键行业的专职机构，隶属于国家技术研究组织（NTRO）。政府将关键信息基础设施定义为“一些设施、系统或功能，其能力受到破坏或者中断会损害一国的国家安全、治理、经济和社会福祉”[33]。能源、交通、银行和金融、电信、制造、国防、执法、电子政务和水资源等 12 个行业处于 NCIIPC 的管理范围[34]。这种整合公私部门的政府组织授权是值得关注的——它提供了进一步信息共享和协作的机会。国家关键信息基础设施保护中心（NCIIPC）的主要职责包括：确定下级的关键行业；签发网络安全警告和建议的日报和月报；执行恶意软件分析和网络取证；跟踪恶意软件和僵尸网络；提高网络安全意识和培训；24 x7 小时运行的帮助平台[35]。为帮助关键信息基础设施提供商更好地应对网络事件，在其确定的关键行业范围内，国家关键信息基础设施保护中心（NCIIPC）在每个组织或部门都设有“节点官员”或计算机信息安全官（CISO），作为 NCIIPC 的主要联络点。

印度 CERT 成立于 2004 年，如今作为国家中央机构负责网络事件响应、跨部门协调，并采取积极措施降低联邦政府和州政府、行业和学界的网络风险。印度 CERT 也是服务于公共部门和关键信息基础设施的咨询机构，并努力为所有企业开发网络安全标准[36]。

2008 年修正案和 2014 年 IT 规则赋予印度 CERT 更广泛的目标，包括收集、分析和通报网络事件信息；预测和发布网络安全事件警报；提供处理网络安全事件的应急措施；协调网络事件反应活动；发布与信息安全实践、程序、预防、响应和事件报告相关的行动指南、警告、脆弱性笔记和白皮书；网络安全相关的其他功能[37]。

随后，印度 CERT 发布框架文件，记录并跟踪其达成 2008 年 IT 修正案所述目标的进展情况，每个目标都配套有相关的成功行动和措施。自框架文件发布以来，印度 CERT 更新了网络危机管理计划（CCMP），以应对网络攻击和网络恐怖主义，以及影响国家重要资产、危及公共安全和国家安全的其他网络相关事件。此外，印度 CERT 正在进行关键基础设施安全审计；举办行业、国家和国际级别的网络安全演习；签订与其他国家和行业 CERT 合作的正式协议。印度 CERT 也利用媒体广告来提高公民意识和提供额外的网络意识培训[38]。

此外，印度 CERT 建立了安全警报系统，在其网站上发布潜在网络威胁和漏洞的每日“警告”和“脆弱性笔记”，分发给印度 CERT 服务名单上的订阅用户[39]。印度 CERT 还发布年度报告，包括僵尸网络跟踪培训工作组的小结和关于网络相关事件的统计[40]。最后，为应对不断增加的网络欺诈事件和数字交易的潜在不安全性，印度财政部长 Arun Jaitley 最近宣布成立专门的印度金融业 CERT（CERT–Fin），以加强印度金融体系的安全性和韧性[41]。

在 2015—2016 财年，印度政府分配 ₹85（约 1360 万美元）给以下三项活动：印度 CERT、网络上诉法庭[42] 和网络安全研发（R&D）[43]。

电子犯罪和执法

由于认识到网络犯罪的严重性和影响，印度政府通过和更新了一些规定，以便更好应对网络犯罪和信息技术基础设施的安全漏洞。2000 年的 IT 法案——尔后在 2008 年修订，为印度政府提供了解决一系列网络安全相关挑战的广泛的法律框架，包括：“惩罚篡改计算机源文件”（第 65 条款）；“惩罚通过通信服务发出进攻信息等”（第 66A 条款）；“惩罚以电子形式出版或传播淫秽材料”（第 67 条款）；在其他网络犯罪中，“为了网络安全，授权通过任何计算机资源，监控和收集流量数

据或信息的权力”（第 69 B 条款）[44]。2008 年法案的修正案通过后，印度最高法院讨论了防止“攻击性材料”传播的合法性。2015 年最高法院推翻了第 66 条款，认为其违宪，指出法律已被各州警察广泛滥用来逮捕在网上就社会政治问题和政治领导发表批评的无辜人士[45]。

此外，根据 2000 年法案（第 84 条款），印度政府采用了“国家加密政策”。2015 年印度政府公布了由前 DeITY（电子和信息技术部门）专家小组制定的政策草案。草案强调在网络安全、网络犯罪和合法拦截之间存在一些技术和制度上的重叠。文件中关于针对所有公民使用加密服务的一些解释引发了广泛批评，例如 WhatsApp 需要储存 90 天纯文本格式的加密通信，否则将面临潜在的执法行动。而且，政策还指出电子商务网站有义务保持用户自交易之日起 90 天的纯文本数据和加密文本数据[46]。批评结果是印度政府在政策发布后一天就将其删除了，并声明文件“只是草案，而不是政府观点”。[47]然而，推动创建“国家加密政策”草案的一些安全关切也推动印度建立中央监控系统（CMS），进行“合法拦截和监视通信以解决……国家安全方面的担忧”。[48]但是，许多执法官员还不完全了解在 2008 年信息技术法案下的裁决权力，成功的网络犯罪调查和起诉仍缺乏搜查、抓捕、取证数字证据的标准程序[49]。

为帮助提高能力和理解科学、技术、政策及法律的交叉问题，印度政府建立了一系列培训中心。例如，位于班加罗尔的印度大学国家法学院的网络法律和审查的先期研究、发展和训练中心，致力于法律术语和技术术语的互译，向司法官员、检察官、调查机构、网络安全人员、技术人员和其他人员提供培训和教育。在 DeITY 的资金支持下，该中心提供独特的实习培训组件[50]。此外，政府通过公私伙伴关系——印度数据安全委员会（DSCI）[51]和国家软件服务公司协会（NASSCOM）[52]，在孟买、班加罗尔、浦那和加尔各答建立了网络实验室[53]。实验室主要用于执法官员和行业伙伴的使用网络安全和取证培训。到目前为止，已有 4 万 9 千人接受了 DSCI 网络实验室“跨印度计划”的训练[54]。此外，在 MeitY（电子和信息技术部）的最初支持下，印度大学法律学院建立网络法律中心和网络取证实验室，对网络执法机构进行网络法律和网络取证方面的定期培训。

民政部（MHA）也提倡提高应对网络犯罪和网络不安全感的国家能力。民政部门发布咨询报告，建议州政府建立应对网络犯罪所需的技术能力，包括对网络犯罪进行检测、注册、调查和起诉的专业人员培训。因此，在印度每个州的警察现代化计划框架下，民政部门正在筹建网络犯罪警察局（CCPS）和网络犯罪调查和取证培训设施（CCIFTC），并已经在喀拉拉邦、阿萨姆邦、米佐拉姆邦、那加兰邦、阿鲁纳恰

尔邦、特里普拉邦、梅加拉亚邦、曼尼普尔邦、查谟和克什米尔建立了网络取证培训和调查实验室。政府还在海德拉巴的国家警察学院（NPA）建立了用于网络犯罪调查的先进设施，帮助训练负责打击网络犯罪的警察[55]。

印度中央调查局（CBI）——调查违反法律的中央领导机构，从两种不同角度评估网络犯罪：一是计算机犯罪的方法，另一种是计算机犯罪的目标。由此，中央调查局成立了各种不同部门帮助打击网络犯罪。中央调查局有网络犯罪研发部门、网络犯罪调查部门和网络取证实验室（包括数码影像中心）和网络监控中心。中央调查局也有一个单独的经济犯罪部，领导调查与银行和金融服务相关的网络犯罪[56]。中央调查局的网络犯罪调查部门成立于2001年，拥有一个核心人员团队，经常与美国联邦调查局（FBI）、国际刑警组织和其他国家的警察部队对接[57]。

2016年，政府投资₹400（约6400万美元）建立印度网络犯罪协调中心（IC4），隶属于民政部的“网络控制中心”，负责监视“儿童色情和网上恶意破坏”。[58]2016年12月印度政府开始建立清理僵尸网络和恶意软件的分析中心（Cyber Swachhta Kendra），该中心属于印度CERT的一部分。僵尸网络中心与互联网服务提供商一起检测僵尸网络，提醒设备受感染的软件用户，并指导他们按照印度CERT网站推荐的流程删除恶意软件，清除感染[59]。该项目是“数字印度”的一部分，启动资金为₹100（约1600万美元）[60]。

由于意识到网络安全的重要性，并将其作为数字包容和电子政务的重要前提，各州政府发起了应对网络犯罪和数据盗窃的相关项目。例如，马哈拉施特拉邦政府已启动预算为₹1000（约1.5亿美元）的“网络马哈拉施特拉邦”项目[61]，其他州如Andhra Pradesh[62]和Telangana[63]紧随其后。在国际层面，印度政府与其他国家和国际组织开展合作，以减少网络犯罪。印度已经与不同国家签署了39项多边司法互助条约（MLATs），通常包括在签署国家间的网络犯罪信息交换，以便达成更快的事件反应和起诉罪犯。民政部的国际安全第二部门是处理境外犯罪信息请求的中央机构，包括网络犯罪。中央调查局最近成立了一个7成员机构，确保响应多边司法互助的所有请求[64]。

尽管如此，印度没有签署欧洲委员会的《网络犯罪公约》（俗称《布达佩斯公约》）。拒绝《布达佩斯公约》的原因是公约第32 b条款允许成员国访问或接收另一个成员国存储的计算机数据，发出请求的成员国应该获得合法和自愿的同意。印度认为这是对一个国家主权的侵犯[65]。尽管印度尚未成为上海合作组织（SCO）“确保国际信息安全领域合作协议”的正式成员，但为了全面加入上海合作组织，印度政府官员2016年与上合组织元首理事会国家签署了“谅解备忘录义务”。印度的成员国

资格可能会在 2017 年 6 月阿斯塔纳的上合组织成员国领导人峰会中被接受。作为其加入上合组织的一部分，印度将必须接受上合组织成员国在过去 15 年里已经通过的所有文件，也将包括“确保国际信息安全领域合作协议”[66]。

信息共享

如前所述的 2008 年 IT 修正案 （第 70 b 条款），印度 CERT 被指定为紧急事件反应的国家机构，包括网络事件的收集、评估和信息共享[67]。印度 CERT 负责 24 X7 小时共享关于网络攻击、漏洞、解决方案和网络危机管理的相关信息。此外，国家关键信息基础设施保护中心（NCIIPC）负责与关键基础设施机构及其关键部门共享恶意软件的分析和其他信息[68]。尽管印度没有国家信息共享政策，但 2013 年的“国家网络安全政策”将信息共享作为一个关键战略领域，强调信息共享和合作的重要性。国家网络安全战略强调三个主要行动领域：① 发展与其他国家在网络安全领域的双边和多边关系；②增强与安全机构、CERTs、军队、执法和司法系统的国家和全球合作；③建立关于网络安全技术和操作的产业对话机制，包括关键信息基础设施在内，促进系统恢复和弹性方面的努力[69]。

此外，2013 战略指出创建国家级信息共享机制的重要性，及时交换威胁信息。前国家网络安全战略发布两年后，印度政府留出 ₹775（约 1.24 亿美元）在 5 年内创建国家级机制，旨在构建现实和潜在网络威胁的态势情景，促进信息共享[70]。

尽管数量有限，但印度政府和行业之间的信息共享已有实例。2010 年印度中央调查局（CBI）与国家软件服务公司协会（NASSCOM）、印度数据安全委员会（DSCI）签订了谅解备忘录（MoU），促进执法部门和行业之间在新兴技术、安全标准和最佳实践的信息共享[71]。虽然这是一个重要倡议，但是在 2012 年，印度数据安全委员会（DSCI）和印度政府共同发布报告，指出强调公私信息交换是不够的，要建立“参与私营部门的网络安全的联合工作组”。文件提出了建立公私伙伴关系的路线图，倡导建立相关制度和机制，促进公私部门之间的融合与协调。文件还概括指出，私营部门希望在不同领域建立信息共享和分析中心（ISACs），在操作级别上与行业的 CERT 实现合作[72]。

随后，2014 年印度储备银行（Reserve Bank of India）的银行技术开发和研究所，仿照美国金融业的工业安全咨询委员会（FS–ISAC），成立了印度银行风险和威胁分析中心（IB–CART）。该中心的主要目标包括：发布和促进成员间相关的、可操作的威胁信息共享，以确保公众对银行业的持续信心；援助行业资源，以帮助整个行业的

网络态势感知和提前预警；进行研究和情报收集，向成员发布现实威胁或威胁演变的提醒。迄今为止，银行风险和威胁分析中心（IB-CART）在印度已吸引 90 多家机构，至少 60 家国有、私有和外资银行[73]。尽管其他私有的、实时的网络安全威胁情报网在金融服务业使用更为广泛，但银行风险和威胁分析中心（IB-CART）总有一天会成为工业安全咨询委员会的未来模型，例如电力[74]和石油行业[75]。

研发投资

印度 2013 年国家网络安全战略（“国家网络安全政策”）概述了印度致力于网络安全研发，以实现短期、中期、长期的经济和政策目标。战略提出研发的行动领域列表，包括值得信赖的系统开发（如整个系统生命周期的测试、部署和维护）；用研发促进定制的、高收益的、本土解决方案，以应对未来出口的网络安全挑战；促进学术界和产业界对尖端技术与安全研究的联合研发。

由于应用到国家安全，MeitY（电子和信息技术部）进一步认识到本土网络安全研发的重要性。面对发达国家先进的产品和系统的出口限制，自主研发可以使印度开发量身定制的解决方案和产品。政府的科学技术路线图倡导自主研发，并以此作为手段来保护其 ICT 供应链不受操纵。此外，印度对进口产品表示了关切，因为它相信这些产品带来隐藏的安全威胁。”[76]

MeitY（电子和信息技术部）也注意到私营部门在短期研发中发挥的重要作用——导致可用的商业产品。尽管印度已成为世界上计算机和信息服务第二大出口国，在电子商务上正在取得重大进步，但是私营企业仍然面临着挑战[77]。例如，在经商创业舒适度、施工许可证、执行合同和纳税方面，世界银行给印度的排名比较低[78]。此外，不稳定的电力和宽带服务的质量问题在过去也是一个障碍，特别是对网络安全领域研发而言。这些约束继续影响当地的企业家和跨国公司在印度开展业务的兴趣，但是总理莫迪承诺将解决这些问题[79]。例如，“数字印度”的公私合作关系推出名为“eBiz”的用户友好网站，为用户提供更容易的创业能力[80]。此外，2013 年国家软件服务公司协会（NASSCOM）发起了 1 万项创业项目（创业仓库）。这个倡议仿照“启动智利”，旨在创建初创公司创始人一起工作的微生态系统，分享最佳实践。创业仓库建在加尔各答，得到西孟加拉邦政府（部门）和印度小型工业银行大约 3,500 万美元的启动资金。创业仓库由国家软件服务公司协会（NASSCOM）构思设计，现在已得到全球超过 35 家公司的支持，包括 Google、科塔克银行、日立、IBM、英特尔、微软、索尼、惠普。至少 8 个其他州政府跟随加尔各答新建和孵化创业中心。他们意识到这个活动的经济潜力和

重要性，能够让全球市场接触到印度企业家，从而也让印度连接到全球市场[81]。

除了培养有利的商业环境，印度还计划通过能力建设、技能发展和培训，到2018 年建立一个拥有 50 万熟练工人的更专业的网络安全劳动力[82]。特别是 MeitY 发起了一项广泛的信息安全教育和意识（ISEA）项目，旨在满足该国的人力资源需求、政府人员训练、提高网络安全意识和创建国家信息安全课程资源库[83]。它还设立专项拨款管理框架，征集各 ICT 领域研发的建议，诸如加密和密码分析、网络和系统安全、安全架构、脆弱性和保障、监控、监视和取证[84]。

此外，印度很多大学都提供各种各样的网络安全相关课程和学位课程。著名的印度理工学院（IITs）提供本科、研究生和博士学位培养项目，学生可以专注于网络安全和与网络相关问题的研究。许多大学设有网络安全的本科和硕士学位课程，如孟买的印度理工学院、班加罗尔的 M.S. Ramaiah 理工学院（MSRIT）和 SJES 管理研究学院、加尔各答的 Jadavpur 大学和新德里的 K.K. 莫迪国际学院[85]。最近，坎普尔的印度理工学院成为最大的学生网络安全挑战赛的一部分，该竞赛测试学生的信息安全知识，包括从硬件到软件，从渗透测试到保护、数字取证和政府政策[86]。虽然新一代学生可以用到学术编程，但离开大学的学生却不一定具备了行业所需的必要技能[87]。

因此，行业正在努力建设网络能力。例如，2015 年国家软件服务公司协会（NASSCOM）发起“NASSCOM 网络安全工作组”，旨在使印度成为网络安全的研究、训练和产品中心，预计到 2025 年创造 350 亿美元的市场[88]。印度数据安全委员会（DSCI）还打算训练至少一百万网络安全专业人士，建立 1,000 个成功的网络安全相关公司[89]。印度发展数字化社会和知识经济的愿望需要对网络安全基础研究、应用研究、更广泛的大学计划等方面保持强劲的投资，以此缩小人才可用性和劳动力需求之间的差距。

外交和贸易

印度外交部（MEA）将网络安全作为一级外交政策因素之一，这些年印度一直积极从事与网络安全相关的外交贸易和商务谈判。外交部的政策规划联合秘书担任网络问题主任，负责与第三国的谈判协定。外交部设有电子政务和互联网技术部（EG&IT），完全致力于网络安全，配备 4 名永久代表[90]。外交部还设有一个全球网络问题部门，负责追踪国际事务对国内政策的影响，并且代表印度在国外的网络安全利益[91]。

在塑造网络空间国际准则的国际舞台上，印度一直非常活跃。印度国家安全顾问多瓦尔，称网络空间为“全球公域”，在外交或冲突中需要新的方法和新的规范[92]。

为进一步推动网络外交议程，印度参与了各种国际论坛的多边讨论，包括国际安全与信息通信技术的联合国政府专家（UN GGE），加强合作的联合国委员会科学技术工作小组，联合国毒品和犯罪办公室可扩展政府间网络犯罪工作组[93]。印度政府一直认为“网络安全是全球安全的首要议题”，并且强调印度应对网络威胁的承诺。

此外，印度一直参加与许多国家的高层双边和多边网络对话，包括澳大利亚、加拿大、中国、德国、法国、日本、肯尼亚、俄罗斯、韩国、美国、英国和阿拉伯联合酋长国。虽然印度在网络安全和互联网治理的关键问题上采用了不同方法，但印度有时看上去似乎是支持一派的立场也支持另一派立场。例如，2016 年 4 月印度、俄罗斯和中国的三边外交会谈后发布的声明似乎表明印度支持多边网络治理问题[94]。此外，2016 年 9 月印度和美国之间签署的“美印网络关系框架”协议指出，两国致力于互联网治理的多利益相关方模式。该协议承诺两国就网络威胁和其他共同关心的问题进行信息交流；促进两国在合作执法和网络犯罪问题上的双边合作；协调网络能力建设的努力；支持一个开放、互联、安全、可靠的网络空间；鼓励网络空间负责任的国家行为[95]。

虽然印度工商部门没有将 ICT 和网络安全问题列为对外贸易政策的一个顶级要素[96]，但是印度正在推进其数字议程，并在许多其他经济论坛和贸易谈判中关注网络安全问题。例如，印度是金砖四国峰会的活跃成员国。在 2015 年第七届金砖国家峰会上，巴西、俄罗斯、印度、中国和南非的领导人解决共同关心的问题，优先加强和扩大金砖国家内部合作。该组织强调，体现《联合国宪章》的国际法原则的重要性，特别是政治独立、领土完整、国家和主权平等、不干涉别国内部事务以及对人权和基本自由的尊重[97]。对于潜在的故意滥用 ICT 技术威胁国际和平与安全，印度表示深切关注。2016 年，在印度果阿举办的第八届金砖国家峰会上，印度呼吁公共和私人部门投资基础设施，特别是连续性的投资，以确保可持续的长期增长[98]。领导人强调了他们经济伙伴关系的重要性，主张在基础设施方面建立融资桥梁，确定新开发银行（NDB）的任务[99]——该多边开发银行由印度在 2012 年第四次金砖国家峰会上提出，2015 年正式成立，旨在由金砖国家、新兴经济体和发展中国家推进可持续发展项目。印度代表被任命为第一任银行行长，而且印度将举办下届新开发银行理事会年会和 2017 年第一届金砖国家贸易会。

印度还认识到地区全面经济伙伴关系（RCEP）对其未来的战略重要性。目前处于最后几轮谈判的地区全面经济伙伴关系，是一个亚太地区的自由贸易协定，包括东盟地区 10 个经济体（文莱、柬埔寨、印度尼西亚、老挝、马来西亚、缅甸、菲律宾、新加坡、泰国和越南）和 6 个自由贸易伙伴国（澳大利亚、中国、印度、日本、新西

兰和韩国）。参与地区全面经济伙伴关系的 16 个国家占全球国内生产总值（GDP）的近 30%，出口超过世界的四分之一。在 2016 年 11 月的部长会议上，印度说服其他国家将商品、服务和投资等不同部分进行打包谈判[100]。如果印度成功，地区全面经济伙伴关系将成为世界上最大的区域性贸易集团[101]。其目标是降低贸易壁垒、促进经济技术合作、保护知识产权、鼓励竞争、促进争端解决、改善出口商品和服务的市场准入。地区全面经济伙伴关系也给印度提供了平台，影响其在亚太地区的战略和经济地位，实现其“东向政策”。尽管谈判没有最后完成，但贸易措施已包括数据保护措施、知识产权、版权例外的限制规则和出于国家安全目的的数据主权要求等要素。

虽然印度政府认为网络安全是其外交政策的一个顶级要素，但是外交部持续人手不足，很难解决外交和贸易中广泛的网络问题。鉴于网络安全政策的重要性，该问题可能对印度日益凸显。

防御与危机应对

印度政府有四家网络安全机构负责国家网络防御：总理办公室、内政部、电子信息技术部和国防部。国家技术研究组织（NTRO）——仿照美国国家安全局的模式——在总理办公室的行政控制下专门负责技术研究和情报收集。该组织成立于 2004 年，对卫星和陆上互联网通信进行战略监测。该组织是印度技术资产的首要储备，包括侦察卫星、无人机系统和侦察飞机，负责向政府其他机构提供关于内部和外部安全问题的技术情报[102]。此外，国家密码学研究和开发研究所（NICRD）负责向国家技术研究组织（NTRO）报告工作。NICRD 成立于 2007，主要设计和开发用于国家安全的加密产品。该研究所也是亚洲第一家试图建立服务于国家安全的网络安全和信息安全专家库[103]。国家技术研究组织（NTRO）还向非盈利组织——印度联盟小组提供资金资助，该小组由印度领先的信息安全专家和研究人员组成，经常提出网络相关问题方面的政策建议。

内政部（MHS）负责印度内部安全，在它的行政控制下有一系列组织授权执行网络防御任务。情报局（IB）是首要的情报机构，负责国内安全。尽管在情报局可以公开的信息有限，但是内政部 2015 年同意情报局创建“网络安全架构”，或者说是一支侧翼，独立于国家技术研究组织开展工作。这支侧翼计划编制 500 人，打击“伊斯兰国”（ISIS）等恐怖组织的网上极端主义行为[104]。此外，新成立的国家网络协调中心（NCCC）将协调情报、执法和防御部门间近实时的态势感知和对网络安全事件的快速响应。该协调中心（NCCC）将在一个集中位置对主要互联网服务提供商不同网

关路由器的互联网流量数据进行收集、整合和扫描分析，以便提供主动的网络威胁检测和国家层面的防御。然而，正如前面提到的，目前还不清楚 NCCC 将如何把网络安全威胁情报分享给公共和私人实体，分享到什么程度，从而减轻威胁。

在国防部（MoD）内部，在武装部队之外，主要有两个机构执行网络安全相关任务。国防情报局（DIA）将三军情报——陆军、空军和海军——整合为军方可操作的信息。国防情报局下设国防信息战处，负责处理与信息战相关的所有要素，包括心理作战、网络战、计算机网络安全和电磁频谱作战[105]。此外，国防研究与开发组织（DRDO）主要负责国家安全所有相关领域的研发、测试和评估，包括网络安全。除了基础设施外，国防研究与开发组织（DRDO）还参与设计、开发、生产最先进的传感器、武器系统和军事平台。在一个项目中，国防研究与开发组织（DRDO）建设了两个靶场用于测试电子武器系统[106]。

虽然在军队没有单个的国家级组织负责国家的网络防御，但每个军种都在各自的军事条令中包含有网络防御——有时甚至是进攻。2004 年“印度陆军条令”是公开发表的最新条令，定义了 7 种不同形式的信息战；然而，它并没有明确指出陆军需要具备这种作战能力[107]。2009“印度海上条令”也提供了信息战的高级定义，包括电子战和欺骗。然而与陆军条令不同的是，海军条令把电子战确定为印度海军的关键任务，跟港口防御、水雷战和其他更传统的海军职责平齐[108]。最后，除了网络战之外，2012 空军条令还定义了防御性和进攻性信息作战。印度空军（IAF）概括了其受到的关键网络威胁，包括基础设施的攻击、复杂的恶意软件和其他基于硬件和软件的威胁。最后，印度空军承认网络空间带来多重挑战，也带来潜在的作战效益，印度空军需要为未来建立一个“明确的路线图”[109]。

除了官方条令之外，每个军种都在努力为未来冲突情景增强网络能力。2005 年印度陆军建立了网络安全企业，以确保师级的网络安全并进行安全审计。陆军还在通信工程军事学院建立了网络安全实验室[110]，并在其情报团内设立两个部队，以应对针对陆军网络和人员的外国网络间谍活动。在位于 Viskahapatnam 的东部司令部遭受网络攻击后，印度海军成立了独立的网络战士部队——首个军种建立这样的结构[111]。此外，据报道，印度政府 2014 年批准了“加强印度网络空间网络安全框架”，但目前还没有对外公开。该框架包括防务部门组建网络作战中心（COCs），由此每个军种都建立了临时网络作战中心[112]。印度联合参谋总部（The Indian Headquarters Integrated Defense Staff）也负责所有三军的信息安全和相关网络项目[113]。尽管为发展网络能力作出了这些努力，但武装部队几乎没有采取行动以合作途径发展网络安全和作战能力。

在经历了一系列针对海军东部司令部和国防研究与发展组织（DRDO）的网络破坏之后，印度陆海空三军参谋长提交了一份草案，建议在国防部建立三军联合网络战司令部。虽然提案草案于 2013 年提交，但国防部仍未决定是否建立专门的网络司令部[114]。

CRI 2.0 基线

根据 CRI 2.0 评估，印度仍处于向着网络弹性和网络准备发展的早期阶段，在 7 个 CRI 基本要素中，目前只有一个处于部分操作中。

分析结果反映了印度当前不断变化的格局。印度持续制定并更新其经济（数字）议程、国家网络安全战略、政策及各项举措，寻求国家经济愿景与安全重点工作之间的平衡。国家概况的变化反映出国家在各个方面发生的变化，有利于监测、跟踪并评估印度社会所取得的显著进步。

CRI 2.0 利用全面、可比较、基于经验制定的方法论，帮助国家领导人在网络化、竞争激烈、冲突丛生的世界中做出规划，打造安全、有活力的数字世界。

如需了解更多 CRI 2.0 的相关信息，请参阅：http://www.potomacinstitute.org/academic-centers/cyber-readiness-index。

注释

1. BiswarupSen, “Digital Politics and Culture in Contemporary India: The Making of an Info-Nation,” (New York, NY: Routledge, 2016): 71-72.

2. Ibid.

3. Institute for Defense Studies and Analyses, “IDSA Task Force: India’s Cyber Security Challenge,” (March 2012): 19.

4. International Telecommunications Union, “Percentage of individuals using the internet,” (2015).

5. World Bank, “World Development Report 2016: Digital Dividend,” Washington, DC: World Bank (2016): 7-8

6. “India Internet Users,” Internet Live Stats, July 1, 2016, http://www.internetlivestats.com/internet-users/india/.

7. Ministry of Communications and Information Technology, “National e-Governance Plan,” http://meity.gov.in/content/national-e-governance-plan.

8. Unique Identification Authority of India, “UIDAI Background,” https://uidai.gov.in/about-uidai.html.

9. Unique Identification Authority of India, “UIDAI Background,” https://uidai.

gov.in/about-uidai.html.

10.Ministry of Electronics and Information Technology (MeitY), "Digital India: About the Programme," http://www.digitalindia.gov.in/content/about-programme,and "Digital India: Programme Pillars," http://www.digitalindia.gov.in/content/programme-pillars.

11.This is based on a World Bank report that noted that that a 10 percent increase in mobile and broadband penetration can deliver increases in per capital gross domestic product of 0.81 percent to 1.38 percent, respectively in developing countries. For statistics, see: Deloitte, "Digital India: Unleashing Prosperity," Deloitte (2015): 3.

12."Digital India: PM Modi Says India Can Play a Big Role in Cyber Security Globally," July 2, 2015, NDTV,http://www.ndtv.com/india-news/digital-india-pm-modi-says-india-can-play-a-big-role-in-cyber-security-globally-777319.

13.NASSCOM, "IT-BPM Overview," http://www.nasscom.in/indian-itbpo-industry.

14.NASSCOM, "IT-BPM Overview," http://www.nasscom.in/indian-itbpo-industry.

15.DhruvaJaishankar, "Internet Freedom 2.1: Lesson's from Asia's Developing Democracies," German Marshall Fund (March 2015): 13.

16.Digital India: PM Modi Says India Can Play a Big Role in Cyber Security Globally," July 2, 2015, NDTV.

17.Venkatesh Ganesh, "India Lagging in Cyber Security Awareness," The Hindu BusinessLine, August 29, 2016, http://m.thehindubusinessline.com/info-tech/india-lagging-in-cyber-security-awareness/article9046626.ece.

18."Cyber frauds cost India $4 billion," The Hindu, October 23, 2013, http://www.thehindu.com/business/Economy/cyber-frauds-cost-india-4-billion/article5261594.ece.

19.Press Trust of India, "Internal Security Will be a Big Challenge for India: AjitDoval," NDTV, October 31, 2015, http://www.ndtv.com/india-news/internal-security-will-be-a-big-challenge-for-india-ajit-doval-123873 .

20.Department of Electronics and Information Technology, "Digital India," http://www.cmai.asia/digitalindia/pdf/Digital-India-DeITY-Details.pdf.

21.Dilip Kumar Mekala, "The government needs to be more serious about India's cyber security," Force, July 2015, http://forceindia.net/MuchtoWorryAbout.aspx.

22.AbhishekBhalla, "Modi government gets cracking on cyber espionage," Mail Today, June 28, 2016, http://indiatoday.intoday.in/story/modi-govt-gets-cracking-cyber-espionage/1/702377.html .

23.[SD Pradhan, "Cyber security: Need for an overall national cyber strategy," The Times of India, January 18,2016,http://blogs.timesofindia.indiatimes.com/ChanakyaCode/cyber-security-need-for-an-overall-national-cyber-strategy/.

24.DhruvaJaishankar, "Internet Freedom 2.1: Lesson's from Asia's Developing

Democracies," German Marshall Fund (March 2015): 8.

25.[Vijay Mohan, "Fresh wave of cyber attacks hits India", The Tribune, February 11, 2016, http://www.tribuneindia.com/2010/20100212/main7.htm .][Pukhraj Singh, "Thinking Offensively!",Seminar: The Monthly Symposium, October, 2016, http://www.india-seminar.com/2013/650/650_pukhraj_sing.htm .

26.Ministry of Communications and Information Technology, "National Cyber Security Policy," Department ofElectronics and Information Technology(July 2, 2013): 2.

27.Ibid, 3.

28.For an organizational overview of the Ministry of Communications, see: Department of Telecommunications, "Organizational Structure," http://www.dot.gov.in/about-us/organizational-structure.

29.GeethaNandikotkur "India Opens Cyber Coordination Centre" April 13, 2015, http://www.bankinfosecurity.asia/india-opens-cyber-coordination-centre-a-8100 .

30.Melissa Hathaway's interview with Arvind Gupta, Deputy National Security Advisor, at the Cyber 360: A Synergia Conclave, Bangalore India, September 29, 2015.

31.The Gazette of India, "The Information Technology Act of 2008," Indian Ministry of Law and Justice, (February 5, 2009): 14, http://meity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf.

32.Pukhraj Singh, "In Cyberspace Warfare, India is Still Shooting in the Dark", The Quint, February 26, 2016, https://www.thequint.com/opinion/2016/02/25/in-cyberspace-warfare-india-is-still-shooting-in-the-dark .

33.MukteshChander, "National Critical Information Infrastructure Protection Centre (NCIIPC)," National Technical Research Organisation, http://www.slideshare.net/CERCatIIITD/national-critical-information-infrastructure-protection-centre-nciipc.

34.MukteshChander, "National Critical Information Infrastructure Protection Centre (NCIIPC)," National Technical Research Organisation, http://www.slideshare.net/CERCatIIITD/national-critical-information-infrastructure-protection-centre-nciipc.

35.National Technical Research Organisation, "National Critical Information Infrastructure Protection Centre (NCIIPC): Role, Charter, and Responsibilities," http://www.slideshare.net/CERCatIIITD/national-critical-information-infrastructure-protection-centre-nciipc.

36.Indian Computer Emergency Response Team, "Welcome to CERT-In," http://www.cert-in.org.in.

37.The Gazette of India, "The Information Technology Act of 2008," (February 5, 2009), and "The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013," (January 16, 2014), http://meity.gov.in/sites/upload_files/dit/files/G_S_R%2020%20(E)2.pdf .

38.[Department of Information Technology, “RFD: Results-Framework Document for ICERT 2011-2012,” (2012), http://www.cert-in.org.in/Images/CERT-In_RFD2011-12.pdf.

39.Indian Computer Emergency Response Team, “Welcome to CERT-In,” http://www.cert-in.org.in.

40.Indian Computer Emergency Response Team, “Annual Report,” http://www.cert-in.org.in.

41.PTI, “Cashless push: Computer Emergency Response Team to check cyber frauds,” The New Indian Express, February 1, 2017, http://www.newindianexpress.com/business/union-budget-2017/2017/feb/01/cashless-push-computer-emergency-response-team-to-check-cyber-frauds-1565845.html.

42.The Cyber Appellate Tribunal allows any person that may be aggrieved by an order by the Controller of Certifying Authorities, or by an adjudicating officer, to file an appeal before the Tribunal. For more information, see: Ministry of Electronics and Information Technology, “Cyber Appellate Tribunal,” http://meity.gov.in/content/cat.

43.Government of India, Ministry of Communications and Information Technology, “Unstarred Question No: 4671, Answered On: 22.04.2015, Budgetary Allocation to Counter Cybercrime, Bharatendra Singh,” LokSabha, (April 22, 2015).

44.Ministry of Law, Justice, and Company Affairs, “The Information Technology Act, 2008,” LokSahba (2008), http://www.tifrh.res.in/tcis/events/facilities/IT_act_2008.pdf.

45.AmitChoudhary and DhananjayMahapatra, “Supreme Court strikes down Section 66A of IT Act which allows arrests for objectionable content online,” The Times of India, March 24, 2015, http://timesofindia.indiatimes.com/india/Supreme-Court-strikes-down-Section-66A-of-IT-Act-which-allowed-arrests-for-objectionable-content-online/articleshow/46672244.cms.

46.“National Encryption Policy draft withdrawn: 13 things to know,” The Times of India, September 22, 2015, http://timesofindia.indiatimes.com/tech/tech-news/National-Encryption-Policy-draft-withdrawn-13-things-to-know/articleshow/49056912.cms.

47.“Criticisms forces government to roll back its draft encryption policy,” The Indian Express, September 23, 2015, http://indianexpress.com/article/india/india-others/government-withdraws-draft-national-encryption-policy-after-furore/.

48.Press Information Bureau, “Surveillance System,” Government of India, March 9, 2011, http://pib.nic.in/newsite/erelease.aspx?relid=70747.

49.[ArunabhSaikia, “Why most cybercrimes in India don’t end in conviction,” Live Mint, July 29, 2016, http://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html.

50.Advanced Center for Research, Development, and Training in Cyber Laws and Forensics, “Academic Programs,” National Law School of India.

51. 印度数据安全委员会（DSCI）是一个行业组织，其成立是为了促进数据保护，并且为使用信息系统的所有印度工业部门开发和实践安全和隐私的最佳实践。DSCI 由国家软件和服务公司协会（NASSCOM）成立。

52. 国家软件和服务公司协会（NASSCOM）是一个贸易协会，覆盖印度信息技术和业务流程外包行业。

53.Data Security Council of India, “Cyber Labs,” https://www.dsci.in/taxonomypage/283.

54.Melissa Hathaway’s interview with NandkumarSaravade, CEO of the Data Security Council of India (DSCI) Mumbai, India, September 22, 2015.

55.Ministry of Communications and Information Technology, “Unstarred Question No: 5763, Answered On: 29.04.2015, Cyber Training, Janardan Singh Sigriwal,” LokSabha, (April 29, 2015).

56.Internet Democracy, “Watchtower: Mapping the Indian Government’s Cyber Institutions,” https://internetdemocracy.in/watchtower/ and Central Bureau of Investigation, “Divisions in CBI,” http://cbi.nic.in/aboutus/div.php.

57.PrashantBakshi, “Security Implications for a Wired India: Challenges Ahead,” Strategic Analysis (2001): 114.

58.Press Trust of India, “New cyber-control hub to check pornography, online trolls”, The Times of India, July 18, 2016, http://timesofindia.indiatimes.com/india/New-cyber-control-hub-to-check-pornography-online-trolls/articleshow/53269223.cms .

59.CERT-In, “Welcome to Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra), http://www.cyberswachhtakendra.gov.in.

60.“Government facility in 3 months to clean malware from mobiles, PCs,” The Economic Times, May 24, 2015, http://economictimes.indiatimes.com/tech/software/government-facility-in-3-months-to-clean-malware-from-mobiles-pcs/articleshow/47404157.cms.

61.PriyankaPugaokar, “MahaGovt Invests 1000 Cr In ‘Cyber Maharashtra’ Project,” ChannelTimes.com, August 28, 2016, http://www.channeltimes.com/story/maha-govt-invests-1000-cr-in-cyber-maharashtra-project/ .

62.Sridhar Raavi, “AP - First in India to have 24X7 Cyber Security”, Mirchi9, November 30, 2014, https://www.mirchi9.com/politics/ap-first-in-india-to-have-24x7-cyber-security/ .

63.Express News Service, “Telangana government formulates cyber security policy”, The New Indian Express, Sep-tember 16, 2016, http://www.newindianexpress.com/states/telangana/2016/sep/16/Telangana-government-formulates-cyber-security-policy-1520023.html .

64.Ministry of External Affairs, “Mutual Legal Assistance Requests,” http://www.

mea.gov.in/mlatcriminal.htm.

65.Council of Europe, “Convention on Cybercrime,” Council of Europe (2001): 20.

66.PTI, “India likely to join Shanghai Cooperation Organisation within a year,” The Indian Express, June 14, 2016, http://indianexpress.com/article/india/india-news-india/india-likely-to-join-shanghai-cooperation-organisation-within-a-year-2852341/.

67.The Gazette of India, “The Information Technology Act of 2008,” 14.]

68.[Indian Computer Emergency Response Team, “Welcome to CERT-In,” http://www.cert-in.org.in and National Technical Research Organisation, “National Critical Information Infrastructure Protection Centre (NCIIPC): Role, Charter, and Responsibilities,” http://www.slideshare.net/CERCatIIITD/national-critical-information-infrastructure-protection-centre-nciipc.

69.Ministry of Communications and Information Technology, “National Cyber Security Policy,” Department ofE-lectronics and Information Technology (July 2, 2013): 9-10.

70.Government of India, Ministry of Communications and Information Technology, “Unstarred Question No: 4671, Answered On: 22.04.2015, Budgetary Allocation to Counter Cybercrime, Bharatendra Singh,” LokSabha, (April 22, 2015).

71.DSCI, “CBI, NASSCOM-DSCI signs MoU to fight Cyber Crimes,” November 23, 2010, https://www.dsci.in/node/529.

72.DSCI and Government of India, “Recommendations of Joint Working Group on Engagement with the Private Sector on Cyber Security,” (2012), https://www.dsci.in/sites/default/files/Data%20Security%20Council%20of%20India%20(DSCI)%20-Recommendations%20of%20JWG.pdf.

73.Institute for Development and Research in Banking Technology, “Indian Banks-Center for Analysis of Risks and Threats (IB-CART),” http://www.idrbt.ac.in/ib-cart.html.

74.The Indian Ministry of Power in its overview of the power sector includes: coal, gas, oil, hydro, nuclear, and renewable power sources. Ministry of Power, “Power Sector at a Glance ALL INDIA,” http://powermin.nic.in/en/content/power-sector-glance-all-india.

75.Government of India, Ministry of Communications and Information Technology, “UnstarredQuestionNo: 91, Answered On: 14.07.2014, CyberAttackTerrorism, Bhartruhari Mahtab HansrajGangaramAhir, Lok Sabha, (July 14, 2014).

76.Ministry of Electronics & Information Technology, “Strategic Approach,” http://meity.gov.in/content/strategic-approach.

77.World Trade Organization, “International Trade Statistics 2015,” World Trade Organization (2015): 140.

78.World Bank Group, “Ease of Doing Business in India: 2016 data,” http://www.doingbusiness.org/data/exploreeconomies/india/.

79.DhruvaJaishankar, “Internet Freedom 2.1: Lesson’s From Asia’s Developing

Democracies," German Marshall Fund (March 2015): 15.

80.Ministry of Commerce and Industry, "Welcome to e-Biz," https://www.ebiz.gov.in/home/.

81.Melissa Hathaway's interview with Ravi Ranjan, Managing Director of Start-up Warehouse, Kolkata, India, September 24, 2015, and "1000 Start-ups" http://10000startups.com/

82.Ministry of Communications and Information Technology, "National Cyber Security Policy," Department ofE-lectronics and Information Technology (July 2, 2013): 4.

83.Information Security Education and Awareness (ISEA), "About ISEA," http://isea.gov.in/isea/home/index.jsp .

84.Ministry of Electronics and Information Security, "Call for R&D project proposals in Cyber Security area," http://meity.gov.in/sites/upload_files/dit/files/in%20Cyber%20Security%20area.pdf.

85.Shiksha, "Cyber Security/IT Security Courses in India," http://it.shiksha.com/it-cyber-security-courses-in-india-categorypage-10-127-1-0-0-1-1-2--none-1-0.

86.Virendra Singh Rawat, "IIT Kanpur to host global cyber security challenge," Business Standard, August 8, 2016, http://www.business-standard.com/article/current-affairs/iit-kanpur-to-host-global-cyber-security-challenge-116080801015_1.html.

87.Venkatesh Ganesh, "India lagging in cyber security awareness," The Hindu BusinessLine, August 29, 2016, http://m.thehindubusinessline.com/info-tech/india-lagging-in-cyber-security-awareness/article9046626.ece.

88."Nasscom task force to make India hub for cybersecurity research," ETTelecom, May, 26, 2015 和梅丽莎·海瑟薇对 Venkathesh Murthy 的采访，其任国家印度大学法学院网络安全法律和取证的先进研发和培训中心，DSCI 网络实验室主任，班加罗尔，印度，2015 年 10 月 1 日。

89. 梅丽莎·海瑟薇对印度数据安全理事会的首席执行官（DSCI)NandkumarSaravade 的采访，孟买，印度，2015 年 9 月 22 日。Remarks by NandkumarSaravade at the Cyber 360: A Synergia Conclave, Bangalore India, September 29, 2015.

90.Ministry of External Affairs, "About Us: Administration," http://mea.gov.in/divisions.htm.

91.Internet Democracy, "Watchtower: Mapping the Indian Government's Cyber Institutions," https://internetdemocracy.in/watchtower/.

92.Full speech by AK Doval at the annual Hindustan Times Summit, held in November 2014, https://www.youtube.com/watch?v=eccxX_H_8OQ.

93.Ministry of External Affairs, "Annual Report 2013-2014," Ministry of External Affairs (2014): xviii.

94.Indian Ministry of External Affairs, "Joint Communiqué of the 14th Meeting of the Foreign Ministers of the Rus-sian Federation, the Republic of India and the

People's Republic of China," April 18,2016,http://mea.gov.in/bilateral-documents.htm?dtl/26628/Joint_Communiqu_of_the_14th_Meeting_of_the_Foreign_Ministers_of_the_Russian_Federation_the_Republic_of_India_and_the_Peoples_Republic_of_China.

