NSFOCUS

2024
网络安全趋势

关于绿盟科技

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 50 余个分支机构，为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和办事处，深入开展全球业务，打造全球网络安全行业的中国品牌。

NSFOCUS

CONTENTS

序

“善弈者谋势”。

加强对行业发展趋势的关注和研判，是了解行业动态、明确发展目标的重要途径。对于网络安全行业而言，其意义更加明显：洞察趋势并顺势而为，对于及时感知并防范风险、优化资源和发展策略等，具有十分重要的实践意义。

何以观势？如业界所熟知，“合规”和“攻防”是网络安全行业发展的两大基石。“合抱之木，生于毫末；九层之台，起于垒土”，网络安全趋势的发端与形成，从对合规和攻防实践的分析中可以见其端倪。

绿盟科技依托扎实的网络安全保障实践，立足重大需求深入理解国家政策导向，立足技术创新密切跟踪攻防异动，立足专业视角全方位多维度分析，总结提出了“2024年网络安全行业十大趋势”。特此凝练成册，以资参考。

“察势者明，趋势者智”。诚挚期待本报告能为网络安全行业管理和产业发展略尽绵薄。并期待依托我司技术、产品和服务创新，全力投身打造网络安全新质生产力，为实现国家高质量发展战略目标贡献力量。

叶晓虎

2024 年 3 月

01

趋势 1：生成式人工智能中的各类新型攻击兴起，围绕其特有的提示词内容的攻防将会不断深入，多模态攻击形式以及模型 AGENT 风险正在成为该领域未来的攻击趋势；隐私合规和数据泄露风险将成为其应用面临的重大安全挑战。

生成式人工智能（Generative Artificial Intelligence,GAI）技术的蓬勃发展，特别是以大模型为代表的关键技术突破，促进了新一轮人工智能产业革命。2023 年 Gartner 安全运营炒作曲线 (Hype Cycle for Security Operations,2023) 首次将生成式网络安全人工智能 (Generative Cybersecurity AI）纳入创新启动区。以 ChatGPT 为代表的人工智能和大模型应用正在逐渐深入到各行各业的关键场景，然而，当前的 AI 大模型发展得尚不成熟，同时随着其能力的提升和应用的扩展，潜在的安全漏洞和隐患会引发更大范围和更为严重的后果。

面向人工智能的攻防始终是学术界的热点，针对 AI 大模型的攻击技术也在不断提高且变得更加复杂，例如模型逆向工程、数据投毒攻击、模型窃取等，这些都对大模型的可用性和机密性构成了严重威胁。大模型自出现以来就面临着诸多特有的风险，如提示词注入、角色扮演、反向诱导等新攻击手法。当前，针对大模型安全威胁的检测和防御措施在面对攻击者不断变化的攻击手段时显得力不从心，2023 年已经涌现出经典的 DAN(Do Anything Now) 攻击（即通过精心设计的提示词诱导大模型执行任何操作，包括一些潜在的危险行为）、奶奶漏洞（即通过角色扮演等手段诱导 AI 系统产生意料之外的回复）等针对自然语言特性的各类提示词（Prompt）攻击，以及结合跨站脚本攻击（XSS）等传统攻击技术进行的 Prompt 攻击，仅靠大模型厂商自建的安全围栏还不足以应对。因此，需要对大模型在 Prompt 内容安全方面进行风险评估，并据此在用户输入侧、模型输出侧进行防御检测。同时，通过优化增强业务模型侧的 Prompt 内容以及文本结构，针对逃逸攻击、角色假定、Prompt 泄露等攻击手段展开防御检测，从而有效提升针对模型的攻击成本。

多模态能力在给大模型业务应用带来各种业务机会的同时，也为其带来了更加多样化的攻击形态以及安全风险。在多模态交互形式（如文本、图像、声音、视频等）成为业务常态形式的情况下，攻击载荷也具备了更多形态以及复杂组合的突破方式，给企业的防御体系带来了新的挑战。作为模型获取外部能力的关键技术，Agent 机制在为模型提供图数据库操作、文件交互以及命令执行等各类能力的同时，也可能被攻击者利用多模态的形式来操纵模型行为，间接控制模型 Agent，造成更加广泛的攻击危害。相比在单一模态数据上训练的模型，多模态模型的安全性更为复杂，因此多模态内容安全也是相当有价值的研究方向。

在用户采用大模型的过程中，满足隐私合规和避免自身敏感或隐私数据泄露成为重大安全挑战。目前，多数国家都颁布了隐私合规的法律法规，例如，要求数据相关方采取一系列措施来保护用户的隐私和敏感信息，其中包括美国的《格雷姆 - 里奇 - 比利雷法》（GLBA）和《加州消费者隐私法案》（CCPA）、欧盟的《通用数据保护条例》（GDPR）、英国的《数据保护法案》（DPA）等。然而与此同时，大模型引发的个人隐私和敏感数据的泄露事件初现，

如三星被曝芯片机密代码遭 ChatGPT 泄露，引入不到 20 天就发生 3 起事故，内部考虑重新禁用。

因此，未来大模型应用将更加注重合规性，同时内置的隐私保护功能也会得到进一步的强化，这些保护措施包括但不限于数据加密、数据脱敏、权限控制、匿名化以及用户数据的精细访问控制机制。我国在 2023 年 8 月 15 日开始施行《生成式人工智能服务管理暂行办法》，旨在规范生成式人工智能服务提供者在处理敏感信息时的行为，保障用户的隐私和个人信息安全，促进生成式人工智能服务的健康发展。因而，AI 服务商可通过提升安全性来获得竞争优势，安全厂商也可推出相关安全产品以满足出现的人工智能安全需求，最终减小大模型及其数据成为攻击目标的风险，保障安全大模型系统的稳定性和可靠性。

02

趋势 2: 生成式人工智能将重塑安全运营技术与流程，大模型可承担“安全副驾”角色，提供分析、推理和报告等运营能力，同时，大模型技术也被广泛用于漏洞挖掘、恶意软件分析、内容检测、自动化渗透等多种攻防场景。

2023 年安全运营的智能化技术军备已进入白热化，其中 Microsoft Security Copilot 技术平台的预告发布，无疑拉开了网络空间安全大模型技术竞争的序幕，Google Sec-PaLM、SentinelOne Purple AI 等国内外厂商安全大模型紧随而来，给智能安全运营技术提供了全新的交互范式、任务分析范式，并从分析维度、整合维度、协同维度，为经典网络空间人工智能技术栈的升级提供了重大机遇。

