



战略文章

Editorial cutoff: 25 October 2026 · Publication: 26 October 2026

一切都在运转。我们究竟知道什么？

一次打击让云落回地面：海湾与沙特的数字繁荣悖论

The Digital Prosperity Paradox: Cloud Infrastructure, Common-Cause Failure, and Saudi Service Continuity

MERIDIAN | 第一篇战略文章 M01 | 2026 年 10 月 25 日 | 分析范围：2026—2035 年

导语：战争期间，海湾地区的美国云设施受损。暴露出来的与其说是技术本身的弱点，不如说是某些成功指标一直忽略的问题：当服务及其记录共同依赖的场所遭到破坏，究竟还能留下什么？本文考察数字国家如何兼顾效率与持续运行能力，梳理我们对沙特实际知道什么，以及在宣布安心或恐慌之前还需要检验什么。

编辑说明：文中事实均注明来源和日期。有关沙特系统韧性的判断属于假设和条件性推论。配图与模拟采用公开说明的合成数值，不对应任何具体的沙特设施或服务。

1. 云第一次发现自己脚下有土地

技术语言让我们每次谈到“云”（Cloud）时都不由得抬头。我们想象它无处不在、随处可用，地理似乎只是一张列表，我们从中选择离用户最近的位置。2026 年 3 月，这种想象不得不迅速落回地面。

3 月 2 日，路透社（Reuters）转述了亚马逊云科技（Amazon Web Services；AWS）的一则更新：该公司在阿拉伯联合酋长国（United Arab Emirates）的两处设施遭到直接打击，巴林（Bahrain）一处设施附近的无人机袭击则对基础设施造成了物理损坏。公司提到建筑受损、供电中断，以及灭火行动对部分设备造成影响。故障波及多项云服务；鉴于损坏性质，公司预计恢复将耗时很久。据报道，事件发生在战争期间伊朗袭击海湾国家的背景下。[S05](#)

这里不涉及秘密技术位置或目标地图，也不需要这些信息。一个一般事实已经足够：看似无所依附的服务，依赖真实的场所、真实的电力、真实的进入通道，以及能够修复损坏的人员。数据几乎可以按光速传输；更换毁坏的设备、确保人员安全进入设施、重新配置复杂系统，却服从完全不同的时间尺度。

随后出现的信息改变了整个故事的性质。2026 年 9 月 15 日，据路透社（Reuters）跟进的公司更新，AWS 已无法恢复访问那些仅托管在巴林受损云区域内的资源 and 数据，也无法恢复访问阿联酋一处受损可用区中的此类资源。公司称，巴林的损坏涉及多个可用区，超出了其区域级和多区域服务原本设计的承受范围。公司仍在协助客户从其他区域恢复业务。[S07](#)

“仅”这个字值得停下来细读。因这一条件而无法恢复访问的内容，被绑定在现有恢复机制无法跨越的地理和技术边界内。亚马逊（Amazon）表示，拥有可用副本或可迁移资源的许多客户则能够在其他地点恢复运行。[S06S07](#) 因此，同一事件同时提供了两类证据：某些承受边界被突破，以及迁移和持续运行路径取得程度不一的成功。

在写下“整个数字区域已经崩溃”之前，我们必须先说清楚：哪个区域、哪些资源、哪些服务、哪一段时间。在写下“所有数据都丢失了”之前，我们也应再读一遍“仅”这个字。准确并非破坏叙事张力的官僚程序；它防止叙事张力破坏事实。

2. 成功本身制造的悖论

问题出在设计哲学上。共享网络越快、越便宜、越容易维护，就越有吸引力。各机构无须分别建立独立的身份、支付、托管或运行监控系统，可以使用专业化的共享能力。使用规模越大，收益也可能越高：经验集中积累，一处故障修复后，众多用户都能受益。这些是真实的潜在收益，并非投资推介中的装饰。

但让收益流动的连接，也可能让损害流动。如果五项服务共享一个关键依赖，故障发生时，问题就会同时涉及五项服务，即使每项服务都有优秀的界面、安全认证和良好的运行记录。研究者把这种可能性称为共因故障（Common-Cause Failure），把故障影响在相互依赖的层级之间传播称为级联故障（Cascading Failure）。

