互联网碎片化与网络安全：

入门指南

Samuele Dominioni 博士

要点概述

- 促进开放、安全、稳定、无障碍、和平的信息通信技术环境是联合国有关国际安全和信息通信技术（信通技术）安全多边进程的一个连续性目标。不限成员名额工作组（OEWG）本身正代表了就信通技术环境安全开展国际合作的重要里程碑。
- 互联网的基础设施依然稳定，基本保持开放和安全。然而令人担忧的是，互联网碎片化现象日益突出。关于碎片化，利益攸关方性质不同，理解方式也不相同。不过，这里还是可以从技术层面予以区分。碎片化可能对互联网中保障网络和设备互操作性的关键组成部分造成影响。
- 互联网碎片化的技术层面主要涉及寻址、命名和路由三个主要关切领域。其中，一些领域和必要的创新有关，多利益攸关方为应对日益增加的信通技术使用而必须进一步完善且仍未得到充分实施（如 IPv4 和 IPv6）的创新；另一些领域则涉及从现行国际标准和协议分化而来的关键技术组件的发展新趋势（如域名系统）；最后，还有一些领域涉及互联网关键组件（如路由）设计和发展中的技术缺陷或局限性。
- 这些碎片化的领域不仅损害了全球互联网的开放性、稳定性和可及性，还对网络安全产生了影响。其中一些领域涉及标准和协议本身（如路由协议）的网络安全，这些标准和协议可能受到各种恶意信通技术活动的影响。另一些领域危及数据的可及性、可用性和安全性（如可替换名称系统）。总之，由于互联网结构的复杂性和相互依赖性，技术层面的碎片化会给网络安全带来复杂、多方面的风险（即所谓的“恶性问题”）。
- 今后的研究将探讨本入门指南中确定的风险领域和趋势如何影响网络空间负责任国家行为框架的实施，进而影响国际和平与安全。

导言

促进开放、安全、稳定、无障碍及和平的信通技术环境是联合国有关国际安全和信通技术安全多边进程的一个连续性目标。例如，2021 年政府专家组（GGE）关于从国际安全的角度推动网络空间负责任国家行为的最终报告申明，“一个开放、安全、稳定、无障碍、和平的信通技术环境对所有国家都至关重要，需要各国开展有效合作，以降低对国际和平与安全的风险”。[1]不限成员名额工作组（OEWG）关于从国际安全的角度看信息和电信领域的发展的最终报告回顾中提到，“不限成员名额工作组（OEWG）代表了为建设一个开放、安全、稳定、无障碍及和平的信通技术环

[1]联合国大会，2021 年，A/76/135，https://undocs.org/Home/Mobile?FinalSymbol=A%2F76%2F135。

境而开展国际合作的重要里程碑”。[2]此外，两份报告均强调了保护互联网的普遍可用性和完整性关键性技术基础设施至关重要。[3]设立本届不限成员名额工作组（2021--2025 年）的联大决议确认“政府专家组（GGE）在其 2013 年和 2015 年报告中得出的结论是，国际法，特别是《联合国宪章》，对于维护和平与稳定，以及促进开放、安全、稳定、无障碍与和平的信通技术环境是适用的，也是必不可少的”。[4]然而，信通技术环境的碎片化，特别是互联网碎片化的问题属性日益凸显，并已在某些特定情况下有所显现。事实上，互联网碎片化会在不同层面，有时甚至是相互交织的层面产生影响，比如政治、商业和技术层面。[5]越来越多的国家和利益攸关方对互联网碎片化的情况表示担忧。联合国秘书长的报告《我们的共同议程》将避免互联网碎片化列为一项需要考虑的行动，这也是即将纳入《全球数字契约》的主要议题之一。

