观点

如何确保 IP 网络韧性

2023 年 9 月

Simon Sherrington

目录

图表列表

本白皮书由华为资助生成，白皮书的使用受我们版权声明中的条款和条件的约束。Analysys Mason 不为供应商的任何产品或服务背书。

本白皮书包含了 T/ZGTXXH072-2023《计算网络融合网络基础设施 IP 网络韧性规范》的详细信息，由（1）中国信息通信研究院；（2）华为；（3）中国联通研究院；（4）中国电信研究院；（5）中国科学院计算机网络信息中心。我们从华为收到了规范的详细信息。我们已采取合理和适当的谨慎措施，以适当的详细程度对所提供的材料进行了交叉检查和调查。对于因提供给我们的材料中的错误或遗漏而造成的损害或损失，Analysys Mason 不承担任何责任。

1. 执行摘要

消费者和企业使用的大多数数字服务都在 IP 网络上运行，IP 网络为宽带和移动服务以及企业数据网络提供了骨干传输基础设施。由电信服务商运营的最大的全国性网络连接了数千个网元、数亿个消费者和企业客户设备以及数十亿个物联网设备。由银行等大型组织运营的 IP 网络支撑着使这些组织能够正常运作的关键数字基础设施。IP 网络互连了每天有数十亿人使用的最大互联网内容和应用程序提供商的数据中心。

因此，当 IP 网络的某些部分出现故障时，其影响可能是重大的。中断导致宽带和移动服务下线，切断了整个国家与互联网的联系，阻止金融机构处理支付，阻止大型社交媒体公司提供服务，阻止人们拨打紧急服务电话。IP 网络的大规模故障可能会造成严重的后果，而且代价也会非常高昂。然而，IP 网络中断的情况非常频繁。

这一切都清楚地表明，各行业都需要投资于提高其 IP 网络的韧性能力。确保网络的韧性意味着确保在发生非常事件的情况下，服务水平可以维持在可接受的水平。这些事件可能包括设备故障、恶意攻击或人为错误。确保网络韧性并不等同于监控可靠性，也不等同于网络安全。确保韧性意味着采取战略性方法，通过改进网络的架构和配置来提高网络的健壮性，以便先发制人并预防问题的发生。而是从设计开始建设网络韧性。

尽管 IP 网络故障带来了负面影响，但许多组织并没有尽其所能来预防和预防问题。根据 Analysys Mason 于 2023 年 8 月对 IP 网络运营商进行的一项调查，不到一半（43%）的受访者表示他们进行了风险分析或故障模拟，或网元运行状况检查，只有 26%的受访者表示他们模拟了网络上的攻击，不到 20%的受访者表示他们进行了故障生存性或灾难韧性分析。[1]

一系列障碍正在阻止 IP 网络的运营商为确保 IP 韧性做更多的工作。这些问题包括缺乏内部专业知识，缺乏预算和时间，或者无法观察网络内正在发生的事情：专业技能不足尤其重要；人为错误会导致大量的停机——例如，在系统升级或系统重新配置期间人为错误。

提高 IP 网络韧性的传统方法已经可能已经无效，因此各行业需要考虑一种新的方法。考虑到风险的规模，以及提高 IP 网络韧性的潜在好处，运营商需要从战略的构建韧性策略。他们需要努力通过设计来实现 IP 网络的韧性——确保韧性是内置的，并且网络架构、设备配置、服务结构和操作流程都设计为避免问题，或者在不影响客户的情况下缓解问题。

[1]这项调查包括 23 名受访者，他们都为运营 IP 网络的公司工作，这些公司经历了 IP 网络的中断或下线。所有参与调研的公司的年收入至少为 5 亿美元，22%的公司的年收入超过 200 亿美元。

组织可以通过使用韧性成熟度模型对其韧性水平进行基准测试，并衡量其提高 IP 网络韧性的举措的进展。该模型应详细说明专门为确保网络韧性而设计的指标和评估标准，并使组织能够评估其网络不同部分的 IP 韧性水平。

IP 网络运营公司应部署支持对 IP 网络进行详细可视化分析的工具和服务。IP 韧性的设计要求对设备、配置、网络拓扑、流量和服务利用率进行全方位的视图。它要求能够分析设备、系统、配置、流量或服务更改、故障或恶意攻击的潜在影响。IP 网络的运营公司应该投资于一个端到端的工具，以实现网络数字孪生的详细可视化。

各行业可以使用数字孪生网络来测试复杂的场景，并在一系列威胁、问题和故障的背景下评估网络的性能和韧性能力。通过使用与现实世界网络匹配的数字孪生，可以在一个安全的环境中进行测试和评估，然后再对现存系统进行修改。孪生网络可用于测试新的网络架构和配置，以便预测和避免问题，从而提高业务连续性和业务成果。

2. 各行业必须更加关注网络韧性

- IP 网络的重要作用和日益复杂的问题
- IP 网络公司遭受的重大中断示例
- 网络中断造成的损坏和损失，包括调查数据

2.1 IP 网络在支撑关键应用和服务方面发挥着至关重要的作用

IP 网络是全球通信服务的基础，为宽带和移动服务以及企业数据网络提供骨干传输基础设施。IP 网络为海量设备提供服务。由消费者服务提供商运营的最大的全国性网络连接着数千个网元，数亿个消费者和企业客户设备，以及数十亿个物联网设备。由银行等大型组织运营的 IP 网络支撑着使这些组织能够正常运作的关键数字基础设施。IP 网络互连了每天有数十亿人使用的最大互联网内容和应用程序提供商的数据中心。IP 网络是许多支持紧急服务通信的网络的基础，因此，如果这些网络出现故障，人们在紧急情况下就无法轻易地呼救。IP 网络是任何大型通信服务提供商、政府或大型企业的关键基础设施的一部分。如果没有 IP 网络，人们就无法访问他们所依赖的服务。

尽管 IP 网络在确保全球数字连通性方面具有重要意义，尽管 IP 网络被用于支持越来越多的服务（例如面向消费者的流媒体服务和游戏，关键政企服务），这些服务不容忍网络性能差，但 IP 网络是尽力而为的网络，而不是最初设计以保证服务水平。它们相当健壮——但基于旨在实现全球信令、寻址和流量路由的基础设施，并根据从网络其他部分接收的信息在本地做出决策。这使得如果配置不正确，它们很容易传播问题。IP 网络被设计为使用统计复用和尽力转发。路由是基于路由的可用性逐跳（由路由器）流转的。这导致流量容易发生拥塞，从而导致延迟和丢包。几乎没有整体的控制和可见性。

