

**涉足油流**

**海底通信电缆和  
负责任的国家行为**

卡米诺·卡瓦纳

## 致谢

裁研所核心资助者的支持为该研究所的所有活动奠定了基础。本报告是裁研所安全与技术方案领导的网络工作流的一部分，该方案由捷克、法国、德国、意大利、荷兰、瑞士、英国政府以及微软公司资助。作者对来自工业界、政府和学术界的众多专家表示感谢，他们对本文的不同版本和章节提供了实质性的反馈意见。

## 关于裁研所

联合国裁军研究所（裁研所）是联合国内部一个由自愿捐款供资的自主机构。裁研所是世界上为数不多专注于裁军的政策研究所之一，提供裁军与安全方面的知识，并促进这方面的对话和行动。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。

## 引文

C.卡瓦纳《涉足浊流：海底通信电缆和负责任的国家行为》。瑞士日内瓦：裁研所，2023年。

## 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，不一定反映联合国、裁研所、其工作人员或赞助者的观点或意见。

## 目 录

关于安全与技术方案.....	2
缩写与缩略语.....	3
执行摘要.....	4
导言.....	5
现代海底通信电缆包含哪些组成部分？.....	7
威胁和脆弱性.....	12
海底通信电缆管理制度.....	17
海底电缆治理去向何方？.....	21
对特定工作的分析.....	22
助力全球海底电缆系统提升韧性.....	25
结束语.....	27

## 关于安全与技术方案

当代科学技术的发展为国际安全与裁军带来了新的机遇和挑战。裁研所的安全与技术方方案（SecTec）力求建立对特定技术创新的国际安全影响和 risk 的了解和认识，并召集利益攸关方共同探讨思路，开发应对这些挑战的解决方法。

## 关于作者

**卡米诺·卡瓦纳（Camino Kavanagh）博士**是伦敦国王学院的高级客座研究员，也是卡内基国际和平基金会的非常驻学者。她还担任网络、新兴技术、国际安全和冲突等问题的国际顾问。卡米诺曾担任 2019-2021 年信息和通信技术与国际安全问题不限成员名额工作组（OEWG）和政府专家组（GGE）主席顾问，以及2016-2017年同一主题由政府专家组报告员/顾问。

## 缩写与缩略语

<b>GGE</b>	政府专家组
<b>ICPC</b>	国际缆线保护委员会
<b>ICT</b>	信息和通信技术
<b>OEWG</b>	不限成员名额工作组
<b>UNCLOS</b>	《联合国海洋法公约》

## 执行摘要

本报告系关于海底通信电缆。这些电缆是信息和通信技术生态系统的重要组成部分，几乎承载了我们所有的电信和数据传输。它们的安全性和韧性对于全球社会的福祉和运作以及国际安全与稳定至关重要。技术进步使海底通信电缆的数据传输速度达到了约 150 年前将首条电缆铺设在海床上时难以想象的水平。这些进步不仅连接了历史上偏远或被忽视的国家和地区，结合其他努力，有望带来急需的社会和经济红利。此外，这些进步还为科学研究，包括对了解影响地球的环境变化至关重要的研究赋能。然而，全球海底通信电缆网络及其传输的数据正面临风险。

本报告指出，迫切需要加快努力以增强这一关键基础设施及其物理、网络和数据层的韧性。报告充分注意到国家支持的活动可能对海底电缆、陆地电缆或网络电缆造成的影响，以及许多政策决策对海底电缆投资和路由选择的影响。报告认为，个别国家及某些区域或次区域对海底通信电缆系统的安全存在正当关切，特别是在当前地缘政治紧张局势和技术竞争加剧的环境下。然而，报告质疑当前应对措施的方向，主张为了避免重蹈覆辙，还需要采取合作的方式，立足于加强全球系统的韧性。报告提出的建议主要针对国家，虽然也承认私营部门、学术界和技术界在这些努力中的重要性。它借鉴了现有的建议和承诺，包括国际缆线保护委员会和联合国会员国在大会裁军与国际安全委员会（联大第一委员会）框架下关于信息和通信技术及国际安全的建议和承诺。这些建议分为三个主题领域：(1) 作为关键基础设施的海底通信电缆；(2) 加强公私合作；(3) 更全面且基于原则的政策议程。希望这些建议能够为推进该领域的负责任国家行为讨论提供基础。

## 导言

就在十多年前，第三届信息和通信技术（ICT）与国际安全政府专家组（GGE）即将完成其工作时，一些关于海底通信电缆的学术报告相继发表。<sup>1</sup>这些报告揭示了海底电缆系统面临的新风险，还强调了国际海底电缆法律制度中的许多空白及更广泛的治理挑战。当时，只有两百多条海底电缆在运行，且主要由电信运营商拥有和运营。如今，运营中的电缆数量翻了一番，光子学领域的技术进步带来了前所未有的速度和容量提升。行业性质发生了巨大变化，电缆系统也面临着新的风险。与此同时，我们对电缆和更广泛的信息和通信技术生态系统的依赖程度也在不断增加。尽管过去与海底通信电缆相关的威胁在网络安全政策圈中很少受到关注，但现在这种情况正在改变。

2022年3月，在当前的2021-2025年信息和通信技术安全与使用问题不限成员名额工作组会议上，一位来自地缘战略位置重要但规模较小的国家代表的发言中提到了海底电缆。其目的是强调保护通过该国水域的海底电缆所需的资源和能力，并指出在确保这些关键通信链路对于非洲之角、南亚和欧洲多个国家的可靠性和可用性方面所面临的挑战，尤其是在地缘政治紧张局势不断加剧的背景下。在同一会议上，另一位代表提醒，尽管存在国际公认的信息和通信技术相关行为规范，一些国家仍在针对诸如海底通信电缆等关键基础设施，这可能会造成重大的破坏性影响。<sup>2</sup>

在不限成员名额工作组的一次会议上，上述简短而重要的发言提到了海底通信电缆、其易受攻击性以及相关的韧性和容量问题，反映出各国对围绕这一最关键的信息基础设施新出现的威胁的日益关注。<sup>3</sup>然而，这些关注几乎被无视。几个月后，北溪管道爆炸事件将各国的注意力转向了海底和海底电缆系统，凸显了我们对这些系统的集体依赖程度。这种情况表明，相关行业和政府行动方之间需要加强信息共享，并且可能需要采取新的措施来加强其韧性。<sup>4</sup>

不过目前尚不清楚外交官们是否准备好进行这样的对话。尽管海底电缆有着悠久而曲折的历史，但政策和研究界因对“[全球电缆网络]如何运行、如何监管、由谁控制以及如何保护其免受脆弱性影响”缺乏了解而遭受批评。<sup>5</sup>在政策层面，关于一些政策制定者或拥有和运营大多数海底通信电缆系统的私人利益方愿意透露或公开讨论的内容，可能存在很大的战略模糊性。但在许多决策层中，这种认识 and 理解的依然极为匮乏。在研究层面，关于海底电缆相关问题的文献数量显著增加，其研究方法涵盖了科学技术、工程、海上安全、国际公法、环境保护、治理与安全研究、历史和考古学等多个领域。<sup>6</sup>亟需的跨学科研究也在不断涌现。<sup>7</sup>尽管如此，最近的事态发展表明，现在是时候进行更深入的关于海底通信电缆、现有电缆治理机制的充分性以及如何加强这些机制的对话。这种对话已经在区域和国家层面展开。<sup>8</sup>本报告旨在为更具全球化和包容性的对话提供基础，并将其牢牢根植于正在进行的多边讨论之中。

<sup>1</sup> 例如，参见 Douglas R. Burnett 等（主编）（2013 年），《海底电缆：法律与政策手册》，BRILL 出版社；Michael Sechrist（2012 年），“新威胁、老技术：海底通信电缆网络管理系统中存在的薄弱环节”，哈佛大学肯尼迪学院；以及 Michael Sechrist（2010 年）“位于深海的网络空间：通过创造形成国际公私部门合作关系进行海底通信电缆防护”，哈佛大学肯尼迪学院。

<sup>2</sup> 参见吉布提和美国代表的发言，不限成员名额工作组第二届实质性会议，[https://meetings.unoda.org/meeting/57871/statements?f%5B0%5D=segment\\_statements\\_%3ASecond%20substantive%20session&f%5B1%5D=segment\\_statements\\_%3AThird%20substantive%20session](https://meetings.unoda.org/meeting/57871/statements?f%5B0%5D=segment_statements_%3ASecond%20substantive%20session&f%5B1%5D=segment_statements_%3AThird%20substantive%20session)。

<sup>3</sup> 新加坡政府曾在联合国框架下，信息和通信技术以及国际安全问题提出过相关议题。然而，由于多种原因，该议题在该论坛上并未引起广泛的关注。

<sup>4</sup> 例如，参见 2022 年 12 月 5 日美国-欧盟贸易与技术委员会联合声明中的“未来安全连接项目”部分。

<sup>5</sup> Christian Bueger 和 Tobias Liebetrau（2021 年），“保护隐藏的基础设施：全球海底数据电缆网络的安全政治”，《当代安全政策》42:3，第 392 页。

<sup>6</sup> 同上。

<sup>7</sup> 例如，参见 Christian Bueger 和 Tobias Liebetrau（2022 年），“对海底通信电缆和基础设施的安全威胁——对欧盟的影响”，[https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO\\_IDA\(2022\)702557\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf)。

<sup>8</sup> 同上。

本报告从系统视角出发，将海底通信电缆视为更广泛的信息和通信技术生态系统的核心要素。报告首先概述了海底电缆技术及其相关“湿端”（海底）和“干端”（陆地）设备基础设施的发展情况，以及参与海底电缆行业的主要行动方。<sup>9</sup>然后概述了与海底电缆系统及相关基础设施有关的常见威胁和脆弱性，随后介绍了现有的海底电缆治理制度。本报告部分借鉴了国际缆线保护委员会的政府最佳做法<sup>10</sup>以及在联大第一委员会框架下谈判达成的现有建议。<sup>11</sup> 报告最后就各国政府可采取的合作步骤提出了一些初步建议，以促进负责的国家行为，加强海底电缆系统及相关基础设施的韧性。这些建议围绕三个主题领域：作为关键基础设施的海底通信电缆；公私合作；以及更全面且基于原则的政策议程。

---

<sup>9</sup> “湿端设备”是指从一个陆地上的海滩检查井到另一个陆地上的一段电缆。它包括光纤电缆、中继器、均衡器和分支装置。传统上，“干端设备”是海底光缆系统的陆地段，从海滩检查井到光缆登陆站，通常位于海滩检查井数百米之外，通过短的无中继器光纤链路连接，不过随着光缆系统架构的发展，这种配置也在发生变化。

<sup>10</sup> 2022年，经过大量磋商，国际缆线保护委员会发布了《保护和促进海底电信缆线韧性的政府最佳做法》，以“协助各国政府制定法律、政策和做法，促进海底电信缆线（互联网的基础设施）的发展和保护”；参见 <https://www.iscpc.org/publications/icpc-best-practices/>。

<sup>11</sup> 自1998年以来，联合国成员国在大会裁军和国际安全第一委员会的主持下，一直在就信息和通信技术与国际安全的问题进行讨论。随着时间的推移，一系列政府专家组和一个不限成员名额工作组相继提出了一系列与各国在使用信息和通信技术方面负责的行为有关的措施建议。其中包括三项专门针对关键基础设施的规范。2021年，193个会员国参加的第六次政府专家组会议和第一次不限成员名额工作组会议推进了关于这些规范的讨论，相关建议中提到的关键基础设施概念，应涵盖那些对维护互联网整体完整性和可用性起到至关重要作用的设施。这份报告假定后者包括了海底通信电缆及其相关的陆地基础设施、组件和系统，共同促进数据传输。

## 现代海底通信电缆包含哪些组成部分？

第一条海底电缆铺设于19世纪，最初连接英国和法国，随后跨越大西洋，连接爱尔兰的瓦伦西亚岛和纽芬兰的哈茨康坦特。<sup>12</sup>在这些系统中，电信号通过铺设在两个电报站之间的电线传输。莫尔斯电码为英文字母的每个字母分配了一组点和划，从而可以实现复杂信息的简单传输。信息传递的速度是开创性的，这项新技术被视为“比战场上的征服者赢得的任何东西都更有益于人类”，有可能成为国家间“永久和平与友谊的纽带”。<sup>13</sup>

