全球网络空间
稳定委员会

推进网络稳定

最终报告
2019 年 11 月

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

维护网络空间稳定，构建和平繁荣的网络空间

全球网络空间稳定委员会 (GCSC) 将编制相关规范和政策提案以加强国际安全与稳定，并指导国家和非国家行为体在网络空间中采取负责任的行为。

www.cyberstability.org
info@cyberstability.org | cyber@hcss.nl
@theGCSC

推进网络稳定

最终报告
2019 年 11 月

The Hague Centre for Strategic Studies

海牙战略研究中心
Lange Voorhout 1
2514 EA The Hague

info@hcss.nl
www.hcss.nl

EastWest INSTITUTE

东西方研究所
纽约 |布鲁塞尔
莫斯科 | 旧金山

cyber@eastwest.ngo
www.eastwest.ngo

主席

Michael Chertoff，美国
Latha Reddy，印度
Marina Kaljurand，爱沙尼亚 *（前主席）*

委员

Abdul-Hakeem Ajijola，尼日利亚
Virgilio Almeida，巴西
Isaac Ben-Israel，以色列
Scott Charney，美国
Frédérick Douzet，法国
Anriette Esterhuysen，南非
Jane Holl Lute，美国
Nigel Inkster，英国
Khoo Boon Hui，新加坡
Wolfgang Kleinwächter，德国
Olaf Kolkman，荷兰
Lee Xiaodong，中国
James Lewis，美国
Jeff Moss，美国
Elina Noor，马来西亚
Joseph S. Nye, Jr.，美国
Christopher Painter，美国
Uri Rosenthal，荷兰
Ilya Sachkov，俄罗斯
Samir Saran，印度
Marietje Schaake，荷兰
Motohiro Tsuchiya，日本
Bill Woodcock，美国
Zhang Li，中国
Jonathan Zittrain，美国

特别代表和顾问

Carl Bildt，瑞典
Vint Cerf，美国
Sorin Ducaru，罗马尼亚
Martha Finnemore，美国

主任

Alexander Klimburg，奥地利
Bruce W. McConnell，美国

研究咨询小组主席

Sean Kanuck，美国
Koichiro Komiyama，日本
Marília Maciel，巴西
Liis Vihul，爱沙尼亚
Hugo Zylberberg，法国

秘书处

The Hague Centre for Strategic Studies

EastWest INSTITUTE

合作伙伴

Ministry of Foreign Affairs of the Netherlands

CSA SINGAPORE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

Microsoft

Afilias

主办单位

瑞士联邦外交部
全球安全论坛
爱沙尼亚外交部
日本总务省

支持单位

非洲联盟委员会
美国黑帽大会
极客大会
欧盟常驻联合国日内瓦办事处代表团
全球网络专家论坛
谷歌
海牙市
Packet Clearing House
特拉维夫大学
联合国裁军研究所

目录

主席寄语

网络空间是人类最伟大的发明之一，重塑着人际关系、社会关系、商业关系和政治关系。遗憾的是，由于针对和利用网络空间进行的攻击频发，亟需采取行动来确保网络空间的稳定性。网络空间稳定的概念类似于与其同宗的国际稳定，需要确立共同愿景，推动各方以相对和平的方式解决影响网络空间的地缘政治分歧和变化，为网络空间的稳定保驾护航。

全球网络空间稳定委员会自工作之初便一直坚信，如果不与其他利益相关方合作，长期以来一直困扰各国的国际和平与安全问题将无法得到解决。网络空间是一个涉及多利益相关方的环境，其中既有网络空间的创建者和管理者，又有抵御网络攻击（针对和利用网络空间进行的攻击）的保护者，他们可能是非国家行为体，也可能是政府官员。这一点在我们的委员遴选中得到了体现。除了拥有国际安全问题处理经验的前政府高级官员之外，我们的队伍中还包括互联网治理、人权与发展共同体以及技术产业领域的公认领袖。来自 16 个国家/地区的 28 位委员能够分享大量宝贵经验和独到见解，同时通过委员会的外联活动听取公众意见，集思广益。

委员会最终报告是三载辛勤工作的结晶。这一成果离不开各位委员、顾问和研究人员（包括多位志愿者）、资助方以及管理委员会的大力支持，我们在此表示衷心感谢。最后要向秘书处致谢，他们不但将进程管理得井井有条，而且促成了以公民团体倡议的形式创立本委员会。

在整个工作过程中，委员会一直在持续关注既往和现行的其他网络空间倡议。我们的报告《推进网络稳定》*(Advancing Cyberstability)* 在补充和巩固他方工作的同时，也为推进网络空间的稳定性提供了新思路。

Michael Chertoff
联席主席
全球网络空间稳定委员会

Latha Reddy
联席主席
全球网络空间稳定委员会

执行摘要

大国之间长达 25 年的战略稳定与相对和平如今走到了历史终点，国家间的冲突呈现出新的形式，而网络活动在这一动荡的新环境中扮演着主导角色。过去的十年间，国家和非国家行为体的网络攻击数量和复杂程度与日俱增，网络稳定遭受持续威胁。简言之，个人和组织可能不再确信自己能够安全可靠地使用网络空间，或是无法确保服务和信息的可用性与完整性。

在这一大背景下，全球网络空间稳定委员会 (GCSC) 应运而生，旨在为推进网络稳定出谋划策。我们首先确定了基于七项要素的网络稳定框架，具体包括：(1) 多方参与；(2) 网络稳定原则；(3) 制定和执行自愿性规范；(4) 遵守国际法；(5) 建立信任措施；(6) 能力建设；(7) 公开发布和广泛使用能确保网络弹性的技术标准。确定这一框架后，委员会深入探讨了其中三项要素：多方参与、原则和规范。

尽管多项国际协定都号召多方参与，但这一提法仍存在争议。部分观点仍然认为，确保国际安全与稳定几乎完全是国家的责任。然而实际上，网络战场（即网络空间）主要由非国家行为体设计、部署和运作，我们认为他们的参与对于确保网络空间稳定必不可少。非但如此，其参与也不可避免，因为非国家行为体往往会率先对网络攻击做出反应，甚至本身就是网络攻击的源头。

因此，委员会认为，这些非国家行为体不仅对确保网络空间稳定至关重要，而且也应以原则为指导并受规范约束。以下四项原则反映了这一观点，呼吁所有各方承担责任、克制自身、采取行动并尊重人权：

- 承担责任：各方行为体都有责任维护网络空间稳定。
- 克制自身：任何国家或非国家行为体均不得采取危害网络空间稳定的行为。
- 行动要求：国家或非国家行为体应采取合理、适当的措施来确保网络空间稳定。
- 尊重人权：维护网络空间稳定的工作必须尊重人权和法治。

在这些原则的基础上，为补充而非重复他方工作，委员会制定了八条规范，旨在更好地维护网络空间稳定，并解决或弥补先前公布的规范中存在的技术问题或不足：

1. 国家和非国家行为体不得从事或纵容故意并实质损害互联网公共核心的通用性或完整性并因此破坏网络空间稳定性的活动。
2. 国家和非国家行为体不得从事、支持或允许旨在破坏选举、公民投票或全民公决所需的技术基础设施的网络行动。
3. 在可能严重损害网络空间稳定性的情况下，国家和非国家行为体不得在开发和生产中篡改产品及服务，也不得允许他方对其进行篡改。

4. 国家和非国家行为体不得征用公共信通技术资源来制造僵尸网络或将其用于类似目的。

5. 各国应建立一系列程序上透明的框架，以评估是否以及何时披露其所了解但不为公众所知的信息系统和技术漏洞或缺陷。默认的程序应有利于信息披露。

6. 网络空间稳定所赖以实现的产品和服务的开发者和生产者应当：(1) 重视安全性和稳定性；(2) 采取合理措施确保其产品或服务不存在重大漏洞；(3) 在发现漏洞时及时补救，并对这一过程保持公开、透明。所有行为体都有义务分享相关漏洞信息，以帮助预防或减少恶意网络活动。

7. 各国应采取适当措施，包括颁布法律法规，确保基本的网络卫生。

8. 非国家行为体不得参与攻击性网络行动，国家行为体应对此类活动加以防范，并在发生时及时响应。

建议

委员会认识到多方参与的重要性，并了解发布行为规范无法确保这一点，因此提出六点建议，重点强化多方参与模式、促进规范采纳和实施，并确保违规方受到追责。具体建议如下：

1. 国家和非国家行为体应制定并实施相应规范，通过加强克制和鼓励行动来提高网络空间稳定性。

2. 国家和非国家行为体应按照其职责和限制，对违反规范的行为做出适当应对，确保违规方承担可预见的严重后果。

3. 国家和非国家行为体（包括国际机构）应加大人员培训和能力建设力度，促进各方对网络空间稳定的重要性达成共识，并尽量考虑不同方的需求。

4. 国家和非国家行为体应收集、分享、审查和发布有关违规活动及其影响的信息。

5. 国家和非国家行为体应形成利益共同体并彼此支持，以维护网络空间稳定。

6. 建立一个长期的多方参与机制，使各国、私营部门（包括技术社群）和公民团体都能充分参与和协商，以解决稳定性问题。

这份报告的发布既是一个终点，又是一个新的起点。委员会的任务已告一段落，但对于 GCSC 成员和支持单位以及协助我们达成目标的各方来说，这些原则、规范和建议的实施之路任重而道远。如果稳定性得不到保障，网络空间便会失去所有优势。因此，我们必须即刻出发，全力以赴。

1. 引言

数字演进和网络空间为人类生活带来巨变。[1] 在全球范围内对数据进行数字化、存储、分析和传输的能力对社会各行各业都产生了深远影响，也改变了我们处理个人、商业和政治事务的方式。如今，全球近半数人口都是互联网用户，[2] 并且这一数字还在迅速增加。即使本人并未连接到网络空间，也深受其影响，因为他们赖以提供产品和服务的实体往往依托网络空间来处理沟通、物流和财务事宜。

网络空间的优势以及确保其稳定的必要性一直是人们热议的话题，所面临的挑战亦不例外。最值得一提的是，网络空间既能为高尚目的打开方便之门，也会为卑鄙意图留下可乘之机。例如，全球连通性、匿名性和缺乏可追溯性使个人和机器无需验证身份即可连接数据和系统，但犯罪分子也可能利用这些特点来实施犯罪行为并逃脱惩罚。因此，世界各地的政府、企业和个人都面临着两难境地。政府注重保护网络空间、提供公共服务及推进其他重要活动（例如教育和网上银行），同时也需要维护国家安全利益，包括执法、情报和军事能力。企业致力于保护客户、声誉及盈利情况，却可能频频遭到攻击，需要追查恶意活动，且/或满足政府数据要求。而个人，无论他们本人是否联网，对数字技术的依赖度和接受度都日益上升，但同时也担忧着相关技术的持续可用性和完整性。在过去十年中，网络攻击的数量和复杂程度与日俱增，对政府系统和关键基础设施的攻击也不例外。[3] 因此，无论是当下现状还是可以预见的趋势，都不甚乐观。

国家和非国家行为体均可能发动网络攻击，这也清楚地表明，世界需要网络稳定框架。这一框架将有助于降低网络空间遭受重大破坏的可能性，进而避免削弱网络空间优势及损害人权和自由等人民福祉。毫无

1 “网络空间”具有多种定义 (https://en.wikipedia.org/wiki/Cyberspace)。剑桥词典将其定义为“一种电子系统，使世界各地的计算机用户能够相互通信或出于各种目的访问信息”(https://dictionary.cambridge.org/us/dictionary/english/cyberspace)。在英国，“网络空间一词旨在描述用于存储、修改和传递信息的数字网络的电子媒介，其中不仅包括互联网，还包括为企业、基础设施和服务提供支持的其他信息系统”(https://www.cpni.gov.uk/cyber)。因此，可以说其范畴比互联网更广，后者被通俗地描述为“互连计算机网络的全球系统，使用互联网协议簇 (TCP/IP) 链接全球设备”。请参阅 https://en.wikipedia.org/wiki/Internet。另请参阅国际电信联盟的《定义互联网》(Defining the Internet)讨论文件（2013 年 5 月），https://www.itu.int/dms_pub/itu-s/md/13/wtpf13/inf/S13-WTPF13-INF-0008%21%21MSW-E.docx。

2 互联网世界统计机构的《互联网使用情况统计》(Internet Usage Statistics)，最后修改于 2019 年 10 月 4 日，https://internetworldstats.com/stats.htm。

3 战略与国际研究中心 (CSIS) 的*《自 2006 年以来的重大网络事件》*(*Significant Cyber Incidents Since 2006*)，https://csis-prod.s3.amazonaws.com/s3fs-public/190904_Significant_Cyber_Events_List.pdf；Louis Marinos 和 Marco Lourenço 编写的《ENISA 2018 年威胁态势报告》(*ENISA Threat Landscape Report 2018*)，ENISA（2019 年 1 月），https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018；Abhishek Agrawal 等编写的*《Microsoft 安全情报报告》*(*Microsoft Security Intelligence Report*)，第 24 卷（2018 年 12 月），https://clouddamcdnprodep.azureedge.net/gdc/gdc09FrGq/original；联合国大会*《从国际安全角度看信息和电信领域的发展：秘书长的报告》*(*Devel-opments in the field of information and telecommunications in the context of international security: report of the Secretary-General*)，A/74/120（2019 年 6 月 24 日），https://undocs.org/zh/A/74/120。

疑问，产品和服务如果设计制作精良，并得到 IT 专业人员和计算机用户的妥善管理，将会提升安全性和稳定性；相反，如果它们设计粗劣或操作错漏百出，则将有损安全和稳定。但仅仅改善开发和运作还远远不够，在国家和非国家行为体将网络空间视为战场来争夺政治、军事或经济优势的情况下尤为如此。持续攻击者可能会突破安全措施，导致“互联网防御难敌进攻”之说，并造成网络空间的不稳定。[4] 因此在关注技术的同时，行为也不容忽视：如何鼓励所有行为体以负责任的方式行事，进而增强而非威胁网络空间稳定？

