2024 车联网安全年报

第一章：导言

1.1 报告目的与范围

本报告旨在全面回顾与分析 2024 年度全球及中国车联网安全的发展态势、关键挑战、技术进展与未来趋势。随着汽车智能化、网联化程度的不断加深，车联网已成为网络安全领域不可忽视的关键基础设施。本报告系统梳理了年内重要的法规更新、攻击事件、技术突破以及行业应对策略，旨在为汽车制造商、零部件供应商、科技公司、研究机构及政策制定者提供有价值的参考，共同推动车联网安全生态的健康发展。报告范围涵盖全球主要汽车市场的法规标准、安全威胁、技术动态，并重点关注中国市场的具体情况与特色。

1.2 2024 年车联网安全核心关注点

2024 年，车联网安全领域呈现出若干核心关注点，这些关注点不仅反映了当前的技术发展水平，也预示了未来的挑战方向。

首先，**法规遵从性成为行业发展的基石**。以联合国 UN R155《网络安全和网络安全管理体系》和 UN R156《软件更新和软件更新管理系统》法规为代表的强制性标准在全球范围内逐步落地实施，对汽车制造商提出了覆盖车辆整个生命周期的网络安全管理要求 [1]。这不仅仅是合规层面的挑战，更深远地推动了汽车行业在设计、开发、生产、运维等各个环节对网络安全的系统性重塑。企业必须建立并运行有效的网络安全管理体系（CSMS）和软件更新管理体系（SUMS），确保车辆从设计之初就融入安全理念，并能在漫长的使用周期内得到持续的安全保障和更新。

其次，**攻击手段的复杂化与攻击面的持续扩大对防御体系提出更高要求**。随着车辆功能的日益丰富和车联网生态的不断扩展，从车载信息娱乐系统（IVI）、电子电气架构到云端平台、移动应用乃至充电基础设施，都可能成为攻击者的目标 [2]。供应链攻击、勒索软件、数据泄露以及针对新兴技术（如 V2X 通信、人工智能应用）的潜在威胁，共同构成了 2024 年车联网安全面临的严峻挑战 [2]。

第三，**数据安全与隐私保护的重要性日益凸显**。智能网联汽车作为移动的数据中心，收集、处理和传输大量敏感数据，包括个人身份信息、行车轨迹、驾驶行为等。如何在保障数据安全、符合各国数据保护法规（如 GDPR、中国《个人信息保护法》）的前提下，实现数据的合规利用与价值挖掘，成为全行业关注的焦点 [4]。

第四，**新兴技术的双重影响不容忽视**。人工智能（AI）在提升驾驶体验和安全性的同时，其自身安全性以及被恶意利用的风险也开始显现 [6]。例如，生成式 AI 可能被用于制造更逼真的钓鱼攻击或虚假信息，而 AI 模型的安全性、数据投毒等问题也对车联网安全构成

潜在威胁。同时，AI 也被积极应用于提升网络安全防御能力，如智能威胁检测和响应[6]。

第五，**供应链安全管理的复杂性与紧迫性**。汽车产业链条长、参与者众多，软件和硬件组件往往来自不同的供应商。确保整个供应链各个环节的安全性，防止恶意代码植入或漏洞引入，成为保障车辆整体安全的关键环节[1]。UN R155 法规也明确要求制造商对供应链的网络安全风险进行管理[1]。

这些核心关注点共同塑造了 2024 年车联网安全的整体图景，并指引着行业未来的发展方向和应对策略。

第二章：全球车联网安全法规与标准进展

2.1 联合国法规的强制实施

2024 年是联合国关于车辆网络安全和软件更新法规（UN R155 和 UN R156）全面影响新生产车辆的关键年份。这些法规的生效，标志着汽车行业网络安全从自愿性措施向强制性合规的重大转变，对全球汽车制造商提出了统一的基线要求。

UN R155：网络安全与网络安全管理体系 (CSMS)

UN R155 法规要求汽车制造商建立、实施并维护一个经过认证的网络安全管理体系（CSMS）。该体系必须覆盖车辆从概念设计、开发、生产到生产后阶段的整个生命周期[1]。这意味着制造商不仅要关注车辆本身的技术安全，更要从组织流程、风险管理、供应链协同等多个维度构建持续的网络安全保障能力。

CSMS 的核心要求包括：

- **风险管理**：识别、评估和缓解车辆网络威胁的风险，并覆盖整个产品生命周期，包括开发阶段到终端客户的操作阶段[1]。
- **安全设计**：采用“安全设计 (Security-by-Design)”方法，在车辆开发初期即融入网络安全考虑，以减少价值链上的风险，并最大限度地减少攻击者的入口点[1]。
- **攻击检测与防御**：具备识别和防御网络攻击的措施，并能够通过测试验证其功能[1]。
- **事件响应与报告**：建立网络安全事件响应机制，并要求汽车制造商至少每年向审批机构报告一次相关情况[1]。
- **供应链安全**：确保整个供应链（包括供应商）满足网络安全要求，鉴于供应商目前占软件总体量的 70%以上，这一点至关重要[1]。

UN R155 的实施，促使制造商从过去主要关注功能安全，转向功能安全与网络安全并重。这种转变要求企业投入更多资源进行安全体系建设、人员培训和技术升级，以适应法规带来的持续性合规压力。

UN R156：软件更新与软件更新管理体系 (SUMS)

UN R156 法规针对车辆软件更新过程中的安全问题，要求制造商建立并运行符合标准的软件更新管理体系（SUMS）[1]。该法规旨在确保车辆在整个生命周期内能够安全、可靠地接收和安装软件更新，包括修复漏洞、增加新功能等。