这并不意味着所有集中化都是错误，也不意味着所有分布式设计都能幸免。分布式系统可能在多个位置复制同一个软件缺陷，增加协调成本，也可能使冲突数据更难核验。集中化则可能带来专业管理、统一流程、故障预警，以及小型机构难以单独建设的备用能力。关键不在图中节点的数量，而在其故障原因是否独立、是否存在有效替代方案，以及人们能否安全地继续工作。

把假设说清楚就是：一体化数字化可能提高常态下的平均服务质量；但若众多功能集中依赖一组会同时失效的条件，它也可能扩大某些冲击造成的损失。如果一体化带来更好的备用能力、更清晰的运行信息和更快的恢复，结果也可能相反。因此，我们把这个问题称为数字繁荣悖论（The Digital Prosperity Paradox）：它是关于成功条件及其连带影响的假设，并非预设好的定罪结论。

3. 三个沙特数字，三个不同问题

这个问题与沙特阿拉伯（Saudi Arabia）有关，因为当地技术应用的扩张赋予它经济和社会分量。但测量首先要尊重每个数字的含义，而不是把数字堆在我们偏好的结论周围。

指标	数值及其所描述的时期	发布机构与正确的推论边界
互联网普及率 (Internet Penetration)	2026 年发布的《Saudi Internet 2025》报告称为 99.6%	通信、空间与技术委员会 (Communications, Space and Technology Commission; CST)。这是按报告定义计算的普及指标，不衡量危机期间每项数字服务能否持续。 S01
数字体验成熟度指数 (Digital Experience Maturity Index)	2025 年一轮评估覆盖 50 个政府平台，结果为 86.71%	数字政府管理局 (Digital Government Authority; DGA)。指标涵盖受益人体验等方面，不等于共因冲击下业务恢复的概率。 S02
网络安全市场规模	2025 年为 163 亿沙特里亚尔，报告发布于 2026 年 10 月 14 日	国家网络安全管理局 (National Cybersecurity Authority; NCA)。这是产品与服务市场规模，不代表故障成本，也不是恢复测试的绩效指标。 S03

这些指标在各自领域都有用。普及率说明按该测量定义，接入十分广泛；体验成熟度反映受评服务渠道质量的某些方面；网络安全市场规模描述经济活动与投资。三者都没有直接测量：同步故障后，有多少必要请求在可接受时间内完成，有多少被延误，以及恢复用了多久。

这三个高数值可能与高韧性同时存在，也可能与某种指标尚未检验的依赖同时存在。仅凭表格，我们不能推出其中任何一种结论。我们知道的是，高度使用技术的国家值得测量技术在运行条件改变时还能发挥什么作用。要作出判断，目前缺少的是有时间约束的服务数据、恢复演练，以及经过授权的聚合依赖测量。

数字管理语言里有一种不动声色的反讽：一份报告可以描述页面打开速度、用户对按钮的满意度、接入平台的机构数量，却因为评估表里没有这一项，把中断后如何恢复的问题留白。如果报告的目的本来就是测量体验，这不是报告的缺陷。真正应受质疑的是，我们要求它证明一种它从未被设计用来测量的能力。

4. 系统恢复了，人们的生活还在排队

先把战争事件与它检验的一般机制分开。2024 年 7 月，CrowdStrike 的一个组件向 Windows 设备推送错误更新，引发大范围技术故障。公司承认该缺陷，并确认事件并非网络攻击 (Cyberattack)。[S08](#)

7 月 22 日，英国国家医疗服务体系 (National Health Service; NHS) 的一家地方机构宣布，其所列服务使用的 EMIS 病历与预约系统已经恢复，但中断期间积压的工作仍在延误处方请求处理和纸质记录录入。[S09](#)

这则范围不大的机构说明揭示了更大的问题：软件恢复，不会自动清除等待它处理的工作。如果团队在故障前有 50 项按时提交的请求，系统恢复时面对的却是 100 项积压任务，那么屏幕可能已经显示绿色，用户的生活却仍未回到正常轨道。这里的数字只是说明性示例，并非该机构的数据。