全面观察以 Microsoft Security Copilot 为代表的大模型驱动安全运营的技术体系，我们看到基于大模型技术的生成式人工智能在安全运营领域展现出了多项显著的技术优势，包括：

1）安全知识语义增强。随着参数规模的指数级提升，大模型储备了领域知识 + 领域常识，极大缓解了困扰网络空间人工智能发展的一个核心难题——数据模式与安全语义的鸿沟问题。这是传统小模型（LLM 之外的经典机器学习、深度学习、知识图谱等技术）所难以解决的。

2）攻防领域分析逻辑增强。小模型技术主要擅长统计分析问题，大部分能力在于拟合学习。然而，网络空间安全的任务多元性、环境开放性，导致经典的拟合学习能力受限且极易衰减。基于大规模参数基础及指令学习等核心框架，大模型已具备逻辑分析基础，为少样本、零样本的学习场景提供了支持，能够从海量数据中高效提取关键信息，形成深刻洞察，迅速筛选出对安全运营至关重要的数据。

3）人机交互决策增强。网络空间对抗的主体终归在人。大模型技术大幅推动了语言模型的交互水平。安全团队通过基于自然语言的安全指挥平台界面交互，大幅降低成本、提升体验。对于安全运营中面向数据、工具、文档等目标复杂的分析场景来说，这是重大的技术革命。具体来说，大模型能够在日常告警分诊、攻击溯源调查、恶意软件分析、报告生成等多个方面，极大减少对高级安全分析专家的依赖，大幅提升高级威胁发现的精度与自动化水平。

当然，大模型只是智能安全运营技术体系中的核心能力之一，典型安全分析能力，如统一消歧的数据图谱、完整完备的工具支撑体系、专用专精的“小模型”库以及支撑协同调度的统一执行框架等，仍然是发挥大模型安全价值的关键基础。因此，结合已有安全分析能力，形成智能辅助决策支撑核心能力，将是未来大模型驱动的“安全副驾”典型范式。

在考虑生成式人工智能技术为网络安全运营提供了新的辅助决策支持和分析能力的同时，我们也看到了其在漏洞挖掘、恶意软件分析、内容检测和自动化渗透等关键安全领域的巨大潜能，以及被攻击者所利用产生的风险。

漏洞挖掘是网络安全中不可或缺的一环，传统上依赖于安全研究人员的专业知识和经验。然而，生成式人工智能技术被用于自动化漏洞挖掘可以提高发现软件漏洞的效率。但也意味着攻击者可以利用这些工具快速识别并利用新的漏洞，对网络安全构成了新的挑战。

恶意软件分析通常需要大量的人力资源来识别、分析。生成式人工智能使得自动化恶意软件分析成为可能，提高了防御效率。然而，恶意攻击者也在用生成式人工智能创建新型恶意软件，以便绕过现有的检测机制，使得恶意软件的识别和防御更加困难。

自动化渗透测试是评估网络安全防御能力的重要工具。利用 AI 进行自动化渗透测试可以模拟攻击者的行为，帮助识别脆弱性。然而，恶意 AI 工具也能执行自动化攻击，以更低成本、更有效率地发现并利用系统弱点，对企业和组织构成更大威胁。

内容检测是识别和阻止恶意内容传播的关键技术。AI 技术的进步有助于提高内容检测的准确性和速度。然而，恶意 AI 工具的能力，比如生成逼真的假新闻或钓鱼邮件，Deepfake 可生成虚假视频，对内容检测系统提出了新的挑战，这些系统需要不断进化以识别和对抗由 AI 生成的复杂内容。

综上，面对生成式人工智能在网络安全领域的双面性，我们既要积极拥抱其带来的机遇，提升网络安全运营的智能化水平，也必须警惕并积极应对恶意 AI 工具可能带来的风险和挑战，通过全面的策略和措施，确保网络空间的安全和稳定。在法规层面，加强对 AI 技术应用的法律监管，确保其发展和使用不会伤害社会公共利益；在教育层面，提高公众对 AI 技术潜在风险的认识，鼓励负责任的 AI 技术使用，特别是现阶段大力加强围绕 Deepfake 类威胁的安全意识教育；在技术层面，研发防御策略和技术，以便识别并抵御由恶意 AI 工具生成的攻击，提升现有身份认证机制的健壮性，使其具备抵御 Deepfake 的内生安全性。

03

趋势 3: 监管方式多元化以及攻击烈度持续攀升，风险管理的建设重心将从大而全的风险发现向 CTEM 的威胁与风险相结合的精确、可控、动态风险治理办法转变。

持续威胁暴露面管理（CTEM）预计会在 2024 年成为网络安全行业的热点，主要由于其对综合安全风险态势的了解和持续性评估的能力。

风险治理一直以来是网络安全领域永远的话题，每一个新的技术亮点或者评估方法发布都会引来业界的广泛关注，今天我们先从攻击的角度，分析一下漏洞爆发和利用的情况。

看漏洞利用：2023 年观测到的漏洞 CVE、CNVD 等漏洞编号的发布超过 30,000 个，但只有 500 多个高危漏洞被发现具备成熟利用的手段，也就是说仅 1.9% 的漏洞会直接快速地造成巨大风险，而安全治理者将面临的是 30,000 多个漏洞的跟踪、识别和修复工作。

看组织自身：随着组织风险发现能力的逐渐完善，企业将会深刻认知全面的资产管理和风险管理投入产出比非常不经济、跨部门执行力度难以把握最终导致风险治理难以推动，安全部门风险治理指标难以有效达成。而国内特色的攻防演练也让越来越多的企业意识到自建安全蓝军的重要性，蓝军在企业中全面、高效地识别关键攻击路径和关键风险，确实是纯人工或服务所不能单独解决的问题。所以企业蓝军未来势必会借助自动化的入侵和攻击模拟（BAS）以及渗透测试工具，让企业能够实际感受到有效风险带来的损失，从而有计划有方案地处理发现的网络安全风险。

看攻击态势：随着 APT 和勒索软件逐渐转向 SaaS 化交付，国际攻击态势愈发严峻。在之前提到的 500 多个漏洞中，已有 25% 当天即被武器化，而剩余的 75% 的武器化周期也短于三周，这也给安全团队风险的发现以及修复的时效提出了极大的挑战；