与此同时，IP 网络也变得越来越复杂。设备的功能范围从能够为单个家庭或分支机构提供服务的本地用户设备，到驻留在运营商和企业核心网络中的多千兆或太比特设备。IP 网络很少包含来自单一供应

商的设备。它们通常是多供应商环境。设备运行的协议（例如 IPv4 或 IPv6）也有很大的差异。企业网络可以运行数十万台设备；服务提供商网络甚至可以拥有数百万台设备。

企业和政府网络也在发生变化，以适应构建和操作 IT 系统以提供服务的新方式。由大型组织（如银行）运营的 IP 网络正在演变为包括多云环境中托管的应用程序（包括公共云和私有云解决方案），应用程序从分布在多个地点的数据中心管理或交付。这些分布式云和数据中心架构需要响应迅速、高韧性和高度安全的网络，以确保中心和远程或分支站点的员工可以访问服务，以及客户可以每周 7 天、每天 24 小时访问服务。

IP 网络也正在以更复杂的方式使用。IP 网络的运营商正在引入需要端到端可视性和服务管理的服务和应用。可以部署流量工程来确保选定的客户、服务、应用或路由的服务质量。多个重叠系统（例如，IP 域控制器、网络管理系统和 SDN 层）可用于影响网络如何运行或如何管理流量。

然而，对人来说，看到和理解整个网络中发生的事情（无论是在物理层、协议层、切片层和服务层），实在太挑战了。IP 网络的规模和复杂性已经超出了人脑的极限，这使得传统依赖人力确保 IP 网络的业务韧性变得越来越难。

2.2 故障可能会导致严重停机

IP 网络故障可能会导致服务大规模和长时间的中断，影响数百万用户，有时会长达数小时。主要停机的公共示例包括以下。

- 加拿大的运营商 A (2022 年 7 月）——由路由器错误配置导致的持续近 20 小时的加拿大全境服务中断。此次停电影响了数千万客户，并导致有线、固定电话和无线网络服务的损失，包括客户无法拨打紧急服务电话。

- 日本的运营商 B（2022 年 7 月）——一次巨大的停电，影响超过 3000 万手机用户以及关键业务服务（如 ATM、送货和天气系统）超过 3 天。此次故障是由于在日常维护过程中，核心传输网络中的路由器配置错误，导致一系列问题的发生。配置错误导致 VoLTE 网络内的位置登记功能中断（VoLTE 呼叫需要终端进行位置登记）。这触发了大量的重传，进而导致了交通拥堵。分布式处理导致了拥塞的进一步蔓延。更糟糕的是，用户数据库不堪重负。VoLTE 节点和移动分组网关必须对每个呼叫进行身份验证-每次重新传输都会导致一个新的请求，并导致用户数据库中的数据不一致。这引发了更多的问题。运营商 B 用了超过 72 小时才修复了故障。

- 2021 年 10 月，韩国的运营商 C 遭遇全网中断，导致固定和移动服务无法运行超过 1 小时。服务的损失影响到学校、医疗服务、金融交易组织和消费者。中断最初被归因于网络攻击，但运营商 C 随后证实，边界网关协议（BGP）配置错误导致了停机。

- 2020 年 4 月，据信由 BGP 优化器导致的边界网关协议（BGP）配置错误导致与 8000 个前缀相关的流量（包括与 Akamai、Amazon、Cloudflare Facebook 和 Google 相关的流量）通过俄罗斯

Rostelecom 的网络路由，然后出现黑洞。尽管 Rostelecom 撤销了这些路由，但它们已经被其他一些 ISP 传播到了对等点。问题持续了大约 5 个小时。[2]

- 2020 年 1 月，冈比亚国家运营商 Gamtel 宣布全面互联网中断，影响全国超过 8 小时。故障是由于备份链路上的网卡故障导致的——连接该国与互联网的主要海底电缆的电缆中断。[3]

欧盟网络安全局（ENISA）报告了该地区的网络安全事件。其报告《电信安全事件 2021》指出，2021 年欧洲的网络运营商报告了 168 起事件，损失超过 50 亿用户小时的服务。受安全事件影响的主要资产是寻址服务器（23%）和交换机和路由器(18%)。5 年来，交换机和路由器是事故的最大原因，占 2017 年至 2021 年向 ENISA 报告的所有事故的 18%。[4]

由 IP 网络问题引起的中断并不限于电信服务提供商。2021 年 10 月，Facebook（现为 Meta）的 Facebook、Instagram、Whatsapp 和 Messenger 平台遭遇数以亿计的用户中断数小时。在一份公开声明中，该公司表示，故障是由于在其数据中心之间协调流量的主干路由器的配置更改导致的。众所周知，IP 网络问题也导致了金融机构和其他主要国家关键基础设施提供商的中断——尽管根本原因通常不会公开。

2.3 IP 网络故障会造成重大损失和经济成本

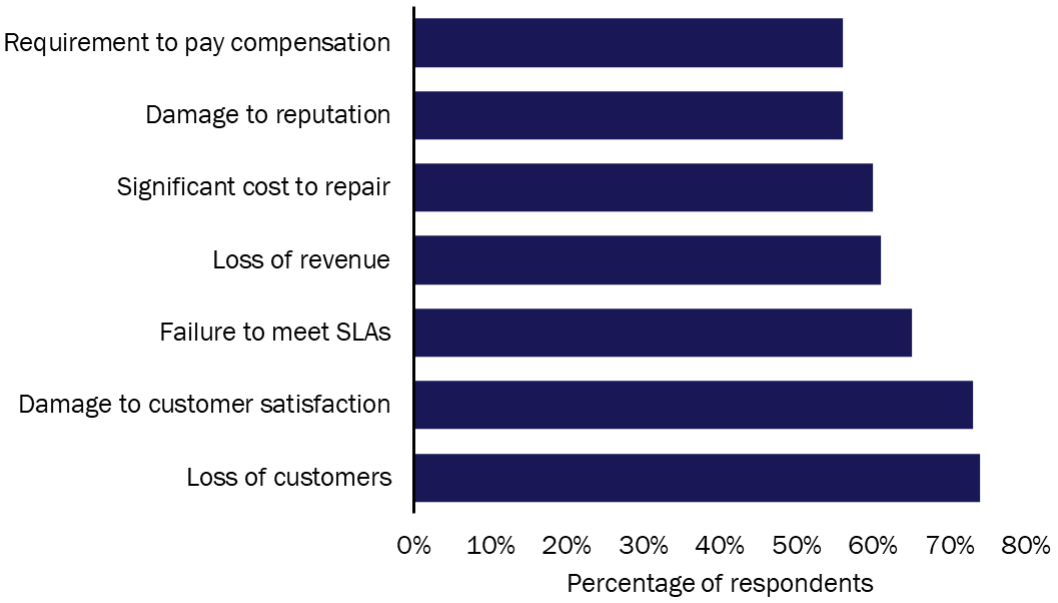
Analysys Mason 在 2023 年 8 月对大型 IP 网络的运营商进行了调查，以了解 IP 网络故障的程度和影响。这些答复表明，IP 网络故障可能会对组织产生重大的破坏性影响。74%的受访组织表示 IP 网络故障导致客户流失，73%的组织表示 IP 网络故障损害了客户满意度。57%的受访者表示，由于 IP 网络故障，他们被要求向客户支付赔偿。