为帮助解答这一问题，一些政府和非政府实体推动设立了全球网络空间稳定委员会 (GCSC)，[5]并指出：

> 大国之间长达 25 年的战略稳定与相对和平如今走到了历史终点，国家间的冲突将呈现新的形式，而网络活动可能在这一动荡的新环境中扮演主导角色，使和平利用网络空间以促进经济增长并扩大个体自由面临着与日俱增的风险。
>
> 为应对这些新态势，全球网络空间稳定委员会将编制相关规范和政策提案以加强国际安全与稳定，并指导国家和非国家行为体在网络空间中采取负责任的行为。GCSC 将使所有利益相关方参与其中以达成共识，并通过促进信息交流和能力建设、基础研究以及提出倡议来维护网络稳定。[6]

值得注意的是，委员会本身也涉及多利益相关方并且具有全球性，成员背景和专业十分多元。有些委员曾在政府任职，参与过网络问题的双边和多边谈判，有些委员在构建、维护和保护互联网方面拥有丰富经验，还有一些委员代表着公民团体。

委员会的工作并非凭空而来，GCSC 深知有很多其他机构和进程（无论过去还是现在）都在关注网络空间的稳定性，因此力求不重复他方工作。确切来说，GCSC 竭力在其他多利益相关方和政府进程的基础上开展工作，为未来奠定基础。这些进程包括联合国信息安全政府专家组 (UN GGE)[7] 持续开展的基础性工作、不限成员名额工作组 (UN OEWG) 的工作及以

4　请参阅 P.W.Singer 和 Allan Friedman 的《对网络攻击的崇拜》(The Cult of the Cyber Offensive)，《外交政策》(*Foreign Policy*)（2014 年 1 月 15 日），https://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/；世界经济论坛 (WEF) 的《*2019 年全球风险报告*》(*The Global Risks Report 2019*)（2019 年），http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf。

5　有关 GCSC 的更多信息，请参阅“附录 C：GCSC 的历史、目标与进程”。

6　全球网络空间稳定委员会，https://cyberstability.org/。

7　2015 年，联合国大会在一项重要决议中一致确认了 UN GGE 的结论。请参阅大会第 70/237 号决议《*2015 年 12 月 23 日大会决议[根据第一委员会的报告 (A/70/455) 通过]*》，https://undocs.org/zh/A/RES/70/237。包括《联合国宪章》在内的国际法就国际上针对敌对行动的响应对策建立了专属框架，该框架同样适用于网络行动。我们的工作以所有国家在 2015 年联合国大会上达成的协议为基础，以负责任的行为规范为指导，致力于提高信通技术使用的稳定性和安全性，并履行国际法规定的尽职调查与合作承诺。

下各方的努力：全球网络专家论坛 (GFCE)、[8] 信息社会世界首脑会议 (WSIS)、全球互联网治理委员会（比尔特委员会）、互联网治理论坛 (IGF)、全球网络空间会议（GCCS/伦敦进程）、NETmundial 倡议、欧洲安全与合作组织 (OSCE)、非洲联盟委员会 (AUC)、《信任宪章》、《网络安全技术协定》、海牙网络规范项目、联合国裁军研究所 (UNIDIR)、《网络空间信任与安全巴黎倡议》（简称《巴黎倡议》）以及联合国秘书长设立的数字合作高级别小组。与此同时，委员会的工作还受到了委托研究和公众意见的启发。

所列部分工作在某种程度上聚焦于网络空间的稳定性，并认为网络空间稳定与治理密不可分。也就是说，如果没有强有力的治理模式，社会便缺乏确保稳定所需的互动和决策流程。例如，比尔特委员会提议“在公民、民选代表、司法机构、执法和情报机构以及企业、公民团体和互联网技术社群之间就数字隐私和安全建立多利益相关方社会契约，以期恢复信任，增强对互联网的信心。”[9]

对于各方先前就动荡的网络空间新领域中的行为制定原则、规则和规范的努力，我们深表赞赏，同时认为必须建立完善的框架来提高网络空间稳定性。历史记录表明，在某些情况下，社会和政府可能需要历经数十年的时间，才能为重大突破性新技术建立广泛、正式的国际治理体系。[10] 网络空间作为全球经济、社会和安全相互依存的关键层面，在 20 世纪 90 年代末方才出现，彼时万维网刚开始得到广泛应用。因此，治理发展进程尚处于规范的一致性与不一致性并存的早期阶段。[11] 例如，与域名系统相关的规范和制度相对完善，而各国和各企业在内容监管方面则存在重大分歧。国家和非国家行为体有时会借鉴知识产权、贸易等其他机制中的规范，而越来越多的私营企业本身也在制定规范。[12] 本委员会的目的并非解决这些不同的治理问题，而是将其置于一个旨在确保网络空间稳定的通用框架内。

我们还注意到，积极维护网络空间稳定的各方一直在极力对抗试图破坏网络空间的攻击势力，并密切关注着技术发展和地缘政治冲突的演变。我们面临的部分挑战在于，网络空间改变了行为体实现政治和军事目标的方式：由于进入壁垒较低，成为网络强国的难度要低于成为传统军事强国的难度。此外，一些掌握新技术的行为体不愿接受约束，在这类约束尚未得到广泛遵守的情况下尤为如此。国际社会亟需建立一个通用的网络稳定框架，使其既能够维护网络空间稳定，又能够在技术变革步伐不断加快时持续发挥作用。因此，我们首先要确定核心目标，即维护网络空间稳定。

8　GFCE 一直在积极参与能力建设。请参阅全球网络专家论坛《关于 GFCE 全球网络能力建设议程的德里公报》(Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building)（2017 年 11 月 24 日），https://www.thegfce.com/delhi-communique/documents/publications/2017/11/24/delhi-communique。

9　全球互联网治理委员会，*《同一个互联网》*(*One Internet*)（2016 年），第 IX 页，https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf。“我们呼吁各国政府、私营企业、公民团体、技术社群和个体共同为数字时代订立新的社会契约。”

10　或许核武器是说明此类治理体系的最佳示例，整个体系的建立过程需要耗费大量时间和精力。即使《不扩散核武器条约》(NPT) 生效至今已有 60 年的时间，核武器治理安全问题依然存在。

11　该早期阶段称为“机制复合体”。请参阅 Joseph Nye 的《用于管理复杂全球网络活动的机制复合体》(The Regime Complex for Managing Complex Global Cyber Activities)，全球互联网治理委员会，第 1 号文件（2014 年 5 月），https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf。

12　请参阅 ISOC 和 Microsoft 制定的规范：《路由安全性的相互商定规范》（Mutually Agreed Norms for Routing Security，简称 MANRS），互联网协会（2014 年），https://www.manrs.org/；Angela McKay 等编写的*《国际网络安全标准：减少网络世界的冲突》*(*International Cybersecurity Norms Reducing Conflict in an Internet-dependent World*)，Microsoft（2014 年 12 月），https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA；以及 Scott Charney 等编写的*《从表述到实施：支持网络安全规范进程》*(*From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*)，Microsoft（2016 年 6 月），https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8。

2. 网络空间稳定的含义

定义：

所谓网络空间稳定，是指每位用户都有理由确信自己能够安全可靠地使用网络空间，在网络空间内和通过网络空间提供的服务和信息的可用性和完整性通常能够得到保证，以及能够以相对和平的方式管理变更，并妥善解决紧张局势，避免进一步升级。

委员会的定义以“稳定性”的标准定义为基础，[13] 在两个方面略有差别。首先要提及的是用户信任。信任至关重要，因为人的决定可能基于认知而不仅仅是事实，如果用户认为缺乏稳定性，他们可能不愿意使用网络空间及从中获益。举例来说，使用网络空间可以简化流程并提高效率，这意味着某些功能（例如访问政府服务、网上银行）可受益于网络空间。但如果此类系统不可靠，或用户认为此类系统不可靠，则其使用将非常有限，继而失去相应技术优势。

其次必须谨记，网络空间是一个不断变化的领域。如今，技术、商业模式、功能以及社会对技术在日常生活中所扮演角色的期望都在发生变化。因此，与词典中的“稳定性”定义（包括“恢复到初始状态”）不同，我们需要的是敏捷的机制，以确保网络空间在技术发展过程中始终保持稳定。简单来说，即使网络空间及其所处环境发生变化，每位用户都必须对网络空间的可用性和完整性保持信心。

13 “稳定性”被定义为“稳定状态”(https://www.lexico.com/en/definition/stability)。“稳定”意指：(1) 稳定，稳固，牢固；(2) 不太可能改变或失效，持久；以及 (3) 不容易发生物理变化。请参阅 https://en.oxforddictionaries.com/definition/stable。在国际关系中，“国际稳定”一词较为普遍的定义为“（国际）系统保持其所有基本特征的可能性；不存在一国独大的局面；大多数政权长期存续；不会发生大规模战争。”Karl W. Deutsch 和 J. David Singer，《多极权力体系与国际稳定》(Multipolar Power Systems and International Stability)，*《世界政治》*(*World Politics*) 第 16 卷第 3 期（1964 年 4 月）：第 390-406 页，http://users.metu.edu.tr/utuba/Deutsch.pdf。

3. GCSC 网络稳定框架

为了应对上述挑战，GCSC 也像其他组织一样，[14] 提出了完善的网络稳定框架。具体包括：(1) 多方参与；(2) 网络稳定原则；(3) 制定和执行自愿性规范；(4) 遵守国际法；(5) 建立信任措施；(6) 能力建设；(7) 公开发布和广泛使用能确保网络弹性的技术标准。GCSC 的工作主要侧重于其中三项——多方参与、原则和规范，并分别在第 4、5、6 节中进行了论述。关于规范，我们不仅关注其制定问题，同时还关注其采纳、实施以及违规者问责等棘手问题。

需要指出的是，当前多项工作均致力于网络稳定框架中的各个要素，但由于网络空间本身的性质，这些工作相对分散。GCSC 认为，要取得进展，有赖于全球多利益相关方的共同努力。因此，除了解决实质性问题，GCSC 还提出了一些流程性建议，以期充分利用既有努力成果，同时查缺补漏，或可为其注入新活力。

14 请参阅《*相互依存的数字时代：联合国秘书长数字合作高级别小组报告*》(*The Age of Digital Interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation*)（2019 年 6 月），第 39 页，https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf。“我们建议制定《全球数字信任与安全承诺》，来塑造共同的愿景，确定数字稳定性的属性，阐明并加强负责任使用技术规范的实施，并提出行动重点。”

网络稳定框架图片中所用图标的制作者为来自 www.flaticon.com 的 Freepik、monkik、smalllikeart、Eucalyp 和 Itim2101。

4. 多方参与

尽管各国之间的多项国际协定皆引证多方参与做法的重要性，但这一提法仍存在争议。部分观点认为，这不过是哲学意义上的讨论，侧重于国家和非国家行为体在技术政策和国际事务中的相对角色。其他观点则相信多方参与流程切实可行，认为单凭国家行为或者仅辅以最低限度的非国家支持，将无法确保网络空间稳定。[15]我们赞同后一种观点。

关于多方参与的利弊之争已持续数十年。这一问题往往在管理互联网资源的语境下出现，随之而来的还有规范和国家安全问题。例如，在联合国信息社会世界首脑会议 (WSIS) 的第二阶段会议上，联合国互联网治理工作组 (WGIG) 否定了单一利益相关方主导的理念。更确切地说，工作组认为互联网规模过于庞大，无法由单一利益相关方团体或单一组织独立管理，继而提出了多方参与的做法。因此，在 2005 年 WSIS 突尼斯议程中，各国首脑声明：“有关互联网治理的工作定义是由政府、私营部门和公民团体通过发挥各自的作用制定和应用的，它们秉承统一的原则、规范、规则、决策程序和计划，为互联网确定了演进和使用形式。”[16]

十年后，联合国大会关于 WSIS 成果执行情况全面审查的高级别会议重申了这一观点，联合国第 70/125 (2015) 号决议也指出：

> 我们还重申多利益攸关方合作和参与的价值和原则，这种合作和参与是信息社会世界首脑会议进程从一开始就具有的特征，确认各国政府、私营部门、民间社会、国际组织、技术和学术界以及所有其他相关利益攸关方在其各自作用和责任范围内的有效参与、伙伴关系和合作，特别是在发展中国家享有均衡代表性的前提下，对于建设信息社会一向且仍然至关重要。[17]

15 “WSIS 定义（2005 年）引入了‘各自角色’的概念和‘共享’理念。《NETmundial 宣言》（2014 年）将关键要素定义为自下而上、公开、透明、包容和基于人权。换言之，我们有一些关于多方参与做法的一般规范，但并没有统一的多方参与模式。迄今为止已出现两种不同的多方参与模式：协商模式和协作模式。”Wolfgang Kleinwächter 的《采取整体方法制定互联网相关公共政策》(Towards a Holistic Approach for Internet Related Public Policy Making)，全球网络空间稳定委员会（2018 年 1 月），https://cyberstability.org/wp-content/uploads/2018/02/GCSC_Kleinwachter-Thought-Piece-2018-1.pdf。有关多方参与模式的进一步讨论，请参阅 Virgilio Almeida 等编写的《多方参与模式的起源和演进》(The Origin and Evolution of Multistakeholder Models)，《*IEEE Internet Computing*》第 19 卷（2015 年 1 月至 2 月）：第 74-79 页，https://doi.ieeecomputersociety.org/10.1109/MIC.2015.15。

16 “信息社会突尼斯议程”，WSIS（2005 年 11 月 18 日），第 34 条，https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html。

17 请参阅联合国大会第 70/125 号决议《*关于信息社会世界首脑会议成果文件执行情况全面审查的大会高级别会议成果文件*》，A/RES/70/125（2015 年 12 月 16 日），第 3 条，https://undocs.org/zh/A/RES/70/125。

同样，该声明超出了关键互联网资源管理的范围，直抵国家安全问题核心：

> 我们确认各国政府在涉及国家安全的网络安全问题上发挥的领导作用。我们还确认所有利益攸关方在各自的作用和职责范围内所发挥的重要作用和做出的重要贡献。[18]

具体到规范，八国集团 (G8) 于 2011 年声明：

> 互联网上的网络和服务安全性问题属于多利益相关方问题，需要各国政府、区域和国际组织、私营部门[以及]公民团体之间的协调配合...在所有利益相关方的支持下，各国政府可在制定网络空间使用行为规范和通用做法方面发挥作用。[19]

