网络就绪报告2.0

针对网络就绪水平的计划：基准与报告

主要研究者: Melissa Hathaway

Chris Demchak、Jason Kerben、Jennifer McArdle、Francesca Spidalieri

2015年11月

POTOMAC INSTITUTE FOR POLICY STUDIES

波托马克政策研究所发布

波托马克政策研究所
901 N. Stuart St, Suite 1200
Arlington, VA, 22203
www.potomacinstitute.org
电话: 703.525.0770; 传真: 703.525.0299

电邮: *CyberReadinessIndex2.0@potomacinstitute.org*

关注我们的Twitter账号:
@CyberReadyIndex

鸣谢

波托马克政策研究所衷心感谢下列机构一如既往的支持:国际电信同盟旗下的ICT应用与网络安全部、美洲国家组织旗下的美洲反恐怖主义委员会。此外，笔者还要对Sherry Loveless和Alex Taliesen的编辑和设计工作表示感谢。

网络就绪报告 2.0

针对网络就绪水平的计划：基准与报告

目录

网络就绪报告 2.0

针对网络就绪水平的计划：基准与报告

主要研究者: Melissa Hathaway
Chris Demchak、Jason Kerben、
Jennifer McArdle、Francesca Spidalieri

《网络就绪报告2.0》是对2013年11月发布的《网络就绪报告1.0》的拓展延伸。

引言

目前没有一个国家做好了应对网络的准备。

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，从而推动完善的管理。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，危及到网络经济。

全球的领导人们明白，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。网络就绪报告（CRI）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，解决网络安全问题造成的经济衰退。

在网络就绪报告1.0的基础上，网络就绪报告2.0考察了125个已经或即将实行的信息通信技术（ICT）和网络，采用七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，网络就绪报告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（ICT）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，以创造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全国安全重点相统一。

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的意识的提高，能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%，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/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]

举例来说， 20国集团（G20）经济体预计因假冒和盗版已经损失了250万份工作，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。

经济增长会受到网络安全问题的掣肘。

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。CRI2.0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。

网络就绪报告2.0——方法论

CRI2.0主要由两个部分组成：其一，CRI2.0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；以及
7. 防护与危机应对。

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，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。

CRI2.0方法论目前应用于评估125个国家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和服务上的成熟度和投入（数据1和表1）。

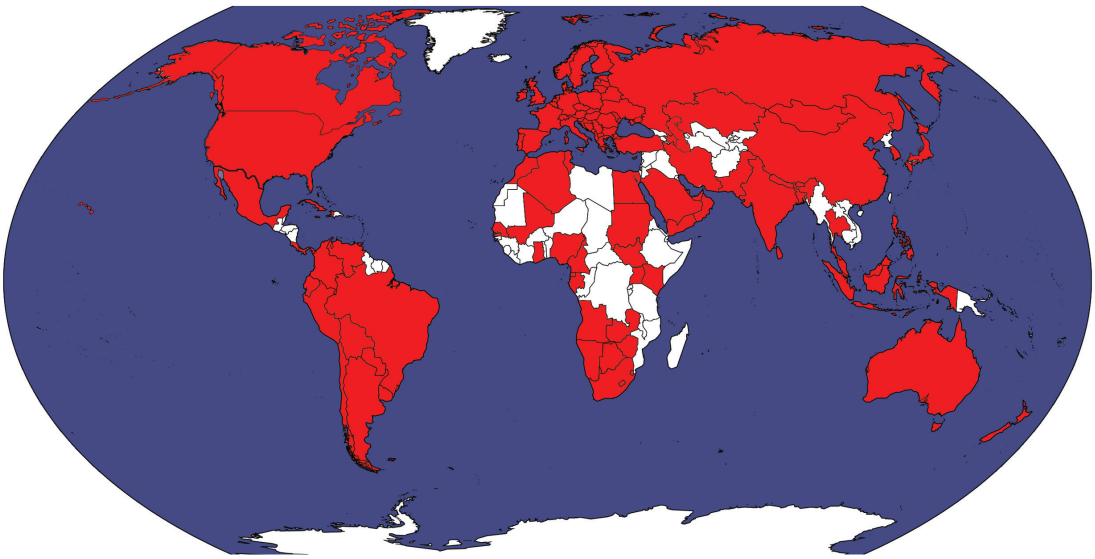
选择的国家包括国际电信联盟（ITU）通信技术发展指数排名前75的国家，用以强调连通性的重要性；还囊括了G20国家，因为它们代表了全球九成的GDP、八成的国际贸易、64%的世界人口和84%的矿物燃料排放。

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）、

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]



数据 1: CRI 2.0 选择的国家

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	台湾
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	香港	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

Table 1: CRI 2.0 Country Selection

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，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、也门以及黎巴嫩。[16]

这125国家代表了全球的大部分国家，体现出CRI2.0在国家选择标准上的多样性和代表性。

CRI2.0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扎实的基础，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，CRI2.0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，CRI2.0还有助于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，CRI2.0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和辅助手段。

以下是对CRI2.0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，采用至少十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，但是侧重独特的国家方案。

1. 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，人人TM，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，网上银行正在替代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。

> 全国网络安全战略必须反映网络安全的经济重要性。

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、可评估的、可实现的、基于结果和时间的目标；并且意识到必须要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（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：

A. 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：

A. 指定主管机关并明确职权；

B. 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；

C. 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：

A. 确定实施该战略所要求和分配的财政和人力资源；

B. 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：

A. 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；

B. 确定通过实施战略、安全性和应变能力将有所提高的关键服务（并非关键的基础设施）；以及

C. 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，CRI2.0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。

2. 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]