接入与功能之间还有更危险的落差。在澳大利亚 (Australia)，澳大利亚通信与媒体管理局 (Australian Communications and Media Authority; ACMA) 认定，2023 年 11 月 8 日 Optus 网络中断导致 2,145 名用

户无法接通紧急呼叫服务，并有 369 次应当进行的安全回访在呼叫失败后未能完成。这是监管机构对特定事件的计数，并非伤亡人数或医疗结果。[S10](#)

我们现在面对三种不同的事实：部分云资源无法恢复；医疗系统在积压工作完成之前已经上线；通信网络未能送达一种价值与时间密切相关的请求。这些例子不属于同一机构或同一国家，也不能证明沙特阿拉伯发生了同类情况。但它们说明，成功的定义为何必须从必要服务出发，纳入安全、时效和积压，并一直延伸到用户端。

5. 数学说了什么，又没有说什么？

2010 年发表于《自然》（Nature）的一项研究中，谢尔盖·布尔季列夫（Sergey Buldyrev）等人建立了相互依赖网络模型。模型表明，在特定条件下，从一个网络移除少量元素可能削弱依赖它的另一个网络，继而使损害级联回到第一个网络。其行为可能与分别检验每个网络的强度有很大差异。[S11](#)

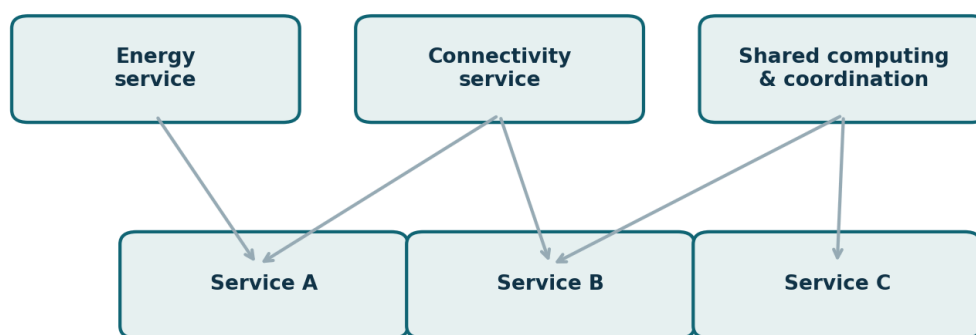
这个观点看似直观，直到我们看清它的含义：供电层能跨过某些故障，通信层也能跨过某些故障，并不能自动保证复合系统也能跨过故障，因为控制通信依赖电力，而部分电力运行又依赖通信。各部分的强度不能简单相加，变成整体的强度。

科学本身也提醒我们警惕“连接越多，脆弱性越高”这句话。2017 年发表于《物理评论 X》（Physical Review X）的一项研究中，菲利波·拉迪基（Filippo Radicchi）与吉内斯特拉·比安科尼（Ginestra Bianconi）在另一种多层网络（Multiplex Networks）模型下说明，**冗余相互依赖（Redundant Interdependencies）**可以提高稳健性。一个节点需要所有路径同时工作，和只需多条有效且独立的路径中任意一条工作，两者有决定性差别。[S12](#)

想象一扇门，需要三把钥匙同时使用才能打开。钥匙越多，可能阻止你开门的条件也越多。再想象另一扇门，三把分别保管的钥匙中任何一把都能打开。此时，选择反而增加了。两扇门都有“三把钥匙”，依赖的含义却不同。这个比喻说明的是模型逻辑，并不把门变成真实的基础设施。

系统科学从更早的思想史中得到过相近启示。查尔斯·佩罗（Charles Perrow）在《常态事故》（Normal Accidents）中区分复杂交互与部件的紧密耦合，说明为何高风险系统中的某些故障难以预测。[S14](#) 赫伯特·A·西蒙（Herbert A. Simon）在 1962 年发表的《复杂性的架构》（The Architecture of Complexity）中强调**近可分解性（Near-Decomposability）**结构的重要性：系统各部分的大量行为可以被理解和管理，而不必让其中每个动作都取决于整个系统的每个动作。[S15](#)

这不是要在一个国家里建设五个彼此隔绝的数字国家。主张要精确得多：服务界面和标准可以统一，而某些故障路径与持续运行能力可以经过设计后相互分离。共享知识是一项优势；共享唯一故障点，则是另一项工程决策。