SUMS 的关键要求包括：

- **更新过程的安全性**：保护更新交付机制不被篡改，保证更新的完整性和真实性[1]。
- **软件识别码保护**：保护软件识别码或软件版本不被擅自修改，并能通过车辆接口读取[1]。
- **OTA 更新的法律基础**：为"空中下载 (Over-The-Air, OTA)"更新提供了法律依据，使车辆无论在何处都能及时获得更新[1]。
- **更新失败的恢复机制**：如果更新失败，必须存在恢复功能[1]。
- **用户告知与执行条件**：每次更新及其完成时都应通知用户，并且只有在车辆具备相应能力（如足够的电源，非行驶状态下执行特定更新）时才执行更新[1]。

UN R156 的实施，特别是对 OTA 更新的规范，极大地推动了汽车软件定义化的进程。它不仅要求技术上的安全保障，也对更新流程的透明度、用户体验等方面提出了要求。这两项法规的强制实施，共同构成了汽车网络安全监管的基石，深刻影响着全球汽车产业的格局和发展方向。从 2024 年 7 月起，这些法规适用于所有新生产的车辆，此前从 2022 年 7 月起已对新车型强制执行[1]。

2.2 主要国家和地区政策动态

在联合国法规提供全球性框架的同时，主要汽车生产和消费国家及地区也在积极制定和调整本国/区域内的车联网安全政策，以适应技术发展和本土需求。

中国

中国政府高度重视车联网产业发展和安全保障。近年来，工业和信息化部、公安部、交通运输部等多部委联合发布了一系列政策文件，如《关于加强车联网网络安全和数据安全工作的通知》、《车联网网络安全和数据安全标准体系建设指南》等，系统部署了车联网安全工作[7]。这些政策强调：

- **企业主体责任**：明确汽车生产企业和相关服务提供商的网络安全和数据安全主体责任[8]。
- **全生命周期管理**：要求覆盖车辆设计、生产、销售、运维、报废等全生命周期的安全管理。
- **数据安全与出境管理**：针对汽车数据处理活动，特别是重要数据和个人信息的处理与

出境，制定了严格的规定。

- **标准体系建设**：加快推进车联网安全相关国家标准和行业标准的研制与实施，目前已发布 4 项车规级安全标准和 10 余项平台安全标准，汽车整车信息安全强制性国家标准已完成技术审查 [8]。
- **试点示范与产业协同**：通过试点示范项目推动安全技术的应用和验证，并成立了车联网安全产业发展联盟，促进产学研用协同创新 [8]。
- **基础设施安全**：关注车路协同路侧单元（RSU）等基础设施的安全问题 [9]。

中国在政策层面展现出积极主动的姿态，不仅快速响应国际法规要求，更结合国内产业发展特点，力图构建自主可控的车联网安全保障体系。特别是在 C-V2X 技术应用和标准制定方面，中国走在全球前列，相关政策也体现了对车路云一体化安全协同的重视 [10]。

美国

美国在车联网安全方面采取多管齐下的策略，强调政府引导、行业自律与市场驱动相结合。

- **NHTSA 指南**：美国国家公路交通安全管理局（NHTSA）发布了《机动车网络安全最佳实践》等指导性文件，为汽车行业提供网络安全建议。
- **立法尝试**：国会层面有过多项关于汽车网络安全和数据隐私的立法提案，例如要求车辆配备网络安全系统、规范数据收集和使用等。加州等州份也在积极探索相关立法，如 2023 年签署通过了关于车载摄像头的法案，限制其收集图像视频的商业用途 [9]。
- **研发投入与公私合作**：美国交通部（USDOT）持续投入研发资金，支持车联网安全技术研究和试点项目。同时，鼓励汽车信息共享与分析中心（Auto-ISAC）等行业组织发挥作用，促进威胁情报共享和协同防御。
- **州级行动**：明尼苏达州等州份成立了专门的网联与自动驾驶汽车（CAV）委员会，将网络安全、数据隐私和数据治理作为重点工作方向，探索数据分类、隐私保护框架和公私数据共享激励机制 [4]。该委员会认识到立法进程往往滞后于技术发展，因此强调通过最佳实践和技术专家建议来指导数据安全工作，并努力平衡隐私安全需求与商业投资激励 [4]。

美国车联网安全政策更侧重于风险评估、信息共享和技术创新，同时也在逐步加强对数据隐私的法律保护。

欧盟

欧盟除了全面采纳联合国 UN R155 和 R156 法规外，还通过《通用数据保护条例》（GDPR）等法规对车辆数据的处理和隐私保护提出了严格要求。欧盟网络安全局（ENISA）也发布了针对汽车行业的网络安全指南。欧盟的政策重点在于构建统一的数字

市场，并确保高水平的网络安全和数据保护。

日本

日本在汽车网络安全方面主要遵循联合国 WP.29 制定的规定和要求，重视数据安全和隐私保护 [11]。日本汽车工业协会（JAMA）等行业组织也在积极推动成员企业加强网络安全能力建设。

总体而言，全球主要国家和地区在车联网安全政策上既有共性（如强调风险管理、生命周期安全、数据保护），也因各自产业基础、法律体系和技术路线的不同而各有侧重。这种政策环境的动态发展，对跨国汽车企业提出了更高的合规适应性要求。

2.3 行业标准进展 (ISO/SAE 21434 等)

在法规之外，行业标准的制定和推广对于统一技术规范、提升行业整体安全水平至关重要。其中，ISO/SAE 21434《道路车辆-网络安全工程》标准是车联网安全领域的核心国际标准。