两年后的 2013 年，UN GGE 发布了*《从国际安全的角度来看信息和电信领域的发展》报告*。UN GGE 在“开展合作创造和平、安全、有弹性和开放的信通技术环境”一节中指出，“虽然各国必须带头应对这些挑战，但私营部门和民间社会的适当参与有利于开展有效合作。”[20] 报告在“关于国家负责任行为的规范、规则和原则的建议”一节中继续表示：

> 会员国应考虑如何以最佳方式进行合作，执行上述负责任行为准则和原则，同时考虑到私营部门和民间社会组织可能发挥的作用。[21]

UN GGE 的 2015 年报告重申了这些立场，声明：

> 虽然各国对维持一个安全、和平的信通技术环境负有首要责任，但是，确定私营部门、学术界和民间社会组织适当参与的机制将有利于开展有效合作。[22]

2018 年联合国大会*《从国际安全角度促进网络空间国家负责任行为》*决议中也重申了这一声明。[23] 其他国际协定明确表达了同样的观点。例如，《巴黎倡议》指出，“我们认识到，强化多方参与做法，进一步致力于降低网络空间稳定性风险以及增强信心、能力和信任，实属必要。”[24]

18 同上，第 50 条。

19 八国集团《G8 宣言：对自由与民主的新承诺》(G8 Declaration: Renewed Commitment for Freedom and Democracy)，八国集团多维尔峰会（2011 年 5 月 27 日），第 17 条，http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-en.html。

20 联合国大会*《从国际安全的角度来看信息和电信领域的发展》报告*，A/68/98（2013 年 6 月 24 日），第 7 页，第 12 条，https://undocs.org/zh/A/68/98（以下简称《UN GGE 2013 年报告》）。

21 同上，第 8 页，第 25 条。

22 联合国大会*《从国际安全角度看信息和电信领域的发展》报告*，A/70/174（2015 年 7 月 22 日），第 13 页，第 31 条，https://undocs.org/zh/A/70/174（以下简称《UN GGE 2015 年报告》）。

23 联合国大会第 73/266 号决议*《从国际安全角度促进网络空间国家负责任行为》*，A/RES/73/266（2018 年 12 月 22 日），https://undocs.org/zh/A/RES/73/266。

24 《网络空间信任与安全巴黎倡议》（2018 年 11 月 11 日），https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf。另请参阅 NETmundial 的《NETmundial 多利益相关方声明》(NETmundial Multistakeholder State-ment)（2014 年 4 月 24 日），http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf。

最近一次在 2019 年 6 月，联合国秘书长数字合作高级别小组在其报告*《相互依存的数字时代》*中指出：

> 尽管目前存在各种压力，但只有加强多边主义才能实现有效的数字合作，同时还应辅以多方参与，即不仅各国政府，还有更广泛的其他利益相关者，如公民团体、学术界、技术专家和私营部门共同参与合作。[25]

尽管实践证明多方参与的做法能够取得成功，但这一理念尚未得到普遍支持。部分政府仍然认为，确保国际安全与稳定几乎完全是国家的责任。这种较为传统的安全观源于国家有责任通过强力手段保护其公民免遭攻击的观念，这一观念体现在《联合国宪章》第二十四条所规定的联合国安全理事会职责中。[26] 过去的经验也可能会强化这一思路，因为在物理领域，各国政府不仅对武力合法使用情形享有专断权，而且还控制着用于相应领域攻击和防御的军用级武器（例如飞机、坦克）。

实际上，网络战场（即网络空间）主要由私营部门设计、部署和运作。政府尽管负有独一无二的责任，但并非这一领域的专属保护者。即使各国政府对网络空间中的武力合法使用情形维持*法律上*的专断，它们也不再实际专断其中的攻击和防御情况，同样也无法阻止强大网络武器的扩散和使用。实际上，技术社群、公民团体和个人在保护网络空间（包括颁布标准）方面也发挥着重要作用。因此，多方参与的做法十分必要，有助于改善结果、建立健全可维护网络空间稳定的规范和政策，并避免不良后果。

同样重要的是，即使各国希望单独行动，也无法如此。非国家行为体不可避免地参与到影响网络空间稳定的事务中。例如，私营部门和技术社群可能有多位成员负责关键协议和服务，他们还可能为使用其商用和开源产品的国家提供保护。此外，属于政府传统角色和政治特权的攻击调查和归因也不再是其专有知识和责任领域，非政府实体已经查明并公布了一些值得注意的国家攻击事件。简言之，尽管国家能够在攻击中和攻击后发挥独特作用（包括执法活动和/或采取外交手段或其他国家行动），但对于调查和归因并没有专断权，实际上也无法将非国家行为体排除在外。因此，制定行之有效的网络空间规范和政策并确保其得到遵守，需要所有利益相关方的共同参与，同时也是所有利益相关方的责任，各国政府必须集中力量建立相关机制，便于私营部门、技术社群、学术界以及公民团体的其他代表参与其中。这也正是多国政府的诉求。

25 *《相互依存的数字时代》*，第 7 页，https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf。

26 《联合国宪章》，“第五章：安全理事会”，《联合国各机关惯例汇编》，http://legal.un.org/repertory/art24.shtml。

5. 原则

规范的行为源自价值观。因此，我们必须以阐明这些价值观作为出发点，无论它们涉及个体责任、国家责任还是基本人权。诚然，不同的价值观可能为达成共识带来困难，并导致不同国家或区域在解释和实施国际协定时产生差异。但这并不意味着必须就原则达成一致意见才能取得进展；有时，即使动机各不相同，但各方会就可接受的行为达成共识。然而，共同原则和相互依存有助于加深彼此的合作，并降低未来出现分歧或冲突的风险。因此，各方必须开诚布公地探讨作为思路指引和规范依据的高级别原则。

下列四项原则对于维护网络空间稳定至关重要：

1. **承担责任：**各方行为体都有责任维护网络空间稳定。
2. **克制自身：**任何国家或非国家行为体均不得采取危害网络空间稳定的行为。
3. **行动要求：**国家或非国家行为体应采取合理、适当的措施来确保网络空间稳定。
4. **尊重人权：**维护网络空间稳定的工作必须尊重人权和法治。

A. 承担责任原则

第一项原则说明了网络空间的分散性和分布式特点。这一原则重申了采取多方参与做法来维护网络空间稳定的必要性，特别是扩大“利益相关方”的范围，让所有个体都参与其中。每个个体都有责任以个人和/或专业身份维护网络空间稳定。负责政府网络政策的人员和管理云服务的员工需要各尽其责，但连接到网络空间的每一个人也都必须做出合理努力，确保自己的设备免遭入侵或被用于攻击。即使是未连接到互联网的人员，也可能需要依赖互联网功能来接收产品和服务，因此他们同样有责任确保在其社区遵守相应的网络空间政策。

B. 克制自身原则

第二项原则包含克制的一般要求。对各国而言，这与联合国大会 (UNGA) 2018 年关于网络空间中负责任国家行为的决议[27] 和《UN GGE 2015 年报告》一致，其中指出：“各国应遵循联合国宗旨，包括维持国际和平与安全的宗旨...并防止发生公认对国际和平与安全有害或可能对其构成威胁的信通技术做法...”[28] 但这项要求不仅仅关乎国家，因为非国家行为体也可能采取行动，例如通过黑客技术发动反攻击，而这也可能破坏网络空间的稳定。

27 联合国大会第 73/27 号决议《*从国际安全角度看信息和电信领域的发展*》，A/RES/73/27（2018 年 12 月 5 日），https://undocs.org/zh/A/RES/73/27；联合国大会第 73/266 号决议，https://undocs.org/zh/A/RES/73/266。

28 《UN GGE 2015 年报告》第 7 页，第 13 (a) 条，https://undocs.org/zh/A/70/174。

C. 行动要求原则

第三项原则包含采取积极行动来维护网络空间稳定的一般要求。各国在采取行动时，应注意避免不经意间导致紧张局势升级或不稳定性加剧。这与《UN GGE 2015 年报告》中指出的“合作制定和采用各项措施，加强信通技术使用的稳定性与安全性”义务一致。[29]该要求同样不仅仅关乎国家，因为私营企业和个人也可能采取合作措施来帮助维护网络空间稳定。例如，私营企业可以彼此协作来减轻网络威胁，而个人可采用升级、打补丁和使用多重身份验证等最佳实践，以此降低计算机被僵尸网络接管，继而被用于发起广泛攻击而威胁网络空间稳定的风险。

D. 尊重人权原则

第四项原则确认了保障人权的重要性，将其视为网络空间稳定的重要因素。由于个人对信息和通信技术的依赖程度日益增加，因其可用性或完整性受到威胁而对人类活动造成的破坏性影响也随之加剧。因此，各国在网络空间中追求自身的国家战略利益时，必须充分考虑对个人造成的影响，尤其是人权影响。同样，非国家行为体应考量并最大限度地降低其活动对个人在线上和线下享有权利构成的风险。根据“尊重人权原则”的要求，各国在从事网络空间活动时至少须遵守国际法规定的人权义务。

《世界人权宣言》已列明公认的基本人权。[30] 此外还有多项国际协定规定了各类具体人权，并确立了对缔约国具有约束力的法律义务。联合国大会、[31] 联合国人权理事会 (HRC)[32] 以及《UN GGE 2013 年报告》和《UN GGE 2015 年报告》均明确确认了国际人权法在网络空间中的适用性。[33] 保障用户权利并确保其相信自身权利得到尊重，对于维护网络空间稳定至关重要。

需要指出的是，这四项原则并非旨在囊括所有内容，或是纳入网络空间政策的方方面面，有许多组织已经制定了涵盖各种问题的广泛原则。此外还有一些其他组织重点关注与互联网治理和网上人权相关的问题（包括隐私、言论自由和结社自由等）。我们的目标是使有助于维护网络空间稳定的原则得到普遍接受，特别是在敌对活动空前广泛且错综复杂的时代，因为这一时代的规则可能不甚明确，或者即使非常明确也无法得到采纳或施行。

29 同上。

30 联合国大会第 217 A (III) 号决议《*世界人权宣言*》（1948 年 12 月 10 日），https://www.un.org/zh/universal-declaration-human-rights/index.html。

31 请参阅联合国大会第 68/167 号决议《*数字时代的隐私权*》，A/RES/68/167（2013 年 12 月 18 日），https://undocs.org/zh/A/RES/68/167；以及联合国大会第 69/166 号决议《*数字时代的隐私权*》，A/RES/69/166（2014 年 12 月 18 日），https://undocs.org/zh/A/RES/69/166。

32 联合国人权理事会《*在互联网上增进、保护和享有人权*》，A/HRC/20/L.13（2012 年 6 月 29 日），https://undocs.org/zh/A/HRC/20/L.13。

33《UN GGE 2013 年报告》，https://undocs.org/zh/A/68/98；《UN GGE 2015 年报告》，https://undocs.org/zh/A/70/174。

6. 规范

原则是制定政策和指导战术行动的关键出发点，但由于其高度抽象性，需要辅以更加细化的协定来界定可接受的行为。换言之，原则必须以规范作为补充。规范代表期望的适当社会行为。[34] 讨论规范时，必须参照其他组织的工作，尤其是 UN GGE 及其 2015 年报告。[35] UN GGE 认识到，“鉴于信通技术的独特属性，可能需要在一段时间后制定更多规范。”[36] 而 GCSC 的任务实际上是“编制相关规范和政策提案以加强国际安全与稳定”。为了在先前工作的基础上确定哪些方面可能需要其他规范，必须首先查阅 2015 年商定的规范（规范全文请参阅附录 A）。

正如 UN GGE 在 2015 年指出，其任务包括“确定需要在哪方面制定考虑到信通技术复杂性和独特属性的更多规范”。[37] 在此之后，信通技术产品和服务及其滥用情况一直在不断变化。为解决这一问题，GCSC 重点弥补当前规范中的缺陷，在规范讨论中增加技术专向性并解决实施问题。例如，在弥补缺陷方面，GCSC 批准了旨在保护互联网公共核心的规范[38] 以及旨在保护选举制度的规范。[39] 同样地，UN GGE 规范提及了“供应链的完整性”，[40] 而 GCSC 规范则更具体地说明了必须应对的供应链攻击类型。[41]

34 https://en.oxforddictionaries.com/definition/norm。
35 联合国政府专家小组 2015 年报告，https://undocs.org/zh/A/70/174。
36 同上，第 8 页，第 15 段。
37 同上，第 7 页，第 11 段。

38 全球网络空间稳定委员会 (GCSC)，*呼吁保护互联网公共核心 (Call to Protect the Public Core of the Internet)*（2017 年 11 月，新德里），https://cyberstability.org/wp-content/uploads/2018/07/call-to-protection-the-public-core-of-the-internet.pdf。荷兰研究人员 Dennis Broeders 是最早提出保护互联网公共核心的倡导者之一，他主张确定互联网公共核心以进行特殊保护。请参见 Dennis Broeders 所著的*互联网的公共核心：互联网治理国际议程 (The Public Core of the Internet: An International Agenda for Internet Governance)*（阿姆斯特丹：阿姆斯特丹大学出版社，2015年），http://www.oapen.org/download?type=document&docid=610631。
39 全球网络空间稳定委员会 (GCSC)，*呼吁保护选举基础设施* (Call to Protect the Electoral Infrastructure)（布拉迪斯拉发，2018 年 5 月），https://cyberstability.org/wp-content/uploads/2018/05/gcsc-call-to-protection-election-infrastructure.pdf。
40 《2015 年联合国政府专家小组报告》，第 8 页，第 13(i) 段。“各国应采取合理步骤确保供应链完整，让最终用户对信息通信技术产品的安全抱有信心。各国应努力防止恶意信息通信技术工具和技术的扩散以及有害隐藏功能的使用。”
41 全球网络空间稳定委员会 (GCSC)，*在新加坡通过的规范 (Norms Through Singapore)*（2018 年 11 月），https://cyberstabile-ity.org/wp-content/uploads/2019/04/singaporenew-digital.pdf。“在可能严重损害网络空间稳定性的情况下，国家和非国家行为体不得在开发和生产中篡改产品及服务，也不得允许他方对其进行篡改。”