95.U.S. Embassy & Consulates in India, "Framework for the US-India Cyber Relationship," https://in.usembassy.gov/framework-u-s-india-cyber-relationshi

96.Ministry of Commerce and Industry, "Welcome to the Department of Commerce," http://commerce.nic.in/DOC/Index.aspx.

97."Ufa Declaration," 7th BRICS Summit, Ufa, Russian Federation, July 9, 2015, http://mea.gov.in/Uploads/PublicationDocs/25448_Declaration_eng.pdf.

98."GOA Declaration," 8th BRICS Summit, Goa, India, October 16, 2016, http://brics2016.gov.in/upload/Goa%20Declaration%20and%20Action%20Plan.pdf .

99.New Development Bank, "Genesis," http://ndb.int/genesis.php .

100.KirtikaSuneja, "RCEP countries agree to Indian demand on services, investment negotiation," The Economic Times, November 8, 2016, http://economictimes.indiatimes.com/news/economy/foreign-trade/rcep-countries-agree-to-indian-demand-on-services-investment-negotiations/articleshow/55305824.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst .

101.AsitRanjan Mishra, "India to talk tough at RCEP trade meet," Live Mint, November 2, 2016, http://www.livemint.com/Politics/mOzWKi4gvcNzK7KkBTqJWI/India-to-talk-tough-at-RCEP-trade-meet.html .

102.RS BediVrC, "NTRO: India's Technical Intelligence Agency," Indian Defence Review, April 23, 2015, http://www.indiandefencereview.com/spotlights/ntro-indias-technical-intelligence-agency/

103.[Ashok Das, "Key security outfit now near Hyderabad," Hindustan Times, May 7, 2007, http://www.hindustantimes.com/india/key-security-outfit-now-near-hyderabad/story-UZz98GoeIXjaHheFU6CfKK.html, Internet Democracy, "Watchtower: Mapping the Indian Government's Cyber Institutions," https://internetdemocracy.in/watchtower/ .

104.Vijaita Singh, "MHA nod for cyber security wing under the IB," The Indian Express, June 18, 2015, http://indianexpress.com/article/india/india-others/mha-nod-for-cyber-security-wing-under-ib/.

105.VinodAnand, "Debate," Institute for Defence Studies and Analyses: Journal of Defence Studies (2008), http://www.idsa.in/jds/2_2_2008_IntegratingtheIndianMilitary_VAnand.

106.Center for Strategic and International Studies, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Organization and Doctrine," UNIDIR Resources (2011): 74.

107.Headquarters Army Training Command, "Indian Army Doctrine," (October 2004): 20-22.

108. Indian Navy, “Indian Maritime Doctrine: Naval Strategic Publication 1.1,” (2009): 52 and 92, http://www.indiannavy.nic.in/sites/default/files/Indian-Maritime-Doctrine-2009-Updated-12Feb16.pdf.

109. Indian Air Force, “Basic Doctrine of the Indian Air Force, 2012,” (2012): 131-134.

110. Center for Strategic and International Studies, “Cybersecurity and Cyberwarfare: Preliminary Assessment of National Organization and Doctrine,” UNIDIR Resources (2011): 72.

111. “Indian Navy creates exclusive cyber warriors cadre,” Deccan Herald, July 12, 2012, http://www.deccanherald.com/content/263791/indian-navy-creates-exclusive-cyber.html.

112. Security Risks, “Security Issues with South Asia: Cyber Security Threats Enhanced,” Security Risks Monitor, December 3, 2014, http://www.security-risks.com/security-issues-south-asia/iw-cyber-security/cyber-security-threats-enhanced-3936.html.

113. Indian Air Force, “Basic Doctrine of the Indian Air Force, 2012,” (2012): 132.

114. VivekRaghuvanshi, “India Still Unsure on Need for Cyber Command,” DefenseNews, December 8, 2014.

荷兰网络就绪度报告

国家人口	1690 万人
人口增长率	0.4%
市场价格 GDP（美元）	7502.84 亿美元
GDP 增长率	2%
引进互联网年份	1982
国家网络安全战略发布	2011, 2013
互联网域名	.nl
每 100 名用户中，互联网用户量	93.1
每 100 名用户中，固定宽带用户量	41.7
每 100 名用户中，移动电话用户量	124

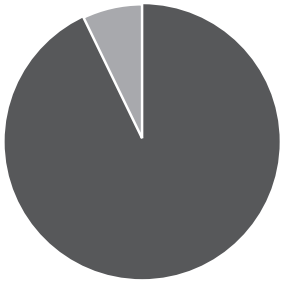
信息通信技术（ICT）发展和连通性排名

国际电信联盟（ITU）信息通信技术发展指数（IDI）	8	世界经济论坛网络就绪度指数（NRI）	6

数据源：世界银行（2015）、国际电信联盟（2015）、世界经济论坛网络就绪度指数（2015）和 Internet Society.

概述

早在 1982 年，欧洲 UNIX 网络（EUnet）首先在荷兰引入了互联网服务的早期实例，包括电子邮件和一个名为 USENET 的公告板系统。这些最初的连接给荷兰国家数学和计算机科学研究所（Centrum Wiskunde & Informatica, CWI）的科学家们以灵感，他们建立了欧洲第一个在传输控制协议 / 互联网协议（TCP–IP）上运行的光纤网络，加速了互联网的发展。然而，这第一个互联网基础设施并不属于荷兰政府总体战略计划的一部分，而是由那些相信互联网机遇的科学家提出的一项自下而上的倡议。数学和计算机科学研究所及其母组织——荷兰科学研究组织（NWO）——看到了互联网的巨大潜力，并培育了这个新生的网络，最终使 NLnet 得以建立。尽管最初互联网标准的缺乏阻碍了全球通信，但是荷兰在 1988 年 11 月与美国建立连接，后成为了全欧洲的关键互联网门户之一。



荷兰互联网渗透率：93.1%

在接下来的 10 年里，荷兰和许多其他国家一样，认识到电信自由化是以更低成本为消费者提供普遍接入的必要条件。荷兰在成为欧洲的互联网门户上看到了战略价值，并在 20 世纪 90 年代初，建立了阿姆斯特丹互联网交换中心（AMS–IX）这一非盈利、中立且独立的互联组织。今天，阿姆斯特丹互联网交换中心通过向互联网服务提供商（ISPs）、国际运营商、移动运营商、内容提供商、网络主机和云服务提供商、应用提供商、电视广播公司、游戏公司以及其他相关公司提供专业互联服务，连接了 800 多个通信网络。该交换中心已经扩展到 4 个，很快就会扩展到 5 个，是目前世界上最大的互联网交换中心。

有了这些历史基础，在欧洲速度最快、最强大的一些宽带连接的帮助下，荷兰已经成为世界上技术最先进、连接最紧密的国家之一，成为全球连接程度最高的 10 个国家之一。它的互联网普及率超过 93%，超过 95% 的家庭接入了互联网。此外，荷兰在网上银行领域占据领先地位，接受率超过 80%，其公民和企业组成了欧洲第四

大电子商务市场。荷兰的信息通信技术（ICT）贡献了近乎 5% 的荷兰国内生产总值（GDP），该国是全球信息通信技术产品和电信服务十大出口国之一（尽管近年来荷兰信息通信技术服务的全球出口份额有所下降）。2015 年，据估计，荷兰广义数字经济占荷兰经济总量的 22.9% 或 1580.1 亿欧元（约 1722 亿美元），预计到 2020 年，这一数字将达到 25% 或 1904 亿欧元（约 2075 亿美元）。

然而，荷兰不仅仅是欧洲的互联网门户。鹿特丹是欧洲最大的港口，阿姆斯特丹史基浦机场是世界上国际旅客和货物最多的机场之一。荷兰政府明白这两个商贸门户（鹿特丹和史基浦机场）的重要性并正在加强其行业关系，以增强其安全姿态。因此，荷兰意识到，尽管它的领土和人口数字相对较小，但是随着国家间的联系越来越紧密，其经济的未来会变得更加依赖数字，它也必须解决网络安全问题，成为一个“能够安全做生意的地方”。

要成为“最适合”做生意的国家，现在可能比以往任何时候都重要，在英国决定退出欧盟后，荷兰有机会成为英国和欧洲之间的桥梁，帮助英国与欧洲过渡。欧洲各地民粹主义运动的不断增加，使荷兰有机会将自身宣传为一个政治相对稳定的国家。

荷兰为实现其雄心勃勃的 2011—2015 年数字战略——《数字议程》（Digital Agenda）建立了基础。数字战略强调，荷兰必须“更明智地利用信息通信技术推动增长和繁荣，促进创新和经济增长”。与 2010 年欧洲数字议程（European Digital Agenda）——《欧洲 2020 战略》（Europe 2020 Strategy）七大主要内容之一——相符合，荷兰的数字战略确定了重点和具体行动，以促进信息通信技术的更广泛使用，增强高速宽带的连通性，促进互联网自由和开放，移除“互联网中的国际贸易壁垒”，这将“可能使欧盟的 GDP 增长至少 4%”。在设定目标后，荷兰的数字战略认为其数字化未来有着双重责任：经济进步和支撑经济的信任与韧性。经济进步的实现，可以通过接受信息和通信技术、创新、基础设施的现代化以及物联网（IoT）。然而，要实现这一增长潜力，荷兰的基础设施必须更有韧性，互联网及通过网络空间进行的交易必须是安全可信的。

荷兰数字战略认为，要从信息通信技术所有的可能性中获益并“提高荷兰的竞争力”，其前提条件是：①安全、有保障且可靠的信息通信基础设施；②用户信赖的“开放且可访问的高速互联网”；③“用户群拥有使用信息通信技术所需的数字技能”。数字战略认识到了国家安全和经济健康之间的直接联系，警告说“实施解决互联网安全威胁的措施很有必要，它可以防止由于缺乏信心而导致的阻碍接受信息通信技术，这会限制经济增长和创新的步伐”。2016 年 7 月，荷兰政府向议会提交了一份报告，

表示 2011 年数字战略中的许多目标和目的已经达成，并附上了有关“创新、信任和加速”的《2016—2017 年度数字议程》（2016—2017 Digital Agenda）。虽然之前数字战略的重点主要是加强先决条件，使每个人都能从信息通信技术中获益，使荷兰政府进一步数字化（如为公民和企业开放的电子政府服务），2016 年更新版的数字战略包含了一种全面的方法，其范围也更广泛，旨在进一步推动医疗和机动等其他部门的数字化。新的国家数字战略预计将于 2018 年由新政府公布，增加的资金可能被用于创新和网络安全。

然而，与许多欧洲国家一样，荷兰也面临着很多网络犯罪、工业间谍活动、关键服务中断以及其他恶意的网络活动。2010 年，一项由荷兰应用科学研究组织（Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek, TNO）进行的研究估计，荷兰因网络犯罪导致的损失至少为 100 亿欧元（约 110 亿美元）——相当于本国 GDP 的 1.5% 至 2%（德勤于 2016 年 4 月发布过类似统计，强调荷兰最相关的经济部门中，有至少 100 亿欧元面临网络犯罪和恶意活动的风险）。为了应对网络威胁日益增长的范围、数量和复杂性，荷兰政府表示将保护数字投资的价值并维护国家和经济安全。2010 年，荷兰议会要求起草一篇《全国网络（防御）战略》——被称为《国家网络战略制定修正案》（Amendment Knops to Create a National Cyber Strategy）。因此，荷兰安全与司法部门协调了一项政府整体措施，从而于 2011 年 2 月颁布了荷兰第一个《国家网络安全战略：通过合作取得成功》（National Cyber Security Strategy: Success Through Cooperation）。

这一战略任命安全与司法部长领导政策协调，由国家安全与反恐协调员（NCTV）负责执行。战略还呼吁建立国家网络安全中心（NCSC），作为公私伙伴关系的平台，向国家安全与反恐协调员报告。最后，该战略主张成立荷兰网络安全理事会（Dutch Cyber Security Council）作为国家和战略咨询机构。当荷兰面临第一次已知网络危机时，这一战略接受了考验。事件发生于 2011 年 6 月，地点为 DigiNotar——一个荷兰的证书颁发机构，它发行的加密密钥用于为“安全”通信创建数字（签名）证书，特别用于荷兰政府的域名。DigiNotar 的公司网络服务器被成功攻破，黑客获得了系统管理权，发行了伪造证书，这破坏了荷兰政府通信的完整性、真实性和安全性。DigiNotar 的伪造证书也被用于其他国家，双因素验证的真实性受到怀疑。这一事件不仅提高了整个荷兰政府的安全意识，也影响了公民对在互联网上开展业务以及与政府分享信息的信心。此外，这一事件加速了国家网络安全中心的创建和运营，中心于 2012 年 1 月开始运营。

在 DigiNotar 危机之后，荷兰政府开始修订其网络安全策略，采用了基于风险的方法，以平衡对荷兰利益的保护、对利益的威胁和可接受的社会风险为基础。它采用的是每一个荷兰人都知道的事件管理原则——水位管理与海平面抑制。1953 年大洪水过后，政府启动了“三角洲计划”，该计划将一种全国方案制度化，每一个公民都有保护荷兰的责任，通过警告和警报系统监测水位并抑制海平面。2013 年，荷兰公布了其第二个战略，名为《国家网络安全战略 2：从意识到能力（NCSS2）》，扩大了国家的网络安全视野，使其超越技术和孤立的网络事件。策略试图将水位管理的责任感用于网络安全，提倡每一个公民都有责任确保国家的抗打击性，防止和遏制来自互联网的威胁，保证网络可行性、信任度和韧性，使其作为货物、服务、资本和跨国界数据自由流动的平台。21 世纪的《数字三角洲计划》（Digital Delta Plan）同时聚焦内外部。它还建立了网络安全、经济和社会进步、自由和隐私之间的三角关系。第二个国家网络安全战略包含了一个 38 项行动计划，计划完成时间为 2016 年底。

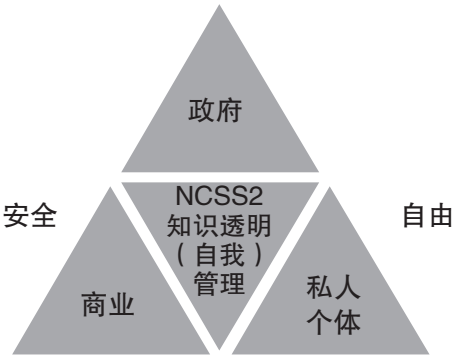


图 1.《国家网络安全战略（NCSS 2）：从意识到能力》

在 DigiNotar 危机之后，与《国家网络安全战略 2》的制定同步，荷兰国防部（MoD）开始公开讨论其在网络防御方面的作用，并计划投资增强网络战争能力，即使其他领域的预算削减。基于 2012 年《网络防御策略》中已经详细体现出的意图，荷兰重申了其增强军事行动和进攻能力的意图，并宣布在荷兰国防部内建立一个专门的网络防御司令部（Defense Cyber Command）。这一司令部的建立有助于发展各种强有力的能力，目标为早期检测、主动防御以及必要时的干预。此外，国防部最近成立了专门的安全操作中心（Security Operation Center），显示了其在网络空间内和通过网络保卫国防部和荷兰经济的作战决心。此外，荷兰政府一直在努力确保网络安全在其情报和安全社区内的优先级，扩展能力并提供额外的工具和权力，调查并打击高级网络攻击。

荷兰了解要为合法、必要、均衡的网络操作留出足够的空间，并仍在探讨两个草案——一个将修改情报和安全服务相关法律，另一个将给予警察和其他调查队伍在没有搜查令的情况下远程侵入嫌疑人电脑的特殊权力。

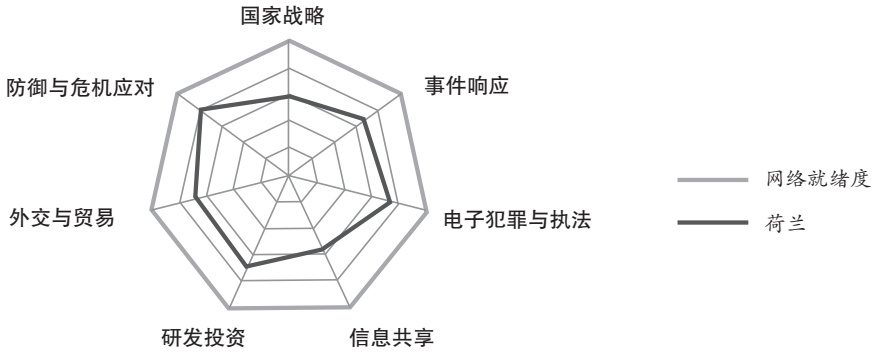
2015 年，荷兰首相马克·吕特承认，该国正面临“严重网络安全挑战”，并鼓励国内外合作伙伴，包括公司、大学和其他国家的政府“共同努力……确保互联网保持自由、开放和安全……以维持我国的繁荣、人民的隐私和生活质量”。然而，尽管已经出台了两次网络安全策略，建立了服务于全国网络防御的强大的国家网络安全体系和情报服务，主动参与了多个国际论坛的网络政策讨论，荷兰仍在努力以最好的方式接受信息通信技术和物联网，同时管理数字议程相关风险并加强国家整体网络的韧性。

安全与司法部，更具体地说，国家网络安全中心正受到任务整合的挑战。目前至少有 20 个机构肩负着加强荷兰网络安全态势的单独和集体责任，但没有一个机构拥有确保国家网络安全架构实现的支配权力。成功的结果取决于著名的荷兰波德模式（Polder Model），即在不同的部门之间进行合作，即使它们各自有着不同的观点。随着针对荷兰的网络威胁范围、规模和复杂性的持续增长，加快民事军事合作或是明确划分责任将是必不可少的。

此外，荷兰政府提出了多项计划和策略，但往往没有分配必要的资源（如资金、物资和人力）来执行被认为是重要的倡议。事实上，荷兰在网络安全方面的支出仍不到其国民生产总值的 0.01%，与美国、英国、澳大利亚、德国和法国等其他发达国家相比，这一比例（占国民生产总值的比例）要低得多。此外，公共部门和私营部门的许多组织仍在努力解决如何以高成本效益的方式，取代承载着关键服务的复杂且过时的遗留系统。许多其他组织仍然缺乏合格的网络安全人员来应对网络威胁。思维方式的转变是必要的，从意识到信息通讯技术创新和互联网接受率所带来的风险和机遇，到对这些风险进行管理，做适当的安全投资，只有这样荷兰才能够继续从数字经济中获利，达到其战略中所列出的雄心勃勃的目标。

2017 年 3 月的全国选举中，4 个政党被确认要求组成一个拥有多数席位的联盟（76 个席位）。现任总理马克·吕特（Mark Rutte）很可能将继续留任新政府。虽然移民、融合和国家认同是选举活动的中心议题，但组成联盟的所有四个政党都认为网络安全是国家安全和经济繁荣的一个重要问题。新一届政府应该为荷兰提供新的机会，更新荷兰的网络安全战略，加强整个国家的网络安全能力和韧性。它还将测试荷兰是否准备好巩固其作为欧洲门户的地位，并在与英国保持长期关系、在欧洲保持广泛领导地位的同时，成为最适合做生意的国家。

网络就绪度指数 2.0 的方法被用于评估荷兰目前的网络风险防范水平。这一分析为荷兰提供了一个可行的蓝图，更好地了解其互联网基础设施的依赖和漏洞，其当前网络安全态势与实现数字未来所需的国家网络能力之间的差距，评估缩小该差距的承诺和成熟度。基于网络就绪度指数 2.0 的 7 个基本要素（国家战略、事件反应、电子犯罪和执法、信息共享、研发投资、外交和贸易、国防和危机应对），全面评估了荷兰的网络安全相关努力和能力。



荷兰网络就绪度评估（2017）

国家战略

2011 年，通过颁布其第一个《国家网络安全战略：通过合作取得成功》，荷兰政府应对的设备感染、网络犯罪案件和分布式拒绝服务（DDoS）攻击越来越多。该战略承认“安全可靠的信息通信技术”是荷兰社会“繁荣和福祉”的基础，应该成为“促进经济可持续增长的催化剂”。战略还明确了荷兰成为“欧洲数字门户”（Digital Gateway to Europe）的宏伟目标。

首个《荷兰国家网络安全战略》于 2011 年发布，次个于 2013 年发布。

2011 年战略的重点是将连贯性和一致性引入与网络安全相关的各种全国性活动中，明确参与者之间的责任分工，并主张任何与信息通信技术安全相关的措施都是必要且合适的。为了实现这些目标，战略制定了以下五项基本原则：①联系并加强现有倡议，避免重复努力；②采取措施加强公私伙伴关系；③推广个体责任，保障自身信息通信系统和网络并为他人防范安全风险；④追求国际合作；⑤在自律与立法之间取得平衡。它还呼吁公布年度国家威胁和风险分析，即《荷兰网络安全评估（CSAN）》，以了解国家目前面临的趋势和挑战。此外，该战略还呼吁建立一个国家网络安全中心，

以监督全国倡议的协调，建立荷兰网络安全理事会作为国家战略咨询机构。这一战略的行动计划列出了一系列优先事项，包括加强荷兰应对信息通信技术中断和网络攻击的韧性；培养快速响应能力；加强执法能力；提高全社会网络安全意识；大力推进研究、发展和教育。

然而，尽管采取了一系列行动，但该战略并没有在 2011 年为这些倡议提供专门的资金。事实上，它指出，所述活动将“在现有预算之内执行”。一些机构确实在现有预算中重新分配了资金来提供能力和人员，并发展现行倡议。然而，鉴于优先事项和资源的冲突，额外的进展仍然难以实现。此外，直到针对 DigiNotar 的网络攻击和其他高曝光度的网络事件发生后，政府才于 2012 年 1 月最终开启了国家网络安全中心（National Cyber Security Centrum, NCSC），由安全和司法部及国家安全与反恐协调员（NCTV）领导。国家网络安全中心将网络活动集中在一个指挥部下，成为公私伙伴关系的平台。

2011 年战略中的一些活动，特别是《荷兰网络安全评估》年度报告的发布和荷兰网络安全理事会的成立（Nederlandse Cyber Security Raad, CSR），加速了对网络威胁和漏洞的战略理解。这些项目和顾问也强调，荷兰需要改变方式，在不同的参与者间，尤其是在国际舞台上，进行更强硬、更深思熟虑的领导。

荷兰网络安全理事会于 2011 年 6 月开始运行，负责向荷兰内阁提供网络安全问题的战略指导，并监督国家网络安全战略的实施。该委员会有着独特的公私伙伴关系，由 18 个成员组成，其中 7 个来自政府，7 个来自行业，4 个来自科学界。国家安全与反恐协调员作为理事会的联合主席之一，代表的是政府，KPN（荷兰最大的电信供应商）的首席执行官代表私营部门。该理事会是一个独立的国家战略咨询机构，负责为政府和私营企业提供网络威胁和网络防御的指导。它没有操作义务。相反，它在实施和发展国家网络安全战略上建议政府；通过强调国家研究和发展（R&D）的未来需求，为荷兰网络安全研究议程作出贡献；并通过一系列的董事会对话，提高私营部门高管的网络安全意识。

在第一个国家网络安全战略所制定倡议的基础上，荷兰安全与司法部在 2013 年公布了《国家网络安全战略 2：从意识到能力》（NCSS 2）。第二个战略的起草过程包含了许多不同的利益相关者，包括公共部门、私营部门、学术界和市民社会。新的网络安全战略明确了不同利益相关者之间的关系；鼓励公私参与和国际合作；确定了政府在建立必要的网络安全要求、规章和标准方面的作用，以保护和改善信息通信技术产品和服务的安全性；采用了基于风险的方法，平衡对荷兰利益的保护、对荷兰利

益的威胁和可接受的社会风险。这种新方法利用的责任感和风险意识，帮助了 1953 年《三角洲计划》的有效和成功。这一战略创造了 21 世纪的《数字三角洲计划》，主张个人、企业和政府在网络安全方面有明确的责任划分。事实上，公民应该遵守基本的“个人上网安全（Cyber Hygiene）”做法，对自身的网络安全承担一部分责任；企业应履行关怀客户的责任，提供更安全的信息通信技术产品和服务；政府应该通过“提高公民、企业和组织对网络安全的认识”，提高公民的数字技能，提高用户数据收集和保护的透明度来协助这些努力。

《国家网络安全战略 2》承认，荷兰抗击网络威胁的能力仍然不足。

此外，荷兰政府宣布了一项雄心勃勃的目标，即进一步加强其电子政务服务提供，“到 2017 年，使所有公民和企业能够数字化且安全地处理与政府的事务”。目前，荷兰在世界上排名第七，在欧洲的电子政务发展和在线服务提供方面排名第四，低于其原定于 2017 年实现的目标。

《国家网络安全战略 2》重申，政府致力于创造“一个安全有保障的数字领域”，使荷兰更加“能够抵抗网络攻击，保护其在网络空间中的重要利益”，“在国家和国际层面”加强和扩展“与公共和私营部门的联盟”。它强调了几项活动来更好地应对荷兰的网络威胁环境，在网络安全中的安全、自由和社会经济利益之间取得正确的平衡。这一战略潜在的基本原则是：①“适用于现实领域的责任，也应该适用于数字领域”；②与战略中各利益攸关方进行的网络安全相关讨论，应以“（自我）规范、透明度和知识的发展”为基础。它还展示了一种更广泛的政府对网络安全的看法，这一看法超越了孤立的技术问题，将网络安全置于人权、互联网自由、隐私、经济增长与可持续发展、创新等其他外交政策和经济问题的背景下，战略承认“数字领域安全”与充分利用“社会的数字化带来的经济和社会机遇”之间的联系，认识到“由于基于信息通信技术的产品和服务不断上升的复杂性、依赖性和脆弱性，荷兰的针对以上和其他网络威胁的数字领域韧性仍然不足”。

此外，《国家网络安全战略 2》将国家网络安全中心的地位提升到荷兰网络安全的“专家权威”，负责国家的数字安全和网络韧性，将重点放在中央政府和关键基础设施过程。中心的任务被扩展为创建“一个安全、开放和稳定的信息社会”，这需要通过三个主要角色和部门来完成：①在收到请求和主动行动的情况下，为公共和私营实体提供咨询，改善信息安全政策和活动（专业知识与咨询部）；②作为网络安全的信息中心和网络专业知识中心（市场发展与伙伴关系部）；③在遭遇大型信息通信技术危机时，协调荷兰政府和关键基础设施的运营，提供网络事件响应措施（监测与响应部）。

在组织结构的任务方面，国家网络安全中心是网络安全理事会（DCS）的一个部门，并由国家安全与司法部的国家安全与反恐协调员（NCTV）管理。网络安全主管也是国家安全与反恐的副协调员。

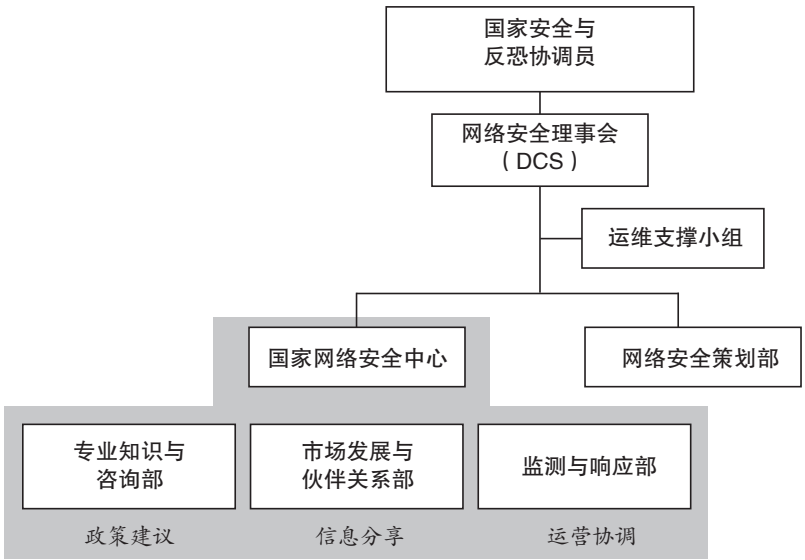


图 2 国家网络安全中心结构图

然而，网络安全责任并不完全属于安全与司法部。安全与司法部和国家网络安全中心负责监督荷兰范围内的大部分网络安全相关活动，但因为政府形式分散，它们没有责任也没有权力指导其他部门的活动，如经济部或外交部。《国家网络安全战略 2》确定了至少 20 个机构，它们有着实现战略中列出的网络安全目标的个体和集体责任。在政府方面，这些机构包括荷兰安全与司法部门，它负责协调各部门（有着网络安全责任的各民间和军事部门）间的网络安全，内政和王国关系部、经济事务部、国防部、外交部、教育、文化和科学部；其他政府机构如国家警察部，以及情报和安全部。在私营部门方面，在《国家网络安全战略 2》中定义的大部分责任，都落在了金融服务和电信部门，以及其他关键服务的提供者。学术界也有涉及，通过荷兰科学研究组织（Nederlandse Organisatie voor Wetenschappelijk Onderzoek, NWO）——教育、文化和科学部支持下的独立研究委员会，也通过政府资助独立研究组织，如荷兰应用科学研究组织（Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek, TNO）。当有这么多的参与者在网络任务领域的各个方面开展工作时，建立一套完整的政府战略和协调机制，确保各部门努力的和谐，就变得至关重要。

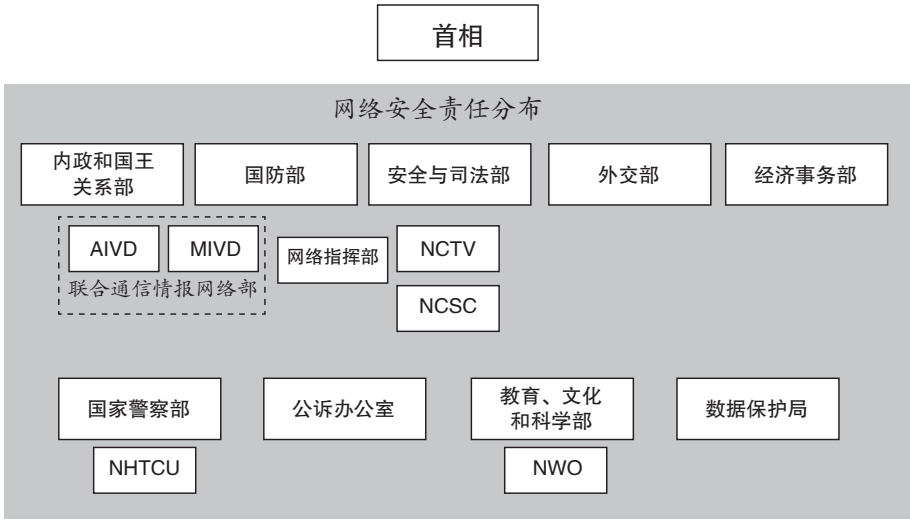


图 3　荷兰国家网络安全组织结构图

《国家网络安全战略 2》的附件载有详细的 2014—2016 行动计划（方案），以实现战略目标和长期目标。行动计划详细列出了具体措施，建立了时间线，确定了负责保证措施成功按时完成的实体。然而，即使是第二个国家网络安全战略，也没有承诺任何具体的资金来支持所有提及的倡议和措施。相反，它指出“政府（将）与所有相关方一道，通过参与、重新确认优先级、有效联盟和整体措施实施这一广泛战略”，所述的活动将由“常规部门预算和合作伙伴预算承担”。因此，它得出的结论是，“关于附件中所述行动的执行细节”，只能通过“与相关私营部门和政府机关协商或合作”决定。《国家网络安全战略 2》目标执行的分布式性质，再加上低效的融资机制，可能会使战略达不到预期结果。荷兰政府表示，网络安全属于优先事项，但它并没有为执行这些倡议的项目或机构提供资金，就像它们对国家的经济福祉或国家安全并不具有战略重要性一样。

事实上，在 2015 年公开的预算案中，荷兰政府只投入了 2,800 万欧元（约 3,050 万美元），即其 GDP 的 0.004% 到民用、军事和执法机构的网络安全中。那一年，国家网络安全中心收到的资金为 270 万欧元（约 290 万美元），2016 年，这一资金增加到 1,260 万欧元（约 1,350 万美元），用于国家监测网络前沿部署。虽然总国防预算有分类，荷兰国防部收到了 500 万欧元（约 540 万美元）——2016 年增加到 900 万欧元（约 980 万美元）。荷兰国家警察部收到了 1,380 万欧元（约 1,500 万美元）用于打击网络犯罪，增强其安全能力。最后，2015 年荷兰政府一次性投资 650 万欧

元（约 710 万美元，在 2014 年花费的 200 万欧元的基础上追加）用于组织第四届全球网络空间峰会（4th Global Conference on Cyberspace）。荷兰国内其余的网络安全措施都依赖于现有项目的抵消资金。2016 年末的“在线提醒”网络安全意识周中，受荷兰网络安全理事会的请求，PostNL 首席执行官赫娜·费尔哈亨向首相马克·吕特展示了一份咨询报告（“Digitaal Droge Voeten”），她敦促荷兰政府及企业拿出其年度信息通信技术预算的 10%，投资于特定网络安全措施。

虽然网络安全投资未能得到足够的资金，但很明显，荷兰正投资于信息通信技术能力。荷兰将近 1% 的国内生产总值，超过 230 亿欧元（约 250 亿美元）都被政府和私营部门投资于信息通信基础设施。荷兰 2011—2015 年数字战略（“Digital Agenda”）承诺为该国信息通信技术基础设施现代化提供额外资金，在 2011 年和 2013 年国家网络安全战略中也有类似内容，承认了信息通信技术对经济增长的重要性和网络空间安全的必要性。在战略中，荷兰政府重申了其利用信息通信技术促进经济增长和繁荣的意愿，拥有开放、可靠、安全、有保障的信息通信基础设施，以及充分的信息通信技术知识和专业技能，是实现其所述目标的必要先决条件。为了在国家层面和国际层面提高信息和通信技术的安全性和韧性，数字战略和国家网络安全战略都提到要用一种全面的、涉及多方利益攸关方的方法，建立一个安全、有保障、自由与和平的网络空间。

此外，数字战略强调对 ICT 的信任对于数字通信、电子商务和欧洲数字单一市场的成就至关重要。荷兰政府承认，公民和企业担忧信息通信技术的安全性和可靠性，并怀疑对个人数据的保护会阻碍电子商务和电子政务扩张，政府表示，“公众对 ICT 的广泛信任可能会额外产生超过 10 亿欧元（约 11 亿美元）的网上贸易营业额”。

然而，这些策略之间虽然是紧密联系的，但在全国经济中，关键服务的不断数字化带来了新兴的 ICT 威胁，政府当前的网络安全支出却仍然无法满足加强安全与韧性的财政和人力资源需要。过去一年中，荷兰政府一直在审查其国家网络安全战略，预计到 2018 年将发布更新版本。此外，一旦新政府成立，新的国家数字战略也将于 2018 年出版。除了资金和有效执行计划设计的持续挑战外，在一个越来越相互连接、易发冲突的地缘政治系统中，新政府能否提出一个更平衡的方法，将国家经济的愿景与其国家安全优先级统一起来，仍然是未知的。

事件响应

国家网络安全中心（NCSC）作为荷兰国家网络安全管理当局，通过全政府和全

社会的预防、检测、缓解和响应来影响信息安全政策和活动，同时作为国家中央网络事件报告办公室。

国家网络安全中心负责网络事件响应管理和协调，是国家事件报告中央办公室。

NCSC 于 2012 年 1 月开始运营，自成立以来一直致力于公私合作伙伴关系。今天，NCSC 是荷兰政府机构的网络事件响应管理和协调的主要机构，也是关键基础设施的运营商（关键运营商或一系列重要产品和服务的关键运营商，其可用性和可靠性对荷兰社会至关重要）。在这种能力下，NCSC 包含了计算机应急响应小组（CERT）的功能，这些功能原属于已被取代的 GOVCERT.NL。

荷兰国家网络事件响应计划（国家危机计划 ICT）是《危机状况决策手册》（Manual of Decision-making in Crisis Situation）的一部分，最近一次更新在 2017 年 3 月。手册为包括“大规模网络危机”在内的各类危机情况提供了参考指南和通用程序。这些计划在小型演习和国家级演习中都测试过，小型演习包括部分国家危机管理结构，国家级演习每两年举办一次。在发生重大 ICT 中断或网络危机的情况下，NCSC 将利用其分散式结构做出响应，如果需要，将根据事件的类型和严重程度（持续时间、影响范围、受影响的人数或企业数量）、受影响的部门、经济、物理或社会影响，与其他机构和私人伙伴建立起临时伙伴关系。国家安全与反恐协调员（NCTV）中的安全与司法部下属网络安全主任，是负责协调事件响应活动和管理国家危机结构内危机组织的主要公务员。2015 年 6 月，国家安全与反恐协调员开展了一项全国范围的演习，以测试荷兰的网络防范措施——ISIDOOR 行动召集了 30 个公共和私人合作伙伴，包括数据泄露和系统漏洞等一系列模拟网络事件。政府与这些公共和私营部门合作，对每一事件采取适当的响应行动。

网络安全部门在战略和战术层面处理危机，除了“在危机决策结构中起建议和通知作用”外，NCSC 还提供事件响应和行动协调。如果多个部都参与处理某次网络事件，就会引发国家危机。NCSC 还将激活信息通信技术响应委员会（IRB）。IRB 是政府机构和关键部门之间的公私伙伴关系，于 2010 年建立。它作为国家危机管理结构的咨询委员会，负责分析局势，并向国家危机管理机构和受影响的各方提供关于缓解战略的建议。例如，在 2011 年 DigiNotar 事件中 IRB 就曾被激活，它将继续在国家危机响应结构中发挥重要作用。

2015 年 7 月，国家安全与反恐协调员进行了一次“关键基础设施政策审查”。在这次审查中，政府将关键基础设施定义为“一系列国家运转所必需的产品、服务和基础过程，它必须是安全的，能够承受并从所有危险中迅速恢复……关键基础设施的

失去或受损将影响国家安全，并造成有害影响。”作为这次审查的结果，荷兰已经更新了对关键基础设施的保护，采取了更为严格的措施。这包括更关注关键领域内关键进程的危急和破坏程度，基于危急程度 / 可能中断的影响，将关键基础设施分为两类：A 类和 B 类，以更有效地在事件中分辨优先级，定制韧性增强方案。例如，A 类别（Category A）基础设施的中断、损坏或故障会导致约 500 亿欧元（约 545 亿美元）的损失；或死亡、重伤、患慢性病人数超过 1 万人；或超过 100 万人患有情绪问题或影响基本生存的严重问题；或造成至少两个其他关键部门的中断或崩溃。B 类别（Category B）基础设施的中断、损坏或故障会导致约 50 亿欧元（约 54 亿美元）的损失；或超过 1,000 人死亡、受伤或长期患病；或超过 10 万人患有情感问题或有关基本生存的严重问题。规划过程确定了 5 个不同部领导下的 10 个关键部门。

2016 年 5 月进行的一次国际演习，对电气设施可用性的跨境依赖性进行了压力测试。能源短缺——无论是由于动力故障还是其他方式——都可能造成国家和国际经济和社会影响。因此，由国家安全与反恐协调员组织，欧盟委员会内部安全基金资助（ISF），VITEX 2016 演习帮助提高了认识，测试了欧盟政府机构和运输系统运营商在电力设施能力低下或缺失时的危机管理程序。这次演习重申了欧盟成员国在保护关键基础设施方面合作的重要性。

通过对关键基础设施的审查，对其中断、损坏和崩溃的可能阈值的理解，以及诸如 VITEX 2016 的演习，荷兰政府意识到需要继续计划和制定危机场景。演习、战争游戏和危机规划机制有助于建立机构能力，有效地响应事件。这还需要大量的规划和资源。在 2016 年，荷兰政府制定了 4 个假设场景，以指导规划和发展机构能力和响应机制的过程。这些场景已被用于制定新的国家网络安全战略。

如前所述，国家级的网络安全演习每两年进行一次，包括私人和公共实体。除了内部规划演习和事件响应准备之外，荷兰还定期参加由欧盟（如网络欧洲演习，Cyber Europe Exercise）、北约（网络联盟和网络大西洋演习，Cyber Coalition and Cyber Atlantic Exercises）、欧洲防务局（EDA）、欧洲网络和信息安全机构（ENISA），以及美国国土安全部（如网络风暴，Cyber Storm）组织的多国演习，以加强各国的网络事件响应能力，提高国际防范水平。

除了网络事件协调功能外，NCSC 还对信息通信技术产品和服务中的恶意软件和安全漏洞发出威胁警报和警告，向有关各方和公众发布信息，就应对措施提出建议。NCSC 还开发了各种应用程序来监控大量的信息来源，如网站、社交媒体、受信任的合作伙伴的通知，并用传感器和蜜罐网络来监测网络流量，分析基于互联网

的威胁和它们的攻击向量。例如，“Taranis”应用程序（被其他一些应急小组使用的开源软件）在内部使用，它会收集、分析和发布信息通信技术漏洞警告，而“Beita”项目由安装在政府组织的多个蜜罐和传感器网络组成，用于监控针对这些组织的自动网络攻击。

荷兰政府正在推动开放标准，并实施软监管——“遵守或解释”名单——以鼓励快速采用。

在检测能力和网络危机期间的应急分配角色之上，NCSC 正在提升额外的能力，提高意识、韧性、检测、报警、报告和危机管理。2015 年，NCSC 与通用情报和安全部（Algemene de Inlichtingen- en Veiligheidsdienst, AIVD）以及军事情报和安全部（Militaire Inlichtingen en Veiligheidsdienst, MIVD）合作建立了国家检测网络（NDN）作为试点项目，为中央政府和其他重要部门提供实时分析，共享网络威胁信息，从而防止层叠效应。该传感器网络安装在不同的组织中，监测高级持续威胁（APTs）指标。试点项目得到了积极的反馈，并在 2016 年进一步扩大，成为 NCSC 提供的标准管理安全服务。目前，大约有 30 个中央政府组织已经加入了这一网络。一旦全面运行，国家检测网络将连接 250 个组织。

根据 2013 年国家网络安全战略目标——使荷兰成为“做生意的安全的地方”，增加电子政务服务，使所有“公民和企业能够数字化且安全地处理他们与政府的事务”——荷兰政府采取了几个步骤，使数字化变得安全，公民和企业与政府的大多数事务都可以电子的方式进行。例如，因特网标准平台（Internet Standards Platform）——荷兰政府与网络社区的合作成果——建立了网站（internet.nl），使用户能够检查其网络连接、电子邮件或 Web 服务器是否符合现代安全互联网标准，包括 IPv6（持续可达性）、HTTPS（加密网站连接）、DNSSEC（真实域信息）、域名密钥邮件确认（DKIM）、发送方保护框架（SPF）和基于域的消息身份验证、报告和合规性（DMARC，可帮助减少电子邮件诈骗）、START-TLS 和 DANE（帮助减少电子邮件窃取）。这一网站测试服务器同时适用于网络和电子邮件流量的连接安全性检测，并指出流量在多大程度上满足了荷兰标准化论坛（Dutch Standardization Forum）上的“遵守或解释”（Comply or Explain）标准。此外，该网站已被证明为一种有效的手段，可以帮助各方更好地使用安全互联网标准，被访问者在 Internet.nl 测试过的网站，其中超过 50% 在过去的一年里提高了它们的安全得分。

当投资于 ICT 系统时，政府实体需要在“遵守或解释”清单中选择开放标准。这是一种软规则形式，意味着用于执行这些安全标准的规则并不会被严格执行，除了

声誉风险，不遵守这些规则没有其他惩罚。此外，所有政府机构都必须遵守国际标准化组织（ISO）和国际电工委员会（IEC）的《27001：信息安全管理系统》（27001: Information Security Management System）标准，以及荷兰国家政府信息安全基准中一些针对政府的具体措施（Baseline Informatiebe-veiliging Rijksoverheid, BIR），这一基准是基于 ISO / IEC 的《27002：信息安全控制》标准制定的。国家和地方机构必须遵守《地方政府信息安全基准》（Baseline Informatiebeveiliging Nederlandse Gemeenten, BIG）中所包含的措施。