Illustrative dependency classes; NOT a map of Saudi infrastructure

相互依赖类别的概念示意图，不展示任何真实运行网络

图 1——技术与服务依赖类别的概念图。箭头为假设，仅用于说明；此图不代表沙特阿拉伯（Saudi Arabia）或海湾地区（Gulf region）任何真实设施网络或弱点。

6. 一个不知道沙特在哪里的小实验室

为了不让悖论悬在空中，我们执行了一项可复现的合成模拟。设想五类抽象服务，在一个 48 小时的假设窗口中保持恒定需求。模型包含三种架构：一条共享计算路径；假定相互独立的两条路径；以及在此基础上增加一种备用模式，在中断期间能够以假定有效且安全的方式执行一小部分功能。

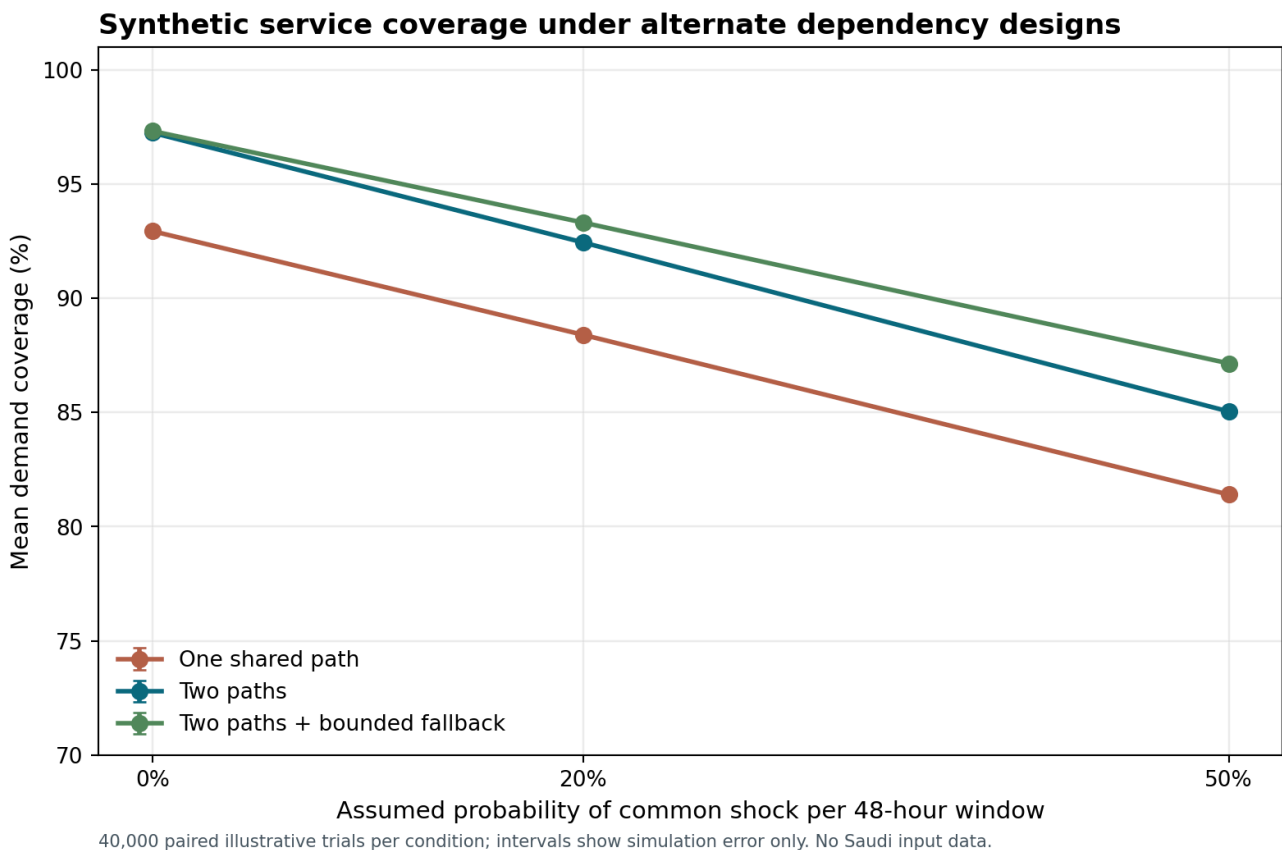
我们对每组假设执行了 40,000 次计算实验，使用有记录的随机生成方式；比较同一组中的不同架构时，对冲击采用相同处理。独立组件事件的概率、共同冲击的概率、故障时长、服务权重、备用能力比例，全部是为了检验数学逻辑而设定的数字。它们并非从沙特服务、攻击记录或客户数据中推导而来。我们还假定，两条独立路径需承担少量运行成本，因此其常态标称能力降至 98.5%。这同样是可以修改的假设。