UN GGE 规范与 GCSC 规范之间的另一项主要区别在于，GCSC 认为也应赋予非国家行为体相应的责任，因为他们必须保持克制或采取积极行动来维护网络空间稳定。我们这里所说的并非是由一些犯罪分子发动的网络攻击；对于这些犯罪分子，如果政府行动都起不到震慑作用，规范更加力所不及。但随着技术的日新月异，法律做不到与时俱进，因此在相关法律缺位的情况下，如果能准确描述应当鼓励或加以制止的非国家行为，多少会有所助益。例如，一些观点主张应允许黑客行为的受害者实施“黑客回击”。即使并无法律明文允许或禁止这种行为，GCSC 也认为此举并不可取，原因涉及诸多方面，比如初始攻击者可能通过第三方系统（例如云提供商或医院）对其攻击进行路由，而黑客回击行为可能导致无辜用户（例如云客户或患者）受到牵连。此外，由于此类攻击波及无辜，黑客回击可能被视为或者会引发形势升级。总之，鉴于事态可能复杂化，即使相关法律缺失，用于约束私营部门行为体的规范也可能对行为施加影响，从而起到积极作用。

A. GCSC 拟议规范

考虑到上述几点，GCSC 制定了以下拟议规范：

1. 国家和非国家行为体不得从事或纵容故意并实质损害互联网公共核心的通用性或完整性并因此破坏网络空间稳定性的活动。

2. 国家和非国家行为体不得从事、支持或允许旨在破坏选举、公民投票或全民公决所需的技术基础设施的网络行动。

3. 在可能严重损害网络空间稳定性的情况下，国家和非国家行为体不得在开发和生产中篡改产品及服务，也不得允许他方对其进行篡改。

4. 国家和非国家行为体不得征用公共信通技术资源来制造僵尸网络或将其用于类似目的。

5. 各国应建立一系列程序上透明的框架，以评估是否以及何时披露其所了解但不为公众所知的信息系统和技术漏洞或缺陷。默认的程序应有利于信息披露。

6. 网络空间稳定所赖以实现的产品和服务的开发者和生产者应当：(1) 重视安全性和稳定性；(2) 采取合理措施确保其产品或服务不存在重大漏洞；(3) 在发现漏洞时及时补救，并对这一过程保持公开、透明。所有行为体都有义务分享相关漏洞信息，以帮助预防或减少恶意网络活动。

7. 各国应采取适当措施，包括颁布法律法规，确保基本的网络卫生。

8. 非国家行为体不得参与攻击性网络行动，国家行为体应对此类活动加以防范，并在发生时及时响应。

值得注意的是，组织最恰当的语言来表述规范可能颇具挑战性。如果规范过于精确，不留解释余地，可能难以达成共识，覆盖广度或将大打折扣。反之，如果规范含糊其辞，则无法提供必要的指导来指引行为，并针对特定行为群体设定明确期望。目标是取得适当的平衡，并视需要制定进一步规范，以确保不当行为得到处理。举例来说，2015 年通过的 UN GGE 规范可保护关键基础设施，但这一术语是否涵盖互联网公共核心，却不甚明确。多数观点认为关键基础设施是指公用事业和服务（例如电力、通信和银行业）。[42] 此外，UN GGE 并未具体提及选举制度，这一担忧在 2015 年之后变得更加严重。[43] 有些国家在援引时可能将选举制度纳入其中（一些国家当前认为选举制度属于关键基础设施，因此将其列入关键基础设施规范的范围内），[44] 但有些国家可能并不认同这种做法。

因此，尽管网络空间具有全球性，规范保护却可能并非如此。为了帮助解决有关 GCSC 规范的解释问题，委员会决定为上述各条规范提供背景信息（请参阅附录 B）。

最后，网络空间行为规范不可一成不变。GCSC 规范反映的是不断变化的技术格局中的某个时刻。随着技术不断进步以及我们对现有技术含义的理解发生变化，国家和非国家行为体都应做好制定新规范的准备。

无论是偏重 UN GGE 规范、GCSC 规范还是其他提案，我们都必须认识到，规范需要得到采纳和实施，并且须对违规行为追究责任。我们接下来将解决这些问题，然后探讨分散在世界各地的非国家行为体如何能与政府合作，共同制定应对网络稳定挑战的可行性解决方案。

B. 规范采纳

规范若要产生成效，必须先获得普遍接受。接受规范的行为体（甚至包括部分观点认为的潜在违规者）将维护揭发违规行为的行动以及为应对此类违规行为而采取的适当集体行动的正当性。虽然普遍采纳是理想情况，但由志同道合的国家或其他实体组成的小型团体也可以商定和实施特定规范。为此，GCSC 提出一种灵活且可扩展的做法，使国家和其他利益相关方能

42 关键基础设施定义为包括“至关重要的系统和资产，不论是有形还是虚拟的系统和资产，如果上述系统和资产失效或遭到破坏将对网络安全、国家经济安全、国家公共健康或安全，或上述安全事宜的任何组合产生破坏性影响。”*2001 年《关键基础设施保护法》*，2001 年《美国法典》第 42 编第§ 5195c(e) 条。还有一个定义是“对维持社会功能、健康、安全、社会保障、人民经济或社会福祉至关重要的资产或系统”。欧盟理事会，*理事会 2008 年 12 月 8 日第 2008/114/EC 号指令关于识别和指定欧洲关键基础设施和评估改善其保护的必要性*，《欧洲联盟公报》，（2008 年 12 月 8 日），https://eur-lex.europa.eu/legal-content/en/TXT/pdf/?uri=celex:32008l0114。

43 Erik Brattberg 和 Tim Maurer，*俄罗斯干涉选举：欧洲应对假新闻和网络攻击 (Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks)*，卡内基国际和平基金会（2018 年 5 月 23 日），https://carn-egieendowment.org/2018/05/23/Russion-election-int European-s-counter-to-Fake-News-and-Cyber-Attacks-pub-76435。Michael McFaul，*确保美国选举安全 (Securing American Elections)*，斯坦福网络政策中心（2019 年 6 月），https://cyber.fsi.stanford.edu/securing-our-cyber-future。

44 例如，请参见美国国土安全部“Jeh Johnson 部长关于将选举基础设施指定为关键基础设施细分产业的声明”（2017 年 1 月 6 日），https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastruc-ture-critical。

够求同存异，在接受某些规范的同时拒绝或弃用其他规范。这种做法不但可以指明意见一致和存在分歧的具体方面，而且使各方能够接受、完善和实施特定规范，尽管需要更多时间来评估其他规范。无论如何，规范的普遍采纳将是一项长期的工作。

在推行规范的过程中，还要应对一些客观存在的独特挑战。所谓的独特挑战在于，我们所面对的是相对较新的、破坏稳定的行为。由于规范具有“常态化、典型化、标准化”的特点，[45] 就未来行为起草相应规范的做法很有意义。如果所有人都以某种方式行事，书面规范就只是汇编现有做法。但是，如果没有“典型行为”，那么起草规范则是在倡导日后的常态行为，即使这种行为在当下并不常见。仅仅阐明理想标准并不足以构成规范，而是需要促使其得到采纳。

另外，有能力实施规范的实体以及规范旨在保护的对象必须更加了解拟议规范。即使在联合国及众多其他论坛属于高活跃度话题，但规范的采纳仍处于起步阶段，要推行拟议规范并使其得到普遍接受，还需要进行大量工作，在某些地区更是如此。因此，在这一领域进行能力建设至关重要；组织的能力越强，越有可能推动规范的采纳，而获得更多拥护者则是所有全球规范结构的基础。此外，信息必须触达受规范保护的对象，因为他们可能尚未认识到其潜在影响。例如，计算机应急响应小组 (CSIRT/CERT) 似乎并非普遍了解 UN GGE 的这一规范：各国不得攻击国家级 CSIRT，而是仅将其用于防御目的。如下文所述，受保护实体往往在实施和问责（以及拟议规范的设计）环节发挥作用，但如果他们不了解或不清楚国家和非国家行为体所提出的建议，便无法履行这些职责。显然，各国政府和国际组织需要开展更多工作，方可触达拟议规范旨在帮助的群体。

45 请参见 https://www.lexico.com/en/definition/norm。

C. 规范实施

得到采纳之后，国家和非国家行为体必须采取具体措施来实施规范。持续开展的联合国进程（OEWG 和 GGE）以及区域性工作似乎正在形成共识，将规范的实施视作行动重点。[46] 在某种程度上，实施是指采行规范，涉及能力建设和信任建立，或是就已商定规范的含义达成更加细化的共识。[47] 虽然这些措施是实施规范的重要先决条件，但它们并非主要用来实施规范。例如，尽管能力建设对于各国必不可少，可确保各国保障自身安全，并具备参与国际活动所需的带宽，但能力建设可在未采纳或实施相关规范的情况下进行。同样，建立信任有助于维持网络空间稳定，包括推动各国就网络原则交换意见、建立国家网络专家之间的快速通信热线，以及鼓励分享最佳做法和安全标准，但即使不实施相关规范，这些措施也能实现。更确切地说，实施规范需要采取具体措施为其添砖加瓦。在国内层面，这可能包括将拟议规范纳入国家政策、立法和军事理论。在国际层面，则可能包括在攻击归因或采取外交行动时引用某条规范的规定。以这种方式运作规范也有助于赋予其更精准的定义。

46 联合国大会第 73/266 号决议，第 3 页，第 1(b) 段，https://undocs.org/zh/A/RES/73/266；联合国大会第 73/27 号决议，第 5 页，第 5 段，https://undocs.org/zh/A/RES/73/27。另请参见欧洲安全与合作组织 (OSCE) *秘书长 Thomas Greminger 开幕致词*，2019 年欧洲安全与合作组织网络/信息通信技术安全主席会议（布拉迪斯拉发，2019 年）。“区域性国际组织可以成为与建立信任措施相关的新想法和实践努力的孵化器，也可以成为全球公认协定（比如政府专家小组报告）的执行者。因此，区域性国际组织既可以是孵化器，也可以是执行者。”

47 联合国大会邀请所有会员国考虑 GGE 和 OEWG 报告中所载的评估和建议，继续向秘书长通报它们对报告的看法和评估意见，*尤其是*对“在国家一级为加强信息安全和促进这一领域的国际合作所作的努力”和“国际社会为加强全球一级信息安全可能采取的措施”的看法和评估意见。请参见联合国秘书长第 74/120 号报告，https://undocs.org/zh/A/74/120。有关成员国的更多观点，请参见 https://www.un.org/disarmament/ict-security/。

D. 问责机制

规范得到采纳和实施后，就必须对违规方追责。随之而来的是复杂的归因和应对问题，这两者已证明是处理网络攻击事件的难点。

要对国家或非国家行为体的不当行为进行认定，需进行可靠的归因。首先要收集和分析证据，此时可从技术和程序两方面入手，以提高归因质量和及时性。更具体地说，与其他技术学科一样，采用公认的证据收集和分析原则对提高调查质量至关重要。因此，必须对调查方法进行标准化；这样一来，即使归因必须逐案判断，也可减少对证据完整性的担忧。除了从技术层面改善归因外，还可执行多项工作，以精简归因判断的繁琐程序，并适时予以公开。事件发生和责任声明之间往往间隔较长时间，这很大程度上是由于在国家层级作出此类判断的流程不明确或不灵活，在多个国家参与并作出集体归因声明时尤为如此。设计和实施国家及国际层级的归因流程，并改善国家之间的信息共享，可显著改善归因声明的及时性和有效性，且有助于进一步采取适当行动。

即使在证据指向特定行为体之后，下一步（归因）也可能困难重重。过去，一些国家和非国家行为体声称归因无法进行，或者需要绝对证据。不过绝对证据其实并非必需，虽然归因可能较为困难，但也不像一些观点指出的那样无法实现。在民族国家的语境下，无论是网络领域还是物理领域，归因通常都是政治行为，尽管没有特别商定的举证标准，但各国仍强烈建议不要提出虚假指控，以免丧失可信度。简言之，归因需要令其他国家和公众信服。

即使受害方确信特定行为体负有责任（且归因实际发生于国际案件中），对行为体予以追责实际上也颇具挑战性，这损害了规范的价值。毕竟，如果违反公认规范者未承担不利后果，规范将成为一纸空谈，很难对破坏稳定的活动起到阻止作用。

对非国家行为体实施的网络攻击进行追责相对简单，主要通过根据相关国家的国内法律追究民事或刑事责任来实现。当然，其中也存在挑战，因为许多网络攻击具有国际性，且收集证据在技术层面并不容易，这些都可能对国家行动构成障碍。但从概念上而言，前行道路十分明确，即简化国际执法程序，并竭力查明和起诉网络罪犯。

对国家违规行为追责难度更大，[48]这是因为网络空间中的攻击应对很大程度上取决于当时的背景。关于是否需要问责，国家和非国家行为体将权衡不同的因素，例如对违反规范做出回应的国家可能会考虑政治影响，而私营企业可能需要考虑商业和声誉影响。关于如何处理违规情况，可从连续性角度看待针对违规行为的国家行动，对应的响应级别可能是轻微（如私人投诉）、显著（如经济制裁）或重大（如显而易见的动态响应）。尽管并不存在普适性响应对策，但违反规范和国际法的行为必然会产生严重后果。过去实施规范的努力收效甚微，因此需要制定更有效、更及时的响应对策，同时注意这些对策应极力避免引发更严重的动荡。

48　各国可能要对由其进行、指挥或允许进行的网络行动负责。尽职调查原则也可能有助于界定各国在网络空间中所需的谨慎程度。Joanna Kulesza，*国际法中的尽职调查*，（Leiden：Brill Nijhoff，2016 年），https://doi.org/10.1163/9789004325197。另请参见*国家对国际不法行为承担责任条款*，由国际法委员会在 2001 年第五十三届会议通过，附入联合国大会 2001 年 12 月 12 日通过第 56/83 号决议，并经 A/56/49 (Vol I)/Corr4 号文件第 4条和第 11 条更正，http://legal.un.org/ilc/texts/instruments/draft_articles/9_6_2001.pdf。