ISO/SAE 21434

该标准于 2021 年 8 月正式发布，为汽车产品（包括系统、硬件和软件组件）的整个生命周期（从概念、开发、生产、运营、维护到报废）提供了网络安全工程的框架和要求 [1]。它并非提供具体的安全解决方案，而是规定了一套系统化的流程和方法，用于管理网络安全风险，确保产品在设计和开发过程中充分考虑网络安全。

ISO/SAE 21434 的主要内容包括：

- **网络安全管理**：要求组织层面建立网络安全策略、目标和流程。
- **项目依赖的网络安全管理**：针对具体车辆项目进行网络安全管理。
- **持续的网络安全活动**：包括漏洞监控、分析和管理。
- **风险评估方法（TARA）**：提供了威胁分析和风险评估（Threat Analysis and Risk Assessment）的指导。
- **产品开发各阶段的网络安全要求**：覆盖概念、系统、硬件、软件等不同开发层面。

该标准与 UN R155 法规紧密相关，遵循 ISO/SAE 21434 有助于企业满足 R155 中关于 CSMS 的要求。它强调网络安全是工程问题，需要系统化的方法和跨部门的协作。

其他相关标准

除了 ISO/SAE 21434，还有一系列与车联网安全相关的标准正在制定或推广中：

- **中国国家标准（GB 标准）**：中国正在加速制定一系列强制性和推荐性国家标准，覆盖车载操作系统、车载信息交互系统、汽车网关、V2X 通信等关键领域的安全要求[8]。例如，《智能网联汽车车载操作系统技术要求及试验方法》等标准正在撰写中，旨在解决车载操作系统架构、功能、性能和安全要求缺乏统一标准的问题[12]。
- **AUTOSAR 标准**：在车载软件平台层面，AUTOSAR（Automotive Open System Architecture）标准中也包含了安全相关的规范，如安全通信、安全启动、安全诊断等。
- **充电安全标准**：针对电动汽车充电过程中的安全风险，相关的国际和国内标准（如 ISO 15118 系列）也在不断完善，涉及充电通信、身份认证、数据加密等方面。

行业标准的不断完善和推广，为汽车制造商和供应商提供了具体的技术指引和最佳实践，有助于降低安全风险、提升产品互操作性，并促进整个产业链的网络安全水平提升。然而，标准的有效实施仍面临挑战，如标准的理解和应用、测试认证体系的建立、以及如何适应快速发展的技术和不断变化的威胁等。

第三章：2024 年车联网安全威胁态势

2024 年，车联网领域面临的网络安全威胁持续演变，攻击手段更加复杂多样，攻击目标也从单一车辆扩展到整个车联网生态系统。

3.1 主要攻击类型与趋势

根据年度安全事件分析，以下几种攻击类型和趋势在 2024 年尤为突出：

- 勒索软件攻击 (Ransomware Attacks)
  勒索软件攻击持续对汽车行业构成严重威胁。攻击者不仅针对汽车制造商及其供应商的 IT 系统，导致生产中断和数据泄露，也开始探索直接攻击车辆或车联网平台的可能性 2。2024 年上半年，汽车行业遭受了多起勒索软件攻击，影响范围波及经销商和供应链的其他环节 2。这些攻击往往造成巨大的经济损失和运营混乱。
- 数据泄露 (Data Breaches)
  数据泄露仍然是车联网安全的主要风险之一。智能网联汽车产生和存储大量敏感数据，包括用户个人信息、车辆数据、位置信息等。攻击者通过入侵车联网平台、移动应用或车辆本身窃取这些数据，用于身份盗窃、欺诈或其他恶意目的 2。2024 年，多起涉及汽车行业的数据泄露事件被报道，凸显了数据保护的紧迫性。
- 针对 IT 系统、云后端、充电设施的攻击 (Attacks on IT Systems, Cloud/Back-end, EV Charging Infrastructure)
  车联网的正常运行高度依赖于后台 IT 系统和云服务。2024 年，针对这些后端系统的攻击（如数据泄露和勒索软件）最为常见 2。从 3 月到 6 月，针对云和后端服务的攻击有所增加 2。此外，电动汽车（EV）充电基础设施及其相关应用也成为新的攻

击热点。研究人员和攻击者都将目光投向了 IVI 系统和 EV 充电桩，发现了诸多漏洞并进行了利用尝试 2。针对充电设施的攻击可能导致充电服务中断、用户数据泄露，甚至可能影响电网稳定。

- 供应链攻击 (Supply Chain Attacks)
  供应链攻击的威胁日益受到重视 3。攻击者通过入侵安全性相对薄弱的供应商，将其作为跳板攻击汽车制造商或在零部件中植入恶意代码/后门。鉴于汽车供应链的复杂性和全球化特性，以及供应商通常被授予特权访问权限以进行监控、维护和更新，这使得它们成为攻击者的高价值目标 3。SolarWinds 事件已为全行业敲响警钟。
- OTA 更新威胁 (OTA Update Threats)
  OTA 更新为车辆提供了便捷的软件升级和漏洞修复途径，但也引入了新的安全风险。如果 OTA 更新过程本身不安全，攻击者可能劫持更新信道、推送恶意固件，从而控制车辆或窃取数据 2。确保 OTA 更新机制的完整性、真实性和机密性至关重要，这也是 UN R156 法规的核心要求之一 1。
- 车内通信与硬件接口安全风险
  车内网络（如 CAN 总线）的安全性以及各种硬件接口（如 OBD-II、USB）的防护仍然是关注重点。不安全的车内通信可能导致关键车辆功能被恶意操控 13。外部设备通过不安全的硬件接口接入，也可能引入恶意软件或导致非授权访问 13。
- 第三方集成风险
  车联网生态系统越来越多地依赖第三方应用和服务集成，例如导航、娱乐、支付等。这些第三方集成点也可能成为攻击入口，特别是涉及电动汽车充电的第三方集成，在 2024 年是频繁的攻击目标 2。