模型让我们检验“备用”一词经常掩盖的问题：备用路径会不会与主路径同时失效？如果备用路径独立失效，它就能在第一条路径中断时承载需求。如果两条路径共享同一个事件和同一段中断时间，把它们称为“两条路径”并不会产生两个彼此独立的存续原因。

假设的 48 小时内共同冲击概 率	两条路径是否共享故障事 件	一条共享路 径	两条路 径	两条路径+有限持续运 行
0%	在模型中相互独立	92.93%	97.24%	97.31%
20%	在模型中相互独立	88.40%	92.44%	93.31%
20%	共享假设的故障事件	88.37%	87.04%	88.81%
50%	在模型中相互独立	81.40%	85.04%	87.14%

表 2——实际运行模型得到的 48 小时内合成需求平均完成比例。“共享故障事件”不是根据真实运行估计出的相关系数，而是本实验的设计假设。同一情景不同重复结果之间的小数点后差异包含模拟误差，不是对某个国家绩效差异的估计。

在第二行中，相较单路径，备用路径使覆盖率增加约 4.04 个百分点；加入有限持续运行后，结果进一步增至 93.31%。第三行假设两条路径共享同一故障事件，此时仅有两条路径的平均结果反而低于单路径，因为我们保留了假设的运行能力成本，却失去了独立性的收益。部分持续运行挽回了一些收益，但没有解决全部问题。



合成计算实验显示共同冲击对平均需求覆盖率的影响

图 2——三种架构的合成实验，假定备用路径的个别故障相互独立，并比较三种共同冲击概率。小误差条表示由实验次数产生的蒙特卡洛误差 (Monte Carlo)，并非沙特绩效的不确定区间。代码与详细数据见科学附件。

一个不含沙特阿拉伯数据的实验有何科学价值？它展示的是结果改变的条件。我们看到，仅仅改变故障是否共享这一假设，选项排序就会翻转，技术名称和服务器数量都无须改变。但实验并未证明这些概率符合现实，也没有证明五类服务与实际服务分布相似，更没有证明降级模式对任何特定服务都合法或安全。模拟也没有计算工作积压、记录损失、财务成本或供应商延误。这些是后续研究问题，不是可以藏进脚注的细节。

7. 同一个“恢复”的四种含义

技术事故过后，常会听到“系统已经恢复”这样的安抚话语。但这句话可能把时间和含义各不相同的四个阶段压缩在一起：

1. 组件可用性（Component Availability）：服务器、连接或软件恢复工作。
2. 功能连续性（Functional Continuity）：可以按可接受的质量与安全标准处理真实请求。
3. 积压清理（Backlog Clearance）：中断期间被延误的请求或审核已经完成。
4. 可恢复性（Recoverability）：数据、备用能力、支持团队和供应商已经准备好应对下一次故障。

此前事件中，这些含义彼此分离。一家医疗机构称软件已经恢复，但工作仍需时间清理积压。[S09](#) 亚马逊（Amazon）称客户已迁移到其他区域，但一些仅存于受损位置的资源仍无法访问。[S06S07](#) 对用户而言，能够打开页面与业务已经办结并不相同；今天办结与其权利所依赖的记录明天还能恢复，也不相同。

我们可以用一个拟议研究指标表达这个问题，即有效需求覆盖率（Valid Demand Coverage）：

$$C_{j,s,T} = \frac{\int_0^T \min(Q_{j,s}^{\text{valid}}(t), D_{j,s}^*(t)) dt}{\int_0^T D_{j,s}^*(t) dt}, \quad R_{s,T} = \sum_j w_j C_{j,s,T}.$$