因此新的风险治理方案就必须面对如下问题：

1. 需要对漏洞的危害性、有效性、及时性等内容有足够认知；

2. 通过对漏洞属主的部署位置、业务属性和防御能力有足够了解，重新评估风险修复的优先级及解决方案；

3. 需要持续不间断的对整体 IT 资产进行风险监测，以确保问题能够被及时发现；

4. 需要对风险的认知进行广泛的扩充，包括但不限于口令、身份、新媒体、软件供应链以及数字资产等泛资产领域，进行风险管理；

CTEM 凭借内网攻击面以及供应链风险管理平台结合为基础，配套持续监测、防御识别和 VPT 技术，正在尝试去解决这四大风险治理新难题。

04

趋势 4: 在机读 IOC 威胁情报基础上，人读威胁情报及其平台和应用的需求会快速增加。

威胁情报经过多年的发展，可机器自动化消费的 IOC 情报发展已经进入到成熟区间。但是随着 2023 年 GPT 技术尤其是 AIGC 技术的爆发，对人读情报的需求有望快速发展。

相对于机读威胁情报（Machine Readable Threat Intellgience）, 人读威胁情报（Human-readable threat intelligence，简称 HRTI）在多个方面展现出其独特价值和优势。以下是对两者在定义、定位、价值、形式等多方面的对比：

对比项	机读威胁情报	人读威胁情报
定义	通过机器可读、结构化的格式呈现，且能够被计算机程序或自动化工具解析和应用的威胁情报数据。	经过整理、解释和归纳的安全领域的情报信息，以人类可读的形式呈现，以便人类能够理解和运用。
定位	侧重于提供快速、准确且可自动化的威胁分析和响应。	侧重于提供深入、全面的威胁分析和战略决策支持。
价值	提高威胁检测和响应的效率和准确性，减少人工分析的工作量。	提供深入的威胁洞察、技战术情报和战略建议，帮助组织制定针对性的安全策略。
形式	结构化数据，API、XML、JSON 等格式呈现，便于机器解析和处理。	以报告、摘要、图表或者简要说明等形式呈现，包括文本报告、聊天机器人呈现等方式，便于人类阅读和理解。
处理速度	快速处理大量数据，实现实时威胁检测和响应。	处理速度相对较慢，大模型有望改善生产慢、理解慢等难题。
准确度	依赖于自动化工具和算法的准确性，可能存在误报或漏报。	依赖于原始数据语料质量和人读情报转化的水平，通常具有较高的准确性。大模型技术成熟度也会成为重要影响因素。

在机读情报应用越来越成熟的基础上，随着大模型技术的快速发展，人读情报被更大范围应用的难题正逐步得到化解，HRTI 的应用场景和范围在迅速扩展。

（1）人读情报涉及数据范围逐渐展现出更高价值。传统威胁治理更多聚焦攻击者 IP、漏洞等情报数据，然而在 2023 年俄乌网络战和重要攻防演练中，可以人读的开源情报正扮演越来越重要的角色（明网、深网、暗网数据）。据绿盟威胁情报中心监测，仅 2023 年就有 5,609 起与中国有关的数据交易在黑市（黑客论坛和暗网网站）上售卖，总数超过 429 亿条。受害者覆盖快递、电商、运营商、教育、医疗、司法、公安、银行、政府等各类企业。招投标、供应链等明网情报、数据泄露暴露的深网情报、黑客组织交易的高价值暗网情报等均被大量用于网络攻防对抗中。

（2）人读情报生产成本高难题在被瓦解。2023 年大模型技术的快速发展，使得人读情报生产的诸多环节均被攻克，包括：数据智能分类、知识自动提取、文本数据理解、人读报告生成。更新的 AI 模型甚至可以对图像、视频等多媒体数据进行情报的提取和理解。有媒体报道，部分先进的情报单位（例如 CIA）已经开始利用 AI 技术对开源情报进行处理和提供服务，情报搜集渠道包括报纸、广播、电视、互联网等。

（3）人读情报应用产品呈现新形态。除了传统文档形态的人读报告，ChatGPT 等聊天机器人提供了更便捷、更实时的人读情报应用产品。AI 技术的智能推荐，也有助于人读情报的精准推送。据第三方媒体报道，2023 年美国 CIA 正在构建一个类似 ChatGPT 的项目供整

个美国情报界使用，该项目有望为 CIA、NSA、FBI 和各大国家机构提供强力支持。另有知名以色列安全公司 Cybersixgill 推出了 Cybersixgill IQ 产品，以 GPT 方式提供人读情报的使用。

（4）人读威胁情报应用场景“玩出新的花样”。一方面，随着大模型技术的成熟，人读情报已经可以快速、自动、准确地转化为机读情报。据 2023 年绿盟观察，许多国家的情报部门和知名商业情报公司已能够熟练地从人读报告中自动提取机读情报，并每日更新至威胁情报库，实现设备的自动化处理。相信这个技术应用趋势会在 2024 年复制到更多情报使用部门。这也会加速人读情报的使用场景。另一方面，人读情报除了描述当前的威胁，还能预测未知可能的安全威胁，并帮助情报人员采取措施提前构建防御阵地。例如俄乌网络战中的对俄乌技战术的研究报告可为各国网络安全建设提供经验、2023 年金融行业巨头被勒索的详细分析报告能够为同行业单位提供自查与处置参考。预测在 2024 年，通过更好人机接口的升级，人读情报可以在传统机读情报场景上拓展更多的“新花样”。

（5）越来越多的国家情报部门和商业公司在发展人读情报领域。在 2023 年的公开资料里 CIA、Cybersixgill 等情报机构 / 公司均在布局甚至推出人读情报的项目或产品，国内一些主流威胁情报公司也在构建相关产品。在俄乌网络战中大量技战术级人读情报帮助诸多国家分析和提升自身网络安全防御能力，推测人读情报的“甜头”会在 2024 年扩展到更多的威胁情报使用组织，可能也有更多商业公司会推出人读情报的服务。

考虑到安全大语言模型技术的不断成熟，在传统语料基础上，结合 CTEM 的理念，增加对暗网、黑客论坛内容、电报群群组、安全人员 / 黑客人员社交媒体账号等原始情报数据的收集（形成特色化安全语料），结合网络告警等本地化数据，生产的面向网络安全处置决策和参考的人读情报甚至趋势分析或预警将越来越流行和具备市场需求。