2016 年，全国数字政府委员会（National Council for Digital Government）同意包括额外安全标准，这些标准类似互联网标准平台宣传的“遵守或解释”名单。这些标准旨在认证电子邮件的发送者，确保电子邮件通信的完整性和机密性，并打击垃圾邮件和网络钓鱼。国家数字政府委员会希望所有政府组织在 2018 年之前采纳这些标准。尽管满足全国数字政府委员会设定的目标仍然是政府的一个挑战，标准化论坛的监测显示，采用率有了明显增长。

除了“遵守或解释”列表之外，NCSC 还定期为许多行业特定安全标准发布指导方针和其他情况报告（如《保护域名免受网络钓鱼》（Protect Domain Names from Phishing）和《保证邮件服务器通信》（Secure the Communications of Mail Servers）情况报告）。荷兰政府还与私营部门伙伴合作，向各组织提供基本网络安全规范和标准，帮助它们更好地保护和改善信息通信技术产品和服务的安全。例如，近年来，越来越多的 .nl 域名和中央政府网站都采用了 DNS 安全扩展（DNSSec）——一种检查域名是否指向正确 IP 地址的协议——添加了额外的真实性和完整性监视功能。虽然荷兰政府尚未向软件和数字服务供应商提供真正的激励措施来提高其产品的安全性，或施加最低产品责任的法律规定，但荷兰网络安全理事会最近已经发布了一份指导性文件，帮助企业解决这些问题。此外，广泛适用于欧盟的规定是否有利于长期平衡荷兰的经济增长与安全也有待商榷。

为了更好地与公民和企业用更加数字化、安全和标准化的方式互动，荷兰政府扩大了 eID 计划——标准在线身份识别系统，用于电子政务服务的安全访问，设置了个性化的环境（MijnOverheid.nl），允许公民以电子的方式，接收政府机构（如税务及海关管理局）的信件。现在，越来越多的政府机构、市政府和养老基金都在使用这一数字消息框给它们的选民发送消息。新的 eID 系统的最终目标，是在允许公民和企业选择访问数字政府服务的首选验证方案的同时，避免单点故障。在这个数字身份框架中，将有几种可用的身份验证方案，如 DigiD（公共部门）、iDIN（银

行）和 Idensys（商业）。所有这些方案若要在公共部门使用，都需适用一套严格的公共需求。

为了对抗 DDoS 攻击的不利影响，不同的利益攸关方和信息通信技术提供商近年来发起了另外两项倡议：网络信任倡议（TNI），这一倡议从未投入运营，以及荷兰连续性委员会（DCB）——服务提供商的合作委员会，也加入了前网络信任倡议项目的成员。这项倡议的目的是限制 DDoS 攻击对荷兰关键基础设施的影响，尽快为荷兰用户恢复被干扰的服务。荷兰连续性委员会自 2016 年年底以来一直在运营，并为参与各方提供了在大型 DDoS 攻击事件中，将成员之间的通信与所有其他互联网通信隔离的可能性。2014 年发起的另一项倡议（即 NaWas 倡议），旨在解决针对特定目标的大规模网络攻击行动，在最近的全国选举中有效地挫败了 DDoS 攻击。

最后，NCSC 定期发布与网络安全相关的白皮书、情况报告、指南和报告，例如年度荷兰网络安全评估报告（CSAN）就是其与其他机构和私人合作伙伴合作拟订的，报告包括网络事件数据和全球网络威胁分析。虽然这是政府和其他利益攸关方之间合作的一个很好的例子，也被所有合作伙伴高度重视，CSAN 报告却未能实现第一个国家网络安全战略中提出的所有初始意图——每年对荷兰政府、关键基础设施和重要商业服务网络面临的网络威胁进行详细的定量分析。然而，CSAN 报告对国际网络风险和威胁、全球网络安全趋势和事件提供了定性的概述，并对国外实施的网络安全相关倡议更新进行记载。

为了开始量化网络不安全的成本，2016 年 7 月，荷兰中央经济政策分析局和荷兰议会 NCSC 提交了一份新的额外网络安全风险评估（CSRA），试图对国家面临的网络威胁进行经济分析，“重点关注市场失灵对网络安全的限制，以及对荷兰企业和消费者的后续风险”。

荷兰正在增强事件响应能力，并采取一系列积极步骤来识别关键部门，对危机应对机制进行演习。威胁会针对并危害荷兰关键基础设施和服务，提高人们的威胁意识对于加强国家的韧性至关重要。衡量荷兰网络不安全的真实成本，将有助于行业优化投资，为政府领导人提供丰富的信息，让其将适当的资源分配给这一首要目标：推动以信任和韧性支持的经济发展，同时成为最适合做生意的国家。

电子犯罪和执法

荷兰已经表明了保护社会免受网络犯罪的国际承诺，签订了（2001）和批准了（2006）《欧洲理事会网络犯罪公约》（Council of Europe Convention on Cybercrime，

俗称《布达佩斯公约》），并在国内执行了这一公约，通过了额外的一些网络犯罪和数据保护法律（如《电子签名法（Electronic Signatures Act）》《个人资料保护法（Personal Data Protection Act）》《2014 年计算机犯罪法案（Computer Crime Act of 2014）》。

荷兰国家警察和公共检察部（Dutch National Police and the Public Prosecution Service）负责网络犯罪的预防、调查和起诉。

在 2013 年的《国家网络安全战略 2》中，荷兰政府认识到需要有效利用有限的资源来解决网络犯罪问题，并重申其致力于在《布达佩斯公约》的基础上协调各国刑法的承诺。为了促进这些努力，荷兰积极参加各种国际会议和有关活动，旨在打击网络犯罪活动，提高打击网络犯罪战略的效力，加强国际伙伴关系。NCSC 和荷兰国家警察积极与欧洲刑警组织的欧洲网络犯罪中心（EC3）、国际刑警组织、欧洲委员会的缔约国委员会（Committee of Contracting States）、欧盟应对有组织犯罪政策周期（EU Policy Cycle to Tackle Organized Crime）、欧洲安全与合作组织（OSCE）和联合国毒品与犯罪办公室（UNODC）合作。此外，内阁的《2015—2018 年安全议程》要求国家安全与司法部门加强打击网络犯罪的国际努力，并协调荷兰国家警察与其他部门的国家合作伙伴的活动。

在国内，荷兰议会正在考虑制定两项新的法律，以扩展各情报和安全部门的能力，并为它们提供额外的工具和权力，以调查和打击高级网络攻击。《数据处理和强制报告网络安全法》（Wet Gegevensverwerking en Meldplicht Cybersecurity）将增加警方侦查重大网络犯罪的权力，要求关键组织向 NCSC 报告网络入侵。这项立法进一步为 NCSC 提供了法律基础。新的《计算机犯罪法案 III》（Wet Computercriminaliteit III）将赋予警察和其他调查队特殊权力，在某些情况下，如果犯罪行为发生，它们可以远程渗透（或者侵入）嫌疑人电脑。这项法律给予警察利用软件漏洞更广泛的权力，因此受到了严重的批评，之后颁布的一项修正案中，警方有责任立即告知软件开发人员其发现的任何软件漏洞，包括零日漏洞。如果警方不想披露漏洞信息，必须由法庭同意并进行“独立审查”，以确保警方的调查并未凌驾于软件的安全性之上。这两项法律已在众议院通过，但尚未在参议院通过。

尽管欧洲国家有着不同的数据违反通知要求，但是荷兰政府已经采用了 1995 年《欧盟数据保护指令》、2016 年的网络和信息安全（NIS）指令以及欧盟通用数据保护条例（GDPR）中的大部分规定，旨在提高网络安全能力，促进全欧洲的合作。例如，荷兰已经建立了数据保护局（DPA，前数据保护“学院”），以确保遵守个人数据使用相关法律，并在最近加强了保护局的权力。2016 年 1 月，荷兰《数据保护法案》

（Dutch Data Protection Act）的补充法案生效，这使得数据泄露报告成为强制责任。这项新法律要求荷兰所有组织在发现的 72 小时内，将可能泄露个人资料的事件报告给荷兰数据保护局（DPA），与 GDPR 规定相同。荷兰 DPA 可以发起调查，在适当情况下，违反某些规定可受到 820,000 欧元（约 893,510 美元）或年收入 10% 的罚款。在法律通过后的几个月内，虽然荷兰 DPA 收到了成千上万的报告，但许多其他组织可能仍然不愿意对事件进行上报，只要它们相信预期的名誉损害，将大于因未报告而受到的 DPA 罚款。此外，由于 2014 年《数据安全港》以及之后关于《隐私盾》（Privacy Shield）的争论，一些公司将数据转移到了美国，对于这些公司的违规，罚款可能尤其麻烦。在新的《数据处理和强制报告网络安全法》（Data Processing and Compulsory Reporting Cyber Security Act）中，有一项数据泄露报告义务特别适用于关键基础设施组织，它们需要向 NCSC 通报网络事件。

在执法能力方面，荷兰已经建立了一种成熟的机构能力，可以处理网络犯罪的不同因素，多次努力打击国内和国际上的网络犯罪，并将罪犯绳之以法。安全和司法部负责打击网络犯罪，但荷兰国家警察和公诉部（OM）为主要的执法机构，负责网络犯罪预防、调查和起诉。近年来，它们已经发现、逮捕并定罪了越来越多的网络犯罪嫌疑人，包括网络诈骗、洗钱、恶意软件攻击、钓鱼诈骗、假报警、使用银行恶意软件勒索钱财以及发起 DDoS 攻击。此外，荷兰国家高科技犯罪单位（NHTCU）——下属荷兰国家警察机构的团队，致力于调查高级形式的网络犯罪，负责解决被归类为“高科技犯罪”的案件，涉及的犯罪形式为“有组织、目标为计算机系统并使用复杂的新技术或方法”。NHTCU 与国际同行合作打击跨国网络犯罪，并启动了“荷兰电子犯罪工作组（The Dutch Electronic Crime Task Force），与金融和其他私营部门组织合作，将公私伙伴关系制度化，作为积极打击某些类型的网络犯罪的手段”。另有一些执法专家也在接受培训，学习调查网上的儿童色情、假冒或被盗商品的销售以及过激言论。2015 年，荷兰政府将 1,380 万欧元（约 1,500 万美元）分配给国家警察，以打击网络犯罪，加强其未来多年的安全能力。

随着高速网络的普及，网络中设备的增加提供了更多的感染和利用途径，网络犯罪也随之增多。认识到这一点，2013 年荷兰经济部与各互联网服务提供商合作，共同建立了滥用信息交流（AbuseHUB）计划，作为信息交流中心，对僵尸网络感染和其他网络滥用进行收集、分析和信息采集。AbuseHUB 成员包括荷兰的主要服务提供商、主机提供商、SIDN（“.nl”一级域名注册）和 SurfNet（国家研究和教育网络运营商），它们对荷兰 95% 以上的互联网连接和 75% 以上“.nl”域名注册负责。通过

这个平台，大量的国家和国际来源（“可靠通知者”，reliable notifiers）就可以将安全风险、僵尸网络感染和其他互联网滥用信息直接传送到服务提供商成员的自动事件响应流程中，随后，提供商可以迅速与客户合作，快速且有针对性地清理他们的机器。它类似于欧洲高级网络防御中心（ACDC）——由欧洲委员会资助的一个非营利项目，旨在改善预防、检测和减少僵尸网络，将全欧洲的支持中心通过一个基础设施与中央交流中心连接起来——AbuseHUB 计划已被证明可以成功地减少僵尸网络，降低感染水平，并已在社区内得到了高度重视。

荷兰政府还发起了一项“荷兰清洁”项目，使主机提供商意识到，有一些客户可能会利用其基础设施进行恶意活动，并鼓励它们清理其基础设施。例如，欧盟里很大一部分的恶意命令和控制域的主机都在荷兰。荷兰还拥有大量的洋葱路由器（TOR）网络，这些网络使得匿名通信经常与不正当和非法活动联系在一起。这些用于评估不同荷兰主机提供商“作恶”程度的一系列方法，都是基于公共和私人信息。数据和威胁情报的来源不断增多，政府与反儿童色情互联网热线、国际法律援助国家中心（LIRC）、荷兰公共检察办公室以及消费者和市场管理局（ACM）也有着紧密的合作关系。警方甚至质问了“作恶”最多的主机提供商，指出它们是如何助长网络犯罪的，并提出了应对措施。

荷兰还在努力提高能力，并加入了各种执法网络培训项目，如 2014 年开启的欧洲理事会“Cybercrime@Octopus”，该项目旨在协助各国实施《布达佩斯公约》，加强数据保护和法律保护。在各种活动之中，这一计划向法官和执法人员教授网络犯罪和电子证据课程。还有一些其他的国内项目为警察提供培训，但尚不清楚是否有足够的培训检察官、律师和其他调查人员项目。

荷兰国家网络安全中心负责事件响应协调和全社会信息共享。

虽然荷兰已经是欧洲刑事司法和打击网络犯罪能力的中心，而且是世界上最大的互联网交流中心之一，但要在这一重要领域里成功实现其所有雄心，仍需要进一步的努力。荷兰面临着将其愿景和抱负与国家能力相匹配的巨大机遇，这将会减少网络犯罪，加速创新，增强人民对数字经济的信任。2017 年底，我们将会知道新的荷兰政府将在多大程度上致力于这些举措。

信息分享

正如《2013 年国家网络安全战略》所述，荷兰国家网络安全中心（NCSC）负责事件响应协调和信息共享。NCSC 作为政府和私人企业之间的信息流动中心，负责管

理威胁信息，制定与利益攸关方讨论的新战略和战术，对上报的网络事件进行响应。

NCSC 协助数个信息共享分析中心（ISACs），它们按部门划分，共享部门特殊威胁信息。共享信息包括但不限于基于信息通信技术的产品和服务的弱点及漏洞、网络攻击的形式、犯罪者的档案等。各部门分析中心由部门成员领导，包括能源、金融、饮用水、健康信息共享分析中心等。NCSC 与伙伴组织之间的联系人，无论是在公共还是私营部门，都会在每周开会讨论和分享网络与安全相关的信息。NCSC 还在全国范围内推广网络安全意识和教育。网络安全和信息共享的其他相关的公私伙伴关系，包括信息社会平台（ECP）——为促进荷兰信息通信技术使用安全的平台，以及国家连续性论坛（NCO-T）——荷兰政府和电信网络供应商之间的伙伴关系。

此外，荷兰参与各种跨国和跨部门的伙伴关系，促进信息共享，如北约的恶意软件信息共享平台（MISP）、欧盟为加强各应急响应小组之间威胁数据流动提出的多个倡议、国际观察和预警网络（IWWN）、事件响应和安全小组论坛（FIRST）、计算机安全事件反应工作组（TF-CSIRT）以及国家网络取证和培训联盟（NCFTA）——美国的非盈利公司，其使命是促进私营企业、学术界和执法机构之间的合作，以识别、减轻和消除复杂的网络相关威胁。它还与邻国比利时和卢森堡签署了一份谅解备忘录，其中包括有关发展公私伙伴关系的网络安全合作和专业知识共享。

荷兰政府认为负责任的披露（Responsible Disclosure）是“加强信息系统、软件和其他 ICT 产品安全的重要一步”。安全与司法部门与行业受害者、信息通信技术软件或硬件开发商合作，开发了一套负责任披露指南。这些指南“促进了负责任的报告和漏洞处理”及“帮助组织起草了自身的负责任披露政策”。在 2016 年荷兰担任欧盟轮值主席国的第一期，荷兰 CIO 平台和 Rabobank 发起了一项合作机制，协调漏洞披露。这一过程之所以重要，是因为越来越多的商业产品被不正当和非法活动作为目标利用。这一努力使《漏洞披露协调宣言》（Coordinated Vulnerability Disclosure Manifesto）得以起草并采用，《宣言》认识到研究者和黑客社区参与向系统所有者报告漏洞的重要性，允许组织有机会在早期发现并修复漏洞。自 2016 年 5 月出版以来，交通、医疗、能源、银行和科技行业有超过 30 家跨国公司签署了《宣言》。全球网络专家论坛（Global Forum on Cyber Expertise）负责任披露倡议将其列为全球最佳实践。

在负责任披露倡议的基础上，KPN 与国家安全和反恐协调员开始合作记录信息通信技术漏洞，为所报告的漏洞提供解决方案建议，从而大大缩短漏洞造成伤害的时间。此外，为荷兰商业发声的行业联盟——荷兰工业和雇主联合会（简称 VNO-NCW）与经济部共同发起了一项倡议，将有关安全威胁和解决方案的知识传递给各

个部门。

对荷兰来说，随着其对数字技术的依赖不断增加，将本身带有漏洞的信息通信技术纳入其核心业务和关键服务，那么网络威胁的规模、范围、复杂性和速度都有可能造成更大的伤害。荷兰尝试了许多不同的信息共享路径，NCSC、信息共享分析中心、部门特定线索甚至行业协会。提高韧性、缩小攻击面、创造使企业发展的环境都属于重要的第一步。NCSC 是一个促进信息共享的极佳平台。然而，我们目前还不清楚是否存在必要的激励措施来促进及时和可操作的数据交换。荷兰的两个主要商业港口（斯希波尔机场和鹿特丹港）及其安全是需要加强的关键领域，并可以作为案例研究证明，公私信息共享对企业和经济都是必要的。

研究和投资

荷兰将企业、知识机构和政府机构这一“金三角”之间的研发、创新和合作视为其未来竞争力和经济实力的关键。因此，荷兰追求的是现代化的工业政策——高端产业政策（Top Sector Policy），利用行业特有的经济实力和市场份额，保持荷兰经济的增长繁荣。高端产业被视为荷兰国家科学议程（NWA）以及欧盟地平线 2020 战略（Horizon 2020）的关键。高端产业的特点包括劳动生产率高、出口导向、研发支出规模大，更注重解决社会挑战。荷兰已经确定了 9 个创新高端产业，在这些产业中，荷兰领先世界，并采用了具体的政策来维持其在这些产业的领先地位：①农业和粮食；②化学；③创意产业；④能源；⑤高科技系统和材料；⑥生命科学与健康；⑦物流；⑧园艺和原材料；⑨水。9 个部门共同构成了全国 90% 的（私营）研发支出。

在高端产业政策中，信息通信技术被认为是一个跨产业主题，它“旨在促进和刺激有关高端产业的信息通信技术创新”。2014 年底，特别工作组（Team ICT）成立，负责对知识和人才进行评估，使其发展更加针对应用、服务、产品、工作流程和就业。随后，在 2015 年底，2016—2020 信息通信技术知识和创新议程（KIA）发布，详细阐述了与所有行业和高端产业都相关的信息通信技术挑战，如大数据和网络安全。今天，有关是否将信息通信技术作为第 10 个高端产业的讨论仍在进行中。

荷兰已经确定了三个核心目标，将其作为 2020 年高端产业政策和愿景的一部分。首先，它希望荷兰继续成为世界上最具创业精神和竞争力的经济体（今天，荷兰属于全球最具竞争力的五大经济体）。第二，它为荷兰设定了领导知识与创新顶级联盟（TKIs）的目标，即公共和私营方对研发的参与和贡献需超过 8 亿欧元（约 8.72 亿美元），其中至少有 40% 为私人融资。最后，它挑战荷兰将其研发活动占 GDP 的比重从 2014

年的 2% 提高至 2.5%。

作为高端产业政策的一部分，经济部提供了各种税收优惠，以促进软件开发、信息和通信技术以及信息安全解决方案的发展。这包括：WBSO（研发税收抵免），它降低了从事研发活动人员的工资税和社会保障贡献额；研发津贴，对于有资格的、直接与有资格的研究活动相关的非工资费用，研发津贴将作为超级减免；创新箱（以前称为专利箱）。虽然这些税收优惠都未专门适用于网络研发，但 WBSO、研发津贴和创新箱都是相当广泛的，它们对所有行业都适用，包括网络安全创新。此外，为了未来的创新和重要研究，有专门的创新未来基金（Innovative Future Fund）为中小企业（SMEs）提供投资。2016 经济部的预算中包括给该基金的 2 亿欧元（约 2.18 亿美元）。

高端产业政策与荷兰数字战略（Digitale Agenda）只有松散的联系，与国家网络安全战略之间的关联更少，即使它们都承认投资网络安全创新和研发的重要性。根据第一个《国家网络安全战略》和《国家数字战略》中概述的目标，和 2008 年欧盟顾问委员会的对信息社会的安全、隐私和可信赖性的研究与创新的相关建议，2013 年荷兰《国家网络安全研究议程（NCSRA）II》主要集中在以下两个特定方面：①公民安全和信任（包括隐私保护、移动服务安全、数据和政策管理、问责制）；②信息通信技术基础设施的安全性和可靠性（包括恶意软件检测和删除、入侵检测和预防、软件安全、工业控制系统安全和操作系统安全）。这项研究议程强调了大学和学术机构中基础和应用研究的重要性——包括培养博士生——并鼓励引入多方利益相关者来促进创新。

此外，《国家网络安全战略 2》强调需要在网络人才的供需之间进行更多的协调，以聚集创新人才和专家，让他们能够在一起工作，并建议将创新倡议与高端产业政策联系起来。它还鼓励追求教育项目的广泛性，“从初级教育到高等教育，从基于工作的培训到大学，从董事会到采煤工作面”，以增加网络安全专家的数量，提高用户的网络安全能力。有了这个目标，荷兰政府、商界、学术界决定一同提高学术水平上信息通信技术教育的质量和广度，并推出了网络安全平台，为企业、学生、决策者、消费者、生产者和研究人员提供“连接、相互鼓励、协调研究供给和需求”的平台。这一平台名为荷兰高等教育和研究网络安全平台（Dutch Cyber Security Platform for Higher Education and Research），由荷兰安全与司法、经济事务、教育、文化和科学部以及荷兰科学研究组织（NWO）于 2016 年建立。Dcypher（安全平台）的使命是支持国家研究和教育议程，特别强调网络安全领域的高等教育，以创造充足的网络安全知识和技能，并鼓励创新。这一网络安全教育方面的公私合作伙伴关系仍处于起步阶段，在计算机科学和网络安全课程的改进方面，政府与商界正开始进行磋商，但尚

未取得成果。《国家网络安全战略 2》战略指出，《国家网络安全研究议程 II》和其他公私伙伴关系将同样有助于这一发展。

2010 年，由荷兰应用科学研究组织（TNO）、其他学术组织和私营部门组织构成的联盟发起了一个项目（Pieken in de Delta Project），其目标是在海牙建立一个创新中心，解决一些最紧迫的国家、城市和网络安全问题。这一项目于 2013 年建立了海牙安全三角洲（HSD）——由海牙、Twente 和 Brabant 三地的安全中心组成的安全集群。HSD 旨在通过荷兰企业、政府和学术机构通力合作，共同应对网络安全和信息通信技术创新，从而利用荷兰的创新驱动经济发展。位于海牙的 HSD 校园是国家安全创新中心，拥有最先进的实验室、教育和培训设施以及多个办公场所。这使得这座城市成为欧洲主要的网络安全中心之一。2016 年底，荷兰应用科学研究组织（TNO）正式在 HSD 校区开设了网络威胁情报实验室（Cyber Threat Intelligence lab），以尝试新技术，改善早期的网络威胁检测、信息收集以及机密数据交换。TNO 和 HSD 也在设计一个新的国家网络试验台（National Cyber Testbed），以解决对关键基础设施的网络威胁。鹿特丹大都会地区和海牙（MRDH）提供了 200,000 欧元（约 217,930 美元）的初始投资，帮助实现这一计划。

2012 年《国家网络安全研究议程》强调了小型企业创新研究（SBIR）的重要性，并资助了将从可行到原型的短期研究项目。最初的 SBIR 项目投入了 270 万欧元（约 290 万美元），在业务取证、实时监控和电网安全等 8 个领域建立了原型。第二个《国家网络安全研究议程》又投入了 270 万欧元（约 290 万美元），用于 SBIR 2013—2014 年的运营。来自 6 个部门的资金进入了 21 个可行项目，在自携设备（BYOD）数字识别、取证、数字身份和网络侦察领域发展出 6 个原型，用于进攻和防御目的。2016—2017 年，欧洲委员会内部安全基金（European Commission’s Internal Security Fund）是《国家网络安全研究议程》SBIR 的主要资助者（超过 90%）。额外的 330 万欧元（约 360 万美元）被分配给安全与司法部在这一领域最新的优先事项。

荷兰政府明白在研发和创新方面合作的重要性。除了与欧洲委员会的倡议，荷兰也有许多双边协定。例如，《美国—荷兰关于国土和民事安全问题的科学与技术合作协定》（US-Netherlands Agreement on Cooperation in Science and Technology Concerning Homeland and Civil Security Matters）促进了两国在对国家安全产生直接影响的领域进行双边合作。从 2012 年开始，两国同意在网络安全方面进行合作，包括事件管理和响应活动、控制系统安全以及网络安全演习。强有力的国际合作和经验分享促进了成本和知识共享，激发了创新和有效（国家）网络安全能力的发展。

荷兰在网络研发方面的投资由多个荷兰政府部门监管，荷兰应用科学研究组织和荷兰科学研究组织做出了重要的贡献。

荷兰的网络研发投资由多个政府部门监督，如国防、经济事务、安全与司法、基础设施和环境部，以及其他实体如 CSR——独立的国家网络安全委员会，负责在国家网络安全战略实施和发展、网络安全研究议程的执行等方面为政府提出建议。荷兰应用科学研究组织和荷兰科学研究组织也为网络研发做出了卓越贡献。荷兰科学研究组织每年会收到约 4 亿欧元(约 4.36 亿美元)的资金，其中 3 亿欧元（约 3.26 亿美元）直接来自教育、文化和科学部。荷兰科学研究组织有一个专门的网络安全计划，致力于将学术界和商界联系起来，促进产品、服务和知识的发展，提高荷兰数字化社会的安全。

例如，荷兰工业和学术中心在量子计算的材料科学和构成量子软件的信息协议及算法两方面有着各种倡议。在量子信息技术领域，世界各国都在争分夺秒。量子信息技术是一项重要应用，将改变网络中基础设施的安全性、隐私和完整性，以及通过这些基础设施进行的交易。其中一项名为 QuTech 的项目是由 TU Delft 和荷兰应用科学研究组织创建的，并接受来自荷兰经济事务部和教育、文化和科学部、荷兰应用科学研究组织、TU Delft、荷兰科学研究组织和私营部门等多种来源的资金。这一先进的研究所专注于量子技术和材料科学，十年之间已从政府方面收到超过 1.35 亿欧元（约 1.485 亿美元）的资金。此外，微软（Microsoft）和英特尔（Intel）等科技公司也对 QuTech 的量子研究进行了重大投资。除了 QuTech，荷兰科学研究组织通过荷兰国家数学与计算机科学研究所，与阿姆斯特丹大学、阿姆斯特丹自由大学和私营部门合作，共同资助对量子计算的新协议和算法的研究，并在最近推出了 QuSoft——一个新的量子软件研究中心。QuSoft 也将参与欧盟投资量子科学和技术的战略，并为其做出贡献，这是《地平线 2020》工作计划的一部分。欧盟表示它希望在 2035 年之前拥有量子能力。

荷兰科学研究组织的项目与《国家网络安全研究议程 II》和荷兰数字三角洲的 2016—2019 ICT 知识和创新议程（KIA）相一致，并与国际科学家、地方和全球企业以及高等教育机构进行跨学科合作。荷兰科学研究组织为网络安全相关项目提供的资金，分布于《国家网络安全研究议程 II》的 9 个研究主题，其中包括：身份、隐私和信任管理; 恶意软件和恶意基础设施; 攻击性网络能力等。然而，2011 年第一轮融资中，其长期研究的预算仅为 350 万欧元（约 380 万美元），2013 年第二轮融资中的预算也大致相同。荷兰政府在 2011 年的第一轮融资中，对短期研究项目的资助几乎是这

一金额的一倍，为 650 万欧元（约 700 万美元），在 2013 年的第二轮融资中却降低到 550 万欧元（约 600 万美元）。在这几轮融资中，政府总共资助了 40 个与网络安全有关的项目。在 2014—2016 年期间，荷兰科学研究组织没有在网络安全研究项目上大举投资。

此外，荷兰还参与了欧盟的《地平线 2020》计划，利用其高端产业政策，通过开创性的研发来加强私营部门和公共部门之间的合作，促进信息通信技术行业的增长。隶属于经济部的荷兰企业机构（RVO）的一部分，国际研究与创新合作小组（International Research and Innovation Cooperation team）是荷兰的欧盟项目国家联络点。

尽管有这些创新计划和雄心，然而要使荷兰成为“安全做生意的地方”和“欧洲的数字门户”，荷兰仍严重缺少能够保护其关键的基础设施和数字资产的网络安全专业人员。为了应对网络安全人才的短缺，2011 年国家网络安全战略建立了网络教育和培训中心，开始培养人力，支持该国日益增长的数字经济。《国家网络安全战略 2》重申了培训大量合格的网络安全专业人员的需要，并警告称，到 2017 年，荷兰的 IT 人员缺口将超过 6800 名。2016 年，荷兰网络安全理事会再次表示网络安全专业人员严重短缺，并建议加强各级网络安全教育。

荷兰各大高校和学术机构都提供带有网络安全集中课程的本科和研究生学位，但现有的大多数课程，包括阿姆斯特丹大学和莱顿大学等精英大学，仍然有着高度的技术性，或缺乏多学科的方法，无法将技术与政策、法律、经济、伦理和其他社会科学结合在一起。一些大学最近推出了硕士学位课程，将技术、法律、犯罪和心理问题结合在一起，包括隐私、知识产权、网络犯罪以及电脑相关的犯罪中的人为因素。例如，莱顿大学、代尔夫特理工大学和海牙应用科学大学，在海牙市政府的支持下，建立了一个多学科研究中心——网络安全学院，提供非全日制的管理硕士学术项目、短期课程和定制跟踪一系列的网络安全问题。然而，目前的网络安全项目应进一步扩展，纳入所有主要的技术性和非技术性学术项目，大学应该努力优化它们的校园资源，提供综合课程，将网络安全研究中的技术、政策、经济、社会学和法律组成部分结合起来。

最后，《国家网络安全战略 2》认识到荷兰在提高网络风险意识方面已经取得了进展，但要提高对网络威胁的认识，并提高整个社会的个人上网安全（Cyber Hygiene）水平，还需要做更多的工作。为了回应这一需求，荷兰政府（尤其是国家网络安全中心）定期赞助并参与一年中多项网络安全意识活动。其中包括：10 月份的欧洲网络安全月；“网上警报”运动是为期两周的公众努力，不同利益相关者将通

过组织讲习班、会议、演示和其他活动，共同促进荷兰公民、政府和私营部门的网络安全；“挂电话、别点击、给你的银行打电话”活动——由荷兰支付协会（Dutch Payments Association）推动，旨在告知荷兰公民如何保护自己不受网络欺诈；互联网安全日（Safer Internet Day）。尽管如此，这些意识活动将在何种程度上防止网络钓鱼或其他网络犯罪依然是未可知。最近，荷兰消费者协会（Dutch Consumers' Association）发起了“更新!”运动，鼓励安卓智能手机制造商向消费者提供软件更新，告知设备漏洞。作为这项运动的一部分，荷兰消费者协会在2016年对三星提起诉讼，指控三星“软件更新政策不佳”，并要求该公司遵守注意义务，在购买设备后至少两年向客户提供更新。

在2016年末的网络安全意识周“网上警报”期间，在荷兰网络安全理事会的请求下，PostNL的首席执行官赫娜·费尔哈亨向首相吕特展示了一份咨询报告（“Digitaal Droge Voeten”），其中她敦促荷兰政府以及企业将其年度信息通信技术预算的10%投资于特定网络安全措施。该报告被荷兰媒体广泛报道，原因是它发出了网络威胁增加这一令人担忧的信息，报告建议内阁任命一名网络安全高级官员，但并未提供有关荷兰网络研发投资状况的更多信息。

荷兰外交部发表了《国际网络战略》，承认所有利益相关者之间需要进行持续、开放和务实的对话。

荷兰高端产业政策承认了信息通信技术研发的重要性，但是为了面对费尔哈亨女士对首相所述的挑战，使荷兰实现其经济愿景，它需要将信息通信技术提升为第十个高端产业，将私人和公共资金的力量用于额外的研发。目前，网络研发分散于多个机构，因此局部最优化可能需要一个更广泛、更有影响力的愿景。此外，网络专家严重短缺，大学项目仍然缺乏超越技术手段的、全面的网络教育方法。荷兰与欧盟委员会（European Commission）、美国和其他国家采取的联合行动，提供了一个利用全球创新社区的机会。海牙安全三角洲和荷兰应用科学研究组织的网络威胁情报实验室，可能会被证明是建立数字未来网络安全解决方案的重要基础。

外交和贸易

网络安全是荷兰外交政策的首要任务。

荷兰政府已经将网络安全作为其外交政策中的一级优先事项，积极参与网络安全相关外交、贸易和商务谈判，促进网络空间务实合作，以及欧盟的数据保护和隐私相关倡议。荷兰目前正在进行各种关于网络安全、

网络犯罪检测和起诉、CSIRTs 合作和关键信息基础设施保护（CIIP）、信任建立措施（CBM）、网络能力建设、互联网治理、数字权利和负责任国家国际行为准则的国际讨论。

在2016年慕尼黑国际安全会议上，荷兰外交部长伯特·柯恩德斯（Bert Koenders）承认，“随着社会越来越依赖网络基础设施，增长和创新的机会似乎是无止境的、充满希望的。但我们面对网络事件、攻击（以及）破坏性极强甚至是毁灭性的网络事件也越来越脆弱”。他强调，荷兰承诺“加强网络防御系统，构建国际共识保护关键基础设施，如能源、电信、银行和互联网本身……保护数字版权，促进创新，提高网络安全，使用网络外交来开发一个通用规范框架，规范网络空间国家行为，维护国际稳定。”

此外，网络安全是 2013 年荷兰《国际安全战略》的一个重要主题，它确定了荷兰在国外采取的各种行动，并与其他国家合作，确保荷兰的国内和国际利益，促进国际标准和网络安全条例的发展。在 2013 年的《国家网络安全战略》（NCSS 2）中，荷兰政府重申了其与国际伙伴合作“建立一个安全开放的数字领域”，并“保护基本权利和价值观”的坚定承诺。它还重申要“在寻找新的防御、外交与发展联盟中扮演重要角色”，成为数字领域国际合作中的“网络安全调解人和中心”。2017 年 2 月，荷兰外交部（MFA）发表《构建数字桥梁》（Building Digital Bridges）——外交部的《国际网络策略：整合国际网络政策》（International Cyber Strategy: Toward an Integrated International Cyber Policy）——强调荷兰在外交、国防、发展方面应对来自敌对国家和网络罪犯的网络攻击的威胁的重要性。该战略呼应了之前的文件，支持“安全、自由和开放的互联网”，并鼓励荷兰在改善国际网络安全协议中发挥领导作用。它还强调有必要加强荷兰在各种国际论坛中的作用，提出“荷兰国际网络政策的明确愿景，以确保所有政府部门以连贯和有效的方式运作。”

为了促进网络空间稳定，达成包含各方的国际公认标准，荷兰一直倡导建立一个包含多方利益相关者的“互联网治理模型，将各参与者的利益考虑在内”，努力在欧盟内外建立各种正式和非正式的联盟。荷兰在国际舞台上非常活跃，它与联合国（UN）、欧洲理事会（Council of Europe）、北约（NATO）、经济合作与发展组织（OECD）、欧洲刑警组织（Europol）和其他跨国组织都有合作。国家网络安全战略和 2011—2015 年《数字战略》（Digitale Agenda）中的多方利益相关者主题，被荷兰积极表达在全球网络空间会议（Global Conference（s）on Cyberspace）——2011 年以来在伦敦、布达佩斯、首尔和海牙举行的一系列部际会议，被称为“伦敦进程”；表达在各国间建立信任措施（CBMs），它类似于欧洲安全与合作组织（OSCE）成员国之间的协定；

也通过参与国际电信联盟（ITU）、互联网治理论坛（IGF）和世界经济论坛（WEF）等其他多方利益相关者的组织被表现了出来。2015 年在海牙举行的第四次全球网络空间会议的一个重要成果是，发起了全球网络专家论坛（GFCE）——这是各国政府、政府间组织、科技界和学术界在网络能力建设方面交流最佳实践和专业知识的全球平台。GFCE 的任务是“确定可以在全球范围内复制的成功的政策、实践和想法”，并“制定切实可行的措施来建设网络能力”。

此外，荷兰开启了海牙进程——50 多个国家和《塔林手册 2.0》（Tallinn Manual）的作者之间进行的一系列的协商会议和活动，旨在建立和平时期的国家间法律。这项倡议的主要目标是促进国家间讨论，就国际法在网络空间中的应用达成共识。荷兰还与爱沙尼亚建立了网络规范平台（Cyber Norms Platform），以讨论联合国政府专家小组（UN GGE）在国际法上的投入，并于 2016—2017 年以正式成员身份加入联合国 GGE。此外，荷兰政府在建立新全球网络安全委员会（GCSC）方面发挥了关键作用。该委员会是一个全球机构，负责制定规范和政策倡议，以改善网络空间的稳定和安全。新的 GCSC 总部设在海牙，由来自 15 个不同国家的知名国际专家组成，包括外交官、学者和私营部门公司、公民社会和科技界的代表。荷兰外交部的柯恩德斯在 2017 年 2 月的慕尼黑安全会议上宣布 GCSC 成立。他说：“这是一项独特的倡议，它将确保我们将（现有的）活动向正确的方向发展……这需要我们所有人更加协调。需要制定规范，为所有人提供一个稳定和安全的环境。”

有海牙作为公认的国际和平与安全之城，荷兰致力于发展一个“网络外交国际中心”，汇集国际专家、政策制定者、外交官、军事人员和非政府组织，以促进网络空间的和平利用。该国已经将现有的荷兰中心的知识结合在一起，建立一个强大的多学科专业知识网络，来处理不同的话题，如冲突预防、军民合作和网络空间不扩散的国际标准。这些努力将成为一系列多方利益攸关方高层会议的基础。

另一个多方利益攸关方方法的例子，是建立一个安全、有保障、自由与和平的网络空间，它的捍卫者就是荷兰自由网络联盟（FOC）——荷兰外交部在 2011 年发起的一项联合行动，旨在支持互联网自由，并在网上促进民主和人权。今天，联盟有 30 个来自世界各地的成员国，荷兰正在推动其他国家加入。除了提供一个平台外，联盟使多方利益相关者开展会议和峰会，使联盟成员共享网上人权侵犯的信息，共同关切、限制网上言论自由的措施，并与公民社会和私营部门讨论有关互联网自由的紧迫问题，同时鼓励将现有标准融入新的创新产品和服务的设计中。

2011 年荷兰数字战略加强了经济、网络安全、ICT 信任和能力建设之间的联系。

事实上，荷兰经常处理发展合作问题，参与致力于发展中国家网络能力建设、网络安全能力建设和网络信任建设的项目。此外，荷兰是第一个提出支持加密和反对限制开发、可用性或使用加密算法的国家。

网络安全问题也经常被卷入贸易谈判和安全条约中。荷兰在上述各种国际论坛上参加了许多这样的讨论和谈判，并一直在国内实施和执行国际协定。荷兰在贸易谈判中作为数据隐私的拥护者，呼吁各国采用技术不可知论，以促进商品、服务、数据和跨境资本的自由流动。例如，荷兰参与了许多关于加密、入侵软件和军民两用技术出口规定的对话，比如《关于传统武器与军民两用货物和技术的出口控制的瓦森纳协议》（Wassenaar Agreement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies）中的规定，已经成为促进负责任披露（Responsible Disclosure）的先行规范。

网络问题逐渐出现在许多不同的传统国际关系领域，包括人权、经济发展、贸易协定、军备控制和两用技术、安全、稳定、和平与冲突解决。荷兰外交部负责协调荷兰在多国论坛上讨论网络安全问题时的参与和努力。然而，国际论坛上很多像计算机安全事件反应工作组和 CSIRTs 网络的技术讨论都超出了外交部的范围。当跨领域的问题需要多种专业知识来解决时，荷兰会建立特别工作组。例如，2015 年网络特别工作组（Task Force Cyber）成立，它作为安全政策部门和多边组织及人权部门的一部分，发展和倡导荷兰国际网络政策一体化。荷兰还在部门内设立了一名国际网络政策特使，直接负责网络安全相关的外交政策协定谈判，并“进一步传播全球网络空间峰会的结果和荷兰在网络领域的雄心与优先事项”。在经济和贸易谈判方面，经济事务、安全与司法、外交事务和国家网络安全中心开会讨论，决定共同立场，以确保经济或贸易代表团达到所期望的结果。荷兰打算在一些大使馆激活网络外交官网，加强其外交倡议。该网络将在外交部现有预算下运行。

荷兰除了拥有自己的外交和经济政策立场外，还利用 2016 年其欧盟轮值主席国地位，更广泛地推进网络安全对话。通过荷兰的领导，在网络犯罪国际合作领域产生了新的倡议，重申了全面的欧盟网络安全战略的重要性。到 2017 年底，欧盟委员会预计将发布第二个欧洲网络安全战略。

显然，荷兰在这方面有着根本的国际利益，而且一直倡导自由、开放和安全的互联网。在经济上，它是信息通信技术产品和电信服务的十大出口国之一，荷兰广泛的数字经济增长超过了 22%。它的外交行动集中在加强国际合作和法律框架，同时减少犯罪、间谍活动、人权侵犯和其他有害的网络活动。今后，荷兰政府应采取一种更

综合的方法，将外交、经济事务、安全与法律部的专门知识集中起来，在实现经济目标的同时确保其安全优先事项。荷兰政府努力确保其国内和外交政策议程之间的一致性，这样它就不会破坏其在谈判桌上的信誉。荷兰已经建立了品牌，并通过海牙市被认可为国际和平与安全的领导人。今天，在这个品牌的基础上，荷兰通过利用欧洲刑警组织的网络犯罪中心、建立海牙安全三角洲进行网络创新，并启动海牙进程，理清国际法律应如何适用于网络运营，成为了网络安全的领导者。

防御和危机响应

在 20 世纪头十年的末期，使用军事级武器攻击国家关键基础设施，以及在军事行动中使用网络，催化了荷兰国防部（MoD）采取措施更好地训练、组织和装备武装部队，以保护荷兰并增强其军事姿态。尽管有军备缩减和其他领域的广泛预算削减，国防部仍积极投资其武装部队的网络作战能力。与此同时，国防部开始公开讨论建立更加健全的网络安全态势这一任务的重要性和必要性。为了“保护国家，荷兰正在发展强大的能力，以早期发现、积极防御和必要时干预为目标”，增强这些能力以支持荷兰利益。

2010 年里斯本北约峰会和《北约网络防御概念、政策和行动计划》的发布，使荷兰政府开始反思其 2011 年第一个《国家网络安全战略》和随后的网络防御计划中的一些相同概念和承诺。

2012 年荷兰《网络防御战略》（Defence Cyber Strategy）承认，军事和民用、公共和私人、国家和国际行为者在网络空间中相互交织。国防部长在给这一战略的附信中称，网络空间是“除了空中、海上、陆地和太空的第五个军事行动领域”。2012 年国防网络战略描述了荷兰武装部队在数字领域的作用，并提出了 6 个重点行动领域：①采用综合方法；②加强防御组织的网络防御（防御性因素）；③加强进行网络行动的军事能力（进攻性因素）；④加强网络空间情报工作（情报要素）；⑤加强网络空间防御组织的知识地位和创新力量，包括有资格人员的招募和保留（适应和创新要素）；⑥加强国内和国际合作（合作元素）。

在 2012 年战略的基础上，2015 年《网络防御战略》（Defense Cyber Strategy）扩大了荷兰的整体网络行动，并强调了“为荷兰在网络空间的成功创造合适条件”的 7 项关键举措。其中包括：①吸引知识渊博的网络专业人士；②加快能力建设，促进快速吸收；③通过伙伴关系加强国家数字韧性；④培训和教育人才，使其了解数字世界的机遇和危险；⑤加强和强化国防网络、IT 服务和系统；⑥使 2002 年《情报和安全部队法》（Intelligence and Security Services Act）现代化，扩大网络情报能力；⑦增强

军队网络作战能力。

为了实现这些目标，荷兰将这一领域的职责进行分类并划分为以下主要职能领域：

（1）联合信息管理组织（Joint InformatieVoorzienings Commando, JIVC）自 2013 年开始运营，负责保护和监测荷兰和行动领域的所有军事网络、IT 服务和系统。它的主要作用是保护和防御。荷兰国防计算机应急响应小组（DefCERT）是 JIVC 的一部分，负责监督和确保信息系统的可靠性和畅通，支持军事行动。DefCERT 是报告和响应国防部内部网络事件的第一联络点，负责进行威胁和脆弱性评估，为武装部队安全措施提出建议。