这本入门指南是有关互联网碎片化和国际安全的更广泛项目的第一项成果，旨在介绍互联网碎片化这一主题，并概述广义上的网络安全可能面临的主要挑战。在第一项成果的基础上，研究项目的第二部分将探讨互联网碎片化如何影响国际安全，特别是《网络空间负责任国家行为框架》（以下简称《框架》）的实施。本入门指南旨在为政策制定者、外交官和其他非技术相关人员提供有关互联网碎片化发展及其对网络安全的影响的介绍性概述。本文涉及的材料来自公共可用资源、专家访谈（2023 年 9 月至 11 月期间），以及 2023 年 10 月 17 日与私营部门、学术界和民间社会发言人举行的多利益攸关方在线对话。

什么是互联网碎片化

互联网碎片化是一个有争议的概念，利益攸关方性质不同，可能会有不同的解释。尽管如此，根据某些学者的研究，可以发现从三个层面理解互联网碎片化是一种趋势，这是指技术、商业和政府碎片化。[6]其他学者则对从三个层面理解碎片化持略有不同的见解。[7]由于本入门指南侧重于互联网碎片化对网络安全的影响，因此主要从技术层面展开分析。[8]

[2]联合国大会，2021 年，A/75/816，https://undocs.org/Home/Mobile?FinalSymbol=A%2F75%2F816。
[3]2021 年政府专家组（GGE）报告称，“互联网的普遍可用性或完整性”。见联合国大会，2021 年，A/76/135，第 10 段。
[4]联合国大会，2020 年，A/RES/75/240，https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf。
[5]William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, 2016,《互联网碎片化：概述》，《互联网未来倡议白皮书》，世界经济论坛，https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf。
[6]同上。
[7]例如，IGF 互联网碎片化政策网络关于互联网碎片化的讨论文件使用了以下维度：用户体验的碎片化、互联网技术层的碎片化以及互联网治理和协调的碎片化；PNIF，2023，PNIF 讨论文件（对 IGF2023 的投入），9 月 15 日，https://www.intgovforum.org/en/filedepot_download/256/26218。
[8]今后的出版物将考虑政治和商业碎片化对网络安全的影响。

根据世界经济论坛（WEF）关于互联网碎片化的白皮书，当"底层基础设施（即互联网层）中存在阻碍系统充分互操作、交换数据包以及互联网在各端一致运行的条件"时，就会出现技术碎片化。[9]专栏 1 简要介绍了互联网各层及其功能。

专栏 1：互联网层。

开放系统互联（OSI）和传输控制协议/互联网协议（TCP/IP）模型是划分互联网分层结构最常用的方法之一。这些模型通常表示为垂直堆栈。每一层都承担着不同但相互关联的功能，这些功能将信息（如浏览器中的文本查询）转化为数据包，使两个（或多个）设备之间的通信成为可能。

开放系统互联（OSI）模型包含七层：应用层、表示层、会话层、传输层、网络层、数据链路层和物理层。

1. **应用层**为使用互联网的网络应用程序提供服务，如浏览器、电子邮件和电信应用程序。
2. **表示层**，将来自应用层的信息格式化，以便显示（若接收）或进一步处理（若发送）。
3. **会话层**，进行身份验证和授权的过程。例如，进行身份验证（即登录应用程序），以在用户和应用程序服务器之间建立连接，从而启动会话。
4. **传输层，**确保设备和网络之间通信的可靠性。实现这种“传输”的主要协议有两个，即传输控制协议（TCP）和用户数据报协议（UDP）。TCP 协议用于建立连接，在设备间提供可靠的信息传输，但传输速度可能较慢。第二种协议，即用户数据报协议（UDP），用于要求传输速度更快，但对数据传输准确性要求较低的连接（如流媒体视频）。
5. **网络层，**为不同网络之间的设备提供数据传输服务。该层的功能之一是逻辑寻址，将每个用户的 IP 地址附加到数据包上，以确保数据包能到达正确的目的地。之后，这些数据通过路由器从一个网络传输到另一个网络。网络层通过路径选择找到最佳的数据传输路径。
6. **数据链路层，**帮助准备在不同网络之间发送的信息，并尽量防止在下一层传输过程中可能出现的错误。
7. **物理层**，开放系统互联（OSI）模型的最后一层，将数据转换成二进制代码，再转换成信号，经本地介质进行传输（或反过来转换，用于接收数据包），本地介质是设备之间的物理连接（如电缆、光纤或无线电波）。