相比起机读情报领域催生的产品形态，如威胁情报 IOC 数据服务和威胁情报平台，未来可能会有新的威胁情报产品形态出现，例如面向多源人读情报语料接入，并进行多 AIGC 引擎集成后进行人读情报生成和推荐的智能平台。

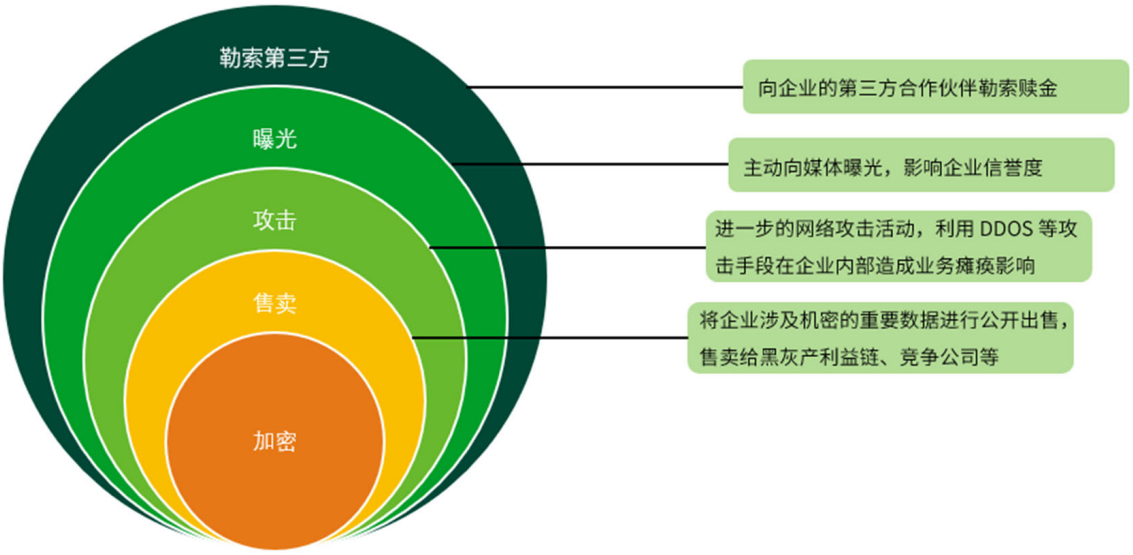
05

趋势 5: 勒索软件仍然是对全球各国企业最具危害的网络犯罪形式，双重勒索、多重勒索等威胁持续增长，勒索手段更加多样化。

勒索软件仍然是对全球各国企业最具危害的网络犯罪形式，2023 年在双重勒索和多重勒索模式下，勒索威胁持续增长，在利益的驱动下形成更多的勒索团伙和更加多样化和复杂化的勒索形式。

如果不支付赎金，勒索软件攻击者通常会威胁受害者将瘫痪某关键业务流程，将涉及企业核心机密的数据进行公开出售，或售卖给黑灰产利益链，还有可能直接卖给竞争公司用于不正当竞争。同时，勒索团伙也可能会发动猛烈的网络攻击，利用 DDOS 等攻击手段给受害者造成某种业务瘫痪。近年来，除上述勒索形式以外，更为严重的是，这些攻击者还可能主动将泄露的数据提供给媒体，以诋毁企业的声誉，使其在公众心目中的形象受到严重损害。此外，他们还可能将黑手伸向企业的第三方合作伙伴，通过勒索赎金的方式进一步扩大攻击范围，增加企业的应对难度。

有趣的是，随着美国等多个国家通过了强制的网络安全事件上报制度，其中也包括数据泄漏，勒索团队也增加了一种勒索形式，如果不支付赎金，攻击者将会向监管机构报告该受害者实际发生的安全事件，从而让受害者遭受名誉和监管方面的损失。



这种从双重勒索向多重勒索的转变，无疑给企业的安全防护工作带来了更大的挑战。由此可见在往后的对抗中企业不仅要预防勒索软件攻击，也要及时的发现和阻断对内的网络攻击活动，而且更重要的是防止企业内部数据泄露，这三点在企业安全防护中同等重要，可使勒索软件攻击带来的危害降至最低。

近年来，围绕直接经济利益的 APT 攻击活动强度持续增加，这一现象在勒索攻击领域尤为明显。部分老牌 APT 组织，例如 Lazarus，利用勒索软件作为获利手段，曾被指控参与多起网络抢劫和勒索软件攻击活动。在获利方面，顶级勒索组织 LockBit 在 2023 年创造了破纪录的勒索攻击次数与赎金总金额，仅在上半年就对 522 个企业实施了勒索，仅美国就向 LockBit 支付了 9100 万美元的赎金。

另外，利用网络设备 0day 漏洞进行勒索的攻击活动将日益增多。包括但不限于 Citrix、Cisco、Fortinet 等知名品牌的设备，2023 年 Lockbit 勒索软件组织就曾利用 Citrix Bleed 漏洞连环攻击了包括波音、工行美国子公司等大型企业，给全球金融、货运等关键领域造成巨大损失。0day 漏洞由于其未知性和难以预防的特点，成为勒索软件攻击者青睐的攻击手段。攻击者利用这些漏洞可以迅速获得系统权限，进而植入勒索软件，实现数据加密和赎金要求。预计 2024 年，这一类漏洞的利用在勒索软件攻击中也将会持续增加。

随着勒索软件威胁的不断增加，Cyber Insurance（网络安全保险）近年来也获得快速发展，2022 年全球网络安全保险市场规模达到 121 亿美元。Cyber Insurance 可以为投保企业提供一定的经济保障，帮助修复或减缓勒索攻击带来的损失。

根据保险公司 Coalition 发布的《2023 上半年网络安全保险索赔报告》，勒索软件攻击索赔频率在 2023 年上半年增加了 27%，其中造成这一峰值的最大因素是 5 月份的频率显著增加。与此同时，勒索软件的索赔严重程度也创下历史新高，平均损失金额超过 36.5 万美元，六个月内飙升了 61%，一年内增长了 117%。赎金要求也有所增加，2023 年上半年的平均赎金金额为 162 万美元，比前六个月增长 47%，比去年增长 74%。有趣的是，今年上半年有 36% 的 Coalition 保单持有人选择支付赎金。