2014 年成立的荷兰网络司令部，其使命是为网络空间的操作自由和荷兰武装力量的战斗能力做出贡献。

（2）军事情报和安全部（MIVD）与内政部和王国关系的一般情报和安全部队（AIVD）一同负责网络情报。2015 年，AIVD 和 MIVD 将其信号情报和网络能力结合为信号情报网络部门（JSCU）——一个负责保护国家安全和荷兰互联网免受网络威胁的部门，同时也在任务中为武装部队提供更好的支持。此外，MIVD 还积极与 DefCERT 在计算机网络防御（CND）领域合作，一起对国防部内部的网络事件进行调查。

（3）网络防御司令部（DCC）是负责武装部队指挥官网络任务的直接联络点。DCC 还负责协调国防部所有四项部队（陆军、海军、空军和军事警察）行动的所有任务和网络作战能力，包括攻击能力加强和部署。

2014 年 9 月，荷兰宣布成立专门的网络防御司令部（DCC）。今天，DCC 是军事行动的组成部分，为所有任务提供防御和进攻能力，任务包括和平时期行动、危机管理和人道主义援助。荷兰是第一个公开讨论攻击性网络行动作为重要国家力量要素的北约国家。“与部署其他类型的部队一样，在部署进攻性网络能力方面，荷兰认为必须采取极端克制，只有在国家或国际法方面有足够的基础时采取行动。”作为 DCC 的指挥官，准将汉斯·福尔默说：荷兰网络司令部的使命是通过准备、培训和部署网络作战小组，为在网络空间的行动自由和荷兰武装部队的战斗力做出贡献。这些团队提供综合的军事行动网络能力，支持荷兰武装部队的全部网络军事作战。作为联合网络行动特遣部队的一部分，从防御性网络行动到进攻性网络行动，他们都会参与计划、协调和执行，产生直接或间接影响。

除了保护、情报和行动之外，DCC 还协调所有的 DOTMLPF 活动（包括任何理论、组织、培训、军备、领导和教育、人员和设施的组合）。它“在荷兰国防部内，与军事和民用、国内和国际伙伴一起，协调并促进这些网络活动和能力”。此外，司令部

获得、传播和管理整个荷兰武装部队的网络专业知识，为教育、培训和训练做出贡献。

荷兰 DCC 已经公开讨论了 6 种不同类型的网络行动，有些类似于其他国家制定过的，有些是荷兰制定的新的、更独特的行动：

（1）网络安全行动——注重保护、防止损害和恢复的被动防御措施。

（2）防御性网络反击行动或积极对策——中和荷兰网络中活动威胁的行动，对网络入侵、网络攻击或即将到来的网络行动进行检测和信息收集，确定入侵来源或终止恶意网络活动——这些操作不超越荷兰国防部的网络范围。

（3）在荷兰国防部网络之外进行的进攻性反击网络行动。这些是对攻击进行响应的军事网络行动，包括对网络威胁源发起先发制人和预防性的反击行动。

（4）网络情报、监视和侦察行动——较低水平的网络操作，其唯一目的是收集有关网络空间中其他参与者活动的一般数据或信息。这些行动不包括国防情报和安全部队的活动。

（5）支持型网络操作——在和平时期、危机或冲突情况下，支持其他更多的战术级别活动的小型技能行动。由于其种类繁多，这些行动特别有助于信息战的支持，例如心理作战、欺骗、作战安全、法律战和电子战。

（6）进攻性网络作战或作战行动——要么作为另一领域作战的支持，要么只在网络空间执行，只是为了实现军事目标（赋予指挥官实现作战的能力）。

“网络作战现在必须整合在军事任务中，成为任务指挥官工具箱中的另一个工具。”

在2016年国际网络冲突会议(International Conference on Cyber Conflict）上，准将福尔默承认，“荷兰在所有的军事作战中都包含了攻击性网络行动选择”，并强调“现今的网络作战必须被包含在军事任务中，成为指挥官工具箱中的一个工具。在发展军事进攻能力的时候，我们应该把重点放在打击正当目标上，减少负面的间接影响。这意味着重点应该放在计划、决策、记录、测试、培训等方面。”除了国内的努力外，荷兰与北约通讯和信息机构以及加拿大、丹麦、挪威和罗马尼亚，还参加了北约多国网络防御能力发展项目（Multinational Cyber Defence Capability Development Program）。

荷兰国防部参加了两年一次的国家级危机应对演习。此外，荷兰武装部队积极参与多国和联合网络演习——正如事件反应部门所指出的那样，特别是所有与北约有关的如“网络联盟”和“网络大西洋”演习。它还与德国和其他北约国家一起进行了双边合作演习。此外，荷兰政府领导了北约内部将网络融入正式军事过程的情景制定和讨论。在 2016 年 7 月华沙峰会期间，北约成员国同意加强国家网络和基础设施的网

络防御，提高韧性和快速有效应对网络攻击的能力，调整网络防御能力。北约认同网络空间是第五个战争领域。

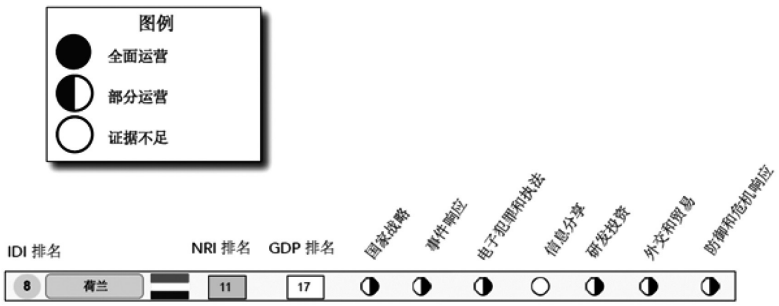
DCC 和国防部明显正在从现有预算中支持网络任务。虽然大部分国防部的预算是保密的，但是 2017 年的国防预算显示网络预算增加 1657 万欧元（约 1850 万美元）。同一国防预算还将 4.12 亿欧元（约 4.6 亿美元）分配到 IT，但还不清楚有多少分配给了网络防御或进攻能力。荷兰正在投资培训和招聘活动，专注于研发和国际合作，以支持其网络防御任务。荷兰国防部正在使用招募技术来吸引道德黑客，并强调这些任务在正确的权力下是合法的。他们还与关键行业的领袖合作开发了一项技能培训计划，培训有志向的士兵成为网络技术专家。最后，认识到顶尖人才的稀缺性和优化方法的必要性，AIVD 和 MIVD 成立了联合信号情报网络部门。在这一不断变化、挑战越发严峻的领域，集中稀缺的知识和资源（资金和人员）是必不可少的。

荷兰宣布网络空间为“军事行动的第五个领域”，并正在组织执行这项任务。该国清楚地认识到，安全不仅是一个正常社会运转的先决条件，而且是其经济的未来。然而，它的愿景和雄心并没有得到足够的资金、物资或人力支持。这意味着荷兰人必须充分利用他们的务实态度，找到吸引、发展和留住人才的创造性手段；与欧盟、北约和其他联盟合作，利用它们获得能力；并说服新政府为其雄心勃勃的议程设立专项资金。

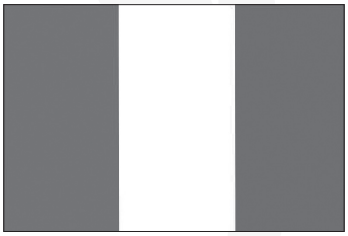
CRI 2.0 结论

根据网络就绪度指数（CRI）2.0 的评估，荷兰正走在网络就绪度完全的道路上，目前在大部分 CRI 的基本要素中都有部分行动。

现状是动态且不断变化的，这一分析结果只是一个概要。荷兰将继续开发和更新其经济（数字议程）和国家网络安全战略、政策和计划，找到更为平衡的方法，使其国家经济愿景与其国家安全优先事项对应，对荷兰状况的更新将会反映这些变化，并对实质性的、显著的改进进行监控、跟踪和评估。



意大利网络就绪度报告



人口	6080 万人
人口增长率	0%
市场价格 GDP（美元）	1.815 万亿美元
GDP 增长率	0.8%
引进互联网年份	1988
国家网络安全战略发布	2013
互联网域名	.it
每 100 名用户中，固定宽带用户量	23.5
每 100 名用户中，移动宽带用户量	70.9
每 100 名用户中，移动电话用户量	154.2

信息通信技术（ICT）发展和连通性排名

国际电信联盟（ITU）信息通信技术发展指数（IDI）	8	世界经济论坛网络就绪度指数（NRI）	5

数据源：世界银行（2015）、国际电信联盟（2015）、世界经济论坛网络就绪度指数（2015）和 Internet Society.

概述

意大利最初的计算机网络出现于 20 世纪 80 年代，当时，一些核物理学家将该国所有的核研究机构连接在了一起。1988 年，它成为一项更广泛的科学学术项目的一部分，将各科学机构及其大型计算机统一在一个网络中（Gruppo Armonizzazione UNK della Ricerca,GARR）。

几年后，第一家商业互联网服务提供商（ISPs）诞生（1992—1993），意大利开始将其电信行业私有化。直至 20 世纪 90 年代，电信服务都是由意大利政府控股的一批企业提供的，政府通过工业重建研究所和意大利电信协会（Istituto per la Ricostruzione Industriale/Societa Italiana per l'Esercizio Telefonico, IRI–STET）对这些公司进行控制。1994 年，根据《电信行业改革规则》（Rules for the Reform of the Telecommunications Industry），这批企业中的五家公司合并组建了意大利电信（Telecom Italia）。三年后，意大利电信与 STET 合并，保留意大利电信的名称并成立了一家私营企业。20 世纪 90 年代末，政府所有权已被逐步撤销。尽管意大利电信仍为该国最大的通讯服务提供商，但在 20 世纪 90 年代私有化之后的一段时间内，也出现了许多其他互联网服务提供商。

自 20 世纪 90 年代以来，意大利政府支持互联网的发展并将其作为增长经济、发展旅游业、减少通讯成本和促进政务高效的催化剂。然而，意大利的互联网普及率（62%）与其他欧洲国家（79%）相比仍然较低，其高速互联网连接的可用性在欧盟国家中是最低的。与此相反，移动宽带用户数量稳步增长，为总人口的 154% 以上——这意味着意大利公民更偏向于移动宽带连接。手机用户数量的激增，可能是由于 2012 年至 2014 年间意大利移动服务价格的大幅下降，这是整个欧洲价格降幅最大的一次。

尽管如此，意大利人在电子政务、电子银行和电子商务方面的参与度（约为 20%）仍然落后于欧洲大部分地区（欧盟平均参与度为 40% ~ 50%），只有不到 10% 的国内公司开放在线销售。这些数据较低的原因是基础设施的限制、下一代接入（NGA）网络的低可用性以及过往政府投资策略的片面和重复。提高互联网普及率的其他障碍，包括人口老龄化、先进技术技能缺乏、对在线交易的不信任和意大利南北部地区间长期存在的数字化、教育和收入差距。过往挑战和长期挑战的叠加束缚，使意大利无法在互联网速度和可访问性、数字素养和网络现代化上达到欧盟水准。

2015 年，意大利政府实施了 60 亿欧元（约 67 亿美元）的《数字增长战略 2014—2020》（Strategia per la Crescita Digitale 2014—2020）。数字战略旨在扩建互联网基础设施并使其现代化、改善高速宽带接入并扩大电子政务功能（如数字身份、公共电子服务和智能社区），这些机制将“通过发展商业技能并在公民中传播数字文化，保证经济增长和社会进步”。国家数字增长战略承认意大利在经济发展、互联网普及率、公共和商业活动数字化以及数字素养方面落后于其他欧洲国家。它还承认利用市场手段（如《欧洲单一数字市场战略》中所规定的）干预的必要性，以使国内生产总值（GDP）增长 3%。

根据 2010 年《欧洲数字议程》（European Digital Agenda）——《欧洲 2020 战略》（Europe 2020 Strategy）的七大内容之一——中设定的目标，2015 年意大利国家数字增长战略确定了几项重点和具体行动，以帮助促进信息通信技术的广泛应用、保证数字服务访问安全并鼓励各政府机构间信息系统的合作及其与欧盟之间的合作。此外，战略还设定了明确的目标和截止日期，用于显示数字战略目标进程。特别地，随着网络上电子政府和医疗服务的增多，数字战略强调要改善其中关键服务的安全性，以确保公民通讯的隐私和完整以及通讯服务的连续性。

数字意大利机构（Agenzia per l’Italia Digitale, AgID）于 2012 年在总理办公室成立，它负责实施国家数字战略及各种相关任务，如推动和传播信息倡议；公民和公务员的数字化培训；监督 ICT 计划实施，以提高公共管理效率和透明度；加强公共信息系统之间的合作；协调为公民和企业提供网络服务的倡议；制定技术要求和指导方针，确保全国服务互通性。在中央和地方政府，包括自治区和省政府以及其他部门的积极参与下，该机构按要求协调各方努力。

此外，总理办公室与经济发展部（Ministry of Economic Development）、数字意大利机构和协调机构（Agency for Cohesion）正合作执行其他项目，例如“全国超高速宽带计划”（National Plan for Ultra-Wide Broadband）”和“数字增长”（Digital Growth）计划，以加速实现国家数字战略目标。这些目标包括在 2020 年之前为至少 50% 的意大利人提供高速互联网接入，以及将光纤网络扩展到农村地区。意大利主要的互联网服务提供商，如 Fastweb、Vodafone 和 Wind 也形成了共同投资伙伴关系——“意大利光纤”项目，这一项目与意大利电信宣布的另一个计划相结合，计划在 2018 年将光纤网络普及到所有大城市。

与许多发达国家一样，网络安全对意大利来说是一个重要挑战。在过去，由于缺乏官方统计数据，且受害者倾向于不报告事件或通知当局，要想评估恶意网

络活动对意大利的个人和组织有多严重的影响，是有些困难的。意大利安全情报部门（DIS）在其年度报告中指出，2015 年，针对政府实体和高科技产业的网络间谍活动，其规模、数量和复杂性都有所增加。报告估计，在意大利，几乎 70% 的网络攻击是针对公共实体的，而主要的威胁者（以攻击活动记录的百分比为准，并非威胁级别）是各种黑客组织。此外，在 2016 年，意大利信息安全协会（Associazione Italiana per la Sicurezza Informatica, CLUSIT）估计，2016 年上半年，意大利网络犯罪增长了 9%，造成了 71% 的网络攻击。协会在 2016 年半年报中还指出，自 2013 年以来，由于网络安全造成的经济损失翻了两番。网络攻击来源国家排名中，虽然意大利的名次不高，但它却是欧洲和中东地区第二大受感染国家。土耳其、意大利和匈牙利是欧洲、中东和非洲地区网络机器人最多的三个国家。事实上，因为近几年这三国的高速互联网和连接设备的大幅普及与增加，对黑客来说它们是很有吸引力的目标，且增加的连通性也并未引起安全意识的提升。

网络安全这一主题是由当时的副总理兼意大利议会安全委员会（COPASIR）主席弗兰西斯科·鲁泰利在 2009 年提出的。他首次发起了一系列议会磋商，讨论“网络空间的使用对国家安全的潜在影响和威胁”。意大利议会安全委员会的后续讨论和听证会结果，形成了 2010 年《给议会和政府关于网络安全及其对国家安全影响的第一次报告》（First Report to the Parliament and the Government on Cybersecurity and Its Implication for National Security）。报告敦促政府制订战略计划和适当的机制，以打击网络犯罪并保护计算机网络。特别的是，报告建议制定国家网络安全战略，以“保证充分的领导和明确的政策指导方针，以打击（网络）威胁，并促进所有利益攸关方之间的协调”。此外，它还建议设立主管部门，将其放在内阁办公室（Presidenza del Consiglio dei Ministri）的职责下，负责执行所有网络安全相关活动。当时，报告中的大部分建议被忽视，直到意大利经历了一系列的网络事件，其中包括匿名者（Anonymous）对意大利内政部的大范围攻击，这次攻击曝光了大量敏感文件和电子邮件。

最终，意大利政府花了 3 年时间制定了其第一个国家网络安全战略。2013 年总理的《国家网络保护和信息安全战略指导方针》（Decree Containing Strategic Guidelines for National Cyber Protection and Information Security）首次概述了国家网络安全架构中的机构和组织结构，并赋予总理国家网络安全的直接责任。在这一方针之后，《国家网络空间安全战略框架》（National Strategic Framework for Cyberspace

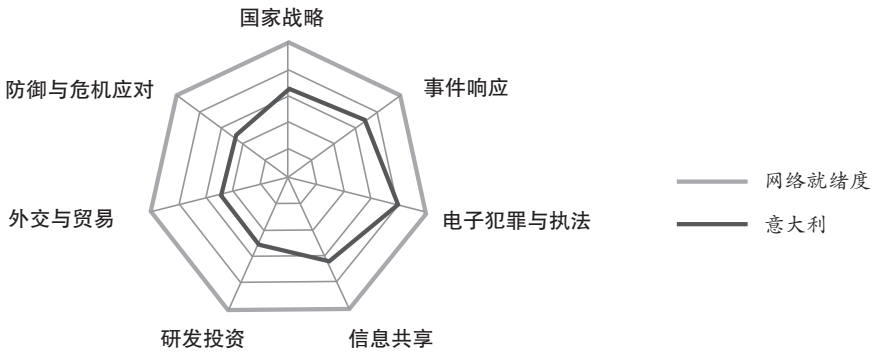
Security）及其配套实施方案《国家网络空间保护与信息通信技术安全计划》（National Plan for Cyberspace Protection and ICT Security）于 2013 年发布。这两份文件一起构成了一个全面的战略，它包括：描述网络不安全对国家安全和经济造成的风险；评估意大利的网络安全能力；明确界定涉及国家网络安全的不同实体的作用和责任；要实施的具体战略和业务目标。

除了国家网络安全战略和实施计划，意大利安全情报部门和数字意大利机构还支持了 2015 年的《国家网络安全框架》，框架由意大利网络安全国家实验室（Italian Cybersecurity National Laboratory）和罗马大学网络情报和信息安全中心（CIS–Sapienza）根据 2013 年美国国家标准与技术研究院（NIST）《改善关键基础设施网络安全框架》（Framework for Improving Critical Infrastructure Cybersecurity）所制定，是自愿指南。这一自愿框架为反映意大利国情进行了扩展和更新，旨在为组织提供“一种同质且自愿的方式来面对网络安全。”它还为各主体提供了现有标准和法规的参考指南，帮助其评估目前的风险状况和成熟度水平，确定网络防范的优先级和目标级别，最终降低网络威胁相关风险。这一自愿框架的重要目标之一是提供指导方针，提高意大利中小企业（SMEs）的网络安全水平，为大型公司 C 级管理人员提供建议，帮助关键基础设施运营商制定网络安全风险管理过程。

尽管发布了国家网络安全战略并重组了相关国家网络安全架构，但在国家层面上，意大利和欧盟成员国之间的网络风险预备程度仍然存在很大差距。虽然意大利已经提出了一些与网络安全有关的倡议，但其中许多仍是支离破碎的，似乎没有一个中央协调机制来保证国家的经济和安全目标得以实现。然而，意大利政府承认使用信息通信技术的好处和威胁，2013 年的《国家网络安全战略》和 2015 年的《国家数字增长战略》都清楚地认识到了将互联网连通性和信息通信技术作为推动经济增长的关键因素的重要性。此外，2015 年《国际安全与防御白皮书》（White Paper for International Security and Defense）从战略上将网络防御和防御性军事行动列为 2016—2018 年的主要投资项目之一。意大利政府决定在国防部内部建立网络司令部（Cyber Command），该司令部的第一个部门有望在 2017 年开始运营，这似乎意味着在网络空间内，意大利政府对自身和经济的保卫正逐渐加强。

网络就绪度指数 2.0 被用来评估意大利的网络风险防范水平。这一分析为意大利提供了一个可行的蓝图，以更好地了解其网络基础设施的依赖和漏洞，其当前网络安全态势与实现数字未来所需的国家网络能力之间的差距，评估意大利缩小该差距的承诺和成熟度。基于网络就绪度指数 2.0 的七个基本要素（国家战略、事件反应、电子

犯罪和执法、信息共享、研发投资、外交和贸易、国防和危机应对），全面评估了意大利的网络安全相关努力和能力。



意大利网络就绪度评估（2016）

国家战略

在 2013 年颁布的总理《国家网络保护和信息安全战略指导方针》后，网络安全工作组（Tavolo Tecnico Cyber, TTC）成立，由国家安全跨部门委员会（Comitato Interministeriale per la Sicurezza della Repbblica, CISR）赞助，主席由安全情报部门（Dipartimento delle Informazioni per la Sicurezza, DIS）担任，负责制定第一个意大利国家网络安全战略。

2013 年，意大利第一次发布了国家网络安全战略，应对网络空间安全威胁和挑战的能力得以增强。

依照 2013 年的总理法令和 2013 年欧盟网络安全战略（紧随其后的是 2016 年欧盟《关于网络和信息安全的指令》（NIS）），每个欧盟成员国都应建立《网络与信息安全战略》。意大利于 2013 年颁布了《国家网络空间安全战略框架》这一国家战略，以及实施方案《国家网络空间保护与信息通信技术安全计划》。该国家战略“突出了网络威胁和国家信息通信技术网络漏洞的性质和发展趋势，概述了公共和私人利益攸关方在网络安全中的角色和任务，确认了提高国家网络就绪度程度的工具和程序”，实施方案则“确定了一组有限的优先事项，提供了具体的目标和指导方针以具体实施《战略框架》”。这两份文件共同构成了一个全面的国家网络安全战略，“围绕这一战略协调各方努力，使意大利自信地面对网络空间中的安全威胁和挑战，追求国家利益，积累国家财富，变得更加繁荣”。

专注于互联意大利的长期目的和目标的同时，要减少其网络不安全因素可能很难，因为意大利还面临其他互相冲突且长期存在的结构性挑战。平衡经济优先事项和国家安全需要是很棘手的。意大利面对着 GDP 增长迟缓、生产率低下、背着“坏”债的银行部门和高失业率的挑战。意大利政府提出了一系列振兴经济、解决意大利财政问题的方案，但这些努力还未见成效。此外，即将举行的有关参议院（议会上院）未来的宪法公投，可能会进一步分散政府在重要国家网络安全问题上的注意力。

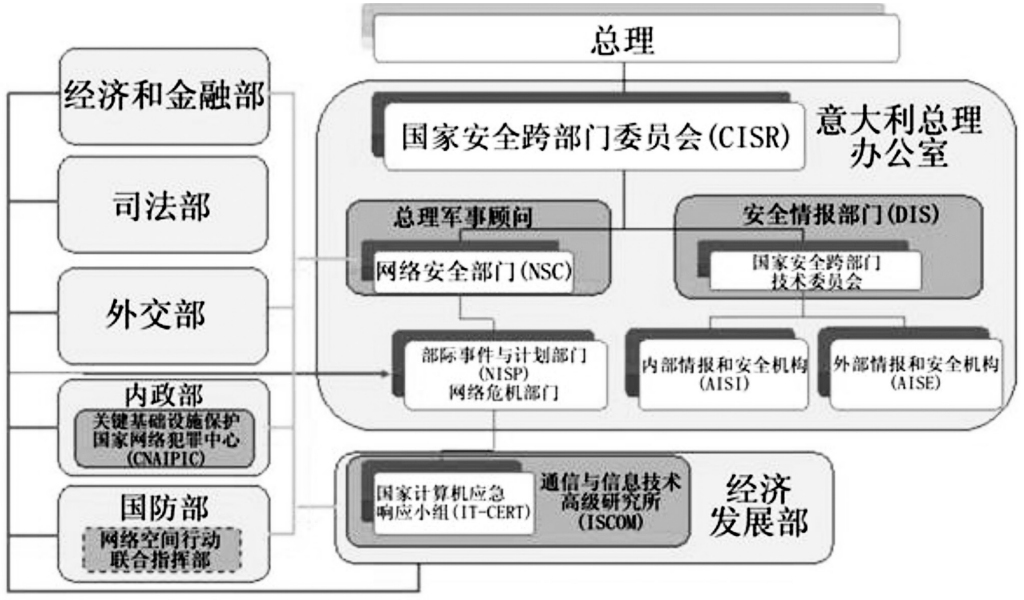
2013 年《国家网络安全战略》承认，考虑到“当前的金融和经济紧缩”，政府和利益相关方不应“有任何重复努力”，应“寻求任何可能的协同作用，要记住，与网络攻击可能造成的破坏相比，分配预算不仅是一种节省，而且是文化、社会和经济增长的非凡机会”。《实施计划》制定了明确的目标，其中许多已经开始执行，有些甚至已经完成，这包括加强情报、治安、民事保护和军事防御能力；建立国家计算机应急响应小组（CERT）；进行国际演习；促进临时立法和国际义务履行。

总理办公室下的网络安全部门（NSC）负责协调国家网络安全架构中所有政府机构的活动。

网络安全协调直接由内阁办公室（Presidenza del Consiglio dei Ministri）负责。意大利总理办公室（或 Presidency of the Council of Ministries）将通过颁布具体指令，正式负责制定、执行《国家网络安全战略》和《实施计划》。国家安全跨部门委员会（CISR）将支持总理办公室的这项努力，它主张采用额外立法倡议，批准促进公私伙伴关系的指导方针，引入政策以加强信息共享安排并拥护最佳实践，促进国家网络安全领域中机构和私有市场参与者之间的协作，批准其他措施，增强国家网络安全。国家安全跨部门委员会由总理主持，由外交、内政、司法、国防、经济和金融，以及经济发展部门组成。当讨论网络安全问题时，总理的军事顾问将参加委员会会议。意大利安全情报部门总干事担任委员会秘书。工作级别的国家安全跨部门委员会被称为国家安全跨部门技术委员会（Technical CISR），负责支持委员会工作，进行内部定期审查和评估，确认安全战略和相关计划的及时正确执行。此外，在活动中，工作级别委员会将得到各种国家情报公共实体的协助，包括安全情报部门、外部情报和安全机构（Agenzia Informazioni e Sicurezza Esterna, AISE）及内部情报和安全机构（Agenzia Informazioni e Sicurezza Interna, AISI）。意大利政府目前正在更新实施计划。

2013 年的总理法令建立了网络安全部门（Nucleo per la Sicurezza Cibernetica,

NSC），它是总理办公室的常设机构，由来自外交部、内政、国防、经济和金融、经济发展、民防部门、安全情报部门、外部情报和安全机构、内部情报和安全机构、数字意大利机构的代表组成。网络安全部门直接向总理的军事顾问汇报。它负责协调国家网络安全架构中各种机构的活动。特别地，它负责所有的国家网络安全防范、风险评估和缓解、事件应对和危机管理活动。网络安全部门也负责恢复网络和系统功能，是国家和国际组织的正式联络点。在发生需要多个部门参与的大规模网络事件时，网络安全部门将以部际网络危机部门（Tavolo Interministeriale di Crisi Cibernetica）的形式，启动部际事件与计划部门（Nucleo Interministeriale Situazione e Pianificazione, NISP）来监督事件响应合作。国家计算机应急响应小组负责技术响应措施，并通过意识、预防和网络事件响应（参见“事件响应”部分）支持公民和公司。



意大利网络安全组织图（2016）

2015 年的总理指令为所有主要利益相关者提供了有关 2013 年国家网络安全战略的额外实施指导，包括提高国家层面的网络就绪度、安全和抗打击能力，并“将战略能力与国际标准结合起来”。该指令的其他方面包括指导建立更全面的机构架构，培养更强的事件响应能力，与公共实体以及电信和关键基础设施行业的私营部门经营者进行更密切的合作。

2013 年国家网络安全战略提到了分配“足够的人力、财力、技术和物力资源”对实现目标的重要性，但它并没有承诺任何的特别资金。在 2015 年的数字增长战略中，意大利政府承诺 5000 万欧元（约 5600 万美元）用于保护公民和企业的数字身份，确保数字服务的安全访问，包括从移动设备的访问。2016 年《稳定法》（Legge di Stabilit á 2016）批准了 2016 财政年度预算，分配 1.5 亿欧元（约 1.66 亿美元）给国家网络安全工作，其中 1500 万欧元（约 1660 万美元）将用于意大利邮政和通信警察队（Italian Postal and Communications Police Service）及其关键基础设施保护国家网络犯罪中心（National Cybercrime Centre for Critical Infrastructure Protection, CNAIPIC），该中心特别负责所有针对重要基础设施的网络犯罪和其他恶意网络活动的预防、控制、减轻和调查。最后，最近一次 2016 年 9 月的总理法令，将剩余的 1.35 亿欧元（约 1.49 亿美元）的 2016 财政年度预算分配给了安全情报部门下的国家网络安全工作，以加强国家层面网络风险的传统防范和防御措施，同时将保护国家网络空间优先化。

事件响应

2015 年，意大利成立了其第一个国家计算机应急响应小组（IT-CERT），负责遏制和应对大规模网络事件。

意大利没有一个统一的国家事件响应计划，2013 年有关国家网络保护与信息安全的总理法令和《国家网络安全战略》都将协调网络事件应对活动、恢复网络和系统功能的责任分配给了网络安全部门（NSC）。此外，在发生的网络事件与国家安全有关，或其规模较广，需要各部长合作应对时，网络安全部门可以激活部门间网络危机事件与计划部门（Inter-ministerial Situational and Planning Unit for Cyber Crisis, NISP）这一非常设部门。

此外，提供信息服务的意大利私营部门公司以及关键基础设施运营者，不论是国家还是欧洲级别，都必须将其网络中所有相关违法行为通知网络安全部门，并采取具体的网络安全措施。

国家计算机应急响应小组（CERT Nazionale 或 IT-CERT）成立于 2015 年，响应了 2013 年《国家网络安全战略》的临时指南，符合 2013 年欧盟战略中“开放、安全、可靠的网络空间”的要求和随后的《欧盟网络安全指令》。应急响应小组设于经济发展部中，由通信和信息技术高级研究所（Istituto Superiore delle Comunicazioni e delle Technologie dell’Informazione, ISCOM）主任领导。它的任务是促进大规模的网络事件的遏制和应对。它还为广大国内选民提供了一系列其他自主或选择服务，例如：及时

发布网络漏洞和威胁的警报和建议；宣传网络安全意识和最佳做法；与国内和国际的应急响应小组合作；支持恢复活动。

除了国家计算机应急响应小组发布的网络安全新闻和警报，安全情报部门还会定期对网络威胁进行分析和评估，发布年度《安全情报政策和成果报告》（Report on Security Intelligence Policy and Results Achieved）。这一年度报告会突出对关键、有形和无形基础设施的防御活动；国家网络空间以及信息安全。

2012 年，意大利政府通过了一项法律，要求安全情报部门对关键基础设施的安全控制提供技术指导，并与私营部门共享网络威胁和预警数据。此外，拥有国营成分的公司，如 ENEL（电力）、ENI（石油 & 天然气）、Poste Italiane（邮政服务）、ENAV（空中交通管制）、TrenItalia（铁路网络），以及意大利中央银行（Italian Central Bank）与安全情报部门签署了一项合作协议，自愿报告泄露事件并共享威胁数据。2013 年的《部长法令》更新了 2012 年的法律，要求所有电信运营商和其他关键基础设施运营商，与安全情报部门和其他负责国家安全的政府实体合作（如 IT-CERT、CNAIPIC）响应网络事件，确保服务的连续性。

虽然欧洲各国间的数据泄露通知要求仍然不同，但是意大利政府已经采纳了 1995 年《欧盟数据保护指令》和 2016 年《欧盟网络和信息安全指令（NIS）》的许多规定，以提升网络安全能力，促进全欧洲的合作。例如，意大利在 1996 年已经建立了一个数据保护机构（Garante per la Protezione dei Dati Personali）。这一由四人组成的学院机构，其成员每 7 年由议会选举产生，负责监督政府和非政府实体对所有意大利数据保护和隐私法的合规。数据保护机构对公共行政实体和其他组织采取了一系列规定，这些规定详细说明了数据泄露的通知要求。例如，电信和互联网服务提供商（ISP）在经历数据泄露后，要在发现事件的 24 小时内通知数据保护机构，并在 3 天内通过其网站上提供的表格补充额外信息。

此外，两个委员会——行业技术工作组（Tavolo Tecnico Imprese）和政府网络安全工作组（Tavolo Tecnico Cyber, TTC）将作为关键行业和政府实体的额外联络点，这些实体对于关键服务和基础设施的运营和恢复至关重要。此外，包括内政部、国防部、公共行政和创新部、基础设施部、警察和其他执法机构、民防部门和情报机构在内的，所有与国家安全事件有关的政府机构和办公室，都将参与关键基础设施保护协调工作组（Critical Infrastructure Protection Coordination Working Group）。最后，2013 年《国家网络安全战略》要求意大利与公共部门利益相关者和相关私营部门经营者合作，定期进行全国网络安全演习。

电子犯罪和执法

2001 年，意大利签署了《欧洲委员会关于网络犯罪的公约》（Council of Europe Convention on Cybercrime，通常被称为《布达佩斯公约》），该公约于 2008 年被批准。尽管意大利自 20 世纪 90 年代初以来已经修订并加强了其《刑法》，对计算机犯罪和电子犯罪进行了全面覆盖，但它还未完全执行《布达佩斯公约》中所包含的跨境援助选择。政府早期试图监管互联网的一些尝试所依赖的法律，也同样适用于印刷和广播媒体，传统媒体对人权、隐私和信息自由的影响与网络不同。例如，一些早期的法律提出，关于数据保护，出版商应对其所有出版物的内容负责，当这些法条应用于互联网，特别是由用户生成内容的网站时，就可能被视为网络审查，与欧盟对互联网内容的指令相矛盾。

2011 年的一项法律废除了一项有争议的条款，该条款是 2005 年在伦敦和马德里恐怖袭击后通过的一套反恐措施。该法律名为“Legge Pisanu”，是以当时内政部长的名字命名的，限制了新无线网络（WiFi）热点的开放，要求提供公共通信服务的实体（如酒店和网吧）申请批准许可，并保留客户身份证明的复印件和客户网站访问日志。该法律是所有西方国家最严格的法律之一，在数年内限制了意大利各地区新热点的开放，进一步放缓了意大利缩小与欧洲其他国家数字差距的步伐。另一项法律要求互联网服务提供商监控互联网活动，存储用户数据 5 年的法案，在 2003 年积极分子和反对党的抗议下未能通过。

2015 年巴黎恐怖袭击事件发生后，意大利通过了一项新的反恐法，将在网上招募恐怖分子、支持或煽动恐怖主义的行为定为犯罪。该法律还委托公诉人（Postal Police）将恐怖分子网站列入黑名单，要求服务商将其屏蔽或下线。此外，法律延长了互联网服务提供商保留用户网络流量记录——“元数据”，并非通信内容——的时间到 2016 年 12 月，尽管 2014 年的一个欧洲法院裁定，已经将类似措施认定为对基本隐私权的限制。批评人士担心这项法律可能会被广泛应用，进而阻碍正当言论——在国际准则中可能属于被保护的言论自由。然而，在颁布该法律之前，政府确实取消了该法案中授权执法机构远程侵入私人电脑的规定。

与欧盟许多国家一样，意大利也会监管某些类别的网站，包括儿童色情和非法在线赌博的网站，以及一些侵犯版权法的端对端（P2P）网站（如海盗湾，The Pirate Bay）。在 2006 年和 2007 年，意大利政府推出了新

关键基础设施保护国家网络犯罪中心（CNAIPIC）属于意大利邮政和通信警察队，负责预防网络犯罪和保护关键基础设施。

的互联网过滤法，要求互联网服务提供商屏蔽被国家垄断管理局（AAMS，监管赌博和其他垄断的中央政府机构）列入黑名单的国际网站或未经批准的赌博网站，以及那些含有儿童色情的网站，服务商需在被告知网站存在的 6 个小时内对其进行屏蔽。国家打击儿童色情中心（National Center for the Fight Against Child Pornography）是邮政和通信警察队（ Postal and Communications Police Service）的一部分，负责维护屏蔽网站清单，意大利刑法典规定对分发和出版儿童色情的行为进行严惩。

意大利邮政和通信警察队是预防网络犯罪、保护意大利关键基础设施的主要执法实体。几十年来，意大利邮政服务一直在向数以百万计的客户提供在线服务，它开发了一个成熟的系统，用于监视并保护其电子网络免受网络攻击。因此，该机构的警察部门是最适合额外承担反计算机犯罪这一责任的部门。2005 年，上文提到的反恐法（Legge Pisanu）将司法管辖权授予意大利内政部，并将邮政和通信警察队认定为负责执法行动的部门，负责打击针对关键信息基础设施的网络攻击。2008 年，内政部依法令建立了一个专门的关键基础设施保护国家网络犯罪中 心（Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, CNAIPIC），将其作为意大利邮政警察队的分支，直接负责所有针对重要基础设施的网络犯罪和其他恶意网络活动的预防、控制、减轻和调查。作为执法机构，国家网络犯罪中心全天候活动，包括运营、技术和调查小组。此外，网络犯罪中心是 G-7 高科技犯罪网络（G-7 High-Tech Crime Network）的国家联络点，该网络是《布达佩斯公约》为所有会员国提供的。该网络旨在加强合作，提高网络犯罪的实施和起诉的有效性。通过 2016 年的《稳定法》，意大利政府将 1,500 万欧元（约 1,660 万美元）分配给邮政和通信警察队以及国家网络犯罪中心的运营、技术、鉴定和培训活动。

还有其他负责打击网络犯罪的执法机构。意大利警察和 Carabinieri（肩负军事和民事警察职责的国家宪兵队）成立了特别部门，专门打击网络犯罪，进行计算机取证和科学调查。此外，财务卫士（Guardia di finanza, GdF）负责执行有关网站屏蔽的决策，这些被屏蔽网站通常涉嫌侵犯版权以及其他网络犯罪和欺诈问题。

意大利正在努力提高其能力，参加各种执法网络培训，如欧洲理事会 2014 年启动的“Cybercrime@Octopus”，计划旨在帮助各国实施《布达佩斯公约》，加强数据保护和法律保护。该计划包括了各种各样的活动，其中就有为法官和执法人员提供的网络犯罪和电子证据课程。为了提高反对网络犯罪战略的有效性，被选中的警察代表将加入常设工作小组，该小组由政府或国际组织建立，包括网络安全跨部门小组

（Gruppo Interministeriale per la Sicurezza delle Reti）、G-7、欧共体、欧洲委员会、欧洲安全与合作组织（OSCE）、国际刑警和欧洲刑警组织。

意大利国家反僵尸网络支持中心（National Anti-Botnet Support Center)积极应对僵尸网络的传播，它是欧洲网络防御计划的一部分。

此外，意大利还参与了多种其他跨部门伙伴关系，以加强在网络安全、信息共享、边境安全以及监视方面的合作。例如，意大利内政部与美国特勤局（US Secret Service）和联邦调查局（FBI）——这两个美国联邦执法机构负责的是预防和打击包括网络犯罪在内的金融犯罪——密切合作打击跨国网络犯罪。作为这一倡议的一部分，经过网络训练的联邦调查局调查员每 6 个月来一次意大利，与意大利执法机构分享网络犯罪调查的工具和信息。2009 年，意大利邮政和通信警察队与美国特勤局联手，成立了一个名为欧洲电子犯罪特别工作组（European Electronic Crime Task Force, EECTF）的国际工作队。该机构专注于广泛的“以计算机为基础的犯罪活动”，包括身份盗窃、网络入侵以及其他影响金融部门和其他关键基础设施的计算机相关犯罪。该工作组总部设在罗马，使用意大利邮政服务（Poste Italiane S.p.A.）的威胁软件监视整个欧洲的计算机网络，并收集来自执法部门、企业、安全解决方案提供商、情报机构和欧洲专家的网络犯罪信息。此外，工作组还积极分享与网络犯罪有关的信息和警报，开发了专门的工具，从而与其他成员组织交换专业技能、知识、最佳做法和通用解决方案。其他组织包括：国际执法机构（如保加利亚警方、罗马尼亚警方和西班牙警方）、金融机构（如美国运通、花旗银行、万事达）、国际组织（ENISA、反钓鱼工作组 APWG、联合国区域间犯罪和司法研究所 UNICRI，以及数字犯罪联合会 Digital Crimes Consortium）、信息通信技术安全供应商（如卡巴斯基、赛门铁克和威瑞森）和学术界（如博洛尼亚大学、萨勒诺大学和都柏林大学）。2010 年，工作组在英国创建第二个部门，扩大了其欧洲参与。

认识到网络犯罪可能会与高速互联网的普及同步增加，随着更多的联网设备成为感染和利用的工具，国家计算机应急响应小组建立了第一个意大利国家反僵尸网络支持中心（Centro Nationale AntiBotnet）。该中心是欧洲网络防御推进中心项目（ACDC）的一部分，是由 14 个欧盟国家组成的非盈利项目，受欧盟委员会资助，旨在防止僵尸网络的传播。尽管如此，意大利的中小型企业（意大利经济的支柱）仍然会受到知识产权盗窃、恶意软件和商务电子邮件入侵的困扰。这是由于缺乏对威胁的认识、缺乏安全且抗打击的产品和服务以及意大利数字设备和基础设施的高僵尸网络感染率造成的。尽管有反僵尸网络项目，事实上意大利仍面临着欧洲和中东地区最高的感染

率。这些感染助长了非法活动，使意大利减少其领土内的犯罪活动、打击跨国犯罪的承诺面临质疑。为了有效应对这些挑战，意大利可能需要加大执法机构和互联网服务提供商以打击网络犯罪为目的、减少僵尸网络途径的努力。

信息分享

正如 2013 年《国家网络安全战略》及其执行计划所述，意大利承认公私伙伴关系的重要性，致力于与私营部门密切合作，在危机管理规划领域进行信息共享与合作。

网络安全部门（NSC）是在危机和紧急情况下负责事件响应协调和信息共享的主管部门。

在危机和紧急情况下，网络安全部门将负责事件响应协调，促进与公共和私人利益相关者的信息共享。安全情报部门（DIS）会与网络安全部门和其他公共和私人利益相关者分享被认为对网络安全有重要意义的情报信息。安全情报部门也在全国范围内培养网络安全意识，促进网络安全教育。除了网络安全部门，国家计算机应急响应小组也是一个全社会的信息收集和共享中心，它拥有更多的技术专业知识。响应小组为有限的关键公共和私人组织用户提供专门的“信息共享”服务，以促进组织之间的互动。通过这个平台，用户可以交流与网络威胁和事件相关的信息和体验，扩展他们的集体“知识库”，并在发生大规模事件时提高其整体响应时间。

另外，政府公共行政部门的计算机应急响应小组（CERT–PA）成立于 2014 年，它取代了公共连接系统应急响应小组（CERT–SPC），扩展了其原有的任务，是意大利政府机构的内部网络信息共享中心。它也是欧洲其他公共行政部门响应小组的中央联络点，帮助信息交换和程序商定。

意大利邮政警察队的国家关键基础设施保护网络犯罪中心（CNAIPIC）开发了该中心专用的、受保护的信息共享网络，实现了信息双向交流，与关键基础设施运营商交换网络威胁预防、评估和压制的信息。此外，特别成立了“计算机犯罪分析小组”（Nit à Di analisi del Crimine Informatico — UACI），它与意大利主要大学、公司和公共机构合作研究和分析网络犯罪，开发新的计算机犯罪调查工具与技术。当地单位也为分析小组提供类似的服务，并可以帮助管理从公民报告到警察热线的法律案件和紧急情况。此外，意大利还是国家网络取证和培训联盟（NCFTA）的成员，该联盟是美国的非盈利组织，其使命是促进私营行业、学术界和执法部门之间的合作和信息共享，从而识别、减轻和中和复杂的网络相关威胁。

虽然意大利电信和其他关键基础设施运营商有义务向负责国家安全的政府实体

报告网络相关事件和信息泄露，但是意大利还未能建立唯一的、专门的制度结构，以提供跨部门事件信息交换机制，这些信息包括操作信息（近乎实时）和鉴定信息（事后）。此外，对某些关键行业公司，它们被要求与每一个负责网络安全的政府机构（如安全情报部门、国家计算机事件应急响应小组、国家关键基础设施保护网络犯罪中心）都建立信息共享伙伴关系，这就导致了工作的重复和资源分配的效率低下。在各组织之间，电信和关键基础设施的运营商更愿意与政府有单一的联络点，这样可以加快信息的流动，同时减少报告的行政成本。