这些攻击趋势表明，车联网安全防护需要一个纵深防御体系，覆盖从云端、管端到车端的各个层面，并特别关注新兴的攻击向量和薄弱环节。技术的快速演进，如 5G、大数据、人工智能等在车联网领域的融合应用，使得网络通信能力、感知计算水平和业务应用都在快速发展，同时也导致车联网安全环境日益复杂，安全需求更多、保障要求更高、防护范围更广 [8]。例如，车路云网通信交互显著增多，车星通信能力持续增强，都对通信安全保障提出了更高要求 [8]。

3.2 重大安全事件与漏洞披露

2024 年，一系列重大安全事件和漏洞披露进一步揭示了车联网安全的脆弱性，并推动了行业对安全问题的重视。

- Pwn2Own Automotive 等赛事的影响
  网络安全竞赛，特别是针对汽车行业的 Pwn2Own Automotive，对发现和披露车辆安全漏洞起到了积极的推动作用。2024 年 1 月由 VicOne 与 Trend ZDI 联合举办的首届 Pwn2Own Automotive 赛事，就发现了特斯拉、电动汽车充电桩、车载信息娱

乐系统（IVI）和汽车操作系统等多个类别的零日漏洞 2。这类赛事不仅激励了安全研究人员投入到汽车安全研究中，也迫使汽车制造商更加重视其产品的安全性，并及时修复已发现的漏洞。上半年记录的一百多起汽车网络安全事件中，部分与此类赛事披露的漏洞有关 2。

- 已披露的重大漏洞及召回事件
  2024 年，汽车行业面临了超过 200 起报告的网络安全事件和创纪录的漏洞发现数量 2。多个汽车品牌因软件缺陷和网络安全问题发起了大规模召回 2。这些漏洞涉及车辆的多个方面，包括但不限于：
  - **车载信息娱乐系统（IVI）漏洞**：IVI 系统因其功能丰富、联网特性和复杂的软件栈，成为漏洞的多发区。
  - **ECU 固件漏洞**：车辆电子控制单元（ECU）的固件漏洞可能导致关键车辆功能（如制动、转向）被远程控制。
  - **通信协议漏洞**：蓝牙、Wi-Fi、蜂窝网络等通信协议的实现缺陷可能被利用。
  - **移动应用漏洞**：与车辆配套的移动应用如果存在安全漏洞，可能被用作攻击车辆的入口。
  - **自动驾驶系统相关的软件误判和召回**：自动驾驶功能的安全性是重中之重，任何软件误判都可能导致严重后果，进而引发召回 [2]。

例如，2023 年曾有报道指出，某汽车制造商的联网服务平台存在访问控制缺陷，可能被利用以远程控制车辆 [8]。丰田公司也承认其日本车主数据库因配置问题，导致约 215 万用户数据面临近 10 年的泄露风险 [8]。这些事件不仅对品牌声誉造成损害，也可能导致用户对智能网联汽车安全性的担忧。值得注意的是，针对车联网服务平台的攻击在 2023 年已达到 805 万次，同比增长 25.5%，服务平台因其业务类型多、数据价值高、网络架构相对简单等特点，成为攻击的重点目标 [8]。

3.3 财务影响评估

网络攻击对汽车行业造成的财务影响日益显著。2024 年，汽车网络攻击导致的估计财务损失（包括勒索软件、数据泄露和运营中断）超过 220 亿美元 [2]。这一数字反映了网络安全事件对企业盈利能力、品牌价值和市场信心的巨大冲击。

财务损失主要来源于以下几个方面：

- **运营中断**：勒索软件攻击或 DDoS 攻击可能导致工厂停产、服务中断，造成直接的生产损失和收入损失。
- **数据泄露成本**：包括调查取证、用户告知、法律诉讼、监管罚款、信誉修复等。
- **召回成本**：因网络安全漏洞引发的车辆召回，涉及软件修复、硬件更换、物流运输等巨大开销。
- **研发投入增加**：为应对日益严峻的安全威胁和满足法规要求，汽车制造商和供应商需

要在网络安全研发、测试和验证方面投入更多资金。
- **品牌声誉受损**：重大安全事件会严重影响消费者对品牌的信任度，导致销量下滑和市场份额流失。
- **股价波动**：安全事件曝光后，相关上市公司股价往往会受到负面影响。

日益增长的财务损失凸显了将网络安全视为核心业务风险，并加大投入进行有效防护的必要性。企业在网络安全方面的预算也更加充裕，并更加专注于预防措施[3]。

第四章：中国车联网安全现状与挑战

中国作为全球最大的汽车市场和重要的智能网联汽车技术创新中心，其车联网安全状况备受关注。近年来，中国在政策引导、标准制定、技术研发和产业生态建设方面取得了积极进展，但也面临着诸多特有的挑战。

4.1 十大安全挑战 (CATARC)