非国家行为体也在努力确保违规方对自己的行为负责。例如，GFCE[49] 将政府、公民团体和私营部门成员联合起来，帮助协调能力建设工作，这是规范采纳、实施和问责的必要前提。此外，私营部门在攻击归因过程中发挥了更大的作用，结合使用专有信息和公共信息来揭露行为体并说明他们造成的破坏。最后，一些私营部门实体已提议或启动相关工作，例如 CyberPeace Institute[50]，旨在以更系统的方式和更大的规模监测和公开大型网络事件。

非国家行为体应在追究违反规范者的责任方面发挥更大作用。私营部门实施规范的想法并不新鲜：例如，1977 年，在南非反种族隔离斗争期间，通用汽车公司在该国推广了一套广泛采用的关于进行生意合作（和不进行生意合作）的原则，导致超过 125 家外国企业撤资。[51] 最近，许多公司（和政府）对沙特谋杀反对派记者 Jamal Khashoggi 一事作出反应，抵制沙特未来投资计划，以此表示反对，这件事更具象征意义。[52] 这些努力的成效尚待进一步考察。

E. 利益共同体

尽管在规范的通过、实施和问责方面采用多利益相关方模式至关重要，但如何利用这些群体的能量和能力却是一项艰巨的挑战。各国政府经常使用“志同道合的国家”一词来反映观点相似的一些国家，但没有一个对等的词来描述对某一特定问题持相同观点的国家、私营公司、非营利组织（包括标准组织）、民间团体和个人的集合。而这一点十分重要，因为 UN GGE 和 GCSC 提出的规范可能会影响到不同的群体、不同的组织和社会成员，他们可能比其他组织和成员更愿意倡导某些规范。由于政府、私营部门、技术界、学术界和民间社会并非铁板一块的实体，因此务必考虑如何给大家创造一种协调一致而不是集中的努力方向，让不同社区参与处理与规范相关的问题。[53] 通过建立利益共同体，可以让熟悉具体规范的专家致力于继续发展和实施这些规范。例如，计算机应急响应小组 (CERTs/CSIRTs) 可能对实施和监督旨在保护本共同体的 UN GGE 规范特别感兴趣，就像负责选举制度的人可能对 GCSC 关于选举制度的规范特别关注一样。同样，互联网共同体可以帮助推进、实施和监督委员会提出的有关保护互联网公共核心的规范，而开发人员可能对涉及产品防篡改的规范最感兴趣。

利益共同体可以定向组建，也可以自下而上临时形成。事实上，成员本身可以自己组成一个共同体，但这并不表示他们的发展和成功应该听之任之。相反，务必要关注令共同体取得成功的因素，具体如下：(1) 共同的原则；(2) 问题焦点；(3) 主题专业知识；(4) 财务和行政支持；(5) 透明的流程。事实上，也许可以确定一个最佳实践模板，说明应该如何建立和实施共同体，从而让各种规范制定过程采用一个类似的共同体模式。这样做将有助于协调不同的工作流程，确保工作效率和重点，在规范的通过、实施和问责上采用最佳实践。

49 全球网络专家论坛，https://www.thegfce.com/。
50 CyberPeace Institute，https://cyberpeaceinstitute.org/。
51 一般而言，可以参见“苏利文原则”，维基百科，2018 年 8 月 12 日，https://en.Wikipedia.org/wiki/sullivan_Principles。
52 参见《西方抵制 2018 年未来投资计划》*皇家新闻*，2018 年 10 月 16 日，https://en.royanews.tv/news/15500/2018-10-16。
53 一般而言，可以参见*数字相互依存时代*，https://digitalcooperation.org/wp-content/uploads/2019/06/digitalco-operation-report-for-web.pdf。

7. 建议

关于确保网络空间稳定性的六条建议基于我们关于责任、约束、行动要求和尊重人权的原则。由于大家对确保网络空间的稳定性都负有责任，而且采取多利益相关方模式对确保网络空间稳定至关重要，我们还建议充分利用国家和非国家行为体的能力（在一定程度上通过利益共同体来实现）。简而言之，我们应该把重点放在*应该*做什么和*如何*做上。

1. **国家和非国家行为体必须制定并实施相应规范，通过加强克制和鼓励行动来提高网络空间稳定性。**先前已同意采纳规范的国家行为体必须更明确地定义所使用的术语，通过进一步谈判并结合实施现有规范的实际经验即可完成这一工作。国家和非国家行为体都应该通过公开声明、政策和行动的改变，证明已经通过并实施规范。

2. **国家和非国家行为体应按照其职责和限制，对违反规范的行为做出适当应对，确保违规方承担可预见的严重后果。**如果违反规范的人清楚这样做没有代价，那么制定和实施规范就不可能有成效。因此，国家和非国家行为体应开发内部能力，根据行动要求原则，评估违法行为，迅速决定并采取适当的个人和集体应对措施。

3. **国家和非国家行为体，包括国际机构，应该加大工作人员培训力度，加强能力建设，促进对网络空间稳定性重要性的共识，并考虑到各方的不同需求。**提升能力、扩大共识将增强世界执行国际法、规范和其他建立信任措施的能力，这些措施既可以增强网络空间的稳定性，同时又能尊重人权。所有各方应充分利用侧重于能力建设的现有组织（包括多利益相关方参与的全球网络专家论坛），因为这是通过和实施规范、落实问责制、采取其他稳定措施和尊重人权的先决条件。

4. **国家和非国家行为体应收集、分享、审查和发布有关违规活动及其影响的信息。**尽管全球已经出现违反联合国制定和 GCSC 提议的规范的行动，但报告内容往往是零散的，不够全面。各组织，特别是那些独立于任何国家或商业利益团体的组织，应系统收集和公布违反规范及其影响的信息。这样做将有助于促进国家和非国家行为体对违反规范的行为作出响应，并帮助改善规范的遵守情况。

5. **国家和非国家行为体应形成利益共同体并彼此支持，以促进网络空间稳定。**建立和支持共同体将有助于确保包括国家、私营部门、技术界、学术界和民间团体在内的所有相关方都能履行各自的责任，以确保网络空间稳定。这些共同体可以重点关注本报告和其他地方提出的网络安全规范的解释、通过和实施，责任归因的证据标准是否健全，以及是否及时有效地对违反规范者追究责任。

6. **全球网络空间稳定委员会建议建立一个长期的多方参与机制，使各国、私营部门（包括技术社群）和公民团体都能充分参与和协商，以解决稳定性问题。**责任原则确认了每个人在确保网络空间的稳定方面都可以发挥作用，并强调了多利益相关方模式的必要性。从 2011 年到 2017 年，全球网络空间会议 (GCCS) 为此类交流提供了平台，其他领域负责确保全球稳定的外交部和安全部的部长级与会者参加了会议，此次会议还进行了一项重要的能力建设工作——设立全球网络专家论坛。互联网治理论坛 (IGF) 也为多利益相关方参与讨论提供了一个重要平台。最近，“巴黎呼吁”召集了有史以来规模最大的由多利益相关方组成的网络安全规范支持者共同体。这些努力表明，发展一个全球性、包容性和注重行动的多利益相关方共同体的时机已经成熟，工作重点是切实实施本报告和其他地方提出的网络安全规范。应设立常设机构为该机制提供支持，从而确保工作的持续性和连续性。

附录 A：联合国政府专家小组通过的规范[54]

a. 按照联合国宗旨，包括维持国际和平与安全的宗旨，各国应合作制定和实施各种措施，加强信息通信技术使用的稳定性和安全性，并对公认有害国际和平与安全或可能威胁国际和平与安全的信息通信技术做法予以防范；

b. 在发生信息通信技术事件时，各国应考虑所有相关信息，包括事件的大背景、信息通信技术环境下归因面临的挑战以及事件后果的性质和范围；

c. 各国不得蓄意允许他人利用本国领土使用信息通信技术实施国际不法行为；

d. 各国应考虑如何以最佳方式开展合作，交流信息，相互协助，起诉利用信息通信技术开展犯罪活动的恐怖分子和犯罪分子，以及采取其他合作措施应对上述威胁。各国可能需要考虑是否需要在这方面制定新的措施；

e. 各国在确保安全使用信息通信技术时，应尊重人权理事会关于在互联网上促进、保护和享有人权的第 20/8 号和第 26/13 号决议，以及大会关于数字时代隐私权的第 68/167 号和第 69/166 号决议，保证充分尊重人权，包括言论自由权；

f. 一国不应违背国际法规定的义务，从事或故意支持故意损害关键基础设施的信息通信技术活动，或以其他方式损害向公众提供服务的关键基础设施的使用和运营；

g. 各国应采取适当措施，保护其重要基础设施免受信息通信技术的威胁，同时考虑到大会关于建立全球网络安全文化和保护重要信息基础设施的第 58/199 号决议以及其他相关决议；

H. 对于关键基础设施受到恶意信息通信技术行为影响的国家提出的正当协助请求，各国应作出响应。各国还应在适当考虑主权的情况下，回应适当的请求，以减少源自其领土的针对另一国关键基础设施的恶意信息通信技术活动；

i. 各国应采取合理步骤确保供应链的完整性，以便最终用户能够对信息通信技术产品的安全性充满信心。各国应努力防止恶意信息通信技术工具和技术的扩散以及有害隐藏功能的使用；

j. 各国应鼓励负责任地报告信息通信技术漏洞，并分享关于此类漏洞的可用补救措施的相关信息，以限制并尽可能消除对信息通信技术和依赖信息通信技术的基础设施的潜在威胁；

k. 各国不应开展或蓄意支持损害另一国授权应急响应小组（有时称为计算机应急响应小组或网络安全事件响应小组）信息系统的活动。国家不应利用授权的应急响应小组从事恶意的国际活动。

54 请参见联合国大会*关于从国际安全的角度看信息和电信领域的发展政府专家组的报告*，第 A/70/174 号决议（2015 年 7 月 22 日），https://undocs.org/zh/A/70/174。

附录 B：
GCSC 规范

1. 不干涉公共核心

规范：

国家和非国家行为体不得从事或纵容故意并实质损害互联网公共核心的通用性或完整性并因此破坏网络空间稳定性的活动。

背景

界定互联网的公共核心是一项挑战，因为许多不同类型的攻击最终可能会损害互联网整体的可用性或完整性（这是需要避免的结果）。也就是说，如果希望产生如此广泛的影响，人们显然将针对某些环节，而且至少可以提供这些关键要素的非详尽清单。在最高级别，委员会对“普遍可用”一词的定义是：行为体的行为对一般人群产生重大影响。因此，本规范认为，支持本规范的国家仍然可以从事目的和范围受到限制且对一般人群没有实质性影响的活动。

委员会对术语“互联网公共核心”的定义包括了互联网基础设施的如下关键要素：数据包路由和转发、命名和编号系统、安全和身份的加密机制、传输介质、软件以及数据中心等。

数据包路由和转发要素包括但不限于：(1) 便于将分组通信从其来源地传输到目的地的设备、设施、信息、协议和系统；(2) 互联网交换点（产生互联网带宽的物理站点）；(3) 向用户传输上述带宽的主要网络的对等路由器和核心路由器；(4) 保证路由真实性和保护网络免受滥用行为影响所需的系统；(5) 用于上述目的的设备的设计、生产和供应链；(6) 路由协议本身及其开发、标准化和维护程序的完整性。

命名和编号系统包括但不限于：(1) 互联网域名系统运行中使用的系统和信息（包括注册管理机构、名称服务器、区域内容、基础设施和流程，如用于加密签名记录的 DNSSEC）；(2) 用于根域、反向地址层级、国家代码、地理和国际化顶级域名以及新的通用和非军事通用顶级域名的 WHOIS 信息服务；(3) 常用的公共递归 DNS 解析器；(4) 互联网分配号码管理机构和区域互联网注册管理机构的系统，提供并维护互联网协议地址、自治系统编号和互联网协议标识符的唯一分配；(5) 命名和编号协议本身，以及协议开发和维护的标准化程序和结果的完整性。

安全和身份的加密机制包括但不限于：(1) 用于认证用户和设备并保障互联网交易安全的密钥；(2) 为生产、通信、使用和弃用上述密钥提供支持的设备、设施、信息、协议和系统；(3) PGP 密钥服务器、证书颁发机构及其公钥基础设施；(4) DANE 及其配套协议和基础设施；(5) 证书撤销机制和透明日志；(6) 密码管理器；(7) 漫游接入认证器；(8) 精确时间和时间优先的建立机制，如网络时间协议及其基础设施；(9) 加密算法和协议开发和维护的标准化过程和结果的完整性；以及 (10) 用于实现加密过程的设备的设计、生产和供应链。