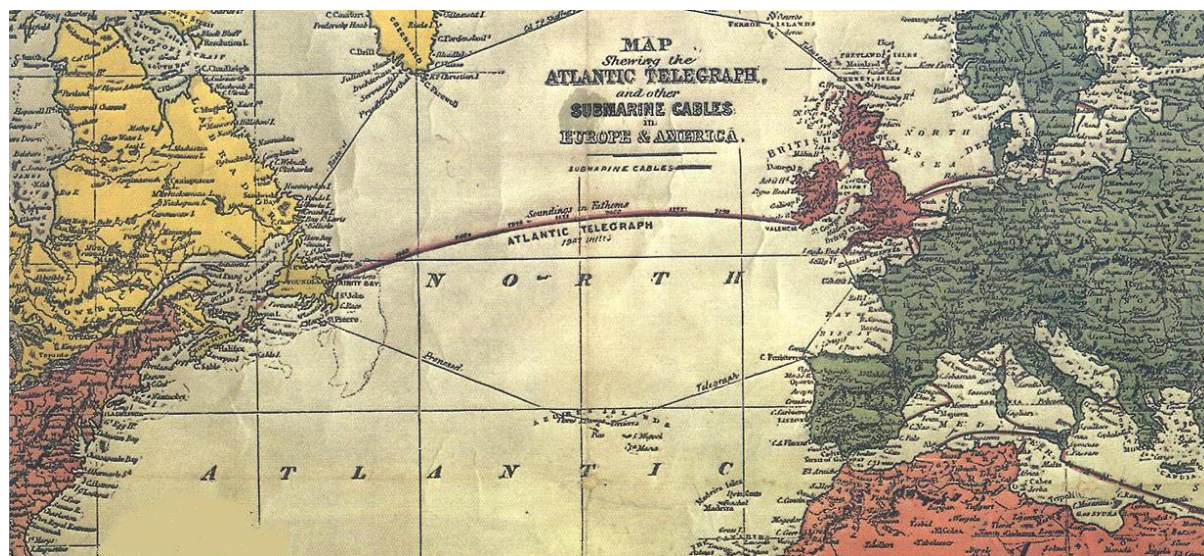


图1. 1858年跨大西洋电报电缆地图

尽管在最初的几十年里电报电缆遍布世界各个大洋，但在二十世纪初，电报电缆被电话和后来的传真等新兴技术所取代。随着通信技术的进一步发展，二十世纪五十年代铺设了第一个跨大西洋电话电缆系统，随后在三十年后又铺设了第一个跨大西洋光纤电缆系统。从那时起已经过去了三十五年，目前大约有530个电缆系统正在运行或建设中。<sup>14</sup>海底光缆现已成为我们通信基础设施的骨干：全球95%以上的互联网、语音和数据流量都通过这一庞大的海底网络进行传输。实际上，所有私人、商业和军事通信都依赖于它，全球金融交易和许多国防系统也是如此。随着我们对数字技术的依赖不断增加、5G时代到来和经济中心对高质量、低延迟连接的需求，基础设施的战略价值同时不断增长。此外，进入新市场和访问其中托管或可获取的数据所带来的商业和战略价值也在增加。<sup>15</sup>

<sup>12</sup> 为了纪念这一时刻在全球通信史上的重大意义，爱尔兰与加拿大正携手合作，共同为位于瓦伦蒂亚港和内心港的跨大西洋电报站争取联合国教科文组织世界遗产的认定；参见 <https://www.irishtimes.com/ireland/2022/07/22/valentia-islands-transatlantic-cable-to-be-put-forward-for-unesco-world-heritage-status/>。

<sup>13</sup> 1858年，美国总统詹姆斯·布坎南在通过第一条横跨大西洋的电报线路向维多利亚女王发送的贺电中的言辞。第一条横跨大西洋的信息发送耗时17小时，每个字母需要2分5秒。

<sup>14</sup> TeleGeography公司，<https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions>。

<sup>15</sup> Hilary McGeachy (2022年)，“海底电缆战略意义的变化：旧技术，新担忧”，《澳大利亚国际事务杂志》76:2。

如今的海底电缆使用光纤技术传输数据。有些独立的电缆系统长达45,000公里。<sup>16</sup>这些投入使用的电缆总长约130万公里，遍布全球。这些电缆由多对直径约为人类头发粗细的光纤组成，然后覆盖硅胶，并包裹在多层塑料、钢丝和铜中。有时，会在电缆外侧附加多层钢丝，以防止外部损坏。钢铠装的厚度一般取决于海水深度和靠近商业海洋活动的程度。在浅水区（通常定义为小于1000米），电缆也可以埋在海床下，以进一步保护其免受船只锚链和渔业作业等的损害。

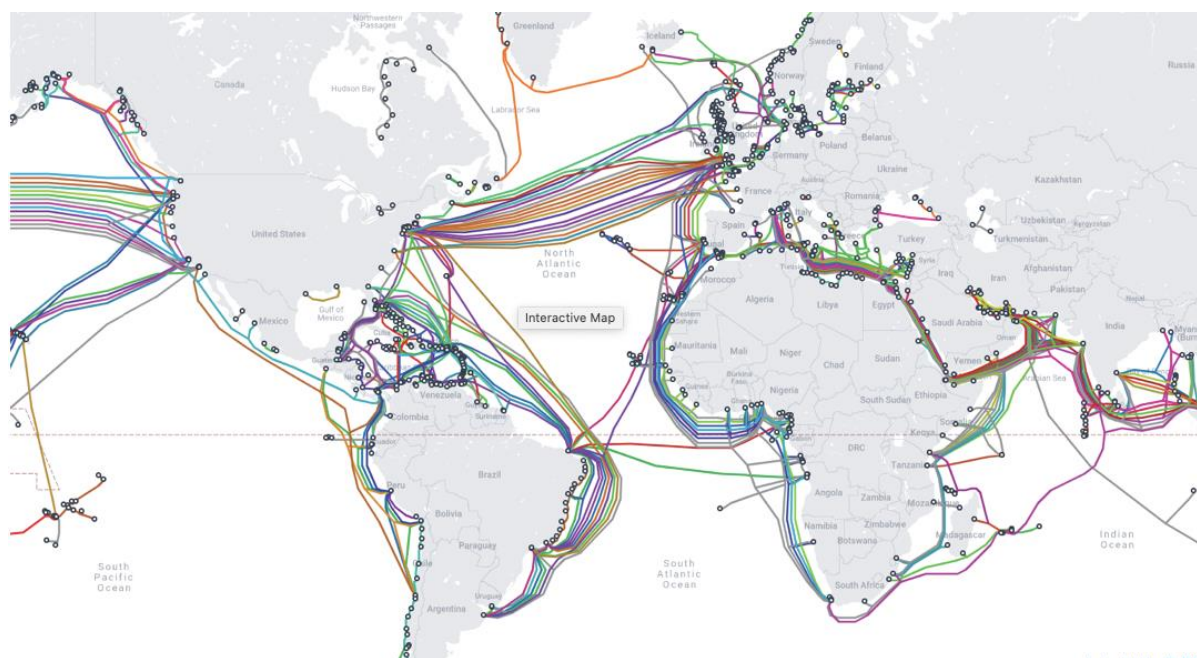


图 2. 2022 年海底电缆地图<sup>17</sup>

直到十多年前，强度调制直接检测仍是海底电缆最常用的光传输技术。这种方法利用激光脉冲对数字数据进行编码，从而通过海底和陆地光纤传输信息。此后，相干光传输技术的进一步发展使单通道数据传输速率提高了100多倍。<sup>18</sup>此外，波分复用技术增加了每条光纤承载的信道数量。<sup>19</sup>电缆的通信容量因电缆系统而异，但诸如空分复用等技术的进步将使新系统能够达到每秒500太字节的传输能力。<sup>20</sup>在长度超过几百公里的系统中，光放大器（安装在称为中继器的防水容器中）大约每隔100公里就会增强一次信号。

传统的海底电缆在目前全球运行的1,306个海缆登陆站之一铺设，然后数据通过这些站点被路由连接至地面系统。<sup>21</sup>在传统的站到站系统中，这些站点包含“干端设备”基础设施，包括控制其运行的海底线路终端设备以及为电缆供电的设备。近年来，这种传统架构发生了变化，推

<sup>16</sup> DataCenterDynamics 公司 (2022 年), “世界上最长的海底电缆登陆东非吉布提”,

<https://www.datacenterdynamics.com/en/news/worlds-longest-subsea-cable-lands-in-djibouti-east-africa>; 路透社 (2022 年), “MTN 公司在南非登陆海底电缆促进非洲的连接”,

<https://www.reuters.com/world/africa/mtn-lands-subsea-cable-south-africa-boost-africas-connectivity-2022-12-13/>。

<sup>17</sup> TeleGeography 公司的 2022 年海底电缆地图描绘了正在运行或建设中的 486 个电缆系统和 1,306 个着陆点; 参见 <https://submarine-cable-map-2022.telegeography.com/>。

<sup>18</sup> 参见 Ciena, “什么是相干光学”, <https://www.ciena.com/insights/what-is/What-Is-Coherent-Optics.html>; 以及谷歌 (2022 年), “谷歌海底光纤通信, 详解”, <https://cloud.google.com/blog/topics/developers-practitioners/googles-subsea-fiber-optics-explained>。

<sup>19</sup> 同上。

<sup>20</sup> 通过空间分隔复用技术, 可以显著提升传输容量, 利用更多的光纤来承载数据通道, 每个通道的功率和信噪比相对较低; 参见 <https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions>。

<sup>21</sup> 同上。

动了海底和陆地光纤网络与数据中心之间进一步融合。例如，在连接数据中心的系统中，电力设备可安装在靠近海岸的小型模块化登陆站内，终端设备则安装在内陆的数据中心或“具备强大连接能力、运营商中立的互联主机托管设施”中。<sup>22</sup>这种所谓的“开放式电缆”系统将终端设备与“湿设备”分开，允许包括传统系统在内的系统升级和设备多样化。最终选择哪种系统类型将取决于终端用户对所购买容量的需求（如接入主要市场、端点、一级IP网络、互联网交换节点、冗余选项、连接云聚合服务等），尽管最终决定将取决于一系列因素，包括是否为联合建设（即由两个或多个购买方共同委托），以及市场开放程度、成本、距离、地理条件、监管环境（包括国家外商投资法规）等。<sup>23</sup>未来一段时间，新的生态系统可能会继续涌现。

实施一个新的电缆项目从初步规划到系统投入使用通常需要2.5到5年的时间。与任何基础设施项目一样，该项目涉及多个步骤和漫长的谈判。<sup>24</sup>一旦达成协议，建设工作就开始了。这包括安装“湿端”（海底）设备和“干端”（陆地）设备基础设施，以及海底电缆系统可靠运行所需的网络管理和监控基础设施。<sup>25</sup>电缆系统的设计寿命周期约为25年，但如果收入持续超过成本，许多系统可以延长使用时间。<sup>26</sup>目前，大量电缆即将达到其使用寿命。

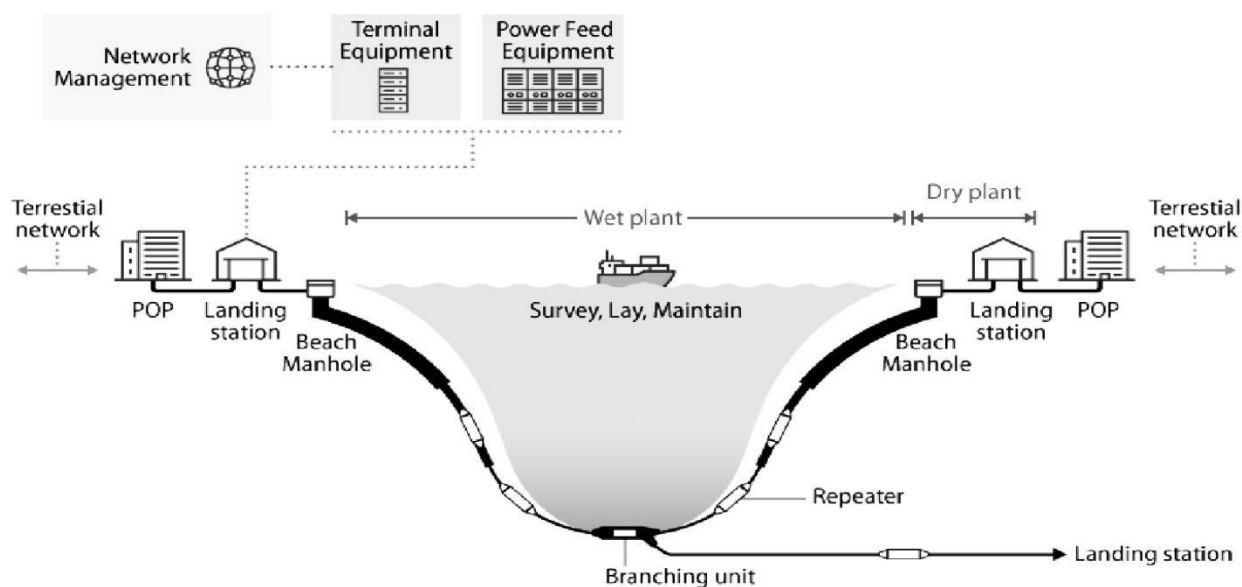


图 3. 海底电缆系统——湿端和干端设备基础设施及组件<sup>27</sup>

原则上，风险管理和缓解措施整合进入电缆系统设计和网络管理流程中，以抵消系统停机的潜在风险和维修费用，并确保最高程度的韧性。<sup>28</sup>首先，电缆系统的架构可确保在系统中具

<sup>22</sup> Vinay Nagpal (2019 年)，“数据中心、海底和地面光纤的融合”，太平洋电信理事会。

<sup>23</sup> 同上。

<sup>24</sup> 例如，仅供应合同通常就包括六个主要部分，包括合同条款和条件；项目技术规格；定价表；工作计划；计费表和供应商的系统说明。通常，这些合同协议需要与一系列行动方进行协商，因为电缆项目历来是经由财团合作或采取合资建设的方式进行的。

<sup>25</sup> 见脚注 9。

<sup>26</sup> 为了抵消容量价格下降对收入的负面影响，电缆需要不断增加容量；参见 Alan Maudlin(2018 年)，“下一次大灭绝：老化的海底电缆”，<https://www2.telegeography.com/submarine-networks-world-2018>。

Jill C. Gallagher (2022 年)，“海底电信电缆：国会技术概览及问题”，美国国会研究服务部，第 5 页

<sup>27</sup><https://crsreports.congress.gov/product/pdf/R/R47237>。

<sup>28</sup> 根据 Subcom 公司，海底电缆的修复费用可能高达 100 万美元以上，通常需要两周时间才能将电缆重新投入使用。然而，具体修复时间可能会因许可审批、气象条件以及其他变量的影响而进一步延长。面对网络安全威胁，连接服务提供商需确保通过内嵌的安全特性，保护其网络中传输的数据流量。这些可能包括下一代防火墙 (NGFW)、安全远程访问和统一威胁管理 (UTM) 服