2 Rostelecom's Route Hijack Highlights Need for BGP Security (thousandeyes.com)

3 The Gambia's Internet Outage Through an Internet Resilience Lens (internetsociety.org); https://twitter.com/Gamtel/status/1478310096639770625

4 https://www.enisa.europa.eu/publications/telecom-security-incidents-2021?v2=1

图 2.1:IP 网络中断造成的损害类型-承认每种损害类型的受访者百分比 21[5]



Source: Analysys Mason

损失的规模可能是巨大的。2022 年 7 月中断后，Rogers 经历了巨大的公众危机，随后承诺了为期 3 年的 100 亿加元投资计划，以提高其网络韧性。运营商 B 也遭受了财务影响，近 280 万无法使用服务超过 24 小时的客户，有权从每月账单中扣除 2 天的订阅费用，总共超过 3600 万客户平均每人可以从账单中扣除 200 日元。

IP 网络故障造成的损害并不局限于公开的例子。当被问及过去一年中组织中最严重的 IP 网络故障时，Analysys Mason 调查的公司表示，他们在过去 12 个月中经历的最严重的中断影响了大量客户。近一半的受访者表示，中断影响了 40%或更多的客户。这些单个中断的财务成本规模经常超过 2000 万美元，在一个案例中超过 1 亿美元。[6]

5 Question: “What impact have IP network failures had on your business? (IP network failures have never caused this / have sometimes caused this / have often caused this).”

6 Question: “Thinking about the worst IP network outage you have suffered over the last year, please estimate:

- How many hours were services down? Enter the number of hours.
- What was the percentage of customer affected? Enter the percentage value.
- What was the total cost (including lost revenue, compensation to customers, and cost to fix)? Enter the cost in units of USD million.”

图 2.2：受去年网络中断影响最严重的每家受调查公司的客户百分比 22[7]

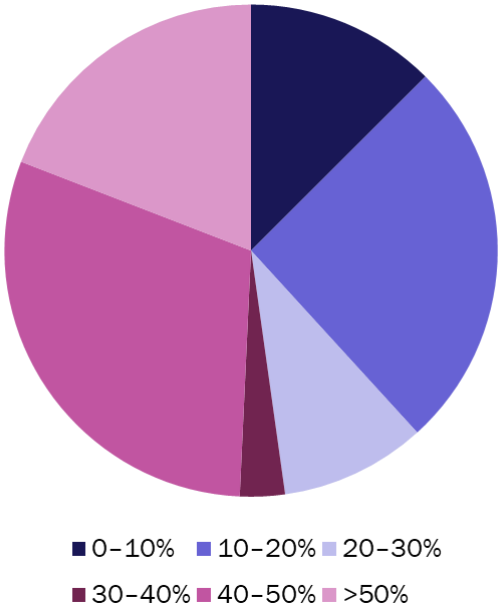
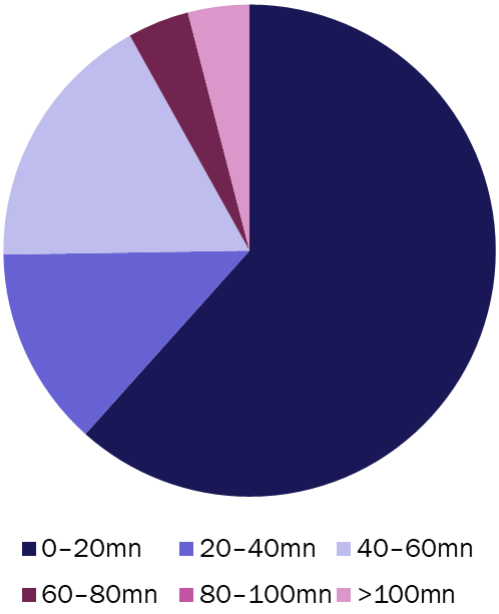


图 2.3：每家受访公司去年网络中断最严重的总成本（美元）23[8]



来源：Analysys Mason

调查结果证明，确保 IP 网络的韧性必须是 IP 网络运营商战略的关键组成部分，否则会造成重大损害。

3. 传统的准备和预防网络事故的方法并非最佳

- 拥有 IP 网络的组织所使用的系统和流程的差距，包括调查数据
- 提高 IP 网络韧性的组织障碍，包括调查数据

3.1 组织的 IP 韧性保证战略存在许多差距

Analysys Mason 对 IP 网络运营商的调查显示，公司采用了多种方法来确保 IP 网络的韧性。IP 网络审计通常至少每月进行一次（69%），约 26%的人声称他们会持续进行此类检查。这突出了一个事实，即大多数公司在审计实践中至少在某种程度上是主动的。然而，调查结果也揭示了审计过程中的重大差距。