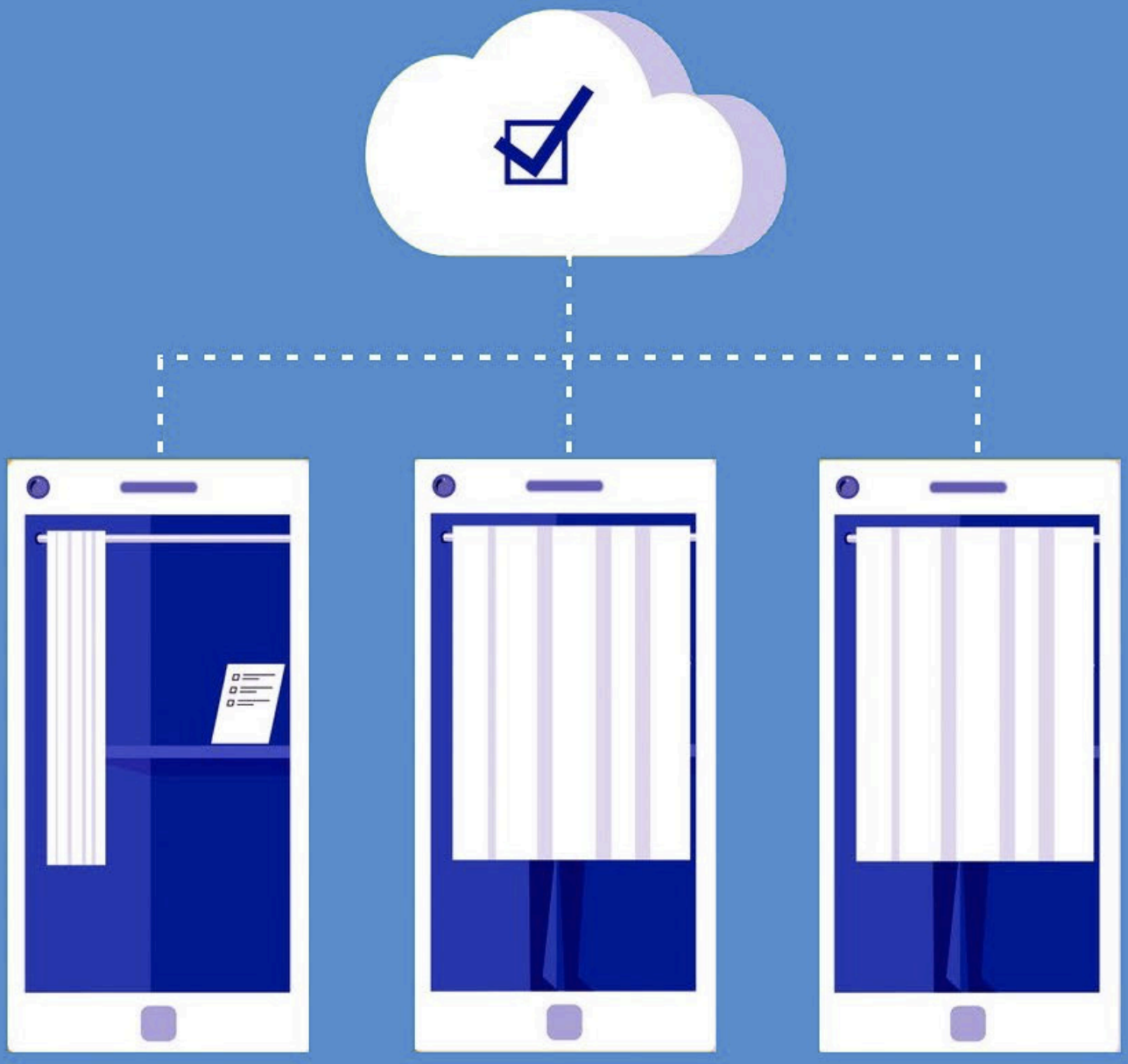
传输介质包括但不限于 (1) 为公众提供服务的通信基础设施、系统和装置，无论是光纤、铜缆还是无线；(2) 地面和海底电缆以及着陆站、数据中心和其他配套物理设施；(3) 蜂窝和其他无线语音和数据通信；(4) 受管制和不受管制的广播通信；(5) 支持传输、信号再生、分支、多路复用和信噪比鉴别的系统；以及 (6) 为地区或人口服务，而不是为个别公司客户服务的有线系统。

软件包括但不限于互联网核心以及大部分互联网用户所使用的软件的开发过程、源代码和补丁分发基础设施的可用性和完整性。

数据中心包括但不限于：(1) 存放服务器、内容和互联网基础设施的物理设施；(2) 用于确保数据中心安全、安保、物理访问控制、操作、管理、维护和冗余系统工作的系统；和 (3) 用于和数据中心通信的通信系统。

专家们认为，有更多种类的互联网和支持信息通信技术的基础设施值得保护，因此，今后可能会扩大定义的涵盖范围。

2. 保护选举基础设施



规范：

国家和非国家行为体不得从事、支持或允许旨在破坏选举、公民投票或全民公决所需的技术基础设施的网络行动。

背景

在国际礼让中指导各国行为的所有规则、戒律和原则中，不干涉规范可能是最神圣的规范。《联合国宪章》第二条第四款阐明了这一规范，并将其提升为一项具备法律性质，因而具有约束力的原则：

> 各会员国在国际关系中不得进行武力威胁或使用武力，或采用违背联合国宗旨的其他任何方式，侵害任何国家的领土完整或政治独立。

通过这一规定，《宪章》的起草者承认，对不干涉原则的最严重威胁来自针对一个国家的实体或政治自治的强制性措施，而事实上，这两者对于国家主权来说都不可或缺。国家控制的领土可能是其主权能力的表现，但如果不享有政治代理权和独立性，它就毫无价值。此外，最能体现真正政治独立的莫过于参与国家治理进程，比如举行自由、公平的选举。《联合国宪章》力求提供强有力的保护，以防止受到外来的不正当干涉。

现在，这些保护措施在数字时代再次受到挑战。

专家们一直在辩论，近期发生的与网络相关的选举干扰属于非法侵犯主权（因为它干扰了政府行使其固有职能）还是非法干预。[55] 然而，无论是否违反国际法，恶意行为体无论单独行动、集体行动还是代表国家行动，显然有可能通过数字手段操纵选举。随着国民参与进程的规模越来越大，越来越复杂，管理这些进程的数据、机构和基础设施也在迅速增加。如今，许多国家都在网上公布选民名册，这是防止操纵投票或舞弊的一项基本的、传统的保证，结果却让这些数据库受到网络攻击和利用。同样，选举投票工具也要在一个国家的偏远地区使用，这些地区的操作人员并不完全了解与数字操纵有关的风险和问题。地方级或“投票站”级投票软件供应商和计算机系统仍然容易遭受这种入侵。

考虑到参与进程受到的威胁越来越多并且日益严重，并认识到这种攻击是不可接受的，GCSC 建议采取更有力的国家措施和开展有效的国际合作，防止、减轻和应对针对选举技术基础设施的网络入侵。委员会承认，在区域、地方或联邦一级实际进行选举或参与选举进程完全是各国的职权，应根据各自国家的法律进行。然而，对其选举基础设施的网络攻击可能来自境外，而这需要多边合作才能解决。随着越来越多的国家选择将其选举机制数字化，与上述选举基础设施相关的风险和漏洞开始成倍增加，大规模攻击性网络行动也将随之暴增。因此，各国政府必须承诺不参与针对另一国选举技术基础设施的网络行动。推荐采纳这一规范时，委员会只是申明，干扰选举无论是否被视为违反国际法，都是不能容忍的。

55 请参见 Michael N.Schmitt 的“‘虚拟’剥夺公民权：干预网络选举处在国际法灰色地带 (Virtual' Dis-enfranchisement: Cyber Election Med-dling in the Grey Zones of International Law)，”*芝加哥国际法杂志*第 19 卷第 1 期，和 Nicholas Tsagourias 的“网络干扰选举、自决和不干涉网络空间的原则”(Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace)，https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-princi-ple-of-non-intervention-in-cyberspace/。

3. 关于避免篡改的规范

规范：

在可能严重损害网络空间稳定性的情况下，国家和非国家行为体不得在开发和生产中篡改产品及服务，也不得允许他方对其进行篡改。

背景

在一项以“不干涉互联网公共核心”为重点的规范中，GCSC 呼吁国家和非国家行为体不要蓄意和实质性地损害互联网公共核心的普遍可用性或完整性。为支持这一规范，委员会特别提到其他基础设施越来越依赖于稳定和安全的互联网，以及互联网中断可能造成的严重后果。虽然公共核心规范侧重于“互联网核心”，但个人和组织严重依赖某些商业产品来接触公共核心并利用其提供的连接。因此，篡改软件和硬件信息技术产品（包括但不限于操作系统、工业控制系统、交换机、路由器和其他关键网络设备、关键加密产品和标准、微芯片设计和广泛使用的最终用户应用程序）中的关键组件可能同样会剥夺社会安全使用和利用互联网的能力，削弱对其正常功能的整体信任。虽然此类攻击频频见诸报端，但是很少引起大家关注的是，甚至在产品或其更新上市之前，攻击就可能发生。例如，在产品的设计和制造阶段或其中一个更新过程中，通过插入漏洞或秘密删除安全功能，就可以对产品发起攻击。换句话说，一个产品在发布或投产之前就可能被篡改，对广大公众造成影响。从插入漏洞到激活漏洞以进行恶意使用之间的时间可能会有所不同。

在处理信息技术产品时，各国的利益和责任相互冲突。一方面，他们有义务提升网络基础设施的抗风险能力和完整性，帮助阻止未来恶意行为体的网络攻击，使整个数字生态系统更加安全。另一方面，国家对其公民负有保护国家安全、打击犯罪分子和网络空间其他恶意行为体的义务。各国利用对手使用的数字产品和服务中的漏洞实现其国家安全和公共安全使命。因此，如果各国认为利用漏洞是履行其责任的一种有效途径，它们也可能会发现故意在对手使用的产品和服务中引入漏洞或后门会有所帮助。反过来，非国家行为体也可能篡改产品和服务，因为它们破坏网络空间稳定性的能力可能有助于实现自身目标。值得注意的是，篡改产品或服务系列将危及网络空间的稳定性，本规范明确禁止此类行为。这一规范不会禁止对网络空间的总体稳定风险不大的有针对性的国家行动，例如，为了方便开展军事间谍活动或刑事调查需要，有针对性地拦截和篡改有限数量的最终用户设备。这类活动除非发生在公共核心自身基本基础设施内，或严重削弱全球用户对互联网的信任，否则不大可能削弱对网络空间的整体信任，而这种信任是网络稳定的一个条件。虽然非国家行为体也可能以有限的方式针对系统发起攻击，但这种活动可能违反现行刑法和民法。

虽然国家和非国家行为体不应断然篡改开发或生产中的产品，业内人士也有责任阻止此类活动。因此，产品和服务的创造者必须在产品和服务的设计、开发和产品交付和服务中尽到合理努力，将安全放在优先地位，从而降低出现漏洞的可能性、频率、可利用性和严重性。有关各方还必须拒绝任何明显破坏产品和服务的国家或非国家行为，采取措施降低篡改风险，并在发现篡改时允许他们作出响应。

4. 关于禁止将信息和通信技术设备纳入僵尸网络的规范

规范：

国家和非国家行为体不得征用公共信通技术资源来制造僵尸网络或将其用于类似目的。

背景

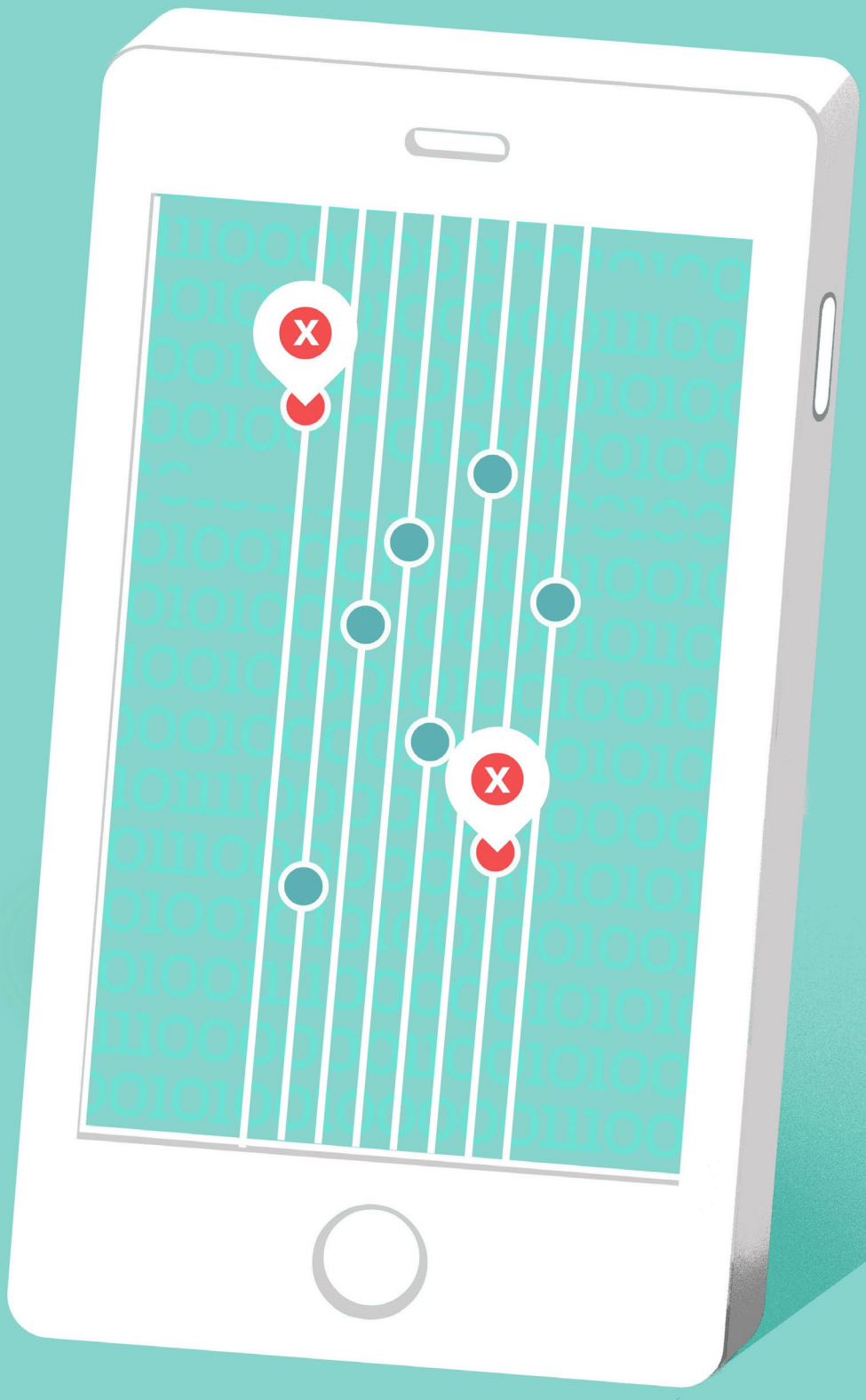
如今，互联设备已在全球范围内成为人们生活不可或缺的一部分。具有多种计算、网络、传感和驱动能力的设备充斥着每个角落。恒温器、电视、医疗设备、闹钟和汽车都有计算、存储和网络能力，而这些能力可能被盗用或滥用。利用底层代码中的漏洞可能会给使用设备的个人带来物理安全问题：在设计参数之外工作的设备可能起火或造成其他不安全的情况，例如门意外开锁、从室内播放视频或导致（医疗）设备故障。