分子表示在质量、安全和时效要求下实际提供的服务量，上限为有合理依据的参考需求；分母表示该期间参考需求总量。权重 w_j 是公开说明的价值判断，必须接受敏感性检验。所有量须非负，每项纳入计算的服务还必须有大於零的分母。这个指标仍是有待效度检验的提案，不是政府指标，也不是国家韧性数值。

在分别理解各项功能之前，我们不必把电力、支付和信息查询压缩成一个数字。读者应看到一张按功能分列的仪表板：完成了什么、未完成什么、最严重的性能下降期、恢复到可接受阈值所需时间、工作积压，以及维持持续运行的成本。单一全国平均值可能掩盖某个地区或依赖关键服务群体遭遇的严重延误。

测量最危险的自我欺骗之一，是危机期间记录到的需求下降。人们若无法进入门户，系统看到的请求数可能变少，甚至会使“仅对已经进入系统的请求”计算的完成率上升。因此，分母需要对本应获得服务的需求作出有理有据的估计，并检验结果对这一假设的敏感程度。不能因为屏幕上的队列消失，就认定队列已经处理完毕。

8. 悖论的经济学：那条我们希望永远用不上的路径，成本是多少？

清晰的预算喜欢看见年度节省：统一中心减少设备重复，大额采购合同带来规模优势，一个专业团队，统一维护。这在经济上可能确实成立。但要决定系统能否在复合冲击下持续运行，就必须比较全生命周期成本（Lifecycle Cost），包括恢复演练、部分资源冗余、更新负担、数据迁移、场所与监管要求、可接受延误，以及在常态下没有回报、却能在危机中购买选择权的投资。

对于使用频繁、容许延误很短的服务，最佳替代方案可能是定期测试的小型备用能力。对于不紧急的服务，排程、延期并向用户如实说明，可能比复制整个基础设施更合适。某些数据还受驻留或保护要求约

束，复制到另一国家需要事先进行法律和运行设计。如果第二台服务器依赖同一软件身份、同一访问密钥，或危机中无法联系的同一供应商，购买它并不能带来独立性。

因此，投资问题不只是“我们有多少个数据中心”，还包括：增加的能力服务于什么功能？能否缩短恢复时间差距？当身份、电力或通信服务中断时，副本是否仍可用、可核验？实现这种独立性需要多少成本？

宣布计划与证明经济选择合理之间差距很大。我们可以宣布建设价值数十亿的基础设施，或列出庞大的处理器数量。这些是资本或设备规模；有用的服务则取决于实际使用的能力、愿意付费或确实需要它的需求，以及成本上升或环境变化时仍能维持的性能。系列将在第十二篇文章“GPU 资本陷阱（GPU Capital Trap）”中更深入地讨论这个问题。

9. 如何诚实地检验沙特问题？

如果今天有一组公开指标显示，接入广泛、体验先进、技术支出不断增长，科学上的下一步应是要求提供经过授权、以聚合形式呈现的服务连续性测量，说明共同依赖的影响，同时不泄露具体设施的敏感地图。

检验首先要把在时效重要性和受益人权利方面相近的服务分组。选取获准研究的机构样本，定义应持续的功能；设计防御性故障情景；测量正确完成的比例、性能下降时间、恢复与积压。随后比较一体化程度不同的系统，并控制可能影响结果的差异：预算、机构能力、服务复杂度、需求性质、供应商类型，以及此前恢复演练的结果。

集中平台建设与服务改善同时发生，并不足以证明集中化是原因。管理可能更好，维护可能更完整，资金也可能更多。邻国的一个云中心遭到攻击，也不足以判定沙特系统会承受同样结果。估计因果效应（Causal Effect），需要定义比较对象和可能混淆比较的差异来源；如果事实和数据允许，还可能需要经过设计的恢复实验或准实验设计。

