全球政府在主权方面的转变

公共部门组织需要执行新的生存战略

对于美国以外的公共部门组织而言，数字主权已从法规检查清单演变为生存战略。各政府逐渐意识到，仅实现主权或遵守司法管辖区法律，不足以应对如今的挑战。新的数字主权目标被称为战略自主性：即使在外部支持撤回或全球供应链中断的情况下，仍能独立运维、创新并维护关键服务。

联合国贸易和发展会议（UNCTAD）近期的一份报告指出，“在已立法保护隐私和数据的国家/地区中，79% 的国家/地区对数字主权问题表示担忧[1]。”政府已无法继续忽视封闭式专有系统固有的依赖性。向战略自主性转型受到三大因素影响：

- **地缘政治风险：**在和平时期，对全球超大规模云服务商的依赖尚且可控，但在冲突情境下，对外部支持的依赖会成为致命弱点。物理破坏或互联网中断会使依赖云端的运维陷入瘫痪。当国际合作无法实现或不可靠时，各国必须具备独立行动能力。这种行动要求建立能够在拒止、中断、间歇及受限（DDIL）环境中运维的系统，确保任务关键功能（从国防指挥控制系统到紧急公民服务）保持正常运行，即使国家/地区与全球互联网断开连接，也不会受到影响。

- **网络弹性：**国家资助的网络攻击正变得日益复杂、频繁且影响广泛。主权保障了能源电网、医疗卫生系统和国防系统网络等关键基础架构能够抵御外部干扰，在供应链遭到破坏时也能保持运行。相关风险不仅包括数据失窃，还涉及在软件更新传输过程中插入恶意代码。政府需要主权保障：即能够独立验证其软件供应链的完整性以防止外国间谍活动，并确保系统未被入侵。

- **经济竞争力：**各政府日益将数字主权视为国家安全的基石。通过实现 AI 开发和数据治理的本土化，未来经济增长的引擎能够保留在国内管辖范围内，而非受外部监管。人们越来越担忧，依赖国外的“黑匣子”AI 模型会导致知识产权流失，文化相关性削弱。战略自主性使各国能够构建这些数字能力，培育本土创新生态系统，并确保数字化转型所创造的经济价值留存于国民经济中。

红帽官方微博　红帽官方微信

1　“全球范围内的数据保护和隐私立法”，联合国贸易和发展会议，2026 年 2 月 17 日。

全球需求与区域差异

虽然数据管控需求是全球性的，但各个公共部门面临的具体影响和障碍存在显著地域差异。

欧洲、中东和非洲地区（EMEA）及加拿大

欧洲、中东和非洲地区的主要矛盾在于，既需要先进技术，又依赖于非欧盟（EU）提供商。这使政府面临司法管辖风险，特别是域外法律方面的风险，如美国颁布的《澄清境外数据合法使用法案》（CLOUD）或《1978 年外国情报监视法案》（FISA）等法律。

欧洲机构面临一套复杂且严苛的法规体系，既要遵循欧盟关于网络安全的《网络和信息安全指令》第二版（NIS2），以及关于运维弹性的《数字运维弹性法案》（DORA），也要满足法国 SecNumCloud 等国家层面的强制要求。国防基础架构仍呈碎片化状态，北大西洋公约组织（NATO）内部的互操作性差距阻碍了数据交换效率。此外，各国还面临通过安全审查的员工严重短缺的问题，难以运维主权环境。虽然加拿大在地理上位于北美洲，但与欧洲、中东和非洲地区一样，面临着基础架构过时的挑战。加拿大国防部受困于统一机密网络基础架构（CSNI）的碎片化拼凑问题，官僚主义障碍也拖慢了现代化功能的采用进程。这种风险程度导致政府机构选择隔离敏感数据，以免受外国法律干预，并通过培育自主能力来弥合软件缺口。

亚太地区（APAC）

亚太地区的特征体现为严格的贸易保护主义政策和较高的合规风险，旨在实现技术上的自力更生。

- **数据本地化：**中国、印度和印度尼西亚等国家/地区实施严格的数据本地化政策，要求关键数据完全驻留在国境内，这限制了全球公共云的使用。
- **高度问责制：**新加坡实施严格的端到端安全标准，公职人员可能因数据滥用或保管不当面临刑事处罚，由此形成了规避风险的采购文化。
- **全球本土化需求：**亚太地区强烈倾向于采用全球与本土优势相结合的“全球本土化”（glocal）模式，即通过本土企业交付全球技术，以确保掌控主权。