有一定程度的冗余容量。这意味着电缆损坏通常不对服务或基础设施产生二级或三级影响。随着现有系统增加新的容量，预计韧性将进一步提高。过去，人们最关注的是与电缆系统的物理基础设施和组件有关的风险，主要是商业海事活动造成的故障和损坏。如今，关注范围已扩展到涵盖系统数据层和网络层可能出现的风险。后者包括在制造过程中或易受攻击的节点（如水下硬件组件、海滩检查井、电缆登陆站、“存在点”或互连设施、互联网交换点和数据中心）以及运行在软件上的电缆网络管理系统中可能出现的光纤和网络安全风险，这些系统通常是远程操作的。<sup>29</sup>相关的风险管理方法包括加强相关建筑物的实体安全，包括通过加强外围安全以及模块化电缆登陆站建设中的创新，并在所有核心要素中应用网络安全地网架构、强大的数据加密和其他零信任安全控制和技术。<sup>30</sup>电缆系统架构的进步也有助于提高韧性，因为据报道，较新的共享系统会限制对终端设备上电缆的实体和虚拟元素的访问。<sup>31</sup>同样，一些标准和技术也有助于预防和检测光学硬件中的漏洞以及对光学网络的潜在干扰或攻击。例如，光学干涉测量法和分布式声学传感等传感技术越来越多地应用于监测近岸段电缆，以探测附近的活动或电缆传输中的异常情况和故障。<sup>32</sup>最近系统其他部分的传感技术不断取得新进展，为网络完整性和环境监测带来了令人鼓舞的信号。<sup>33</sup>

海底光纤通信电缆主要由私营企业拥有和运营。传统上，主要的所有者和运营商是电信运营商，他们采用财团模式与有意使用电缆的各方合作，并分摊成本。在二十世纪九十年代繁荣与萧条并存的十年中，一些私营公司投资海底电缆，通过向电信公司和其他私营企业出售容量来获取利润。<sup>34</sup>如今，这两种融资模式都已存在，但在地域分布和参与的私营实体类型方面都出现了重大的新发展。例如，在过去十年中，中国公司通常是作为财团的一部分在世界各地的海底电缆项目投资及区域性电缆维护和维修方面发挥着越来越重要的作用。<sup>35</sup>这些投资与国内对超高速和大容量光传输及相关海底电缆和网络技术的研发和制造投资相结合。<sup>36</sup>该行业还见证了主要流媒体服务提供商和超大型数据中心的到来，如Meta、Alphabet、微软和亚马逊。在推动连接新的大型数据中心和云网络的过程中，这些全球巨头“在2015年至2019年期间，在全球七个

务。此外，提供端到端加密、网络安全和应用层过滤的连接性，可以保证更高的服务质量，并且能够预防网络安全威胁；参见 Brendan 出版社（2021年），“海底电缆在走向本地化的世界中的作用”，<https://datacentremagazine.com/automation/role-subsea-cables-world-going-local>。

<sup>29</sup> Michael Sechrist（2012年），“新威胁、老技术：海底通信电缆网络管理系统中存在的薄弱环节”，哈佛大学肯尼迪学院；另见 Nadia Schadow 和 Brayden Helwig（2020年），“保护海底电缆必须成为国家安全的优先事项”，防务一号，<https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/>；以及 Olga Khazan（2013年），“海底电缆窃听的诡异长期做法”，大西洋月刊，<https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/>。

<sup>30</sup> 所提及的核心要素包括身份、端点、数据、应用程序、基础设施和网络；见微软（2022年），“零信任指导原则”，<https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview>

<sup>31</sup> 与行业代表的交流，2022年12月。

<sup>32</sup> 不同于以往需要通过在电缆两端安装硬件设备来实现远程监控功能，新型电缆系统中，光纤本身就是传感器。有关 DAS 的更多信息，参见 SAGE 杂志，“分布式声学传感 (DAS) 研究协调网络 (RCN)”，[https://www.iris.edu/hq/initiatives/das\\_rcn](https://www.iris.edu/hq/initiatives/das_rcn)。

<sup>33</sup> 新的研究还展示了“首个内置实时相位和偏振传感功能的实时相干收发器，同时还能传输信息”。研究人员报告称，他们“在持续进行环境传感的同时，成功地传输了 12,800 公里的距离”；参见 M. Mazur 等人。(2022年)，“使用实时相干收发器的跨洋相位和偏振光纤感知技术”，光纤通信会议 (OFC 2022年，第 1-3 页，<https://opg.optica.org/abstract.cfm?uri=OFC-2022-M2F.2> 关于地面系统的相关发展，参见美国光学学会 (2023年)，“科学家们成功在长达 524 公里的实时架空光纤上实施了实时环境监测”，<https://phys.org/news/2023-01-scientists-real-time-environmental-kilometers-aerial.html>。

<sup>34</sup> “萧条期”这一术语描述的是，随着互联网行业的崩溃，产能需求消失，众多公司相继陷入破产的困境。

<sup>35</sup> 例如，中国公司 HMN Technologies（前身为华为海洋）在 2012 年至 2019 年间参与了 13 个不同的电缆项目，其中大部分在其本土以外地区；Lane Burdette（2021年），“利用海底电缆获取政治利益：美国对中国战略的回应”，《公共和国际事务杂志》，<https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy> 另见 Hilary McGeachy（2022年），“海底电缆战略意义的变化：旧技术，新担忧”；Jonathan E. Hillman（2021年），“保护海底网络：政策制定者手册”，战略和国际研究中心；Christian Bueger 和 Tobias Liebetrau（2021年），“保护隐藏的基础设施：全球海底数据电缆网络的安全政治”，《当代安全政策》42:3。中国公司在电缆铺设项目中的参与度已有所下降，这一变化源于多个因素，其中不乏受到其他国家对国家安全担忧的影响。中国维护修理公司 SBSS 主要在亚洲活跃，为光纤和电力电缆行业提供服务。

<sup>36</sup> 国务院关于印发《中国制造 2025》的通知，国发[2015]28号，中华人民共和国国务院，第 19 页，“新一代信息技术产业”。安全与新兴技术中心提供的译文，2022 年 3 月 10 日，<https://cset.georgetown.edu/publication/notice-of-the-state-council-on-the-publication-of-made-in-china-2025/>。

区域中的六个区域，以至少70%的复合年增长率<sup>37</sup>增加了容量，改变了其中许多区域传统的电缆投资和所有权结构，并“超越互联网骨干网提供商，成为海底电缆容量的主要所有者”。<sup>38</sup>拥有并运营电缆系统的独立海底电缆基础设施开发商的数量也在增加。据报道，他们从其他所有权结构的挑战中吸取经验教训，在市场上创造了意想不到的差异化。<sup>39</sup>这些都是业内最引人注目的行动方。在幕后，大量专业私营公司和技术机构提供贯穿整个电缆系统生命周期的服务。

政府部门和机构在海底电缆的治理和保护方面也发挥着重要作用，其监管和政策作用贯穿电缆系统及其海底和陆地基础设施的整个生命周期。传统上，这些包括负责电信、海事和航运事务、渔业、环境、海关、执法和国防的部委、部门和机构。如今，还包括负责网络安全和关键基础设施保护、数字化转型、外交政策、创新、贸易、投资和发展领域的部委和机构。<sup>40</sup>诸如亚太经济合作组织 (APEC) 论坛、东南亚国家联盟 (ASEAN) 和欧盟各机构等区域组织发布了与海底通信电缆相关的政策、研究和指导。<sup>41</sup>专门的国际机构也在发挥作用，例如国际电信联盟（负责技术标准）、国际水道测量组织（负责制图和空间分隔问题）、联合国毒品和犯罪问题办公室（负责与海上安全相关的技术援助和能力建设问题，包括海底电缆保护），以及国家管辖范围以外区域海洋生物多样性政府间会议（涉及关于可持续利用国家管辖范围以外区域海洋生物多样性的第72/249号决议），该会议刚刚商定了一项新的具有国际法律约束力的文书。<sup>42</sup>此外，很多非政府组织、技术机构和研究机构也发挥了重要作用。<sup>43</sup>

<sup>37</sup> Matthew P. Goodman 和 Matthew Waylan (2022 年)，“确保亚洲海底网络的安全”：《美国利益与战略选择》，CSIS 简报，第 3 页。

<sup>38</sup> 同上。另见 Alan Mauldin (2017 年)，“内容提供商海底电缆持有状况完整清单”，<https://blog.telegeography.com/telegeography-content-providers-submarine-cable-holdings-list>。

<sup>39</sup> Suvesh Chattopadhyaya (2018 年)，“海底电缆系统——独立基础设施开发商”，<https://www.submarinenetworks.com/en/insights/a-new-coming-for-submarine-cable-systems-the-independent-infrastructure-developers>；Olivier Pinaud (2023 年)，“大科技公司殖民海底以掌控互联网”，《世界报》，[https://www.lemonde.fr/en/international/article/2023/01/02/big-tech-colonizes-seabed-to-assert-control-of-the-internet\\_6010073\\_4.html](https://www.lemonde.fr/en/international/article/2023/01/02/big-tech-colonizes-seabed-to-assert-control-of-the-internet_6010073_4.html)。

<sup>40</sup> ICPC (2022 年)，“保护和促进海底电信电缆恢复能力的政府最佳做法”，<https://www.iscpc.org/documents/?id=3733>。

<sup>41</sup> 例如，亚太经合组织出版物，包括源于其《供应链连接框架行动计划》的《东盟 2025 年数字总体规划》及其《2019 年加强海底电缆的韧性和维修指南》；2022 年 12 月 14 日第 2022/2555 号指令（欧盟），<https://eur-lex.europa.eu/eli/dir/2022/2555>；另见 Christian Bueger 和 Tobias Liebetrau (2022 年)，“对海底通信电缆和基础设施的安全威胁——对欧盟的影响”，[https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO\\_IDA\(2022\)702557\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf)。

<sup>42</sup> 联合国秘书长在关于制定《联合国海洋法公约》下具有法律约束力的文书以保护和管理国家管辖范围外海域生物多样性的政府间会议上的声明，2023 年 3 月 5 日，<https://www.un.org/bbnj/sites/www.un.org.bbnj/files/sgstatementbbnj5resumed.pdf>。另见 <https://www.un.org/bbnj/>。

<sup>43</sup> 这份名单颇为冗长，但其中一些核心机构包括专注于海事问题的 Safe Seas，以及致力于技术及网络/网络安全领域的电气和电子工程师协会 (IEEE) 和互联网协会。

## 威胁和脆弱性

与十九世纪的铜缆相比，如今的光纤电缆具有极高的可靠性，符合所谓的“五个九标准”，即可用性达到99.999%，并且“相对于其在全球广泛分布的情况，很少发生重大中断”。<sup>44</sup>尽管如此，故障还是时有发生，估计每年约有200起。<sup>45</sup>正如下文进一步讨论的那样，当故障和中断发生时，可能会造成重大影响，特别是当无法自动重新切换到其他海底电缆和陆地或卫星网络上未使用的可用容量时。

海底光缆通信系统面临的威胁是多领域的，遍及海洋、陆地和网络空间。这些威胁可能由自然现象或人为活动（无意或有意）引起，影响电缆本身和数据传输或其他基础设施部分，包括放大器、登陆站、维护和维修船、网络管理系统和电缆供应链。<sup>46</sup>电缆在地理上也往往高度集中在海上和陆地上所谓的“咽喉要道”，因此在正常情况下，电缆的铺设和维修十分困难，而在紧张或危机情况下则很容易受阻。<sup>47</sup>

电缆本身容易受到与天气（风暴潮、台风、飓风）、地质（地震、断层线、海底滑坡、火山爆发）和海洋环境（海流密度、波浪）有关的自然现象的影响。自然现象造成的中断往往发生在靠近陆地的地方，会同时影响多条电缆，导致冗余丧失。当一个国家仅依赖一条电缆提供服务时，此类状况就会更加棘手。例如，2022年1月15日汤加附近的海底火山爆发及其引发的海啸，切断了汤加通过斐济连接到世界其他地区的唯一海底电缆。虽然在海啸发生一周后通过卫星链路保证了低等级的连接，但修复电缆和恢复与汤加主岛汤加塔布的全面连接还是耗费了五个多星期，而修复连接主岛与受海啸影响最严重的离岛的国内电缆也耗费了几个月的时间。<sup>48</sup>

捕鱼和抛锚等商业性海洋活动也可能导致电缆故障或中断。根据国际缆线保护委员会的统计数据，捕鱼和抛锚往往是最常见的造成中断的形式，约占大多数电缆故障的70%。<sup>49</sup>可能导致电缆中断的其他商业活动包括航运、疏浚以及深海采矿，这些活动在某些海域正在增加。

有时，市场动态也可能导致电缆故障。如果所有者在建造电缆系统时使用质量较差的设备和组件，试图降低电缆建造成本，就会出现这种情况。<sup>50</sup>提高效率的努力也会产生问题。例如，向远程网络管理系统转变引起了关注，因为这些系统的软件容易被利用。尽管在过去十年中，随着对网络安全风险的关注增加，这些远程系统已经得到了显著加强。<sup>51</sup>人们还担心，日益复杂的数字生态系统，其中包含在全球范围内运行的分层依赖关系，可能会引发一系列目前尚未在当前风险管理及缓解框架中考虑的分层故障。<sup>52</sup>