中国汽车技术研究中心数据有限公司（CATARC-ADC，简称中汽数据）连续多年发布“车联网网络安全十大挑战”，为行业提供了重要的风险预警和应对参考。2024 年 11 月 22 日发布的十大挑战，是基于对网络安全事件、威胁报告、漏洞数据和行业案例的收集分析，并结合专家调研和评审形成的[13]。这些挑战具体如下（注：原始报告未提供每个挑战的详细解释，此处基于行业普遍认知进行解读）：

1. **不安全的生态系统 (Insecure Ecosystem)**：车联网涉及主机厂、供应商、服务商、基础设施等多方参与者，生态系统复杂。各环节安全水平参差不齐、接口标准不一、数据共享与安全责任界定不清，导致整体安全防护存在短板[13]。这与全球趋势中对供应链攻击的担忧相呼应[2]，并与中国车联网“车路云网”一体化发展的特点紧密相关，后者使得攻击面进一步扩大[8]。将“不安全的生态系统”列为首要挑战，表明中国专家认为，仅靠单点防护已不足以应对系统性风险，构建一个整体安全、协同联动的生态体系至关重要。
2. **车辆固件和软件存在已知漏洞 (Known Vulnerabilities in Vehicle Firmware and Software)**：大量车辆固件和软件组件中仍存在已公开或未及时修复的漏洞，这些漏洞可能被攻击者利用[13]。
3. **车辆固件和软件可被非授权获取 (Unauthorized Access to Vehicle Firmware and Software)**：攻击者可能通过物理接触或远程手段非法获取车辆固件和软件，进行逆向工程分析，挖掘漏洞或窃取知识产权[13]。
4. **外部设备威胁 (External Device Threats)**：通过 USB、OBD 等接口连接到车辆的外部设备（如诊断工具、U 盘）可能携带恶意软件，或被用作攻击跳板[13]。
5. **不安全的车载通信 (Insecure In-vehicle Communication)**：车内网络（如 CAN 总线）缺乏足够的加密和认证机制，易受嗅探、伪造和重放攻击，可能导致关键车辆

功能被干扰或控制 [13]。

6. **不安全的硬件接口 (Insecure Hardware Interfaces)**：车辆硬件接口（如 JTAG、UART）若未得到妥善保护，可能被用于调试、提取敏感信息或刷写恶意固件 [13]。
7. **数据非法传输 (Illegal Data Transmission)**：车辆数据在采集、存储、传输过程中可能被窃取、篡改或未经授权发送至境外，违反数据安全和隐私法规 [13]。
8. **隐私数据泄露 (Privacy Data Leakage)**：大量个人敏感信息（如身份、位置、驾驶习惯、生物特征）面临泄露风险，对用户隐私构成严重威胁 [13]。
9. **不安全的密钥管理 (Insecure Key Management)**：车辆和车联网服务中使用的加密密钥如果管理不当（如硬编码、弱密钥、密钥泄露），将导致整个安全体系失效 [13]。
10. **不符合法规要求 (Non-compliance with Regulatory Requirements)**：未能满足日益严格的网络安全和数据保护法规（如 UN R155/R156、中国相关法规）要求，面临市场准入受阻、行政处罚等风险 [13]。

这些挑战反映了中国车联网安全在技术、管理和合规等多个层面存在的薄弱环节。

4.2 行业面临的共性问题与市场动态 (Common Issues Faced by the Industry and Market Dynamics in China)

除了上述具体的技术挑战，中国车联网安全行业还面临一些共性的深层次问题，并呈现出独特的市场动态。

- **企业安全意识与投入不足**：尽管法规压力和安全事件频发，部分企业仍然存在“重发展轻安全”的观念，在网络安全方面的资金投入和专业人才配备不足 [8]。这种现象在快速发展的市场中尤为突出，技术迭代迅速，但安全基础相对薄弱，形成了安全能力与发展速度不匹配的局面。这种差距为潜在的大规模安全事件埋下了隐患，亟需通过持续的教育、政策引导和市场激励来提升行业整体的安全成熟度。
- **缺乏针对性的安全产品与服务**：通用的网络安全解决方案往往难以直接适用于车载环境的特殊需求（如资源受限、实时性要求高、安全标准独特等）。行业需要更多针对车联网特点定制化的安全产品和服务，但这面临研发周期长、成本高、适配难度大等挑战 [8]。
- **公共服务能力有待提升**：目前，中国在车联网安全领域的专业化威胁情报共享、风险预警和应急响应公共服务能力尚不充足，难以有效支撑行业应对大规模、有组织的攻击 [8]。
- **专业人才短缺**：车联网安全是一个涉及汽车工程、通信技术、网络安全、数据科学等多个领域的交叉学科，对复合型人才的需求非常迫切。然而，目前市场上既懂汽车又懂安全的专业人才严重短缺，成为制约行业安全水平提升的瓶颈 [3]。
- **市场快速增长与潜力巨大**：尽管存在挑战，中国车联网安全市场正迎来发展机遇。据

赛迪顾问预测，2023 年中国车联网安全市场规模为 8.8 亿元人民币，预计到 2025 年将达到 16.1 亿元人民币，年复合增长率高达 35.3%，市场潜力巨大 [9]。这一方面反映了车联网技术的快速普及，另一方面也体现了安全需求的日益增长。