7 Does not sum to 100% due to rounding.

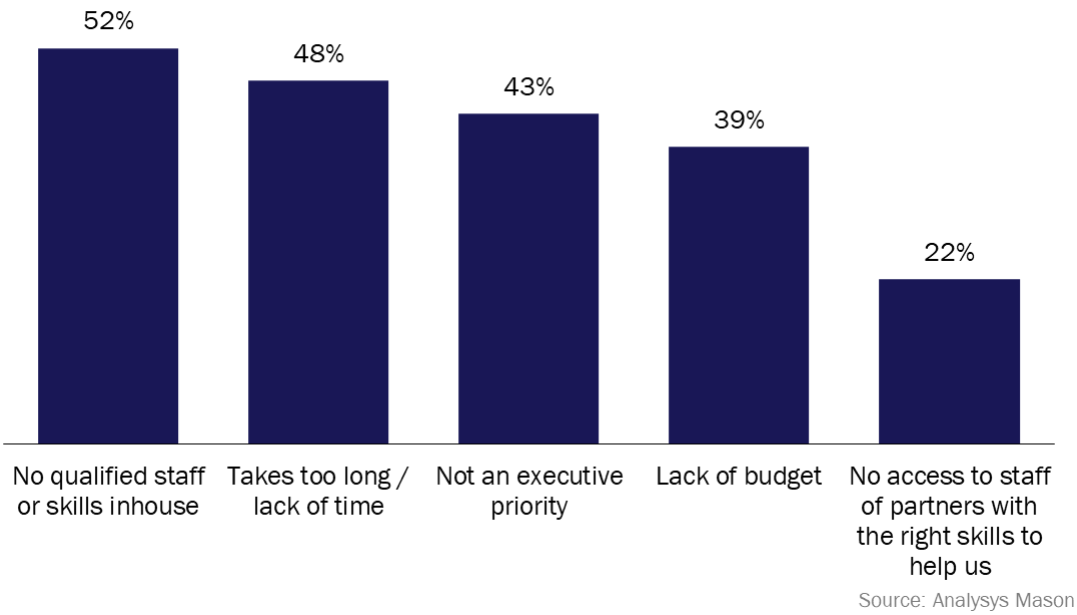
8 Does not sum to 100% due to rounding.

值得注意的是，在 Analysys Mason 调查的所有受访者中，只有大约一半的人报告他们系统地进行了网络拓扑分析或 IP 优化分析，不到一半（43%）进行了风险分析或故障模拟或网络元素运行状况检查，只有 26%模拟了网络攻击，不到 20%进行了故障生存性或灾难韧性分析。[9]

3.2 组织在确保 IP 网络韧性能力方面面临巨大障碍

公司在确保其 IP 网络的韧性能力方面受到一系列组织和技术因素的阻碍。提高 IP 网络韧性的组织障碍包括缺乏内部技能（超过 50%的受访者表示），以及时间和预算不足。43%的受访者还表示，防止 IP 网络中断不是其公司内部高管的优先事项。

图 3.1：确保 IP 网络韧性能力的组织障碍 31[10]



技术壁垒也阻碍了公司提高 IP 网络的韧性。Analysys Mason 调查的受访者最常提到的障碍包括无法足够详细地观察 IP 网络行为（74%的受访者）和缺乏实时信息（52%的受访者），以及 43%的受访者提到的一系列其他因素（如缺乏对拓扑、服务性能和单个设备配置的掌握）。

3.3 需要一种新的方法

很明显，各企业均了解其 IP 网络对支持其服务和客户的服务的重要性，而且很明显，他们正在采取一系列措施来在意外事件发生时维持服务。然而，确保网络韧性能力的传统方法存在漏洞和薄弱点，并且无法防止严重的网络中断，显然需要一个新的战略。各企业均需要考虑更广泛的措施方案，包括对广泛的网络指标进行评估和测量，采用新的韧性评估方法，以及引入工具，以实现对网络中正在发生（或可

9 Question: “Which of the following activities do you undertake to pre-empt and prevent failures? Select all that apply.”

10 Question: “What factors have hindered or limited your ability to prevent IP network outages? Select all that apply from the list of organisational factors.”

能发生）的情况的改进和更精细的可视化。他们还应该考虑根据结构化框架对其网络的韧性进行基准测试，这样他们就可以清楚地判断其系统的韧性。

4. 组织需要从网络规划阶段开始确保网络韧性能力

- 从设计开始提升韧性
- 创建数字孪生的好处
- 使用韧性成熟度模型评估 IP 网络的韧性
- 使用数字孪生评估架构的薄弱点并测试异常事件

4.1 确保网络的韧性意味着在非常情况下，业务可以继续运行

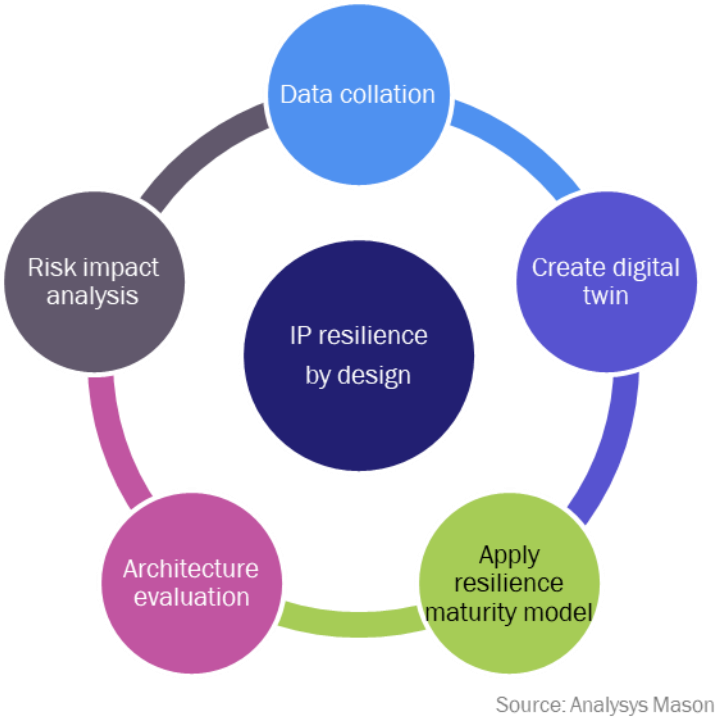
证据清楚地表明，如果组织要避免网络中断可能对其业务造成的灾难性故障和损害，就需要投资提高其 IP 网络的韧性能力。