---

<sup>44</sup> Christian Bueger 和 Tobias Liebetrau (2021 年), “保护隐藏的基础设施: 全球海底数据电缆网络的安全政治”, 《当代安全政策》42:3, 第 396 页。

<sup>45</sup> 根据 2019 年国际缆线保护委员会全体会议讨论, 尽管在役电缆总长度有所增长, 但每千公里故障率在过去十年中保持不变或略有下降。

<sup>46</sup> 例如, Quintillion 公司指出, 需求增长和 Covid 等现象导致光纤电缆和 ODN 基础设施以及闪存、电容器和半导体等电子元件短缺。Quintillion 公司, “光纤连接世界: 海底电缆行业面临的五大难题”, 2021 年 11 月 26 日,

<https://www.quintillionglobal.com/connecting-the-world-to-fiber-the-subsea-cable-industrys-5-biggest-challenges/>

<sup>47</sup> 例如, 参见 Matt Burgess(2022 年), “互联网上最脆弱的地方”, <https://www.wired.com/story/submarine-internet-cables-egypt/>, 其中讨论了红海航线作为“世界上最大的互联网咽喉”之一的脆弱性。

<sup>48</sup> 西蒙·斯卡尔等人(2022 年), “重建汤加的竞赛”, 路透社, <https://www.reuters.com/graphics/TONGA-VOLCANO/znpnejbjov/>。

<sup>49</sup> ICPC (2022 年), 《保护和促进海底电信电缆韧性的政府最佳做法》, 第 2 节, “捕鱼和抛锚风险”,

<https://www.iscpc.org/publications/icpc-best-practices/>

<sup>50</sup> 与电缆行业代表的通信, 2022 年 12 月 2 日。

<sup>51</sup> Michael Sechrist (2012 年), “海底电缆战略意义的变化: 旧技术, 新担忧”, 哈佛大学肯尼迪学院。

<sup>52</sup> 与国家网络安全中心主任的通信, 2022 年 1 月 24 日。

除了电缆故障本身，核心组件短缺或依赖等供应链问题也会构成重大风险，尤其是在需要紧急维修时。<sup>53</sup>同样，对维护和修理航运能力的投资不足以及应对熟练劳动力短缺的问题，也是目前业界的主要关切。<sup>54</sup>

虽然不常被讨论，但制定不当的政府政策和监管框架也可能加剧电缆系统的损坏风险并降低其韧性，并延误维修工作。同时，<sup>55</sup>国家主管部门的职责和责任不明确也会造成这些问题。对许多业内人士来说，基于国家安全考虑的电缆路由和投资决策也会削弱行业行动方的竞争力，并阻碍创新。这些决策还可能产生新的安全风险。

直到最近，最常见的蓄意损坏电缆的行为与盗窃电缆材料有关，尤其是铜。<sup>56</sup>可以说，陆地网络也面临着类似的挑战，因为海底电缆常常被误以为其中含有铜而被盗。然而，这种比较也仅限于此，因为修复海底电缆损坏的成本要高得多且耗时更长。人们还担心恐怖组织会破坏关键基础设施，包括海底电缆等关键通信基础设施。这些关切甚至被纳入安全理事会决议，但至少据公众所知，尚未发生过此类事件。<sup>57</sup>

然而，最近更加显著的是各国对海底通信电缆构成的现有和潜在威胁。这种威胁由来已久。例如，在1884年《保护海底电缆公约》谈判之前，随着当时的领土扩张主义加剧，国家对电缆项目的干预显著增加。对电缆运行所需关键资源的竞争加剧。电缆窃听和破坏逐渐成为冲突的一个特征——首先是在内乱中，然后是在国际冲突中，大国逐渐将电缆窃听和破坏纳入战争计划。<sup>58</sup>即使当时世界对信息技术的依赖程度不如现在，当大规模战争爆发时，其影响也是重大的。如今，虽然大多数电缆项目都采用风险管理方法，并建立了较高的冗余度，以确保发生故障时保持可用性或相对较快的恢复速度，但情况并非如此简单。对于地理位置较偏远且存在单点故障的国家而言，恢复速度会大大降低。如果试图破坏关键的咽喉要道，阻断维修船只和备件仓库的通道，或破坏供应链，那么恢复能力也可能显著减弱。

上文提到的许多国家行为在今天依然可见，反映出我们这个时代强烈且令人担忧的地缘政治潮流。在陆地上，这些行为包括报告的针对电缆登陆设施和互联网交换点的网络攻击；<sup>59</sup>在实际

<sup>53</sup> 关于供应链问题，特别是组件供应（包括半导体），参见 Jim Fagan，“在全球海底连接中管理紧张的供应链”，Mission Critical 杂志，2022 年 10 月 25 日，<https://www.missioncriticalmagazine.com/articles/94311-managing-tight-supply-chains-in-global-subsea-connectivity>；Sebastian Moss，“全球光纤电缆短缺导致延迟和价格上涨”，DataCenterDynamics，2022 年 7 月 25 日，<https://www.datacenterdynamics.com/en/news/global-shortage-of-fiber-optic-cables-leads-to-delays-price-increases/> 另见上文注释 47。

<sup>54</sup> 与行业专家交流，2022 年 11 月。另见上文注释 47。

<sup>55</sup> ICPC (2022 年)，“政府保护和促进海底电信电缆恢复能力的最佳做法”，<https://www.iscpc.org/documents/?id=3733>；Andy Palmer-Felgate 等人 (2013 年)，“海洋区域维护：全球海底电缆维修启动时间的比较分析”，<https://minz.org.nz/i/2018-challenges/Marine-maintenance-in-the-zones.pdf>。

<sup>56</sup> 例如，参见 Robert Martinage (2015 年)，“海底之下：公共领域的脆弱性”；Mick P. Green 和 Douglas R. Burnett，“国际海底电缆基础设施的安全性：是时候重新思考了吗？”ICPC，第 5 页，<https://www.iscpc.org/documents/?id=2974>。

<sup>57</sup> 安全理事会，联合国文件 S/RES/2341 (2017)；另见也请参阅联合国秘书长在 2017 年关于“防范恐怖袭击对关键基础设施的保护”安理会公开辩论中的致辞，<https://www.un.org/sg/en/content/sg/statement/2017-02-13/secretary-generals-message-security-council-open-debate-protection>。

<sup>58</sup> 卡米诺·卡瓦纳 (即将发表)，“紧密相连的纽带……以及可能解体的地缘政治”，SubOptic 电信会议，2023 年 3 月。

<sup>59</sup> 例如，参见 CyberScoop (2022 年)，“国土安全部调查人员称他们挫败了对夏威夷海底互联网电缆的网络攻击”，<https://www.cyberscoop.com/undersea-cable-operator-hacked-hawaii/>；Colin Wall 和 Pierre Morcos (2021 年)，“隐形而至至关重要：海底电缆与大西洋安全”，美国战略与国际问题研究中心，<https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security>；Devirupa Mitra (2022 年)，“因印度团队访问互联网登陆站毛里求斯爆发监视风暴”，The Wire 网站，<https://thewire.in/diplomacy/mauritius-snooping-storm-india-internet>；路透社 (2021 年)，“美国通过丹麦电缆监视默克尔和其他欧洲人——广播公司 DR”，<https://www.euronews.com/2021/05/30/us-denmark-defence>；Olga Khazan (2013 年)，“海底电缆窃听的诡异长期做法”，《大西洋月刊》，<https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/>；Yuval Shavitt 和 Chris C. Demchak (2022 年)，“从首个网络化冲突时代的教训中未能汲取教益——BGP 劫持事件持续上演”。《网络防御评论》7:1，[https://cyberdefensereview.army.mil/Portals/6/Documents/2022\\_winter/20\\_Shavitt\\_Demchak\\_CDR\\_V7N1\\_WINTER%202022.pdf](https://cyberdefensereview.army.mil/Portals/6/Documents/2022_winter/20_Shavitt_Demchak_CDR_V7N1_WINTER%202022.pdf)。

冲突中争夺对有线电视系统陆地<sup>60</sup>设施的控制权或破坏有线电视系统陆地设施；以及公司和个人向间谍机构提供物质支持和情报。<sup>61</sup>在海上，这些事件包括在多个国家的领海或专属经济区内的报告的可疑活动。<sup>62</sup>

此外，还有报道称发生由国家蓄意支持的电缆破坏事件（幸运的是，这样的例子仍然很少），以及对此类活动对军事行动产生潜在影响的担忧的报道。<sup>63</sup>通常认为，离海岸越远，大国参与的可能性越大，因为需要强大的技术及海上能力和资源才能到达和介入电缆。公海上的电缆窃听就属于这种情况，尽管据报道，由于光学传感技术和数据加密技术的进步，探测和防止此类活动变得更加困难。<sup>64</sup>

这些实体和网络安全威胁，在各国技术竞争愈演愈烈的背景下日益凸显，不仅在国家及区域政策与战略中被频繁提及或暗示，<sup>65</sup>而且在国家间的双边合作协议中也清晰可见。<sup>66</sup>各国纷纷加大在海军能力和战略技术领域的研发投入，旨在监控和防范可能对海底电缆系统造成影响的活动，并在这一领域取得相对优势。<sup>67</sup>这些威胁也促使各国立法机构加大投资，以提升电缆修复

<sup>60</sup> 参见 Celine Alkhalidi 和 Mostafa Salem (2022 年)，“空袭在也门造成 70 人死亡并导致互联网中断”，美国有线电视新闻网，<https://edition.cnn.com/2022/01/21/middleeast/yemen-detention-strike-internet-outage-intl/index.html>；Recorded Future 公司 (2018 年)，“也门内战的深层维度：对互联网的控制”，<https://go.recordedfuture.com/hubfs/reports/cta-2018-1128.pdf>。

<sup>61</sup> 2018 年，美国财政部制裁了五家俄罗斯公司和三名俄罗斯国民，据称他们为俄罗斯联邦安全局追踪水下光纤电缆提供了支持；Morgan Chalfant 和 Olivia Beavers (2018)，“Spotlight Falls on Russian Threat to Undersea Cables”，The Hill，<https://thehill.com/policy/cybersecurity/392577-spotlight-falls-on-russian-threat-to-undersea-cables/>。

<sup>62</sup> 美国国际战略研究中心 (2022 年)，“海底之下：中国对海洋海域的勘察”，<https://amti.csis.org/what-lies-beneath-chinese-surveys-in-the-south-china-sea/>；Huong Le Thu 和 Bart Hogeveen (2022 年)，“英国、澳大利亚与东盟合作打造更安全的海域，澳大利亚战略政策研究所”，<https://www.aspi.org.au/report/uk-australia-and-asean-cooperation-safer-seas>；Naomi O'Leary (2022 年)，“爱尔兰关键的海底电缆易受攻击”，《爱尔兰时报》，<https://www.irishtimes.com/world/europe/2022/09/28/irelands-submarine-cables-are-vulnerable-to-attack/>；国家情报总监办公室 (2022 年)，“《美国情报界年度威胁评估》”，<https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf>。

<sup>63</sup> Atle Staalesen (2022 年)，“‘人类活动’导致斯瓦尔巴特群岛电缆中断”，《巴伦支观察家》，<https://thebarentsobserver.com/en/security/2022/02/unknown-human-activity-behind-svalbard-cable-disruption>；Rishi Sunak (2017 年)，“海底电缆：至关重要却易受威胁”，政策交流论坛，<https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>；关于海外军事行动，参见 Michael Sechrist (2010 年)，“深水网络空间：通过建立国际公私伙伴关系保护海底通信电缆”，哈佛大学肯尼迪学院。Sechrist 讨论了当时意大利与埃及之间的三条通信电缆遭到切断，据称这一事件显著降低了美国在伊拉克的无人机作战能力。

<sup>64</sup> 在光纤时代来临之前，电缆窃听是各大海军强国普遍采取的实践。相较于历史上的铜线和同轴电缆，如今对光纤电缆及其放大器进行物理窃听变得更加困难。据称，只有少数国家拥有所需的特殊设备。这包括装备精良的潜艇或者由船只部署的潜水器，它们能够隐秘地提取并解密电缆中的数据。相反，电缆系统的陆地基础设施和网络管理系统却更加易受间谍活动的攻击。尽管目前正积极采取措施加强这些物理和网络安全，但要实现包括抵御内部威胁和防范国内政治决策影响在内的全面保护，始终是一项艰巨的任务。

<sup>65</sup> 例如，以美国为例行政命令 13873 (2019) 关于确保信息和通信技术及服务供应链安全；法国国防部 (2022 年)，海底战争部长级战略，[https://archives.defense.gouv.fr/content/download/636000/10511901/file/20220214\\_FRENCH%20SEABED%20STRATEGY\\_key%20pints.pdf](https://archives.defense.gouv.fr/content/download/636000/10511901/file/20220214_FRENCH%20SEABED%20STRATEGY_key%20pints.pdf)；2022 年 12 月 14 日第 2022/2555 号指令 (欧盟)，<https://eur-lex.europa.eu/eli/dir/2022/2555>；北约 (2023 年)，“北约成立海底基础设施协调小组”，[https://www.nato.int/cps/en/natohq/news\\_211919.htm](https://www.nato.int/cps/en/natohq/news_211919.htm)。此前，欧盟-北约曾宣布成立一个联合工作组：北约 (2023 年)，“北约和欧盟成立韧性和关键基础设施工作组”，[https://www.nato.int/cps/en/natohq/news\\_210611.htm](https://www.nato.int/cps/en/natohq/news_210611.htm)。