TCP/IP 与开放系统互联模型相似，但将开放系统互联模型中的应用层、表示层和会话层合并为一层，在 TCP/IP 模型中称为应用层。其余层的名称与 OSI 模型中的层相同，即传输层、网络层、数据链路层和物理层。

<table>
<tr><th><u>开放系统互连 OSI</u></th><th><u>TCP/IP</u></th></tr>
<tr><td>应用
(人机交互）</td><td rowspan="3">应用
(数据呈现、编码和会话控制）</td></tr>
<tr><td>表示
(数据表示和加密）</td></tr>
<tr><td>会话
(主机间通信）</td></tr>
<tr><td>传输</td><td>传输</td></tr>
</table>

[9]William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, 2016,《互联网碎片化：概述》，《互联网未来倡议白皮书》，世界经济论坛，https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf，第 14 页。

	(TCP 和 UDP）	(TCP 和 UDP）	
	网络 (路由和 IP 地址）	**网络** (路由和 IP 地址）	
	数据链路 (错误修复和重传）	**数据链路** (错误修复和重传）	
	物理 (通过电子、光学或无线电波发送数据）	**物理** (通过电子、光学或无线电波发送数据）	

事实上，互联网之所以能够作为一种开放的全球公共产品发挥作用，是因为互联网的基础设施和属性允许任何人在任何地方通过任何设备连接到互联网，进行通信和信息交换（以数据包的形式）。其中一些关键组成部分可以确保网络和设备的互操作性（见专栏 2）。

专栏 2：互联网的关键组成部分。

以下倡议有助于着重指出了互联网的关键组成部分的构成。

全球网络空间稳定委员会提出了互联网公共核心的概念，其中包括

1. 数据包路由和转发
2. 命名和编号系统
3. 安全和身份的密码机制
4. 传输介质
5. 软件
6. 数据中心[10]

国际互联网协会提出了定义互联网网络基本功能的五个关键属性：

1. 无障碍基础设施，采用开放、门槛低的通用协议。
2. 基于用户社区自愿采用的开放式标准开发流程，互操作和可重用构件的开放式架构。
3. 分散式管理和单一分布式路由系统，具有可扩展性和灵活性。
4. 通用全球标识符，具有明确性和通用性。
5. 技术中立的通用网络，简单且适应性强。[11]

互联网治理论坛关于互联网碎片化政策网络（PNIF）的讨论文件称，互联网技术基础设施的碎片化与“保证互联网运行的技术传输层互操作性面临的一系列挑战”有关。[12]的确，全球互联网“基本上以互联网传输层的设计和相同技术协议（TCP/IP、DNS、BGP、HTTP、IPv4 和 IPv6 等）的共同使用为根本，以各种互联网通信所用的统一但分散的根服务器系统为基础”。[13]因此，由

[10]全球网络空间稳定委员会，“推进网络稳定”，2019 年 11 月，https://hcss.nl/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf。
[11]互联网协会，“互联网联网方式：定义互联网的关键属性”，2020 年 9 月，https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/。
[12]PNIF,2023,PNIF 讨论文件（对 2023 年互联网治理论坛的投入），9 月 15 日，https://www.intgovforum.org/en/filedepot_download/256/26218，第 12 页。
[13]Wolfgang Kleinwächter 和 Alexander Klimburg，2023 年，《碎片还是完整——这是一个问题吗？一个世界——一个互联网“能否经受住今天的地缘政治压力测试？”，Circle ID，6 月 6 日，