最后，欧盟委员会通过欧盟预防和打击犯罪方案（ISEC）资助了唯一的信息共享倡议。邮政和通信警察队与全球网络安全中心（Global Cyber Security Center）、Abi实验室、意大利联合信贷银行（UniCredit）、Booz & Company、罗马尼亚警方总督察（General Inspector of the Romanian Police）和国家犯罪机构（National Crime Agency）合作，为银行和执法机构创造了一个信息交换平台，以共享可疑交易、金融诈骗和针对银行系统的潜在网络攻击信息。这一网络诈骗中心和专家网络（OF2CEN）将有助于信息交流和信息分析，并及时向所有利益相关者提供可疑犯罪活动信息。这一倡议的积极成果促使意大利在 2015 年与欧洲刑警组织和欧洲银行业协会合作，启动了第二个项目（OF2CEN v.2）。下一代信息共享平台将业务扩展到所有欧盟成员国。

研究和投资

2013 国家网络安全战略和相应的实施计划都包含了促进研究与发展（R&D）投资的意向，认识到需要“与大学、公共和私人研究中心合作，提升方法和技术创新，更好地检测和分析威胁和漏洞”。然而，2013 年的战略并没有明确说明政府将如何支持、推进和维持这些努力。在 2015 年的《2014—2020 年数字增长战略》中，意大利政府承诺投资 1,200 万欧元（约 1,340 万美元），发展信息通信技术相关技能，将其作为增加就业机会的关键。投入这些资金的目的是：提高数字素养，特别是公务员的数字素养；拓宽数字技能相关课程主题；增加与信息通信技术技能相关培训数量；增加信息通信科技领域毕业生人数。此外，不同的政府实体也各自独立，更直接地参与网络研发工作。例如，意大利政府的尤格波多尼基金会（Ugo Bordoni Foundation）是经济发展部下的一个信息通信技术研究机构，最近，它与美国国家网络取证和培训联盟（NCFTA）启动了一项新的战略伙伴关系，旨在促进以电子商务活动为目标的研究活动、保护商标和专利并进一步打击假冒产品。尽管如此，与其他欧洲国家相比，意大利的实际研发支出仍然很少。

网络安全国家实验室包括全意大利 38 所公立和私立大学及研究中心，促进和协调基础和应用科学研究以及计算机科学、计算机工程和信息技术的技术转移。

与所有欧盟国家一样，意大利也参与了欧盟的研究和创新地平线 2020 计划（Horizon 2020）。意大利是参与该项目的最大欧盟国家之一，获得了开展其部分技术发展项目的大量资金。虽然意大利政府没有制定出一套统一的方案或激励措施来鼓励大学和学术机构进行网络安全教育和应用研究，但给所有公立大学和国家实验室提供了支持和资金，其中一些机构已经在这一领域开发了自己的研究项目。特别地，教育部与大学和研究（MIUR）基金将监督并资助国家大学间信息学联盟（Consorzio Interuniversitario Nazionale per l'Informatica, CINI）。该联盟将公立大学、高等教育学院和研究机构连接在网络安全联合国家实验室（Laboratorio Nazionale di Cybersecurity）中，其中包括 38 个意大利公立和私立大学以及研究中心。

网络安全国家实验室在计算机科学、计算机工程和信息技术等多个领域，促进和协调基础与应用科学研究和技术转移，领导数个与关键基础设施供应链安全、恶意软件分析、网络情报收集有关的全国性研究项目。网络安全国家实验室与美国国家标准技术研究所建立了双边合作关系，促进科学技术合作联合委员会会议的开展，并重点关注网络安全。意大利方面，这一工作组包括国家研究委员会（CNR）和 ENEA。网络安全国家实验室也在 2015 年《国家网络安全框架》的制定中发挥了关键作用，该框架基于 2013 年美国国家标准技术研究所的《提高关键基础设施网络安全框架》，属于自愿指导框架。它扩大并更新了原框架，并根据意大利的具体业务部门进行了调整。最后，网络安全国家实验室正在制定一项新的网络安全计划，以扩大意大利网络安全人员的规模，实验室最近还发表了一篇论述网络安全对国家安全和经济影响的白皮书。这份白皮书是由来自 20 多家意大利顶尖大学的 50 多位科学家撰写的，讨论了意大利在未来几年将面临的一些主要网络安全挑战，并提出了具体建议，以帮助政策制定者解决这些问题。

此外，总理办公室通过国家大学间信息学联盟支持罗马大学的网络情报和信息安全研究中心（CIS）。该中心是一个多学科研究中心，致力于制定信息安全方法、威胁概况和更好的预防和防御战略。中心最相关的项目之一——TENACE 项目致力于研究技术和组织方法，以保护关键基础设施免受网络威胁。中心和网络安全国家实验室每年发布一份《意大利网络安全报告》（Italian Cyber Security Report）。意大利其他公立大学也已经发展出了先进的网络安全项目，意大利的程序员和开发者在世界上名列前茅。

全球网络安全中心（GCSEC）是一个由 Poste Italiane 和其他成员公司资助的非营利性组织，它负责推动和传播网络安全知识和意识，使参与互联网使用和保护的不同

利益攸关方的能力、技能、合作、沟通得到改善。安全中心与意大利和国际上的政府机构、私营公司、国际组织和搜索机构合作，推广各种项目，包括培训活动、高级搜索工作、特定部门间信息交流、能力建设项目和国际活动。

此外，意大利邮政警察队与意大利各大学间建立了不同的合作伙伴关系，共同开发打击网络犯罪的创新解决方案，建立输送网络安全专业人员的渠道，方便有兴趣在毕业时加入专门网络犯罪部门的学生。

近年来，意大利政府批准了针对不同行业的研发税收减免，对投资于创新初创企业的私营部门公民和公司也会给予特殊税收优惠。此外，在 2016 年 9 月，政府公布了一项新的《工业 4.0》（Industry 4.0）国家刺激计划，旨在帮助意大利工业为数字时代做准备，并支持在研究和创新方面的投资。该计划包括税收减免和其他激励措施，还有为确保所有的初创企业和工商企业都能使用互联网和宽带技术的额外措施。意大利政府承诺为该项目新拨款 130 亿欧元（约 146 亿美元），该款项还将支持“2017 年盘活额外 100 亿欧元（112 亿美元）私人投资”的各个计划。

另外，由网络安全专业人士和学者组成的一个非营利性的协会（CyberPARCO）推广了一个新的项目，计划将 2015 年世界展览会（Expo Milano 2015）使用过的米兰市中心以外的广大地区转化成为网络科技园区，建立网络安全卓越中心。伦巴迪亚区（米兰所在的地区）的政府最近成立了一个专门的网络安全工作组来讨论和评估各种与网络安全相关的项目，包括建立第一个欧洲—地中海枢纽网络安全中心（Euro-Mediterranean Hub for Cyber Security）。这个被称为“网络公园”的计划旨在创造新的就业机会，为正在不断扩大的意大利网络安全产业吸引投资和人才，鼓励创业创新公司的发展，促进网络安全公司、投资者、企业家和学术研究组织之间的密切合作，促进与国际组织、协会和类似中心之间的合作。

意大利的研发项目必须克服研发停滞的遗留问题，找到合适的机制，以鼓励建立一个充满活力的创业社区，服务提供商和其他机构增加的投资将支撑这一社区。政府推动其数字增长战略的措施和资金有限，再加上对《地平线 2020》项目资金的依赖，可能不足以在加速公共和私人活动数字化的同时，减少国家网络不安全因素。

外交和贸易

2013 年意大利国家网络安全战略明确指出，“意大利全面参与了多边机构，首要的就是欧盟（EU）和北大西洋公约组织（NATO），以及与其他双边伙伴有关的机构”。此外，战略凸显了意大利政府意图全力“支持网络安全领域国际合作计划”和“促进对数字领

域中，符合我们价值观的行为规则的拥护和尊重，促进网络空间治理共享方法的出现，使国际社会能够作为一个整体来有效地应对未来的挑战”。确实，该战略的主要目标之一就是“促进意大利参与国际倡议，以加强网络安全，一个方法是参与有意大利作为成员的国际组织的现有努力，另一个方法是加强与友好国家和盟国的关系”。

根据国家网络安全战略目标，意大利定期参与网络安全跨国谈判和讨论，它是所有处理网络相关事务的主要国际机构的一员，包括欧盟、欧洲理事会、北约、G-7、联合国专家组（UN GGE）、经济合作与发展组织（OECD）、欧安组织（OSCE）以及欧盟委员会建立的网络和信息安全平台（NIS Platform）。2015 年，意大利成为第一个发表非约束性议会声明——《互联网权利宣言》（Declaration of Internet Rights）的欧洲国家，宣言促进了互联网接入、数据保护、网络中立、匿名性以及所谓的“被遗忘权”（Right to be Forgotten）这些权利。一个议会间委员会发布了这份文件，旨在提高公众对数字权利的认识，对负责修改国家现行法律的立法者造成影响。

网络安全问题也常常与贸易谈判和安全条约纠缠在一起。虽然意大利在这些讨论中可能没有发挥主导作用，但它确实参加了上述各国际论坛的所有类似对话和谈判，并已在国内实施和执行多个国际协定。例如在 2016 年 3 月，经济发展部作为监督“军民两用”技术出口的国家机关，如那些适用于《瓦森纳有关常规武器以及两用货物和技术出口管制的协定》（Wassenaar Agreement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies）的技术，基于《瓦森纳协定》中对出口的限制，取消了意大利黑客团队（Hacking Team）用于出口其间谍软件的“全球授权”（Global Authorization）。黑客团队是一家以其卖给政府的监视和黑客工具而闻名的公司，它被指控向那些可能将产品用于人权侵犯的国家出口其部分产品。

意大利在双边层面上采取了更多行动。最近，意大利的网络安全贸易代表团去以色列达成了一项协议，旨在加强两国之间的商业和学术合作。此外，意大利内政部积极与美国执法机构联络，加强双方在网络安全、信息共享、边境安全以及监视方面的合作。

网络安全国家实验室包括全意大利 38 所公立和私立大学及研究中心，促进和协调基础和应用科学研究以及计算机科学、计算机工程和信息技术的技术转移。

意大利外交部负责协调意大利在各种网络安全问题多边论坛上的参与和努力。意大利还在外交部内设立了专门的网络安全协调员职位，直接负责与网络安全相关外交政策和贸易协定谈判，并在政府的网络安全工作

组（Cybersecurity Working Group）内代表外交部。此外，总理办公室下设的网络安全部门“在涉及联合国、欧盟、北约以及其他国际组织和国家的网络危机局势中，作为国家联络点”。

防御和危机应对

意大利国防部（MoD）将网络安全定义为对国防和安全的威胁，并承认网络空间现今是第5个战争领域，这在2016年7月华沙峰会上北约成员国发表的声明中被重申。《关于2013年军事政策的部长级指令》（Ministerial Directive on the Military Policy for the Year 2013）承认了现代冲突的混合性质，并强调意大利需要加强包括“网络领域在内的”常规和非常规能力。2015年《国际安全与防御白皮书》（Libro Bianco per la Sicurezza Internazionale e la Difesa）强调了网络攻击对全社会的潜在破坏性影响，这种影响与传统纷争的影响不相上下，明确表示政府意图培养意大利军队的“防御能力，以应对可能使民用机构现有能力瘫痪的网络攻击”。白皮书特别指出，网络空间内的防御性军事行动将是意大利的战略重点之一，也是2016年至2018年的主要投资项目之一。

为了实现在2015年白皮书中所述的有关网络防御的宏伟目标，意大利已经开始建立网络空间行动联合指挥部（Comando Interforze per le Operazioni Cibernetiche, CIOC），预计将在2017年开始运行。指挥部将有两个功能。首先，它将集中并加强所有网络防御能力，以保护军事网络和国家免受网络攻击。其次，它将建立一个具有计划和管理能力的计算机网络运营（Computer Network Operations, CNO）部门，用于支持意大利内外的军事行动。

尽管目前有关该指挥部的信息有限，但是意大利武装部队（Italian Armed Forces）官员最近的发言表明，相当于这一网络指挥部的第一个部门可能在2017年中期开始运转。参与该新实体发展的人正在讨论其三种主要活动：①建立组织结构；②识别其运营所需的技术能力；③劳动力培训。

新司令部将与意大利国防计算机事件应急响应小组（CERT Difesa）坐落于同一位置，计划将国防响应小组技术中心的一些能力运转起来，以便进行防御性的网络操作。国防计算机事件应急响应小组目前负责保卫军事网络、发出威胁预警和警告并提出可能的解决方案、管理事件响应、促进与其他民间响应小组的信息共享和合作。网络司令部将是国防部的一部分，但它也将直接与其他政府机构和国际组织合作。

虽然最终组织还未成型，但是意大利网络司令部最有可能被放置在国防部现有的命令、控制、通信和电脑司令部（Joint C4 Command, 联合 C4 司令部）之内，国防参谋长（Capo di Stato Maggiore della Difesa, CaSMD）作为意大利国防部的技术和军事负责人，网络司令部可能会通过作战副指挥官（Vice Comandante per le Operazioni, VCOM–OPS）向其汇报，副指挥官负责在军事行动（包括网络行动）中进行行动规划和部队的部署。国防联合 C4 司令部已经存在于意大利国防部，其目的是管理联合行动，这些行动旨在确保指挥、控制、电信和信息通信技术的效率。该网络司令部在国防联合 C4 司令部中可能也会承担 IT 任务。必须制定适当的法律来规范新的网络司令部。

国防部的多年经济规划文件中并没有明确指出网络司令部的资金来源，但它被列入了“联合 C4I 系统（Joint C4I Systems）”资金分配的一部分。国防部预算案将增强网络防御能力定义为意大利国防最重要的资金项目之一。2016 年至 2018 年期间，这些网络防御能力可能会占有多达 2,240 万欧元（约 2,500 万美元）的“联合 C4I 系统”资金。

意大利武装部队通常为多国网络演习的积极参与者，这些演习由欧盟（如网络欧洲演习）、北约（如网络联盟和网络大西洋演习）和欧洲网络与信息安全机构（ENISA）组织，目标是测试和提高国家准备水平。特别地，国家计算机事件应急响应小组和国防部联合 C4 司令部共同参与了所有国内和国际网络安全演习。

意大利刚刚开始在网络空间内建立国家防御能力。在 2016 年 7 月华沙峰会期间，北约成员国同意加强国家网络和基础设施的网络防御，提高其抗打击性以及快速有效应对网络攻击的能力，调整其网络防御能力。因为这项协议，意大利可能会加快其在网络防御方面的活动和投资，以加强其对北约的承诺。

网络就绪度指数 2.0 结论

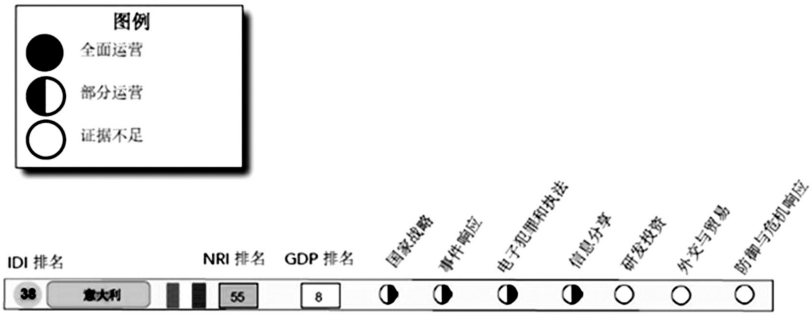
根据网络就绪度指数 2.0 的评估，意大利正在努力完成网络就绪度，在网络就绪度指数的 7 个基本要素中，其中很多在意大利都有部分体现。

意大利的现状是动态且不断变化的，这一分析结果只是现状的一个概要。随着意大利持续制定并更新其经济（数字议程）和国家网络安全战略、政策和倡议，用一种更为平衡的方法，使其国家经济愿景与安全优先事项一致，对这一国家概况的更新将反映这些变化，对实质性的、显著的提升进行监控、跟踪和评估。

网络就绪度指数 2.0 为各国领导人提供了一种全面的、比较的、基于经验的方法，

在这个充满网络、竞争和冲突的世界里，帮助他们规划通往更安全、更抗打击的数字未来的道路。

有关网络就绪度指数 2.0 的更多信息，请参见：http://www.potomacinstitute.org/academic-centers/cyber-readiness-index。



德国网络就绪度报告

国家人口	8,140 万人
人口增长率	0.5%
按市场价格计算的 GDP （美元现价）	3,356 亿美元
GDP 增长率	1.7%
引进互联网的年份	1983
国家网络安全战略	2011
域名	.de
每 100 名用户中固定宽带的订阅数	35.8
每 100 名用户中移动宽带的订阅数	63.6
每 100 名用户中移动电话的订阅数	120.4

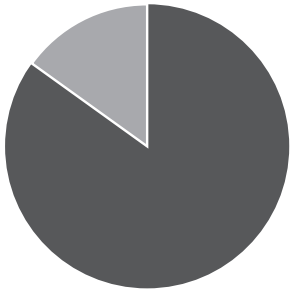
信息通信技术（ICT）发展和连通性排名

国际电信联盟（ITU）ICT 发展指数（IDI）	5	世界经济论坛网络就绪指数（NRI）	3

来源：世界银行（2015），国际电信联盟（2015），世界经济论坛网络就绪指数（2015），以及国际互联网协会。

概述

1983 年，互联网首次被引进德国，它借助了德国电信（一家政府所有并运营的企业）提供的叫做 Bildshirmtext （BXT）的早期数据网络服务。第一封从美国发出的以“欢迎来到计算机科学网络”为题的邮件，一年后到达德国，由此德国互联网正式成立[1]。在 1995 年德国互联网接入向更广阔的商业市场开放之前，德国电信是德国唯一一家互联网服务提供商（ISP）。德国电信私有化后，其三分之一的股份仍由德国州和联邦政府控制[2]，该公司依旧是德国占据主导地位的互联网服务提供商。



德国互联网普及率：86.2%

如今，随着 1990 年重新统一以来密集的资本支出，德国电信系统已成为世界上技术最为先进的系统之一，互联网普及率超过 86%。自互联网被发明以来，德国政府大力推动 ICT 发展，增强互联网连通性，成为诸多互联网相关项目的开拓者。事实上，德国是万维网建立以来全球首个实现图书馆数字化的国家。作为“信息作为创新的原材料”项目的一部分，德国数字图书馆“全球信息”项目于 1998 年成立。这一项目旨在推进与大学、出版社、书商、特别专题信息中心、学术团体以及学术和研究图书馆之间的合作[3]。

德国是首个到 2018 年能为移动宽带分配 700 兆赫兹频段的欧洲国家。尽管无线宽带只覆盖了 20% 的农村地区，但德国的《数字议程 2014—2017》计划通过在这些偏远地区发展高速宽带，为所有家庭提供至少 50 兆 / 秒的下载速度，在 2018 年前解决这一问题[4]。此外，IPV6 正在以超过 10% 的接入率快速增长。与此相比，2014 年 4 月时其他发达国家的平均发展速率不过只有 3.5%。

德国拥有一项清晰的数字战略，旨在提高竞争力、促进经济增长和社会福利。其强调，增强高速网络和信任将有助于“激发创新潜能以进一步促进增长和就业”。[5]这一战略致力于通过增强制造业数字化和自动化，加大对 ICT 的工业化应用、IT 安全研

究、微电子和其他数字服务的投入，将德国打造为互联网经济的领头羊。目前，德国ICT市场是欧洲最大、世界第四大市场，其巨大规模将有助于德国政府实现这一战略[6]。

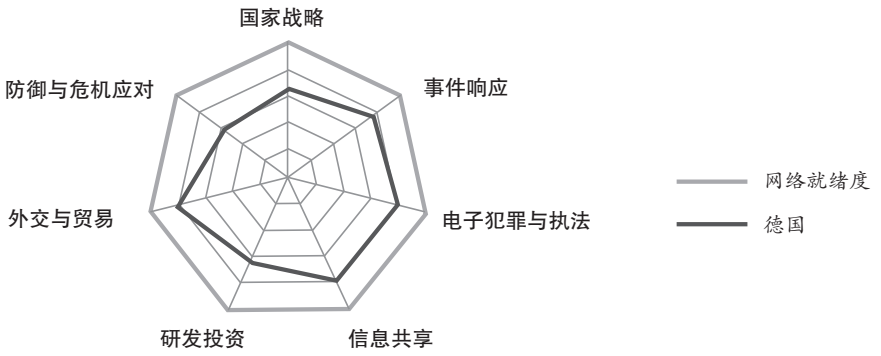
不过，德国在《2016年国防白皮书》中承认，地理和人口上的中等规模是其在快速发展的世界中的主要挑战。尽管德国是世界第四大经济体，但其认识到“从长远来说……它将保持这个位置不变”的可能性较小[7]。在21世纪知识社会中，国家安全与经济福利之间存在着直接关联。其还认为，出于对“安全供应链、稳定市场和有效运作的信息和通信系统”的严重依赖，并且这一“依赖还将继续得到强化”，“知识对德国来说是一种战略性资源”。

自2011年以来，德国政府在所谓的第四次工业革命中独占鳌头，其“工业4.0”项目是《高科技战略2020年行动计划》的一部分[8]。这一倡议鼓励企业进入物联网，尤其是360万中小制造商，后者贡献了德国60%的就业和将近4,000亿美元经济体量的三分之二[9]。德国政府投入2亿欧元（2.22亿美元）鼓励跨政府、学界、商界的“工业4.0”研究，以期增强高质量、低成本、高效率与经济增长之间的联系，获得这种密切联系所带来的成果。德国总理安吉拉·默克尔也正在说服整个欧洲接受这一倡议。她曾在2015年达沃斯世界经济论坛中指出：“谁在数字领域取得领先，就将在工业生产中取得领先……而我们还未在这场竞赛中胜出。”[10]

作为世界ICT发展和应用领域的领导者，德国受到程度较高的网络犯罪、工业间谍、关键服务中断和其他恶意网络活动的威胁。2012年，一个产业协会估计德国因知识产权被窃取而遭受的损失至少为其国内生产总值的1.5%。据2013年的估计，每五个德国互联网用户中就有两位受到过网络犯罪的侵害，而受到网络攻击的企业和政府部门数量惊人[11]。为应对网络威胁范围、规模和程度的上升，德国政府领导人表达了保护数字投资价值、维护国家和经济安全尤其是隐私和数据保护的意愿[12]。然而，在直接涉及网络安全与应对不断上升的IT威胁所需的创新技术方面，“工业4.0”目前的投入十分有限[13]。德国正努力促进货物、服务、人员、资本和数据的跨境流动，与此同时，其还带领欧洲国家展开探讨数据保护需求的对话。这些目标是“欧洲单一数字市场”倡议的基石，也是欧洲和德国经济健康发展的关键。德国将在汉堡主办2017年G20峰会，并可能利用这一平台强调各国增强网络安全能力和弹性的必要性。

网络就绪指数2.0曾针对德国防范网络风险的水平进行评估。该研究为德国提供了一个可操作的蓝图，以更好地理解其网络基础设施的依赖性和脆弱性，并评估该国如何致力于缩小当前网络安全态势与支撑未来数字发展所需的国家网络能力之间存在的差距。基于网络就绪指数2.0的七个核心部分（国家战略、应急响应、电子犯罪

与执法、信息共享、研发投入、外交与贸易、防务与危机应对），本文将对德国的网络安全相关努力和能力进行全面评估。



德国网络就绪指数评估（2016）

国家战略

2008 年，为应对互联网连接设备受感染和网络犯罪事件的日益增多，德国政府向每位公民发放一张光盘，供他们清理个人设备和电脑上的病毒，并指出保护国家是他们的责任所在。伴随 2011 年首份《德国网络安全战略》（以下简称《战略》）的公开发布，德国政府采取了一种更系统、更集中的网络安全战略[14]。该文件承认 ICT 与经济社会发展之间的相互关联性，并将互联网及其下的 ICT 归入德国社会的关键基础设施[15]。

2011 年，德国政府发布首份《德国网络安全战略》，承认 ICT 与经济社会发展之间存在相互关联。

《国家网络安全战略》指出德国更好应对网络威胁环境的若干关键战略领域和目标，包括：保护关键基础设施和 IT 系统；通过建立统一的“联邦网络”增强公共行政的 IT 安全；成立有关应急响应和保护的国家网络响应中心；成立促进公私部门合作的国家网络安全委员会；推进有效的网络安全国际协调；以创新推动发展可信可靠的 IT；培训联邦机构技能人才；有效运用公共部门手段（如法定权力）打击网络攻击行为。

此外，该文件指定德国内政部下属的联邦信息安全局（Bundesamt f ü r Sicherheit in der Informationstechnik, 以下简称 BSI）作为国家网络安全机构，负责执行《战略》。BSI 成立于 1991 年，为联邦政府、IT 制造商、私人和商业用户以及 IT 供应商提供 IT 安全服务。应《战略》要求，该局设立国家网络响应中心（Nationales Cyber–Abwehrzentrum, 下称 NCAZ），主要负责发现、分析和发展消除潜在威胁的必要手段。[16]

与《战略》一致，德国成立了国家网络安全委员会，为各部部长共同应对关涉所

有政策的网络安全事务提供平台。该委员会旨在协调公共和私营部门就预防性的方法和跨领域网络安全手段进行探索。除联邦总理府和各州代表外，联邦各部（包括国防部、内政部、经济和技术部等）部长参加委员会会议。商业代表作为准会员也经常受邀与会。2012 年，BSI 与联邦 IT 协会（Federal Association for Information Technology）、电信和新媒体协会（Telecommunications and New Media, BITKOM）合作成立了网络安全联盟（the Alliance for Cyber Security），这是一个非盈利组织，为广泛的政府政策及执行提供协助。该组织的主要任务是增强德国的网络安全及应对网络攻击的韧性。为实现这一目标，其正建设一个广泛的知识库，支持信息和经验的共享[17]。自成立以来，该联盟的会员数得到快速增长，与合作伙伴之间的交往愈发密切。

与《战略》的内容相呼应，德国 2014 年数字战略（《数字议程 2014—2017》）认识到 ICT 对经济增长的重要性，以及增强网络空间安全的必要性。该战略同样指出，半数德国互联网用户并不相信其网上数据的安全性。由于对 ICT 的信任是数字通信、电子商务以及实现“欧洲单一数字市场”的关键，政府十分关注这一统计数据，并采取了增强互联网安全等诸多措施来强化信任[18]。例如，BSI 正在贯彻落实《2015 年 IT 安全法案》，该法案是德国数字战略及保护重大关键基础设施努力的核心[19]。这些努力包括与关键基础设施运营者继续合作为关键基础设施企业及子部门制定最低网络安全标准，提高德国 IT 安全的有效性、可靠性、保密性和完整性。

为增强 ICT 的安全和弹性，《战略》和《数字议程》正寻求一个全面的、多利益相关方的路径来增强在线服务和关键基础设施的安全。不过，在增进关键公共与私营利益相关方之间及各自 IT 系统之间的协调与互通方面，在更好应对日益增多的、与涵盖德国经济的关键服务数字化相关的 IT 安全风险方面，德国政府还需要做更多的努力。

应急响应

2011 年，德国政府发布首份《德国网络安全战略》，承认 ICT 与经济社会发展之间存在相互关联。

作为德国国家网络安全机构以及中央网络应急响应办公室，BSI 通过全政府和全社会的介入、检测、反应来塑造信息安全政策与活动。BSI 负责发布有关 IT 产品和服务中的恶意软件和安全漏洞的警告，向有关方面和社会公众发布信息，并提出对策建议[20]。其还与超过 5 万家私人机构交换信息。BSI 早期预警系统是模仿美国金融服务信息共享与分析中心（FS–ISAC）建立的，目前尚未完全建成[21]。

1991 年起，德国就建立了多计算机应急小组（CERTS）及同类组织。1994 年，BSI 成立了第一支计算机应急小组（BSI–CERT），属为联邦机构进行信息收集的虚拟团队。2001 年，一个政府性的 CERT 从 BSI–CERT 中独立出来，取名为 CERT–Bund。自那时起，CERT–Bund 变为一个正式的国家应急小组，作为一个预防、应对和积极处理网络安全事件的平台和联络中心开展工作。如今，CERT–Bund 与州一级和非政府的计算机应急小组密切合作并提供广泛的服务。其主动采取应对网络安全事件的措施，按照自愿原则对选民进行监控——包括 IT 生产商和供应商、私人和商业用户。其还提供预警、信息服务、主动提醒以及拥有一个记录网络安全事件的在线报告系统[22]。2006 年，BSI 成立了一个公民计算机应急小组（B ü rger–CERT），专门负责提高社会公众和小企业的网络安全意识[23]。

尽管德国没有一个统一的、单一的国家应急响应方案，但有两个文件，一个是2005年的“全国信息基础设施保护计划”，同时适用于政府和行业，一个是2007年的“关键基础设施保护（CIP）实施计划”，旨在当发生重大网络事件时，进行危机处理并为关键性业务的连续性管理提供建议[24]。据 2007 年 CIP 计划，关键基础设施运营者已“设置了适当的警告和预警程序，根据发生的事件区分标准来明确需要被警告或预警的单位和个人。”[25]此外，根据网络安全的不同层面如危机管理、演练、关键服务的可用性，该计划成立相应的工作组。其同样针对如何完成关键信息基础设施保护所需的任务以及有效及准确地应对 IT 安全时间，规定了政府和私人运营者之间的协议。

2011 年《战略》要求 BSI 建立国家网络响应中心，负责增进政府与私营部门之间在应急响应上的协调和及时信息共享。作为全国指挥、控制和研究中心，BSI 国家网络响应中心的建立是为了使“所有有能力的机构能迅速就严重事件进行反应，为所有相关机构提供事件分析和评估，并与地方和行业内部的危机管理部门展开协作”。[26]除了德国联邦宪法保护局（Bundesamt f ü r Verfassungsschutz, BfV）和联邦民事保护和灾难救助局（Bundesamt f ü r Bevölkerungsschutz und Katastrophenhilfe, BBK）的直接参与外，还有其他政府部门处理网络安全事务——包括联邦刑事警察局（Bundeskriminalamt, BKA）、联邦警察（Bundespolizei, BPOL）、海关犯罪办公室（Zollkriminalamt, ZKA）、联邦情报局（Bundesnachrichtendienst, BND）、联邦国防军及其他监督关键基础设施运营者的机构——参与中心工作，并相互之间及与私营部门保持密切、直接合作。德国《数字议程》承诺未来将增强中心的应急响应能力。

德国已举行了多次国家网络安全演习，以为政府部门和关键基础设施的特定运营者演练危机处理。其中之一，2011 年危机计划和就绪演习，就发生多重攻击如针对

关键基础设施的分布式拒绝服务攻击、银行系统受恶意程序入侵、空中交通管制系统被注入虚假流量时，促进政府响应程序的理解[27]。德国还参与了由欧盟和北约组织的多国演习。尽管近年来举行多次演习，CIP 实施计划仍建议“举办更多的演习以对现有概念进行验证和更新”。

最后，德国联邦宪法保护局（德国的内部情报机构）每年发布网络威胁报告。2016 年报告指出，俄罗斯和中国是针对德国的网络攻击的主要来源地。该报告还透露，德国已监测到来自伊朗对诸多受害者的信息安全威胁[28]。

电子犯罪和执法

德国在 2001 年和 2009 年分别签署和批准了欧洲委员会的《网络犯罪公约》（通常称为《布达佩斯公约》）并努力推动《公约》在国内的实施，就保护社会免受网络犯罪威胁做出国际承诺。同样，德国也签署和批准了《公约》中关于通过计算机进行种族主义和排外行为入罪的附加条款。德国在《战略》中重申了针对以《公约》为基础的刑法进行国际协调的承诺。

2015 年 7 月，德国通过了一项新的 IT 安全法案，该法案旨在防止重要的 IT 系统如经由 BSI、电信供应商、关键基础设施运营者等使用的 IT 系统的丢失。BSI 正在落实该法案，包括为超过 2,000 家关键基础设施企业制定最低网络安全标准。与法案相适应，为保障这些最低安全要求，德国需要提高 IT 安全的有效性、可靠性、保密性和完整性，增强公众的互联网安全，更有效地保护具有国家重要性的关键基础设施[29]。此外，德国还有其他一些法律直接禁止如计算机诈骗、篡改数据、破坏计算机、数据间谍、网络钓鱼以及由传统犯罪法规起诉的相关网络犯罪[30]。在法案实施的两年内，所有有关的运营者都应该采取适当的组织和技术安全手段保护 IT 系统、部件或关键基础设施运作所需的相关进程。这些安全手段必须与最先进的技术相适应。进一步说，关键基础设施的运营者应当至少每隔两年进行 IT 安全审计与认证，并就具体行业的安全标准提出建议。

在执法方面，德国已具备成熟、机制性的能力来应对各种类型的网络犯罪。国家网络响应中心、BSI 和联邦刑事警察局共同主导打击国家网络犯罪工作。尤其要指出的是，国家网络响应中心整合了不同政府部门如联邦警察和对外情报机构以及来自行业的资源[31]。

《战略》承诺增强执法部门、BSI 以及私营部门打击网络犯罪的能力，保护国家不受间谍和破坏活动的侵害。德国已“在相关执法机构的参与下，与行业建立了联合

机制”。[32] 如《2015 年 IT 安全法》所示，成功实施这些雄心勃勃的计划还需要进一步的努力。到 2017 年底，我们将能够知道政府与行业在共同强化大幅减少网络犯罪的能力方面取得了什么样的成绩。从这个意义上说，目前还不清楚是否有足够的计划来培训法官、检察官、律师、执法官员、法医学专家和其他侦查员。

信息共享

正如 2011 年《战略》所言，德国国家网络响应中心负责应急响应协调和全社会信息共享。共享的信息包括 IT 产品的漏洞、攻击方式、犯罪者或其轮廓描述等。一个关键需求是建立一个包含行业和其他非政府行为在内的组织，提供全国范围内现有的、有效网络安全信息，为利益相关方准备和减少网络事件提供建议。网络安全联盟是一个 2012 年建立的合作与信息共享平台——与国家网络响应中心共同承担这项工作。其帮助促进经济、学术和行政领域的伙伴及具有特殊公共利益的企业之间的紧密合作。

德国国家网络响应中心负责协调应急响应和全社会信息共享。

由 BSI 运营的国家信息技术状态中心（Nationales IT-Lagezentrum）协助全国信息分享，跟踪全国和全球 IT 安全状况，以迅速发现和分析重大 IT 安全事件并提出保护措施。一旦发生 IT 相关的危机，其可扩展职权并转变为国家信息技术危机反应中心（Nationales IT-Krisenreaktionszentrum）。该中心集中力量应对 IT 危机，对包括政府网络和关键基础设施在内的所有国家层面进行全覆盖。

此外，德国参与了诸多国家和机构间的合作以培育信息共享。例如，美德网络双边会议成为推动跨境网络安全资源共享的公认伙伴关系[33]。德国还是国家网络取证与培训联盟（National Cyber Forensics and Training Alliance, NCFTA），后者是美国一家非营利组织，致力于推动私营企业、学术界、执法部门之间的合作，以发现、减轻和抵销复杂的网络相关威胁[34]。

由于德国联邦和各州都存在相关政策和项目，因此许多信息共享计划的实施可能面临挑战。各州的网络安全能力及成熟度存在差别，从而应对最先进和复杂的威胁手段的能力也是不同的。信息共享对中央政府的所有努力的实施而言非常关键，但在近期可能难以实现。

研发投资

《战略》主张将 IT 安全和关键基础设施作为未来实施的关键战略领域加强研究。

2014 年《数字议程》强调扩大对工业 ICT 应用、IT 安全研究、微电子和数字服务的广泛投入，即全国层面的网络研发投入[35]。为与《数字议程》相一致，德国在柏林成立了两个大数据中心，以推动以大数据为驱动力的创新、工业应用、科研和医疗[36]。

2015 年 3 月，德国政府发布了一项促进 IT 安全研发的计划，名为“2015—2020 数字世界中的自决与安全”（Self-Determination and Safety in the Digital World 2015—2020）。该计划包含了从现在到 2020 年间 1.8 亿欧元（约 1.98 亿美元）的预算，以推动研发特殊加密技术、保护个人数据和通信服务安全。其集中关注四个关键领域：新技术、安全和可靠的信息与通信系统、IT 安全的应用领域、数据隐私和保护。

为促进政府研发任务的进行，德国教育和研究部（BMBF）在三所大学成立了三个 IT 安全中心：在萨尔布吕肯的 IT 安全、隐私和责任中心（Center for IT Security, Privacy and Accountability, CISPA），在达姆斯塔特的欧洲设计安全和隐私中心（European Center for Security and Privacy by Design, EC-SPRIDE），在卡尔斯鲁厄的应用安全技术能力中心（Competence Center for Applied Security Technology, KASTEL）。2009 年，德国教育和研究部及内政部同意开展 IT 研发的联合合作项目，因而“IT 安全研究”工作组得以成立，以研究和开发新的 IT 安全应用[37]。

政府意识到，为确保可持续的 IT 安全研究，必须培训更多合格人才。

此外，政府意识到，为确保可持续的 IT 安全研究，必须培训更多合格人才。政府鼓励应用安全技术能力中心的学生取得 IT 安全专家的证书，这相当于一个专业硕士学位。达姆施塔特工业大学自 2010 年起就开设 IT 安全的硕士课程项目。在职的专业人员可以在该校的达姆斯塔特高级安全研究中心（Center for Advanced Security Research Darmstadt, CASED）选修有关安全基础课程，并可获得 IT 安全证书。弗莱堡大学计算机系为专长于网络安全的学生授予计算机硕士学位。另外，学生还可以选修政治学和其他社会科学学科的课程，以培养其对网络安全事务更为全面的理解[38]。

此外，德国政府在三个重点领域激励企业在网络安全上的研发：计算机技术——在数字化世界中工作、ICT——网络安全事件检测和处理、电动交通——价值链。前两个领域对所有行业部门开放，最后一个领域则只面向生产和 ICT 部门。激励措施包括给予企业、联盟和研究机构无偿现金补助[39]。政府最近也强调对 ICT 进行风险投资的重要性，尤其是对 IT 新兴企业的支持。为刺激 IT 新兴企业的增长，政府为以下领域提供一些风险投资支持：为创办人提供信息和咨询、通过提供有竞争力的工作条件和大量投资促进融资，通过市场活动为新兴企业与传统行业建立联系，建立国际新兴

企业“中心”，包括商业培育中心[40]。

随着德国作为主席国为主办 2017 年 G20 汉堡峰会进行准备，德国将有机会展现其在 ICT 创新和研究上的领先地位。实际上，2016 年 6 月，汉堡大学接受欧盟 100 万欧元资助成立了一个网络安全研究项目。汉堡大学和石勒苏益格—荷尔斯泰因隐私保护独立中心（Schleswig-Holstein’s Independent Center for Privacy Protection）与七国 9 所机构联合成立了“构建价值驱动型网络安全联盟”（Constructive an Alliance for Value-driven Cybersecurity, CANVAS）研究网络。来自该联盟的研究人员将在以下三个应用领域关注如何平衡网络安全与基本民主价值观之间的关系：医疗、金融、国家安全[41]。不过，德国还存在网络安全人才的严重短缺问题，这一问题在政府中尤其严重。德国教育研究部正资助建立一个新机构：德国网络研究院（Deutsches Internet Institut, DII），并将在未来 5 年内为其投入多达 5,000 万欧元（5,600 万美元）。该研究院将关注互联网的道德、法律、经济和公众参与层面以及多学科视角下的数字化问题[42]。此外，爱因斯坦基金会和柏林州 5 年内投入 3,850 亿欧元（约 4,300 亿美元）在数字包括 IT 安全领域内提供 50 名教授职位，并建立了爱因斯坦数字未来中心（Einstein Center of Digital Future, ECDF），这是一个公私合作的伙伴关系，就德国社会的数字化进行研究[43]。新的爱因斯坦中心将与许多公立实体和学校展开合作，包括柏林工业大学、柏林自由大学、洪堡大学、柏林艺术大学、柏林夏里特医学院以及 8 所知名研究机构和 2 所应用科学类大学。

外交与贸易

多年以来，德国积极参与有关网络安全的外交和贸易及商业谈判，还是欧美“隐私盾”和欧盟内部及欧美之间其他数据保护协议的首席谈判方。

外交部设立了国际网络政策协调员和网络事务大使。

德国在《战略》中提及：“鉴于 ICT 的全球性特质，有关外交和安全政策的国际协调……不可或缺。”[44]事实上，德国在国际舞台上一直十分活跃，与联合国、欧盟、欧洲委员会、北约、七国集团、欧洲安全合作组织和其他多边组织都有合作。《战略》中涉及的多利益相关方模式在《数字议程》中被再次提及，并在以下论坛中得到积极推广：国际电信联盟（ITU）、互联网治理论坛（IGF）、经济合作与发展组织（OECD）和联合国信息安全政府专家组（GGE）。值得一提的是，德国还通过持续参与所有与网络相关的政府专家组来显示其在国际对话中的承诺。

此外，德国还与诸多伙伴就网络事务进行正式和非正式的对话，并参与全球范围内的会议和讨论。德国的《数字议程》重申经济与网络政策之间的关联。例如，德国经常性地处理发展合作问题，并参与有关发展中国家网络能力建设、网络安全能力建设和网络信心建设的项目。

2016 年 3 月，美德承诺共同合作保护关键基础设施，并“在增强关键基础设施的网络安全、强化事件管理与协调、建立其他国家的网络能力上继续展开密切合作”。[45] 作为跨大西洋网络对话的一部分，美德还就最近关于建立一套德国路由系统、加密事务和新的软硬件标准进程的倡议进行探讨。

2011 年，德国外交部设立了网络政策协调员，与其他部门和行为者共同合作出台一项推动自由、开放、安全和稳定的网络空间的外交政策。外交部将国际网络政策视为能对外交政策的所有领域产生影响的工作。该政策旨在抓住互联网创造的经济机会、推动互联网的负责任使用以及网络空间的安全[46]。外交部工作的主要国际优先议题是就良好治理的标准、国际法的应用、网络安全的信心建设达成一致。德国还在许多大型城市设立了网络事务大使，直接对外交部有关部门负责。

防御与危机应对

2016 年 6 月，德国国防部发布了新的《德国安全政策和国防军的未来白皮书》，强调网络风险是一种高级国家威胁[47]。《白皮书》认识到“网络和信息领域已成为一个几乎不受限的、具有国家和战略重要性的领域，并且其重要性将持续上升。”[48] 新政策将德国视为欧洲的“关键国家”，并勾画了“主动帮助塑造全球秩序的责任”。

2016 年，德国开始成立网络和信息空间司令部。

在该文件中，“全政府的网络安全防御被列举为国防部和国防军的核心任务”。此外，国防部负责发展“推动全政府手段和与研究机构、行业和伙伴合作”的国家能力[49]。计划的核心部分是拥有强大的网络防御态势与“保障德国网络空间自由”的军事力量。

2015 年 9 月，国防部长乌尔苏拉·冯德莱恩宣布此项计划。此后不久，德国于 2016 年 4 月开始成立一个网络和信息空间司令部[50]。这个司令部（Kommando Cyber und Informationsraum, KCIR）整合了国防军里网络相关的单位，负责网络、IT（网络）、军事情报、地理信息和有效沟通[51]。其将以一位中将为首，有望于 2017 年 4 月全面运转。该司令部计划拥有 13,500 名人员，主要来自其他军种和组织，这些人员将分布在司

令部和两个新的中心之中——网络运营中心和国防军网络安全中心[52]。对国防军和其他公共部门来说，搜罗足够的 IT 人才并不容易。不过，国防军以“保护德国网络空间自由”为口号，希望能在当年年底吸收到 800 位专家[53]。

德国国防部也指出，其希望国防军有能力使用网络部队进行反击，并希望新网络司令部使德国能够与其他国家如美国在同一水平上进行合作。国防军战略侦察部下属的信息和计算机网络运营局正在着力发展大型防御能力。经过 21 世纪初进行的广泛法律分析之后，国防部基于对机密的网络战争能力将只会被用于防御目的的理解，在 2005 年开始进行有限的尝试，发展一些潜在的进攻能力如红队[54]。国防部同样与国内顶级学院如欧洲管理与技术学院（European School of Management and Technology, ESMT）在高级研究和专业培训上进行合作。

德国政府倾向于将网络安全防御与情报系统分离开来。2011 年，德国政府在内政部下建立了国家网络响应中心。该中心整合了不同政府部门如联邦警察和对外情报机构以及来自行业的资源，并向联邦信息安全局汇报[55]。其最初是由来自 BSI、联邦宪法保护局和联邦民事保护和灾难救助局的部分雇员组成。自成立以来，联邦警察、联邦刑事警察局、联邦情报局、国防军、海关犯罪办公室均派遣专业人士进驻中心。国家网络安全委员会也负责协调防御技术和网络政策。人员队伍中还包括高级军事代表[56]。虽然国防部在网络空间和网络防御上的能力已获得较大增强和提升，但政府正在提议收紧对联邦情报局的控制，并对其监视活动实施新的法律限制。这些法律上的变革经德国议会批准后，将禁止联邦情报局对欧盟国家、公民和组织进行监视，除非对方存在恐怖主义活动的嫌疑[57]。这一协议将要求联邦情报局局长、总理办公室和由法官组成的独立小组来批准基于关键名单之上的战略性对外间谍活动。这种做法与许多其他国家迥异，后者将情报系统与网络军事能力直接串联起来。

就绪指数 2.0 概要

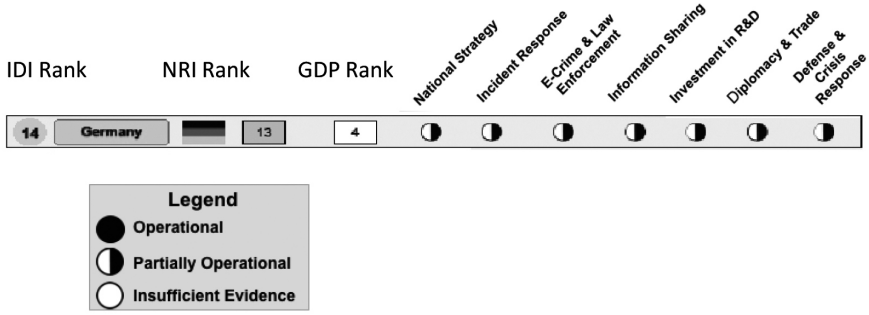
根据网络就绪指数 2.0 的评估，德国正在建设网络能力的过程中，目前在所有七个核心部分上处于部分运营的阶段。

这一研究发现只是动态和变化环境中的一瞥。随着德国继续发展和更新其经济，《数字议程》和网络安全战略、政策和倡议，以一种更加平衡的方式将其经济远景与国家安全优先事项相联系，对德国情况的更新将反映出这些变化，并监督、跟踪和评估具体的进展。

在一个深度网络化、竞争性和冲突易发的世界中，网络就绪指数 2.0 为国家领导

人寻求实现更安全、有生命力的数字未来提供一个全面的、比较的、经验的方法论。

有关网络就绪指数2.0的更多信息，详见：http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.