确保网络的韧性意味着确保在发生非常事件的情况下，服务水平可以维持在可接受的水平。这些事件可能包括设备故障、恶意攻击或人为错误。确保网络韧性与监控可靠性不一样。网络在大多数时候都可以具有非常高的可靠性水平，但当出现问题时，仍然可能会出现非常严重的故障——尤其是当问题影响了整个基础设施。但这也不意味着确保网络安全——这也是至关重要的。确保韧性意味着采取战略性方法，通过改进网络的架构和配置来提高网络的健壮性，以预防和预防问题。它涉及通过从设计开始构建韧性，以便在发生安全问题时，或发生导致网络问题的事件时，可以在尽可能快的时间内缓解、控制和解决这些问题，并将服务和客户的中断降至最低。

4.2 IP 网络的运营商需要“从设计开始”提升韧性

对于 IP 网络的运营商来说，关键的是要制定可靠的策略，使他们能够识别问题的根本原因，快速修复问题，实施架构或配置更改以降低未来停机的可能性，并在出现问题时使 IP 网络更具韧性。仅仅监控正常运行时间和服务可用性级别是不够的。依靠人在压力下不犯错是不够的。IP 网络的运营商需要一个全面的数据收集、可视化、分析和 IP 网络优化的计划——所有这些都以明确的指标为基准，他们需要先发制人地找出原因并建模解决方案。

图 4.1：按设计的 IP 网络韧性 41



此过程的起点是运营商了解其当前的网络架构和配置，并能够可视化它们。

4.3 将分布在多个孤岛上的数据结合起来，并详细的分析

IP 网络运营商要采取的第一步是详细了解其 IP 基础设施的当前状态。这需要收集各个网元、IP 网络拓扑、行为、以及在网络上运行的服务的数据。

需要针对配置、位置和利用率级别等因素对单个网络元素进行审计。审计必须包括最终用户驻地的设备以及核心 IP 网络内的设备。考虑到大型 IP 网络中网络元素的年龄、类型和位置的混合，一些数据收集和聚合可能需要使用各种系统手动进行。

考虑到可能需要审核数千台设备，配置是一个特殊的挑战。理想情况下，将对照已知配置问题的数据库检查设备的配置，并使用基于软件的方法自动执行该过程。手动替代方案将非常耗时。这是任何韧性改进策略的重要部分，因为众所周知，配置错误会导致 IP 网络中的重大错误。

然后，这些数据可以在可视化工具中汇集起来，以便进行分析。

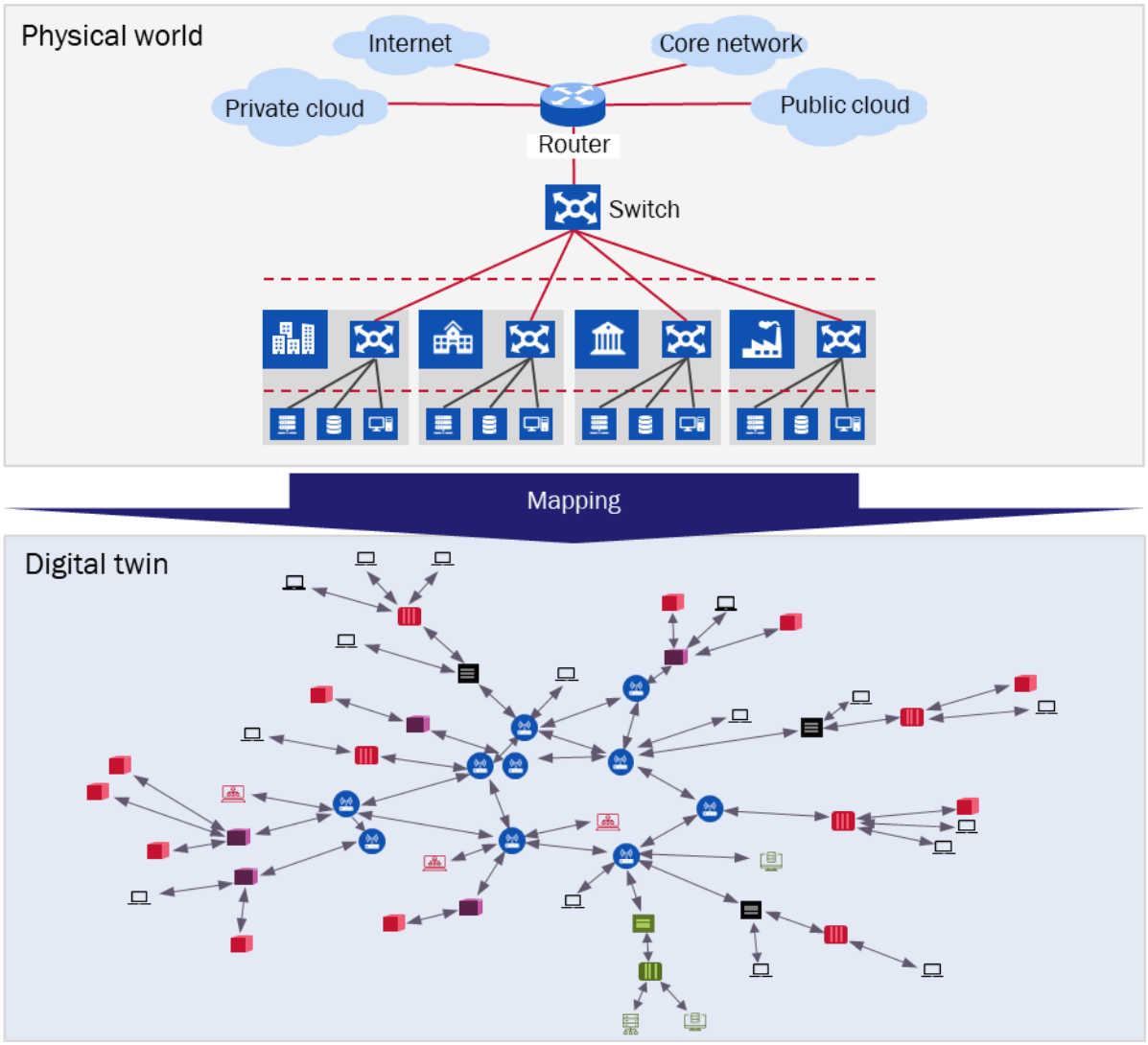
4.4 创建网络的数字孪生可实现高级可视化和评估

在大多数情况下，对 IP 网络的韧性能力进行详细评估所需的数据很可能存在于各种数据孤岛中，并跨多个系统。Analysys Mason 的调查显示，很少有 IP 运营商有一个工具可以用来进行复杂的、整体的