多重勒索模式使得 Cyber Insurance 的赔偿范围变得更加复杂和不确定。除了直接的赎金支付外，还可能涉及到声誉损失、业务中断等多重损失，这为保险公司的定损和赔偿带来了难度。另一方面，网络安全保险也已引起了勒索软件攻击者的注意。他们更有可能会针对已投保网络保险的企业发动攻击，因为这些企业更有可能支付赎金。

另外一个很有趣的值得观察的服务是勒索谈判服务。勒索谈判服务通常作为安全事件紧急响应的一部分，从专业角度帮助客户分析事件过程、勒索影响范围、分析赎金可谈判性、代表客户和攻击者谈判以最大限度降低损失，帮助客户与执法、监管机构沟通等。在某些场合下，帮助客户解决支付和财务操作也会成为勒索谈判服务的一部分。

06

趋势 6: 网络战争加速 DDoS 攻击武器化进程，并经常成为 APT 和勒索攻击的前站，攻击者青睐购买专用云服务器，攻击模式开始向智能策略式攻击发展。

DDoS 攻击已成为网络战中不可或缺的致瘫武器。新兴的 DDoS 利用方式，如 HTTP/2 Rapid Reset 和 SLP 反射放大攻击等不断涌现。攻击者和防御者都在努力提升自身技术水平，以发掘新型攻击和防御策略。DDoS 攻击已不再局限于传统的网络层攻击，而是扩展至应用层攻击和反射攻击等。攻击者利用物联网设备、虚拟专用服务器等新型媒介，提升了攻击的复杂性，使得检测和应对变得愈发困难。随着攻击工具的商业化和服务化趋势，攻击工具的获取变得更加容易，甚至无需攻击者具备高级技术。

观察 23 年巴以冲突网络空间的较量，发起 DDoS 的黑客组织并非始终独立行动，具有共同利益的组织开展互动，迅速组建“战时”利益联盟。这些组织在和平时期各自为战，但在面临冲突时，因共同利益而迅速联手，提升攻击力。如在此次巴以冲突中的社区网络运营联盟机构（C.O.A）团队、Killnet 与 Anonymous Sudan 等黑客团体。此外，部分黑客组织亦会因自身利益诉求而临时组建并参与攻击。

DDoS 攻击模式从简单粗暴的资源耗尽走向智能策略式攻击。智能策略式攻击是指攻击者能够根据攻击目标的环境自适应地选择或预先定义策略路径，智能调整自身攻击模式和行为。与早期的攻击工具不同，智能策略式攻击不仅仅按照预定的顺序执行攻击步骤，而是根据实时情况动态调整策略，以节省攻击资源并规避传统的检测和防御机制，最终最大化的提高攻击效果。

自 2018 年出现的脉冲攻击便是明证，此类攻击在短时间内产生极高的流量峰值，随后突然停止，间隔一段时间后再次发起，以此规避防护设备触发的自动防御机制。发展到 2021 年，扫段攻击粉墨登场，通过对大量 IP 地址实施 DDoS 攻击，尽管单个目标 IP 所承受的攻击流量较小，但汇总起来却不容小觑，此类攻击绕过了 DDoS 防御系统的清洗策略，对整个 IP 段的用户业务产生影响。直至 2023 年，新型测试性 DDoS 攻击更是崭露头角，攻击者利用此类攻击确定目标范围、衡量防御强度，并评估后续所需施加的力量，在这种情况下，最初的 DDoS 攻击可能充当侦察攻击的角色，节省攻击资源，为后续更精确的攻击作好铺垫。

继使用真实主机、僵尸网络、反射节点之后，攻击者逐渐青睐购买专用云服务器 (VPS) 作为攻击源。长期以来，大型僵尸网络主要依赖路由器、打印机、摄像头等物联网设备实施攻击。但这些设备的处理能力有限，通常需要数十万或数百万台设备产生的流量才能对目标造成破坏。如今，攻击者不再仅仅局限于利用物联网（IOT）设备，而是采用云服务提供商提供的虚拟专用服务器（VPS）来进行攻击。云计算提供商提供的虚拟专用服务器，

原旨在让初创公司和企业能以较低成本创建高性能的应用程序。这些虚拟服务器网络拥有更强大的计算性能与网络带宽，攻击者通过购买或入侵控制多台 VPS 组建新型僵尸网络来实现攻击目的。

除此之外，有线索显示 DDoS 逐渐成为 APT 和勒索攻击的前站。DDoS 攻击越来越频繁地试图分散事件响应团队的注意力，以掩盖更大的安全事件。DDoS 攻击本身可能只是烟雾弹，攻击目的不再仅仅是简单的网络干扰，更是为了混淆视线，将防御人员的关注点引向表面，从而在背后为更加隐秘且目的性更强的渗透活动创造条件，发起危害更大的 APT 攻击。

07

趋势 7: 云安全防护重心转向以身份和管理为核心的 CIEM 和 CSPM；而云原生安全将日益实战化、应用化，从基础设施安全转向云原生 API 安全和微服务安全。

当前，云计算安全主要集中于云基础设施安全和云应用安全两个层面，前者趋势从工作负载转向管理控制面安全，而后者则越来越聚焦于云原生体系的安全。

在云计算基础设施安全领域，以往产业界主要聚焦在云工作保护平台（Cloud Workload Protection Platform,CWPP），即关注云主机或容器层面的工作负载，检测并防护相应的威胁事件。然而，2023 年发生的一系列重大安全事件，大多涉及身份、管理和暴露面，而非工作负载。例如：2023 年 5 月，Toyota Connected 云配置错误导致大规模数据泄露长达多年，主要原因是 Toyota Connected 未对其使用的云存储服务进行正确的访问控制；2023 年 9 月，微软 AI 研究团队在 GitHub 上意外暴露了 38TB 隐私数据，主要原因是 SAS 令牌权限配置错误导致 Azure 的 Blob 存储服务可被未授权访问；2023 年 11 月，英国政府承包商 MPD FM 的敏感数据泄露 , 主要原因是其使用的 Amazon S3 存储桶服务被错误地配置了访问权限，导致敏感数据可被任意进行未授权访问。