- **产业协同与生态建设初见成效**：为应对共同挑战，中国汽车行业正在加强合作。车联网安全产业发展联盟已汇聚超过 130 家单位，包括整车厂、零部件供应商、网络安全公司和研究机构，共同推动技术创新和应用示范 [8]。然而，车载操作系统生态的分裂现象依然严重，例如，各大互联网巨头、自主品牌和造车新势力纷纷基于 Android 进行定制化改造，推出各自的汽车操作系统，缺乏统一的架构、功能、性能和安全标准，导致车厂选择困难，也难以实现可复制的规模化推广 [12]。这种碎片化状态，加上供应链安全责任传递不畅的问题 [8]，使得有效的产业协同仍然面临障碍。真正的生态安全需要更深层次、更透明的合作与信息共享，克服竞争壁垒，统一关键接口和协议，才能使产业联盟发挥最大效能。
- **数据合规成为重要驱动力**：日益复杂的汽车数据合规监管环境，正促使整车厂将数据安全与合规置于更优先的位置 [14]。360 车联网安全研究院的专家也指出，汽车安全漏洞不仅造成经济损失，威胁人身安全，还会因地理信息等数据的不当采集和使用带来不良社会影响，相关法规（如自然资源部关于汽车采集地理信息数据的规范草案）正在加强对此类风险的管控 [14]。

这些共性问题和市场动态交织在一起，构成了中国车联网安全发展的复杂背景。解决这些问题需要政府、行业、企业和学术界的共同努力。

第五章：2025 年展望与战略建议

5.1 未来安全趋势预测

展望 2025 年，车联网安全领域将继续在技术创新、威胁演变和防御策略升级的相互作用下不断发展。以下几个趋势值得重点关注：

- **人工智能在网络安全攻防两端的深度应用**：
  - **安全智能体 (Security Agents)**：将成为人工智能在网络安全应用落地的关注热点。安全智能体能通过自然语言与用户交互，记忆上下文，规划需求并调用工具完成任务，从而提升安全输出的准确性和稳定性。未来，安全智能体将从目前主要应用于威胁检测、数据分级、风险评估等工具的智能化，发展为集成解决方案，扮演虚拟安全专家的角色，自主解决复杂安全问题 [6]。
  - **保障人工智能自身安全**：随着 AI 技术的广泛应用，其固有安全风险（如模型算法安全、数据安全、对抗性攻击、数据投毒、隐私泄露）将成为重点研发方向。确保大模型全生命周期的安全以及 AIGC 内容的合规性，将是行业面临的重要课题 [6]。

- 网络安全有效性验证市场的兴起：
  企业安全防护将更加注重实战效果，强调对安全体系抵御真实攻击威胁能力的有效性验证。因此，网络安全有效性验证市场预计将逐渐兴起，其中，攻击与入侵模拟（Breach and Attack Simulation, BAS）技术作为一种新兴的验证方法将受到更多关注 6。这种趋势表明，企业在安全投入上正从单纯采购工具转向追求可衡量的风险降低效果和投资回报。对于安全至关重要的车联网领域，验证安全控制措施能否有效防止车辆受控或数据泄露，将对满足法规和获取用户信任至关重要。
- 软件供应链安全向技术与管理并重方向发展：
  开源技术和云原生技术的普及使得软件供应链日益复杂，安全风险随之增加。未来，软件供应链安全将更加强调技术手段（如漏洞扫描、成分分析）与管理措施（如安全开发流程、供应商风险评估）并重，以应对合规要求和不断演变的安全挑战 6。
- 网络安全与新兴领域融合趋势更加明显：
  网络安全作为伴生行业，将与新技术、新领域的基础设施升级紧密相关，驱动安全技术创新和安全边界拓展。
  - **车联网 (Connected Vehicles)**：未来的安全需求将持续聚焦于漏洞利用防护和数据安全保障 [6]。
  - **低空经济、卫星互联网、算力网络**：无人机物流、卫星通信、分布式计算等新兴领域的发展，将带来新的安全挑战（如信号干扰、链路安全、数据隐私），并催生新的网络安全市场增长点 [6]。这种融合趋势预示着车联网安全将不再孤立，而是成为更广泛的“智慧出行生态系统”安全的一部分，需要应对更复杂的“系统之系统”安全挑战，并加强跨域安全协同。
- **持续关注数据安全与合规**：随着全球数据保护法规的日趋严格以及车联网数据的爆炸式增长，数据安全和合规仍将是未来几年的核心议题。
- **PQC（抗量子密码）的逐步过渡与应用**：随着量子计算技术的发展对传统密码体系构成威胁，PQC 的研发和应用将加速。预计将出现更多经典密码+PQC 混合方案或纯 PQC 迁移方案的探索与实践，以保障长期信息安全 [6]。

下表总结了 2024 年关键安全技术趋势及对 2025 年的展望：

表 1：2024 年关键安全技术趋势与 2025 年展望

技术领域 (Technology Area)	2024 年主要动态 (Key Developments in 2024)	2025 年展望与预测 (Outlook and Predictions for 2025)	相关挑战 (Associated Challenges)