元素、拓扑、流量和服务分析。74%的受访公司表示，无法足够详细地观察网络行为是确保和提高 IP 网络韧性的障碍。

克服这种情况的一种方法是使用软件和高级可视化技术来构建 IP 网络的数字孪生（图 4.2）。

图 4.2:IP 网络的数字孪生 42



来源：Analysys Mason

创建数字孪生意味着将所有相关的数据集集成在一个工具中，并使用先进的可视化技术来创建一个整体的数字版本的网络，最终将物理世界映射到数字世界。

数字孪生实现了所有网元、物理和逻辑拓扑、流量利用率级别和流量的可视化。有了对 IP 网络内正在发生的事情的详细了解，就可以确定薄弱点，并确定提高网络韧性能力的机会。通过模拟恶意攻击、服务提供商故障、环境灾难、设备故障和操作或配置错误，数字孪生还可用于分析广泛可能场景下的网络

韧性。这些模拟将识别其他薄弱点，或优化机会，从这些模拟中学习的知识可以用于对现实世界的网络进行进一步改进。

至关重要的是，创建数字孪生可以在网络本身内进行更改之前，评估潜在的威胁及其对服务的影响。人为故障是 IP 网络中断的重要原因。ENISA 的报告指出，人为错误是其报告的所有事故的 23%的原因，这些事故通常是灾难性的，占所有损失小时数的 91%。Analysys Mason 对 IP 网络运营商的调查还调查了 IP 网络故障和中断的原因。这也证实了人类活动的影响。虽然设备故障在调查受访者列举的故障原因中占重要位置，但人为错误也是如此；57%的受访者报告了因系统升级期间的错误导致的停机，39%的受访者报告了因重新配置期间的错误导致的停机。使用数字孪生可以使 IP 网络运营商避免一些人为引起的错误。组织可以在安全的环境中测试网络调整、优化和维护活动，然后再对现网进行调整。

4.5 根据韧性成熟度模型评估 IP 韧性，可以显示需要改进的地方

组织可以通过根据 IP 韧性成熟度模型评估网络，来衡量其提高 IP 网络韧性的计划进展。中国通信学会（CIC）开发了 IP 韧性成熟度模型的一个示例。起草了适用于各类 IP 网络运营商的规范。它旨在确保五个操作阶段的韧性：预防、检测、响应、韧性和持续适应。[11]

该规范设想了五个级别的韧性（级别 5 是最具韧性的），并建议网络的不同部分应具有针对性，以实现不同级别的韧性——例如，核心网络应实现韧性级别 5，而标准互联网服务应实现韧性级别 3 或以上。

该规范建议在六个方面（图 4.3）评估韧性。

图 4.3:IP 韧性评估模型 43

	1 级	2 级	3 级	4 级	5 级
抗同时冲击次数	0	1	2	3	4
业务影响程度	>30%	<=30%	<=20%	<=10%	<=5%
业务恢复感知	天	小时数	分钟级	秒	微秒
故障扩散范围	全网	全网	仅 BGP 域	仅 IGP 域	单站
网络恢复能力	弱	相对较弱	相对强势	相对强势	强强
故障感知能力	弱弱	相对较弱	相对强	相对强	强的

来源：中国通信学会

该规范规定了在这六个领域中的每一个领域进行分析的详细指标。

- **抗同时冲击次数**：衡量网络能够承受并发模拟攻击的次数。在 5 级时，它可以承受 4 次并发攻击。
- **业务影响程度**：衡量受影响的服务级别，范围从 30%以上的客户服务受影响到 5%以下的客户。更详细的评估指标包括业务质量（丢包、时延、跳数）、受影响客户比例等。
- **业务恢复感知**：业务韧性所需的时间。

11 More details are available from https://www.ttbz.org.cn/StandardManage/Detail/84652.

- **故障扩散范围**：衡量故障传播的广度。要达到 5 级状态，故障仅限于单个站点。该领域的评分可以包括技术部署情况和激活的软件协议，包括软硬件补丁部署、二三层防环路协议部署、二三层故障域隔离、BGP 故障隔离等因素。
- **网络恢复能力**：评估核心网业务运营、网络管理与维护的物理分离，接入网业务运营与网络管理与维护的物理或逻辑分离，以及账号登录策略等方面的管理架构。
- **故障感知能力**：IP 网络运营商实时可视化网络拓扑和网络服务路径的能力；实时监控路由器和内部网关协议(IGP)和 BGP 活动以及警报的能力；通过延迟、带宽和数据包丢失等指标查看实时网络质量。

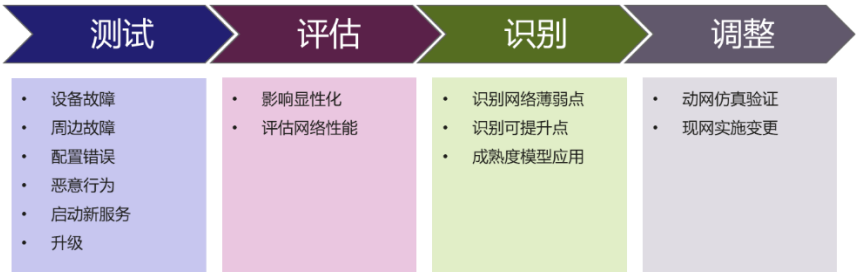
该规范为这些领域中的每一个都规定了详细的评分机制。

通过一个可用作评估框架的模型，组织可以评估其起点，并可以监控其在提高 IP 网络的韧性方面的进展。

4.6 利用现网数据进行动态测试，支持 IP 网络精细化

通过使用现网的数字孪生，运营商可以测试网络在一系列场景下的行为和韧性（图 4.4）。可以直观地分析可能导致部分或全部网络出现故障或以次优化的方式运行的异常事件的风险和影响。