事实上，早在 2018 年，Gartner 首次提出了云安全态势管理（Cloud Security Posture Management,CSPM）（Gartner,Top 10 Security Projects for 2018,2018），通过事前预防、及时检测云基础设施风险，持续管理 IaaS 和 PaaS 的安全态势。如今随着企业上云成为主流趋势，CSPM 的功能也在不断丰富迭代，目前 CSPM 工具不仅包含云配置管理，还包括数据安全态势管理（Data Security Protection Management,DSPM）、云上身份特权管理（Cloud Infrastructure Entitlement Management,CIEM）等新的能力（Gartner,How to Make Integrated IaaS and PaaS More Secure Than Your Own Data Center,2023），可应对前述针对身份和数据的威胁。

CSPM 与 CWPP 的关注点不同，前者更注重于租户层面的安全，如某企业 AK/SK 遭泄露，攻击者可未授权访问该企业购买的云存储、VPC、云数据库、K8s 集群等众多云服务，并通过不同攻击路径窃取敏感数据，这也是近年云安全事件频发的主要原因之一。通过 CSPM，企业可感知到自身的云服务、服务间的拓扑关系、服务所对应访问权限，以及针对这些云服务的可能攻击路径，再组合相应的检测、响应能力，可有效解决云租户层面的安全问题。IDC 在《IDC FutureScape: Worldwide Cloud 2024 Predictions》报告中预测，到 2024 年，23% 的组织将利用 AI 技术赋能云原生应用保护平台（Cloud Native Application Protection Platforms,CNAPP）和 CSPM。其中，CSPM 会更聚焦于自动化和智能化，通过 AI 算法提升对云安全错误配置自动识别能力，从而降低风险利用。

随着敏捷开发和新型基础设施建设的发展，以容器、编排和微服务技术为代表的云原生

的生态发展迅猛，企业纷纷开始投资云原生安全，安全运营对象从面向底层云基础设施转向面向微服务。出于安全建设的思路，安全团队或对云原生环境进行安全核查和加固，或部署第三方安全产品，以确保云原生环境的安全性，但即使如此，也很难回答“云原生系统是否安全”这一问题，因为缺乏及时更新或安全产品中错误策略都可能会产生风险。事实上，无论是真实的攻击，还是大型攻防对抗演练，都曾出现攻破云平台或云上应用的案例。考虑到云上业务变化频繁，云计算应用规模庞大，仅依靠人工评估很难达到完备。因而，云原生入侵和攻击模拟（Cloud Native Breach & Attack Simulation，CNBAS）将成为云原生安全的发展趋势，一方面，CNBAS 可依托于针对云计算 ATT&CK 矩阵的攻击武器，对云环境进行自动、持续、无害化的攻击模拟；另一方面，参考国内外针对云原生系统的合规性要求和成熟度评估机制，评估系统整体的安全成熟度。可预见越来越多的 BAS 厂商将会提供云原生安全验证的能力，同样，CNAPP 厂商也需要安全验证证明其防护能力和安全策略的有效性。

此外，越来越多的开发团队在拥抱面向应用（微服务）的敏捷开发模式，越来越多的应用交互正从传统的 Web 应用转变为基于云原生技术栈的 API 微服务。然而，这种转变带来了包括功能组件化、服务数量激增、配置复杂等多项挑战，未经管理的微服务本身将是攻击者关注的焦点，同样也是云原生环境中巨大的风险。可预见在 2024 年，面向云原生 API 和微服务的安全服务将得到进一步发展，以有效应对日益增长的安全威胁和填补目前国内云原生安全市场在应用安全层面的短板。以 eBPF 和 API 安全为技术底座，构建面向微服务应用的安全能力，包括东西向零信任的微服务微隔离、API 威胁防护、服务调用可观测性和安全治理等。

08

趋势 8: 随着法律法规的不断制定和完善，以隐私计算与机密计算为基础的安全协同计算和数据安全流转迎来新的发展机遇，相关的互联互通标准化以及打通生态隔离成为关键。

2024 新年伊始，国家数据局会同网信办、工信部、科技部等部门联合印发《“数据要素×”三年行动计划 (2024—2026 年)》（下称《行动计划》），要求通过实施“数据要素 ×”行动充分发挥数据要素乘数效应，赋能经济社会发展。《行动计划》中明确指出，要打造安全可信流通环境，深化数据空间、隐私计算、联邦学习、区块链、数据沙箱等技术应用，探索建设重点行业和领域数据流通平台，增强数据利用可信、可控、可计量能力，促进数据合规高效流通使用。

可预见，在《行动计划》指引下，数据要素的价值将被充分挖掘，通过流转得到最大化的利用。在此过程中，如何保证数据要素的安全，将是至关重要的问题。以隐私计算、机密计算为基础的新技术将赋能多方安全协同计算，以及数据在多方可控、安全的流转。

隐私计算通过社区化运营，孵化了如 FATE、隐语等多个有影响力的开源项目。在商业化方面，隐私计算在金融领域得到了广泛应用，如多方联合建模进行征信查询等。多个垂直领域间进行协作的应用也开始孕育，总体而言，隐私计算产业处于早期，生态初步形成。

机密计算以可信 CPU 为底座，构建可信的执行环境，确保了运算、数据的机密性和完整性。近年信创产业发展迅猛，极大推动机密计算技术落地。平安证券预计 2023 年 -2028 年，我国信创 PC 和服务器合计出货量将超过 3,000 万台，合计市场规模将超过 4,000 亿元。2023 年，财政部发布政府采购需求标准征求意见稿中强调，应当将 CPU、操作系统符合安全可靠测评要求纳入采购需求；中国信息安全测评中心在年底发布了《安全可靠测评结果公告 (2023 年第 1 号)》，包含 CPU、数据库、操作系统三方面的安全可靠测评结果。在国产硬件厂商出货的信创服务器产品中，大多全系引入了可信执行环境技术，有能力为客户提供机密计算环境，保障数据受控、受信、可度量地进行计算、流转和消费。

基于机密计算技术和信创硬件，多家安全厂商推出安全协同计算和数据安全流转产品，部分已在重点行业和机关单位落地应用。在信创需求推动下，基础设施面临大规模更新，此类产品基于机密计算可确保程序和数据安全，避免敏感数据被恶意内部人员或攻击者所窃取。此外，基于虚拟化的可信执行环境还可无摩擦迁移客户已有的业务，对外提供弹性、云化的服务。最终在保证技术先进性的前提下，还能保护数据要素在存储、流转和销毁等过程中的安全性。