亚太国家/地区致力于发展本土能力，以减少对外国势力的长期依赖，将数字主权视为抵御地缘政治脆弱性的盾牌。

拉丁美洲地区（LATAM）

拉丁美洲地区的现代化进程受运维连续性影响，并且常因为结构性不稳定而受阻，而非受制于政策。

- **不稳定性和不连续性：**在地缘政治气候不确定的背景下，政治领导层的频繁更迭与经济波动会危及长期 IT 规划和多年期采购合同的执行。

- **聚焦内部安全防护：**拉丁美洲地区的国防机构优先考虑内部安全防护（边境保护、禁毒），倾向于采用敏捷的监控工具，而非重型战略基础架构[2]。
- **采购风险：**公共采购中的低效和腐败风险降低了技术预算的有效价值，促使各国寻求经济高效、开放灵活的系统。这类系统既能承受预算削减和政治变动带来的影响，又可避免国家受限于昂贵、僵化的专有供应商。

红帽的数字主权之道

为了取得成功，全球公共部门机构必须在上述这些不同的层面上解决主权问题。红帽提供了相应的工具和生态系统，帮助机构充分理解各个层面。

数据主权和 AI

红帽充分理解在关键数据和 AI 模型方面实现完全控制与自主权的标准，能够确保数据驻留在国境内，且治理方式符合当地法律。政府机构必须实施主权 AI 战略，保留其模型和训练数据的所有权，并将它们部署到本地化基础架构上，而非依赖应用编程接口（API）访问外国控制的模型。红帽® OpenShift® AI 支持在数据驻留位置部署主权 AI 功能。我们采用机密计算技术保护使用中的数据，实现对数据位置和访问权限的精准管控，确保遵守《欧盟 AI 法案》等法规要求。

技术主权

若要实现长期独立性，并确保不受限制地迁移应用，必须能够在不依赖特定提供商基础架构或专有软件的情况下运行工作负载。政府应采用开放标准和可移植的容器平台，规避供应商锁定风险。这样一来，当云提供商政策发生变化或地缘政治紧张局势升级时，工作负载无需重构即可迁移至其他基础架构。红帽通过开源标准降低供应商锁定风险。我们的平台支持多种硬件架构（x86、高级精简指令集机器（ARM）、RISC-V），因此国家系统能够按照自身规划实现演进与更新，摆脱外部依赖的束缚。

运维主权

政府机构需要对其关键 IT 运维保持完全的行政管理权和独立性，以便在断联状态下也能保持运行。国防和关键基础架构必须优先保障运维弹性。此类基础架构应能够自动执行应对战时条件的灾难恢复计划，并确保其支持和运维由通过安全审查的本地公民负责管理。例如，红帽提供经确认的主权支持，即由通过审核的本地公民（如欧盟境内公民）提供技术支持，确保支持人员可访问的数据始终不离开司法管辖区。此外，红帽 Ansible® 自动化平台可实现弹性自动化，即使在非联网（DDIL）环境中也能快速完成恢复和修补。

2 “五角大楼新战略聚焦于本土和西半球”，DefenseNews，2025 年 9 月 25 日。

保障主权

独立验证数字系统和流程的完整性、安全性和可靠性，有助于机构保持合规。政府机构必须摒弃盲目信任，建立可验证信任机制。这种转变需要对软件供应链进行严格审计，并能够证明其符合通用标准、联邦信息处理标准（FIPS）和 NIS2 等标准。红帽提供值得信赖的软件供应链，这些软件经过加密签名，具有可验证的来源和软件物料清单（SBOM），使机构能够审计每个组件，确保未注入恶意代码。这些安全措施有助于确保各机构满足《欧盟网络弹性法案》等新颁法规的要求。

通过开源实现战略自主性

红帽采用灵活开放的基础来应对挑战，赋予政府机构更多的选择与控制权，而非僵化的隔离方案。这种灵活的方法基于一个认知：单一提供商难以全面解决数字主权问题。红帽提供跨各种基础架构提供商和云区域构建主权云的选择，避免了单一解决方案的局限性。

30 多年来，红帽始终致力于提供值得信赖的企业开源解决方案，帮助企业组织满足最严格的安全与合规要求。企业开源不仅仅是一项技术，更是政府机构实现真正数字主权与战略自主性的关键架构基础。与依赖封闭、不透明系统并要求盲目信任的专有供应商不同，红帽帮助机构保持对其数字命运的绝对掌控，而非受制于人。这种开放方法有助于全球公共部门掌控从战术网络边缘到主权 AI 的全球创新节奏，同时确保工作负载保持可移植性和弹性。开源方法还能保障任务关键型运维免受供应商锁定和技术过时风险的影响。通过采用开源技术，红帽与欧盟等地区普遍奉行的“默认开放”原则相契合。此类模式既可防止对单个供应商产生依赖，又允许检查和修改代码，已成为保障国家安全与建立信任的必要条件。