于互联网关键组成部分的这一基本特征，指向技术层面碎片化的行动将对互联网的开放性和互操作性构成最严重的威胁。

技术层面互联网碎片化的风险领域

技术碎片化是一个频繁出现的问题，尤其是对互联网关键组成部分的多利益攸关方群体而言。世界经济论坛 2016 年发布的《互联网碎片化白皮书》称，“互联网仍然稳定，基本保持开放和安全”。[14]将近八年过去，对于技术而言一个不短的时间跨度，尽管脆弱性和风险与日俱增，但这些基础依然稳固。[15]为了与现有文献，特别是世界经济论坛白皮书保持一致，本入门指南所使用的风险领域与其保持一致，即互联网的寻址、命名（域名系统）和路由（互联），[16]，来确定当前削弱互联网基础的各种趋势。

寻址

寻址与唯一标识符有关。唯一标志符也称为 IP 地址，以十进制值表示，用于指定互联网上的唯一服务点。IP 和碎片化存在两个主要问题，第一个问题与两个版本的 IP（IPv4 和 IPv6）的采用和兼容性有关，第二个问题与 IP 号码的管理有关。

互联网协议（IP）寻址主要有 IPv4 和 IPv6 两个版本。IPv4 由 32 位地址空间组成，最多可生成约 43 亿个地址。由于互联网上的终端（如设备）在过去几十年中急剧增加，IPv4 的可能组合地址逐渐枯竭。因此，为了满足更多的唯一标识符需求，推出了具有 128 位地址空间的新版 IP（IPv6）。IPv6 可覆盖多达 340 兆兆端点[17]。但是，IPv4 和 IPv6 不能直接互操作。这意味着 IPv4 网络上的设备无法与 IPv6 网络上的设备通信。[18]只有通过双栈网络等过渡技术才能实现兼容性。如果过渡技术无法支持世界各国和各地区之间的 IP 版本不一致，就会出现碎片化。IPv6 的采用正在稳步提高[19]，但各国之间存在差异。

---

https://circleid.com/posts/20230606-fragment-or-not-fragment-is-this-the-question-will-one-world-one-internet-survive-todays-geopolitical-stress-tests。

[14]William J. Drake,Vinton G. Cerf,and Wolfgang Kleinwächter, 2016,《互联网碎片化：概述》，《互联网未来倡议白皮书》，世界经济论坛，https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf，第 8 页。

[15]2023 年 10 月 26 日，采访世界经济论坛《互联网碎片化白皮书》作者之一 VintonG.Cerf 博士。

[16]理解寻址、命名和路由的一个简单方法是将这些术语理解为“寻址表示我们在寻找什么，地址表示它在哪里，而路由则告诉我们如何到达那里”；John F. Schoch，1978 年，"A Noteon Inter-Network Naming, Addressing, and Routing"，InternetExperimentNote#19，NotebookSection2.3.3.5，https://www.rfc-editor.org/ien/ien19.txt。

[17]WilliamJ.Drake,VintonG.Cerf,andWolfgangKleinwächter,2016,《互联网碎片化：概述》，《互联网未来倡议白皮书》，世界经济论坛，https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf。

[18]Erik Bais，“IPv4vsIPv6：安全专业人员应知”，Prefix Broker，https://www.prefixbroker.com/news/ipv4-vs-ipv6-what-security-professionals-should-know/。

[19]《世界经济论坛白皮书》发布时，IPv6 连接仅占互联网的 4%，而到 2023 年 10 月，这一比例将达到 40% 左右（来源：https://www.google.com/intl/en/ipv6/statistics.html）。