图 4.4: IP 网络韧性场景分析 44

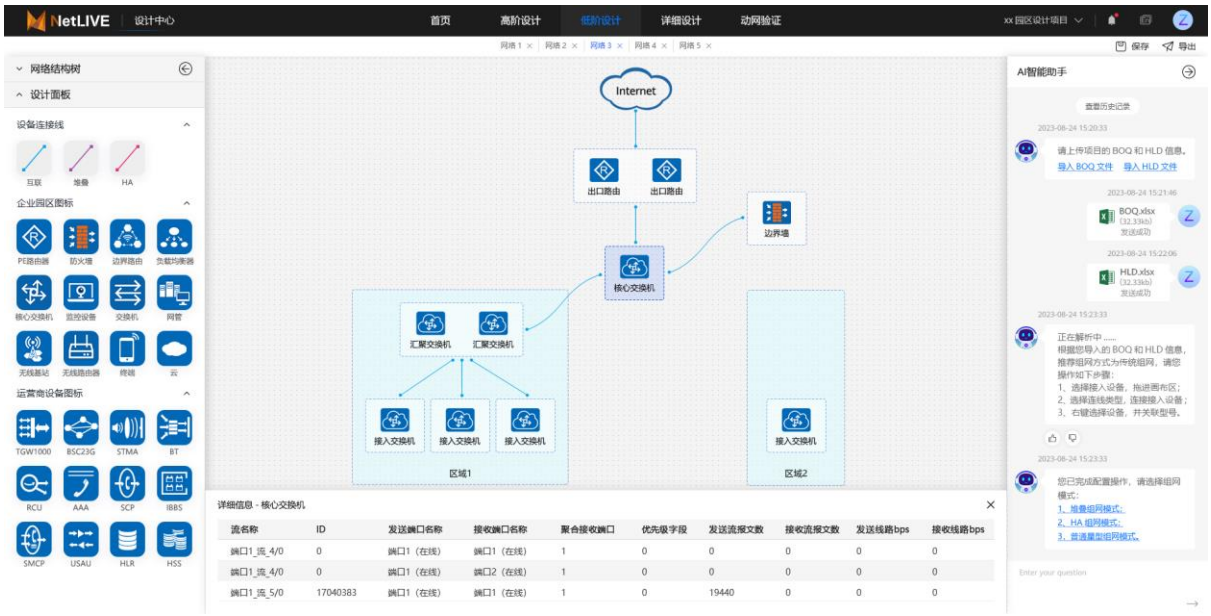


通过在数字孪生网络中引入受控和不受控干扰的混合，可以测试多种场景。这些可能包括针对设备故障、配置错误或故障的外部原因（如恶意活动或环境灾难）推出新服务或系统升级的管理。理想情况下，可以在一系列不同的场景下对网络进行压力测试，网络规划人员可以直观地看到结果。可以评估网络不同部分的性能，以确保核心区域具有更高水平的韧性能力，并为不重要的站点或服务提供足够的韧性能力。

4.7 数字孪生可用于测试架构变化

许多问题的出现是因为 IP 网络架构的设计并没有最大限度地提高韧性。单点故障导致了 IP 网络的大段故障，以及它所支持的服务。一旦网络的数字孪生被开发出来，就有可能审查 IP 网络的整体结构，并实时分析拓扑和使用的路由。通过高级可视化，IP 网络运营商可以进行详细的架构评估。可以分析是否需要改变现有结构，以及在网络中引入新的分层级别或网状拓扑，或者使用 IGP/BGP 保护机制是否可以提高韧性能力。

图 4.5：利用数字孪生分析网络薄弱点 45



来源：华为

IP 网络运营商可以审查任何架构变化对规避问题能力的影响，以及其提高韧性的模型，并考虑服务影响、故障限制和韧性速度等因素。审查还可能包括对 IP 网络上运行的服务的评估，包括容量利用率、服务水平协议（SLA）的审查和体验质量。

当识别出薄弱点时，可以调整数字孪生以确定如何先发制人、防止或最小化停机的影响，或确保更快地韧性。一旦在数字孪生中安全测试了这些变化，就可以适应现网。

5. 结论和建议

证据表明，IP 网络故障和中断会对 IP 网络的运营商及其客户造成重大影响。不投资于 IP 基础设施的韧性的组织可能会受到声誉损害、客户满意度降低、收入或客户损失以及要求向客户支付赔偿。大规模停电发生得太频繁了，而且后果很严重。确保网络韧性的传统方法显然是不工作的。

组织应考虑新的方法和系统来确保其 IP 网络的韧性。提高 IP 网络的韧性的积极好处可能包括改善客户体验、提高客户满意度以及避免成本和损失。由于将避免收入损失，对提高 IP 韧性的投资也可能带来收入的增加。此外，新的工具和方法可以帮助组织提高业务连续性，避免在进行重要投资时出现问题，例如从 IPv4 升级到 IPv6、新服务部署或新网络部署。

5.1 主要建议

组织应该采取几个步骤来确保 IP 网络的韧性。

- **建议 1。从战略角度出发，提高 IP 网络的韧性，从设计上确保 IP 的韧性。**显然，许多 IP 网络的运营商正遭受 IP 网络故障的负面影响。此外，他们还可以采取许多额外的预防措施，以预防和避免或限制 IP 网络中断。这就需要 IP 的韧性设计——确保韧性是内置的，并且网络架构、设备配置、服务结构和操作流程都设计为避免问题，或者在不影响客户的情况下缓解问题。
- **建议 2。根据成熟度模型评估韧性。**使用一个详细的模型来设定韧性目标，并提供明确的指标、要采取的步骤和衡量这些指标的方法，可以帮助组织提高其 IP 网络的韧性。该模型可用于评估起点，以及朝着同类最佳的韧性所取得的进展。
- **建议 3。部署工具和服务，提供 IP 网络的整体视图和可视化分析。**IP 韧性的设计要求对设备、配置、网络拓扑、流量和服务利用有一个整体的视图。它要求能够分析设备、系统、配置、流量或服务更改、故障或恶意攻击的潜在影响。IP 网络的运营商可以访问有关其 IP 网络性能的许多数据集，尽管这些数据集通常分布在一系列不同的应用中。IP 网络的运营商应该投资于单一的工具或服务，使他们能够在单一的应用程序中组合他们可用的所有不同数据源的数据。该应用程序应能够实现网络数字孪生的详细可视化。
- **建议 4。组织应使用数字孪生进行详细的场景测试。**这可以使他们在一系列压力条件下评估网络性能，并在实际网络中进行配置或架构更改之前进行试验。他们可以在韧性成熟度模型的上下文中评估网络的性能，以确定是否需要调整。

6. 附：华为韧性网络解决方案

随着企业的数智化和智能化转型，通信基础设施在企业内部越来越重要，逐渐成为企业日常运营和发展的神经中枢。但随着业务的不断发展，网络架构随之演进，网络的复杂度不可避免地提升，由此导致了网络韧性风险提升，最终导致网络应对不确定冲击的能力降低和业务韧性受到挑战。