- **透明度和信任**

  红帽的开源模式提供 100% 的透明度，允许政府机构检查源代码、验证安全性并审计软件供应链。这种可审计性对于满足欧洲、中东和非洲地区以及亚太地区的保障要求至关重要。此外，红帽提供来源可验证的加密签名软件，符合《欧盟网络弹性法案》等新颁法规的要求。

- **运维主权和本地支持**

  为应对司法管辖风险，红帽支持自主控制基础架构的运维人员，以实现运维主权。

  - **主权支持：**如前文所述，红帽在欧盟提供经确认的主权支持，确保技术支持完全由位于欧盟境内且通过审核的欧盟公民提供。这种技术支持有助于确保支持人员可访问的数据始终不离开所在地区。

  - **本地生态系统：**红帽与经认证的本地云提供商合作构建生态系统，提供符合严格的国家/地区数据驻留法律的主权云功能。

- **技术独立性**

  开放混合云战略支持工作负载在多种环境中运行，如本地、私有云、战术网络边缘或隔离环境。

- **可移植性：**这是防止供应商锁定的基础，而供应商锁定是政府机构（尤其是在拉丁美洲和亚太等地区）最担忧的问题之一。这些地区能否高效迁移工作负载和数据，是确保服务连续性以及高效应对地缘政治变局的关键（例如，政治或经济变化可能导致需要更换技术提供商）。
- **非联网运维：**对于国防机构而言，红帽设备边缘和红帽 OpenShift 等红帽解决方案支持系统在非联网 DDIL 环境中自主运行，即使在无法访问中央云的情况下，也能确保任务的持续执行。

红帽为政府机构提供开放的基础架构，助力打造能够应对不确定性、提供可靠数据安全防护并保障国家持续运转的主权云。

- **主权 AI**

  随着各政府探索并拓展 AI 应用，红帽提供了用于构建主权 AI 的平台。这有助于确保国家/地区保留对其模型和训练数据的所有权，将它们部署到本地化基础架构上，以遵守《欧盟 AI 法案》等法规，而非依赖 API 访问外国控制的模型。

公共部门为何选择红帽？

红帽一直是公共部门值得信赖的合作伙伴，我们的产品部署于美国 100% 的行政部门[3]，并广泛应用于北约组织和全球国防部。红帽的许可模式以及对开放标准的承诺，可确保政府机构不会与特定供应商永久绑定。各组织保留无限期使用和维护软件的权利，从而保护长期投资，免受供应商路线图变更或地缘政治限制的影响。

随着支出的增加（尤其是在国防领域），对红帽解决方案和服务组合的投资可带来显著回报。北约成员国承诺将国防开支翻倍，到 2035 年达到国家 GDP 的 5%[4]。通过在统一平台上实现标准化，各机构不必再投资维护分散的传统系统，而是可以构建有助于完成任务的新能力，从而大幅降低运维成本和总体拥有成本。

开始体验的后续步骤

- 详细了解红帽在全球公共部门的应用，并联系红帽代表。
- 想要评估您的数字主权就绪度？阅读这篇博客文章，开始行动吧。

3　红帽客户数据，2025 年 9 月。

4　“国防开支和北约的 5% 承诺”，北约组织，2025 年 12 月 18 日。

关于红帽

Red Hat 是領先全球的企業開放原始碼軟體解決方案供應商，透過在社群上集思廣益，提供效能卓越且可靠的 Linux、混合雲、容器及 Kubernetes 技術。Red Hat 致力協助客戶開發雲端原生應用程式，整合既有與全新 IT 應用程式，自動處理並管理複雜的環境。Red Hat 是深受《財星》世界 500 強公司信賴的顧問，能提供獲獎肯定的支援、訓練及諮詢服務，為各項產業帶來開放創新的優勢。Red Hat 作為全球企業、合作夥伴與社群的聯繫中樞，致力協助組織成長與轉型，迎接數位時代的未來。

红帽官方微博

红帽官方微信

销售及技术支持

800 810 2100
400 890 2100

红帽北京办公地址

北京市朝阳区东大桥路 9 号侨福芳草地大厦 A 座 8 层　邮编: 100020
8610 6533 9300

cn.redhat.com
#3613114_0326

版权所有 © 2026 Red Hat, LLC。红帽、红帽 logo、Ansible 和 OpenShift 是红帽或其子公司在美国和其他国家/地区的商标或注册商标。