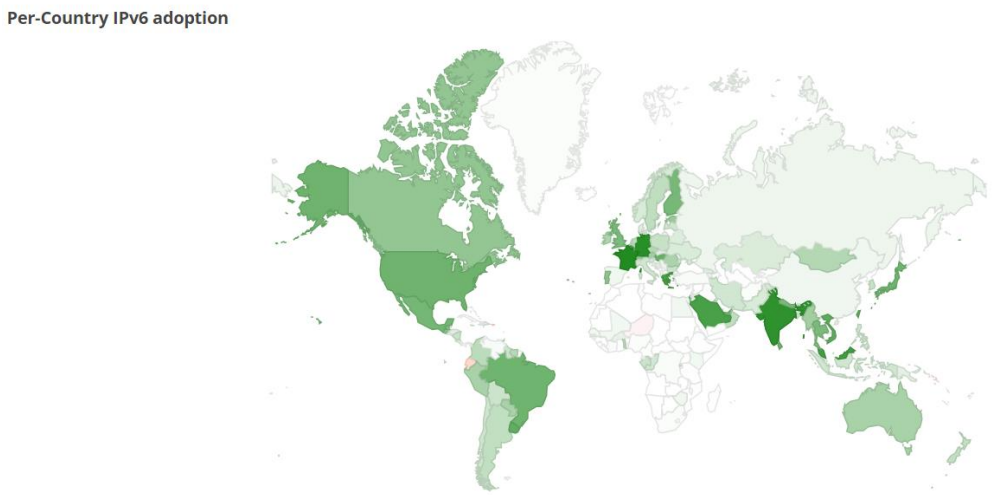

图 1：各国的 IPv6 采用情况--颜色越深，表示 IPv6 连接越多（来源：Google Statistics）

因此，在数字鸿沟的这一层面出现碎片化是可能的，并且，碎片化对各国和各地区网络和设备的整体互操作性构成风险。

IP 碎片化的第二个方面涉及 IP 地址所用 IP 号码的管理。在目前的互联网状态下，这项任务由互联网名称与互联网号码分配局（IANA，互联网名称与数字地址分配机构（ICANN）的附属机构）和区域互联网寻址机构（RIR）共同管理，并在广义区域内贯彻实施，因为互联网结构并不局限于国界。关键的是需要有一个负责 IP 全球唯一性的系统；否则，就有可能产生与现有已部署的基于 IPv4 或 IPv6 的基础设施难以兼容甚至无法兼容的其他无法协调的 IP 地址。[20]

命名

命名是指域名系统（DNS）。域名系统将域名转换为 IP 地址（例如，联合国裁军研究所（裁研所）网站的 DNS 是 https://unidir.org，其对应的 IP 是 34.107.109.130）。为保障这一功能，这一独特的映射和配对任务（由 ICANN 执行）的管理必须保持稳定、一致且合法。试图建立替代域名系统（包括根区的管理[21]）是碎片化的最糟糕形式之一[22]，因为将丢失独特的 DNS 转换。这将导致矛盾和潜在的 DNS 查询错误；例如，不同用户输入 https://unidir.org 可能会打开其他页面，而不是想要打开的页面。

路由

路由是指用于确保信息在网络中传输时遵循正确和最佳轨道的协议。如果信息需要从一个网络传输到另一个网络（互联网由许多不同的网络组成，通常由一个服务提供商单独管理），则边界网关协议（BGP）将不同网络连接起来，从而实现互联网的全球路由。正如世界经济论坛白皮书所

[20]例如，参见围绕“新知识产权”提案的辩论：Alain Durand，2020 年，“新 IP”，ICANN 首席技术官办公室，https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf。
[21]根区是 DNS 层次结构的顶级部分（tlp）（例如，在 https://unidir.org 中，tlp 为“.org”）。
[22]关于互联网碎片化和网络安全的多利益攸关方对话，2023 年 10 月 17 日；William J. Drake、Vinton G. Cerf 和 Wolfgang Kleinwächter，2016 年，《互联网碎片化：概述》，《互联网未来倡议白皮书》，世界经济论坛，https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf。