人工智能与安全 (AI in Security)	生成式 AI 驱动安全技术变革，安全大模型产品研发投入增加，应用于威胁检测、安全运营等 [6]。	安全智能体成为应用热点，AI 自身安全（模型、数据、AIGC 内容）成为研发重点 [6]。	AI 算法的可靠性与偏见、数据隐私、对抗性攻击、人才短缺、恶意利用风险。
抗量子密码 (PQC)	PQC 研发与应用进程加速，出现 PQC 混合加密方案的初步应用（如"本源悟空"量子计算机）[6]。NIST 标准化项目持续推进 [15]。	更多 PQC 迁移模型（混合或纯 PQC）的设计与验证，逐步探索与基础设施的适配度和稳定性 [6]。	算法成熟度与实战检验不足、标准化进程、迁移成本与复杂性、与现有系统兼容性。
数据安全技术 (Data Security Technologies)	隐私计算、数据沙箱、大模型驱动的数据分类分级等技术提升数据安全产品能力，数据安全管理平台深化应用 [6]。	数据安全技术与业务场景结合更紧密，自动化、智能化数据安全治理与保护能力增强。	海量数据处理性能、多方安全计算效率、法规遵从性、技术融合难度、用户数据控制权。
攻击面管理 (Attack Surface Management)	更注重持续威胁暴露管理（CTEM）能力建设，实现网络资产攻击面可视化，提升主动防御能力 [6]。	CTEM 理念进一步普及，与 BAS 等技术结合，实现更动态、更精准的风险评估与响应。	资产发现的全面性与准确性、漏洞评估的优先级排序、自动化响应的可靠性、跨云环境管理。
软件供应链安全 (Software Supply Chain Security)	针对开源组件漏洞、依赖关系复杂性等问题的关注度提升，SBOM（软件物料清单）应用开始推广。	向技术与管理并重方向发展，构建更全面的软件供应链安全治理体系 [6]。	供应链透明度不足、安全责任界定、第三方组件安全验证、自动化工具的覆盖度。

5.2 对整车厂、供应商及监管机构的建议

基于 2024 年的安全态势分析和对未来趋势的判断，为有效提升车联网安全水平，对产业链各方提出以下战略建议：

对整车厂 (OEMs) 的建议：

1. **深化“安全设计”与全生命周期管理**：严格遵循 UN R155/R156 法规要求，将网络安全嵌入从概念设计到报废处置的每一个环节。建立并持续优化网络安全管理体系（CSMS）和软件更新管理体系（SUMS）[1]。这不仅仅是合规要求，更是构建可信赖产品和服务的基石，需要从“一次性构建”转变为对车辆生命周期内“持续监控、更新和响应”的思维模式。
2. **强化供应链安全协同**：对供应商进行严格的安全评估和准入管理，明确安全责任和要求，建立协同的漏洞披露和事件响应机制 [3]。推动 SBOM（软件物料清单）的应用，提升供应链透明度。
3. **构建纵深防御体系**：针对车辆端、通信链路、云平台和移动应用等各个层面，部署多层次、异构化的安全防护措施。重视对新兴攻击向量（如 AI 对抗攻击、充电桩安全）的防护。
4. **加强数据安全与隐私保护治理**：制定清晰透明的数据收集、使用和共享策略，获取用户充分授权。积极采用隐私增强技术（PETs），如差分隐私、联邦学习等，在保障数据安全和个人隐私的前提下实现数据价值 [4]。
5. **投入安全测试与验证**：加大对车辆和系统的安全测试投入，包括渗透测试、模糊测试、代码审计等。积极参与 Pwn2Own 等安全竞赛和漏洞悬赏计划，主动发现和修复漏洞。考虑引入 BAS 等技术验证安全措施的有效性 [6]。
6. **培养与储备专业人才**：建立内部网络安全团队，加强对现有员工的网络安全技能培训，并积极引进外部专业人才，以应对日益复杂的技术挑战和人才短缺问题 [3]。
7. **积极应对新兴技术挑战**：关注量子计算对现有加密体系的威胁，提前规划向 PQC 的过渡方案。审慎评估和应用 AI 技术，确保其自身的安全性。

对零部件供应商的建议：

1. **内化安全开发流程 (Secure SDLC)**：将网络安全要求融入产品设计、开发、测试和交付的全过程，确保提供的软硬件组件符合整车厂的安全基线和相关标准（如 ISO/SAE 21434）[1]。
2. **提升自身安全能力**：针对自身产品的特点，投入研发和应用相应的安全技术，如安全启动、代码签名、硬件安全模块（HSM）等。
3. **加强漏洞管理与信息透明**：建立有效的漏洞响应机制，及时修复已知漏洞。向整车厂提供必要的安全信息和 SBOM，支持其进行风险评估和集成验证。
4. **主动配合与协同**：积极配合整车厂的 CSMS 和 SUMS 要求，参与联合安全测试和应急响应演练。

对监管机构与标准组织的建议：

1. **持续完善法规与标准体系**：根据技术发展和威胁演变，动态更新和完善车联网安全法规和标准，特别关注 AI 安全、数据安全、PQC 应用等新兴领域 [7]。推动国际标准

与国内标准的协调统一。

2. **加强市场监管与准入管理**：严格执行 UN R155/R156 等强制性法规，确保新上市车辆满足网络安全和软件更新的基本要求。建立有效的市场抽查和后市场监管机制。
3. **推动测试认证与能力评估体系建设**：支持建立权威的第三方车联网安全测试认证机构和平台，开发标准化的测试规范和评估方法，为行业提供公正、高效的安全评估服务 [8]。
4. **促进信息共享与产业协同**：鼓励和支持建立车联网安全信息共享与分析中心（ISACs），促进政府、企业、研究机构之间的威胁情报、漏洞信息和最佳实践共享 [8]。支持产业联盟发展，推动产业链上下游协同创新。
5. **引导人才培养与意识提升**：支持高等院校、职业培训机构开展车联网安全专业人才培养项目。通过宣传教育、技能竞赛等多种形式，提升全行业从业人员和公众的网络安全意识 [8]。
6. **关注数据跨境流动与国际合作**：在保障国家安全和数据主权的前提下，研究和制定合理的数据跨境流动规则。积极参与全球车联网安全治理，加强国际交流与合作。