检验可以形成四条实践研究路径：

研究路径	测量问题	有用证据	需要警惕的做法
功能连续性	性能下降期间，有多少必要需求得到安全服务？	经授权演练的聚合机构记录	只看“服务器在线”，或漏掉未能进入系统的需求。
共同依赖	一次事件会影响多大比例的功能？	对供应商和依赖类别进行分级、匿名描述	发布敏感的场所或运行连接。
替代路径	主路径失效时，哪些功能仍然有效？	切换与恢复测试，包括失败的测试结果	只计算备用副本数量，却不试用。
持续运行经济学	替代能力是否值得其成本？	总成本、需求情景和明确的延误损失	把公布的支出等同于实际交付的服务。

比较结果可能与预期不同：凭借管理、测量和多供应商能力，机构一体化或许是持续性更好的原因；也可能发现某类服务的所有路径最终汇聚到一个必须修复的依赖点。好的研究应允许两种可能都显现出来，让决策服从结果。

10. 到 2035 年，我们应该观察什么？

本文没有为未来十年数字国家的命运计算数值概率。不过，我们可以勾勒会改变当下决策的条件性路径：

路径一——一体化增强持续性。共享管理让监测、处置和有序切换到备用方案成为可能，多项服务因此改善。关键迹象是，有记录的测试显示功能恢复时间和工作积压下降，同时成本仍可接受。

路径二——漂亮的节省，棘手的依赖。日常服务变快，但合同、数据或协调工具集中在会受同一冲击影响的路径上。关键迹象不是袭击本身，而是公布的备用方案在需要时无法工作，或切换到另一供应商的成本上升。

路径三——逐步转向可输出的韧性。恢复管理、测试、依赖分析和低连接条件下的安全运行形成产品，并凭真实表现赢得客户再次购买。关键迹象是可重复的产品收入，以及不同客户处有记录的结果，而不是演示文稿的数量。

2026 年 10 月，路透社（Reuters）报道了伊朗官员关于如果战事重启，可能针对海底电缆的计划和威胁。这里的新闻内容是所称计划与威胁，不是针对这些电缆的新袭击已经实施。报道还提到流量可以改道，并指出与潜在的区域影响相比，全球影响可能有限。[S16](#) 这正是情景分析的价值：我们可以从理论上测试替代方案并为之准备，却不声称知道未来会发生什么。

11. 袭击之后，问题发生了什么变化？

海湾云基础设施（Cloud Infrastructure）遭到打击的故事，并不随着受损的钢铁或不可用的节点结束。有些客户成功迁移了业务；有些数据由于只留存在特定位置，至今无法访问；某些设计边界也被证明窄于这类冲击。[S06S07](#) 最值得注意的是，命运之间的巨大差异来自应用用户看不见的因素：副本在哪里、它是否真正独立、备用方案如何启动，以及何时作出切换决定。

数字国家可以同时向两个有益方向发展：让日常生活更容易，也建立在生活变得困难时继续提供服务的能力。后者需要单独测量。用户在平静早晨拥有一个快速门户还不够；系统还应知道，当某个条件缺失时自己可以做什么，何时应为保证决策安全而停止，如何向用户解释发生了什么，以及应把哪些信息保存在何处，才能在之后完成用户应有的权利。

在这个意义上，系列开篇的问题可以说得更准确：如果五项优秀服务建立在同一个基础上，我们拥有的是五项能够持续的服务，还是建在一个从未测试过其缺席情形的基础上的五扇漂亮窗口？

答案不来自袭击标题、支出规模，也不来自我们的合成模型。答案来自检验：还有多少服务，是否有效，恢复多快，以及以什么代价才能持续。当这些问题进入数字繁荣的核心时，我们并非缩小其成就，而是在辨认其中哪一部分能够穿过一个不按常态条件设计的日子。

阅读与证据说明

- 主要事件：2026 年 3 月，一家区域云服务公司的基础设施遭到物理损坏；同年 9 月，出现带有限定条件的恢复结论。证据包括公司声明与路透社（Reuters）的原始报道。[S05S06S07](#)
- 国家层面的边界：在已审阅来源中，我们没有找到足够的公开数据，用于测量这些打击对沙特特定政府职能持续性的影响。仅凭这起事件，不能推断沙特薄弱或强韧。
- 科学比较：两篇网络研究 [S11S12](#) 采用不同假设下的模型，均不能替代对本地依赖关系和数据的核验。
- 计算实验：表格与图 2 中的数字为合成数据，由随附代码实际生成。不得把它们并入真实统计序列，也不得解释为事故预测。
- 研究附件：research_companion_zh-CN.md 提供方法、假设、结果、文献解读，以及使用经授权信息开展检验的建议方案。