指出的，“从技术上讲，故意或意外破坏路由数据的情况依然有可能发生”[23]。路由系统的安全性仍需改进，例如，通过落实资源公钥基础设施（RPKI），该设施是一个旨在确保边界网关协议（BGP）安全的公钥基础设施框架。[24]总之，如果边界网关协议（BGP）没有得到充分保护，就会因为网络无法保证数据的机密性、完整性和可用性而出现碎片化。

网络安全的关注领域

本入门指南不仅重点关注了解互联网碎片化及其现状，还关注确定可能的网络安全影响。本入门指南基于网络安全三要素[25]和真实性，从非常全面的角度看待网络安全问题。一般来说，互联网的碎片化会给网络安全带来多种风险，其中可能包括所谓的“棘手问题”。这些问题尤其见于复合、互联、多利益攸关方的领域或局域（如互联网），且可能极其复杂而变化万千。[26]应对这些棘手问题，通常需要采用多利益攸关方合作的方法，涉及不同参与者、部门和国家之间的合作。（见表 1）。[27]因此，“一个碎片化的互联网阻碍了处理网络安全问题的任何可能机会，因为它不考虑许多相互依存的因素，并关闭了进行任何潜在合作的通道”。[28]此外，将互联网碎片化为更小的网络可能会降低网络的整体复原力。这是因为，互联网的优势在于它分散且建立在可互操作的组件（如标准和协议、设备等）之上，这一优势允许技术界在需要时能够在不影响整个网络的情况下解决问题。[29]

类型	**特点**	**解决路径**
简单	已知解决方案或解决方案的设计方法	合作：提高认识和信息共享，通常通过网络运营商集团进行
复杂	没有已知的解决方案；问题横跨互联网的多个部分	共识：制定基于共识的开放式标准
棘手	在任何领域都没有解决方案；对问题的存在或特征普遍缺乏共识	协作：超越现有领域和组织的界限，制定确定问题和解决方案的流程

[23]同上，第 23 页。
[24]与《白皮书》作者之一 Vinton G. Cerf 博士的访谈，2023 年 10 月 26 日。
[25]三要素关注数据的安全性，三要素指的是数据的保密性、可用性和完整性。可用性是指数据必须在需要时随时提供给授权用户；任何可能延迟用户访问数据的事件都会影响数据的可用性。保密性是指数据的访问；只有授权用户才能访问特定数据，否则数据必须保持保密或不公开。完整性涉及数据的真实性、可靠性和可信性；这意味着数据不应被篡改。见 Samuele Dominioni 和 Giacomo Persi Paoli，2022 年，"A Taxonomy of Malicious ICT Incidents"，联合国裁军研究所，https://unidir.org/publication/a-taxonomy-of-malicious-ict-incidents/。
[26]大多数严重的恶意信息和通信技术事件都具有跨界性质，涉及不同部门和地域的多种资产和行为者。
[27]Leslie Daigle、Konstantinos Komaitis 和 Phil Roberts，2016 年，《成功合作和解决棘手互联网问题的关键》，互联网协会，https://www.internetsociety.org/resources/doc/2017/keys-to-successful-collaboration-and-solving-wicked-internet-problems/。
[28]Konstantinos Komaitis，2023 年，《互联网碎片化：为什么对欧洲很重要》，《焦点研究》，欧盟网络直通车——欧盟网络外交倡议，https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/ioyLip9O/internet-fragmentation-why-it-matters-for-europe.pdf，第 8 页。
[29]作者与 Konstantinos Komaitis 的访谈，2023 年 11 月 9 日。

表 1：问题类型（来源：Leslie Daigle、Konstantinos Komaitis 和 Phil Roberts “成功合作和解决棘手问题的关键”，互联网协会，2016 年）