<sup>66</sup> 例如，参见 2020 年《澳大利亚-新加坡数字经济协议》，第 22 段，<https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement.pdf>；以及 2022 年《英国-新加坡数字经济协定》，第 7 节，附加条款，“海底电缆登陆系统”，<https://www.gov.uk/government/publications/uk-singapore-digital-economy-agreement-explainer/uk-singapore-digital-economy-agreement-final-agreement-explainer>。美国-欧盟贸易与技术委员会还计划在其信息和通信技术安全与竞争力工作组框架下讨论海底通信电缆议题。讨论内容将涵盖跨大西洋海底电缆的连通性与安全性问题，包括替代路线，如连接欧洲、北美和亚洲的跨大西洋路线；在信息和通信技术供应链中供应商多样化的努力；以及市场向开放、互操作性的方向发展，同时保持对可靠、成熟的体系结构的信任；参见贸易与技术委员会 2022 年美国-欧盟联合声明，标题为“未来安全连通项目”，<https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/05/u-s-eu-joint-statement-of-the-trade-and-technology-council/>。

<sup>67</sup> Charlotte le Breton 和 Hugo Decis (2022 年)，“法国深入探索海底战争”，国际战略研究所军事平衡博客，<https://www.iiss.org/blogs/military-balance/2022/02/frances-deep-dive-into-seabed-warfare>；Martina Bet (2022 年)，“本·华莱士：专业舰船将守护水下电缆抵御俄罗斯攻击”，《标准晚报》，<https://www.standard.co.uk/news/politics/ben-wallace-moscow-russia-keir-starmmer-government-b1029675.html>；Jonathan Beale (2021 年) <https://www.bbc.com/news/uk-56472655>；Alexandra Brzozowski (2020 年)，“北约寻求保护水下电缆免受俄罗斯攻击的方法”，Euractiv，<https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/>；以及 Dimitrios Eleftherakis 和 Raul Vicen-Bueno

能力，<sup>68</sup>并研发可靠的电缆技术和网络，用于军事和防御通信。因此，新工作小组和协调结构在部分区域应运而生。<sup>69</sup>此外，许多国家以国家安全为由，更加积极地介入光缆项目，影响对光缆线路、技术和融资的选择，<sup>70</sup>延长了许可和审批过程。在某些情况下，甚至有国家因为特定公司参与或电缆登陆或连接至特定司法管辖区而否决项目（见下文方框1）。

此类决策与类似的国家或区域安全导向决策相融合，将其他海底通信电缆相关技术列入关键和新兴技术清单和出口管制清单，<sup>71</sup>或在大西洋、波罗的海、地中海、印度洋-太平洋、西北航道、中国南海等具有重要战略意义的海域或非洲和东南亚等具有重要商业意义的数据丰富地区投资海底电缆和其他数字基础设施项目。<sup>72</sup>

简而言之，海底通信电缆正在成为地缘政治竞争的重要特征，对电缆的安全和韧性以及我们社会日益依赖的更广泛的信息和通信技术生态系统，都具有深远的影响。这就引出了一个问题：现行的海底电缆制度是否能够满足其既定目的？

---

（2020年），《提高水下通信电缆安全性的传感器：水下监测传感器综述》，*Sensors 期刊* 20:3, <https://www.mdpi.com/1424-8220/20/3/737>。

<sup>68</sup> 2019年，美国2020财年国防授权法案中纳入了建立“电缆安全舰队”的条款；该法案还涉及了关于如何实际运作这支舰队的挑战性讨论，参见 Douglass R. Burnett (2022年)，《修复海底电缆是战时必需》，《论文集》148:10, <https://www.usni.org/magazines/proceedings/2022/october/repairing-submarine-cables-wartime-necessity>

<sup>69</sup> 见脚注 67。

<sup>70</sup> Hilary McGeachy (2022年)，《海底电缆战略意义的变化：旧技术，新担忧》，《澳大利亚国际事务杂志》76:2.

<sup>71</sup> 例如，参见美国国家科学技术委员会 (2022年)，“关键和新兴技术清单更新”，第4页，<https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf>。

<sup>72</sup> 关于海底电缆基础设施投资的更广泛见解，见脚注 68、72 和 138。

**表 1：十年来的被动路由决策**

- 金砖国家努力建设相互连接的海底电缆，以规避经过欧洲和美国高昂的路由成本，并防止非金砖国家实体截获重要金融和安全信息。尽管进行了积极的市场、交通和可行性研究，但该电缆项目并未继续进行。<https://www.offshore-energy.biz/brics-unveils-new-submarine-cable-system/>。
- 巴西努力寻求替代路线，包括与欧盟合作，以避免经过美国路由流量（2014 年）。<https://www.reuters.com/article/us-eu-brazil-idUSBREA1N0PL20140224>
- 澳大利亚决定出资建设一条长达 4000 公里的海底电缆，该电缆将连接澳大利亚、所罗门群岛和巴布亚新几内亚（2018 年）。<https://www.bbc.co.uk/news/world-australia-44463553>
- 智利决定将电缆铺设到澳大利亚，而非亚洲（2020 年）。<https://www.datacenterdynamics.com/en/news/chiles-transoceanic-cable-connect-new-zealand-and-australia/>。
- 【美国电信团队】向美国联邦通信委员会建议拒绝太平洋光缆网络公司将其香港海底电缆连接到美国的申请（2020 年）。<https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea>
- 公司决定重新提交或撤回在香港登陆的跨太平洋电缆项目的登陆许可申请（2020-2021 年）。<https://blog.telegeography.com/trans-pacific-cables-asian-hubs-plcn-status>
- 俄罗斯联邦做出关于极地快车电缆项目的决定，该项目旨在连接西北海岸沿线的北极社区（2021 年）。<https://www.capacitymedia.com/article/29otdtk3j2ycxulos7b40/news/russia-begins-889m-polar-express-arctic-cable>
- 决定开发远北光纤快线路线——一个通过西北航道的跨大陆电缆项目，而非此前规划的通过东北航道的北极连接项目（2022 年）。<https://www.thearcticinstitute.org/geopolitics-subsea-cables-arctic/>
- 【美国电信团队】向美国联邦通信委员会提出的建议，关于拟议修改 ARCOS-1 光缆系统以包括一个在古巴的授权登陆点，建议拒绝该连接（2022 年）。<https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-application-directly-connect-united-states-cuba-through>
- 古巴国营电信运营商 ETESCA 宣布已开始与法国电信运营商 Orange 合作，通过法国海外领地马提尼克岛为古巴提供额外的连接。（2022 年）<https://www.reuters.com/business/media-telecom/cuba-french-telecoms-operator-orange-begin-work-subsea-cable-martinique-2022-12-08/>。
- 中国电信和中国移动决定撤出对 Sea-Me-We 6 光缆项目的投资，因为该项目决定由美国公司代替中国公司承建（2022 年）<https://www.ft.com/content/8f35bf1e-fe32-4998-9e13-a13bac23506d>。

## 海底通信电缆管理制度

现有的电缆治理体系由一系列国际条约、监管框架、国际和区域组织、行业协会、协议、标准和最佳做法拼凑而成。<sup>73</sup>主要海底电缆机构之一的国际缆线保护委员会是一个论坛，海底电信或电力电缆的所有者、运营商和供应商以及政府代表在此分享技术、法律和环境信息。该组织拥有来自超过69个国家的190多个成员，代表着全球98%以上的海底电信电缆。它提高了人们对海底电缆作为关键基础设施的认识，发布了电缆保护和韧性的最佳做法，提供了技术和监管问题方面的指导以及电缆安装、保护和维护方面的建议。<sup>74</sup>国际缆线保护委员会欢迎政府参与，在过去几年中，政府参与有所增加，但仍然很少。在区域层面也有一些规模较小的协会，例如欧洲海底电缆协会 (ESCA)、北美海底电缆协会 (NASCA) 和大洋洲海底电缆协会 (OSCA)。

75

从政府政策的角度来看，海底电缆保护涉及多个领域，包括海事安全、内政或国土安全、国防、网络安全、数字、通信、贸易、投资和产业政策。目前还没有关于海底电缆治理的国际安排，但如前所述，东南亚国家联盟和欧洲联盟等区域组织涵盖了各种治理方面。<sup>76</sup>

政府在海底电缆保护方面的参与（和责任）可以在现有国际法中找到依据。事实上，多项公约都涉及海底电缆问题，其中最早的可追溯到十九世纪末。其中包括：

- 《1884 年保护海底电缆公约》。<sup>77</sup>
- 1907 年《陆战法规和惯例公约》及其附件：《陆战法规和惯例条例》。<sup>78</sup>
- 《1958 年公海公约》<sup>79</sup>和《1958 年大陆架公约》。<sup>80</sup>
- 《1982 年联合国海洋法公约》（《海洋法公约》）<sup>81</sup>取代了后两者，并规定了涉及电缆的三个海洋管辖区：领海、专属经济区和公海。<sup>82</sup>

73 Christian Bueger 和 Tobias Liebetrau (2021 年)，保护隐藏的基础设施：全球海底数据电缆网络的安全政治”，《当代安全政策》42:3。

74 参见 <https://www.iscpc.org>。

有关其各自任务和成员的详细信息，参见 ESCA, <https://escaeu.org>; NASCA, <https://www.n-a-s-c-a.org>; 以及 OSCA, <http://www.oscagroup.com>。另一个类似的机构是丹麦电缆保护委员会，该委员会汇聚了在丹麦海域工作的海底产业行动方，包括从事电信业务的成员。

76 见脚注 8 和 42。

77 全文参见 <https://www.iscpc.org/documents/?id=13>。

78 《陆战法规和惯例公约》（4 号）及其附件：《1907 年陆战法规和惯例公约》，条例：第 54 条, <https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907>。

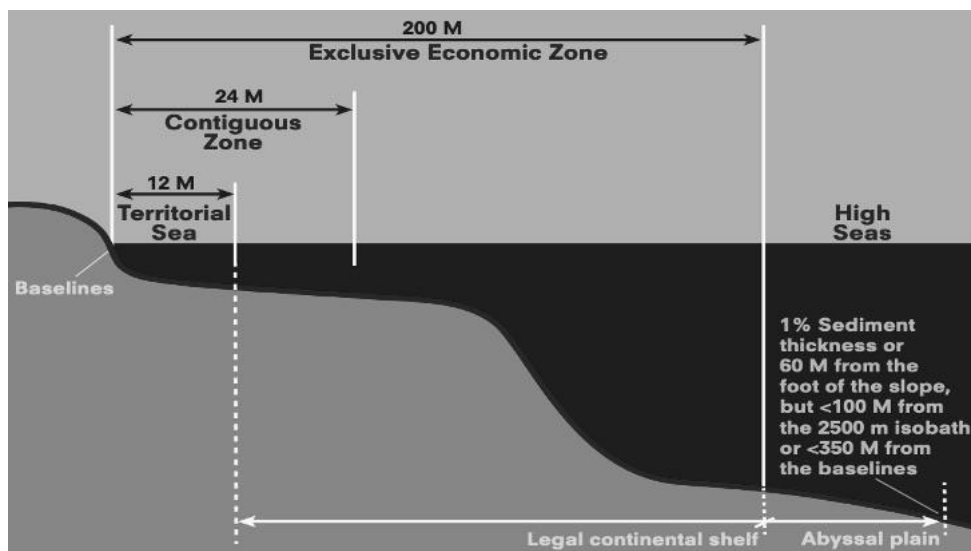
79 第 1、26-30 条；全文参见 <https://www.iscpc.org/documents/?id=14>。

80 第 4 条；全文参见 <https://www.iscpc.org/documents/?id=16>。

81 第 3/21、33、57-58、79、86-87、112-115、297 条；全文参见

[https://www.un.org/Depts/los/convention\\_agreements/convention\\_overview\\_convention.htm](https://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm)。

82 Lane Burdette (2021 年)，“利用海底电缆获取政治利益：美国对中国战略的回应”，《公共和国际事务杂志》，<https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy>

图 X. 《海洋法公约》海区<sup>83</sup>

如今，《联合国海洋法公约》仍然是海底电缆的主要参考依据（相关规定见附件 1）。《联合国海洋法公约》允许各国在公海、专属经济区和大陆架上铺设电缆并维修电缆（第 79 条）。它包括关于海底电缆断裂和损伤的规定（第 113、114 条）和关于损失赔偿的规定（第 115 条）。与《公海公约》一样，第 113 条呼吁缔约国通过国内立法，对悬挂其国旗的船只或在其管辖下的人员损坏公海海底电缆的行为进行处罚。它还扩大了可受惩罚的犯罪范围，包括“蓄意或可能导致……[海底电缆]断裂或损伤的行为”，这一规定解释为允许各国“采取行动防止电缆断裂”。<sup>84</sup>

不过，在法律覆盖和遵守方面，挑战重重。首先，并非所有国家都是《海洋法公约》的缔约国。此外，该公约并未给予足够的管辖权来处理侵权者或登船检查嫌疑船只力，因为在电缆受损事件中的民事和刑事管辖权仅限于责任个体的国籍国或责任船只的旗国。<sup>85</sup>《1884 年保护海底电缆公约》包括一项条款，即允许任何怀疑外国船只损坏电缆的军舰“要求船长或船主出示证明所述船只国籍的官方文件”。<sup>86</sup>然而《1958 年公约》和《联合国海洋法公约》中都未涵盖具有相同效果的规则。<sup>87</sup>此外，虽然《联合国海洋法公约》要求所有国家通过法律，将故意或过失损坏海底电缆的行为定为应受惩罚的犯罪，但很少有国家真正做到这一点。<sup>88</sup>即使有，这类法律也被描述为“严重不足，与蓄意干扰造成的损害不相称”。<sup>89</sup>更重要的是，许多国家不遵守