主要来源

- [S01](#) 通信、空间与技术委员会（Communications, Space and Technology Commission），Saudi Internet 2025，2026 年发布的 2025 年数据。<https://www.cst.gov.sa/en/knowledge-center/reports/saudi-internet-25>
- [S02](#) 数字政府管理局（Digital Government Authority），Digital Experience Maturity Index for 2025，2025 年结果，评估 50 个平台。<https://dga.gov.sa/en/news/rise-in-the-digital-experience-maturity-index-2025>
- [S03](#) 国家网络安全管理局（National Cybersecurity Authority），2026 年 10 月 14 日关于 2025 年行业指标的声明。<https://nca.gov.sa/en/news/report-on-key-economic-indicators-in-the-cybersecurity-sector-in-the-kingdom-2026/>
- [S05](#) 路透社（Reuters），2026 年 3 月 2—3 日，公司有关云基础设施物理损坏的声明。<https://www.reuters.com/world/middle-east/amazon-cloud-unit-flags-issues-bahrain-uae-data-centers-amid-iran-strikes-2026-03-02/>
- [S06](#) 亚马逊（Amazon），关于继续协助客户从巴林区域迁移的声明。<https://www.aboutamazon.com/news/aws-bahrain-region-middle-east-conflict>
- [S07](#) 路透社（Reuters），2026 年 9 月 15 日，公司更新说明仅存于受损位置的资源无法恢复。<https://www.reuters.com/world/middle-east/amazons-aws-is-unable-restore-access-bahrain-one-uae-cloud-data-zone-after-war-2026-09-15/>
- [S08](#) CrowdStrike，2024 年 7 月 19 日关于错误更新的声明。<https://www.crowdstrike.com/en-us/blog/to-our-customers-and-partners/>
- [S09](#) 英国国家医疗服务体系 Shropshire, Telford and Wrekin，2024 年 7 月 22 日关于系统恢复后工作积压的更新。<https://www.shropshiretelfordandwrekin.nhs.uk/news/update-on-it-outage-emis-up-and-running-but-some-delays-expected/>
- [S10](#) 澳大利亚通信与媒体管理局（Australian Communications and Media Authority; ACMA），2024 年 11 月关于 Optus 中断的审查结果。<https://www.acma.gov.au/articles/2024-11/optus-pays-12->

[million-penalty-triple-zero-outage](#)

- [S11](#) Buldyrev 等, *Catastrophic Cascade of Failures in Interdependent Networks*, 《Nature》, 2010。DOI: 10.1038/nature08932。 <https://www.nature.com/articles/nature08932>
- [S12](#) Radicchi 与 Bianconi, *Redundant Interdependencies Boost the Robustness of Multiplex Networks*, 《Physical Review X》, 2017。DOI: 10.1103/PhysRevX.7.011013。 <https://journals.aps.org/prx/abstract/10.1103/PhysRevX.7.011013>
- [S13](#) 美国国家标准与技术研究院 (National Institute of Standards and Technology; NIST), *Developing Cyber-Resilient Systems*, SP 800-160 Vol. 2 Rev. 1, 2021 年 12 月。 <https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final>
- [S14](#) Charles Perrow, *Normal Accidents: Living with High-Risk Technologies*, 更新版, Princeton University Press, 1999。 <https://www.jstor.org/stable/j.ctt7srgf>
- [S15](#) Herbert A. Simon, *The Architecture of Complexity*, *Proceedings of the American Philosophical Society*, 1962, 106: 467 – 482; Santa Fe Institute Press 的学术导读: <https://www.sfi.press.org/21-simon-1962>
- [S16](#) 路透社 (Reuters), 2026 年 10 月 23 日, 有关海底通信电缆风险的条件性声明。 <https://www.reuters.com/world/middle-east/iran-has-detailed-plans-hit-gulf-undersea-cables-if-war-resumes-officials-say-2026-10-23/>