注释

1. Internet Hall of Fame, "Timeline," http://www.internethalloffame.org/internet-history/timeline.

2. Deutsche Telekom, "Shareholder Structure," https://www.telekom.com/shareholder-structure.

3. Diann Rusch-Feja and Hans Jurgen Becker, "Global Info: the German Digital Libraries Project," D-Lib Magazine, vol.5 no. 4 (April 1999), http://www.dlib.org/dlib/april99/04rusch-feja.html.

4. The Federal Government, "Digital Agenda 2014-2017," (2014): 21, www.digitale-agenda.de/DA/Navigation/DE/Home/home.html.

5. Ibid.

6. Federal Ministry of Economic Affairs and Federal Ministry of Labour and Social Affairs, "IT and Telecommunication," (2014), http://www.make-it-in-germany.com/en/for-qualified-professionals/working/industry-profiles/it-and-telecommunications.

7. The Federal Government, "2016 White Paper on German Security Policy and the Future of the Bundeswehr," (July 2016): 22, https://www.bmvg.de/portal/a/bmvg/en/.

8. Matthew Karnitschnig, "Why Europe's Largest Economy Resists new Industrial Revolution," Politico, July 6, 2016, http://www.politico.eu/article/why-europes-largest-economy-resists-new-industrial-revolution-factories-of-the-future-special-report/.

9. Federal Ministry for Economic Affairs and Energy, "Introducing the German Mittelstand," http://www.make-it-in-germany.com/en/for-qualified-professionals/working/mittelstand.

10.Sara Zaske, “Germany’s vision for Industrie 4.0: The Revolution will be digitized,” ZDNet,February 23, 2015, http://www.zdnet.com/article/germanys-vision-for-industrie-4-0-the-revolution-will-be-digitised/.

11.“Two in Five Internet Users in Germany Hit by Cybercrime in 2013,” eMarketer, May 21, 2014, http://www.emarketer.com/Article/Two-Five-Internet-Users-Germany-Hit-by-Cybercrime-2013/1010845.

12.“Merkel: ‘Difficulties Yet to Overcome’ in US Spy Scandal,” CBS DC, May 2, 2014, http://washington.cbslocal.com/2014/05/02/merkel-difficulties-yet-to-overcome-in-us-spy-scandal/.

13.Melissa Hathaway’s interview with Dr. Sandro Gaycken, Director of the Digital Society Institute, ESMT Berlin, September 20, 2016.

14.Federal Ministry of the Interior,“Cyber Security Strategy for Germany,”(2011), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile.

15.Flippa von Stackelberg, “Germany Prepares for Cyber War,” New Security Learning, http://www.newsecuritylearning.com/index.php/feature/88-germany-prepares-for-a-cyber-war

16.The new National Cyber Response Centre pools the cyber defense resources of the Federal Office for Information Security, the Federal Office for the Protection of the Constitution, the Federal Intelligence Service, the Federal Police, the Customs Criminal Investigation Office, the German Military, the Federal Office of Civil Protection and Disaster Assistance, and the Federal Criminal Police Office; and it will cooperate with ISPs.

17.TÜViT, “Alliance for Cyber Security,”https://www.tuvit.de/en/cyber-security/alliance-for-cyber-security-2352.htm.

18.Federal Government, “Digital Agenda 2014-2017,” 5.

19.Federal Office for Information Security, “The State of IT Security in Germany 2015,” (2015): 42, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2.

20.Federal Office for Information Security, “Annual Report,” (2003): 27, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/annualreport/BSI-AnnualReport2003_pdf.pdf?__blob=publicationFile.

21.Melissa Hathaway’s Interview with Arne Schonbohm, Director of BSI, June 8, 2016, in Berlin, Germany.

22.Federal Office of Information Security, "CERT-Bund," https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/Cert-Bund/cert-bund_node.html.

23.Bürger CERT, “About Us,” https://www.buerger-cert.de/about.

24.Federal Ministry of the Interior, "National Plan for Information Infrastructure Protection," (2009), http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf, and "CIP Implementation Plan for Information Infrastructure Protection," (2007) http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2009/kritis.html.

25.Federal Ministry of the Interior, "CIP Implementation Plan for Information Infrastructure Protection."

26.Federal Ministry of the Interior, “Cyber Security Strategy for Germany.”

27.Melissa Hathaway, “Best Practices in Computer Network Defense: Incident Detection and Response,” NATO Science for Peace and Security Series, Information and Communications Security, vol.35, (IOS Press, February 2014): 12, http://www.iospress.nl/book/best-practices-in-computer-network-defense-incident-detection-and-response/.

28.Joe Uchill, "German Intelligence Blames Russia, China for Cyberattacks," The Hill, June 28, 2016, http://thehill.com/policy/cybersecurity/285202-german-intelligence-blames-russia-china-for-cyber-attacks?utm_source=&utm_medium=email&utm_campaign=2679.

29.Watson Farley & Williams, "Briefing: The New German IT Security Act," February 2016, http://www.wfw.com/wp-content/uploads/2016/02/WFW-Briefing-Germany-IT-Security-Feb-2016-EN-15-Feb.pdf.

30.Federal Ministry of Justice and Consumer Protection, (2015), http://www.gesetze-im-internet.de/englisch_stgb/index.html.

31.Center for Strategic and International Studies, “Cybersecurity and Cyberwarfare,” (2011), http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

32.Federal Ministry of the Interior, “Cyber Security Strategy for Germany,” 10.

33.US Department of State, "Joint Statement on US-Germany Cyber Bilateral Meeting," June 27, 2014, http://www.state.gov/r/pa/prs/ps/2014/06/228543.htm.

34.National Cyber-Forensics & Training Alliance, “Become a NCFTA Partner,” https://www.ncfta.net.

35.Federal Government, “Digital Agenda 2014-2017.”

36.Federal Ministry of Education and Research, “Berlin Big Data Center,” http://www.bbdc.berlin/start/.

37.Federal Ministry of the Interior, "Cyber Security Strategy for Germany," (2011): 11, and Federal Ministry of Education and Research, "Digital World: Cybersecurity research to boost Germany's competitiveness," https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html.

38.University of Freiburg, "Department of Computer Science," http://www.informatik.uni-freiburg.de/studies/studies.

39.Deloitte, "Grants and Incentive Program Updates: The Latest Legislative Developments From Around the world," (April 2015), https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/tax/deloitte-nl-tax-grants-and-incentives-newsletter-april-2015.pdf, and Deloitte, "2014 Global Survey of R&D Tax Incentives," (March 2014): 17, http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-global-rd-survey-aug-2014.pdf.

40.OECD, "OECD Digital Economy Outlook 2015," (July 15, 2015): 25, http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm.

41."1 Million Euro for Cyber Security Project at Hamburg University," Hamburg News, June 21, 2016, http://www.hamburg-news.hamburg/en/cluster/media-it/eu-funds-research-project-ethical-cyberspace/.

42.Georg Schütte, State Secretary at the Federal Ministry of Education and Research, "New Year's Reception for the Science Counsellors of the Foreign Embassies," January 25, 2016, https://www.bmbf.de/de/the-ccasion-of-the-new-year-s-reception-for-the-science-counsellors-of-the-foreign-2381.html.

43.Melissa Hathaway's interview with Professor Philip Lark, September 26, 2016. For more information on the Einstein Center of Digital Future (ECDF), see: http://be-digital.berlin/the-einstein-center-digital-future/.

44.Federal Ministry of the Interior, "Cyber Security Strategy for Germany."

45.US Department of State, "Joint Statement on U.S.-Germany Cyber Bilateral Meeting," March 24, 2016, http://www.state.gov/r/pa/prs/ps/2016/03/255082.htm.

46.Federal Foreign Office, "International Cyber Policy,"http://www.auswaertiges-amt.de/EN/Aussenpolitik/GlobaleFragen/Cyber-Aussenpolitik/KS-Cyber-Aussenpolitik_node.html.

47.The Federal Government, "2016 White Paper on German Security Policy and the Future of the Bundeswehr." Germany's Defense White Papers are released periodically; the previous one was released in 2011.

48.Ibid, 37.

49.Ibid, 93.

50.Federal Ministry of Defense, "Keynote Address by Minister von der Leyen at Cyber-Workshop," September 17, 2015, https://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYy7CsJAEEX_aCYrgmCXkBSCjTYaG9nsDnFgH2GcrIOfb7bwHjjNgYsP3Ei28GyVc7IB7zg6Pk4fmGKZIa5BOZJnC4U9ZSvuxQU8OzNy4reScMJbffEELifSaqWkvHkWq1lgyaKhllVkK8Aex8bOXWOa_8y33Q3D5WwO-_7UXXGJsfOB62YR2w!!/.

51.Until this move, the Bundeswehr (i.e., the German uniformed services) like

most modern militaries divided missions between cyber operations units and IT or network units. This new command merges these units in a model similar to that of the US Navy's Fleet Cyber/C10F organizational structure. The speed of this establishment and its innovative structure is a highly unusual step for the German MOD and a testament to the government's intent to both defend itself and to have greater influence on international cyber matters.

52.Federal Ministry of Defense, "Final Report: Building the Cyber and Information Space Command," https://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYyxDsIwDAX_yE4WRNladYENpArKljZRsRQnlXHCwsfTDryTbjnp4RM3kquOOKWcXMQHjjOdpg9MXBfgEpU4eHJQyYfsZH5RBaZEbw1ChfG-X_gAc05Bd2tISpsXcZoF1iwa91JEtgLkcTS274w1_9lv2_SX4Xo4Nv25u-HK3P4AaMgbvg!!/.

53.Christoph Hickmann, "Call to Arms for Cyber War, Trying to Poach Private Sector Recruits," Süddeutsche Zeitung, April 18, 2016, http://international.sueddeutsche.de/post/143005903195/call-to-arms-for-cyber-war-trying-to-poach.

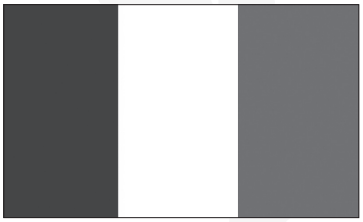
54."Germany Reveals Offensive Cyberwarfare Capability," Atlantic Council, June 8, 2012, http://www.atlanticcouncil.org/blogs/natosource/germany-reveals-offensive-cyberwarfare-capability.

55.James Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare," Center for Strategic and International Studies, (2011): 12-13, http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

56.Federal Ministry of the Interior, "Cyber Security Strategy for Germany," 8-10.

57.Thorsten Severin and Andrea Shalal, "German Government Agrees to Reform BND Spy Agency - Sources," Reuters, June 3, 2016, http://af.reuters.com/article/worldNews/idAFKCN0YP2KG.

法国网络就绪度报告



国家人口	6,660 万
人口增长率	0.5%
按市价计算的 GDP（当前美元）	2.422 万亿
GDP 增长率	1.2%
引入互联网的年份	1981
国家网络安全战略	2011, 2015
互联网域名	.fr
固定宽带用户渗透率	40.2
移动宽带用户渗透率	66.2
移动手机用户渗透率	100.4

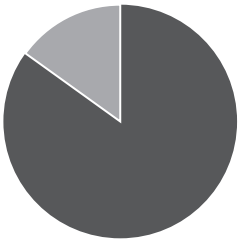
ICT 发展与网络联接指数排名

国际电信联盟（ITU） 通信技术发展指数排名（IDI）	17	世界经济论坛（WEF） 网络就绪指数（NRI）	26

来源：世界银行（2015）、ITU（2015）、NRI（2015）、互联网协会。

概述

1981 年，当时还是国有的法国电信（或其前身法国邮电局）在国内推出了互联网的先驱——一款叫“Minitel”的信息传视在线服务，直到 2012 年才停止提供服务。这一面向法国人的服务基于文本信息，使用完全免费。仅需基本设备，用户就可进行网上聊天、旅行预订和消费、开展网上银行业务以及搜索电话簿。该服务既是技术项目也是政治任务，目的是促进法国社会数字化以及保证法国技术独立[1]。这一由国家资助的项目源自 20 世纪 40 年代末法国制定的工业政策方针，强调国家在电信领域的投资是经济增长的关键驱动力[2]。20 世纪 90 年代，Minitel 的市场被席卷全球的互联网所侵蚀。如今，法国以超过 83% 的互联网渗透率成为欧洲国家中连接率最高的国家之一——高于欧盟国家 79% 的平均连接率[3]。2011 年，法国四分之一的经济增长都来自于数字产业，成功实现 20 世纪 40 年代末设立的工业政策目标[4]。



法国网络渗透率：83.8%

在 2011 年公布的数字化战略《法国数字化计划 2012—2020：总结与展望》（Plan France Num é rique 2012 — 2020:Bilan et Perspectives）中，法国政府将提高全国信息通信技术（ICTs）使用率，还特别提出要将其机制化以拉动就业和经济增长（法国目前成年人失业率约为 11%，青年失业率约为 25%）。2012 年，法国政府启动其首个为企业提供债券基金支持的欧盟项目，通过为农村地区提供高速宽带（无线）连接服务，来促进全国各地区经济发展更均衡[5]。2013 年，法国启动了一项经济刺激计划，准备在 2025 年前用最佳区域性适用技术将特高速互联网络连接到每户家庭。目前法国（通过电缆或电话线连接至家庭或办公室的）固定宽带已经实现全国连接和使用，而且增长迅速[6]。此外，ICT 部门吸收了法国就业的 3.7%，占 GDP 的 5.2%，私营部门总增加值的 7.9%。2014 到 2015 年，ICT 部门有望创造超过 450,000 份工作和 1,300 亿欧元（约 1,466 亿美元）的增加值[7]。《法国数字化计划 2012—2020：总结与展望》延续了法国政府长期以来以电信（即如今所有的 ICT）行业为主要支撑来促进（尤其

是青年）就业和经济竞争力以及增加社会价值[8]。

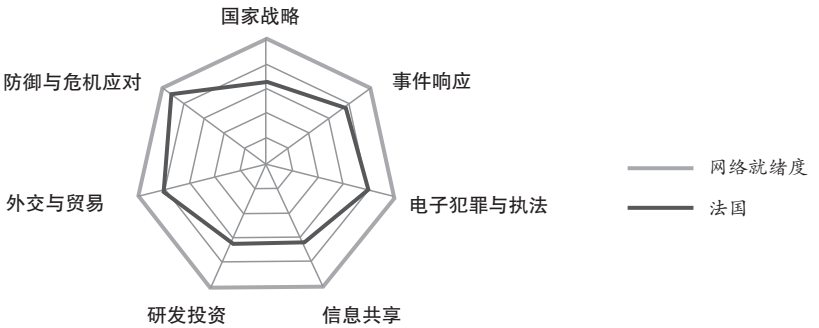
法国数字化战略为2020年前的经济增长设定了57个目标。这些目标中，法国政府主要寻求在2020年前：提高法国各大企业的数字化应用，将所有地面数字频道转换成高清频道，以及将所有政府行政程序转变成为无纸化办公。在该战略之后，法国政府又启动了一个国家级ICT投资项目，包括划拨20亿欧元（约23亿美元）用于全国范围内的互联网基础设施（如高速移动带宽、光纤、数字卫星传输等）建设；22.5亿欧元（约25亿美元）用于数字化服务、内容和应用创新；2.5亿欧元（约2.82亿美元）用于发展智能电网。此外，2012年，法国还启动“大巴黎”（Greater Paris）项目，计划将首都巴黎打造成一个能吸引全球数字企业、人才和投资的数字枢纽[9]。法国公共投资银行（ Public Investment Bank）最近也发起一个名为“公共投资银行数字雄心基金”（Digital Ambition Fund of BPI）的倡议，旨在促进互联网相关的数字创业公司以及物联网（IoT）相关的新兴商业模式的发展。该倡议感兴趣的主要技术领域包括数据区块链、云技术、联网汽车、数字化营销、数字安全等数字产品和服务，这些领域都鼓励使用创新型商业模式。法国公共投资银行称，其初始投资额将介于100万欧元（约110万美元）和1,000万欧元（约1,120万美元）之间[10]。除这些数字经济倡议外，法国还出台了4个层面的政策性文件，以解决网络安全问题对法国经济和安全带来的不利影响。2012年，一份法国参议院的报告将网络安全带来的国家损失形容为“对其外交、文化、科技和经济遗产的一种掠夺”[11]。这些组成整体法国国家网络安全战略的中央政策文件包括：①2008年《国防与国家安全白皮书》；②2011年《法国网络战略》；③2013年《国防与国家安全白皮书》；④2015年《法国国家数字安全战略》[12]。其中第四个文件由法国总理Manuel Valls公布，据称将有力支持法国社会的数据传输建设。Manuel Valls称，该文件的发布“通过加强数字安全建设，我们将有力支持网络空间发展，为法国企业提供可持续增长源泉和更多商机，以此来维护我们的民主价值观和保卫我国公民的数字生活和个人数据”[13]。

法国政府将其经济福祉与国家网络安全直接联系到一起。例如，近期的三起事件有力地显示了网络空间是怎样被恐怖分子用于协调和谋划恐怖袭击活动，新闻媒体是怎样迅速向全世界通告该袭击事件，以及最后法国有关部门又是怎样找出袭击者的。2015年1月，讽刺性杂志《查理周刊》（Charlie Hebdo）责任人因被认为刊出对宗教信仰和近期一些事件不敬的内容，遭到枪杀袭击。2015年11月，巴黎发生6起针对酒吧、体育馆等公共场所的武装袭击。调查显示，恐怖分子是通过WhatsApp和Telegram两款应用的加密通信来策划和实施袭击活动的[14]。2016年7月，尼斯发生的巴士底狱节

（Bastille Day，即法国国庆节）袭击使法国总统延长了“全国紧急状态”的期限，以保证国家安全部队有时间进行特别搜捕行动和更加不受限制地监控互联网使用情况[15]。此外，法国政府与社交媒体和搜索引擎公司举行多场闭门讨论会议，并要求当政府发出警告时，它们需遵照有关部门指示，立即移除极端主义宣传[16]。2016 年 6 月，为了更好地保卫民众安全，法国政府特地发布了一款智能手机应用，来提醒 2016 欧洲杯球迷们潜在的恐怖袭击风险；之后又计划将其用于提升民众未来恐怖袭击风险意识[17]。

在 2015 年和 2016 年恐怖袭击之前，法国就认识到网络安全的重要性。2001 年，法国政府在其信息安全服务部门外另设了一个中央信息系统安全局（DCSSI）。该局由国防部长直接主管，负责协调政府机构和基础设施的网络保护。2009 年，这一中央指挥办公室升级成为国家信息系统安全局（Agence Nationale la S é curit é des Syst è mes d’ Information, ANSSI）。该局于 2011 年公布了法国首个网络安全战略。同年，ANSSI 作为国家机构，又承担起保障信息系统安全的整体社会责任，负责为全国重点行业系统和企业就保护措施提供指导甚至制定规章。法国政府不断集中力量，加大在全国经济和安全方面的网络安全投入。2013 年《国防与国家安全白皮书》强调，实现网络空间安全需要加入其他力量，同时提出培养进攻性网络能力是法国网络防御战略的必要组成部分[18]。紧随着 ANSSI 的成立，法国政府又决定设立网络司令部，标志着其采用将经济视野与国家安全重点协调一致来减少网络威胁的整体社会路径。

本报告采用网络就绪指数 2.0（CRI 2.0）来评估法国应对网络风险的准备度，并制定了一个行动蓝图，来帮助法国进一步了解其互联网基础设施之间的依赖程度和存在的漏洞，以及评估其在缩小现有网络安全状况与支撑未来数字化所需的国家网络能力之间差距的承诺实现能力和成熟度。本报告采用 CRI 2.0 方法论，从七大维度（国家战略、事件响应、电子犯罪与执法、信息共享、研发投资、外交与贸易、防护与危机应对）对法国的网络安全工作及能力进行全面评估。



法国网络就绪度评估（2016）

国家战略

近年来，法国大幅调整了其国防和国家安全重点，来应对影响范围、量级、强度和复杂性都在上升的网络犯罪、政治和经济领域的网络间谍、针对关键基础设施的网络袭击以及包括网络干扰在内的网络威胁。2008 年发布的《国防与国家安全白皮书》是法国首个将整体国家受到的网络威胁作为国家安全和主权面临的重大风险进行重点探讨的重大文件。该文件指出了法国国家安全的新重点——例如网络袭击预防和反应等，并要求负责国家安全保障的相关机构作出变革[19]。依照 2008 年《国防与国家安全白皮书》提出的建议，法国总理直属的三大办公室之一——国防部长办公室（SGDN）改名为国防和国家安全部长办公室（SGDSN）。这一变更将仅依靠武装力量进行的传统防御任务，扩展为整个社会层面更大的安全责任，而这些责任仅依靠武装力量或传统国家安全机构远远不够。这一扩展后的任务反映出，在当前更加复杂和动乱的时代中，尤其是网络犯罪以及国家行为体和非国家行为体敌对活动带来的挑战不断上升的情形下，法国社会亟需保护的现实。2009 年，法国计算机安全中央指挥处（DCSSI）升级为国家信息系统安全局（ANSSI），成为国家信息系统安全的主管部门[20]。作为专门应对国内网络袭击不断增长挑战的主管部门，ANSSI 是总理办公室下属的一个跨部门机构，负责协调关键行业和军队在内的公共机构之间的国家网络安全行动[21]。 2011 年起，网络和信息安全局被正式任命为公共和私人部门信息网络和系统防御的国家机构[22]。

国家信息系统安全局（ANSSI）于 2009 年成立，是法国国家信息系统安全的主管部门。

ANSSI 成立后，法国又于 2011 年公布了其首个国家网络安全战略“信息系统防御和安全：法国国家战略”[23]。该战略提出了四点主要目标：在网络防御领域达到世界领先水平，通过保护主权相关的信息来保卫法国国家决策能力，增强关键基础设施的网络安全保护程度，以及确保网络空间实现安全。2013 年《国防与国家安全白皮书》将 2008 年版本的愿景升级，同时特别强调了针对关键基础设施从事的网络破坏活动带来的威胁[24]。

2015 年，作为针对各关键部门遭受网络袭击不断增长的回应，法国政府又公布了第二个国家网络安全战略“法国国家数字安全战略”[25]。基于之前发布的安全相关文件以及数字战略实施经验，2015 版网络安全战略将目标定于将法国转变成为“数字共和国”，

法国于 2011 年公布其首个国家网络安全战略，并于 2015 年公布第二版。

并指出 ICT 既是促进经济增长和创新的推动力之一，同时也带来网络风险。该战略呼吁法国政府构建保护方式，维护法国在网络空间、国家信息系统和关键基础设施上的根本利益[26]。因此，该战略列出了 5 点关键目标领域，以在确保法国信息通讯技术系统的安全和恢复能力的同时，推动法国向“数字共和国”这一目标迈进。这五大战略重点包括：①维护法国在国家信息系统和关键基础设施等网络空间的根本利益；②通过网络安全产品、技术和法律支持，确保数字信任、个人隐私和个人数据保护；③提高国家网络安全意识和安全能力建设；④为信息通讯技术商业投资和创新营造良好的商业环境；⑤为欧洲数字战略独立制定路线图。

法国 2015 年网络安全战略在操作上遵循了 2011 年数字战略的理念，其许多目标与上一版数字战略中提出的网络安全措施也一致。例如，两个文件都寻求提升网络用户的线上信任，保持高层次的网络安全研发来推动经济增长，以及保护个人数据。最为重要的是，两个文件都指出，ICT 不仅是法国经济增长的支撑，同时 ICT 系统恢复能力和安全性能受到保障也是确保法国最终获取经济增长的保证。尽管最新版的战略文件没有提出要提供新的资金，但法国政府已经在此之前划拨了 10 亿欧元（约 11 亿美元）用于网络安全建设。法国总理 Valls 发布这一文件，标志着法国政府开始对网络安全予以重视[27]。

事件响应

作为法国信息系统安全的国家主管部门，ANSSI 同时还负责对“影响到关键行政部门和运营商”的网络事件作出回应以及协调政府、行业参与国际网络事件回应行动[28]。同时，作为主管网络安全的主要实体，ANSSI 还担任法国政府计算机应急响应小组（CERT）角色，对公共网络和关键基础设施部门提供指导和建议，对敏感政府信息安全基础设施进行审计以及对政府人员进行培训。ANSSI 定期在其官网为政府机构、各大公司及民众发布网络安全和最佳做法建议。

法国于 2000 年设立了首个国家计算机应急反应回应小组（CERT-FR），负责集中数据和为紧急事件应急反应提供支持。

ANSSI 同时还主管法国信息系统安全行动中心（COSSI）。该中心是负责监测和降低国家信息系统受袭击状况的政府机构。2000 年，法国在信息系统安全行动中心内设立了首个国家计算机应急响应小组（CERT-FR），负责集中数据和为紧急事件响应提供支持[29]。该中心最初名为 CERTA，2014 年改名为法国计算机应急小组。作为 ANSSI 在 COSSI 内部设立的机构，法国计算机应急小

组能进行全天候事件处理，同时针对影响法国的网络事件，其作为主要国际联络中心发挥作用。该小组可提供对识别出的漏洞和恶意代码的深度分析；对可能发生网络安全事件的选区进行监测；为关键信息基础设施相关的政府和其他实体协调应急反应措施；为危及国家利益的事件提供预警和情报；以及基于电子邮件报告架构来记录各大网络事件。

法国之前实施了一个名为“Vigipirate”的国家事件反应计划。该计划涵盖 12 个领域，其中的网络安全领域由“Piranet 计划”所覆盖[30]。该方案旨在给对法国国家、人民、财产、环境等根本利益或对各类组织机构的关键活动造成重大威胁的网络袭击进行反击。ANSSI 认定，该层面的袭击包括：对网络或系统进行大范围入侵或以其为目标的行为（例如分布式拒绝服务攻击）；大范围散布破坏性软件或以破坏信息系统完整性为精准目标（例如病毒、恶意软件、蠕虫软件等）；令信息系统广泛或特定的拒绝服务，对其进行干扰、摧毁（例如恶意操纵、破坏等）。

在 2013 年《国防和国家安全白皮书》中，法国明确表示将推进包括情报能力的积极主动的 IT 能力建设，来扩大政府的应急反应方案选择范围。这一路径允许实施“不同阶段且对袭击的量级和严重程度能部分逆转、谨慎控制和按一定比例操作”的进攻行为[31]。作为对 2008 版白皮书的响应，该文件重申，针对的网络袭击的检测能力和保护能力以及对敏感信息系统防御能力是“（法国）国家主权和经济福祉的基本组成之一”。该文件承诺对以上任务增加财政和人力投入，并宣布法国政府将通过立法和调控措施为所有关键基础设施运营者（OIV）和公共部门和私营部门的敏感系统制定安全标准。这些标准将集中于审计、企业信息系统映射、紧急事件处理和通告以及 ANSSI 等国家机构能力建设，来有效介入紧急事件中产生的国家危机。

此外，法国国防部与 ANSSI 合作，正着手建立一个有着 4,000 人的民间网络防御储备力量（RCD），以应对法国领土范围内可能发生的重大网络危机。2017 年，法国还将建立一个数字平台，为公共部门与私营机构合作中的公司和个人网络袭击受害者提供支持[32]。

法国政府的首要责任是保证关键基础设施运营者的安全。2013 年《法国军事作战法案》（Loi de Programmation Militaire 2014—2019, LPM）中制定了适用于政府网络和私营部门关键基础设施运营者的 4 项特别安全措施[33]。相应的，ANSSI 被授权：①为关键基础设施运营者的关键系统制定强制性安全规定；②授权进行安全检查；③授权制定重大危机时的特定措施；④接收关键基础设施运营者的关键系统发生的事件的强制性报告。这些措施中许多与欧洲委员会 2016 年 5 月颁布并于 2016 年 8 月生效的新版

《欧盟网络和信息安全（NIS）指令》中的规定相一致[34]。法国已经大力调整国内法律来适应该新指令。其他措施包括确保法国银行、电信提供商、零售商采用入侵检测系统以及将所有事件都报告给 ANSSI， ANSSI 将对私营和公共实体进行审计。

同时，ANSSI 还与行业利益相关者合作，为使用有关键基础设施的部门提出建议，帮助该设施的拥有者、运营者和政府监督者更好地应用网络安全相关法规。此外，ANSSI 还与一些私营企业合作，发起了一个针对 IT 和网络安全部门的认证倡议——法国“网络安全标志”，旨在推动为国内使用和向其他市场出口所使用的法国安全解决方案建立高标准[35]。

最后，法国每两年举行一次由 SGDSN 组织的国家级危机管理演习，包括（网络安全领域的）Piranet 以及（空域的）Pirate–Air、（海域的）Pirate–Mer、（核领域的）Pirate–Nuclear、（放射性、生物和化学领域的）NRBC 和（地铁领域的）Metro–Pirate。它们都遵照国家计划，并被因国家安全原因受到保护和被严格管控。这些演习的策划时间长达 6 个月，通常由 SGDSN、部委和私营部门合作伙伴之间的一系列会议组成，会上将讨论并制定演习的目标、前景和频率[36]。法国目前参加了欧盟（例如欧洲网络演习）和北约（例如锁定盾牌演习 2016，Locked Shields 2016）等多国演习活动[37]。

电子犯罪和执法

法国 2001 年签署并于 2006 年批准了欧盟理事会《网络犯罪公约》（也称《布达佩斯公约》，目前正推动其网络安全法进行国际协调，并制定一系列新的网络反犯罪法。法国支持欧盟成员国之间建立一个简化法律合作的系统，来促进数据共享，遏制网络犯罪[38]。

按照 2013 年《国防和国家安全白皮书》确定的指导原则，法国制定 2013 年《军事作战法令》，要求制定网络安全标准，帮助公共和私人部门关键基础设施运营者（在 ANSSI 协助下）保护自身免遭网络攻击伤害[39]。2015 年《查理周刊》袭击事件后，法国国民议会通过新的《情报法案》，允许情报机构监控涉嫌恐怖主义活动者的手机、电子邮件、互联网使用情况。法国同时还修订现有法律规章，允许政府关闭被认定为“同情恐怖主义”的网站。该法律最新修订后，进一步允许政府监控嫌疑人的社交媒体发布内容[40]。然而，这些规定在司法调查和内容记录层面也存在重大问题，导致政府和社交平台提供商之间的冲突和合作情况复杂多变[41]。

2014 年，法国内政部任命了一个“网络协调官”，来协调内政部的网络行动以及实施部级行动计划来对抗网络威胁。

此外，法国政府还升级了网络相关的其他法规表述[42]。例如，2016 年 1 月，法国国民议会通过《数字共和国法案》（“Digital Republic”Bill），将支持 2011 年国家数字战略框架的一些必要措施确立为法律[43]。该法案对法国 1978 年《数据保护法案》做了几处新的修订。1978 年《数据保护法案》在此前已经被修订 9 次，最新修订版本于 2014 年通过[44]。尤为重要的是，《数字共和国法案》扩大了国家信息技术和自由委员会（Commission Nationale de l’Informatique et des Libertes, CNIL）的权力，使其有权对犯罪相关等类型的个人隐私侵犯行为增加量刑[45]。

内政部下属的警察和宪兵队负责打击网络犯罪。自 20 世纪 90 年代末起，法国宪兵队这一担负有民事警察职责的军事力量为打击网络犯罪设立了多个部门，包括网络犯罪法律研究和文档部门（STRDJ）、宪兵队犯罪研究所（IRCGN）、打击数字犯罪中心（C3N）、国家儿童色情图像中心（CNAIP）以及国家警察培训中心（CNFPJ）特别培训项目[46]。此外，2014 年，内政部任命了一个“网络协调官”（Cyber Prefect）来协调内政部网络倡议和指挥部门内部打击网络犯罪和经济间谍行动计划的实施，通过其构建法国遭受网络威胁时的恢复能力。该行动计划有三大战略目标：在处理网络犯罪和支援受害者上更为积极主动，与网络利益相关者建立更为有效的对话，以及采用相关国内和国际法律框架[47]。

信息共享

2015 年国家网络安全战略中，法国已承诺将建立国内和国际伙伴关系，推动基本数据（例如产品和服务漏洞或缺陷信息）共享，以确保相关标准和相应安全措施在所有关键部门的有效实施。其中 ANSSI 负责协调事件回应和整体社会信息共享两项工作。尽管 2013 年《军事规划法案》中已经立法规定了关键基础设施运营者应执行的安全标准，但之后三年并未真正实行，一直到 2016 年 7 月 1 日才正式生效。这使得 ANSSI 和相关受影响部门有充足时间完成谈判、商定如何最佳实现信息共享和实施相关标准，推动法国建立更强大的网络防御态势[48]。

法国国家反僵尸网络支持中心通过病毒监测和清除服务对私营部门提供援助。

此外，2013 年《军事规划法案》还规定 OIV 须向 ANSSI 通报可能对各自 IT 系统运行造成危害的事件。OIV 可以是医疗、公用事业、电信、交通和财政等部门的一部分。在此背景下，这些部门均设立了工作组以制定出效率和兼容性都较好的规定。另外，2016 年新版《数字共和国法》推出了三条新规定，扩大了公共部门与民众及原则上不涉密

的网络安全研究的私营单位之间的信息共享[49]。

由于 ANSSI 之外，法国并没有其他政府信息共享机构，非盈利研究中心等许多信息交流机制对其进行了补充。例如，2014 年，法国国家反僵尸网络支持中心“Antibot.fr”作为 14 个欧盟国家非盈利网络的一部分正式成立，而该网络由欧洲委员会的 ICT 政策支持项目下的旗舰项目资金资助。该中心由法国打击网络犯罪专家中心（CECyF）和信号垃圾邮件项目（Signal Spam）联合成立，可提供及时有效的信息防止僵尸网络扩散，同事还能通过监测网站受感染情况和网络异常情况协助私营部门清除病毒[50]。最后，至少有 20 个承担了相关使命的具体部门的 CERT 参与了信息共享活动[51]。

研发投资

法国 2011 年数字战略强调了网络安全研发投资对推动经济增长的重要性。该战略确认法国政府计划投入 1.5 亿欧元（约 1.7 亿美元）用于支持五大战略性数字技术和服务领域的研发：物品连接（物联网）、超级计算、云计算、大数据分析以及信息网络安全[52]。作为该战略的一部分，法国政府还启动一个“国家投资计划”（National Investment Programme），初步要求建立云计算技术研发项目的投入，并在斯诺登泄密事件后加大了支持力度[53]。总共有 5 个项目受到了法国政府 1,900 万欧元（约 2,100 万美元）的国家投资支持：Orange 公司的云力量（CloudForce）项目、Prologue 公司的云港（CloudPort）项目、Bull 公司的麦哲伦（Magellan）项目、Non Stop System 公司的 Nu@age 项目以及 INEO 公司的 UnivCloud 项目。

该数字战略还包括对小型孵化器项目的支持。例如，法国政府给弗雷西奈敞厅（Halle Freyssinet）划拨了 2 亿欧元（约 2.27 亿美元）。该孵化器场地 2016 年落成后可容纳超过 1,000 家创业公司。法国也是大量 ICT 创新产业群的聚集地，聚集有致力于打造数字内容及其多媒体分销和交流的巴黎大区 Cap Digital 公司，致力于通信网络的布列塔尼和卢瓦尔地区 Images et R é seaux 公司，致力于安全处理和通信解决方案的普罗旺斯 Secure Communication Solution 公司，以及致力于复杂系统和通用软件的巴黎大区 Systematic 公司等[54]。

2012 年 10 月，法国政府公布了“大巴黎计划：打造数字城市”（The Greater Paris Project: Building a Digital City），打算在巴黎近郊和周边地区建立世界级数字公司产业群，将数字部门从业者聚集到一起来刺激产业发展动力和推动创业、投资。此外，法国前部长佩勒林（Fleur Pellerin）发起了“法国科技”（La French Tech）倡议，将一些有着经济活力、国际气象和创业文化的城市列为“法国科技之城”（M é tropoles

French Tech）。该倡议共筹集到 2 亿欧元（约 2.234 亿美元）资金用于投资，旨在将法国转变成为公共部门和私营部门都参与的“数字共和国”[55]。

此外，在国防工业的资助下，法国政府还通过设立各类“研究主席（Chairs of Research）”，如卡斯泰高级国防研究所（IHEDN）网络战略主席等，对国防研究机构进行支持。在此资助下，卡斯泰高级国防研究所将政府行政部门和军队高级管理人才集中到一起，旨在就国防、外交政策、军备和国防经济等方面战略问题进行高级培训、思考和辩论。此外，法国政府还资助了其他一些优秀的研究中心，例如，专注于陆军领域研究的圣西尔军事学校（École Spéciale Militaire）网络安全主席；专注于各自军事服务研究领域的海军主席、网络空军主席等[56]。

法国政府计划将雷恩地区打造成法国和欧洲先进的网络枢纽。

发展网络研发行业是法国政府的关键目标之一，其正计划将雷恩地区打造成法国和欧洲先进的网络枢纽[57]。2013 年《国防和国家安全白皮书》要求法国政府机构之间、网络行业之间建立更为紧密的合作来对抗网络威胁。作为响应，法国国防部于 2014 年建立卓越网络防御中心（Pôle d’Excellence Cyber, PEC）。该中心与军备信息安全总局（Directorate General for Armaments for Information Security）均位于布列塔尼地区，负责整合国防部网络培训、研究和技术整合。雷恩地区正着手将国防部的卓越网络防御中心、军备信息安全总局、（下属军事计算机紧急响应小组 MilCERT 的）防御性网络作战分析中心（Centre d’Analyse et de Lutte Informatique Defensive, CALID）、陆军信号参谋部（Army Signals General Staff）、807 网络防御军队公司、信号学院、圣西尔军校以及诸多大学和网络安全公司联结成紧密网络[58]。

卓越网络防御中心同时还计划为军队之外的武装部队和研究机构雇员培养作战模拟和训练能力[59]。例如，该中心于 2016 年为网络行业创业公司举办了“西方网络挑战”（CWC）大赛。大赛的重点设在网络安全和网络防御领域，由公司、银行、军事单位和南布列塔尼大学等众多 ICT 行业的合作伙伴协办。该比赛通过特定奖品，如通过承包方式获取专属和安全的场地等，对网络防御创业公司进行支持。该比赛计划建立一个网络产业孵化器，在理想地理位置为这些公司提供良好的产业、研发、训练和军事生态系统[60]。大学、产业和政府机构间的其他跨机构合作也正在推进。

最后，法国政府在 2013 年启动了“法国新工业化”计划[61]。该计划的第二阶段——“未来产业”已于 2015 年 5 月启动，旨在推动法国产业向数字时代迈进，囊括 34 个产业领域，其中涉及网络产业的有：智能电网、数字医院、大数据、云计算、电子教育、

增强现实、非接触服务、超级计算机、机器人和网络安全等领域。法国政府已承诺将投入 37 亿欧元（41 亿美元）资金专门用于该计划[62]。

外交与贸易

2015 年法国网络安全战略旨在推进“欧盟成员国之间的合作，一定程度上促进欧洲数字战略独立，长期确保网络空间更安全和尊重我们的价值观”[63]。此外，该战略重申了法国政府加强“在国际网络安全探讨中的存在和影响……探索预防网络空间冲突的新管理机制……（以及）巩固各国承诺在网络空间遵照国际法行事的国际基础”的计划[64]。

2014 年，法国外交与国际发展部设立网络外交和数字经济大使一职。

根据国家网络安全战略中提出的目标，法国定期参与多边网络安全谈判，并加入了所有网络相关事务的主要国际治理机构，如联合国等（其“于 2013 年承认国际法在网络空间适用性”）[65]。法国是联合国信息安全政府专家组（UN GGE）在讨论国际安全背景下的信息和电信领域发展问题上的“关键网络力量”，推动 UN GGE 在 2013 年的报告中“确认国际法适用于网络空间”，并在 2015 年新达成的报告中提出了负责任的国家行为应该遵守的规范和国际法是网络空间适用性上的建议。2015 年 12 月，联合国大会采纳了报告中推行自愿非约束性网络空间规范的提议，之后的 G20 会议也表示支持[66]。

法国积极加入为信息社会和信息恢复能力建设制定政策建议的经合组织（OECD）信息安全和隐私工作组（WPISP）等其他相关国际组织，致力于网络安全政策制定[67]。法国还是欧盟理事会总统之友网络问题工作组（Friends of the Presidency Working Group）的成员。该工作组于 2012 年成立，旨在为欧盟成员国提供一个跨国网络问题垂直协调和探索各国间潜在协同能力的机制。此外，法国深度参与了“欧盟网络安全战略”的制定。该战略由欧洲委员会和欧盟外交事务及安全政策高级代表团于 2013 年 2 月提出[68]。

此外，法国是关于出口控制的 2013 年《瓦森纳协定》的活跃成员。该协定旨在通过推进常规武器和两用物品及技术转让方面的透明度和责任，来促进地区和国际安全和稳定。通过签订该协定，法国承诺“将军控作为出口政策的一大组成部分，并使其受到最严格的国家军控程序监管”[69]。近期，法国正着手推动完成《跨大西洋贸易与投资伙伴关系协定》（TTIP）谈判，其中就包含有网络内容。然而，该协定在欧洲，尤其是法国和德国，正因“成为民粹主义的温床和对欧洲经济不利”遭受越来越多的

批评，法国官方也承认近期批准该协定不太可能[70]。

法国已制定了一项国家政策，意图通过加大对非官方国际论坛的投资来促进技术团体、学术团体、政策制定者之间的合作，同时推动ICT出口和网络安全产业国际化，以此来增加在国际舞台的影响力[71]。与之前各政府部门独自推出倡议不同，目前这些政策路径都采用了跨政府部门的协作架构。