<sup>83</sup> 联合国（2013 年），“《海洋法公约》30 周年”，第 4 页，

[https://www.un.org/depts/los/convention\\_agreements/pamphlet\\_unclos\\_at\\_30.pdf](https://www.un.org/depts/los/convention_agreements/pamphlet_unclos_at_30.pdf)。

<sup>84</sup> Eric Wagner (1995 年)，《海底电缆和海洋法提供的保护》，《海洋政策》19:2，第 136 页。

<sup>85</sup> 参见 Yoram Dinstein 和 Arne Willy Dahl(eds) (2020 年)，《网络行动国际法塔林手册 2.0 版》，第 67 条，第 61 页以下；另见 Rishi Sunak (2017 年)，“海底电缆：至关重要却易受威胁”，政策交流论坛，第 6 页，<https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>。

<sup>86</sup> 《1884 年保护海底电缆公约》第 10 条。

<sup>87</sup> 与公共法主席沃尔夫·海因茨舍尔·冯·海因格教授博士的通信，重点讨论了国际公法、欧洲法和外国宪法法，奥德河畔法兰克福欧洲大学，2023 年 1 月 19 日。

<sup>88</sup> 迈克尔·施密特 (Michael N. Schmitt) (编辑) (2017 年)，《网络行动国际法塔林手册 2.0 版》，第 54 条，第 19 款，第 258 页。

<sup>89</sup> Tara Davenport (2015 年)，“海底电缆、网络安全与国际法：交叉分析”，《天主教大学法律与科技杂志》24(1)。

《联合国海洋法公约》关于维护和修理的规定，强加冗长的修理许可程序，有些人认为其后果堪比蓄意破坏。<sup>90</sup>

在冲突期间保护电缆方面存在其他空白。《1884年公约》中有一项关于交战行为的具体规定，这实际上允许而非限制交战方的行动自由。<sup>91</sup>《联合国海洋法公约》并未涉及该问题。唯一涉及冲突期间海底电缆的法律文书是《1907年公约》。<sup>92</sup>其第54条对连接被占领国与中立国领土的海底电缆（包括陆地部分）规定了特别保护，指出除非绝对必要，否则不得占领或摧毁电缆，而且必须立即支付赔偿。<sup>93</sup>《关于适用于海上武装冲突的国际法的圣雷莫手册》赞同这一观点，指出“交战方应注意避免损害铺设在海床上且并非专门为交战方服务的电缆和管道”。<sup>94</sup>然而，如今的海底电缆传输的数据对所有国家都具有价值，即使电缆并未直接登陆其领土，这也引发了关于该条款对海底通信电缆持续相关性的问题。<sup>95</sup>专家们还质疑对一国管辖范围以外的海底电缆的攻击是否构成《联合国宪章》第51条规定的武装攻击，如果构成，这将允许国家为了自卫而使用武力。

许多举措弥补了这些空白，还考虑了新的进展，例如影响海底电缆的网络行动。其中一些工作为《网络行动适用国际法塔林手册》和《武装冲突法选定专题奥斯陆手册》等出版物提供了资料。例如，《塔林手册2.0》指出，《联合国海洋法公约》适用于从位于海上的网络基础设施或通过网络基础设施开展的网络行动，并指出“无论是在平时时期还是冲突期间，网络行动可能从海上船只、舰艇、海上飞机、海上平台或通过海底通信电缆部署”。<sup>96</sup>其得出结论认为，“适用于海底电缆（包括海底通信电缆）及其运行的现行国际法总体上反映了国际习惯法”，<sup>97</sup>将海底通信电缆视为任何“由一国拥有、运行或铺设的电缆，以及该国授权用于电信和数据传输的私有电缆”。<sup>98</sup>关于《海洋法公约》第113条，《奥斯陆手册》的结论是，“铺设海底电缆的国家……或其国民铺设和经营海底电缆的国家……有权采取保护措施，以防止或终止任何有害干扰”。<sup>99</sup>而《塔林手册2.0》的结论是，国际习惯法禁止破坏海底电缆的网络行动，尽管它暗示在武装冲突中可以将海底电缆作为攻击目标，但必须遵守区分和相称原则。<sup>100</sup>它还表明，在武装冲突中通过海底通信电缆进行的网络攻击将使该电缆成为合法目标。两本手册都认定，现代通信电缆会引起有关《1907年公约》第54条的问题。其中《奥斯陆手册》特别指

<sup>90</sup> Lane Burdette (2021年)，《利用海底电缆获取政治利益：美国对中国战略的回应》《公共和国际事务杂志》，第4页，<https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy>；Hai Dang Vu(2020年)，《东盟加强海底电缆韧性和维修指南》，《国际海洋和海岸法期刊》36:1。

<sup>91</sup> “兹认为，本公约的各项规定毫不影响交战国的行动自由”，第15条，《1884年保护海底电缆公约》。

<sup>92</sup> 《陆战法规和惯例公约》（4号）及其附件：《陆战法规和惯例公约》（1907年），<https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907>。

<sup>93</sup> 同上，条例：第54条。

<sup>94</sup> 《适用于海上冲突的国际法圣雷莫手册》（1994年），第37款。请注意，《圣雷莫手册》是一组法律和海军专家在1988年至1994年期间以个人身份制定的“适用于海上武装冲突的国际法的当代重述”；参见<https://ihl-databases.icrc.org/en/ihl-treaties/sanremo-manual-1994>。

<sup>95</sup> 《塔林手册2.0版》对这一规定给予了特别关注，指出“由于海底电缆为网络通信提供便利，这一点与网络背景息息相关；Michael N. Schmitt(编纂)(2017年)，《网络行动国际法塔林手册2.0版》，第150条，第10款，第549页。另见Lane Burdette(2021年)，“利用海底电缆获取政治利益：美国对中国战略的回应”，《公共和国际事务杂志》，第3页，<https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy>，他强调“美国的先例允许在目标专属经济区内切断目标国和中立国之间的电缆，这一先例后来在1923年美英仲裁法庭上得到维持”，而《塔林手册》专家的评估并未反映出这一点。

<sup>96</sup> 迈克尔·施密特(Michael N. Schmitt)(编辑)(2017年)，《网络行动国际法塔林手册2.0版》，第54条，第1，第252-253页。

<sup>97</sup> 同上，第252-258页。

<sup>98</sup> 同上。

<sup>99</sup> Yoram Dinstein和Arne Willy Dahl(编纂)(2020年)，《武装冲突法若干专题奥斯陆手册：规则和评注》，第67条，第61页。

<sup>100</sup> 迈克尔·施密特(Michael N. Schmitt)(编辑)(2017年)，《网络行动国际法塔林手册2.0版》，第54条，第15款，第256页。

出，“只有在极少数情况下，才有可能确定它们专门为一个或多个交战方服务”，因此必须“区分海底通信电缆和其他海底电缆”。<sup>101</sup>

一些学者主张为影响海底电缆的活动提供额外的国际法律保护，包括商定一项新文书。<sup>102</sup>为此，有人建议“以[联合国]反恐公约体系”为指导。<sup>103</sup>其他人则采取了一种较为有限的方法，建议制定新的《联合国海洋法公约》条款，明确责任、义务和合规措施，并加强在打击犯罪活动方面的相互合作。<sup>104</sup>其他一些更为有限的方法建议在沿海地区的高价值通信走廊建立电缆保护区，尽管这可能会使电缆更加脆弱。<sup>105</sup>

一些学者还建议在联合国系统下设立一个负责海底电缆法律 and 政策的国际机构。<sup>106</sup>另有一些人建议利用国际海洋法法庭具有约束力的争端解决系统，“以创建一个保护海底电缆免受损害的国际制度”和“保护隐私权不受侵犯的国际制度”。<sup>107</sup>与此同时，学术界提出的更适用于武装冲突期间海底电缆的国际法建议，包括修订《1884年公约》关于交战行为的条款，禁止以实体或网络手段蓄意破坏电缆。另一项公约建议在冲突期间对海底通信电缆进行特别保护，类似于武装冲突期间对文化财产的保护。<sup>108</sup>还有人建议修改在确定目标<sup>109</sup>时适用相称性的普通规则。

<sup>101</sup> Yoram Dinstein 和 Arne Willy Dahl(编辑)(2020年)，《网络行动国际法塔林手册 2.0 版》，第 69 条，第 63 页。

<sup>102</sup> Robert Beckman, “海底电缆：故意损害的安全缺口”，道格拉斯·R·伯内特等人（2013年）编纂的《海底电缆：法律与政策手册》，BRILL 出版社；Tara Davenport (2015年)，《海底电缆、网络安全与国际法：交叉分析》，天主教大学法律与技术杂志 24(1)；Zoe Scanlon (2017年)，《解决专属国旗国管辖的缺陷：提升海底电缆保护的法律制度》，《海商法与商业杂志》48:3；Rishi Sunak (2017)，《海底电缆：不可或缺且易受攻击》，第 35-36 页，<https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>。

<sup>103</sup> Christian Bueger 和 Tobias Liebetrau (2021年)，“保护隐藏的基础设施：全球海底数据电缆网络的安全政治”，《当代安全政策》42:3，第 398 页。

<sup>104</sup> Tara Davenport (2015年)，“海底电缆、网络安全与国际法：交叉分析”，《天主教大学法律与科技杂志》24(1)。

<sup>105</sup> Rishi Sunak (2017年)，“海底电缆：不可或缺且易受攻击”，政策交流论坛，<https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>。在国际缆线保护委员会的《政府最佳做法》中，该委员会不推荐在固定的地理区域内建立缆线保护区和走廊，或者至少建议在采取这种做法时与电缆运营商进行协商。后者往往反对这种保护区和走廊，因为它们“（1）在安装和维护方面与其他海底电缆的空间分离不足，以及（2）鼓励海底电缆路线和登陆点的地理集中，这放大了单一自然或人为事件可能损坏多条电缆的风险”；国际缆线保护委员会（2022年），《保护和提高海底电信缆线韧性的政府最佳做法》，第 3 页，<https://www.iscpc.org/documents/?id=3733>。

<sup>106</sup> Christian Bueger 和 Tobias Liebetrau (2021年)，“保护隐藏的基础设施：全球海底数据电缆网络的安全政治”，《当代安全政策》42:3，第 399 页。

<sup>107</sup> Jason Petty (2021年)，“如何根据海洋法追究海底电缆黑客的法律责任”，《芝加哥国际法杂志》22:1。

<sup>108</sup> 例如，《1954年关于发生武装冲突时保护文化财产的公约》（该公约本身以武装冲突期间保护文化财产的原则、1899年和1907年《海牙公约》以及1935年《华盛顿公约》为指导）；参见 Dennis E. Harbin III (2021年)，“瞄准海底电缆：现代战争中武装冲突的新方法”，《军事法律评论》第 229 期，<https://tjagclcs.army.mil/documents/35956/304883/3+Harbin+Final.pdf>。

<sup>109</sup> 参见 Rob McLaughlin, Tamsin Phillipa Paige 和 Douglas Guilfoyle (2022年)，“海底通信电缆与武装冲突法：关于性质界定的某些持久不确定性及一些建议”，《冲突与安全法杂志》27:3。

## 海底电缆治理去向何方？

现有海底电缆治理体系有力表明其自身不足以应对本世纪的挑战。同样我们需要新型全球性文书，特别是考虑到我们对海底电缆连接的依赖，以及现行法律文书不能反映当前技术的本质。然而，许多专家坚称，现行国际法已然足够，各国在考虑新文书之前需要遵守现有的义务和承诺。即使各国同意有必要为专门保护海底电缆制定一项新条约，也可能需要数十年的时间来谈判，因为海底电缆系统虽然是信息和通信技术生态系统的关键要素，但也是众多要素之一，因此在条约范围上达成一致将颇为困难。如前所述，已提出了一些较为有限的方法，即重点增强现行文书。这些方法都有其价值，值得进一步探讨。

还有其他互补性方法可以加强海底电缆系统的治理体系和韧性。例如，可以考虑让军方更多地参与电缆保护和他安全，包括建立专门的协调机构；在具有战略意义的水域进行水下感应探测和侦查、海面巡逻以及卫星监控。<sup>110</sup>此外，还可以加强监管，特别是确保采用可信技术、保障维护和修复的主权能力<sup>111</sup>以及提升与电缆所有者和运营商的信息交流。<sup>112</sup>各类方法固然重要，但都是针对特定国家或区域的韧性和安全关切。还应当辅之以在全球范围内努力增强海底通信电缆韧性。

或许，开启这场全球对话的起点，应当是认识到我们面临的挑战具有系统性特征，并深入理解行业和技术社区已经在采取的风险缓解措施（例如，增加电缆路线和容量的多样性；采用零信任原则和技术，加强陆地基础设施和组件的安全性，提升用于系统监控的光学传感技术）。各国可在此基础上，通过推动执行和遵循与关键信息和通信技术基础设施相关的现有建议和新兴要求，来补充和完善这些努力。其中包括：

- 国际缆线保护委员会用于促进海底电信电缆韧性的最佳做法（其核心源自《联合国海洋法公约》），及其即将发布的关于海滩检查井、前端牵引设备和电缆登陆站的安全建议；
- 联合国就信息和通信技术与国际安全方面谈判达成的负责的国家行为框架的相关内容；<sup>113</sup>以及
- 国家和区域层面出现的新要求，包括欧盟网络和信息系指下的规定。<sup>114</sup>