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）和亚太计算机紧急响应小组(APCERT)的演习活动。此外，新加坡主办过七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]

除了国家计算机安全事件响应小组，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

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。

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，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和交流。[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，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时间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，减少了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：

A. 公布针对紧急事件和危机的事件响应计划；

B. 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；

C. 有证据显示该计划定期实施并更新；

D. 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：

A. 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）；

B. 确认与政府和监管机构接头的全国授权联络人网络；

C. 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；

D. 建立信息警告和预警系统，全国危机/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:

A. 确定国家CSIRT执行命令所需要和分配的财政和人力资源;

B. 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:

A. 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;

B. 全国危机/响应中心具备及时解决和发布预警的能力;

C. 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，分享类似的行动方和战略、技术和程序，以确定模式;以及

D. 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，这一个关键因素的更新将会监督、追踪和评估这些发展。

3. 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。各国必须作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”，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。CRI2.0相信已经批准或同意上述任一一个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] 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，这可谓是一个突破性时刻。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]

CRI2.0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，CRI2.0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，将法律转变为技术领域，同时将技术领域转变为法律。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/培训演习于2015年7月举行。[52]

除了加强应对电子犯罪的能力和执法能力，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]再比如日本历时五年打造的网络清洁中心，2006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。[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

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。

经济增长会受到网络犯罪和诈骗的掣肘。

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：

A. 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；

B. 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：

A. 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、鉴定准假和其他调查人员的培训；

B. 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：

A. 确认打击网络犯罪所需要和分配的财政和人力资源；

B. 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：

A. 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）；

B. 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，以及滥用该等系统、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；以及

C. 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）。

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。CRI2.0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和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。

4. 信息共享

说明一国网络就绪水平的第四个因素就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；以及（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和利益。然而任一个模式要想成功，都离不开两大因素：认可和信任，这就要求必须具备明确目标、角色、责任和结果。简而言之，

信息共享必须依托于所有利益相关者的信任和认可。

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），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/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实施面临的网路威胁。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：

A. 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/信息的交换交流；

组织：

A. 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）；

B. 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）；

C. 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：

A. 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：

A. 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；以及

B. 有证据证明，政府具备能力和及时流程以公开（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。CRI2.0利用直接和间接资料来确定该等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。

5. 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。

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）计划投入预计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]

网络创新中心加速了创意和技术向解决方案的转化。

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多亿美元的资金。2016-2020年的首要研究领域包括：大数据、网宇实体系统、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。目前的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：

A. 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；

B. 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；

C. 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：

A. 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；

B. 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；

C. 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/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：

A. 确定网络安全基础和应用研究和举措所需要和分配的财务和人力资源；

B. 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和人力资源；

落实：

A. 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；

B. 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/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；以及

C. 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/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。CRI2.0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。

6. 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物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。相关方花了五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和/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》（TTIP）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]

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和/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（原则上）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。

网络安全渗透于外交政策和贸易的方方面面。

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；以及(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:

A. 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）；

B. 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:

A. 在国家的驻外办公室或类似组织中设立一只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；

B. 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:

A. 确定参与网络外交所要求和分配的财政和人力资源；

落实:

A. 已经参与国际、跨国、区域和/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；以及

B. 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、区域和/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。

7. 防护与危机应对

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和/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已超过近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，对许多人来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

破坏性和毁灭性的网络活动需要可信的网络防护。

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的军队，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]

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/责任方面的投入，包括以下因素：

声明：

A. 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；

B. 设定网络防御组织的政策，应对网络威胁；

C. 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：

A. 在军队中建立全国性组织，主要负责国家的网络防御；

B. 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：

A. 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；

B. 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：

A. 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；

B. 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；

C. 有证据表明与国际伙伴进行了演习（如北约共同防卫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；

D. 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；以及

E. 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。CRI2.0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

没有一个国家做好了应对网络的准备。

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。CRI2.0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。

CRI2.0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，CRI2.0挑战了传统观念，将网络安全视为国家安全的重要部分。CRI2.0展示了国家安全与是如何与网络连 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。

CRI2.0并非只是简单地研究该问题，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。CRI2.0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。如此这样一来，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，CRI2.0将可以展示各国在保护这些基础设施和服务方面商所做出的努力和完成的进度和发展情况。

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。

如您需要了解更多信息或希望向CRI2.0方法论提供数据，请联系：

CyberReadinessIndex2.0@potomacinstitute.org

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.europa.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）因上世纪七十年代发明了哈维球（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. 通讯部，《部长级法令147号》，1995年5月31日，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_korea_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》，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-cooperation/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/cybersecurity/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-IIS-AgreementRussian.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-INTERPOL-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 Iniciação-Científica 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/application/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/cybersecuri- ty-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-security-pointed-out-the-danger-of-destabilization-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eelnigo 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/PBLICTNEBOOK_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-korea-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》，(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。

关于作者

梅丽莎•海瑟薇 (Melissa Hathaway) 是网络政策和网络安全领域的一流专家。她担任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。她还是加拿大国际治理创新中心的杰出研究员，曾授命加入全球互联网监管委员会（比尔特委员会）。她曾效力于两届政府，为奥巴马总统提供《网络政策评估报告》，并为小布什总统领导过国家网络安全综合计划。她曾制定出一套独特的方法论，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、网络冲突以及网路的结构和风险。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，对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。她的学术研究集中在网络战、信息战和亚洲地缘政治学方面。她目前在伦敦国王学院战争研究学院攻读博士。

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》应用到美国各州。

波托马克政策研究所
901 N. Stuart St. Suite 1200, Arlington, VA 22203
www.potomacinstitute.org