以下标题强调了所确定的每个碎片化领域的安全问题。

寻址

寻址碎片化对网络安全有两大影响。首先，IPv6 在全球的分散采用，不仅可能因两种 IP 模式的直接不兼容而导致碎片化，还可能因受信通技术威胁的程度不同而出现矛盾。IPv6 的主要特点包括集成了互联网协议安全（IPsec），[30]可以提供更高的安全性。[31]不过，IPv6 的实施和配置可能比 IPv4 更具挑战性，需要特定的技术知识和技能。配置 IPv6 设备时出现错误可能会带来漏洞，从而使设备更易遭到攻击。[32]此外，双协议栈（即同时运行 IPv4 和 IPv6）的设备和网络可能因攻击面增加而产生额外的安全问题。[33]

其次，与现有系统无法协调或截然不同的国际 IP 的开发或许很遥远但却存在可能，这将严重破坏全球可及性和国家网络的安全。事实上，在这种情况下，各国需要与互联网服务提供商签订双边协议，并确保为本国网络制定安全标准和协议。并非所有国家都具备实现同等安全水平的能力。目前，每个国家都可以依赖致力于开发、讨论和更新适用所有国家的标准和协议的开放性多利益攸关方群体。

命名

命名层面的碎片化出现于开发替代域名系统，这将导致巨大的网络安全故障。例如，在这种情况下，当用户输入一个网站的名称时，可能无法进入预期的网站，或最终进入另一个网站。总之，在替代域名系统下，用户将无法访问数据，而数据也将无法使用。此外，多利益攸关方将 DNS 与替代域名系统连接起来的尝试可能导致“不可预知的结果、用户挫败感、支持成本上升，最终，导致互联网安全性和稳定性降低”。[34]

路由

边界协议很容易受到黑客攻击，遭遇数据流篡改。事实上，边界网关协议（BGP）防范修改甚至删除数据的恶意行为的内部机制有限，因而会破坏整体网络路由行为。[35]事实上，边界网关协议（BGP）

[30]IPSec 是一种在互联网层提供信道安全的标准。IPSec 是 IPv6 的强制标准，而 IPv4 则是可选标准。参见互联网工程任务组(IETF)，2011 年，“IPv6 节点要求，征求意见 6434”，https://www.rfc-editor.org/rfc/pdfrfc/rfc6434.txt.pdf。

[31]Emre Durda 和 Ali Buldu，2010 年，《IPV4/IPV6 安全与威胁比较》，Procedia-SocialandBehavioralSciences2，www.sciencedirect.com/science/article/pii/S187704281000902X，第 5285-5291 页。

[32]国家安全局，2023 年，《IPV6 安全指南》，U/OO/105622-23|PP-22-1805,ver.1.0，https://media.defense.gov/2023/Jan/18/2003145994/-1/-1/0/CSI_IPV6_SECURITY_GUIDANCE.PDF.

[33]同上。

[34]Alain Durand，2022 年，《替代域名系统面临的挑战》，OCTO-034，ICANN，https://www.icann.org/en/system/files/files/octo-034-27apr22-en.pdf。

[35]IETF，2006，RFC#4272，“BGP 安全漏洞分析”，https://datatracker.ietf.org/doc/html/rfc4272。

很容易受到各种严重的信通技术威胁，包括可能导致互联网碎片化和造成破坏性或利用性影响的路由劫持[36]。[37]大多数情况下这种影响的程度和范围有限；但在有些时候，可能会造成毁灭性的通信故障。[38]落实资源公钥基础设施（RPKI）可以成为一项有效的网络安全措施。

结论和今后的计划

互联网的基础依然稳定，基本保持开放和安全。然而，各个层面的脆弱性和风险都在不断增加。互联网在技术层面上的碎片化可能会破坏一个开放、安全、稳定、无障碍、和平的信通技术环境，对网络安全产生巨大影响。