没有任何单一实体能够独立保障整个车联网生态系统的安全。因此，产业链各方必须摒弃孤岛思维，加强主动协作和信息共享。无论是 OEM 与供应商之间的紧密配合，还是政府主导的公私合作伙伴关系，亦或是行业组织推动的威胁情报交换，都是提升整体安全水平的关键成功因素。这要求行业在竞争与合作之间找到平衡，为可信赖的协作框架和信息共享机制的建立扫清障碍。

第六章：总结

2024 年是车联网安全领域承前启后的关键一年。联合国 UN R155 和 UN R156 法规的全面强制实施，为全球汽车行业设定了网络安全和软件更新管理的新基准，推动了企业从被动响应向主动构建全生命周期安全保障体系的深刻转变。然而，与此同时，网络攻击的频率和复杂性持续增加，攻击面从车辆本身延伸至云端、充电设施乃至整个供应链，勒索软件、数据泄露等传统威胁依然严峻，针对新兴技术和应用场景的攻击也初露端倪。据统计，2024 年汽车网络攻击造成的财务损失已超过 220 亿美元，凸显了安全问题的严重性 [2]。

在中国市场，车联网产业的蓬勃发展伴随着特有的安全挑战。中汽数据发布的“十大安全挑战”指出了生态系统安全、固件软件漏洞、数据与隐私泄露等核心风险点 [13]。尽管市场规模预计将高速增长 [9]，但企业安全意识、专业人才储备、针对性安全产品供给等方面仍存在短板，“重发展轻安全”的现象依然值得警惕 [8]。

展望未来，人工智能在网络安全攻防两端的应用将更加深入，网络安全有效性验证将成为新的市场需求，软件供应链安全和新兴领域（如低空经济、卫星互联网）的网络安全将受

到更多关注[6]。应对这些趋势，需要产业链各方——整车厂、供应商、监管机构——共同努力，深化“安全设计”理念，强化供应链协同，加强数据治理，投入人才培养，并积极参与国际标准制定与信息共享。

车联网安全已不再仅仅是一个技术问题，而是关系到用户生命财产安全、企业可持续发展、乃至国家关键基础设施安全的战略问题。构建一个安全、可信、有韧性的车联网生态系统，需要持续的投入、不懈的创新以及广泛而深入的合作。2024 年的经验与教训，将为未来车联网安全的发展道路提供宝贵的启示。

引用的著作

1. 汽车网络安全：2024 年 7 月起强制实施的新法规, 访问时间为 五月 26, 2025，https://dqsglobal.cn/dqs%E5%AD%A6%E9%99%A2-%E5%9F%B9%E8%AE%AD-%E5%85%AC%E5%BC%80%E6%B4%BB%E5%8A%A8/%E5%8D%9A%E5%AE%A2/%E6%B1%BD%E8%BD%A6%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%EF%BC%9A2024-%E5%B9%B4-7-%E6%9C%88%E8%B5%B7%E5%BC%BA%E5%88%B6%E5%AE%9E%E6%96%BD%E7%9A%84%E6%96%B0%E6%B3%95%E8%A7%84
2. documents.vicone.com, 访问时间为 五月 26, 2025，https://documents.vicone.com/reports/shifting-gears-2025-automotive-cybersecurity-report.pdf
3. assets.kpmg.com, 访问时间为 五月 26, 2025，https://assets.kpmg.com/content/dam/kpmg/cn/pdf/zh/2024/09/control-system-cybersecurity-annual-report-2024.pdf
4. www.lrl.mn.gov, 访问时间为 五月 26, 2025，https://www.lrl.mn.gov/docs/2025/other/250908.pdf
5. 智能网联汽车数据安全年度洞察（2023）报告发布 - 中国汽车报, 访问时间为 五月 26, 2025，http://www.cnautonews.com/zhinengwl/2024/01/17/detail_20240117362489.html
6. 2024 年网络安全技术回顾与 2025 年趋势展望- 安全内参| 决策者的网络 ..., 访问时间为 五月 26, 2025， https://www.secrss.com/articles/77938
7. 中国通信标准化协会发布《车联网安全标准化白皮书(2023 年)》 - 安全内参, 访问时间为 五月 26, 2025， https://www.secrss.com/articles/61866
8. 车联网安全发展形势、挑战与建议- 安全内参| 决策者的网络安全知识库, 访问时间为 五月 26, 2025， https://www.secrss.com/articles/65223
9. 车联网- 安全内参| 决策者的网络安全知识库, 访问时间为 五月 26, 2025，https://www.secrss.com/articles?tag=%E8%BD%A6%E8%81%94%E7%BD%91
10. www.caict.ac.cn, 访问时间为 五月 26, 2025，http://www.caict.ac.cn/kxyj/qwfb/bps/202312/P020240326618179274556.pdf
11. www.shujiaowang.cn, 访问时间为 五月 26, 2025，https://www.shujiaowang.cn/uploads/20240113/25a9e5f3ee8ae0f1f4bb5d6d10b

66579.pdf
12. 全国汽标委智能网联汽车分技术委员会, 访问时间为 五月 26, 2025，https://www.catarc.org.cn/upload/202401/08/202401081536289386.pdf
13. 中汽数据发布 2024 年车联网网络安全十大挑战, 访问时间为 五月 26, 2025，https://www.catarc-adc.com/xwzxDetail/qyyw/b7765b504df84a8f925c90e860b6a5fc
14. 2024 第三届中国车联网安全大会 - 盖世汽车- Gasgoo, 访问时间为 五月 26, 2025， https://m.gasgoo.com/news/70397199.html
15. 智能网联汽车量子通信技术及其安全应用标准领航研究, 访问时间为 五月 26, 2025， https://catarc.org.cn/upload/202312/20/202312200937100327.pdf