这种关注虽然无法直接解决本文中提到的某些更为复杂的地缘政治难题，例如某些国家为了自身利益而威胁关键基础设施——如海底电缆系统——的行为。但无论如何，它能够推动我们保护和加固这些系统，以及与之相连的陆地和卫星网络，进而提升抗风险能力，并增强其在提供亟需的经济和社会利益方面的潜力。

<sup>110</sup> 例如，2022年2月15日宣布的新北约协调小组；另见 Rishi Sunak (2017年)，“海底电缆：不可或缺且易受攻击”，政策交流论坛，第35-36页 <https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>，第35-36页；Andreas Rinke and Matthias Williams (2022年)，“德国和挪威希望北约保护海底基础设施，以防北溪管道袭击事件重演”，路透社，

<sup>111</sup> 伊恩·道格拉斯 (2021年)，《英国关键海底电缆基础设施的未来保障》，全球海洋集团

<https://nationalpreparednesscommission.uk/2021/09/future-proofing-the-uks-critical-subsea-cable-infrastructure/>。

<sup>112</sup> 例如，参见2022年12月14日第2022/2555号指令（欧盟），<https://eur-lex.europa.eu/eli/dir/2022/2555>。

<sup>113</sup> 例如，参见 <https://www.un.org/disarmament/ict-security/>。

<sup>114</sup> 例如，2022年12月14日第2022/2555号指令（欧盟），<https://eur-lex.europa.eu/eli/dir/2022/2555>。

## 对特定工作的分析

国际缆线保护委员会政府的最佳做法是基于现有国际法政策、行业协议和标准、国家做法以及基本常识所制定的推荐建议。<sup>115</sup>它们涵盖一系列问题。例如，一般原则（第1节）建议各国在其国家韧性计划中应侧重于：

- 在统计学上显著的风险领域，政府行动能够最有效地降低风险；
- 在国家管辖范围内推动海底电缆登陆点的多样化；
- 遵守和履行界定国家管辖权和对海底电缆保护的现有国际义务及习惯法；
- 促进透明的监管制度，以促进电缆的快速铺设和按时维修；
- 与行业密切磋商，了解行业技术和运行参数，共享风险数据；
- 补充当前行业的最佳做法；
- 认识到法律和政府政策本身有时会加剧损害风险并降低抗风险能力；以及
- 在全球和区域基础上与其他国家互动，因为其他国家的行动会极大地影响单个国家自身的连通性。

### 国际缆线保护委员会政府最佳做法：缆线保护和韧性提升

1.一般原则
2.捕鱼和抛锚风险（70%的故障）
3.空间隔离
4.图表
5.国内电缆保护法；对损害的处罚
6.海洋空间规划和行业间协调
7.单一联络点
8.航线和着陆优化；地理多样性
9.安装和维修许可
10.舱位和船员限制
11.港口入境要求
12.关税、税费和费用
13.海洋边界主张和争端
14.关键基础设施指定
15.共享风险和事故数据
16.其他公海监管活动的影响。

表 1. 国际缆线保护委员会政府最佳做法

国际缆线保护委员会的最佳做法为各个主题领域提供了更详细的指导，这些领域是加强韧性的关键。例如，建议各国将海底电缆指定为关键基础设施，<sup>116</sup>收集和评估有关脆弱性和威胁的数据，并制定和实施减少这些脆弱性和威胁的政策，这可能会得到所有国家的认同。它还有助于优先关注和分配资源，并有助于区分无意风险及涉及国家和国际安全的风险。建立单一联络点以更好地协调政府在整个电缆生命周期内的行动、安装和维修许可的基本参数，以及电缆运营商和政府之间交换事故数据和威胁信息的机制，也将是向前迈出的重要一步。

<sup>115</sup> ICPC (2022 年)，《保护和促进海底电信电缆恢复能力的政府最佳做法》，<https://www.iscpc.org/documents/?id=3733>。

<sup>116</sup> 同上，第 4 章，第 5 页，指出国际海道测量组织第 4/1967 号决议要求国家和区域制图主管部门在所有海图中加入一个文本框，规定在电缆附近作业的最小距离，并“承认海底电缆是重要的基础设施”，对其造成的损害“可构成国家灾难”[着重部分由作者标明]；另见同上，第 3 节中关于空间隔离的讨论，该节也涉及决议的执行。

通过以符合《联合国海洋法公约》的方式，实施关于国内电缆保护法的推荐措施，可达成成果。这将确保对任何损害行为施加实质性的惩罚。海岸警卫队和其他相关执法机构将“需要对这些电缆保护法律有足够的了解，以便有效执行，并与电缆运营商携手合作，共同调查电缆损害事件”。<sup>117</sup>同样，提升政府对空间隔离、路径选择和登陆点问题的认识，有助于避免不当的政策选择，并促进快速采纳亟需的监管框架和资源分配。<sup>118</sup>此外，进一步明确各国实施这些建议性做法的具体情况以及所面临的挑战，对于当前讨论将是宝贵的贡献。借鉴联合国毒品和犯罪问题办公室及其他机构在支持会员国实施最佳做法方面的努力，也将极具价值。<sup>119</sup>

除了以上最佳做法之外，国际缆线保护委员会的电缆安全工作组还在努力为保护海底电缆基础设施的独特部分（如海滩检查井、前端牵引设备和电缆登陆站）制定建议。该建议不涉及网络或信息安全相关问题，认为“通信安全并非海底电缆独有的问题，电子通信网络的网络安全，这一领域已通过如ISO 27001等电子通信网络安全标准和国家级的网络安全框架得到了妥善处理”。<sup>120</sup>该建议发布后，推广并交流其实施进展，将对行业产生重要的影响和贡献。

在网络安全方面，一系列国际进展同样值得关注。例如，举例来说，联大第一委员会就信息和通信技术与国际安全问题进行的谈判，已逐步构建起一套关于国家负责任行为的框架，该框架中的若干要素明确指向了关键基础设施的保护。<sup>121</sup>事实上，政府专家组在2015年建议的三项与关键基础设施有关的规范中，第一项就涉及各国有责任“不开展或故意支持违反国际法义务的信息和通信技术行为，这些行为旨在蓄意破坏关键基础设施或阻碍其向公众提供服务”。<sup>122</sup>后续发布的两份报告在解释可能被纳入该规范的关键基础设施类型时，表明其包括为多个国家提供服务的设施，如“对互联网的普遍可用性和完整性起到关键作用的技术基础设施”，按照信息和通信技术生态系统的广泛逻辑，海底通信电缆亦被包含在内。<sup>123</sup>

同样适用的还有同一份报告中建议的另外两项与关键基础设施有关的规范，即“各国应采取适当措施保护其关键基础设施免受信息和通信技术的威胁，同时考虑到大会第 58/199 号决议”；<sup>124</sup>以及“各国应对其关键基础设施受到恶意信息通信技术行为侵害的其他国家提出的适当援助请求作出响应。同时，各国也应响应旨在减轻源自其领土、针对他国关键基础设施的恶意信息和通信技术活动的适当请求，并在行动中充分尊重他国主权”。<sup>125</sup>关于如何解读这些规范，

<sup>117</sup> 同上，第 5 节。

<sup>118</sup> 同上，例如第 3、6 和 8 节。

<sup>119</sup> 例如，参见 Kaithlin Meredith (2021 年)，“保护印度洋的海底电缆”，联合国毒品和犯罪问题办公室，<https://www.unodc.org/easternafrika/en/Stories/protection-of-submarine-cables-in-indian-ocean.html>。

<sup>120</sup> 2022 年 1 月 17 日与国际缆线保护委员会代表的通信。

<sup>121</sup> 相关报告见大会，联合国文件 A/70/174 (2015)，[https://digitallibrary.un.org/record/799853/files/A\\_70\\_174-EN.pdf](https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf)；联合国大会，联合国文件 A/76/135 (2021)，[https://front.un-arm.org/wp-content/uploads/2021/08/A\\_76\\_135-2104030E-1.pdf](https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf)；联合国大会，联合国文件 A/AC.290/2021/CRP.2 (2021 年)，<https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>。

<sup>122</sup> 联合国大会，联合国文件 A/76/135 (2021)，规范 13(f)，第 42–46 款，[https://front.un-arm.org/wp-content/uploads/2021/08/A\\_76\\_135-2104030E-1.pdf](https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf)。

<sup>123</sup> 同上。关于“对互联网的普遍可用性或完整性至关重要的技术基础设施”的观点源于荷兰提出的与互联网公共核心有关的建议，而这些建议又源于荷兰学者 Dennis Broeders 关于这一主题的研究成果，后来网络空间稳定问题全球委员会在其关于保护互联网公共核心规范的建议中采用了该观点。联合国相关报告见上文脚注 122。关于 Broeders 的出版物，参见 Dennis Broeders (2016 年)，“互联网的公共核心：互联网治理的国际议程”，荷兰政府政策科学委员会，<https://library.oapen.org/bitstream/handle/20.500.12657/32439/610631.pdf>。关于全球网络空间稳定性委员会的报告及其倡导的一项规范，即不干涉互联网的“公共核心”，该“公共核心”定义为包括“互联网基础设施的关键要素，如数据包路由和转发、命名和编号系统、安全和身份的加密机制、传输介质[包括陆上和海底电缆及其登陆站、数据中心以及其他支持它们的物理设施]、软件和数据中心”（第 30-31 页）。参加全球网络空间稳定性委员会(2019 年)，“推进网络稳定性：最终报告”，<https://hcss.nl/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf>。

<sup>124</sup> 联合国大会，联合国文件 A/76/135 (2021)，规范 13(g)，第 47–50 款，[https://front.un-arm.org/wp-content/uploads/2021/08/A\\_76\\_135-2104030E-1.pdf](https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf)。

<sup>125</sup> 同上，规范 13(h)，第 51–55 款。

2021 年另一政府专家组的报告提供了具体指导，并且该议题在更广泛的不限名额工作组中也有所触及。<sup>126</sup>

### 联合国关于关键基础设施的推荐规范

13(f) 各国不应违反国际法规定，故意破坏关键基础设施或以其他方式损害关键基础设施的使用和运行，并以此来向公众提供服务或故意支持有害的信息和通信技术活动。

13(g) 各国应根据联合国大会第58/199号决议，采取适当措施保护关键基础设施免受信息和通信技术威胁。

13(h) 各国应响应其他国家向本国发出的关于关键基础设施受到恶意信息和通信技术活动影响的援助请求。各国应响应其他国家向本国发出的关于关键基础设施受到恶意信息和通信技术活动影响的援助请求，并在行动中充分尊重他国主权。

表 2. 推荐的关键基础设施相关规范，2015 年政府专家组

这些谈判小组编写的报告中还有许多建议和结论，同样适用于海底电缆及其相关基础设施，并且应当受到广泛理解。其中包括对现行国际法，包括《联合国宪章》在各国使用信息和通信技术方面的适用性、关于规范的其他建议，<sup>127</sup>以及关于与保护重要基础设施有关的建立信任措施建议，包括关于国家之间以及与私营部门之间就威胁和脆弱性以及事故响应进行联系和交流的建议。<sup>128</sup>同样，了解各国在海底电缆和相关基础设施方面是如何遵守上述承诺，对于当前讨论将具有重要意义。

在区域层面，欧洲联盟在其最新版《网络和信息系统指令》中进一步发展了该思路，指出海底通信对“欧盟及其经济的竞争性数字”的重要性。<sup>129</sup>基于欧洲电信框架、《欧盟网络安全法案》和禁止攻击信息系统的指令2013/40/EU等现有框架，该指令通过引入新的报告要求，要求公司报告影响此类系统的事件，并将覆盖范围扩展至电信实体，从而深化了信息交换和事故报告的推荐措施。<sup>130</sup>《网络和信息系统指令》还呼吁各国政府在其国家网络安全战略中考虑海底电缆系统的网络安全问题，并勘察潜在的网络安全风险和制定缓解措施，“以确保提供最高级别的保护”。<sup>131</sup>具体而言，该指令呼吁成员国采取“维护开放互联网公共核心的普遍可用性、完整性和机密性，包括相关的海底通信电缆网络安全”。<sup>132</sup>目前正在努力协调该指令中的措施与近期其他文书中提出的措施。确保相关国家和行业行动方就执行这些措施定期进行双向交流，也将是对正在进行的讨论的重要贡献。

<sup>126</sup> 见脚注 122。

<sup>127</sup> 例如，见规范 13(c)，即所谓的“尽责”准则，各国据此承诺不故意允许其领土被用于利用信息和通信技术的国际不法行为；规范 13(e)，与保护人权有关；规范 13(i)，与确保供应链的完整性有关；联合国大会，联合国文件 A/76/135(2021)，规范 13(g)，第 47–50 款，[https://front.un-arm.org/wp-content/uploads/2021/08/A\\_76\\_135-2104030E-1.pdf](https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf)。

<sup>128</sup> 同上。

<sup>129</sup> 2022 年 12 月 14 日（欧盟）第 2022/2555 号指令，第 97 段，<https://eur-lex.europa.eu/eli/dir/2022/2555>。

<sup>130</sup> 2020 年 12 月 16 日第 COM/2020/823 号提案，<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0823>；2002 年 3 月 7 日第 2002/21/EC 号指令，<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0021>；2018 年 12 月 1 日第 2018/1972 号指令（欧盟），<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AAOJ.L.2018.321.01.0036.01.ENG>；2013 年 8 月 12 日第 2013/40/EU 号指令，<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040>。

<sup>131</sup> 2022 年 12 月 14 日（欧盟）第 2022/2555 号指令，第 97 段，<https://eur-lex.europa.eu/eli/dir/2022/2555>。