其中，外交与国际发展部负责国际网络安全参与，以及制定外交政策推动建立自由、开放、安全和稳定的网络空间。2014年10月，该部门设立了一个特殊的网络安全协调职位——法国网络外交和数字经济大使，负责所有国际网络安全事务，包括但不限于在良好网络空间治理标准、国际法的适用、公民自由和隐私的保护上签订协议以及推动法国公司走出去[72]。

防御与危机应对

按照规定，法国国防部负责保护国防系统和为整个国家提供防御支持[73]。2008年《国防和国家安全白皮书》将网络安全列为国家安全的重点之一，并为发展“进攻性和防御性网络战争能力”提供建议[74]。然而，在该白皮书中的细则完全实施前，飞客（Conficker）蠕虫病毒感染了大量非机密性法国军队内部网络，导致信息传递和后勤服务受到干扰，影响到作战能力。不过，因有备用交流渠道，歼击机部队仅受到部分影响；而严格保密的作战网络则完全未受到影响[75]。

此事件后，国防部大力推动国防和军队网络转型，使其更专业化、更具战略性，以及尤其更能预防和减少潜在网络挑战。2009年，法国迈出新的一步，建立了ANSSI，将国内武装力量和相关军队和警队情报机构囊括其中。2011年，法国政府公布国家网络安全战略“信息系统防御和安全：法国国家战略”，计划将法国打造成“网络防御领域的世界强国”，同时扩大ANSSI的权力[76]。同年，依照2011年《网络联合作战条令》，法国国防部设立了网络防御将官（OG Cyber）一职以及联合作战计划和指挥控制中心（CPCO）内建立的网络防御作战司令部等相关单位[77]。网络防御将官负责在发生网络危机时确保国防信息系统受到保护，以及应邀与ANSSI合作保护其他国家网络[78]。

2013年《国防和国家安全白皮书》延续了2008年版的宗旨，提出要提升国防部在网络防御领域的地位，使其为整个国家提供全方位网络防御能力[79]。在该文件中，法国指出“网络空间已成为一大对抗领域”，网络袭击“能轻易地使整个国家活动瘫痪，引发技术或生态灾难，导致无数人受害。因而它是一种真正的战争行为”[80]。此外，法国国防部还在该文件中指出构建先进“识别和攻击行动能力”的必要性，并将

其列为“对网络袭击实施可行且适当回应的根本能力”[81]。该文件同时还确认，“国防部须在所有情况下都保持行动能力，甚至是上述情形外其他机构发现其运行受到网络攻击破坏或干扰的状况下，也能提供支持”[82]。

网络防御将官以下设立了“网络司令部”类似部门，并配有相关员工、部队和作战能力。

为落实 2013 年《国防和国家安全白皮书》中提出的网络防御目标，法国国防部于 2014 年宣布投入 10 亿欧元（约 1.1 亿美元）建立《网络防御公约》（Pacte D é fense Cyber 2014 — 2016）。该文件设定了六大目标：①加强防务部门以及可信赖合作伙伴信息系统的安全级别；②在对产业基地进行支持的同时，推动未来技术、学术和实际操作领域取得研究成果；③加大网络防御领域人力资源投入；④在布列塔尼地区建立国防部下属的卓越网络防御中心和网络防御团体；⑤构建一个欧洲合作伙伴战略利益网络；⑥基于某一个圈子或合作伙伴以及后备网络，进一步推动建立国家网络防御团体[83]。文件列出了 50 条措施来确定国家网络防御方针和实现以上宏大目标。

这些措施包括：加强 2011 年设立机构的建设、扩大网络防御将官的指挥权以及进一步促进防御性单位甚至在较小程度上的攻击性单位的实际作战能力建设。[84] 该改进措施还包含与 ANSSI 为紧急事件展开更大合作上，包括在同样的前提下，共同为国防部防御性网络行动分析中心（Centre d’Analyse et de Lutte Informatique Defensive, CALID，下属 MilCERT）选址[85]。CALID 是“国防部的中心专家智囊团，同时还是国防部网络袭击准备和反应中心（MilCERT）”，通过全天候监测找出以军队为目标的网络袭击活动[86]。此外，2014 年《网络防御公约》要求建立国家网络防御行动储备（RCD），在重大危机中对国家和国防部进行援助。这些储备单位将与 ANSSI 和国家宪兵队展开紧密合作[87]。

综合以上措施，网络防御将官以下设立了“网络司令部”类似部门，并配有相关员工、部队和作战能力[88]。更准确而言，这一高级职位位于国防部长之下的网络安全和防御作战指挥链顶端。网络防御将官“在规划和作战中心享有控制权，在国防部和武装部队的信息系统上以及对军事行动进行支持的网络作战行动中，负责网络防御规划、协调和实施”，以及“协调和构建国防部内的这三种服务”[89]，因而其在专注于网络作战的法国联合参谋部网络防御处内指挥网络部门和实施备战和规划。作为关键的参谋，中央计算机作战司令（Officier de Lutte Informatique Defensive, OLID）负责监督网络部队在武装部队中的部署，而网络管理部队负责实施网络防御将官的决策[90]。

作战任务和部队扩大的同时，国防预算中的网络部分也随之增加。2014 年，法

国国防部长宣布划拨 10 亿欧元（约 11 亿美元）用于实施 2014 年《网络防御公约》中提出的 50 项措施[91]。例如，其中部分资金将用于将布列塔尼卓越网络防御中心的员工从 250 人扩大近两倍至 450 人。法国政府 2015 年国防支出占 GDP 2.1%，其中网络相关的活动占比有所扩大，总体上达到了北大西洋公约（NATO）有关国防开支不少于 GPD 2% 的规定[92]。

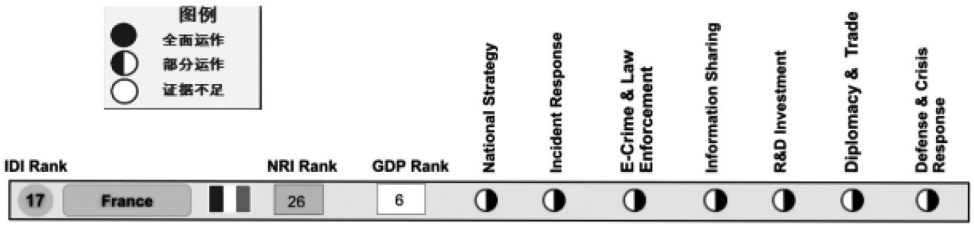
总体而言，正如在紧急事件反应部分所述，法国武装力量在国内和同盟的网络演习，尤其在“网络联盟”（Cyber Coalition）等 NATO 网络防御演习中表现积极。2014 年《网络防御公约》中，国防部提出了一大目标，即“在所有层面的武装力量演习中，系统性地增加网络防御活动”[93]。这些演习的目的在于确保在网络袭击、干扰或确信受到威胁的形势下，各大层面的武装力量仍能正常作战，包括常规化地“将网络空间纳入指挥空间的能力”[94]。 2015 年，法国举办了首次网络防御国际论坛。该论坛重点关注了各类国际网络问题，共有 26 个外国代表团参加[95]。

最后，法国国防部在各大危机中国内网络防御方面扮演了积极角色。例如，为了对 2015 年《查理周刊》袭击事件和后续针对平民和军队的网络袭击做出反应，法国武装部队总参谋部在法国历史上首次设立了网络危机部门[96]。2016 年尼斯发生巴士底狱节袭击事件后，法国国防部召集了至少 12,000 名储备人员参与作战，这些人员中的部分就来自于网络防御储备部队[97]。

CRI 2.0 概要

CRI 2.0 评估结果显示，法国正处于网络就绪的路上，并已开始运作 CRI 七大评估要素中的部分领域。

分析结果反映了法国当前不断变化的格局。法国持续制定并刷新其经济（数字）议程、国家网络安全战略、政策及各项举措，寻求国家经济愿景与安全重点工作之间的平衡。国家概况的变化反映出国家在各个方面发生的变化，有利于监测、跟踪并评估法国社会所取得的显著进步。



CRI 2.0 利用全面、可比较、基于经验制定的方法论，帮助国家领导人在网络化、竞争激烈、冲突丛生的世界中做出规划，打造安全、有活力的数字世界。

如需了解更多 CRI 2.0 的相关信息，请参阅：http://www.potomacinstitute.org/academic-centers/cyber-readiness-index

注释

1.Hugh Schofield, “Minitel: The rise and fall of the France-wide web,” BBC News, June 28, 2012, http://www.bbc.com/news/magazine-18610692.

2.James Foreman-Peck,“European Industrial Policies in the Post-war Boom: ‘Planning the Economic Miracle’,” in Industrial Policy in Europe After 1945, (Palgrave Macmillan UK, 2014): 14, http://www.palgraveconnect.com/pc/doifinder/view/10.1057/9781137329905.0008.

3.World Bank, “Internet users (per 100 people),” 2014, http://data.worldbank.org/indicator/IT.NET.USER.P2.

4.Premier Ministre, “France Numérique 2012-2020: Bilan et Perspectives,” November 2011, http://www.entreprises.gouv.fr/files/files/directions_services/secteurs-professionnels/etudes/2011_plan_france_numerique2020.pdf.

5.Cécile Barbière, “France launches EU’s first digital infrastructure ‘project bond,’” EuroActiv, October 15, 2015, http://www.euractiv.com/section/regional-policy/news/france-launches-eu-s-first-digital-infrastructure-project-bond/

6.Pascal Brangetto, “National Cyber Security Organisation: France,” NATO Cooperative Cyber Defense Center of Excellence (2015): 5.

7.Embassy of France in London, “France aims to put tech at the heart of its economy by 2020,” France in the United Kingdom, http://www.ambafrance-uk.org/France-aims-to-put-tech-at-heart.

8.OECD, “OECD Digital Economy Outlook 2015,”(OECD Publishing: Paris): 21, http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm.

9.Embassy of France in London, “France aims to put tech at the heart of its economy by 2020.”

10.BPI France, “Le Fonds Amibition Numérique,” December 2, 2011, http://www.bpifrance.fr/Bpifrance/Nos-metiers/Fonds-propres/Fonds-directs-Bpifrance/Capital-Innovation/Le-Fonds-Ambition-Numerique.

11.French Senate, “Rapport Bockel,” July 18, 2012, http://www.senat.fr/notice-rapport/2011/r11-681-notice.html.

12.Premier Ministre, “French National Digital Security Strategy,” (2015),

http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf.

13.ANSSI, “Cybersecurity in France,” http://www.ssi.gouv.fr/en/cybersecurity-in-france/.

14.“2015 Paris Terror Attacks Fast Facts,” CNN, April 13, 2016, http://www.cnn.com/2015/12/08/europe/2015-paris-terror-attacks-fast-facts/

15.[Matthew Dalton and Sam Schechner, “France Tried to Ramp Up Defenses Ahead of Paris Attacks,” The Wall Street Journal, November 14, 2015, http://www.wsj.com/articles/paris-attacks-underscore-security-challenge-1447462066.

16.“France asks US Internet giants to ‘help fight terror,’” Al Jazeera, February 21, 2015, http://www.aljazeera.com/news/2015/02/france-asks-internet-giants-fight-terror-150221063706705.html.

17.“France Launches a Terrorism App,” Security Magazine, June 9, 2016, http://www.securitymagazine.com/articles/87182-france-launches-a-terrorism-app.

18.Ministry of Defense, “French White Paper on Defence and National Security,” (2013): 43, http://www.ladocumentationfrancaise.fr/rapports-publics/134000257-livre-blanc-sur-la-defense-et-la-securite-nationale-2013?xtor=EPR-526.

19.Ministry of Defense, “The French White Paper on Defence and National Security,” (2008): 12.

20.ANSSI, “Cybersecurity in France.”

21.Pascal Brangetto, “National Cyber Security Organisation: France,” NATO Cooperative Cyber Defense Center of Excellence (2015): 9

22.NATO Parliamentary Assembly: Science and Technology Committee, “Cyber Space and Euro-Atlantic Security,” Special Report, (November 2014): 9.

23.Premier Ministre, “Information Systems Defence and Security: France’s Strategy,” (2011), http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

24.Ministry of Defense, “French White Paper on Defence and National Security,” (2013).

25.Premier Ministre, “French National Digital Security Strategy,” (2015).

26.World Bank, “Internet users (per 100 people),” http://data.worldbank.org/indicator/IT.NET.USER.P2.

27.Tom Reeve, “French government launches national cyber security strategy,” SC Magazine, October 19, 2015, http://www.scmagazineuk.com/french-government-launches-national-cyber-security-strategy/article/447973/.

28.Premier Ministre, “French National Digital Security Strategy,” (2015): 20.]

29.ANSSI, “CERT-FR – Centre gouvernemental de veille, d’alerte et de réponse aux attaques informatiques,” http://www.cert.ssi.gouv.fr/.

30. ANSSI, “Plan Piranet,” http://www.ssi.gouv.fr/agence/cybersecurite/plans-gouvernementaux/.

31. Ministry of Defense, “French White Paper on Defence and National Security,” (2013).

32. Melissa Hathaway's interview with Valérie Derouet-Mazoyer, Coordinator of the French Nuclear Industry Strategic Committee (CSFN), September 16, 2016.

33. Legifrance, “LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale,” https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825.

34. European Council, “EU-wide cybersecurity rules adopted by the Council,” May 17, 2016, http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/.

35. “Cyber-security: France Leads the Way in Europe,” Media Econocom Blog, May 7, 2015, http://blog.econocom.com/en/blog/cyber-security-france-leads-the-way-in-europe/.

36. ANSSI, “French Cybersecurity Exercises,” June 27, 2012, https://www.enisa.europa.eu/events/cyber-exercise-conference/presentations/9.%20Conf%20Paris%20-June%202012-%20-%20A.%20OGEE%20-ANSSI%20France.pdf, and ANSSI, "Cyber-attaques: l'exercice PIRANET 2012 met l'État à l'épreuve d'une crise informatique majeure," http://www.ssi.gouv.fr/publication/cyber-attaques-lexercice-piranet-2012-met-l-etat-a-lepreuve-dune-crise-informatique-majeure/.

37. Thomas Renard, “The Rise of Cyber Diplomacy: the EU, its Strategic Partners, and Cyber- Security,” European Strategic Partnerships Observatory 7 (June 2014): 14, http://www.egmontinstitute.be/wp-content/uploads/2014/06/ESPO-WP7.pdf.

38. Government of France, “French National Digital Security Strategy,” (2015): 23.

39. Legifrance, “LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale,” https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825.

40. Alessandria Masi, “France's online war on terror sympathizers and extremists has a new cyber security cell,” IBT, http://www.ibtimes.com/frances-online-war-terror-sympathizers-extremists-has-new-cyber-security-cell-1786662.

41. Melissa Hathaway's interview with Frédérick Douzet (Ph.D.), Chairwoman of the Castex Chair of Cyber Strategy and Professor at the French Institute of Geopolitics, Paris 8 University, September 8, 2016.

42. Premier Ministre, “French National Digital Security Strategy,” (2015): 15.

43. Government of France, “Explanatory Memorandum,” January 2016, http://www.

republique-numerique.fr/pages/digital-republic-bill-rationale.

44.Commission Nationale de l'Informatique et des Liberties, "Loi Informatique et Libertes, Act No. 78-17 January 1978 on Information Technology, Data Files and Civil Liberties," (January 1978), https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf.

45.Nadège Martin and Geoffroy Coulouvrat, "French National Assembly adopts "Digital Republic" bill," Norton Rose Fulbright, March 10, 2016, http://www.dataprotectionreport.com/2016/03/french-national-assembly-adopts-digital-republic-bill/.

46.Gendarmerie Nationale, "Cybercriminalité," http://www.gendarmerie.interieur.gouv.fr/Notre-Institution/Nos-missions/Police-judiciaire/Cybercriminalite.

47.Government of France, "Cybersecurity: the Government's Strategy," January 28, 2016, http://www.gouvernement.fr/en/cybersecurity-the-government-s-strategy.

48.Reynald Fléchaux, "Cybersécurité : les grandes entreprises trouvent un modus vivendi avec l'Assi," Silicon, January 26, 2016, http://www.silicon.fr/cybersecurite-grandes-entreprises-trouvent-modus-vivendi-anssi-136930.html.

49.Samuel Greengard, "France Embraces Digital Transformation," Communications of the ACM, June 3, 2016, http://cacm.acm.org/news/203101-france-embraces-digital-transformation/fulltext.

50.Antibot, "Lancement d'Antibot.fr," December 10, 2014, http://www.antibot.fr/blog/lancement-d-antibot.fr.

51.ANSSI, "Les CSIRT Français," http://www.cert.ssi.gouv.fr/cert-fr/cert.html.

52.OECD, "OECD Digital Economy Outlook 2015," (OECD Publishing: Paris): 24.

53.Melissa Hathaway's interview with Frédérick Douzet (Ph.D.), September 8, 2016.

54.Embassy of France in London, "France aims to put tech at the heart of its economy by 2020," France in the United Kingdom, http://www.ambafrance-uk.org/France-aims-to-put-tech-at-heart.

55.Ibid.

56.Ibid.

57.Philippe Vitel and Henrik Bliddal, "French Cyber Security and Defence: An Overview," Information & Security: An International Journal, vol. 32 (2015): 9, http://connections-qj.org/system/files/3209_france.pdf.

58.Ibid.

59.Ministry of Defense, "Cyber Defence Pact: 50 Measures to Change Scale," (2014): 16.

60."Cyber West Challenge," http://www.cyberwestchallenge.bzh/en/.

61.Embassy of France in London, "The Industry of the Future," September 17, 2015, http://www.ambafrance-uk.org/The-Industry-of-the-Future, and http://

tradebridgeconsultants.com/news/government/president-francois-hollande-launches-new-industrial-france/

62.Trade Bridge Consultants, “President François Hollande launches ‘New Industrial France’,” http://tradebridgeconsultants.com/news/government/president-francois-hollande-launches-new-industrial-france/.

63.Premier Ministre, “French National Digital Security Strategy,” (2015): 9.

64.Legifrance, “LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale,” https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825and Alessandria Masi, “France’s online war on terror sympathizers and extremists has a new cyber security cell,” http://www.ibtimes.com/frances-online-war-terror-sympathizers-extremists-has-new-cyber-security-cell-1786662.

65.OECD, “OECD Digital Economy Outlook 2015,” http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm.

66.Ministry of Foreign Affairs, “France and Cyber Security,” December 2014, http://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/.

67.Thomas Renard, “The Rise of Cyber-Diplomacy: the EU, its Strategic Partners and Cyber-Security,” European Strategic Partnership Observatory, (June 2014):12, http://www.egmontinstitute.be/wp-content/uploads/2014/06/ESPO-WP7.pdf.

68.Ministry of Foreign Affairs, “France and Cyber Security,” December 2014, http://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/.

69.“French Policy on Export Controls for Conventional Arms and Dual-Use Goods and Technologies,” http://www.wassenaar.org/wp-content/uploads/2015/12/fr1_en.pdf.

70.AFP, “EU-US trade deal ‘impossible’ in 2016: French minister Matthias Fekl,” The Economic Times, July 5, 2016, http://economictimes.indiatimes.com/news/international/business/eu-us-trade-deal-impossible-in-2016-french-minister-matthias-fekl/articleshow/53065263.cms.

71.Premier Ministre, “French National Digital Security Strategy,” (2015): 40.

72.Ministry of Foreign Affairs, “France and Cyber Security,” December 2014, http://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/.

73.Pascal Brangetto, “National Cyber Security Organisation: France,” NATO Cooperative Cyber Defense Center of Excellence (2015): 11.

74.Ministry of Defense, “The French White Paper on Defence and National Security,” (2008): 9.

75.Kim Willsher, “French Fighter Plans Grounded by Computer Virus,” The Telegraph, February 7, 2009, http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html.

76.Premier Ministre, “Information Systems Defence and Security: France’s Strategy,” ANSSI, (2011), http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

77.Ministry of Defense,“Cyber Defence Pact: 50 Measures to Change Scale,”(2014): 5.

78.Ministry of Foreign Affairs, “France and Cyber Security.”

79.“Europe Proposes New Laws and Regulations on Cybersecurity,” Jones Day, January 2014, http://www.jonesday.com/europe-proposes-new-laws-and-regulations-on-cybersecurity-01-02-2014/.

80.Ministry of Defense, “French White Paper on Defence and National Security,” (2013): 4, 43.

81.Embassy of France in London, “France aims to put tech at the heart of its economy by 2020,”http://www.ambafrance-uk.org/France-aims-to-put-tech-at-heart.

82.Ministry of Defense,“Cyber Defence Pact: 50 Measures to Change Scale,”(2014): 5.

83.Ministry of Defense, “Présentation du Pacte Défense Cyber,” November 2, 2014, http://www.defense.gouv.fr/actualites/articles/presentation-du-pacte-defense-cyber.

84.Ministry of Defense, “Cyber Defence Pact: 50 Measures to Change Scale,” (2014): 6-9.

85.NATO Parliamentary Assembly: Science and Technology Committee “Cyber Space and Euro-Atlantic Security,” Special Report (November 2014): 9.

86.Michel Baud, “American Military Cyberdefense, an Example for France?,” Chaire de CyberDéfense et Cybersecurité, Saint-Cyr Publication Series, vol. 111, n. 8, (July 2013): 1-3.

87.Philippe Vitel and Henrik Bliddal, “French Cyber Security and Defence: An Overview,” (2015): 9.

88.CyberDef-CyberSec, “4th Cyber Def - Cyber Sec Conference 2016,” June 14, 2016, Paris.]

89.Philippe Vitel and Henrik Bliddal, “French Cyber Security and Defence: An Overview,” (2015): 8.

90.Michel Baud, “American Military Cyberdefense, an Example for France?”, 3.

91.Ministry of Defense, “Cyberdéfense,” Direction Général des Relations Internationales et de la Stratégie, June 22, 2016, http://www.defense.gouv.fr/dgris/enjeux-transverses/cyberdefense/cyberdefense.

92.Pascal Brangetto, “National Cyber Security Organisation: France,” (2015): 12.

93.Ministry of Defense,“Cyber Defence Pact: 50 Measures to Change Scale,”(2014): 9.

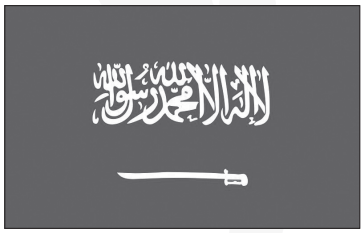
94.Embassy of France in London, “France aims to put tech at the heart of its economy by 2020.”

95.Melissa Hathaway's interview with Frédérick Douzet （Ph.D.), September 8, 2016.

96.Nathalie Guibert, “Cyberattaques: l'armée a activé pour la première fois une cellule de crise,” Le Monde, January 1, 2015, http://www.lemonde.fr/pixels/article/2015/01/17/cyberattaques-l-armee-a-active-pour-la-premiere-fois-une-cellule-de-crise_4558160_4408996.html?xtmc=cyber&xtcr=1.

97.“Nice attack: France calls up to 12,000 reservists,” BBCNews, July 17, 2016, http://www.bbc.com/news/world-europe-36817435.

沙特阿拉伯网络就绪度报告



国家人口	3154 万
人口增长率	2.1%
按市价计算的 GDP（当前美元）	6460.02 亿
GDP 增长率	3.5%
引入互联网的年份	1994
国家网络安全战略	2013 年（尚未发布）
互联网域名	.sa
固定宽带用户渗透率	69.6%
移动宽带用户渗透率	11.9%
移动手机用户渗透率	177%

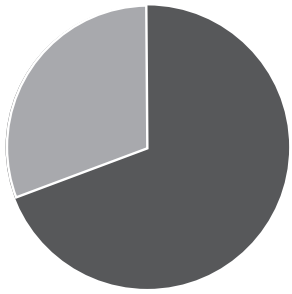
ICT 发展与网络联接指数排名

国际电信联盟（ITU） 通信技术发展指数排名（IDI）	45	世界经济论坛（WEF） 网络就绪指数（NRI）	33

来源：世界银行（2015）、ITU（2015）、NRI（2015）以及互联网协会。

概述

1993 年，互联网作为达兰市法赫德国王石油与矿业大学（KFUPM）的一个学术项目被首度引入沙特王国，在该校计算机科学和工程学院实现了首次连接。[1] 通过卫星，该网络连接直通美国马里兰州贝塞斯达市。当时沙特有限的互联网基础设施也由华盛顿协调中心（Washington Coordinating Center）管理。该中心同时还主管着沙特在美国的政府官网。[2] 由于国际宽带有限以及连接速度慢，当时法赫德国王石油与矿业大学的职工仅能使用电子邮件服务。整个 20 世纪 90 年代，沙特仅有学术、医疗、研究和政府等机构的少数特定员工能实现有限上网。这些机构基本都位于首都利雅得，使用法赫德国王专科医院和研究中心（KFSHRC）提供的 64kbps 互联网频道，并受沙特国家科技创新中心——阿卜杜拉国王科技城（KACST）的管理。法赫德国王专科医院和研究中心通过专有的卫星链路实现联网，阿卜杜拉国王科技城则通过微波链路连接到该中心。1994 年，阿卜杜拉国王科技城成为沙特国家网络域名 .sa 的主管部门，并负责全国范围内所有网络服务的协调。



沙特网络渗透率：69.6%

1999 年，沙特国内所有民众均可上网。

经过数年研究和审议，沙特部长理事会（Saudi Council of Ministries）于 1997 年授权阿卜杜拉国王科技城将互联网接入扩展至全国，同时委任沙特国有企业及唯一的电信服务提供商——沙特电信公司（STC）来建设国内必要信息基础设施，以促进国有互联网主干和其他互联网服务提供者（ISP）之间的相互连接。1998 年，互联网管理工作划归 KACST 下属的互联网服务机构（ISU）负责，可向 KACST 负责科研支持的副主席直接汇报。[3]1999 年，互联网服务机构正式向取得牌照的商业化互联网服务提供者开放其网络，尽管沙特电信公司（直到 2005 年）是当时唯一的互联网服务提供商。通过互联网服务机构，KACST 成为沙特国际和国

内之间唯一的互联网交换节点和网关。[4] 由此，互联网服务机构负责对国内的互联网服务监管、域名（.sa）运营以及制定互联网管理规章，包括入网控制，对“有害”“非法”“反伊斯兰”或“具有攻击性的”网络信息过滤等。作为其职责之一，互联网服务机构实施了一个（可过滤进出信息的）互联网内容控制系统，来使其在推进公众入网率的同时，保证网上的内容符合该国保守的价值观和伊斯兰教义。[5]

2003 年，沙特通信委员会（Saudi Communications Commission）更名为通信和信息技术委员会（CTIC），代替 KACST 接管互联网牌照发放、信息监控和过滤工作。此外，它还向私营部门提供互联网接入服务，以及负责解决私营电信公司之间的争端。[6] 互联网服务机构则继续为政府部门以及学术研究机构提供网络接入。如今沙特通过两大国家层面的数据服务提供商——综合电信公司（Integrated Telecom Company）和 Bayanat al-Oula 网络服务公司（Bayanat al-Oula for Network Services）实现网络连接。同国有企业一样，这些互联网服务提供商必须遵守相关条款（例如过滤内容等）。[7]

1999 年以来，互联网接入在沙特民众中变得普遍，沙特民众对（尤其是商业部门提供的）互联网服务需求不断增长，沙特互联网用户的数量也在迅速增长（从 1999 年的 10 万，增长至 2001 年的 100 万，再到 2016 年底的 1650 万）。2016 年，几乎所有的沙特大学院校都为本校职工和学生提供免费互联网接入。沙特的医院、银行和公司也都推出面向民众的网络服务。近年来，沙特政府越来越重视互联网，并将其视作经济增长和政府高效运行的驱动力，同时在教育和公共服务领域不断扩大网络接入。沙特政府同时还将其视作摆脱过度依赖石油、实现经济多元化的重要手段。

如今，沙特已实现 2100 万（接近其总人口的 70%）的网络接入。尽管阿联酋、卡塔尔和科威特等其他海湾国家有着更高的网络渗透率，但在面对互联网带来的新鲜事物上沙特民众接受度却更高，并在此方面为其他阿拉伯国家做出了表率。[8] 沙特民众是全球最活跃的社交媒体用户之一——沙特拥有阿拉伯地区最大的推特（Twitter）用户群。此外，其高手机持有率（177% 的市场渗透率）也在不断推动互联网在沙特的使用，使得手机宽带服务需求大幅增长。最后，使用翻墙软件（如 Hotspot Shield）以转接到某些政府禁掉的内容和服务的沙特民众数量正不断增加。

就资本存量和消费量来看，沙特是中东地区最大的信息通信技术（ICT）市场，正受到本地和国际公司的青睐。事实上，尽管 IT 产业目前对沙特 GPD 贡献率仅占 0.4%，且其 ICT 市场长期靠进口拉动——超过 80% 的 ICT 消费都流向了外国企业[9]，但是 IT 部门仍被视为其增长最快并能带来巨大发展机会的产业之一。2019 年，其网络安全市场将有望超过 34 亿美元。[10]

高度盈利的沙特电信公司目前已成为一家公开上市公司。由于依然是沙特最大的信息服务提供商和中东最大的网络运营商之一，它提供了沙特绝大部分的手机、固话、互联网和电视服务。[11] 然而在 21 世纪头十年的中后期，Mobily 和 Zain 等信息服务提供商纷纷进入市场，该公司在手机和互联网服务领域的垄断地位开始被打破。2008 年，沙特电信公司推出数字通信量更大、可靠性更高以及速度更快的 3G 技术服务。同年，Zain 公司也携 4G（LTE）通信服务进入沙特手机通信市场。

尽管沙特有着 70% 的互联网渗透率和快速增长的手机使用率，但其电子商务仍有待发展。至少有三大原因导致其在该领域的发展迟缓。首先，沙特国内创办新企业十分困难。其次，沙特 ICT 费用高昂（沙特在世界 ICT 可负担能力上的排名为 101[12]），其国内企业通常不愿将昂贵的 ICT 引入企业运营中。最后，石油经济仍然主导着沙特的经济，贡献了超过 90% 的政府税收，导致其企业大部分集中于石油开采、提炼、石油和液化天然气（LNG）分销等行业。

沙特政府认识到，如要进一步推进其经济发展，必须改变过度依赖石油的现状，实现经济多样化。因此，沙特王储穆罕默德·本·萨勒曼（Muhammad bin Salman）——当前沙特国王萨勒曼·本·阿卜杜勒 – 阿齐兹（Salman bin Abdulaziz Al–Saud）的王位继承人，已制定了改变沙特过度依赖石油的经济改革展望，意图打造一个“强大、繁荣的沙特，为所有行业提供发展机会”，从而不再受“大宗商品价格波动或外部市场变化左右”[13]。该展望内容之后被 2016 年公布的《沙特 2030 愿景》加以陈述，从而为沙特未来经济结构改进提出了包含具体目标的路线图。[14]

该雄心勃勃的经济发展战略将数字化发展列为其目标之一，但并未列入重点领域。尽管如此，该计划也承认，如要充分从 ICT 产业中实现经济利益，必须推动云计算等 ICT 技术的使用以及为民众提供各类面向互联网的服务。该计划提出要打造三大支柱：①将沙特定位于阿拉伯和伊斯兰世界的心脏；②将沙特的角色定位于全球投资的动力源；③将沙特的战略位置打造成连接亚、欧、非三大洲的全球枢纽。[15] 如同过去许多其他改变沙特依赖石油经济的措施一样，该计划试图在宗教保守主义和实现现代化两者之间保持平衡。该计划也带来一大矛盾：如何在有限制地使用现代技术和互联网的同时，又能大力推动沙特的经济增长。[16]

《沙特 2030 愿景》与 2020 年“国家转型计划（NTP）”中列出的重点发展行业相一致，均强调要通过促进医疗、教育、基础设施、娱乐和旅游业发展使经济多样化，来提升私营部门的地位。该愿景的其他目标还包括：推动外国直接投资；使私营部门成为就业市场的主要雇佣者，减少公共部门和官僚机构的比重；创造更多就业机会，

为劳动力市场培养相关技能；提供优良的医疗服务；扩大政府在装备和军火等军队制造业上的投入等。

沙特经济与发展事务委员会（Saudi Council of Economic and Development Affairs ）已被授权建立必要机制和措施来实施该愿景，协调各利益相关部门共同落实，以及监督其进展情况。该委员会已成立大量机构，如国家绩效评估中心（National Center for Performance Measurement）、执行机构（Delivery Unit）、项目管理办公室（Project Management Office）等，来对当前的各类提案以及未来的各大项目进行启动、管理、监督和评估。

尽管《沙特 2030 愿景》承诺将对投资者开放更多经济机会和推动国家快速转型，但这一宏大的经济计划依然没有触及政治或社会改革，也未谈及如何解决当前急需的外国技术工人问题。该愿景中也未明确沙特怎样实现可持续的国家收入，来支持新型服务导向型经济所需的基础设施建设。[17] 当前油价持续下跌导致沙特国家收入锐减，让愿景中提出的变革实施难以为继。

此外，沙特长期饱受复杂多变的地区安全挑战困扰。该安全问题导致了地区不稳定的增加。[18] 这些挑战包括沙特在也门和叙利亚代价不菲的军事行动、伊斯兰国和其他极端组织不断上升的暴力极端活动、与伊朗不断紧张的双边关系以及正在与卡塔尔持续的外交危机。沙特政府试图吸引外国直接投资和推动更多私营部门企业参与经济转型，该计划或将被不断增长的针对关键基础设施和私营企业的网络袭击所破坏。

2012 年 8 月，沙特国有油企沙特阿美石油公司就曾遭受过一场严重的破坏性网络袭击。当时沙蒙（Shamoon）病毒使该公司成千上万的硬盘驱动遭到感染，员工的邮件遭到停用，公司数据遭到破坏，以及四分之三的 IT 基础设施资产遭到破坏。[19] 沙特阿美公司花费了数周时间才使公司恢复正常运营。由于阿美公司贡献了沙特政府收入 80% 且是世界最大的石油生产商，供应了全球超过 10% 的石油和 25% 以上的液化天然气，该事件因而被视为一场针对沙特国家的直接袭击。袭击的恶意软件一度试图从业务系统侵入油气生产和分销网络。即使石油设施局部遭到破坏，也会对石油供应、石油价格甚至相应的全球经济造成直接影响。该事件提升了沙特政府对网络威胁的认识，令其重新关切起应对未来网络袭击的恢复能力。[20]

2012 年沙特阿美石油公司遇袭事件后，沙特政府开始投入大量资源提升自身网络安全能力，以及推进国内和国际措施来解决其网络安全问题。在国内，作为着重在民众、过程和技术方面建立国家网络安全、风险消

“国家信息安全战略”和《沙特 2030 愿景》都强调沙特提升整体国家安全和国家恢复能力的必要性，以“为沙特向知识导向型经济转变提供有效和安全的基础”。

减、恢复能力框架的初步尝试，沙特开始制定“国家信息安全战略（NISS）”。[21] 该文件指出了“当今互相连接的计算机网络（以及）经济和金融活动对 ICT 不断快速增长的依赖带来的复杂性”，试图提出“符合沙特国家信息和 ICT 目标的整体战略”，同时更好地支持沙特的长期国家经济愿景和战略计划。[22]“国家信息安全战略”和《沙特 2030 愿景》都强调沙特提升整体国家安全和国家恢复能力的必要性，以“为沙特向知识导向型经济转变提供有效和安全的基础”。

然而，“国家信息安全战略”将重点置于通过制定必要的政策、规章和培养技术工人来打造一个受中央政府管控的信息安全环境上，而忽略了其他国家网络安全方面建设和关键基础设施保护（CIP）。该战略称，网络安全和关键基础设施保护建设“不在其范围内”，但由于二者是“该战略的重要补充和沙特核心国家利益和资产全面保护的必要组成部分”，应为其制定发展战略。[23] 它同时还警告，如要有效实施该战略，沙特最高领导层需达成共识。同时该战略最大的挑战是，如何让所有政府机构一致同意建立一个集中的国家信息安全环境机构。

除了“国家信息安全战略”外，沙特大部分安全机构和部委也制定了自己的相关规章和措施，并建立了自己的基础设施系统，但均不受中央协调管理。沙特缺乏一个权责清晰且有能力负责整体国家网络安全的主管机构的现实进一步加剧了这些机构各自为营的做法。

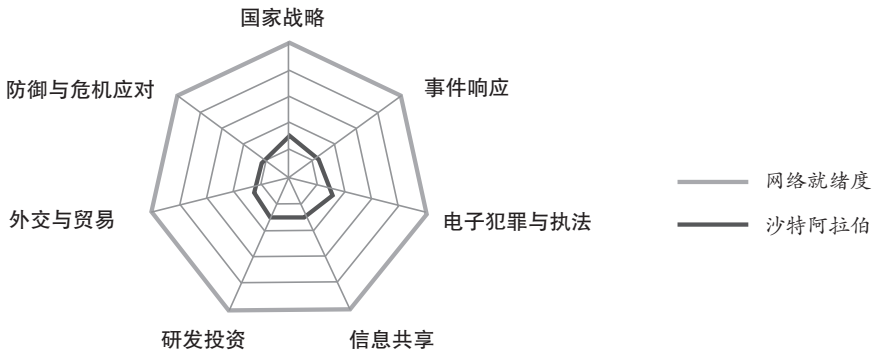
2017 年 7 月，沙特国王萨勒曼发布了一系列法令，成立国家安全部。该机构将兼并此前内政部（MoI）下属的一些部门。国家网络安全中心将成为沙特网络安全的权力中心。

2017 年 7 月，沙特国王萨勒曼发布了一系列法令，其中最突出的就是成立国家安全部（Presidency of State Security）——一个负责反恐和国内情报工作的全新国家安全机构。该机构将兼并此前内政部（MoI）下属的一些部门，如特殊紧急部队、技术事务、航空安全以及民事和军事人员，以及其他负责反恐和安全问题的处室等。根据这些法令，国家网络安全中心（NCSC）最早将于 2018 年 1 月从内政部划归国家安全部下属。届时国家网络安全中心将成为沙特网络安全的权力中心。最后，该法令还下令对内政部和皇家卫队精锐力量的高层作出职位变动，同时将新委任的国家安全部主管 Abdulaziz bin Mohammed al-Howairini 及其副手提升至部长级别。这些举措旨在将网络安全、反恐和国内情报等安全事务上的权力集中化，将其置于单一机构的主管之下，以能对沙特国王和王储的指示作出直接响应。[24]

如要全力支持这一新成立的机构，沙特需在接下来的几个月里组建其领导层和确

定初步行动。当前沙特在国家网络安全方面存在权责过于分散的问题，导致长期以来其网络安全战略规划的缺失。沙特必须解决这一问题，确保其将有限的资源投入到即时和长期网络威胁上，以改善其整体国家网络安全现状。[25] 要实现《沙特 2030 愿景》中提出的宏大目标以及加入全球互联网经济并从中获益，沙特需了解 ICT 创新带来的机会和风险，同时减少其对网上内容的过度筛查。

本报告采用网络就绪度指数 2.0（CRI 2.0）评估了沙特应对网络安全风险的准备度，并制定了一份行动蓝图，帮助沙特进一步了解其互联网基础设施之间的依赖性及脆弱性。基于对沙特当前网络安全形势的分析，本报告还探讨了沙特需要发展哪些能力，才能确保数字化顺利推进。本报告采用 CRI 2.0 方法论，从七大维度（国家战略、事件响应、电子犯罪与执法、信息共享、研发投资、外交与贸易、防护与危机应对）对沙特的网络安全工作及能力评估如下：



沙特网络就绪度评估（2017）

国家战略

2011 年，作为负责网络安全和政府服务数字化的政府机构之一，沙特通信与信息技术部（MCIT）制定了沙特首个“国家信息安全战略”。[26] 这一长达 90 页的文件经国际高级顾问和沙特国内专家的制定和多次完善，目前已是第七版。

沙特通信与信息技术部于 2011 年制定了首个“国家信息安全战略”。

沙特正面临不断增长的国家安全、经济福利和文化价值观等方面的威胁。这一现实凸显出制定国家网络安全战略的必要性。“国家信息安全战略”指出，“沙特国内外的网络相互连接导致其出现巨大的新型安全漏洞，并导致沙特经济文化活动受到新型威胁。一些情况下，这些新威胁甚至能导致关键 ICT 系统停止工作、被破坏或摧毁。”[27]

这些威胁还包括，敌对势力可能“操纵和利用 ICT 系统直接损害沙特国家利益”。[28]

该战略为沙特确立了清晰的发展愿景，并阐明其目标是通过吸收世界最佳实践成果和依靠本国高素质的专家和从业者，来为沙特提供安全坚实的数字化环境，主要包含 5 个方面：①建设安全可靠且恢复能力佳的信息基础设施；②训练一支专业化的网络安全工作队伍；③通过增加透明度和合作，来打造可提升相互信任和信心的信息安全环境；④通过对电子化政府服务和基础设施提供支持，来实现国家安全目标和 ICT 计划及战略；⑤通过研发及改善商业环境推动经济增长。此外，该战略还制定了 10 个含有并支持以上 5 大战略目标的一般目标，包括：①制订适当稳定的信息安全政策、指导方针和实践方案；②提高国家信息系统和 ICT 基础设施的安全性、可靠性、适用性和恢复能力；③改善人力资源条件；④建立信息安全威胁分析和缓解能力；⑤减少和预防正在增长的 ICT 漏洞；⑥实施信息安全合规和跟踪流程；⑦培养研发、创新和创业环境；⑧确保关键 ICT 基础设施和系统受到充分信息安全保护；⑨推动国内外合作和信息共享；⑩提高安全风险和个人责任意识。[29] 然而，尽管提出了 5 大宏观战略目标和 10 大一般目标，这一雄心勃勃的文件却并未给出清晰的实施方案或具体指南来实现以上目标。

该战略也承认其构想或将难以实现。例如，目前沙特国内还未有统一的网络安全政策和标准，各大政府机构和部委普遍都以自己的方式保障自身网络安全，而其各自建立的网络安全系统并没有多少共性。同样，网络安全风险和威胁评估标准存在缺失，导致政府机构无法持续针对各类威胁制定有效的战略和政策。同时，沙特也缺乏精密的综合性灾害恢复规划程序来整合网络安全行动。此外，该战略也未明确沙特的国家网络安全架构，未确认负责监管国家整体网络安全状况的主管部门。最后，要跨越沙特网络安全现状和该战略构想的前景之间的鸿沟，最大的挑战在于沙特缺乏数量充足、技术熟练和高素养的网络安全劳动力——根据通信和信息技术部部长 Abdullah Al-Swaha 的说法，沙特目前缺少超过 50,000 名 ICT 特殊技术工人。[30]

为解决以上问题，该战略提出了大量建议，包括 2020 年前成立一个集中管理的组织架构——国家信息安全环境机构（NISE），将沙特所有网络安全利益相关者纳入其中，“负责将国家信息安全战略的目标和倡议进行具体落实”；以及成立国家风险评估框架来支持建立一个高效安全的信息安全环境机构。[31] 但是国家信息安全环境机构具体如何构建，其具体权力范围以及现有的、合并后的或新成立的机构应承担其他哪些网络安全责任仍未明确。该战略指出，“沙特相关主管部门应做出决定，成立哪些机构及其附属机构，（以及）现有主管信息安全政府机构的具体角色”。[32]2017 年 7 月，国王萨勒曼发布了系列皇家法令，决定成立国家安全部——一个负责反恐和国内情报工

作和网络安全的全新国家安全机构。该部委将作为承担以上责任的唯一机构，直接向国王和王储报告。[33]“国家信息安全战略”是否还会修改以及其建议是否还会重新排序，目前还不清楚。尽管如此，沙特目前尚未发布任何网络安全战略或者政策。

2013 年，沙特发布了一条皇家法令，决定在内政部下成立国家电子安全中心（NCES）。该中心之后被重命名为国家网络安全中心。由于国家安全部或将负责制定下一版“国家信息安全战略”，2017 年皇家法令又将其级别提升并调整为国家安全部下属。此外，该法令同时还决定，国家网络安全中心最早将于 2018 年成为沙特国内负责网络安全的重心。目前，沙特网络安全事务尚处于通信与信息技术部、内政部以及其他政府部委和机构共同管理之下。届时国家网络安全中心将承担类似计算机应急响应小组（CERT）的功能，负责沙特政府和关键国家基础设施（CNI）运营商的信息及通信系统和网络的保护工作。[34]该中心不仅限于在首都利雅得工作，同时还承担大量任务，包括：制定国家信息基础设施和关键资产的标准、规章；识别风险和采集安全威胁情报；在国家层面协调网络事件响应和恢复工作；促进不同行业部门之间的信息和安全预警流动。例如，国家网络安全中心已建立包含分析和鉴别能力的信息保障和端对端的专业网络防御能力，以及与政府机构和大量关键国家基础设施运营商之间进行网络威胁情报分享。目前这些任务仍处于完善中，各自的运行效果也不一。