机密计算和隐私计算都是数据要素安全流转的关键技术，其最终目标都是支撑数据要素在多方流转过程中的安全性，但在落地层面也存在共同的挑战：产品、生态的互联互通。主流机密技术的架构则存在较大差异，有的提供虚拟机级别的安全防护与隔离，有的提供进程

级别的安全防护与隔离。不同处理器架构的平台所使用的操作系统、镜像都存在差异，使得机密计算应用架构兼容性差、难以互联互通。而隐私计算也存在多个开源项目，不同厂商间的隐私计算平台的架构和接口也存在差异。因而，用户应用在跨平台迁移与开发过程中，需要花费额外的成本，阻碍了新应用的推广。 中国信通院评论文章曾指出：“隐私计算有望成为支撑数据流通产业的基础设施，解决不同产品之间的技术壁垒，实现隐私计算跨平台间的互联互通已成为产业内的迫切需求” 。

推进面向安全协同计算和数据安全流转的机密计算和隐私计算应用，以及互联互通框架的标准化，可以打通不同厂商与平台间的生态隔离，通过制定统一接口标准与协议，做到不同架构或不同厂商应用间的互联互通，最终降低用户应用迁移与开发成本，保障数据安全流转与使用。

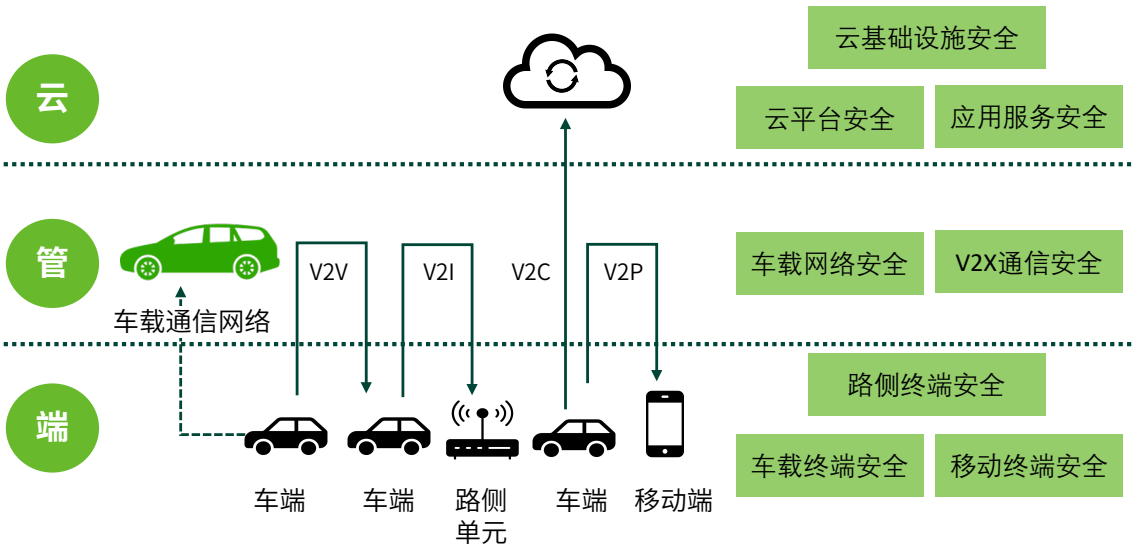
为此，国内隐私计算联盟和开源社区分别起草发布了《金融业隐私计算互联互通技术研究报告》、《金融业隐私计算互联互通平台技术规范》、《金融业隐私计算互联互通 API 接口文档》，为互联互通的实现提供了理论基础。在工业界，联邦学习开源框架 FATE 2.0 分别实现了应用层、调度层、通信层、算法层的互通，为实现异构平台之间的互联互通提供了有力支持。在机密计算方面，相关数据要素流转厂商也对应用架构开始标准化，特别是多方身份、任务、调度等方面的互联互通，从而一方的资源可在另一方可视、可用、可控。

2024 年，数据要素安全流转的重要趋势将是新技术支撑的应用落地，解决真实场景下的问题，打消客户在数据流转过程中的顾虑。相关解决方案能支撑多方间产品和数据的互联互通，逐步扩大整个数据要素的流转范围和参与生态。

09

趋势 9: 智能网联汽车面临信息安全、功能安全、预期功能安全等挑战，有必要构建车路云一体化安全体系建设，加强车联网数据安全保障，建立智能网联汽车多安融合安全态势感知与综合安全治理能力。

随着智能网联汽车的智能化、网联化、数字化发展，车内软件复杂度增加导致汽车电子电气系统故障率提高，复杂场景和多种不确定的长尾效应也造成较大驾驶安全风险。同时，针对智能网联汽车的网络与数据安全攻击事件逐年激增，功能安全、信息安全、人身安全和公共安全面临多重挑战。因而，构建车路云一体化安全体系建设，加强车联网数据安全保障，建立智能网联汽车多安融合安全态势感知与综合安全治理能力，是推进智能网联汽车及智能化路侧基础设施、云控基础平台、V2X 跨域身份互认等产业建设安全落地的重要保障，也是打造汽车产业发展新动能，助力汽车强国、交通强国建设的基础保障。



咨询机构 Upstream 的全球汽车网络安全报告显示，针对智能网联汽车的网络攻击事件数量快速持续增长，2019 年至 2023 年间，公开网络披露的事件激增超 50%，2023 年报道事件数已达 295 起。在 2023 年，汽车和智能出行生态系统后端服务器（远程信息处理、应用程序等）以及信息娱乐系统遭遇的攻击事件急剧增加。与服务器相关的攻击事件占比从 2022 年的 35% 增加到 2023 年的 43%；与信息娱乐系统相关的攻击事件几乎翻了一番，从 2022 年的 8% 增加到 2023 年的 15%。基于车联网新的攻击手段在不断出现，如 1）针对新型 T-BOX 已出现基于车载通信模组信息泄露的远程控制劫持攻击方式、基于 V2V 通信协议的伪造数字签名攻击；汽车智驾模式下又催生出基于生成式对抗网络（GAN）的自动驾驶算法攻击。2）通过电动车辆充电接口的攻击，对智能网联汽车的攻击可以通过充电设备传播到电网基础设施，乃至公用事业系统。轻则造成用户个人财产损失，重则引发充电安全人身事故、社会用电系统故障，甚至威胁国家电力命脉。