华为作为领先的网络设备和服务提供商，勇敢面对行业挑战，与合作伙伴一起探索行业最佳实践，为全面系统性地提升韧性能力，在可靠性、可用性、经济性、风险预测和商誉保障等方面为客户做出贡献，推出华为韧性网络解决方案。

华为韧性网络解决方案以华为的四大能力积淀为基础：从芯片、单板到网络的 E2E **产品技术能力**，全球风险和故障库的**经验沉淀**，行业头部客户的网络**实践**，和从感知到动网的**系统性平台**。在此基础之上，依托 **NetLIVE** 平台，应用 IPDRR 理论框架，构建了从识别到恢复的全套解决方案，全面解决通信、银行、能源等多个行业面临的韧性问题，为客户打造**“防得住”**、**“扛得稳”**和**“可逃生”**的韧性网络，方案全景图，如图 1 所示:

图 1：华为韧性网络解决方案全景图

该方案的核心平台为 **NetLIVE**，其架构为五大技术引擎+四大能力中心，对外以“云+边”的形态提供服务，见图 2：

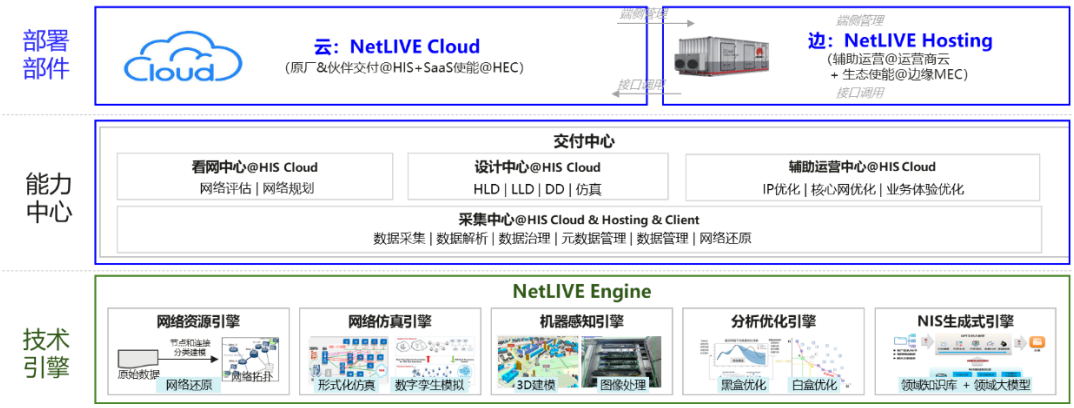


图 2：Netlive 平台架构

四大能力中心：

采集中心：提供数据的采集、存储和建模能力，基于采集资产库构建数据开放能力，为各中心提供数据输入，是整个交付作业的数据中心。

看网中心：支撑看网讲网流程，提供网络管理、看网诉求管理、线索管理、里程碑管理等能力；构建跨域看网能力，集成单域看网能力，沉淀看网经验，降低看网门槛；看网报告结构化在线管理，看网报告自动生成。

设计中心：支撑网络设计和动网验证活动完成，通过 AIGC 和智能交互，输出场景化的设计文档和验证报告，同时支撑现场（远程）交付和企业交付进行能力调用。

辅助运营中心：承接辅助运营 RA 架构的实施和监控环节，基于 Cloud 的大数据&AI 分析能力向客户提供业务性能优化服务，辅助收入提升。

五大技术引擎：

网络资源引擎：通过对采集的网络数据进行还原处理，并对数据进行结构化、模型化存储，描述运营商网络的某个状态，并持续记录此变化。该引擎可作为其它引擎的基础，提供用于分析&优化的特定网络数据底座。典型场景为：网络还原、网络建模、网络动态库等。

网络仿真引擎：基于单域产品线已有的仿真能力，提供形式化配置验证，机理驱动建模，数据驱动建模，混合建模方法及自动化测试等能力，用于网络规划，设计，测试，变更等场景的推演分析。典型场景为：流量负载影响仿真、业务路由&流量仿真
、两网合并交付过程推演等。

机器感知引擎：提供图像识别、视频验收、瑕疵检测、3D 建模&渲染、AR 渲染等能力，用于工程勘察、可视化设计、质检验收等场景，并可外溢到 xToB 各类场景。典型场景为：光缆哑资源设备检测、设备数字化建模&测量、行业应用瑕疵检测等。

分析优化引擎：提供白盒优化（可利用数学公式表达目标及约束，寻找最优解）、黑盒优化（通过不断与仿真系统交互，寻找最优解）及大数据挖掘能力，用于数据采集、网络规划、设计和辅助运营等场景的最优方案求解。典型场景为：两网合并选站方案、家庭宽带潜客识别、数字化物流车间调度等。

网路集成服务生成式引擎：沉淀网络专业知识和华为网络集成服务专有知识，通过交互式界面提供知识和技能辅助，提升一线网络规划、设计和作业效率，用户数据采集、网络规划&设计和现场作业等场景。典型场景为：MV IP 配置翻译、MOP 文档生成、企业园区网络智能辅助设计等。

当前以 **NetLIVE** 为基础的华为韧性网络解决方案，已为部分头部客户提供服务，在现网配置核查、容灾改造、生存性优化和防信令风暴和流控等多个领域取得优异成果，获得客户好评。

7. 关于作者

Simon Sherrington（研究总监）领导了 Analysys Mason 的新的传输网络战略研究项目，以及已建立的电信战略和预测项目。他还负责扩大 Analysys Mason 的研究预测和跨项目的思想领导力。他在行业有近 30 年的经验，曾担任分析师、顾问、市场研究员和出版人。在此期间，他对电信业务的许多不同方面发表了评论和建议。他的简历包括广泛的任务，涵盖固定和移动设备和网络、运营商战略、基础设施发展，以及涵盖零售和批发以及商业和消费者服务的项目。Simon 加入 Analysys Mason 的时候来自他在 2005 年创立的 Innovation Observatory，旨在帮助在电信、媒体、IT 和环境技术领域工作的客户。在此之前，Simon 曾在 Analysys Mason 工作多年，担任过包括定制研究主管在内的多个职位，职业生涯早期他曾在 CIT 出版公司（当时是一家电信和媒体报道的出版商）工作。除这些之外，Simon 还拥有埃克塞特大学的法学士学位。