战略中提出的各项倡议所需的财政支持也未明确。沙特国家预算由财政部和其他各政府直属机构双方协商制定，并不受立法审查，因此也不向民众公开。各政府部门的支出皆有预算可用，但是均并未包含网络安全支出这一具体细项。

尽管沙特在网络安全意识和能力上正在不断取得进步，但其在国家层面应对网络风险的准备度上与发达国家相比仍存在不小差距。沙特已提出了一些网络安全相关的倡议并计划对网络安全创新科技进行大力投入，但仍缺乏一个整体网络安全战略、一套通用的网络安全政策和标准，以及一个长效的国家网络安全架构。今年接下来的几个月里，沙特国家安全部仍有机会通过制定国家网络安全框架和战略来为沙特网络就绪度开辟道路。

事件响应

2016 年，沙特经历了新一轮网络袭击，大量政府机构和私营企业受到影响。该事件再次显示沙特建立网络安全能力和恢复能力的紧迫性。这次袭击与 2012 年沙特阿美公司遭受的攻击事件类似，均利用了一种恶意软件进行入侵，从而导致关键基础设施遭到

2016 年，沙特成立其首个计算机应急响应小组，“作为受国家委托的信息安全权威参照物”。

大范围破坏而无法运行。[35]2017 年 2 月，在利雅得举行的第二届国际互联网安全大会年会上，沙特国家网络安全中心总负责人 Saleh Ibrahim Al-Motairi 表示，仅在 2016 年，沙特就遭受到近 1,000 次的持续网络安全袭击，袭击目标包括关键基础设施、窃取数据、干扰网络服务等。[36]

这类危及国家利益的网络事件由沙特计算机应急响应小组（CERT-SA）负责处理。该小组“作为受国家委托的信息安全权威参照物”，于 2006 年成立。[37]2007 年，在网络事件侦查、预防、意识提高、教育和培训等功能基础上，CERT-SA 开始提供事件处理咨询服务。总体来说，CERT-SA 提供的多种服务包括：①帮助各机构遏制和处理网络安全威胁，在必要时，对国家层面的网络事件作出响应；②通过在线资源、持续网络安全意识推广活动和研讨会提升民众网络安全意识；③提供教育和培训活动，如与各大院校合作，为政府机构和各大企业提供定制培训课程；④发布网络威胁预警、网络入侵警报和咨询意见；⑤协助网络安全利益相关者制定和实施自身安全程序和进程；⑥为特定网络安全相关问题提供反馈意见和相关信息。[38] 此外，CERT-SA 还负责对特定事件和响应行动进行信息收集、事后分析和发布报告。必要情况下，CERT-SA 还会对网络事件进行分析并制订预防和侦测方案，同时对其造成的破坏程度或损失作出计算。[39]

尽管 CERT-SA 提供事件响应支持和其他服务，但其并不是整个政府层面和社会层面负责网络事件响应的中央协调部门，也没有为潜在紧急事件和危机制订任何事件响应方案。CERT-SA 仍在很大程度上被视为一个事件反应机构，主要致力于在现有的网络威胁方面提供出版物发布、咨询和信息服务以及提供特殊事件响应支持。目前，它也未建立起能对全面网络袭击进行响应协调行动和发布及时行动信息的能力。2012 年沙特阿美公司遭袭事件令沙特重新重视起 CERT-SA 等国家计算机应急响应机构在降低网络事件对国家利益损害方面上的作用。此次袭击事件后，CERT-SA 加大了在发布监测和预防网络袭击相关信息方面的工作力度，但仍无法提供整体协调作用和建立机制，来与政府机构之间高效快速共享网络威胁情报和态势感知情况，以预防和降低网络威胁。

此外，沙特还计划在国家网络安全中心下成立一个正式网络威胁情报共享平台，来支持关键国家基础设施和政府机构的安全保障工作，以及提供其他主动和被动服务，例如：网络事件响应行动规划、监督和顾问服务；恶意软件分析；危害评估；以及网络事件修复等。[40] 但该平台仍未落实。

“国家信息安全战略”还要求建立“国家安全运营中心（SOC），负责收集和发布网络威胁和情报信息、分析网络袭击、减轻网络威胁建议行动、协调国家响应（及

作为）资源协助政策制定者了解 ICT 开发和如何最佳解决与减少（网络）风险”。[41] 然而，该战略未具体说明国家安全运营中心是代替 CERT–SA 和国家网络安全中心，还是支持或与其协作来共享即时或者紧急的网络威胁信息。该战略中仅提到，国家安全运营中心将下属于新成立的 NISE 来支持沙特国家层面的危机管理行动，以及“将利用现有的各个中心和能力来促进国家信息分享和协调网络事件危害减轻和响应行动”。[42] 新成立的国家安全部接下来需明确这些中心的各自角色和责任，以最大程度调用资源并提升其整体效率。

为了启动国家层面的网络风险评估以及建立长久的国家网络风险评估和管理程序，该战略提出，应在 NISE 之下成立一个专门的国家风险评估功能部门（NRAF），“以助于实施沙特国家风险进程管理系统（RPMS），来为其提供一个共同的风险管控框架”。[43] 目前，该程序和机构均尚未成立，沙特国内的各大实体均在使用不同标准来评估网络风险及其严重或紧急程度。“国家信息安全战略”指出，这一问题源自两方面。首先，在现有的评估方式下，高级风险管理“须能打破传统国家部委或机构的界限来对网络风险作出评估以及高水平的管控”，然而其“在当前和未来国家重点发展方向已确定、有限的资源和复杂的全球形势背景下，缺乏一个共同的风险评估架构来作出应对网络风险的适当决策”。[44] 其次，沙特各大部委倾向于在各自负责的领域单独行动，尚未认识其数字依赖程度和在网络安全方面需采取共同行动的紧迫性。为了解决该问题，NRAF 将组建一个“严格挑选、有过网络风险处理经历且受训已久的高级主管团队”，并且将“有权对沙特国内的各类国家综合信息基础设施的网络安全风险评估效果进行监督。”[45] 但到目前为止，该机构仍未成立。“国家信息安全战略”也指出，由于一些关键的网络安全利益相关者担心各自机构的缺陷会因此曝光而对该机构缺乏信任，如何让 N3i 高级管理系统在风险评估和管理功能上进行与这些机构有效协作将面临巨大挑战。

图 1 NISS 风险评估和管理环形图

由于缺乏网络威胁监控、分析的正式机制以及对网络安全产品的需求在不断上升，一些外国私营企业已经开始在沙特为政府和商业部门提供网络安全服务，其产品包括网络威胁监控和数据管理服务等。这吸引了大量 IT 和网络安全跨国公司进驻沙特市场，其中一些甚至还与当地 IT 和电信企业合办技术创新公司。例如，IBM 与沙特手机运营商 Mobily 就成立了一家合资公司，该合资公司在利雅得成立了一个跨国的“国家安全运营中心”。该中心使用 IBM 的网络安全服务基础设施协助进行网络安全日志和事件的收集、分析、关联和排序。2014 年，沙特教育部甚至还将该中心选为供应商，来通过实时分析、建立潜在网络威胁前期预警系统，以及保护教育部数据不受国外第三方获取等方式帮助其增强对自身网络安全态势的掌握。[46]

沙特通信与信息技术部也认识到定期进行国家级网络安全演习的必要性，以测试其网络响应、恢复和重建方案的有效性，但这些演习是否会持续进行下去尚不清楚。[47] 目前沙特公开报道的唯一一次网络安全演习是 2014 年代号为“阿卜杜拉之剑”的军事演习，内容包括电子战争演练等。[48]

尽管作出以上初步部署，沙特目前网络事件响应的方式很大程度上仍为被动反应。近来遭受的大量网络袭击事件已经使沙特再度有意抓紧落实提出的倡议，以对网络事件反应更为主动和更具恢复能力。

电子犯罪和执法

沙特是《关于打击信息技术犯罪的阿拉伯公约》（Arab Convention on Combating Information Technology Offenses，通常简称《阿拉伯公约》）的签约国。[49] 这一阿盟（League of Arab States）内部的国际法律框架于 2010 年生效，旨在促进阿拉伯国家之间在“抗击危害其国家安全、利益和联盟安全的信息技术犯罪”方面进行合作，以及使各签约国“在打击信息技术犯罪、保护阿拉伯社会安全上采取共同的刑事政策”。[50] 尽管沙特是《阿拉伯公约》18 个签约成员国之一，其也是目前唯一未正式批准该公约的成员国。此外，该公约在网络犯罪的定义和相关条款上十分模糊，因而尽管已被广泛接受，却仍未正式生效。事实上，其条款未参照任何阿拉伯国家的网络犯罪法规，18 个签约国之间的协调工作也仍毫无效力。[51]

沙特是《阿拉伯公约》18 个签约国之一，但目前仍未批准该条约。

此外，沙特既没有加入任何全球性打击网络犯罪协定，如欧洲委员会的《网络犯罪公约》（Convention on Cybercrime，通常也被称为《布达佩斯公约》）或上海合作组织的《保

障国际信息安全领域合作协定》（SCOAgreement on Cooperation in the Field on Ensuring International Information Security）等，也未参与其活动。

沙特参与了一些旨在促进打击网络犯罪方面进行合作的国际对话和战略伙伴关系。它已经建立了一些警方对警方、机构对机构等领域合作的双边关系和非正式渠道，并且正致力于进一步扩大在制定国际标准、全球 ICT 安全政策、打击网络犯罪倡议和研究等方面的国际合作。[52]

沙里亚法（Shari’a Law）是沙特国内刑事审判的官方法律基础。基于此，沙特已颁布两部主要的网络相关法律——《电子交易法》（Electronic Transaction Act）和《打击网络犯罪法》（Anti-Cyber Crime Law）。这两部法律适用于打击网络犯罪和保障网络安全，同时初步对电子商务和其他面向互联网的服务进行支持和管理。

2007 年颁布的《电子交易法》主要用于管理电子商务，建立起沙特国内电子交易和数字签名的法律体制。[53] 这一法令促进了沙特国内外公共和私营部门在商务、医疗、教育、电子政府和支付系统等应用领域的电子交易。该法旨在保护数字记录、限制和预防潜在数字滥用、造假和盗用。它承认网上和线下交易同等有效，以及电子签名和手写签名具备同等法律效力。

根据此法成立的沙特通信和信息技术委员会负责该法的具体落实，包括向认证服务提供商（ASP）颁发证照；核查认证服务提供商的合规性；确保服务的延续性以及暂停或撤销证照等。沙特内政部和通信信息技术部共同负责为其颁布一般性政策和为电子贸易和签名制订发展方案和流程。内政部成立国家信息中心（NIC），通过其在沙特全国用各个相互连接的分支组成的网络，来提供信息交换和储存服务，为各地区提供运营服务和支持各地朝圣（例如麦加朝圣）活动。此外，该法授权成立了沙特国家数字证书中心（NCDC），为公开密钥基础建设（PKI）管理提供综合系统，来确保互联网用户电子贸易安全进行。通过与财政部合作，国家数字证书中心成立了沙特电子数据互换（Saudi EDI）项目来提升电子商务贸易的速度和透明度。[54] 尽管该法案最初目的是为电子商务（电子进出口贸易）改善交易环境，但目前其重点仍落在政府贸易层面，且已十多年未更新。沙特目前也正面临不断增长的国内压力，要求其顺应最新经济、技术环境和国际标准作出改变。[55]

2007 年，沙特通过了《打击网络犯罪法》（ACCL）。该法主要有四大目标：①保障数据安全；②增加 IT 产业就业；③保护网络知识产权；④保护民众利益和社会公德不受侵犯。[56] 尽管该法旨在保护用户免遭网络犯罪侵害，但同时也包含有限制言论自由的条款。例如，该法将“制造损害公共秩序、宗教价值观、社会公德和个人尊

严的物品，或用信息网络制作、散播或存储该物品”定为犯罪行为。同时该法根据违法和犯罪严重程度对以上行为处以最高达 10 年的监禁和 500 万里亚尔（约合 130 万美元）的刑罚。如果该犯罪行为是犯罪团伙有组织的行为、罪犯是公职人员、犯罪行为造成重大公共影响、案情涉及儿童或重犯行为，还会有相应的附加刑。[57]

尽管《打击网络犯罪法》为处罚窃取敏感数据和网络干扰等犯罪行为提供了法律框架，但由于其未提供沙特国内或与国际伙伴之间怎样进行犯罪预防、侦测或合作措施，沙特起诉跨部门或跨境犯罪时显得尤为困难。2012 年沙特遭受的网络袭击案件中，由于袭击者据信是伊朗政府的一个代理服务器，该法对此几乎无能为力。此外，由于沙特尚缺乏一支训练有素的法官、公诉人、律师以及执法队伍，其在应对网络犯罪的各方面新特点以及如何有效调查和起诉犯罪分子方面仍捉襟见肘。

《打击网络犯罪法》已受到广泛批评。许多法律专家和人权活动家认为该法过度使用破坏“社会公德”条款来对社会活动者、博客异见者，以及有着政治或宗教诉求的沙特民众进行罚款、逮捕和提起诉讼，而并未真正用于处罚网络犯罪行为和保护数据资产上。例如，2015 年，一名 32 岁的沙特妇女因使用 WhatsApp 聊天软件诋毁他人而被处以两个月监禁和 5000 多美元的罚款。2016 年，一名医生因在 Twitter 上诋毁沙特卫生部，被处以 6 个月监禁，另一名药剂师则因同样的罪名被判处 4 个月监禁。[58] 2016 年，该法甚至修改相关条款，给予执法人员更大权限，使其在涉及宗教价值观和社会公德方面案件最终判决已定的情况下，仍能公开传唤犯罪嫌疑人。这一修改将该法的重点和执法资源从打击网络犯罪方面撤走，或将最终影响到沙特吸引外国直接投资和石油主导的经济多样化的成效。[59]

沙特的互联网使用受到通信和信息技术委员会的长期监控，且被其严格过滤被视为“有害”“非法”“反伊斯兰”或“有攻击性”的网络内容和社交媒体状态，以及被长期封锁“色情”、“赌博”“毒品”“极端思想”以及人权或政治活动机构等相关页面。[60] 沙特公开承认其对不符合《沙里亚法》的违反其道德观和敏感的宗教信息进行了审查。近年来，沙特的执法机构甚至还通过解开或绕过加密屏障，以保护国家安全和维持社会秩序的名义，将其审查范围扩大至网页、博客、聊天室、社交网站、电子邮件和手机信息等平台的政治、社会和宗教内容。[61]

沙特文化信息部还要求该国的博客、论坛、聊天室等热门网站运营前须从该部获得牌照，同时通信和信息技术委员会也要求手机网络运营商登记用户的真实姓名、身份证号码，现在甚至还需指纹，来“限制通信使用带来的负面影响和犯罪行为”。[62] 2014 年沙特通过《反恐法》，将恐怖主义行为模糊地定义为“诋毁国家名誉”“损

害公共秩序”“破坏国家安全”等，导致沙特的网络用户在网上发布、分享和点赞时不得不万分谨慎。[63]《反恐法》有效地将所有质疑伊斯兰宗教教旨、支持任何类型“被禁停的组织”或政治改革的网上内容都定位为犯罪性质。[64]

除了上述法规和《治国基本法》中规定的一般性隐私权外，沙特鲜有涉及个人隐私和个人数据保护的相关法规。例如，沙特尚无国家数据保护主管部门。此外，政府或企业收集或处理用户数据时，无需正式通知或登记要求。由于缺乏数据管理程序或规章，沙特国内对数据转移和数据常驻要求经常模棱两可。同时，沙特目前尚无对“个人数据”的明确定义，也未规定向个人或集体用户告知哪一数据安全机构对此负责。[65]

最后，上述战略未提及沙特会划拨多少人力或财政资源用以支持保护社会不受网络犯罪破坏、减少国内的网络犯罪行为或推动建立协调机制来处理国内和国际网络犯罪所需的进一步法律和政策倡议。该战略也并未明确沙特将计划如何提升网络执法能力。由于国内互联网已经越来越普遍以及更为便捷的网络连接不断涌现，同时伴随而来的还有愈加常见的病毒感染和漏洞利用，沙特需提升其执法机构的执法能力，投入更多资源来对不断增长的网络犯罪作出有效回应以及减少网络基础设施的不足之处。

信息共享

沙特目前尚未制定国家信息共享政策，但“国家信息安全战略”中强调了国内外信息共享和合作的重要性，并承诺沙特将扩大在新兴网络威胁、漏洞以及相应减轻威胁的技术方面的信息交流。

沙特目前尚未制定国家信息共享政策，但“国家信息安全战略”强调了国内外信息共享和合作的重要性。

沙特国家网络安全中心目前与政府机构、关键国家基础设施运营机构以及其他利益相关者共享网络威胁情报，但该信息共享能力仍有待提高。沙特已经计划建立更加强大的信息共享机制，包括在国家网络安全中心之下成立网络威胁情报共享平台，以进一步对保障关键国家基础设施和政府机构的网络安全提供支持。其重要且必要的组成部分之一就是对关键国家基础设施或全球其他地区发现的网络威胁和恶意网络活动提供预警。例如，2017 年 5 月和 6 月，利用微软系统软件漏洞的网络安全事件爆发，全球信息共享和对抗网络威胁的响应行动由此打响。只要任何一个国家或行业遭到袭击，其他国家或行业就可迅速吸取其教训，切断其网络基础设施中有漏洞的部分，并互相交流该为其软件打哪种补丁，最终使其网络基础设施和企业免遭破坏。[66]“国家信息安全战略”强调，“这其实是很简单的算法。只要（国内和国际）信息合作、协

作和共享增加了，信息丢失和 ICT 系统漏洞被利用的风险就相应减少。”[67]

尽管如此，沙特缺乏国内信息共享的传统，更不用说与国际机构进行合作。沙特政府各部委之间极力维护己方官僚机构和权限，往往互相敌视和喜欢互较高下。这一状况与当前网络技术日新月异一起，使得“国家信息安全战略”在网络安全信息共享方面难以有效推进。沙特在国际层面的信息共享上显得十分不情愿；同时，其在中东地区与其他国家的经济利益、军事紧张状态以及在政治利益上的争夺使得其跨境信息自由流动受阻。沙特、阿联酋、巴林、科威特、卡塔尔和阿曼等国建立的海湾阿拉伯国家合作委员会（GCC）或许能为其探索怎样增进互信和推进信息共享提供平台。[68]

沙特同时还是伊斯兰会议组织计算机应急响应小组（OIC–CERT）的成员。该组织包含埃及、伊朗、土耳其、尼日利亚等 18 个成员国，囊括了各成员国的计算机应急响应小组，旨在促进伊斯兰国家的信息共享。OIC–CERT 为成员国组织培训、研讨会和演习等活动，试图为其提供网络威胁和危机处理的即时经验，例如及时且实用的信息共享活动等。[69]

“国家信息安全战略”承认，沙特在信息共享领域确实还需大力改进。当前沙特国家网络安全中心和新成立的国家安全部仍有大好机会促进和扩大政府内部之间以及其与外界之间可执行信息的交流。沙特各大部委、关键国家基础设施运营商、企业和国家合作伙伴目前都急需信息共享来改善自身安全状况。目前，沙特政府和关键行业仅有的信息共享机制仍由 CERT–SA 和国家网络安全中心提供。接下来的数月，沙特将考虑建立国家安全运营中心以及打造国家网络安全中心的新角色，届时沙特国内进行及时可行的信息共享或将成为现实。

研发投资

“国家信息安全战略”中明确提出，沙特将建立“一个长久繁荣、鼓励研发和创业的信息安全经济部门”，同时还承认沙特有必要“通过国际合作扩大研发”，以帮助沙特在 ICT 和网络安全部门开发更多功能。[70] 该战略尤其强调“通过激励和引导沙特国内有着高度商业化和信息安全技术突破潜质的信息安全研发项目，如加密互操作性、供应链整合、计算机安全和快速高效访问控制等，来满足未来沙特信息安全需求”的必要性。[71]

沙特指出，其必须在 ICT 和网络安全部门开发更多功能，并将其作为国家信息安全战略的“关键支柱”。

该战略指出，沙特政府最初设立了一些项目用于提升现有的网络能力，包括为研究

人员和创新人员将成功的想法和研究转化成专利和商业化产品提供支持等，但并未明确政府将如何对这些活动进行支持、推进和维系。相反，该战略提出要通过吸收其他国家网络安全团体、政府机构和行业的成果，来制定“科研技术路线图”指导沙特全国。

此外，该战略要求构建“集中的资助咨询能力”，确保研发工作与沙特的战略目标相符。为此，该战略提出建立“研发功能机构（Research and Innovation Function）”来监督对特定网络安全项目的拨款和资助。该机构将归 KACST 主管，并与沙特通信与信息技术部进行协调。[72]

该战略将人力资源视为其“关键支柱”，并提出多条计划“提升沙特信息安全从业者、研究人员、创新人员和企业家的信息安全能力”，同时将推进其网络安全培训和提高其网络安全意识。[73] 例如，沙特已设立一些项目用于鉴别哪些妇女能胜任 IT 和网络安全工作，哪些能在经过进一步培训后迅速满足沙特的即时信息安全需求。该战略还提出，将“雇佣经审查后无正式证书但熟练掌握计算机技能的失业青年”。[74]

作为对这一需求的回应，沙特通信与信息技术部另启动了一些人才培养项目，以及与全球的 IT 企业建立合作伙伴关系，在 2017 至 2020 年间为超过 56000 名沙特青年提供关键 ICT 技能培训。同时其还与沙特阿美公司合作成立国家信息技术学院（National Information Technology Academy），来为沙特培养相关人才。[75] 此外，该战略还设立了一个设在小学的项目，鼓励儿童从小接触计算机、培养分析能力、掌握网络安全技能，并为每两名学生配备一名导师来指导他们直至就业。[76] 这些青年将有望在维护沙特未来国家安全中发挥重要作用。

尽管沙特政府尚未建立任何正式项目或者激励措施来鼓励高校和学术机构在基础和应用网络安全方面进行研究，但其却为所有公立大学提供了政策支持和资助。许多大学现已就 ICT 和信息安全开设了课程和设立了学位项目，例如达兰市法赫德国王石油与矿业大学设立的安全与信息保障理科硕士学位项目。此外，法赫德国王石油与矿业大学在利雅得设立的通信与信息技术研究院（CITRI）参与了一些研发项目，项目范围包括数字模拟集成电路芯片设计、综合电子系统、通信和无线安全、机器人技术与智能系统、雷达防御系统、电子战高级技术、激光和光纤应用科研以及其他遵循了最新国际规格和标准的技术。通信与信息技术研究院在推动法赫德国王石油与矿业大学成为沙特预防网络犯罪和数字犯罪法务研究的国家中心方面发挥了主要作用。该研究院为沙特政府机构、高校和企业提供了专业技能支持、咨询服务和多种主题的研究项目来满足其研究和技术需求，从而实现国家规划中提出的科技创新目标。[77] 最后，CERT-SA 也提供技术培训、组织网络安全意识提升活动，以及与高校、政府机构和

企业合作开发客户培训课程和研讨会、安全质量管理功能机构。

就资本存量和消费而言，沙特是中东地区最大的 ICT 市场。据估计，仅 2016 年，沙特就已投入 140 亿美元到网络安全等 ICT 部门。

就资本存量和消费而言，沙特是中东地区最大的 ICT 市场。据估计，仅 2016 年，沙特就已投入 140 亿美元到网络安全等 ICT 部门。沙特具备高速率的宽带连接和为对抗潜在破坏性网络威胁的网络恢复能力，它对建立本地和国际物联网（IoT）兴趣渐浓。构建利益相关者之间的互信以及提高网络市场参与者在网络安全方面的信心，已成为互联网数据中心首席信息官峰会（IDC CIO Summit）等研讨会和会议的主题。其中近期举行的首席信息官峰会将政府官员、沙特商务官员以及世界各国专家齐聚一堂，来探讨连接和依赖于互联网的基础设施的网络安全威胁解决方案等方面的 ICT 发展趋势。[78]

沙特 2016 年 140 亿美元的 ICT 投入中，相当大一部分被分配到提升电信基础设施（尤其是高速宽带）方面。目前，沙特国家收入在很大程度由通信行业拉动，据估计其 20% 来自于新增的网络连接，并且该领域的国家收入还有望在明年稳步上升。这就要求沙特加大基础设施投入，其中就包括安全领域的产品供应，但沙特目前仍未将网络安全或恢复能力视为重点投入领域。沙特最大的互联网服务提供商和中东最大的互联网运营商之一——沙特电信公司及其竞争者 Mobily 和 Zain 目前正在互联网连接方面加大投入。然而，它们都将焦点主要放在怎样提供更多访问上，而冷落数据安全的步骤和程序。此外，这些公司之间目前几无合作。[79]

私营行业以及私营—公共部门合作成立的公司也开始合作建立创新中心，来研发和展示应对地区或本地经济挑战的技术创新，以及推动各个部门的经济增长。例如，沙特基础行业公司（SABIC）是利雅得技术谷（Riyadh’s Techno Valley）创新中心的主要投资者。这一地区的创新中心或者创新家园（Home of Innovation）致力于石油化工和天然气行业技术创新，旨在落实《沙特 2030 愿景》中提出推动本地下游产业增长、提高企业效率以及构建多样可持续经济等经济战略目标。但上述倡议并未将网络安全作为单独的重点领域加以特别关注。[80]

2012 年沙特阿美公司遭袭后，沙特政府开始扩大其在网络安全技术解决方案和服务（尤其是监察技术、电子侦测设备、网络攻击侦查系统和预防技术以及生物统计学等方面）上的投入。这些领域将物理空间安全和基础设施以及内部网络安全战略相结合。沙特政府近年来也正对来自美国等国际合作伙伴的合作与资助产生浓厚兴趣。[81] 目前，沙特国有的国防企业——沙特军事工业公司（Saudi Arabia Military

Industries）与美国国防承包商雷神公司（Raytheon）建立伙伴关系，在网络安全等国防相关的项目和技术研发上进行合作。作为其协议的一部分，沙特政府将能从该合作中为其国防系统和平台获得更多网络安全解决方案。同时，雷神公司将在利雅得成立一个新公司（Raytheon Arabia）负责项目实施，从而为沙特构建本土国防、航天和安全能力。[82] 该伙伴关系因此将有助于帮助沙特实现《沙特 2030 愿景》中发展沙特本土有着专业能力和能拉动就业的国防生态系统的目标。这将为沙特在此部门的经济发展奠定长远基础。[83]

外交与贸易

沙特并未将网络安全视为其外交政策的首要议题之一，也并未将其列入外交部工作的重点领域。但沙特尤其在面对与伊朗关系紧张且受到源自伊朗境内的网络攻击后，在海湾国家合作委员会内正扮演着更为自信的角色。特别是，沙特正与海合会举行大量会谈，试图扩大双方在网络安全方面的合作以及就和平时期的网络规范达成一致认可。[84] 同时作为 2015 年海合会《戴维营协议》（Camp David Accords）缔约国，它还计划与海合会合作成立工作组。根据该协议，海合会成员国一致同意每年举办两次会议来促进其在反恐上的合作，以及简化关键防御能力、导弹防御能力、军事准备程度和网络安全领域的转移。[85]

沙特在海湾国家合作委员会内的网络安全议题上正扮演着更为自信的角色，但仍未将网络安全视为其外交部外交政策的首要议题之一。

此外，沙特还大量参与同美国、印度等国的双边高级对话，试图推进双方在打击资金支持恐怖主义、洗钱、恐怖主义分子和犯罪集团利用网络从事犯罪活动等方面的信息交流。

沙特同时还通过国家网络安全中心推动地区网络安全合作和建立网络安全意识。作为该努力的一部分，沙特定期举办网络安全论坛年度会议等网络安全相关活动，将阿拉伯国家以及其他国家的政府官员和行业专家聚在一起，探讨如何改善网络安全状况、提升网络威胁情报收集能力以及有效落实《沙特 2030 愿景》中提出的目标。[86] 沙特还举办了由政府背书的年度国际网络安全大会，其参会人员不仅包括世界各国的网络安全专家，沙特甚至派出了内政部的最高级别官员与会。[87]

《沙特 2030 愿景》中强调，要将沙特的战略位置打造成连接亚、欧、非三大洲的全球枢纽。沙特国土安全部应利用其最新被赋予的权力和责任，为货物、服务、数据和资金的跨境自由流动制定愿景。该部应利用沙特的 G20 成员国身份和影响力，推动可信的数字经济交易。网络外交并不仅仅是制定接触和限制行为的规则，还应通

过信息自由流动来推动贸易。沙特如要同时实现经济增长和国家安全两个目标，需打造一支经验丰富的外交队伍以及为保证将带领地区实现其《2030 愿景》中的目标。

防御与危机应对

鉴于其经济、政治和文化以及战略位置在本地区的重要地位，沙特在维护地区安全稳定中扮演着关键的角色。中东地区目前正面临着复杂多变的安全挑战，尤其是沙特与伊朗之间的紧张关系还在不断加剧。因此新一任沙特王储表示，沙特“将不会坐待战争降临沙特境内，而要将其留在伊朗”。[88] 此外，鉴于近年来沙特频繁遭受来自伊朗境内的网络攻击，沙特网络安全和网络防御能力建设已显得越来越紧迫。

由于近年来遭受的破坏性网络袭击不断上升，沙特网络防御能力建设已显得越来越紧迫。

目前沙特政府已授权国防和航空部、内政部等多个部委整合国家网络防御体系。这些部委以及其他政府机构正加大在网络技术上的投入，提升其网络能力。尤其在 2017 年，沙特通过与美国签订《安全合作协定》（Security Cooperation Agreement）来加大双方合作力度，试图以此来改进其特种作战和反恐部队的训练效果，整合其防空和导弹防御系统，提升网络防御能力以及强化海上安全保障能力。[89]

此外，沙特也在试图用网络能力来武装国民卫队（National Guard）等防御力量。例如，沙特国民卫队正投入近 5 亿美元资金用于发展电子作战能力。

目前尚不明确沙特是否制定政策或颁布法令来成立军事或情报服务领域的网络安全部队。沙特财政预算的不作为，导致发展以上机构网络能力的财政资助级别难以确定。同时，沙特国防和航空部是否进行政府内或军事特别演习来展示其国家网络防御准备程度，也尚未明确。尽管如此，沙特最起码还算是 OIC-CERT 内的活跃成员。它曾承诺将组织联合网络作战演习，但其是否真会付诸实践目前尚不得而知。[90]

CRI 2.0 概要

CRI 2.0 评估结果显示，沙特在网络就绪上虽取得巨大进步，但在 CRI 七大评估要素方面均仍不足。

分析结果反映了沙特当前不断变化的格局。沙特持续制定并刷新其经济（数字）议程、国家网络安全战略、政策及各项举措，寻求国家经济愿景与安全重点工作之间的平衡。国家概况的变化反映出国家在各个方面发生的变化，有利于监测、跟踪并评估沙特社会所取得的显著进步。

CRI 2.0 利用全面、可比较、基于经验制定的方法论，帮助国家领导人在网络化、竞争激烈、冲突丛生的世界中做出规划，打造安全、有活力的数字世界。

如需了解更多 CRI 2.0 的相关信息，请参阅：http://www.potomacinstitute.org/academic-centers/cyber-readiness-index。

★ 图片源自沙特通信和信息技术部制订的《沙特国家信息安全战略》草案，
http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SaudiArabia_NISS_Draft_7_

注释

1. Khalid M. Al-Tawil, "The Internet in Saudi Arabia," Telecommunications Policy, vol. 25, issue 8-9, September 2001, 625-632.

2. "The Internet in the Kingdom of Saudi Arabia," The Global Diffusion of the Internet Project, February 1999, http://mosaic.unomaha.edu/SaudiArabia_1999.pdf .

3. The Mosaic Group, "The Global Diffusion of the Internet Project - The Internet in the Kingdom of Saudi Arabia," (February 1999): 2, http://mosaic.unomaha.edu/SaudiArabia_1999.pdf.

4. Hamed A. Alshahrani, "A Brief History of the Internet in Saudi Arabia," Tech Trends 60, no. 1, 2016, https://link.springer.com/article/10.1007/s11528-015-0012-5.

5. Mahdi Abu-Fatim, "Official on Introduction of Internet Into Kingdom," Al-Riyadh, December 6, 1997: 27, as reported in FBIS-NES-97-348, Daily Report: Near East & South Asia, December 16, 1997, via World News Connection.

6. Communication and Information Technology Commission, http://www.citc.gov.sa/.

7. Freedom House, "Freedom on the Net 2016 - Saudi Arabia Country Profile,"(2016), http://freedomhouse.org/report/freedom-net/2016/saudi-arabia.

8. World Bank, "Internet Users (per 100 people)," 2015, http://data.worldbank.org/indicator/IT.NET.USER.P2.

9. Eng. Abdullah Al-Swaha, "ICT Infrastructure Targeted in 1,000 Cyberattacks in 2016," The Business Year, https://www.thebusinessyear.com/saudi-arabia-2017/eng-abdullah-al-swaha-minister-communications-information-technology/vip-interview.

10. For more, see: "Saudi Arabia - Telecoms, Mobile and Broadband Statistics and Analyses," Paul Budde Communication Pty Ltd, https://www.budde.com.au/Research/Saudi-Arabia-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses.

11. Saudi Telecom Company, "Consolidated Financial Statements for the Year ended December 31, 2016," 2017, http://www.stc.com.sa/wps/wcm/connect/english/stc/resources/0/7/07a92210-58ff-4466-9a23-f4fc4f14e559/STC+2016+Annual+Consolidated+FS+-

English.pdf.

12.World Economic Forum, "Saudi Arabia," Networked Readiness Index, 2016, http://reports.weforum.org/global-information-technology-report-2016/economies/#economy=SAU.

13.“Saudi Arabia Vision 2030,” http://vision2030.gov.sa/en.

14.Ibid.

15.“Full Text of Saudi Arabia’s Vision 2030,” Saudi Gazette, April 26, 2016, http://saudigazette.com.sa/saudi-arabia/full-text-saudi-arabias-vision-2030/.

16.Khalid M. Al-Tawil, “The Internet in Saudi Arabia,” 625.

17.Hilal Khashan, “Saudi Arabia’s Flawed “Vision 2030”,” The Middle East Quarterly, vol. 24, no.1 (Winter 2017), http://www.meforum.org/6397/saudi-arabia-flawed-vision-2030.

18.U.S. Department of State, “Fact Sheet: U.S. Security Cooperation With Saudi Arabia,” January 20, 2017, https://www.state.gov/t/pm/rls/fs/2017/266861.htm.

19.Melissa Hathaway et al., “Cyber Readiness Index 2.0 - A Plan for Cyber Readiness: A Baseline and An Index,” Potomac Institute for Policy Studies, November 2015, http://www.potomacinstitute.org/images/CRIndex2.0.pdf.

20.Leon Panetta, speech given to Business Executives for National Security, New York, October 12, 2012, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

21.Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia - NISS, Draft 7," 2013, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategy-of-saudi-arabia/at_download/file.

22.Ibid, 2.

23.Ibid, 2.

24.“Saudi Arabia forms new apparatus of state security,” Arab News, July 21, 2017, http://www.arabnews.com/node/1132466/saudi-arabia.

25.Azhar Unwala, "Cyber security in Saudi Arabia Calls for Clear Strategies," July 27, 2016, http://globalriskinsights.com/2016/07/cyber security-saudi-arabia-calls-clear-strategies/.

26.Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia - NISS, Draft 7," 2013.

27.Ibid, 1.

28.Ibid, 1.

29.Ibid, 2-3.

30.Ibid, 10, and Eng. Abdullah Al-Swaha, “ICT Infrastructure Targeted in 1,000 Cyberattacks in 2016,” The Business Year.

31.Ibid, 2.

32.Ibid, 20.

33.“Saudi Arabia forms new apparatus of state security,” Arab News, July 21, 2017, http://www.arabnews.com/node/1132466/saudi-arabia.

34.National Cyber Security Center, “About Us,” https://www.moi.gov.sa/wps/portal/NCSC 国家网络安全中心/.

35.Raphael Satter, “Cyberattacks against Saudi Arabia continue,” Associated Press, April 26, 2017, and Agence France Press, “Saudi computer systems vulnerable to ‘Shamoon 2’ virus: telco chief,” Arab News, January 26, 2017, www.arabnews.com/node/1044566/saudi-arabia.

36.Aisha Fareed, "Saudi facilities sustained nearly 1,000 cyber attacks in 2016," Arab News, March 1, 2017, http://www.arabnews.com/node/1061151/saudi-arabia.

37.Suliman Al Samhan, “Saudi Arabia Computer Emergency Response Team,” Communications and Information Technology Commission, https://www.itu.int/ITU-D/cyb/events/2008/doha/docs/alsamhan-national-strategy-CERT-SA-doha-feb-08.pdf.

38.Computer Emergency Response Team - Saudi Arabia, "CERT-SA Services," http://www.cert.gov.sa/index.php?option=com_content&task=view&id=186&Itemid=131.

39.Ibid.

40.National Cyber Security Center, “Services,” https://www.moi.gov.sa/wps/portal/NCSC 国家网络安全中心/.

41.Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia - NISS, Draft 7," 13, 43.

42.Ibid, 13.

43.Ibid, 13.

44.Ibid, 33-34.

45.Ibid, 35.

46.“Enhancing Saudi Arabia’s cybersecurity readiness,” Oxford Business Group, 2015, http://www.oxfordbusinessgroup.com/analysis/front-lines-enhancing-kingdom’s-cybersecurity-readiness.

47.MCIT, 44.

48.“What Message is Saudi Arabia sending with war games?” Al-Monitor, 2014, http://www.al-monitor.com/pulse/originals/2014/04/saudi-military-maneuvers-sign.html#.

49.“Arab Convention on Combating Information Technology Offenses,” 2010, http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences.

50.Ibid.

51.Joyce Hakmeh, “Cybercrime and the Digital Economy in the GCC Countries,” Chatham House, June 2017.

52.Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia – NISS, Draft 7," 5.

53.Kingdom of Saudi Arabia, "Electronic Transactions Law," March 26, 2007, http://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_003_%20E_E-Transactions%20Act.pdf.

54.Ira Piltz, "Internet Law – Saudi Arabia's Electronic Transaction Act," Internet Business Law Services,http://www.ibls.com/internet_law_news_portal_view.aspx?s=articles&id=BDFDC5CD-61A1-40AF-99E7-45CD5E03C62B .

55.Ministry of Communications and Information Technology, 2013.

56.Ministry of Communications and Information Technology, "Anti-Cyber Crime Law," 2016, http://www.mcit.gov.sa/En/AboutMcit/Regulations/Pages/CriminalLaws.aspx.

57.Bureau of Experts at the Council of Ministers, "Anti-Cyber Crime Law," MCIT, 2009, http://www.mcit.gov.sa/Ar/MediaCenter/Download/Anti_Cyber_Crime_Law_En.pdf.

58."Imprisonment and lashing for two employees for criticizing the health department in Najran," [in Arabic] Makkah Newspaper, January 10, 2016, http://makkahnewspaper.com/article/128594/Makkah/السجن-والجلد-لموظفين-انتقدا-صحة-نجران-على-تويتر .

59.Dino Wilkinson, "Saudi Arabia Updates Cybercrime Law to Include 'Naming and Shaming' Penalty," Data Protection Report, June 8, 2015, http://www.dataprotectionreport.com/2015/06/saudi-arabia-updates-cybercrime-law-to-include-naming-and-shaming-penalty/.

60.Freedom House, "Freedom on the Net 2016 – Saudi Arabia Country Profile," (2016).

61.Ibid.

62."Communication Commission mandates companies to register fingerprints before issuing cards," [in Arabic] Al-Riyadh Newspaper, January 22, 2015, http://www.alriyadh.com/1121516.

63.Human Rights Watch, "Saudi Arabia: New Terrorism Regulations Assault Rights," March 20, 2014, https://www.hrw.org/news/2014/03/20/saudi-arabia-new-terrorism-regulations-assault-rights.

64.Ibid.

65.Eyad Reda and Turki Alsheikh, "Data protection in Saudi Arabia," Thomson Reuters, October 1, 2012, https://uk.practicallaw.thomsonreuters.com/4-520-9455?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.

66.Melissa Hathaway, "Cybersecurity: The Intersection of Law, Policy and Technology," remarks given at the American Bar Association meeting, June 1, 2017.

67.Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia – NISS, Draft 7," 14.

68.Fariborz Ghadar and Heather Spindler, "IT: Ubiquitous Force," Industrial Management, 2005, 14-20, http://www.ghadar.byethost13.com/Images/IT-Ubiq_force.pdf?i=1.

69.Rahayu Azlina Ahmad and Mohd Shamir Hashim, "The Organisation of Islamic Conference - Computer Emergency Response Team (OIC-CERT)," Cyber security Summit (WCS), 2011 Second Worldwide, 1-5, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5978783.

70.Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia - NISS, Draft 7," 2 and 61.

71.Ibid, 3.

72.Ibid, 61.

73.Ibid, 3.

74.Ibid, 13.

75.Eng. Abdullah Al-Swaha, "ICT Infrastructure Targeted in 1,000 Cyberattacks in 2016," The Business Year.

76.Ibid, 13.

77.KACST, "Communication and Information Technology Research Institute," https://www.kacst.edu.sa/eng/RD/CITRI/Pages/AboutCITRI.aspx.

78.Rabih Dabboussi, "DarkMatter to Underpin Importance of Digital Infrastructure Resilience at IDC CIO Summit 2016, KSA," DarkMatter, 2016, https://darkmatter.ae/en/press_releases/48.

79.Oxford Business Group, "Saudi Telecoms Companies Innovate in a Challenging Market," 2015, http://www.oxfordbusinessgroup.com/overview/finding-their-calling-companies-are-innovating-challenging-market.

80.Mohammed Rasooldeen, "SABIC launches innovation hub," Arab News. May 28, 2016, http://www.arabnews.com/node/930916/saudi-arabia.

81.Virginia Economic Development Partnership, Cyber Security Export Market: Saudi Arabia, George Mason University School of Public Policy, 2014, http://exportvirginia.org/wp-content/uploads/2014/02/Saudi-Arabia.pdf.

82.Raytheon Company, "Raytheon in Saudi Arabia," http://www.raytheon.com/ourcompany/global/middle_east/raytheon_in_saudi_arabia/.

83.Raytheon Company, "Raytheon and Saudi Arabia Military Industries announce strategic partnership," PR Newswire, May 20, 2017, http://www.prnewswire.com/news-releases/raytheon-and-saudi-arabia-military-industries-announce-strategic-partnership-300461082.html.

84.White House, "United States-Gulf Cooperation Council Second Summit Leaders Communique," Riyadh, Saudi Arabia, April21, 2016, https://obamawhitehouse.archives.

gov/the-press-office/2016/04/21/united-states-gulf-cooperation-council-second-summit-leaders-communique.

85.U.S. State Department, “Fact Sheet: US Security Cooperation with Saudi Arabia,” January 20, 2017, https://www.state.gov/t/pm/rls/fs/2017/266861.htm.

86.Bill Leigher, "Saudi Arabia Springs into Cyber Action," May 2015, http://www.raytheoncyber.com/news/feature/saudi_cyber.html.

87.Mark Sutton, "ICSC to Discuss Saudi Cybersecurity," November 6, 2016, http://www.itp.net/610073-icsc-to-discuss-saudi-cyber%20security.

88.Karen Elliott House, “Saudi Arabia in Transition,” Belfer Center for Science and International Affairs at the Harvard Kennedy School, July 21017, https://www.belfercenter.org/publication/saudi-arabia-transition.

89.Ministry of Foreign Affairs, “Saudi Arabia and the Visit of President Trump,” June 2017, https://www.saudiembassy.net/sites/default/files/WhitePaper_TrumpVisit_June2017.pdf.

90.Tan Sri Dato’ Seri Panglima Mohd Azumi, "OIC-CERT: Past, present and future," OIC-CERT, December 14, 2016, https://www.oic-cert.org/event2016/files/Attachment%204%20-%20Keynote%20Address.pdf .