令人担忧的趋势尚存，这些趋势表明，与主要技术性国际标准和协议截然不同的做法和政策可能会增加，给网络安全带来一些挑战。因此，任何和单方面篡改互联网关键组成部分的企图都可能进一步加剧已经发生的碎片化，并破坏网络安全、互联网安全、及其他安全。事实上，互联网碎片化不仅会影响网络安全，还会影响国际安全。今后的研究将探讨本入门指南中所确定的风险领域和趋势如何影响框架的实施，进而影响国际和平与安全。

总之，为了确保一个开放、安全、稳定、无障碍、和平的信通技术环境，包括会员国在内的多利益攸关方群体应考虑保护互联网关键组成部分的完整性、可用性和相互关联性。要做到这一点，关键是要评估这些组成部分的相互依存性，以及篡改这些复杂而又相互关联的系统会给这一全球人类公域带来的连锁反应。本入门指南正在为此做出努力。

---

[36]这种情况发生时，犯罪者通过虚假宣布一个 IP 地址来恶意改变互联网流量的路由，实际上将互联网流量引向了另一个地址。换句话说，“BGP 劫持就好比有人把高速公路上的所有标志都换掉，然后把汽车重新导向错误的出口”；Cloudflare，“什么是 BGP 劫持”，https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/。

[37]每个网络事件都会对目标产生影响，主要影响有两大类：破坏性影响，指干扰通信技术功能；利用性影响，指窃取信息。见 Samuele Dominioni 和 Giacomo Persi Paoli，2022 年，"A Taxonomy of Malicious ICT Incidents"，联合国裁军研究所，https://unidir.org/files/2022-08/UNIDIR_Taxonomy_of_Malicious_ICT_Incidents.pdf；Charles Harry 和 Nancy Gallagher，2018 年，"Classifying Cyber Events"，Journal of Information Warfare，第 17 卷，第 3 期，https://unidir.org/files/2022-08/UNIDIR_Taxonomy_of_Malicious_ICT_Incidents.pdf，第 17 页。3，https://www.jstor.org/stable/26633163，第 17-31 页。

[38]“例如，网上银行、股票交易和远程医疗等关键应用都在互联网上运行”；Kevin Butler 等人，2010 年，《BGP 安全问题和解决方案调查》，《电气和电子工程师学会论文集》，第 98 卷，第 1 期，https://ieeexplore.ieee.org/abstract/document/5357585，第 100-122 页。

致谢

裁研所核心资助者的支持为研究所的所有活动奠定了基础。本出版物由欧盟资助，是联合国裁军研究所安全与技术计划的一部分，该计划得到了捷克、德国、意大利、荷兰和瑞士政府以及微软公司的支持。作者感谢来自业界、政府和学术界的众多专家，他们对本文的不同版本和章节提供了实质性反馈，并参与了多利益攸关方研讨会，其中包括 Ang Benjamin、Jaya Baloo、Vinton Cerf、Alain Durand、Marie Humeau、Konstantinos Komaitis、Allison Mankin、Kevin Reifsteck、Rob Spiger、Bill Woodcock 和 Michael Zappa。Elia Smith 是安全与技术专业的一名研究生，为该研究项目做出了贡献。

关于联合国裁军研究所

联合国裁军研究所（裁研所）是联合国内一个自愿出资的自主机构。裁研所是世界上为数不多的以裁军为重点的政策研究所之一，它就裁军与安全问题提供知识并促进对话和行动。裁研所总部设在日内瓦，协助国际社会提出切实可行的创新想法，以找到解决重大安全问题的办法。

引用

S. Dominioni. Internet Fragmentation and International Security. Exploring the Cyber security Implications. Geneva, Switzerland：联合国裁军研究所，2023 年。

备注

本出版物所使用的名称和材料的编排方式并不意味着联合国秘书处对任何国家、领土、城市或地区或其当局的法律地位，或对其边界或界线的划分表示任何意见。出版物中表达的观点仅由作者本人负责。它们不代表联合国、裁研所、欧洲联盟及其工作人员或赞助者的观点或意见。