我们所说的僵尸网络是指未经许可大量安装软件代理来使用设备的计算、存储或网络资源。然后，这些僵尸网络可以被用来对不同的目标系统产生直接影响，包括影响最终目标的数据保密性、可用性和完整性。因此，未参与行动的“第三方”设备及其所有人/操作人，可能会在不知情的情况下成为恶意网络活动的一方。为了安装恶意软件代理而对设备进行破坏，不仅削弱了设备对其他攻击（例如来自犯罪分子的攻击）的防御能力，或者损害设备的正常功能，而且还让人怀疑所有人/操作人是对最终目标造成损害的潜在罪魁祸首对于下列情形尤为严重：设备遭到损坏可能会无意中使设备及其所有人/操作人成为国家间敌对行动中的不知情交战方，从而招致报复或承担赔偿责任。

随着我们在个人环境中越来越依赖于技术，加之越来越多的互联设备进入市场，对消费类设备的利用以及将其作为僵尸网络，使公众信任和社会稳定不断遭到破坏。委员会承认，在某些情况下（例如为了执法目的），经授权的国家行为体可能认为有必要在专门针对的个别对手或一群对手的设备上安装软件代理。然而，国家和非国家行为体不应征用一般公众（集体）的民用装置，为开展攻击性网络行动提供便利，或者直接开展攻击性网络行动，不论其动机如何。[56]

56 本规范是对先前关于国家和非国家行为体避免在产品发布前对其进行篡改的拟议规范的补充，拟议规范侧重于供应链方面，而本规范针对已部署的设备。

5. 关于各国建立漏洞公平裁决程序的规范



规范：

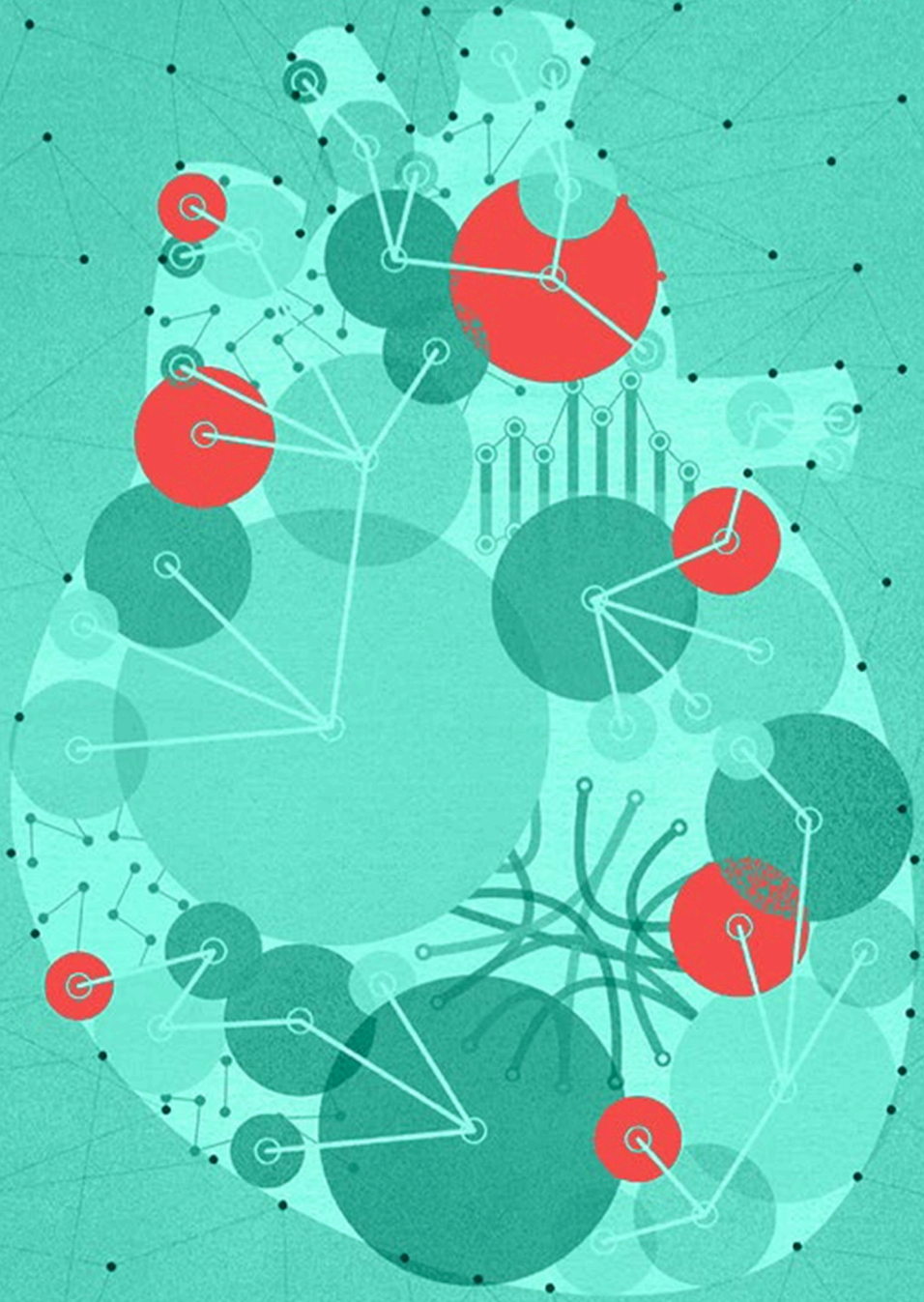
各国应建立一系列程序上透明的框架，以评估是否以及何时披露其所了解但不为公众所知的信息系统和技术漏洞或缺陷。默认的程序应有利于信息披露。

背景

随着操作系统、关键软件和计算机硬件越来越复杂，它们包含的漏洞也越来越多。国家和非国家行为体可能会利用这些漏洞。各国在处理新发现的漏洞时，有时在利益和责任上会相互冲突。一方面，他们有义务提高对网络空间稳定至关重要的基础设施的弹性和完整性，并帮助挫败恶意网络活动，使整个数字生态系统对所有用户更加安全。这就要求国家迅速向供应商和制造商披露新发现的漏洞，让供应商和制造商修补漏洞，并酌情扩大公开披露范围以保护公众。另一方面，各国有义务保护其公民免受犯罪分子的侵害，调查和起诉网络犯罪，并保留实施制裁的权利，这些制裁对未来的恶意活动既有具体的威慑作用，也有普遍的威慑作用。追捕恶意行为体，特别是流氓国家这种特别老练行为体的一个基本工具是利用它们所依赖的数字基础设施中的漏洞。 因此，各国经常辩称，它们必须至少保留某些选定的能力，包括可以使用未披露漏洞，否则将无法发现和遏制能力极强的恶意行为体。

虽然各国不太可能自愿披露其所发现的每一个漏洞，但一些国家最近已开始采取行动，不再假定所有未披露漏洞都会保留，而是假定为了更广泛的系统的网络安全，有必要进行披露。其中关键一环是各国建立一个公开描述的评估披露利弊的程序，该程序要全面考虑政策、经济、社会和技术平等因素。具体而言，这一程序应该透明化，并考虑到各方面意见，包括网络安全和抗风险能力、用户及其数据的安全、执法和国家安全效用以及外交和商业影响等因素。美国最近颁布了这一程序的最新版本，其他国家也在考虑制定自己的漏洞公平裁决程序 (VEP) 政策。鉴于发现和披露漏洞所涉及的范围并不局限于任何特定国家之内，为了提高网络抗风险能力，同时保障国家安全，每个国家都应该制定类似程序，才有利于保持网络空间的长期稳定。此外，各国应努力建立兼容和可预测的程序。这种程序的存在可作为国家间建立信任的措施，因为在某种程度上，可以保证相关权益和利益冲突得到充分考虑。当然，每个国家的能力各不相同，机构间结构也很独特，然而，任何有效的 VEP 程序设计都应集思广益，考虑相关权益。此外，虽然在个别案例中作出的实际决定可能有必要保密，但作出这种决定的一般程序和框架应该公开透明。最后，这一规范只涉及建立作出披露决定的程序。如果一国政府或其他任何实体决定披露，这种披露应以负责任的方式进行，有利于促进公共安全，而不会导致对上述漏洞的利用。

6. 关于减少和减轻重大漏洞的规范



规范：

网络空间稳定所赖以实现的产品和服务的开发者和生产者应当：(1) 重视安全性和稳定性；(2) 采取合理措施确保其产品或服务不存在重大漏洞；(3) 在发现漏洞时及时补救，并对这一过程保持公开、透明。所有行为体都有义务分享相关漏洞信息，以帮助预防或减少恶意网络活动。

背景

由于以下原因，某些 IT 产品和服务对网络空间的稳定至关重要：用于核心技术基础设施（如核心名称解析或路由）中；为用户互联网体验提供了广泛便利；用于关键的基础设施中。产品和服务的创造者必须在产品和服务的设计、开发和产品交付和服务中尽到合理努力，将安全放在优先地位，从而降低出现漏洞的可能性、频率、可利用性和严重性。

由于软件和硬件日益复杂，这些产品中的漏洞已成为不争的事实。虽然这些漏洞通常是无意间形成的，但不怀好意的国家和非国家行为体在发现这些漏洞时往往会加以利用，使网络空间的稳定性受到破坏。

而且，在一个高度互联、高度依赖的世界中，发现的漏洞可能会影响不同生产商和不同环境中的多种产品和服务。如果修补产品时不向其他人披露潜在漏洞，可能会对该产品起到保护，但不会保护网络空间的稳定性。负责开发、生产、安装或操作受漏洞影响的产品的人员通常最适合对漏洞影响进行评估。共享有助于修复安全漏洞或有助于阻止、限制或减轻攻击的信息非常重要。[57]

虽然目前很难确保新发布或更新的产品不存在漏洞，但这一拟议规范建议，参与开发或生产这类产品的人员应采取“合理步骤”，减少上述漏洞的发生频率和严重性。

“禁止篡改”规范针对故意在关键产品和服务中插入漏洞的问题，卫生规范规定了最终用户的义务，而本拟议规范则力求让关键产品开发商或制造商采取合理措施，确保最大限度控制关键漏洞的数量和范围，在发现漏洞时酌情予以披露，确保及时高效地减轻漏洞造成的影响。所使用的过程应该是透明的，以创造一个可预测的稳定环境。

57 联合国政府专家小组 2015 年报告 (A/70/174) 中关于各国负责任行为的规范之一申明，“各国应鼓励负责任地报告信息通信技术漏洞，并分享关于此类漏洞的可用补救措施的相关信息，以限制并尽可能消除对信息通信技术和依赖信息通信技术的基础设施的潜在威胁。”

7. 作为基础防御的基本网络卫生规范

规范：

各国应采取适当措施，包括颁布法律法规，确保基本的网络卫生。

背景

互联网已覆盖全球各个角落，渗透到现代生活的方方面面，无论是个人、组织、企业还是政府，各层级的用户都越来越依赖于技术和对互联网信息的获取。政治、经济、公共信息、教育、发展以及所有其他社会互动方式都严重依赖于互联网和相关技术。然而，作为现代奇迹之一的互联网，其带来的风险仍广泛存在，并且没有人能够幸免。

关于如何在保护公众的同时最有效地优化有前景的网络空间技术，各国尚未达成共识。然而，大多数人都认为，如果不能就网络空间的基本安全达成统一的标准，数字互联生活带给我们的好处就难以为继。为此，委员会强烈赞同广泛通过基本网络卫生制度并核实其实施情况，基本网络卫生制度是一套基本措施体系，代表着为了防御、预防和迅速减轻网络空间中可避免的危险而应优先完成的基本任务。

事实上，鉴于在线互联的广泛性，这些措施构成了所有用户都应该履行的基本注意义务。卫生制度应纳入可靠的实施措施，规定广泛分享技术信息和最佳实践，并接受适当监督。设备和流程的智能化程度日益加深，法律和法规的智能性也要随之提高。在为网络管理这一基本职责设立更多问责制度的同时，各国政府不应限制互联网创新或改变互联网的基本属性。

网络卫生标准已经以各种形式存在。[58] 随着各国政府和企业日益认识到采取措施帮助预防和迅速减轻已知恶意软件的危险的重要性，网络卫生标准已经获得了更广泛的国际认可。此外，这些标准代表了最佳实践，突显了合理、定期监督的重要性，并强调了在可能的情况下自动分享信息以提醒其他用户注意风险的重要性。这些方法中概述的基本网络防御措施说明了这样一个现实，即，没有哪一个政府、组织或用户群体能够单枪匹马地减轻与网络相关的所有风险。委员会还认识到，各级用户在加强网络安全方面发挥着重要作用。

GCSC 认为，通过广泛落实网络卫生制度进行基本的网络安全防御，对于负责任地使用互联网和互联网的有益发展已经变得至关重要。必须将安全视为一个持续的过程，由所有行为体共同分担责任，同时要建立自动报告和信息共享等机制，确保实现适当问责。

委员会还认识到，全世界许多社会在使用信息和通信技术方面面临巨大挑战，呼吁各国分享知识和提供能力建设，落实有效实施基本网络卫生制度的进程，扩大这一规范的影响。

58　例如，其中包括欧洲电信标准协会 (ETSI)、非营利组织互联网安全中心 (CIS) 和澳大利亚国防信号局 (ASD) 等。

8. 关于反对非国家行为体开展攻击性网络行动的规范

规范：

非国家行为体不得参与攻击性网络行动，国家行为体应对此类活动加以防范，并在发生时及时响应。

背景

信息和通信技术在积极改变社会的同时，也带来了新的安全挑战。网络行动的速度之快和覆盖范围之广，往往会给各国的司法系统和国际执法合作带来相当大的困难。尽管存在上述困难，但应当提请注意的是，国家主权是基于规则的国际和平与安全体系的基石。国家对合法使用武力拥有垄断权，但要受到国际法的严格约束。一些非国家行为体，主要是私营公司，主张有权跨越国界开展攻击性网络行动，可能声称这是一种必要的防御行动，因为国家没有能力充分保护它们不遭受网络威胁。这些非国家行为体的攻击性网络行动有时被委婉地称为“主动网络防御”，[59] 包括但不限于所谓的“黑回去”，因为它们是出于防御目的而进行的。

尽管这样做给网络空间的稳定和安全带来了风险，但一些国家对这些做法并不加以控制，或者可能置之不理。然而，在许多国家，这种做法即使不会受到刑事处罚，也属于非法行为，而在另一些国家，这种做法似乎既未被禁止，也未得到明确授权。然而，一些国家正在考虑将非国家行为体的攻击性网络行动合法化。事实上，有些国家已决定或提议通过国内立法，允许非国家行为体开展攻击性网络行动。