<sup>132</sup> 同上，第 7 条，第 2(d)段。

## 助力全球海底电缆系统提升韧性

为了在全球范围内增强海底电缆系统的韧性，并进一步完善与信息通信技术相关的负责任的国家行为框架，可以采取哪些措施？在考虑到前文内容的基础上，可将初步议程聚焦于以下几个方面。

### 海底通信电缆作为关键基础设施

海底通信电缆是信息和通信技术生态系统的重要组成部分。无论直接或间接，我们都依赖于此，因此确保将其视为关键基础设施符合我们共同的利益。在这方面，所有国家包括内陆国家在内，都应将其视为关键基础设施。此外，各国还可以采取以下措施：

- 各国公开重申对联合国在国际安全和信息通信技术工作中建议的三项关键基础设施相关规范及其他相关措施的承诺。各国可公开阐明其对这些措施的承诺，包括海底电缆和相关基础设施的措施，并在双边、诸边或多边论坛和协议中促进对这些措施的遵守。鉴于对蓄意破坏海底光缆系统或影响此类基础设施为公众提供服务的行为日益关切，各国也应努力推动对此类行为后果的讨论，尽管可能颇具挑战性。
- 根据现有义务和做法，各国需强化国内法律、监管架构和政策，以保护海底电缆及其相关设施，并提升其韧性，并明确国家主管部门的作用和责任。
- 各国应强化国家层面的海底电缆系统风险评估与管理策略、以及与应急响应和维修相关的应急准备，并完善对海底电缆及相关设施和组件受影响事故的分类与报告方法。
- 各国就落实国际缆线保护委员会的建议和最佳做法以及即将出台的陆地基础设施安全建议进行经验交流。
- 各国交流在争议海域或自然灾害期间电缆维修的互助合作经验，以及为电缆船维修提供便利的经验，为危机情况建立应对机制。
- 各国交流海岸警卫队和执法部门在调查电缆中断或其他非法活动的合作经验。
- 各国就现有国际法如何适用于危机和冲突中电缆中断或破坏的观点，包括蓄意针对海底电缆组件和基础设施的军事行动，或造成无意破坏的间谍行动，从而影响网络可用性并损害电信和数据流量传输，发布并交流国家观点。
- 各国确保为脆弱国家提供更多的国际援助和能力建设资源，以维护海底电缆基础设施和其他类似设施和系统的实体和网络安全，及国内法律法规的制定和执行。<sup>133</sup>

### 加强公私合作

私营公司拥有并运营着大多数海底电缆系统，对影响系统的威胁和漏洞有着重要见解，并拥有管理和降低风险的长期经验。新的报告要求促进公共和私营行动方之间的更深层次合作。然而，与其他领域一样，这种关系既带来诸多益处，也存在一定妥协。培养这种关系需要时间，而且往往是在信任基础相对薄弱的情况下起步。为确保不断涌现的国家和区域层面的新报告要求能够达成其提升韧性的目标，各国应与产业界和其他相关行动方互动，以加强对以下方面的相互理解：

- 海底电缆系统在更广泛的信息和通信技术生态系统中的地位；
- 为克服当前包括信任缺失等数据共享障碍的激励-问责结构，以及借鉴其他敏感环境中现有最佳做法的潜在安全可信信息共享模式；
- 海底通信电缆系统及其相关依赖性的演变趋势；
- 供应链漏洞；

<sup>133</sup> Christian Bueger 和 Tobias Liebetrau (2021 年)，“保护隐藏的基础设施：全球海底数据电缆网络的安全政治”，《当代安全政策》42:3，第 402 页。

- 海底电缆系统故障和中断的趋势，以确定影响国家或国际安全以及全球金融体系稳定的潜在高风险低概率事件，并更好地明确在此类情况下的职责分工；以及
- 行业管理和降低海底电缆系统风险的方法，以及技术和其他进步助力提升系统的保护与韧性。

### 全面且基于原则的政策议程

关于海底电缆系统的安全性和韧性，确实存在合理关切。然而，将政策辩论过度安全化于海底电缆问题上，可能会引发一系列问题。首先，当前的政策走向有可能进一步分裂全球互联网，阻碍创新和竞争，其长期后果可能远远超过一个更具韧性和互联系统所带来的益处。此外，这样做还可能使发展中国家规划和实施亟需的数字基础设施项目时，偏离透明度、可持续性和问责制等关键原则。而且，也有可能使这些项目偏离以人为本的核心目标，例如确保那些传统上未被充分服务的群体能够享受到更广泛连通性带来的社会和经济效益，这与可持续发展目标9的宗旨相悖。<sup>134</sup>在这方面，各国在继续高度重视安全性和韧性的同时，还应确保：

- 在国内、区域和国际政策议程中处理海底电缆问题时保持适当平衡；
- 就国家安全驱动的路由、融资和投资决策可能产生的社会、经济和环境权衡问题，展开更具包容性的讨论；
- 在海底电缆基础设施项目的规划和实施过程中，加强与相关行动方的磋商，例如目前正在多个发展及基础设施计划中考虑的项目；<sup>135</sup>以及
- 在实施此类倡议时，提升透明度，展示如何更广泛地应用可持续性和问责制等广泛认可的原则。

<sup>134</sup> C.卡瓦纳（即将出版），“纽带.....”，该文件为在曼谷举行的 SubCom 年度会议做准备。

<sup>135</sup> 美国蓝点网络，<https://www.dfc.gov/our-work/blue-dot-network>；中国“一带一路”倡议（参见<https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative>）及相关“和”“全球发展倡议”（参见[https://csis-website-prod.s3.amazonaws.com/s3fs-public/event/220912\\_Global\\_Development\\_Initiative.pdf](https://csis-website-prod.s3.amazonaws.com/s3fs-public/event/220912_Global_Development_Initiative.pdf)）；欧盟的“全球门户战略”，[https://commission.europa.eu/priorities-2019-2024/stronger-europe-world/global-gateway\\_en](https://commission.europa.eu/priorities-2019-2024/stronger-europe-world/global-gateway_en)；七国集团的“全球基础设施发展伙伴关系”，<https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/26/fact-sheet-president-biden-and-g7-leaders-formally-launch-the-partnership-for-global-infrastructure-and-investment/>；美国-欧盟贸易与技术委员会联合声明，2022年12月5日，<https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/05/u-s-eu-joint-statement-of-the-trade-and-technology-council/>。

## 结束语

海底通信电缆作为全球信息和通信技术生态系统的关键要素，承载了几乎所有的电信和数据传输，这一事实正日益得到广泛认同。它们的安全性和韧性对于全球社会的福祉和运作至关重要。同时，尤其是在当前地缘政治紧张不断升级的背景下，各区域国家对于这些电缆安全的合理担忧也为人所共知。鉴于此，当前的状况迫切需要我们采取一种更加全球化和协作性的方法，以增强系统的韧性。本报告强调了当前缆线治理体系中的若干缺陷，同时阐明了有助于保护缆线和提高缆线韧性的其他做法和建议措施。其建议主要针对国家，但也承认工业界和其他行动方在这方面的核心作用和持续努力。其建议表明，所有国家都应将海底通信电缆视为关键基础设施，并与行业行动方互动，了解正在进行的增强韧性的举措，并确定可靠且安全的信息共享方式。此外，报告还强调了在政策制定过程中，我们需要采取一种更全面且基于原则的方法来考虑海底电缆问题，以防止议程的过度安全化。其目的并非回避或批判现有在国家或区域层面保护和确保海底电缆系统安全的做法，而是要确保所有国家和区域都能负责任地贡献力量，共同维护一个更加安全、更具韧性的信息和通信技术生态系统。

## 《海洋法公约》中与海底电缆有关的条款

<p><b>第三条</b> <b>领海的宽度。</b></p> <p><b>第二十一条</b> <b>沿海国关于无害通过的法律和规章。</b></p> <p><b>第三十三条</b> <b>毗连区。</b></p>	<p>每一国家有权确定其领海的宽度，直至从按照本公约确定的基线量起不超过十二海里的界限为止。</p> <p>1.沿海国可依本公约规定和其他国际法规则，对下列各项或任何一项制定关于无害通过领海的法律和规章：(c) 保护电缆和管道；</p> <p>1.沿海国可在毗连其领海称为毗连区的区域内，行使其为下列事项所必要的管制：(a)防止在其领土或领海内违犯其海关、财政、移民或卫生的法律和规章；(b) 惩治在其领土或领海内违犯上述法律和规章的行为。</p> <p>2.毗连区从测算领海宽度的基线量起，不得超过二十四海里。</p> <p>专属经济区从测算领海宽度的基线量起，不应超过二百海里。</p>
<p><b>第五十七条</b> <b>专属经济区的宽度。</b></p> <p><b>第五十八条</b> <b>其他国家在专属经济区内 的权利和义务。</b></p>	<p>1.在专属经济区内，所有国家，不论为沿海国或内陆国，在本公约有关规定的限制下，享有第八十七条所指的航行和飞越的自由，铺设海底电缆和管道的自由，以及与这些自由有关的海洋其他国际合法用途，诸如同船舶和飞机的操作及海底电缆和管道的使用有关的并符合本公约其他规定的那些用途。</p> <p>2.第八十八至第一一五条以及其他国际法有关规则，只要与本部分不相抵触，均适用于专属经济区。</p> <p>各国在专属经济区内根据本公约行使其权利和履行其义务时，应当适当顾及沿海国的权利和义务，并应遵守沿海国按照本公约的规定和其他国际法规则所制定的与本部分不相抵触的法律和规章。</p>
<p><b>第七十九条</b> <b>大陆架上的海底电缆和管道。</b></p>	<p>1.所有国家按照本条的规定都有在大陆架上铺设海底电缆和管道的权利。</p> <p>在沿海国采取合理措施勘探大陆架、开发其自然资源和保护、减少和控制管道污染的前提下，沿海国不得妨碍铺设或维修这些电缆或管道。</p> <p>在大陆架上铺设这种管道，其路线的划定须经沿海国同意。</p> <p>本部分的规定不影响沿海国为进入其领土或领海的电缆或管道规定条件的权利，也不影响沿海国对为勘探其大陆架或开发其资源或在其管辖下的人工岛屿、设施和结构的作业而建造或使用的电缆和管道的管辖权。</p> <p>5.铺设海底电缆和管道时，各国应当适当顾及已经铺设的电缆和管道。特别是，修理现有电缆或管道的可能性不应受妨碍。</p>
<p><b>第八十六条</b> <b>本部分规定的适用。</b></p>	<p>本部分的规定适用于不包括在国家的专属经济区。领海或内水或群岛国的群岛水域内的全部海域。本条规定并不使各国按照第五十八条规定在专属经济区内所享有的自由受到任何减损。</p>
<p><b>第八十七条</b> <b>公海自由。</b></p>	<p>1.公海对所有国家开放，不论其为沿海国或内陆国。公海自由是在本公约和其他国际法规则所规定的条件下行使的。公海自由对沿海国和内陆国而言，<i>除其他外</i>，包括：(a)航行自由；(b) 飞越自由；</p> <p>(c) 铺设海底电缆和管道的自由，但受第六部分的限制；(d) 建造国际法所容许的人工岛屿和其他设施的自由，但受第六部分的限制；(e) 捕鱼自由，但受第二节规定条件的限制；(f) 科学研究的自由，但受第六和第十三部分的限制；</p>
<p><b>第一一二条</b> <b>铺设海底电缆和管道的权利。</b></p>	<p>2.这些自由应由所有国家行使，但须适当顾及其他国家行使公海自由的利益，并适当顾及本公约所规定的同“区域”内活动有关的权利。</p> <p>1.所有国家均有权在大陆架以外的公海海底上铺设海底电缆和管道。</p> <p>第七十九条第 5 款适用于这种电缆和管道。</p>
<p><b>第一一三条</b> <b>海底电缆或管道断裂或受损。</b></p>	<p>各国应制定必要的法律和规章，规定悬挂其国旗的船只或受其管辖的人故意或因重大过失，破坏或损伤公海海底电缆，致使电报或电话通信中断或受阻，以及破坏或损伤海底管道或高压电力电缆，均为应予惩处的罪行。此项规定也应适用于故意或可能造成这种破坏或损害的行为。对于仅为了保全自己的生命或船舶的正当目的而行事的人，在采取避免破坏或损害的一切必要预防措施后，仍然发生的任何破坏或损害，此项规定不应适用。</p>
<p><b>第一一四条</b> <b>海底电缆或管道的所有人对另一海底电缆或管道的破坏或损害。</b></p>	<p>每个国家应制定必要的法律和规章，规定受其管辖的公海海底电缆或管道的所有人如果在铺设或修理该项电缆或管道时使另一电缆或管道遭受破坏或损害，应承担修理的费用。</p>

**第一一五条**  
**因避免损害海底电缆或管道而遭受的损失赔偿。**

每个国家应制定必要的法律和规章，确保船舶所有人在其能证明因避免损害海底电缆或管道而牺牲锚、网或其他渔具时，应由电缆或管道所有人予以赔偿，但须船舶所有人事先曾采取一切合理的预防措施。

**第二九七条**  
**适用第二节的限制。**

1. 关于因沿海国行使本公约规定的主权权利或管辖权而发生的对本公约的解释或适用的争端，遇有下列情形，应遵守第二节所规定的程序：  
(a) 沿海国在第五十八条规定的关于航行、飞越或铺设海底电缆和管道的自由和权利，或关于海洋的其他国际合法用途方面，有违反本公约的规定的行为[。]