近年来，国家有关部委发布了一系列政策文件。2021 年 8 月，国家网信办发布的《汽车数据安全管理若干规定（试行）》，明确要求企业从数据分类分级、数据安全、数据开发利用和共享使用、出境安全管理四个维度，建立汽车全生命周期的数据安全管理机制；2021 年 9 月，工信部发布了《关于加强车联网网络安全和数据安全工作通知》，为智能网联汽车信息安全体系建设给出了指导方针。2024 年 1 月，工信部等六部门联合发布了《关于开展智能网联汽车“车路云一体化”应用试点工作》的通知，标志着我国将持续推进智能网联汽车产品的迭代升级，有机连接“人 - 车 - 路 - 云”各要素，推动智能网联汽车与智慧交通、智慧城市深度融合。安全保障是智能网联汽车产业高质量可持续发展的重要基石，引导城市 / 企业构建车路云一体化安全保障体系，加强车联网数据安全综合治理，开展智能网联汽车多安融合安全态势感知与综合安全防护，是车路云一体化智能网联汽车产业化发展和规模化部署应用的先决条件和重要保障。

构建车路云一体化主动纵深安全监测与防护体系，旨在针对典型车联网安全威胁，实现高效的入侵检测与快速响应处置能力。通过这一体系，预计实现智能网联各业务系统的全生命周期安全防护与统一安全管理，进而达成具备“安全感知、通报预警、智能响应”功能的综合安全态势，确保安全态势的“可见、可管、可控、可信”。终端（车端 / 路侧）安全防护系统，主要应对包括近场攻击、远程攻击 (含来自云端)、车内攻击及对云端的攻击等网络安全威胁，面向代表性的车辆功能安全威胁 (如车辆电池 SOC、温度异常等)，以及驾驶安全威胁 (如预期功能安全失效等)，具备车端与路侧设备的安全威胁监测与主动防御能力，并实时反馈安全风险数据，与云端联动进行及时的安全响应处置，实现全生命周期安全防护闭环。云端安全防护系统，以车联网平台网络安全防护定级备案为指南，进行安全合规性建设部署，形成一套完整的云端安全防护系统架构。V2X 通信安全防护系统，车车、车路通信身份认证能力满足跨域身份认证要求，保障车路安全通信；车云、路云通信具备身份认证、数据加密能力，保障域内车辆、路侧设备与云控基础平台等安全通信。

10

趋势 10: 低空经济崛起，无人机获得广泛应用，无人机安全防护将成发展关键。

2023 年底的中央经济工作会议强调以科技创新引领现代化产业体系建设，提出打造生物制造、商业航天、低空经济等若干战略性新兴产业。作为新质生产力的代表，低空经济在农林、应急、物流、安保等诸多领域发挥着重要作用，这其中，无人机的制造与应用又是低空经济的重要组成部分。据央视数据显示，2023 年我国无人机飞行时长远超传统有人机，达到了 2311 万小时，国内现有注册无人机达 118 万架，其中中大型无人机 10 万架，全国无人机生产厂家 2200 家。目前，我国无人机产业的发展已经处于世界领先水平。

随着无人机在国计民生各领域应用的不断拓展和深入，其数量的迅猛增长已是大势所趋，随之而来的安全问题也将日益凸显。无人机被恶意用作攻击工具或成为攻击目标的事件屡见不鲜。有案例显示，无人机曾被用于近源攻击，攻击者利用两台无人机搭载的一些电子设备，通过 Wi-Fi 入侵了某公司的内部网络；还有一些不法分子通过破解无人机地理围栏系统，使无人机能够突破原本设定的飞行限制，在限高区或禁飞区飞行。在安全研究领域，研究人员也发现了一系列令人担忧的漏洞。2023 年公开的高危漏洞中，无人机操作系统中的远程代码执行漏洞尤为引人关注，该漏洞一旦被利用，无人机便可能完全受控于攻击者；还有固件签名验证绕过漏洞，使固件文件面临被恶意篡改的风险。

为了应对这诸多潜在的安全问题，保障无人机产业的健康发展，有必要将“安全第一”的原则贯穿于无人机研发至应用的每个阶段。在此过程中必然离不开法律、政策层面的保驾护航。一批无人机领域的法律法规和标准已从 2024 年起实施，包括《无人驾驶航空器飞行管理暂行条例》和 GB 42590-2023《民用无人驾驶航空器系统安全要求》，两者都突出同一个关键词“安全”，这里的安全，囊括多个方面。一是管理整治给公共安全造成影响的“黑飞”、“乱飞”现象；另一大方面，是对无人机系统的自身安全及相关数据安全进行规范。还有 2023 年 11 月正式实施的 YD/T 4324-2023《无人机管理（服务）平台安全防护要求》，明确了无人机管理（服务）平台在业务应用、网络规划、设备管理、数据存储及处理等方面应具备的防护能力。

在国家政策层面的高度关注和大力支持下，针对无人机系统及其数据的安全防护类产品、服务及解决方案也必将随着技术的不断创新和市场需求的不断增加，迎来更加广阔的发展机遇。市场上当前已出现还有未来可能会推出的防护检测产品、服务模式、解决方案类型汇总如下：

产品方面，无人机靶场可提供安全测试环境，助早期漏洞发现与修复；入侵检测系统基于预设的规则分析无人机行为，检测异常防范入侵；固件分析平台可加速安全分析过程，提升研究效率；安全芯片提供算法保护措施以及身份识别方案，防范黑客劫持；安全 SDK 保障飞行控制、传感器数据以及通信安全；安全评估系统或可拓展无人机无线链路安全检测功能，用于抗重放攻击测试、合规性检查和模糊测试。服务方面，随着监管政策完善，无人机安全服务将注重合规性、标准化、个性化和定制化，以满足各行业和应用场景的专业需求。解决方案也会各有侧重，如基于零信任的方案强调身份管理、访问控制和数据安全；数字取证方案关注安全事件取证。更多详情参见《2024 无人机安全报告》。

附录 A

1.《安全行业大模型 SecLLM 技术白皮书》

https://book.yunzhan365.com/tkgd/orau/mobile/index.html

2.《2023 年度安全事件观察报告》

https://book.yunzhan365.com/tkgd/ydzq/mobile/index.html

3.《2024 无人机安全报告》

https://book.yunzhan365.com/tkgd/gmpv/mobile/index.html

NSFOCUS

扫码可在手机端直接观看

巨人背后的专家