全球网络空间稳定委员会认为，这些做法破坏了网络空间的稳定性。这些做法可能造成严重的破坏和损害，包括对第三方的破坏和损害，因此，有可能引发复杂的法律争端，让冲突升级。国家若出于自身或第三方目的明确授权或故意允许非国家行为体开展攻击性行动，将开创一个危险的先例，并有违反国际法的风险。委员会认为，攻击性措施应仅限于国家，同时指出，国际法为国家应对敌对行为确立了一个严格的专属框架，该框架也适用于网络行动。同样，根据国际法的规定，代表国家行事的非国家行为体必须被视为国家代理人，因而被视为国家的延伸。[60]

因此，如果国家允许采取上述行动，则可以根据国际法追究其责任。[61] 各国必须从国内和国际两个层面采取行动，对非国家行为体开展的攻击性网络行动加以防范。

59　主动网络防御应该理解为一系列措施，无论是受害者网络上的自我防御，还是在攻击者网络上进行的破坏性活动，都属于此类措施。在本连续统一体中开展攻击性网络行动，意味着防御者可以在自己网络之外采取行动，而不受其意图（攻击或防御）及其行为是否合法的影响。攻击性网络行动与主动网络防御的定义还有待进一步商榷。

60　有关在国际法范围内对本案的更广泛处理意见，请参见“附加说明”，网址为：https://cybersta-bility.org/wp-content/uploads/2018/11/addergy-note-to-the-norm-ant-of-fensive-cyber-operations-by-non-state-actors-norm-packe-singapore.pdf。

61　同上。

附录 C：全球网络空间稳定委员会的历史、目标和程序

2017 年 2 月，在荷兰外交大臣 Bert Koenders 的支持下，全球网络空间稳定委员会在慕尼黑安全会议上正式成立。此后，该委员会一直被视为专门关注网络空间稳定的首批多利益相关方倡议组织之一。该委员会由美国前国土安全部部长 Michael Chertoff、印度前副国家安全顾问 Latha Reddy 担任主席（之前由欧洲议会议员、爱沙尼亚前外交部长 Marina Kaljurand 任主席），由来自不同地区以及与国际网络安全相关的具有不同背景的 28 名杰出人士组成。[62] 委员会得到了特别顾问、秘书处（*海牙*战略研究中心和东西方研究所）、一个研究咨询小组以及众多合作伙伴和主办单位的支持，其中包括荷兰外交部、法国外交部、新加坡网络安全局、微软公司、互联网协会和 Afilias。

成立委员会的初衷是希望延续先前民间团体委员会（包括互联网治理全球委员会）的工作，并与全球网络空间会议 (GCCS) 的工作对接。2015 年，*海牙*战略研究中心 (HCSS) 应邀组织 GCCS 海牙会议的筹备会议，专门讨论国际和平与安全问题。随后的 GCCS 宣言大部分直接借鉴了筹备会议的工作成果，明确指出需要采取多利益相关方模式来讨论国际网络安全问题。因此，HCSS 召集了一个由支持者和资助者（最初是微软公司、互联网协会和荷兰外交部）组成的核心小组，并制定了一项战略计划。2016 年 8 月，东西方研究所 (EWI) 以合作伙伴身份加入秘书处，HCSS 就此在哈佛大学肯尼迪政府学院召开了全球网络空间稳定委员会启动小组会议，会议起草了全球网络空间稳定委员会运作、会员、组织架构和目标及其使命宣言的主要要求。

使命宣言内容如下：

> 全球网络空间稳定委员会 (GCSC) 将编制相关规范和政策提案以加强国际安全与稳定，并指导国家和非国家行为体在网络空间中采取负责任的行为。GCSC 将使所有利益相关方参与其中以达成共识，并通过促进研究、信息交流和能力建设来维护网络稳定。

从设立之初，全球网络空间稳定委员的宗旨就是影响与网络空间有关的国际和平与安全议程，通常称为“国际网络安全”。启动小组认为，有必要在正在进行的国际网络安全讨论中征求各种意见，特别是来自互联网治理和技术界的意见。其目的是更好地为军备控制以及和平与安全界的审议提供信息，因为这些领域的许多优秀成果，特别是规范方面的成果，由于缺乏这些民间团体和私营部门行为体的意见和认可而遇

62 有关委员会完整名单，请参见第 4 页。

到阻碍。因此，多利益相关方模式所存在的问题不在于意识形态层面，而在于实际执行上。

全球网络空间稳定委员会采用“自下而上到自上而下”的方式开展审议工作。首先，对于成员所表达的最明显、最紧迫的并且在其他地方没有得到解决的国际网络安全需求，委员会确定了相应的规范。其次，通过这些现有规范确定网络稳定的有效定义及其基本原则。再次，制定了一个稳定框架，以便更清楚了解国际和平与安全架构需要做些什么才能符合这一定义要求。最后，它就如何实现这一目标向国家和非国家利益相关方提出了建议。

委员们为实现这些目标而进行的审议跨越了地域界限和利益相关方团体。从一开始，委员会就强调在相关会议的间隙举行会议，方便听取更多利益相关方的意见。[63] 此外，委员会还通过开展调查研究的方式向更广泛的社群征求意见。为了将全球网络空间稳定委员会的工作与更广泛的学术界联系起来，特设立了研究咨询小组，配备一名主席和四名副主席，[64] 负责管理涵盖超过 200 名专家的电子邮件列表。这也是一个范围广泛的研究项目的基础，项目最终委托来自世界各地的研究机构和个人进行了 20 多项研究。[65] 这项工作的大部分内容在专门的“网络稳定性听证会”上直接提交给委员们。

在发布本报告和以前颁布的规范之前，委员会一直在广泛征求政府、民间社会和行业利益相关方的意见。通过在委员会整个任期内错开提交，可以不断听取外部意见和评论。就全球网络空间稳定委员会规范和网络稳定性的定义发布了在线咨询请求。从世界各地行为体手中收到 23 份以上的材料，这些材料为委员们审议议案提供了信息。此外，委员会还积极参加了 70 多场会议和活动，并与众多国家和非国家利益相关方举行了圆桌会议、会外活动和专门的网络稳定听证会。

最后，委员们自己也与各自的社群保持着密切联系。这些团体的意见和反馈为与更大范围的国家和非国家专家群体进行互动提供了基本原则，并将为今后推广该报告奠定基础。

63　委员会在下列活动中举行了正式会议：2017 年慕尼黑安全会议（德国慕尼黑）；网络冲突国际会议（爱沙尼亚塔林）；美国黑帽大会（美国拉斯维加斯）；全球网络空间会议（印度新德里）；2018 年 FIC 国际网络安全论坛（法国里尔）；2018 年慕尼黑安全会议（德国慕尼黑 - 会议厅）；全球安全论坛（斯洛伐克布拉迪斯拉发）；以色列网络周（以色列特拉维夫 - 会议厅）；新加坡国际网络周（新加坡）；巴黎和平论坛暨互联网治理论坛（法国巴黎 - 会议厅）；2019 年联合国裁军研究所（瑞士日内瓦）；ICANN 64 社区论坛（日本神户）；欧洲互联网治理对话（荷兰海牙）；全球网络专家论坛年会（埃塞俄比亚亚的斯亚贝巴）。

64　涵盖四大专题领域，包括国际和平与安全、国际法、互联网治理和技术。

65　请参见“致谢”部分。

致谢

全球网络空间稳定委员会 (GCSC) 谨此感谢为本委员会工作提供支持、作出贡献和提供便利的众多机构和个人，包括但不限于我们的主办单位、研究咨询小组、研究论文作者和同行评审专家以及支持人员。以下是为委员会取得成功作出贡献的部分人员名单。

秘书处

*海牙*战略研究中心 (HCSS)

Alexander Klimburg，全球网络空间稳定委员会倡议和秘书处主任
Louk Faesen，全球网络空间稳定委员会秘书处项目经理
Elliot Mayhew，全球网络空间稳定委员会秘书处项目助理

以下人士也提供了支持：**Timon Domela Nieuwenhuis Nyegaard**、**Koen van den Dool**、**Niels Renssen**，以及 **Kaja Karlson**。

东西方研究所 (EWI)

Bruce W. McConnell，全球网络空间稳定委员会秘书处联合主任
Anneleen Roggeman，全球网络空间稳定委员会秘书处项目经理

以下人士也提供了支持：**Abagail Lawson**、**Dragan Stojanovski** 和 **Conrad Jarzebowski**。

合作伙伴、主办单位和支持单位

*海牙*战略研究中心、东西方研究所和委员们谨表彰并感谢下列组织的支持：

合作伙伴：

- **荷兰外交部**，**Timo Koster** 和 **Dimitri Vogelaar**
- **微软**， **Jan Neutze** 和 **Kaja Ciglic**
- **新加坡网络安全局**，**David Koh** 和 **Sithuraj Ponraj**
- **互联网协会 (ISOC)**
- **法国外交部**，**Henry Verdier** 和 **David Martinon**
- **Afilias**、**Ram Mohan** 和 **Philipp Grabensee**

主办单位：

- **瑞士联邦外交部**
- **全球安全论坛**
- **爱沙尼亚外交部**
- **日本总务省**

支持单位：

- **非洲联盟委员会**
- **美国黑帽大会**
- **极客大会**
- **欧盟常驻联合国日内瓦办事处代表团**
- **全球网络专家论坛**
- **谷歌**
- **海牙市**
- **Packet Clearing House**
- **特拉维夫大学**
- **联合国裁军研究所**

这些组织和机构致力于推进辩论，并针对网络空间稳定面临的一些最紧迫挑战提出创造性解决方案。

研究人员

委员会谨此感谢研究咨询小组的成员，该小组由 200 多名在线成员组成，为全球网络空间稳定委员会与广大学术界搭建了沟通桥梁。我们要特别感谢受托撰写简报和备忘录的研究人员，他们为委员会开展审议工作提供了资料。

全球网络空间稳定委员会问题简报第 1 期（2017 年 11 月）

Alex Grigsby，前外交关系委员会 (CFR) 成员
Deborah Housen-Couriel，康菲达斯数码有限公司
Joanna Kulesza，波兰国立罗兹大学和 **Rolf H. Weber**，苏黎世大学
Oluwafemi Osho、**Joseph A. Ojeniyi**，以及 **Shafi'i M.Abdulhamid**，联邦科技大学明纳分校
Analía Aspis，布宜诺斯艾利斯大学
Robert Morgus，新美国智库前成员，**Max Smeets**，前斯坦福大学国际安全与合作中心主任，以及 **Trey Herr**，哈佛大学肯尼迪政府学院
Arun Mohan Sukumar、**Madhulika Srikumar**，以及 **Bedavyasa Mohanty**，观察家研究基金会 (ORF)

全球网络空间稳定委员会问题简报第 2 期（2018 年 5 月）

Shen Yi、**Jiang Tianjiao** 和 **Wang Lei**，复旦大学网络空间治理研究中心
Elana Broitman、**Mailyn Fidler**，以及 **Robert Morgus**，新美国智库前成员
Elonnai Hickok 和 **Arindrajit Basu**，互联网与社会中心
Thomas Uren、**Bart Hogeveen**，以及 **Fergus Hanson**，澳大利亚战略政策研究所 (ASPI)
Dragan Mladenovi 和 **Vladimir Radunovi**，DiploFoundation
Thomas Reinhold，汉堡大学和平研究与安全政策研究所

磋商请求致谢名单

下列个人和组织就新加坡一揽子规范（从 2018 年 12 月 17 日到 2019 年 1 月 17 日）和网络空间稳定的定义（从 2019 年 8 月 14 日到 2019 年 9 月 6 日）的磋商请求提交了广泛的评论意见，委员会在此表示感谢：

Hussein Abul-Enein，Access Partnership
Kayode Akanni，DesignIT
Jonathan D. Aronson，美国南加州大学 (USC)
Aviram Atzaba，以色列国家网络安全局
Arindrajit Basu、**Gurshabad Grover**、**Elonnai Hickok**，以及 **Karan Saini**，因特网与社会中心
Vytautas Butrimas，北约能源安全卓越中心
网络安全技术协议
Michael Daniel，网路威胁情报联盟
全球数字合作伙伴
Arvind Gupta 和 **Dickey Kumar**，辩喜国际基金会
Tara Hairston 和 **Anastasiya Kazakova**，卡巴斯基
Sven Herpig，德国新责任基金会
Drew Mitnick，Access Now
George M. Moore，詹姆斯·马丁防扩散研究中心
Brett van Niekerk 和 **Trishana Ramluckan**，南非夸祖鲁-纳塔尔大学
Peter Swire、**Justin Hemmings** 以及 **Sreenidhi Srinivasan**，佐治亚理工学院谢勒商学院
Johan de Wit，西门子/荷兰代尔夫特理工大学

最后，委员会谨此感谢下列专家，他们的工作和专门知识为委员会开展审议工作提供了指导和参考：

Dennis Broeders，荷兰莱顿大学
Deborah Brown 和 **Verónica Ferrari**，进步通信协会
Michael Daniel，网路威胁情报联盟
François Delerue，法国军事学院战略研究所-IRSEM
Akhil Deo Arun Mohan Sukumar，观察家研究基金会 (ORF)
Martha Finnemore，美国乔治华盛顿大学
Aude Géry，法国鲁昂大学
Duncan Hollis，美国天普大学法学院
Joanna Kulesza，波兰国立罗兹大学
Peter Rowland,Packet Clearing House
Michael Schmitt，英国埃克塞特大学法学院

Patra Kongsirimongkolchai / EyeEm / Getty Images

秘书处

The Hague Centre for Strategic Studies

EastWest INSTITUTE

合作伙伴

Ministry of Foreign Affairs of the Netherlands

CSA SINGAPORE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

Microsoft

Afilias

主办单位

瑞士联邦外交部
全球安全论坛
爱沙尼亚外交部
日本总务省

支持单位

非洲联盟委员会
美国黑帽大会
极客大会
欧盟常驻联合国日内瓦办事处代表团
全球网络专家论坛
谷歌
海牙市
Packet Clearing House
特拉维夫大学
联合国裁军研究所

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE