内部资料 免费交流

出版物准印证号：京内资准字 2123- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯

2024全球数字经济大会 Global Digital Economy Conference 2024

2024北京网络安全大会 2024 BEIJING CYBER SECURITY CONFERENCE

AI驱动安全

AI ∞ CYBERSECURITY

——2024 北京网络安全大会专刊

第42期

2024 年 6 月

奇安信
新一代网络安全领军者

打造新一代中国特色的安全托管服务

时刻守护您的网络安全

奇安信安全托管服务以威胁发现为基础、以分析处置为核心、以发现隐患为关键、以解决客户问题为目标，7*24小时全天候全方位守护客户网络安全。

两种模式
模式随心选择
- 直营服务模式：奇安信产品+MSS
- 合作服务模式：技术、产品、服务整体托管

多种形态
全面助力建成
- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

两化融合
帮您真正实现
- 集中服务化：统一监测、预警与通报
- 服务集中化：标准统一、质量可控、资源共享

首创“云地结合”模式
打破传统的托管仅限“云端监测”的认知开辟“云地结合”模式，云端+地端实现真正的闭环服务。

7*24h实时持续监测
“地球不爆炸，我们不放假”——7*24h持续监测，充分保障常态化运营。

安全事件响应快一步
对APT攻击、网络攻击等长效监测，提前预警，响应快一步。

安全事件处置规范化
事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加固。

专家“一对一”指导
专家通过视频一对一的方式与您“面对面”沟通指导，不仅让您了解现状，还能防患于未然。

你为 AI 驱动安全的时代做好准备了吗?

在生成式人工智能的热潮之下，2024 北京网络安全大会的主题同样选择了 AI 相关的“AI 驱动安全”。结合 RSAC 2024 上的安全产品展示，笔者逐步有了这样的认识：在 AI 时代，网络安全行业将会越来越成为巨头企业主宰的舞台。缺乏足够的数据、实战经验、足够算力的中小网络安全企业，尽管具备某些创新技术，将会在 AI 时代面临较大挑战。

AI 大潮之下，各行各业积极应用大模型，这也带来新的风险，包括标注过程、数据流通、训练过程的安全；包括生成 AI 的虚假内容风险。与会专家认为，针对 AI 带来的安全问题应该通过 AI 来解决。中石化集团信息和数字化管理部副总经理蒋楠有个形象的说法：我们要用魔法打败魔法，而不仅仅用魔法对抗魔法。我们需要从更高的角度来考虑，能否用人工智能来解决安全方面的问题。

国内外的网络安全企业在推动 AI 落地安全方面，都进行了各种尝试和创新，比如，利用 AI 用于威胁检测、安全运营，甚至软件开发安全。但真正实现“AI 驱动安全”的落地，却并非易事。

奇安信董事长齐向东在主题演讲中，对“AI 驱动安全”进行了深度诠释，在他看来推动“AI 驱动安全”落地，需要具备三个条件，那就是高质量的数据、体系化的网络安全建设，以及统一的标准。其中，高质量的数据是高水平 AI 的基础，体系化的网络安全建设，是 AI 发挥效率的平台。统一的标准则为 AI 驱动安全实现体系化落地扫除障碍。真正要让“AI 驱动安全”成功落地，实现网络安全响应从滞后到实时的大跃升，让全时段瞬时响应成为可能，这三个条件缺一不可。

在 AI 时代，大型网络安全企业的优势更加明显：携海量的安全数据、安全经验，以及算力优势，可以真正训练出更智能、通用的安全大模型。在体系化和标准化方面，可以发挥体系化的优势，让安全大模型能够“听得懂”，也能“指挥得动”。

面对正在进入的AI时代，作为政企机构，不管你是不是愿意，都需要做好准备。最重要的是，选择与大型安全企业合作，一方面让业务 AI 大模型的应用安全顺畅，同时让 AI 真正驱动自身的安全体系，在未来 AI 与 AI 的对抗中，与时代大潮同步。

总编辑

2024 年 6 月 1 日

CONTENTS 目录

安全态势

综述

嘉宾观点

主题演讲

大会花絮

论坛

《网安 26 号院》编辑部
主办 奇安信集团

总　编　辑：李建平
安全态势主编：王　彪
月度专题主编：李建平
安全之道主编：张少波
奇安资讯主编：陈　冲
报告速递主编：刘川琦
专　栏主编：任润波

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：京内资准字 2123- L0058 号
编印单位：奇安信科技集团股份有限公司
发送对象：奇安信集团内部人员
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2024 年 6 月 26 日

版权所有 ©2023 奇安信集团，保留一切权利。
非经奇安信集团书面同意，任何单位和个人不得擅自摘抄、复制本资料内容的部分或全部，并不得以任何形式传播。

无担保声明
本资料内容仅供参考，均“如是”提供，除非适用法要求，奇安信集团对本资料所有内容不提供任何明示或暗示的保证，包括但不限于适销性或者适用于某一特定目的的保证。在法律允许的范围内，奇安信在任何情况下都不对因使用本资料任何内容而产生的任何特殊的、附带的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉或预期节约的损失进行赔偿。

内部资料　免费交流

政策篇

国内，关键信息基础设施安全保护再上台阶。国标关键信息基础设施边界确定方法公开征求意见，国家能源局印发《电力网络安全事件应急预案》，中央网信办等发布《互联网政务应用安全管理规定》；

国际上，欧盟理事会正式批准《人工智能法案》，这是全球首部人工智能领域的全面监管法规，违反法规的相关方将被追究责任。

国内

国家能源局印发《电力网络安全事件应急预案》

6 月 7 日，国家能源局公布《电力网络安全事件应急预案》，要求完善电力网络安全事件应对工作机制，有效预防、及时控制和最大限度消除电力网络安全事件带来的危害和影响，保障电力系统安全稳定运行和电力可靠供应。本文件所指电力网络安全事件是指由计算机病毒或网络攻击、网络侵入等危害网络安全行为导致的对电力网络和信息系统造成危害，可能影响电力系统安全稳定运行或者影响电力正常供应的事件。电力网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生特别重大、重大、较大和一般电力网络安全事件。

国家标准《网络安全技术 关键信息基础设施边界确定方法》公开征求意见

5 月 31 日，全国网络安全标准化技术委员会归口的国家标准《网络安全技术 关键信息基础设施边界确定方法》已形成标准征求意见稿，现公开征求意见。该文件给出了关键信息基础设施边界确定的方法，包括基本信息梳理、关键信息基础设施功能识别、关键业务链与关键业务信息识别、关键业务信息流识别和资产识别、关键信息基础设施要素识别和边界确定的流程、步骤等内容，适用于指导关键信息基础设施运营者确定关键信息基础设施边界，也可为关键信息基础设施安全保护的其他相关方使用。

工信部印发《工业和信息化领域数据安全风险评估实施细则（试行）》

5 月 24 日，工业和信息化部印发《工业和信息化领域数据安全风险评估实施细则（试行）》，以落实《工业和信息化领域数据安全管理办法（试行）》有关要求，引导工业和信息化领域数据处理者规范开展数据安全风险评估工作，提升数据安全管理水平。该文件适用于境内工业和信息化领域重要数据和核心数据处理者数据处理活动开展的数据安全风险评估。该文件提出，重要数据和核心数据处理者每年至少开展一次数据安全风险评估，评估报告应当包括数据处理者基本情况、评估团队基本情况、重要数据的种类和数量、开展数据处理活动的情况、数据安全风险评估环境，以及数据处理活动分析、合规性评估、安全风险分析、评估结论及应对措施等。细则自 6 月 1 日起施行。

中央网信办等四部门发布《互联网政务应用安全管理规定》

5 月 22 日，中央网络安全和信息化委员会办公室、中央机构编制委员会办公室、工业和信息化部、公安部发布《互联网政务应用安全管理规定》。该文件共八章四十四条，包

括总则、开办和建设、信息安全、网络和数据安全、电子邮件安全、监测预警和应急处置、监督管理、附则。该文件所称互联网政务应用，是指机关事业单位在互联网上设立的门户网站，通过互联网提供公共服务的移动应用程序（含小程序）、公众账号等，以及互联网电子邮件系统。该文件要求，建设运行互联网政务应用应当落实网络安全与互联网政务应用“三同步”原则，采取技术措施和其他必要措施，防范内容篡改、攻击致瘫、数据窃取等风险，保障互联网政务应用安全稳定运行和数据安全。

四部门印发《关于深化智慧城市发展 推进城市全域数字化转型的指导意见》

5 月 20 日，国家发展改革委、国家数据局、财政部、自然资源部联合印发《关于深化智慧城市发展 推进城市全域数字化转型的指导意见》。该文件提出提升城市安全韧性水平，包括加强物理空间安全管理和安全风险态势感知、数字空间安全管理、数据安全体系、个人隐私保护、数据可信流通体系五部分。该文件要求，健全完善网络安全监测预警和应急处置机制，构建城市网络运行安全管理体系，落实数据分类分级保护制度，健全数据要素流通领域数据安全实时监测预警、数据安全事件通报和应急处理机制等。

国际

美国家情报总监办公室发布情报界 IT 能力建设路线图

5 月 30 日，美国家情报总监办公室发布首份信息技术能力建设路线图文件《美情报界信息环境展望：一个信息技术路线图》，这份融合了美情报界一百余名资深技术专家所提建议的文件，就美情报界各成员机构在 2025 至 2030 财年期间如何开展 IT 能力建设，尤其是涉及云计算环境、网络安全、先进计算、数据分析及人工智能等方面提出了前瞻性的技术指导意见。美情报界在 2025 至 2030 财年期间需重点推进五大聚焦领域的 19 个关键举措落地，包括以可靠且具有弹性的数字底座强化任务、以稳健的网络安全保障任务、以现代化的实践和合作关系赋能任务、以数据中心化增强任务、以先进技术和人员技能发展加速任务。

美国防部发布《零信任覆盖》政策指南

6 月 4 日，美国国防部发布《零信任覆盖》文件，作为帮助国防部实现拜登总统签署的 2021 年行政命令中设定目标的路线图和实施指南。该文件首次统一国防部在整个防务界实施零信任的方式，规定分阶段实施零信任控制的方法，并为系统架构师和授权官员开发零信任差距分析。零信任不仅应在国防部内部实施，还应在国防部和各军种的系统及人员队伍中实现，这将是一项挑战。目前零信任尚未在整个国防部体系实施，预计 2027 财年可达到“目标水平”。

欧洲理事会正式批准《人工智能法案》

5 月 21 日，欧盟理事会正式批准《人工智能法案》。这是一项旨在协调整个欧盟人工智能规则的开创性立法。该法案采用基于风险的方法，即对社会的潜在危害越大的人工智能系统法规要求越严格，如被认定构成系统性风险的通用人工智能模型。作为全球首部全面的人工智能法规，它为人工智能治理设定了新标准。该法案在经欧洲议会和欧洲理事会主席签署后，将于近日在欧盟官方公报上公布，并在公布 20 天后生效。

美国证交会通过新规，受监管机构发现数据违规后需在 30 天内披露

5 月 15 日，美国证券交易委员会（SEC）通过修正案，对管理消费者个人信息处理工作的《S-P 条例》进行了修改。修正案要求，机构在发现未经授权的网络访问或客户数据使用后，必须“尽快在不超过 30 天”内通知受影响个人。新规将对美国证券市场的经纪交易商（包括融资门户）、投资公司、注册投资顾问和转账代理人等受监管机构具有约束力。

事件篇

国内发生多起较大规模网络安全事件。安徽一单位遭入侵，3.54 亿条个人信息被盗，据通报，该单位服务器存在多处安全隐患；国内知名电器售后系统遭入侵，涉案金额高达 1.2 亿元，据分析，该系统 APP 存在 40 余项安全漏洞。

美国政府发布 2023 网络安全年报披露 11 起重大事件

6 月 12 日 The Register 消息，美国白宫管理和预算办公室发布《联邦信息安全现代化法案（FISMA）2023 财年报告》，对联邦机构 2023 财年基于 FISMA 报告的网络安全状况进行了概述和分析。报告显示，2023 财年各联邦机构报告的网络安全事件数量高达 32211 起，同比增长 9.9%，数量排名前三的事件类型分别是不当使用、钓鱼和恶意电子邮件、Web 攻击。报告还披露了 11 起重大事件，涉及卫生与公共服务部、财政部、司法部等 8 个联邦机构，其中多起事件与 MOVEit 软件漏洞被利用相关。

云存储巨头 Snowflake 被黑，165 家知名企业遭殃

6 月 11 日 Ars Technica 消息，谷歌旗下威胁情报公司 Mandiant 发布报告称，云存储巨头 Snowflake 的大量客户实例遭黑客攻击，导致全球 165 家知名企业发生大规模数据泄露，而且发生数据泄露的 Snowflake 客户的数量还在不断增加。据悉，此次攻击事件已经波及了票务巨头 Ticketmaster、桑坦德集团（Santander Group）、汽车零配件巨头 Advance Auto Parts 等一大批知名企业，数以亿计人受到影响。Mandiant 报告显示，针对 Snowflake 客户的黑客攻击“爆炸半径”还在不断扩大中，Mandiant 正与 Snowflake 合作调查与其客户数据泄露有关的一系列漏洞。Mandiant 表示，一群黑客利用信息窃取恶意软件获取的凭据，对未启用多因素认证（MFA）的 Snowflake 账户和未对不受信任位置访问设置限制的 Snowflake 客户实例实施大规模攻击。黑客使用的某些凭据已有数年历史。Snowflake 发表声明称，正在“制定一项安全加固计划，要求客户实施多因素认证”。

勒索攻击迫使越南国家邮政服务瘫痪超 3 天

6 月 11 日 The Record 消息，负责越南当地邮政服务的国企越南邮政于 6 月 4 日遭到勒索软件攻击，邮政和快递服务受到影响。该公司当时报告称，旗下邮政金融、公共物流和货物分发等部分服务未受影响。越南邮政与政府机构和当地网络专家合作，以遏制事件，保护客户数据，并恢复其系统。在发现该事件后，越南邮政联系了国家安全机构，并断开了其 IT 系统以隔离漏洞。截至 6 月 7 日晚上 10 点，越南邮政服务于客户和运营管理活动的 IT 系统已恢复运行。越南邮政没有透露他们认为谁是幕后黑手，或者黑客是否索要赎金。

涉中跨境电商熊猫购支付赎金后被撕票，上千万用户数据遭泄露

6 月 6 日 Bleeping Computer 消息，主打全球用户海淘中国商品的跨境电商平台 Pandabuy（熊猫购）近期曝出数据泄露事件。黑客“Sanggiero”3 月底与 6 月初两次在数据泄露论坛销售 Pandabuy 数据，第一次公布了 300 万条数据，其中包括客户姓名、电话、邮箱、登录 IP、住址及订单详情等；第二次以 4 万美元售价兜售 1700 万条数据。Pandabuy 发言人表示，曾向黑客支付了一笔未公开金额的赎金，试图阻止数据泄露，但黑客可能已将数据共享给其他人，公司决定不再与其合作。根据 Pandabuy 发言人自相

矛盾的陈述，专家猜测 Pandabuy 并未一次性支付所有赎金。

安徽一单位遭入侵 3.54 亿条个人信息被盗，公检联合督促整改

6 月 6 日检察日报正义网消息，2023 年 6 月 29 日，安徽省某单位信息中心向公安机关报案称遭到网络攻击。在司法程序中，当地检察院承办检察官审查发现，嫌疑人利用黑客工具扫描存在漏洞的服务器，攻击目标服务器，非法获取了包含姓名、身份证号、联系电话、不动产信息等内容的公民个人信息 3.54 亿余条。值得庆幸的是，嫌疑人还没来得及出售这些个人信息，就被抓获归案了。经进一步分析，检察官了解到被入侵的近 20 台服务器存在防火墙过期、采用弱口令、未定期修改登录密码、疏于对外包服务单位管理等情况。对此，检察院联合公安机关向被入侵服务器所属单位通报并督促整改。

国内知名电器集团售后系统遭入侵，涉案金额高达 1.2 亿元

6 月 5 日封面新闻消息，四川南充仪陇警方成功打掉开发、销售和使用黑客破坏软件的 4 个犯罪团伙。据悉，当地警方在办案过程中，发现两款黑客软件都攻破了一家知名企业的电器售后服务系统，伪造电器安装服务工单，骗取售后安装服务费。经分析发现，国内某知名电器集团官方 APP 存在源代码未进行强制权限检查、后台服务器数据交互未加密等 40 余项安全漏洞，被犯罪嫌疑人利用，开发出了能够控制官方 APP，轻易侵入售后服务系统，并非法控制进行数据修改的黑客工具。据了解，这两款“黑客”软件是这家电器集团售后服务人员内外勾结，合力研发出来的，研发人员熟悉公司流程和系统规则。警方梳理出北京、浙江、广东等全国 29 省市共有 802 人使用这两款软件，涉及售后合作网点 786 个。涉案总金额高达 1.2 亿余元。

美国发生超大规模电信网络攻击，60 万台路由器集体变砖

5 月 30 日 Lumen 消息，美国电信公司 Lumen Technologies 旗下黑莲花实验室发布报告称，2023 年年底美国发生一起超大规模电信网络破坏事件，黑客在 72 小时内瘫痪了互联网接入服务商 Windstream 的超过 60 万台家庭 / 家庭办公路由器（型号为 ActionTec T3200），这些“变砖”的路由器无法修复，导致大量用户被迫进行硬件更换。公共扫描数据显示，在事件期间，Windstream 的自主系统号（ASN）下接近半数（49%）的路由器被攻击下线。这次攻击对农村和偏远社区影响尤其严重，导致紧急服务中断、农业监控信息丢失和远程医疗服务中断等。

加拿大老牌药店遭勒索攻击闭店，被索要超 1.8 亿元赎金

5 月 22 日 The Register 消息，加拿大连锁药店伦敦药房已确认，勒索软件团伙窃取了一些包含员工信息的公司文件，并表示“不愿意也无力向这些网络罪犯支付赎金”。该公司在声明中称，4 月 28 日的入侵事件是一场“由一帮组织严密的全球网络罪犯策划的攻击”。这次攻击导致伦敦药房所有门店全部关闭约 10 天，期间药房员工被迫在店外填写重要处方。LockBit 勒索软件团伙在 5 月 21 日声称对此次攻击负责，要求伦敦药房在 5 月 30 日前支付 2500 万美元（约合人民币 1.81 亿元），并威胁如果这家连锁药店不付款，将泄露窃取的数据。

大型医疗服务商被黑！澳大利亚政府警告发生“大规模勒索软件数据泄露”

5 月 17 日 The Register 消息，澳大利亚电子处方提供商 MediSecure 于 16 日发表声明称，发现一起影响个人和健康信息的网络安全事件，初步迹象表明，事件可能源自一家第三方供应商。该公司后续表示，“该事件影响了 MediSecure 系统截至 2023 年 11 月保存的数据。”澳大利亚联邦警察正在调查这起入侵事件。澳大利亚国家网络安全协调员发布警告称，这是一次“大规模勒索软件数据泄露事件”，表示政府“继续帮助 MediSecure”，并正在努力了解数据泄露事件的规模和性质。澳大利亚政府正在向卫生部门行业团体通报数字入侵和应对情况，通报对象包括澳大利亚医学协会、澳大利亚药剂师协会和主要私立医院服务商。

漏洞篇

5 月以来，Google Chrome 浏览器官方一反常态，接连发布 4 个在野漏洞利用公告，包括 CVE-2024-4671、CVE-2024-4761、CVE-2024-4947、CVE-2024-5274。鉴于这些漏洞影响范围较大，建议客户尽快做好自查及防护。

SolarWinds Serv-U 目录遍历漏洞 (CVE-2024-28995) 安全风险通告

6 月 14 日，奇安信 CERT 监测到官方修复 SolarWinds Serv-U 目录遍历漏洞 (CVE-2024-28995)，SolarWinds Serv-U 容易受到目录横向漏洞的影响，未经身份认证的远程攻击者，通过构造特殊的请求可以下载读取远程目标系统上的任意文件，对机密性造成很高的影响。目前该漏洞技术细节与 EXP 已在互联网上公开，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

PHP CGI Windows 平台远程代码执行漏洞安全风险通告

6 月 7 日，奇安信 CERT 监测到官方修复 PHP CGI Windows 平台远程代码执行漏洞 (CVE-2024-4577)，未经身份认证的远程攻击者，可以通过特定的字符序列绕过此前 CVE-2012-1823 的防护，通过参数注入攻击在远程 PHP 服务器上执行任意代码，从而导致远程代码执行、敏感信息泄露或造成服务器崩溃。目前该漏洞技术细节已在互联网上公开，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Apache OFBiz 路径遍历漏洞安全风险通告

6 月 6 日，奇安信 CERT 监测到 Apache OFBiz 路径遍历漏洞 (CVE-2024-36104) 在互联网上公开，未授权的攻击者可以通过构造恶意请求绕过认证，进而访问系统中的敏感接口，造成任意代码执行。目前该漏洞技术细节与 EXP 已在互联网上公开，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Check Point 安全网关任意文件读取漏洞安全风险通告

5 月 30 日，奇安信 CERT 监测到 Check Point Security Gateways 任意文件读取漏洞 (CVE-2024-24919) 存在在野利用，远程攻击者可以通过构造恶意请求读取服务器上的任意文件，造成敏感信息的泄漏。目前，此漏洞已检测到在野利用。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Google Chrome V8 类型混淆漏洞 (CVE-2024-5274) 安全风险通告

5 月 24 日，奇安信 CERT 监测到 Google 发布公告称 Google Chrome V8 类型混淆漏洞 (CVE-2024-5274) 存在在野利用，远程攻击者可通过诱导用户打开恶意链接来利用此漏洞，从而获取敏感信息或代码执行。目前，此漏洞已检测到在野利用。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Sonatype Nexus Repository 3 路径遍历漏洞安全风险通告

5 月 23 日，奇安信 CERT 监测到官方修复 Sonatype

Nexus Repository 3 路径遍历漏洞 (CVE-2024-4956)，未经身份认证的远程攻击者通过构造特殊的请求可以下载读取远程目标系统上的任意文件，对机密性造成很大的影响。目前该漏洞技术细节与 EXP 已在互联网上公开，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Atlassian Confluence 远程代码执行漏洞安全风险通告

5 月 22 日，奇安信 CERT 监测到 Atlassian 官方发布新版本修复高危漏洞 Atlassian Confluence Data Center and Server 远程代码执行漏洞 (CVE-2024-21683)。经过身份认证的远程攻击者，通过构造特殊的请求，利用该漏洞可以执行任意代码，对目标系统的机密性、完整性和可用性造成很大的影响。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

GitHub Enterprise Server 身份认证绕过漏洞安全风险通告

5 月 21 日，奇安信 CERT 监测到 GitHub Enterprise Server 身份认证绕过漏洞 (CVE-2024-4985) 细节已公开在互联网。GitHub Enterprise Server(GHES) 中存在身份验证绕过漏洞，该漏洞与 SAML SSO 身份验证机制有关。当利用具有可选加密断言功能的 SAML SSO 身份验证时，攻击者可以利用此漏洞伪造 SAML 响应，从而绕过身份验证机制，这可能允许攻击者配置或获取具有站点管理员权限的用户访问权限。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Zabbix Server SQL 注入漏洞安全风险通告

5 月 21 日，奇安信 CERT 监测到 Zabbix zbx_auditlog_global_script SQL 注入漏洞 (CVE-2024-22120) 在互联网上公开。在 Zabbix 系统中，具有 Detect operating system 权限的用户可以通过时间注入获取管理员凭证，进一步利用可以结合后台功能执行代码。目前该漏洞技术细节与 PoC 已在互联网上公开，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Git 远程代码执行漏洞安全风险通告

5 月 20 日，奇安信 CERT 监测到官方修复 Git 远程代码执行漏洞 (CVE-2024-32002)，由于 Git 在支持符号链接的不区分大小写的文件系统上的递归克隆容易受到大小写混淆的影响，未经身份认证的远程攻击者，利用该漏洞使受害者克隆操作期间执行刚刚克隆的代码，从而导致远程代码执行。目前该漏洞技术细节与 EXP 已在互联网上公开，鉴于该漏洞影响范围较大，只影响 Windows 和 Mac 系统，建议客户尽快做好自查及防护。

Google Chrome V8 类型混淆漏洞 (CVE-2024-4947) 安全风险通告

5 月 16 日，奇安信 CERT 监测到 Google 发布公告称 Google Chrome V8 类型混淆漏洞 (CVE-2024-4947) 存在在野利用，远程攻击者可通过诱导用户，打开恶意链接来利用此漏洞，从而获取敏感信息或代码执行。目前，此漏洞已检测到在野利用。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Google Chrome V8 越界写入漏洞 (CVE-2024-4761) 安全风险通告

5 月 14 日，奇安信 CERT 监测到 Google 发布公告称 Google Chrome V8 越界写入漏洞 (CVE-2024-4761) 存在在野利用，攻击者可通过诱导用户，打开恶意链接来利用此漏洞，从而在应用程序上下文中执行任意代码、获取敏感信息或导致应用程序崩溃。目前，此漏洞已检测到在野利用。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

注：使用公司邮箱发送企业名称和需开通订阅的邮箱地址至 cert@qianxin.com，即可申请订阅最新漏洞通告。

对抗篇

国内攻防演习 5 月态势：哪些薄弱点最易被利用？

作者 | 奇安信安服团队

一、本月演习整体情况

2024 年 5 月，奇安信 Z-TEAM 团队共承接攻防演习服务 31 场，行业级攻防演习 1 场，地市级行业攻防演习 3 场，客户自主攻防演习 27 场。

本月承接攻防演习数量，与上月对比呈下降趋势（见图 1）。

本月承接的攻防演习涉及金融、企业、政府部委行业客户较多，且较上月涉及的行业范围略有扩大。其中，政府部委行业攻防演习场次减少，金融行业攻防演习承接场次略有增多（见图 2）。

本月攻防演习成果如表 1 所示：

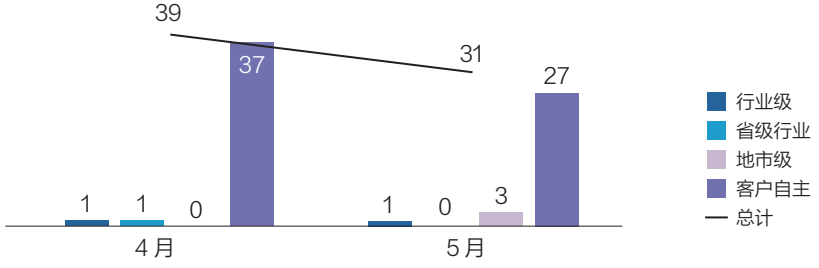


图 1 4-5 月 Z-TEAM 承接攻防演习数量统计

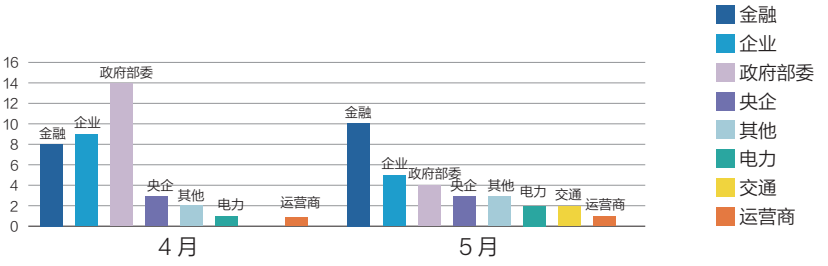


图 2 4-5 月攻防演习涉及行业统计

目标系统	靶标	强隔离内网	核心业务网	网站	堡垒机	安全设备	业务系统	服务器
数量	43	57	66	91	38	112	461	988

表 1

二、本月任务目标特点

本月攻防演习和评估任务覆盖行业比较广泛，涉及目标包括金融、企业、政府部委、央企、电力、交通、运营商、其他行业。随着我国交通基础设施的不断更新和升级，其中越来越多的设备和系统依赖于网络技术。这些设备和系统的运行和控制都离不开网络，一旦网络受到攻击或故障，将直接影响交通系统的正常运行和服务，给人民生命财产安全带来严重威胁。因此，须提高交通行业网络安全能力，建设坚不可摧的网络安全防线。在本月攻防演习中交通行业占比为 6%（见图 3）。

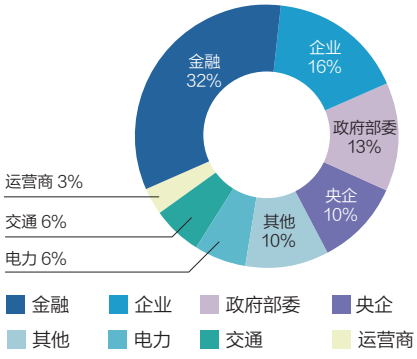


图 3 5 月攻防演习分布

三、主要攻击手段分析

基于本月奇安信 Z-TEAM 团队实战成果分析，对不同的行业目标使用了不同攻击手段，如政府部委、电力、其他行业外网突破的主要手段包括漏洞扫描利用和口令爆破等；企业、央企、运营商行业主要是钓鱼攻击和漏洞扫描利用、VPN 仿冒接入等；金融、交通行业外网突破的主要手段包括漏洞扫描利用和供应链攻击、隐秘隧道外联等。各个行业使用的主要技术手段分布如下（见图 4）。

本月攻防演习服务中，攻击队使用攻击手段主要有：漏洞扫描利用、钓鱼攻击、口令爆破、VPN 仿冒接入、隐秘隧道外联、供应链攻击技术等。

整体攻击手段与上月对比，漏洞扫描利用和 VPN 仿冒接入有明显上升趋势，隐秘隧道外联和供应链攻击手段利用率基本趋同，钓鱼攻击和口令爆破有明显下降趋势（见图 5）。

本月任务中交通行业攻防演习任务占比为 6%，通过对该行业演习数据分析发现，攻击者在外网纵向突破时，会寻找薄弱点并利用漏洞扫描进行攻击。然后以此为基础，在内网进行水坑钓鱼和 VPN 仿冒接入等攻击手段来实现横向拓展和渗透。在攻防演习中，攻击者往往需要多种攻击手段相互配合才能成功地进行渗透和拓展。

四、典型攻击手段实现案例

网络安全威胁对交通运输领域产生的影响不容忽视。首先，黑客攻击可能导致交通系统的瘫痪。例如，通过入侵交通管制系统篡改交通信号灯的控制程序，让交通秩序陷入混乱或拥堵状态；窃取交通系统中的敏感信息，如车辆定位数据、司机身份信息等，进而实施非法利用或恶意操作。

其次，网络安全漏洞的存在可能对交通安全构成潜在威胁，从而可能引发交通事故的发生。在交通运输领域，众多系统均高度依赖于网络连接与信息传输技术的稳定运行，其中包括自动驾驶汽车和列车信号系统等关键设施系统。如果这些系统遭受攻击或损坏，将给乘客与行人的安全带来严重威胁，不容忽视。此外，网络攻击有可能导致交通设备损坏，给交通运输系统的运维带来巨大的挑战。

案例：0day 漏洞形成连环攻击，快速突破多道防线

在针对某交通行业进行防御演练的过程中，奇安信攻击队在开展网络

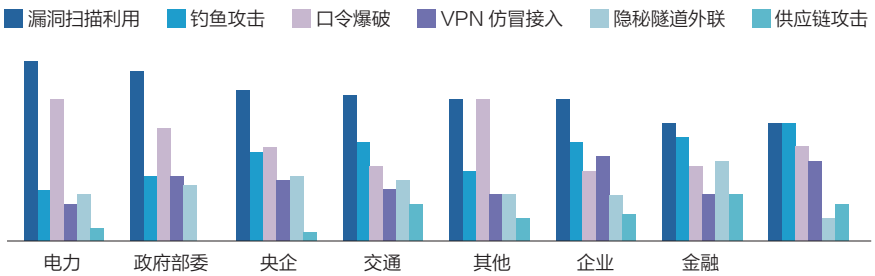


图 4 行业攻击手段分布

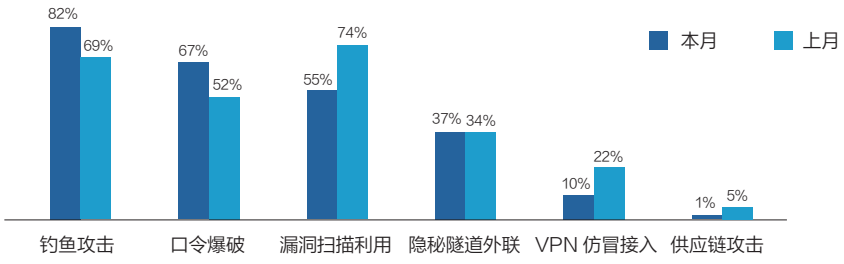


图 5 攻击手段对比

攻击前，首先针对该目标进行了全面且细致的信息收集工作。首先，通过信息收集，攻击队利用 OA 系统 0day 漏洞的 PoC 程序，快速发现该单位某一个业务板块所使用的 OA 系统存在该 0day 漏洞，并且该系统，已暴露于互联网环境中。攻击队利用该 0day 漏洞的 EXP 程序，快速地获取了目标 OA 系统服务器的权限，继而取得了 WebShell 的权限。然而，在尚未稳固立足之际，运维人员便察觉到了 OA 系统的异常情况，迅速对 OA 系统应用及其数据库进行了服务器迁移工作，并同步修复了漏洞。攻击被发现，行动受阻，攻击队的工作永远是具有随机性、挑战性、对抗性的。在工作过程中，总会有各种出其不意的情况出现，只有随机应变，充分利用出现的各种机遇，才能最终突破目标完成任务，攻击队这次的目标就是如此。

在持续进行安全测试的过程中，攻击队意外发现该单位的门户网站存在可被利用的漏洞，从而成为潜在的攻击目标，经过研究和分析，攻击队成功利用一个 0day 漏洞获取了该门户网站应用及操作系统的管理员权限，进而成功获取到该单位办公内网的接入权限。

在横向移动过程中，攻击队又探测到该单位内网中的多个服务系统及数台服务器。通过已经获得的门户网站管理员账号和密码信息进行撞库尝试，成功入侵该单位内网系统，并掌握了其中绝大部分服务器的控制权。这表明，该单位内网中存在大量系统服务器均使用了相同的管理账号和密码。利用密码抓取技术，发现几位服务器管理员使用了弱口令，基于这些弱口令，我们成功地获取到一些服务器和设备的后台管理控制权限，涵盖云平台外网监控系统、项目管理系统等关键系统。

图 6 案例攻击路线图

最终，攻击队利用获取到的账号口令登录到虚拟化平台，定位到演练目标系统的虚拟主机，并顺利获取了管理员权限。至此，渗透工作顺利完成！

五、安全加固建议

1. 案例剖析

交通运输行业作为国家关基建设的主要领域之一，其高度重视防护建设工作。某交通行业客户更是行业中较早入场安全防护建设的先锋，在经历多年的安全运营和攻防沉淀，建立了具备企业特色的安全运营体系，可以监测发现网络安全风险并有效处置。

然而，庞大的企业规模，复杂的分布式网络和供应链体系，致使其存在安全防护盲区和短板，在面对“应用系统 0day 漏洞 + 弱口令 + 集权设备”组合式攻击时，无法有效应对和防护，导致攻击队成功突破企业安全防护壁垒进入内网，通过内网层层突破，最终拿下了大量服务器权限和核心生产设备控制权。

案例暴露问题：主要存在未知威胁攻击的及时发现和阻断，弱口令及相同密码等密码账号登录保护 2 类问题。

2. 防护策略

(1) 通过补能力、增策略、强分析、练应急等多种措施强化未知威胁攻击监测和防护。

① 补能力：基于情报和特征分析能力上，加强异常行为分析、内存异常分析、运营时分析能力；

② 增策略：加强策略自定义维护，加强后门连接检测能力、异常行为检测、制定关键场景威胁建模，加强黑客工具、漏洞特征、报文长度、异常识别、EXP 特征的识别能力；

③ 强分析：利用安全设备，加强跨设备的安全分析能力，协助用户快速找到攻击入口，及时进行溯源；

④ 制定合理、高效的应急、通联方案，并进行充分的演练，提升疑似遭受未知威胁的攻击的应急响应能力。

(2) 以攻击方视角检测账号、口令风险，主动发现账号、口令存在的安全隐患，从风险检测、风险整改到账号口令运维，形成账号口令检测运维体系，做到风险整改闭环，解决账号资产梳理难、风险发现难、管理难等问题。

构建或优化常态化安全运营体系，基于平战融合、云地协同的网络安全运营原则，建立常态化的资产、漏洞、威胁的安全运营，通过人 + 工具 + 流程的方式，基于安全监测、终端和主机安全防护等措施，持续地进行发现识别、监测分析、研判处置等闭环管理，实现漏洞为威胁的动态清零，在持续的运营过程中提升网络安全防御能力。安

规划快一步

奇安信

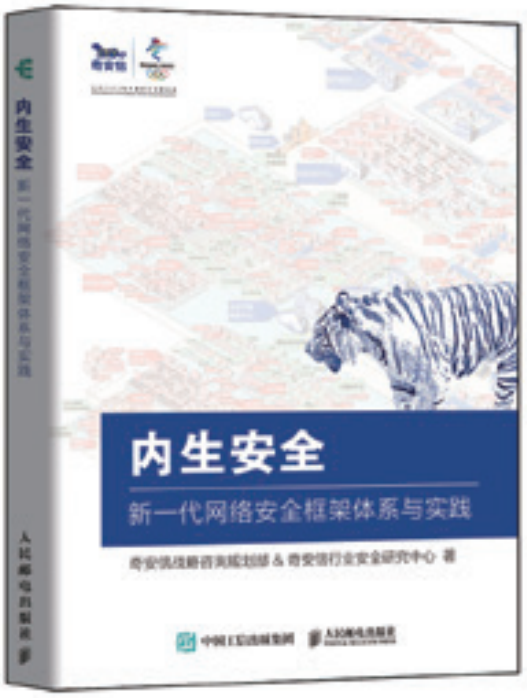
北京2022年冬奥会官方赞助商

新书发布

内生安全权威解读

19支团队、37位专家倾力打造

政企“十四五”网络安全规划必读书籍



- 什么是内生安全
- 内生安全从何而来
- 为什么要内生安全
- 内生安全如何落地
- 新一代网络安全框架
- “十工五任”建设要点

扫描二维码
专享内购价

AI 驱动：网络安全进入智能新纪元

2024 年 6 月 5 日至 6 日，以“AI 驱动安全”为主题的 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会（以下简称“BCS 大会”）在北京国家会议中心举行。来自 10 多个国家和地区的上百位专家学者、10 多个行业领域的上千名业界代表，围绕“AI 驱动安全”主题展开研讨。

与会专家认为，随着 AI 在多个领域的广泛应用，网络安全风险与威胁呈指数级增长，传统的人人对抗、人机对抗已转向 AI 攻防对抗。AI 驱动下，网络安全的边界、技术和场景都出现了全新变革，如何确保 AI 正向赋能网络安全成为智能时代高质量发展的关键议题。

本届北京网络安全大会共举办了 2 场峰会、20 多场分论坛、2 场网络安全大赛，以及网络安全展等系列活动，海内外嘉宾就 AI 驱动安全在数据、能源、金融、交通、制造等领域的情况

展开讨论。

在 BCS 大会开幕式上，全国工商联副主席、中国民间商会副会长 汪鸿雁，中国友谊促进会理事长、国家网信办原副主任 陈智敏，中国职业技术教育学会会长、教育部原副部长 鲁昕，北京市政府副秘书长 许心超，中央网信办网络安全协调局副局长 王营康，中国电子信息产业集团有限公司总经理 李立功致开幕辞。中国工程院院士、鹏城实验室主任、北京大学博雅讲席教授 高文，中国工程院院士、同济大学讲席教授 蒋昌俊，巴基斯坦 NCERT 主席、国际工程技术学会会士、英国计算机学会会士 海德尔 · 阿巴斯，先进计算与关键软件（信创）海河实验室主任、中国新一代人工智能发展战略研究院执行院长 龚克，Forrester 副总裁兼高级研究总监 弗雷德里克 · 吉隆，国家电网有限公司副总信息师、中国电机工程学会会士 王继业，全国政协委员、全国工商联副主席、奇安信集团董事长 齐向东出席论坛并发表主旨演讲。

BCS 产业峰会邀请了联合国副秘书长 李军华、北京市经济和信息化局副局长 顾瑾栩致辞，巴基斯坦 NCERT 执行主席 阿尔塔夫 · 乌尔 · 拉赫曼、中国联通集团网络与信息安全部总经理 苗守野、中石化集团信息和数字化管理部副总经理 蒋楠、比亚迪股份有限公司信息中心基础架构与信息安全部部长 罗小平、奇安信集团总裁 吴云坤进行了主题演讲，数百位网络安全业界专家参会。

2024 北京网络安全大会邀请到来自 10 多个国家和地区的上百位专家学者、10 多个行业领域的 200 多家企业的代表，预计吸引 6000 余人参会。

作为具有全球影响力的网络安全大会，北京网络安全大会已成功举办五届，先后有来自中、美、俄、法、日等全球 30 多个国家和地区，超过 2000 位政要、行业领袖、网络安全专家出席并进行精彩分享。

AI 驱动网安边界拓展

“当前，我国新一代人工智能正在与实体经济深度融合，广泛应用于社会民生领域，激发了创新活力和社

会潜能。”中国友谊促进会理事长、国家网信办原副主任 陈智敏在 BCS 大会上表示。

这一观点得到嘉宾们的普遍认同。在本届 BCS 大会上，多位嘉宾分享了人工智能在网络安全领域应用的优秀案例。总体来看，嘉宾们认为，人工智能打破了网络安全的人力资源边界、效率边界、质量边界。

首先，人工智能打破了网络安全的人力资源边界。“安全人员数量和资源不足，是造成网络安全失陷的主要原因，也是维护网络安全面临的最大问题。根据调研，只有 1% 的万人以上规模企业，拥有超过 30 名安全运营人员，研判告警比例达到 10% 以上，其余企业网安人员严重不足。”全国政协委员、全国工商联副主席、奇安信集团董事长 齐向东认为，生成式人工智能（AIGC）技术浪潮使得安全知识与经验能够大规模快速复制，极大缓解了网络安全专业人才市场巨大的供需矛盾。“只要算力允许，AI 可以创造出无数个拥有安全经验、逻辑推理、自我学习能力的机器人，且能够全天候工作。”

其次，人工智能打破了网络安全的效率边界。“人工智能的自动化和智能化特性可以大大提高网络安全管理的效率。” 作为人工智能治理领域的知名专家，先进计算与关键软件（信创）海河实验室主任、中国新一代人工智能发展战略研究院执行院长 龚克如此判断。

对此，奇安信集团总裁 吴云坤也指出，通过应用人工智能，可以提升威胁判定的准确度，从海量噪声中快速、准确地洞察和判定真正的风险。据其透露，1 个安全大模型处理安全告警的能力相当于 50 ~ 60 个网络安全工程人员。

最后，人工智能打破了网络安全保障的质量边界。由于人力资源不足、人工处理分析安全风险能力过载、人员身心疲惫等因素，网络安全威胁处置的质量难以得到保障，误判、漏报等情况在所难免，但人工智能极大地改变了这一情况。吴云坤透露，奇安信将人工智能病毒引擎 QDE 加入病毒样本检测。通过对 132 万多个样本检测的结果显示，QDE 的检出率为 97.9%，比传统引擎高出 4.13 个百分点，误报率仅 0.009%，大幅低于传统引擎误报率（0.04%）。此外传统引擎需要人工参与，但 QDE 无需人工介入。

“人工智能是新质生产力，智能化大势不可阻挡。要发展 AI 促安全。”龚克提醒，“不发展才是最大的不安全”。

AI 驱动网安技术革命

“人工智能的发展推动了网络安全技术的创新。”龚克呼吁推进 AI 与网络安全融合创新。

在本届 BCS 大会上，与会嘉宾们分享了当前 AI 与网络安全融合创新的理念和最新进展。工信部赛迪研究院网络安全研究所副所长 王超在 BCS 大会信创安全分论坛上作了题为《信创安全的新形势新挑战》的演讲，提出要实施以智能辅助为核心的网络安全策略，实现由被动防御向主动防护转变，利用人工智能等技术增强党政等机构网络安全保障能力。

据中国联通集团网络与信息安全部总经理 苗守野介绍，中国联通在通话、短信、上网、亲情守护等场景，融合使用传统模型和联通元景大模型，迭代网络安全技术，增强风险监测和反诈处置能力。“目前对网络威胁的识别准确率达到 90%，已服务 3000

多万安全产品用户。”苗守野说。

奇安信今年 3 月对外正式发售的“AI 驱动安全”代表性产品 QAX-GPT 安全机器人，也表现出革命性的网络安全防护能力。例如，QAX-GPT 安全机器人对真实网络风险事件研判准确率达到 100%，可以消除 80% 以上的无效告警，助力企业网络安全运营效率提升逾 60 倍。该款产品已经应用于金融、能源等头部企业的网络安全系统。

“AI 驱动安全已是大势所趋，未来网络攻防就是得 AI 者得天下。”齐向东说。

AI 驱动网安场景创新

本次 BCS 大会还举办了网络安全展，主办方在展区设置了 AI 造假、勒索攻击、智能驾驶等沉浸式场景，通过现场体验，让参观者真实感受网络空间无处不在的风险。

参观者在展区扫描面部信息后，可实时伪造一段知名影星的表情或动作视频，足够以假乱真。然而，展区工作人员介绍，奇安信人工智能研究院基于自身积累的海量知识和大数据，能够快速准确识别多种前沿 AI 伪造技术生成的虚假图片和视频，对上述虚假视频可以“一眼识破”。

除了丰富的论坛、会议和现场体验，本届 BCS 大会还举办了两场全国性比赛，以推动 AI 驱动安全的认知普及和前沿技术探索。6 月 5 日举办的第二届“盘古石杯”全国电子数据取证大赛决赛上，参赛者展示了如何快速搜集、固定人工智能电子证据；6 日举办的第九届安全创客汇决赛，则将 AI 技术引入数据安全领域，展示了 AI 自动处理引擎、AI 数据资产识别、数据流转智能分析等技术创新的前沿亮点。

此外，全国工商联网络与数据安全委员会在本次 BCS 大会上召集奇安信、联想等 60 家领军企业共同发起《打造“人工智能 + 安全”新质生产力》倡议，涵盖了芯片、操作系统、网络、数据库、中间件、应用软件等数字经济产业链上的知名企业。

与会专家倡议，积极拥抱人工智能技术，共同推进人工智能技术在数字化产业安全、健康、有序的可持续发展，赋能千行百业；推动数字安全技术创新，持续研发数字安全新产品，开启人工智能 + 网络安全新能力；以人工智能技术为驱动，形成数字安全新质生产力；建立数据安全共享机制，推进人工智能时代下数字经济大发展。安

陈智敏

中国友谊促进会理事长、
国家网信办原副主任

陈智敏：AI 发展须倡导科技向善、造福人民

中国友谊促进会理事长、国家网信办原副主任 陈智敏 6 月 5 日出席 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会战略峰会（BCS2024）时表示，“科研技术人员要树立科技向善理念和造福人类准则。人工智能发展必须坚持以人民为中心，在增进人民福祉的同时，解决好人民群众反映的强烈突出问题，使人工智能发展成果更多、更公平地惠及全体人民。”

陈智敏指出，我国新一代人工智能正在与实体经济深度融合，广泛应用于社会民生领域，激发创新活力和社会潜能。要保障“人工智能的发展与安全”，陈智敏认为应关注五大问题：

一是健全基础性数据制度。应以主体在民、主权在国、企业开发、全民共有、共享共用的基本思路、妥善解决好数据权属问题，进一步健全数据采集、使用、流通、交换、交易、分配等制度。

二是落实产业发展规划战略。引导人工智能发展与国家创新驱动发展战略相衔接，使新技术与实体经济深度融合创新，不断催生新产业新业态新模式，加快培育和形成新质生产力。

三是倡导科技向善理念。要在科研技术人员中树立科技向善理念，为人工智能发展形成正确价值导向和稳定社会预期提供有力保障。

四是坚持以人民为中心。要使人工智能发展成果更多、更公平地惠及全体人民，确保人工智能始终服务于人的全面发展和人类社会的可持续发展。在确保人工智能始终处于人类的安全控制之下，打造可审核、可监督、可追溯、可信赖的人工智能技术，积极构建人工智能伦理法律体系。

五是加强国际合作交流。坚持和尊重数据国家主权，积极推动各国执法合作。要充分发挥海量数据优势，积极参与人工智能治理国际规则的制定，为构建全球人工智能治理体系贡献中国智慧和中国方案。

李立功

中国电子信息产业集团有限公司总经理

李立功：加快打造国家网信事业的核心战略科技力量

6 月 5 日，2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会（BCS2024）战略峰会在京召开。中国电子信息产业集团有限公司总经理 李立功出席开幕式并致辞。

李立功强调，人工智能是引领未来的战略性技术，是新一轮科技革命和产业变革的重要驱动力量。本次大会以“AI 驱动安全”为主题，旨在将 AI 作为网络安全的驱动力，帮助专家快速识别、追溯和处置安全威胁，提升网络安全防御的智能化水平。本次大会的主题，既直面当前全球最关心的网络空间安全问题，又指明了未来网络安全的发展方向，既有现实意义，也有非常强的前瞻性。

中国电子作为网信事业的国家队，聚焦国之所需，服务国家战略，统筹发展计算产业、集成电路、数据应用、网络安全、高新电子五大主业，加快打造国家网信事业的核心战略科技力量。在数字化、网络化、智能化加速演进的新时代，中国电子将牢记职责使命，以奇安信为网络安全平台，扛起国家队的重任，与大家一道深化协同，合力推进网络安全的技术创新，合力拓展网络安全的应用场景，合力打造网络安全的产业生态，为构建人类网络空间命运共同体作出更大贡献。

汪鸿雁：民营企业是网络强国建设的重要力量

6月5日，全国工商联副主席、中国民间商会副会长 汪鸿雁在2024全球数字经济大会数字安全高层论坛暨北京网络安全大会（BCS2024）战略峰会开幕式上致辞表示：“民营企业作为深度参与推动我国网信事业发展的重要力量，在维护网络安全、加快形成新质生产力、助力实现网络强国战略目标进程中，潜力巨大，前景广阔。”

汪鸿雁表示，今年是习近平总书记提出“网络强国战略”目标的十周年。十年来，在以习近平同志为核心的党中央坚强领导下，网络强国的宏伟蓝图徐徐展开，网络安全保障能力得到了全面提升，政府、企业、社会组织、广大网民共筑的网络安全防线越发牢固。

在当前新一轮科技革命和产业变革向纵深推进，既带来了前所未有的机遇，也带来了风险挑战和竞争压力。民营企业作为深度参与推动我国网信事业发展的重要力量，在维护网络安全、加快形成新质生产力、助力实现网络强国战略目标进程中潜力巨大，前景广阔。

一是维护网络安全要强化责任担当。企业作为网络安全产业的重要主体，要充分参与网络安全和数据安全的保障体系和能力，认真落实数据安全和个人信息的保护要求，促进行业健康有序安全的发展，将企业的经营发展融入网络强国建设的伟大实践当中。

二是维护网络安全要坚持创新自立。希望广大企业能够瞄准重大的网络安全科技问题，走自主创新之路，突破掌握关键核心技术，加快信息技术的创新应用和生态建设，在激烈竞争中抢占先机，赢得主动。

三是维护网络安全，扩大开放，争取合作共赢。广大企业要主动把握全球产业链重构带来的新机遇，深度参与全球产业分工和合作，用好国内、国际两个市场、两种资源，积极“走出去”、努力“走进去”、争取“走上去”。积极参与全球互联网治理，助力构建网络空间的命运共同体。

许心超
北京市人民政府副秘书长

许心超：北京将打造引领全国数字安全行业的全产业链

6月5日，北京市人民政府副秘书长 许心超出席数字安全高层论坛暨北京网络安全大会开幕式并致辞。

许心超副秘书长指出，作为2024全球数字经济大会的首场高层论坛，北京网络安全大会为数字安全产业交流合作搭建了良好的平台。北京将努力打造引领全国数字安全行业的全产业链，重点将加强核心技术突破创新，推进标准体系建设，构建繁荣产业生态，为数字安全新产业、新业态、新模式健康发展提供保障。

一是加强数字安全技术攻关。充分发挥科技资源和创新能力优势，加大对数字安全基础设施、技术研发攻关的支持力度，强化数字安全标准，提升数字安全能力。

二是推进数字安全产业发展。完善数字安全相关政策规划，打造优势互补的产业集聚区，重点建设国家网络安全产业园，积极谋划国家数据安全产业园，大力发展京津冀网络安全产业集群，打造引领全国数字安全产业发展的新型空间载体。

三是完善数字安全产业生态。发挥行业组织作用，推动供需对接、标准建设、技术合作、宣传推广等，强化协同联动体制机制，共同构建活力强劲、协作紧密的产业生态体系。

龚克

先进计算与关键软件（信创）海河实验室主任、中国新一代人工智能发展战略研究院执行院长

龚克：人工智能是先进生产力，不发展是最大的不安全

6月5日，先进计算与关键软件（信创）海河实验室主任、中国新一代人工智能发展战略研究院执行院长 龚克在 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会战略峰会上强调，“人工智能是先进生产力，必须大力发展。不发展是最大的不安全。人工智能和网络安全密切相关，应该全力推动人工智能和网络安全的融合创新。”

他认为，ChatGPT 的横空出世，标志着数字化进入新阶段，智能化加速发展。

龚克表示，以大模型为代表的人工智能表现出的强大功能，带来了网络安全、法律、伦理等方面的风险，使很多人产生焦虑。

但人工智能是引领科技革命和产业变革的战略科技力量，正在快速发展，并且表现出跨模态特点，量变正在带来质变。

“发展人工智能，是代表先进生产力的发展方向。”龚克认为，人工智能会带来很多风险，但不发展是最大的不安全，将丧失新的生产力革命的机遇。

针对人工智能的风险，龚克强调了两点：第一，要承认和正视人工智能风险的存在。第二，要具体分析人工智能风险来自于什么地方，既不要神话 AI，也没有必要妖魔化 AI。“从现在的实践来看，人工智能风险并不是来自于技术太强，而是来源于技术不够强，存在各方面的技术瓶颈，特别是管控技术和堵点亟待突破，从而引发很多社会焦虑。”

在龚克看来，人工智能与网络安全是相互依赖、相互促进的关系。人工智能可以加强网络安全，同时也带来数据的安全问题。这就要求网络安全和人工智能要深度融合创新，这是我们的发展方向。

王继业

国家电网有限公司副总信息师、中国电机工程学会会士

王继业：AI 赋能网络安全，助力能源转型

6 月 5 日，国家电网有限公司副总信息师、中国电机工程学会会士王继业出席 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会战略峰会时表示，“3060 双碳目标催生构建新型电力系统，导致电力网络安全风险倍增。绿电时代呼唤 AI 赋能网络安全防护。

王继业指出，“新型电力系统变得更为开放和互动，在网络安全方面也面临重大挑战。由于新型电力系统接入主体类型多、数量大、分布广，接入方式多种多样，网络结构和形态复杂，交互频繁，再加上人工智能技术的广泛使用，使得电网遭受网络攻击的风险急剧上升。”

针对 AI 安全，王继业强调，重点是利用 AI（防守）来防护 AI（攻击），也就是通过 AI 增强安全防护能力和效率，包括异常行为的自动化检测能力，恶意代码识别能力，轨迹趋势分析预测能力，自主决策和自动化执行能力等；还要研究自动化漏洞的识别能力，爆破弱口令的能力和通过 AI 增强网络安全运营效率与能力等。

王继业强调，网络防护的整体性、系统性需要进一步增强，网络安全不是一个部门、一个企业、一个行业的事情，而是涉及各方主体。他呼吁业界各方凝心聚力、携手共进，不断完善网络安全整体防护体系，为守护网络安全，助力能源转型做出更大贡献。

高文

中国工程院院士、鹏城实验室主任、北京大学博雅讲席教授

高文：打造大规模 AI 模型训练的强大底座

6 月 5 日，中国工程院院士、鹏城实验室主任、北京大学博雅讲席教授出席 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会战略峰会，并发表题为《鹏城云脑与脑海系列大模型》的主旨演讲。

高文表示，要想做大的人工智能工作和任务，需要有底座、有模型。鹏城实验室正在推进云脑 3 的建设计划在今年年底完成。云脑作为专门面向大规模人工智能模型训练的底座，可以为大规模人工智能模型的训练提供比较强的基础。

据了解，鹏城云脑 3 是一个 2 万多块卡的机器，算力可达 1.6 万 P，将会是全世界单一系统算力最强的机器，可以支持万亿级大模型的训练，从而可以对企业进行赋能，对整个经济建设、社会发展各种各样应用的赋能。

高文还介绍了大模型训练中的数据安全相关问题。针对有些用户希望数据是别人看不见的，鹏城云脑专门开发了相关技术，使数据可用不可见：只有数据应用者能看得见自己的数据，其他人都看不见，但可以用。训练的时候就可以做到相对比较安全。训练完成后，训练参数拿走前会有检验流程，通过相关工具分析参数里有没有带数据，数据拥有方就可以签发是否允许可以把参数带走。

通过从可信数据空间角度进行划分，使得整个处理流程、授权都有相应的对应，这样在大型数据中心上做人工智能模型训练就放心的多。现在这一工具不仅在单一的数据中心，并且在多中心都可以进行数据安全管理。

蒋昌俊

中国工程院院士、同济大学讲席教授

蒋昌俊：打造一体化的算网安全体系

6 月 5 日，中国工程院院士、同济大学讲席教授蒋昌俊在 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会战略峰会上发表《智能算网系统》的主题演讲。蒋昌俊表示，算力网络面临的安全性不可忽视。要改变当前被动式攻击、孤立式网络安防的现状，必须通过一体化算网体系，以及专业化、多模态化和大规模形式，形成安全有效的算力方式。

人工智能大模型的发展离不开算力。蒋昌俊透露，目前从市场前景和调研可以看到，到 2025 年国家算力网络市场大约在 900 亿元，通用算力将增长 10 倍，人工智能算力将增长 500 倍；另外，算网重点是从建设开始，逐步转向调度应用。

目前算网调度的基数布局来看有一些局限性，如服务模式的单向局限、各自为营的局部局限，以及调度范围的同域局限等，如何应对算网新型需求，我们将改变局部范围，通过技术进行可扩展发展。

蒋昌俊认为，要通过方舱计算等核心技术实现算网协同。方舱计算系统主要由方舱生成与管理系统、虚拟数据中心系统和跨域资源调度系统三部分组成。具有机动性、灵活性的特点，形成方舱专用机动，资源跨域伸缩，系统维护自治的格局。同时，在安全性方面，可以通过行为认证、原位计算、本真计算来保证系统安全和数据安全、模型安全，可以基于方舱计算，形成一体化的算网安全体系。

倪光南
中国工程院院士

倪光南：推动数据存储发展促进新一轮科技革命和产业变革

6 月 5 日，中国工程院院士倪光南出席 BCS 2024 北京网络安全大会 – 信创安全论坛，并发表了《大力推动中国数据存储产业 掌握数字经济发展主动权》主题演讲。倪光南院士认为，随着数据成为关键生产要素，作为数据载体的存储产业应当作为国家战略性、基础性、先导性产业给予大力支持，以促进新一轮的科技革命和产业变革。

IDC、Gartner 等第三方咨询机构预测，到 2025 年，我国存储产业直接投资总额将超过万亿元规模。但存储产业历来是国外厂商占据全球绝大多数市场份额。

对此，倪光南表示，中国存储产业必须打破外国跨国公司的垄断，才能争得自己的一席之地。此外，数据存储同时应该作为产业来抓，乘着人工智能新一代技术变革的黄金时期，在我国数据量即将跃居世界第一的大背景下，作为国家战略性、基础性、先导性产业予以大力支持。

当前，为进一步发展我国存储产业需要解决以下问题。一是，算力、存力和运力的均衡配置。算力是处理数据的能力，存力是存储数据的能力，运力是传输数据的能力，三者应当均衡配置，不能偏废失调。

二是应该加大对先进存储技术研发和创新，推动以先进的固态硬盘 SSD 取代传统机械硬盘 HDD 的“存储革命”。

最后倪光南表示，除了做到以上两点，还要大力推进“行标”“团标”的制定、高校存储产业人才的培养、存储国家实验室 / 国家级科创平台等的成立，打造优越的体制机制环境以及丰富的科技创新资源，全面推动国产数据存储产业繁荣发展。

李克强
中国工程院院士、国家智能网联汽车创新中心首席科学家

李克强：信息安全与数据治理是智能网联车的核心必要条件

6 月 6 日，中国工程院院士、国家智能网联汽车创新中心首席科学家李克强在 BCS2024 智能网联新能源汽车安全论坛以视频形式做主题报告，对中国智能网联汽车产业战略布局进行了全面解读。李克强表示，智能网联汽车是自动驾驶汽车发展新阶段，信息安全、数据治理则是智能网联汽车应用的核心必要条件。

汽车行业正在进入智能网联时代。李克强指出，未来的智能网联汽车是在智能化基础之上运行，同时支撑联网运行和信息安全管理体系保障的新架构车辆。基于这样一种定义，李克强院士提出了中国方案智能网联汽车发展思路。中国方案的智能网联汽车信息物理系统架构，就是充分融合智能化与网联化发展特征，以五大基础平台为载体，实现车路一体化的智能网联信息系统。五大平台包括云控基础平台、高精度动态地图平台、车载终端基础平台、计算基础平台，以及信息安全基础平台。

李克强还强调，未来信息安全建设平台同样需要生态建设的，在生态建设方面开展的方向包括安全企业务要协同，联合检测认证安全企业做产品融合、业务融合，把平台做大。

海德尔 · 阿巴斯

巴基斯坦 NCERT 主席、国际工程技术学会会士、英国计算机学会会士

海德尔 · 阿巴斯：大型语言模型正彻底改变网络安全形势

6 月 5 日，巴基斯坦 NCERT 主席、国际工程技术学会会士、英国计算机学会会士 海德尔 · 阿巴斯在出席 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会战略峰会时表示，大型语言模型正彻底改变网络安全形势。

海德尔 · 阿巴斯强调，我们现在面临的挑战非常明确，很多人在使用人工智能的过程中并没有充分了解 AI 技术本身，以及人工智能技术可能带来负面的影响，从而导致危害。

人工智能在网络安全领域的应用，带来了很多益处和应用场景，如检测速度提升、网络安全响应改善、防止网络诈骗等。但如果人工智能被用于武器化的攻击，可能会导致所使用模型出现训练目之外的结果，并且会出现恶意的架构和机制，且非常复杂、很难监测，可以悄无声息地带来负面结果，如投毒攻击、漏洞利用工具包、僵尸网络等。

此外，阿巴斯认为，当前全球面临“深度伪造”的挑战——生成海量假新闻、假文本，并在网络上快速传播，以达到一些恶意的目的。“在未来几年中，假信息会给整个人类社会带来巨大的挑战。”

海德尔 · 阿巴斯强调，在国家层面需要格外引起重视，需要深度理解人工智能在组织层面和国家层面，甚至对整个人类社会的影响。ChatGPT 确实可以给我们带来益处，但如果这样的技术被用于攻击，则会给整个人类社会带来负面影响，我们完全不能想象。各国都不能忽略人工智能的重大挑战，必须要加强网络安全，因为一旦这些问题真正爆发，将会带来巨大的损失。

弗雷德里克 · 吉隆

Forrester 副总裁兼高级研究总监

弗雷德里克：要权衡 AI 解决方案的风险

6 月 5 日，弗雷斯特市场咨询（Forrester）副总裁兼高级研究总监弗雷德里克 · 吉隆在 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会战略峰会上发表主题演讲。雷德里克强调平衡 AI 的丰厚回报与严峻风险。“我们每天都在权衡，希望解决方案能够提供价值，而不是带来风险。对新技术来说，希望能够权衡技术的风险和收益，能够更好地去应用新科技，同时要对风险保持敏感。”

弗雷德里克认为，生成式人工智能想要实现变革性的力量，离不开安全风险隐私的控制和管理。一方面，生成式人工智能是世界上最重要的技术之一，改变了一切。企业一定要顺应这个时代的潮流，积极应用生成式人工智能。另一方面，要确保生成式人工智能的安全性。建议利益相关方构建更加有建设性的解决方案，也就是用一种权衡的心态去构建解决方案。

弗雷德里克介绍，企业安全团队恰当地应用人工智能技术可以获得更多的益处，现在已经取得了很多激动人心的成就。但弗雷德里克也警告，如果使用不恰当，可能还会变成另外一种场景，如可能会出现新型的网络安全攻击。

因此，弗雷德里克建议，需要从安全角度考虑怎么去部署、使用生成式人工智能工具，防止这些工具给到错误的反馈。

李军华：
人工智能和机器学习的监管问题亟待解决

李军华
联合国副秘书长

联合国副秘书长 李军华在 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会（BCS2024）数字产业创新峰会上致辞时强调，尽管人工智能和机器学习越来越多的应用于威胁检测、响应自动化，以及预测分析，但所带来的监管问题现在还亟待解决。

在当前创新和数字化推动之下，各个行业和各个经济体都在发生深刻的变化和变革，但数字技术在带来巨大收益的同时，也引发了与网络安全和数据有关的新问题，网络威胁和缺陷也大幅增加。

为了充分实现数字化转型对可持续发展的效益，我们必须要增强数字信任和网络安全，要倡导合作、开放、多样性创新等重要原则。

2023 年，“联合国互联网治理论坛”在日本京都发布了相关的四项重要信息：一是网络威胁正在超越全球网络规范，需要抢占先机。二是在寻求制定网络安全规范的时候，应当认识到开放的安全相关标准的价值，并采取相关方法来设计解决方案。三是为制定恰当的网络安全政策，需要世界各国、各行业和各学科的利益相关方深入的参与其中。四是联合国及多边社会应当继续探索切实可行的解决方案，将网络安全能力建设纳入到更广泛的发展场景当中来。

顾瑾栩：
北京市未来将积极培育数字安全核心能力

顾瑾栩
北京市经济和信息化局副局长

6 月 6 日，北京市经济和信息化局副局长 顾瑾栩在 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会（BCS2024）数字产业创新峰会上致辞时表示，“北京市数字安全产业企业位居全国第一，未来将积极培育数字安全核心能力。”

顾瑾栩强调，北京作为首都，聚集大量政务、金融、能源、交通等行业的关键信息基础设施，大力发展数字安全产业，既是推动数字经济高质量发展的有力抓手，也是确保首都政治社会大局稳定的必然要求。

未来，北京市将以国际科技创新中心建设为牵引，加强核心技术创新突破，打造数字安全核心技术路径，提高安全防护能力，提升数字安全治理水平，完善数字安全治理体系。

一是积极培育数字安全核心能力。未来将充分利用好科技资源和创新能力优势，筑牢数字安全底层能力，提升整体行业安全防护水平。

二是持续建全数字安全体系。未来将积极落实国家出台的数字安全相关政策，保障人工智能大模型新技术成为发展新质生产力的强大引擎。

三持续完善数字安全产业生态。着力提升国家网络安全产业园承载能力，吸引更多龙头企业和创新能力强、发展潜力大的企业入驻。积极推进京津冀先进网络安全产业集群建设，促进创新链、教育链、产业链、人才链深度融合。

苗守野
中国联通集团网络与信息安全部总经理

苗守野：人工智能已成为影响网络安全的关键要素

中国联通集团网络与信息安全部总经理 苗守野出席 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会（BCS2024）数字产业创新峰会，并发表《中国联通人工智能赋能网络安全探索与实践》的主题演讲。苗守野表示，“人工智能已经成为影响网络安全的关键要素。人工智能技术对安全领域是一把双刃剑，既可以成为犯罪分子手中的新武器，又具有解决网络安全现成痛点问题的巨大潜力。”

苗守野介绍，有关机构的调查报告显示，人工智能已被用于辅助网络攻击，常见的包括 AI 驱动的网络钓鱼诈骗、恶意软件、APT 攻击、高级 DDoS 和深度伪造攻击；但同时，AI 也可以从防护、检测等方面，给传统网络技术带来显著的赋能效应。基于安全知识的持续智能学习，实现主动发现威胁，提升漏洞管理效能，对威胁做出更好的检测和响应。

中国联通聚焦建设“网络强国、数字中国”的主责和“拓展联网通信，算网数据”的主业，全面融入自动服务国家发展战略，统筹发展和安全，努力做好网络安全现代产业链链长的支撑者、引领者和组织者，积极响应并落实国家的“人工智能 +”行动，聚焦新一代移动通信、人工智能、智能网联、下一代互联网、6G 等重点领域，开展技术创新和联合攻关，特别是将 AI 创新纳入到重点发展行动计划，发布 AI 整体规划，成立 AI 创新中心，统筹推进 AI 创新应用的高质量发展。

罗小平
比亚迪集团基础架构与信息安全部部长

罗小平：新技术不断出现需要新安全思路

6 月 6 日，比亚迪集团基础架构与信息安全部部长 罗小平在 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会（BCS2024）数字产业创新峰会上发表《人工智能时代的数字安全创新与实践》的主题演讲。罗小平表示，“数据作为核心的生产要素，贯穿于数字化系统的各个生产环节。如果不把数据安全阀拧紧，不仅会影响企业经营，甚至关乎国家安全，数据泄露将给企业造成难以承受的后果。”

据罗小平介绍，比亚迪的数据安全建设，从保障内部业务角度出发，针对数据安全目标开展六大举措，同时参考 DSMM（数据安全能力成熟度模型），从管理、技术、运营三个维度，进行整体数据安全能力的建设。

罗小平认为，现在数据安全建设还处于起步期，建设过程中碰到了很多疑问和难点。结合目前行业新动态、新技术，罗小平做出四个判断：

一是在数据合规背景下，相应合规要求会持续升级，监管也会更加趋于严格。

二是对企业数据的各类攻击一定会进一步升级。

三是在数据要素化方面，需要统筹安全与发展。

四是新技术不断迭代和出现，需要新的安全思路。

罗小平强调，当前的计算环境由大数据变为 AI 大模型，新技术的出现既是机遇也是挑战。汽车行业需要充分利用新技术优势，如通过大模型进行数据安全合规运营的政策解读。

蒋楠
中石化集团信息和数字化管理部副总经理

蒋楠：AI 的安全问题要通过 AI 来解决

中石化集团信息和数字化管理部副总经理 蒋楠出席 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会（BCS2024）数字产业创新峰会，并发表《AI 时代网络安全的挑战与应对思考》的主题演讲。蒋楠强调，“AI带来的安全问题可以通过AI解决，用魔法打败魔法，而不仅仅用魔法对抗魔法。针对人工智能，需要从更高的角度来看待，不仅是带来的风险需要应对，还要考虑是否能用人工智能方法、更高效的手段，来解决安全方面的问题。”

蒋楠介绍，目前在人工智能方面面临三类挑战和风险，这也是人工智能的三大要素。

第一是算力。将会面临算力内外结合、边界模糊的挑战，要保障在边界模糊情况下的安全，云边协同的安全要跟得上。

第二是数据。数据分类分级确定可以把哪些数据用于人工智能的基本遵循。在流通、移动、训练、执行、模型、演进和推理的过程，以及数据流通都需要控制。数据标注过程一定要安全，不能出现干扰，同时也不能出现相关泄密的风险。

第三是算法。在算法层面，面临算法攻击、算法欺诈，以及算法不可解释的风险。

针对这些风险，蒋楠建议，要更加主动、更加积极地用人工智能，比如用人工智能更加智能地发现网络安全隐患，更加快速地进行自动化的响应，能够进行相关的修复加固，甚至数据出现泄露的提前预知。

吴云坤
奇安信集团总裁

吴云坤：AI 创新应基于体系在对抗威胁的闭环中寻找方向

6 月 6 日，奇安信集团总裁吴云坤在 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会（BCS2024）数字产业创新峰会上发表《AI 驱动安全体系和产业演进》的主题演讲。

吴云坤提出，网络安全领域基于 AI 的创新，须紧扣加速网络空间 OODA 循环闭环寻找方向，需要基于内生安全思想建设和运行安全体系，才能让单点技术通过体系在对抗威胁闭环中发挥最大效能。

当前以生成式 AI 为代表的 AI 技术在威胁发现、样本判定、安全运营和知识工程支撑攻防四个安全场景下，显著提升了能力、效率，降低了成本，解决了在安全防御方面的能力不足、效率低下和人力资源短缺问题。比如在知识工程支撑攻防实战方面，AI 可以将上千次的实网攻防演习、重保、威胁追踪等安全实战场景和经验积累、萃取形成知识沉淀，与大模型的学习、分析和推理能力充分结合，支撑网络攻防实战。

在网络空间攻防对抗的核心是攻防双方谁能更快速、更高效的建立 OODA（观察 – 判断 – 决策 – 行动）闭环的对抗博弈，网络安全基于 AI 的创新万变不离其宗。

吴云坤认为，网络安全领域没有银弹技术，AI 也不例外，需要基于内生安全思想建设和运行安全体系，才能让 AI 等单点技术通过体系在对抗威胁闭环中发挥最大效能，基于 AI 的创新必须基于体系，紧扣加速网络空间 OODA 循环闭环寻找方向。

AI 驱动安全

——奇安信集团董事长齐向东在 BCS 的主题演讲

尊敬的各位领导、各位院士、各位专家、来宾，媒体朋友们，大家好！

感谢大家参加全球数字经济大会数字安全高层论坛暨 2024 北京网络安全大会。当前，第四次工业革命快速发展，传统社会开始全面网络化、数字化、智能化，网络空间安全形势发生了翻天覆地的变化：散兵游勇式的黑客组织正逐渐退居其次，取而代之的是专业攻击组织和国家级网络力量，它们已经成为网络攻击的两大主力；一般性的网民，网站遭受到的攻击数量骤然下降，取而代之，政府、城市和大型企业的重要设施成为重要攻击目标。网络安全“一失万无”的现状更加突出。

从经济损失层面看，今年以来就爆发了多起重大网络攻击事件，一些事件造成的经济损失甚至高达数十亿元。比如，美国联合健康集团今年为勒索攻击付出的总成本已经达到 63 亿元，国际清洁用品巨头高乐氏因为网络攻击损失超 3.5 亿元。

从高水平攻防对抗层面看，今年 2 月奇安信威胁情报中心发布的 2023 年年度 APT 报告显示，全球至少有 80 个国家遭遇过 APT 攻击，这些攻击组织背后往往有国家力量直接参与，不达目的不罢休，被盯上的政企机构不是业务系统瘫痪，就是机密数据被窃取，有的甚至还会威胁到国家安全。

网络安全形势的变化，催促安全建设同步升级。网络安全防御体系建设的指标有 2 个：“漏报率”和“误报率”，“漏报率”为零，就有可能产生误报，我们以前听说过“宁可错杀一千，也不能漏掉一个”，对业务系统来说，误报错杀就等于影响业务运行。过去，网络攻击是小概率事件，被攻击后，后果也不严重，所以，绝大多数企业追求的是零误报，就是优先考虑的是不影响业务运行，付出的代价是放过大量的可疑告警。网络安全形势变化以后，安全建设指标要变成追求零漏报，但人力不足，无法对

海量的告警进行研判，只能放任不理，结果追求不漏，反倒成了高漏。我们统计了奇安信安服团队处理的 2959 次网络安全应急响应事件，所有被攻陷的企业，它们的安全设备都对潜在威胁发出了告警，但企业并未对这些告警进行研判和处理，造成了事实上的大量“漏报”。

安全人员数量和资源不足，是失陷的主要原因。我们曾经对万人规模以上的企业做过调查。86% 的企业，安全运营人员不到 10 人，研判比例不足 5%；13% 的企业，运营人员有 10~30 人，研判比例在 5%~10%；仅有 1% 的企业，配备了 30 人以上的安全运营团队，但研判告警比例也仅达到 10%。

这个表格点醒我们，人力不足导致大量告警被忽视，是网络安全当前面临的最大漏洞。部署好的安全设备，由于没有人力去处理，造成“漏报”频发。解决有限的安全资源和 100% 的安全追求之间的矛盾，要靠 AI 驱动安全，下面我和大家分享三部分。

第一部分：AI 是网络安全的必然趋势，它正带来指数级的能力跃升

攻击者突破安全防线有几个阶段，先突破单点设备、再突破防护体系，事成之后，还要想办法隐匿踪迹。AI 能给安全防护者带来十倍、百倍乃至千倍的效率跃升，把攻击扼杀在事发之前。

先说单点设备的检测，AI 可以对过去人工漏掉的告警进行全量研判，实现安全能力十倍级提升。

单点设备会为了追求零漏报而产生海量告警，但为了避免“错杀”影响业务，99% 都需要人工分析研判。然而，任何企业的安全专家都是有限的，他们全力以赴也只能研判少量告警，有超 90% 的告警被抛弃，其中隐藏的大量真实威胁被忽略，攻击者就会趁虚而入。

AI打破了人力资源和效率的边界，依托强大的算力资源和持续训练后的研判能力，极大提升了安全工程师的效率，能减少 90% 的漏报，实现安全能力的 10 倍提升。

再说体系化防御，通过 AI 赋能的综合分析和全局联动，实现安全能力百倍级提升。

在 AI 赋能下，单个安全设备减少了 90% 的漏报，但剩下 10% 的威胁会进入系统当中。此时，就需要体系化的防御。体系化防御的核心，是多种网络安全设备的有机结合。由于不同产品之间的数据共享、互访问、互操作非常频繁，漏报和误报问题在这一阶段又会呈现指数级增长。

AI 好比一个智能体，像人一样在工作，不仅可以知道在什么场景下、去调哪个接口、取什么数据，还能根据实际变化进行动态调整，瞬时激发各个设备的安全能力，将遗漏的威胁从 10% 降低到千分之一，达到安全能力百倍级提升的目标。

最后是溯源和反制。从威胁发现到攻击溯源环节，依托 AI 的智能化、自动化，可实现响应能力的千倍级提升。

单设备的检测，叠加体系化的防御，大部分漏报误报都会被解决，但仍无法保证万无一失，可能会有千分之一的几率漏掉单个威胁，从而让攻击者得逞。

AI 的逻辑推理、自我决策能力，可以帮助我们实现安全体系中不同产品的互操作，实现事件溯源和处置的高度智能化和自动化，处理时间可能从过去的一天，缩短到分钟级甚至秒级，实现响应能力千倍提升。

由此可见，AI 在不同安全场景中释放的能量难以估量。AI 驱动安全已经成为大势所趋，未来网络攻防就是得 AI 者得天下。讲到这里，可能有人会问，既然 AI 这么好，是不是我赶紧装上一个 AI 大模型就可以了？答案并非如此，这就是我接下来要讲的。

第二部分：做好 AI 驱动安全的三大必要条件

第一个条件，高质量的数据，是高水平 AI 的基础。高质量的数据有两个特点，一是全，二是新。这样的安全数据是稀缺资源，只有拥有最多人才、承担最多国家关基设施防护任务、处理最多安全应急事件的企业，才能积累下又全又新的数据。

先说全，指的是要有足够多的基础安全数据，用于训练安全大模型。安全设备覆盖越广，得到的数据量越大、越丰富。IDC 等权威机构公布的数据显示，奇安信在终端安全、威胁发现与态势感知、数据安全、云安全、安全管理平台等领域，都稳居市场第一。特别是终端安全市场，连续六年领跑。安全数据规模位居全国首位，

为大模型预训练打下了坚实的基础。目前，我们自主研发的数据存储平台，汇聚了总量超过 380 亿的全球独有样本库、超百亿的恶意网址库、国内最大的互联网漏洞库、2 万亿级的 DNS 日解析量、200 多亿条资产数据等。

再说新，指的是要有足够贴近实战的一手原始语料用于大模型推理。只有丰富的实战经验，才能磨练出专业的原始语料。奇安信有遍布全国的网络安全服务团队，人数规模超过 3000 人，能深入了解客户遇到的安全问题；我们还开通了全国首个行业服务热线 95015，为各地客户解决紧急的安全事件，能第一时间获取威胁信息；我们还举行了近 900 场攻防演习活动，完成了 80 多场国内外重大活动网络安全保障任务，在实战过程中积累了丰富的、先进的安全知识和经验。这既是训练高水平安全大模型的核心要素，也可作为大模型推理时所需的、最新的、实时信息，双管齐下确保生成精准的、高价值的答案。

我给大家看一个有趣的例子，用同样一个恶意域名，去提问最新的 ChatGPT 和我们自己的大模型，看看结果对比。左边是 GPT 的答案，它只是泛泛提供了一些建议。右边是我们自己的大模型，回答的非常专业和有价值，不仅准确判断出这个域名是恶意域名，还给出了专业的判断依据，提炼出核心知识点。包括哪些家族的恶意软件与该域名的通信记录、该域名的注册信息是否有可疑等关键细节，基本匹敌一个安全专家的分析报告。

可见，经过专业知识优化的大模型在实际应用中具有显著优势，其精确性和实用性远超未优化的通用大模型。

奇安信集团董事长齐向东

第二个条件，体系化的网络安全建设，是 AI 发挥效率的平台。从俄乌战场上可以看出，现代战争的核心，是多系统之间的协同联动，从雷达感知情报，送回指挥部，再送到海陆空前线部队，迅速启动火力系统，锁定并打击目标，这是一个整体作战体系，更是高效运转的闭环。

“天下武功，唯快不破”，放到网络空间也是如此。2019 年，奇安信提出的内生安全体系，可以把网络安全设备和业务流转、不同层次的信息系统有机结合起来，感知、响应对业务系统和数据的任何破坏行为。AI 赋能内生安全体系，不仅可以和客户业务完美融合，更能实现网络安全响应从滞后到实时的大跃升，全时段瞬时响应成为可能。

第三个条件，统一的标准，为 AI 驱动安全实现体系化落地扫除障碍。训练好的安全大模型，能否取得好效果取决于设备和体系是否有统一的标准。当前，不同厂商、不同设备读不懂彼此的数据，有时候仿佛鸡同鸭讲，实现标准统一迫在眉睫。

首先是统一数据输入标准，让 AI 读懂“多国语言”，完成体系化分析。

AI 好比一个诊断专家，我们在给医生描述病症的过程中，信息量越大、症状越详细，医生的诊断越精确。目前，许多政企机构的网络安全建设靠 “拼凑”，部署的安全产品是大杂烩，产品、技术、运营标准都不一致，信息量参差不齐，杂乱的数据给 AI，很难进行体系化分析，并得出正确结论。

构建一套统一的数据语料标准至关重要。只有为 AI 提供颗粒度足够细，信息量足够充分，遵循统一标准的数

据，才能让 AI 看得懂，用得好。这就像是给 AI 提供了一个标准化的语言交流环境，面对威胁能够迅速做出反应，保护我们的数据和系统不受损害。日积月累，还会量变引起质变，实现 AI 能力的自成长。

其次是统一指令输出标准，让 AI 实现跨设备、跨系统的能力协同和全局联动。

AI 驱动安全，关键在于“驱动”，这要靠统一的操作指令标准来实现。我们要制定通用的操作指令集，确保所有体系内的网络安全设备都能理解和执行这些指令。指令要具体到每一台设备、每一个功能、每一项操作，明确到操作对象和动作要求，精细到有效调动起某个安全设备的某个功能，这样，AI 驱动安全才能真正实现闭环。

统一度量衡，功在当代，利在千秋。进入 AI 驱动安全的新纪元，全行业要在这一领域找到最大公约数，在数据输入、指令输出两大关键环节实现“车同轨、书同文”。

第三部分：AI 驱动安全 奇安信在行动

认识到 AI 的变革作用并不难，难的是用好 AI、让 AI 真正赋能安全。在“AI 驱动安全”这条路上，我们率先进行了大量探索实践。

下面，我从四个方面，分享我们在客户侧落地的真实故事。

一是 AI 驱动研判，大幅提升了威胁发现效率。以我们今年 3 月正式发售的 AI 战略产品 QAX-GPT 安全机器人为例，它的研判效率相当于人工的数十倍，在大型客户侧广泛落地。

有一家员工规模超万人的大型企业，单日告警量超过 10 万，运营人员只有 12 人，一个团队一天只能研判 6000 条告警，漏报率极高。用上安全机器人以后，他们可以对 10 万告警全量研判，漏报率为 0.05%，揪出了人工漏掉的 700 多条真实告警，极大地提升了集团的整体安全能力。

二是 AI 驱动体系，多设备快速联动实现安全运营能力循环上升，威胁遏制实现秒级、溯源分析实现分钟级。我们有一家金融客户，数字化跑得很快，网络安全建设也相对成熟，但在事件处置方面远跟不上实际需求。攻击者经常把安全防线打穿。

通过部署机器人和 NGSOC 构成的“AI+ 安全运营”方案，奇安信帮助这家企业实现了威胁事件的自动化响应。通过 AI 与防火墙、WAF、SOAR 等安全产品的协同联动，对遏制安全威胁的处置时间从过去的 10 分钟缩短到秒级；对复杂事件的溯源分析缩短到分钟级。安全运营效率大幅提升。

三是 AI 驱动智能攻防，通过持续验证，推动安全能力在博弈中演进。“以攻促防”是提升安全能力的重要方式，我从攻击红队和防护蓝队两方面来说。

先说攻击红队。每年实战攻防演习前，都有很多客户希望使用奇安信的“加特林”打前战。这是款模拟攻击红队的产品，通过全自动化的渗透测试，帮助客户提高演习成绩。虽然效果不错，但创造性不足，遵循固定的流程，面对变化的安全环境和策略不能进行自我调整，无法和专业红队相比。

为弥补这一短板，我们把安全机器人和“加特林”结合，打造出业内独一无二的“智能红队”。“智能红队”让“模拟战”更有实战感，把“以攻促防”变得更便捷。

再说防护蓝队。有一家大型核电企业，希望安排机器人和人工团队比一比。演习期间，客户借助机器人进行防守，共发现 15 起安全事件，同时机器人发现了被专家遗漏的两个高危的安全事件。在真实风险事件研判准确率上，机器人达到 100%。

四是 AI 驱动全场景升维，网络安全的最大效能被激发。

在 AI+ 安全开发方面，基于大模型的代码助手极大提高了开发人员的效率，不仅实现了代码的高效编写，还能自动检测并修复潜在的安全漏洞。

在 AI+ 终端安全方面，奇安信天擎、反病毒、沙箱等产品深度融合安全大模型的分析能力，无论是二进制文件还是非 PE 脚本类代码，都能快速分析并识别。

除此之外，我们还将 AI 全方位应用在漏洞挖掘、电子取证、操作流程自动化等众多产品和业务流程方面，大大提高了产品威胁发现、研判、处置水平，升级整体安全防御能力。

网络空间是看不见硝烟的战场。当攻击者纷纷通过 AI 实现攻击武器的“升维”时，网络安全的战场将由“冷兵器”时代直接进入“核武器”时代。未来，如果不依托 AI，安全也将不复存在。让我们用“AI 驱动安全”，向着无限的安全追求，不断前进！

谢谢大家！

奇安信
新一代网络安全领军者

打造新一代中国特色的安全托管服务

时刻守护您的网络安全

奇安信安全托管服务以威胁发现为基础、以分析处置为核心、以发现隐患为关键、以解决客户问题为目标，7*24小时全天候全方位守护客户网络安全。

两种模式
模式随心选择
- 直营服务模式：奇安信产品+MSS
- 合作服务模式：技术、产品、服务整体托管

多种形态
全面助力建成
- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

两化融合
帮您真正实现
- 集中服务化：统一监测、预警与通报
- 服务集中化：标准统一、质量可控、资源共享

首创“云地结合”模式
打破传统的托管仅限“云端监测”的认知开辟“云地结合”模式，云端+地端实现真正的闭环服务。

7*24h实时持续监测
“地球不爆炸，我们不放假”——7*24h持续监测，充分保障常态化运营。

安全事件响应快一步
对APT攻击、网络攻击等长效监测，提前预警，响应快一步。

安全事件处置规范化
事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加固。

专家“一对一”指导
专家通过视频一对一的方式与您“面对面”沟通指导，不仅让您了解现状，还能防患于未然。

奇安信

新一代网络安全领军者

聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证
态势感知解决方案市场领导者——IDC认证
态势感知技术创新力和市场执行力双第一——数世咨询认证

2024GDEC 数字安全高层论坛暨第四届中国数据要素 50 人论坛召开

2024 年 6 月 5 日，2024 全球数字经济大会数字安全高层论坛暨第四届中国数据要素 50 人论坛在北京国家会议中心召开。本次论坛的主题为“释放数据要素价值 助力新质生产力发展”，来自联合国科学和技术促进发展委员会、北京市通信管理局、中国法学会、欧洲科学院、美国信息产业机构 (USITO)、中国行为法学会、奇安信集团等机构的国内外数据要素领域知名专家学者和企业家参加了本届论坛，围绕数据产权、交易流通、收益分配、安全治理，以及数据要素市场的发展和安全等话题进行了观点碰撞和思想激荡。

联合国科学和技术促进发展委员会副主席 Peter Major

联合国科学和技术促进发展委员会副主席 Peter Major 在致辞中对中数据的定义进行了阐释，他表示，“与原材料和劳动力等传统生产投入不同，数据不是自然产生的，而是由复杂的技术体系和社交互动产生的。生成数据时，个人和组织的选择会受其目标、价值观和偏见及更广泛的社会因素的影响，因此数据本身并不是客观的。”为此，联合国行政首长理事会 2023 年 8 月发布了《国际数据治理——进步之路》，为数据治理构建一个负责任的全球框架而持续努力。

苏少林

北京市通信管理局党组书记、局长

“万物互联，数据互通，作为国民经济战略性、基础性、先导性行业，信息通信业正成为数字经济发展的主力军。”北京市通信管理局党组书记、局长 苏少林谈到，信息通信行业积极推动赋能数据要素治理，并在三个方面发力，一是健全数据流通高速路，构建坚实的数据基础设施；二是当好数据产业服务部，支持数据要素市场，

“中国数据要素 50 人论坛”发起仪式

培育激发产业链各环节潜能，以价值链引领产业链、创新链，推动产业高质量发展；三是织密数据生态安全网，筑牢网络和数据安全屏障，坚持“一盘棋”思路，注重强根基、抓重点、谋全局扎实推进数据要素治理保障价值和能力建设。

中国数据要素 50 人论坛长期以来旨在研究数据要素市场发展规律，以高水平安全促进数据要素高水平应用，推动数据要素协同优化、复用增效、融合创新，充分释放数据要素价值，助力新质生产力发展，在论坛上，中国科学院深圳先进技术研究院、国际数据协会研究部（IDA—Reseach）、联合国世界丝路论坛数字经济研究院、中国行为法学会网络与数据法学研究部、中国政法大学数据法治研究院、浙江大学国际战略与法律研究院、华东政法大学中国法治战略研究院、南京理工大学知识产权学院、深圳大学创新发展法治研究院、奇安信集团、中国电信集团数据发展中心、华为技术有限公司全球政务一网通军团、深圳数据交易所、人民数据管理有限公司、灾备技术国家工程研究中心、西部数字经济研究院等作为首批发起单位，共同参与“中国数据要素 50 人论坛”发起仪式。

江必新

中国法学会副会长、第十三届全国人大宪法和法律委员会副主任、最高人民法院原副院长

“数据要素是数字经济的核心组成部分，数据要素市场是发展数字经济的重要依托，数据要素市场为新质生产力赋能。法治是最好的营商环境也是最有力的保障，数据要素市场的发达壮大离不开法治保障。”中国法学会副会长、第十三届全国人大宪法和法律委员会副主任、最高人民法院原副院长 江必新表示，“构建法治保障的基本框架，可以归纳为八化，分别是特性化、实用化、类型化、制度化、体系化、产品化、协同化、效能化，从而从法治层面为数据要素赋能新质生产力保驾护航。”

陈俊龙

欧洲科学院外籍院士、欧洲科学与艺术学院院士

“当前人工智能的蓬勃发展得益于算力、算法与数据三大要素的共同推动，而近期大模型的兴起为数据利用提供了新视角。”欧洲科学院外籍院士、欧洲科学与艺术学院院士 陈俊龙表示，“大模型的出现让数据变得更有价值，在数据更有价值的交易里，必须要考虑隐私和安全的问题。”目前，隐私计算包括四种不同加密方法，包括同态加密、差分加密、联邦学习、安全多方计算。陈俊龙认为，通过技术创新，如“联邦学习 + 宽度学习”的结合使用，可以有效应对这些挑战，为数据的高效、安全利用开辟新路径，进一步护航数字经济的健康发展。

“人工智能需要在发展创新和保护隐私、尊严等取得平衡，它的不确

Christopher Millward

美国信息产业机构(USITO)总裁

定性、非决定性和非预测性输出是管理挑战。”美国信息产业机构(USITO)总裁 Christopher Millward 带来了《人工智能时代的数据治理》的主题演讲。他表示，“全球都在探索人工智能时代的数据治理，如中国推出的AIGC监管文件，以及美国在技术与隐私保护上的法规、欧盟推出的《人工智能法案》等。”当前普遍存在的问题是，过度聚焦风险而忽视了机遇，尤其是数据最小化策略可能无意中限制了人工智能的效能和创新潜力，导致结果偏见与不公。Christopher Millward强调，创新潜力需要进一步发展而不是被限制，不能因为担心人工智能的风险而耽误可能进一步创新的机会。

董学耕

海南省大数据管理局局长

海南省大数据管理局局长 董学耕在演讲中分享了海南省在数据要素价值化方面的探索与实践，并强调了法治体系的梳理与数据产品化的实现路径。他指出，“首先，数据价值释放的前提是建立清晰的法治体系，海南的做法是探索数据特性化，认识到数据与其他要素的最大区别，其次是建立数据要素基础制度体系，包括“一条例，两办法”等；第三是数据价值化和数据入表的探索，将数据资源逐步实现可控制、可收益、可计量；最后是数据基础设施的重要性，主要分为原数据基础设施、公共化基础设施和数据价值化基础设施三层，以确保数据的安全可信和价值分配。”

何伟

中国信息通信研究院副总工程师

“发展新质生产力，最重要的是生产要素创新性配置，核心是推动以数据为代表的先进生产要素向发展新质生产力方向去流动。”中国信息通信研究院副总工程师 何伟表示，“数据要素有三次价值提升的过程：第一次是在数据产生和管理的环节；第二次在数据应用环节，主要体现在主体自身对数据初步的汇聚和利用；第三次是交易流通过程中，通过对外赋能释放更大价值。”何伟对加速数据要素价值释放提了六点建议：一是进一步完善数据的保障机制；二是进一步提高数据质量；三是让数据要素充分赋能行业与应用；四是建立公平高效机制；五是构建产业生态；六是构建安全可信数据基础设施。

中国社会科学院信息化研究中心主任、中国社会科学院数量经济与技术经济所研究员 姜奇平在《打造适合数据要素的生态市场机制》演讲中表

姜奇平

中国社会科学院信息化研究中心主任、中国社会科学院数量经济与技术经济所研究员

示，“数据要素市场化不仅仅是建交易所，它将演进为‘市’和‘场’两种形式，其中‘市’是交易，而‘场’是交换。‘市’和‘场’之间有三个差别，分别是原子性和关系性的区别、确权和非确权的区别，以及市场类别的区别。”为此，姜奇平提出了生态市场的概念，通过场内交易和场外交易的结合，将无法在市场内部进行经济化的资源，进行价值充分解放，实现1+1>2的效果，并最终实现对实体经济的真正赋能。

张恒山

中共中央党校（国家行政学院）一级教授、中国行为法学会副会长兼学术委员会主任

中共中央党校一级教授、中国行为法学会副会长兼学术委员会主任 张恒山就“数据权利”中的“权利”内涵进行了诠释。他认为，“首先‘数据权利’这一概念并不代表某项单一的权利，而是在由众多的具体权利组合而成的‘权利集群’；其次，在讨论‘权利集群’的时候，必须聚焦以数据为对象的活动中的哪些行为，而

非数据本身；第三，需要以利益超脱的第三方身份对上述行为加以评判、辨识；第四，需要明确规定出正当性行为和权利性行为。”在这个过程中，需要准确的区别把握针对数据的行为与针对行为数据权利这两个概念，进行数据立法或者构建数据制度。

王春晖

国际数据协会（IDA）主席、中国科协决策咨询首席专家、中国数据要素 50 人论坛主席

国际数据协会 (IDA) 主席、中国科协决策咨询首席专家、中国数据要素 50 人论坛主席 王春晖教授表示，“要把数据资源变成要素，需要重构数据生产力的三要素，首先是人，即一大批的数字技术应用人才；其次是算力算法为主的劳动资料，特别是引入生产过程劳动化、数字化和智能化水平的应用；第三是构建数据要素的底层逻辑，完善产权制度，做好数据确权。”王春晖认为，构建良好数据要素市场生态体系，最重要的是要发挥法治固根本、稳预期、利长远的重要作用，数据产权制度体系的基础上，统筹推进数据的流通交易、收益分配、安全治理相互协同和有机统一的数据要素大市场，更好地协调和处理与数据生产力发展相适应的数据化生产关系，助力我国新质生产力的快速发展。

“数据要素需要更多的融合，需要数据与数据之间发生化学反应才能够形成更多的社会化价值。”中国电信集团数据发展中心副主任 张鑫在《构建数据基础设施，服务数据要素市场》的主题演讲表示，“首先，数据要素市场化是中国在改变一种社会治理，或者是信息化投资的一种模式和分配制度；其次，数据基础设施未来是中心化和去中心化相结合，企业需要做好自己的数据中台，在统一的未来区块链隐私计算的标准下才能做好数据流通；最后是在全球化趋势下，做好数据跨境的流动和政策，在世界整个经济主战场上获得更多话语权。”

张鑫

中国电信集团数据发展中心副主任

刘前伟

奇安信集团副总裁、首席数据安全科学家

“人工智能和数据要素就好比发动机和燃料，是推动我们数字经济发展的黄金组合。”奇安信集团副总裁、首席数据安全科学家 刘前伟谈到，“人工智能在数据要素时代，也带来了多个问题。首先，人工智能降低了攻击门槛，没有编程经验也可以借助人工智能进行漏洞挖掘，生成攻击代码；其次人工智能增加了数据泄露的通道，加剧了数据非法获取、数据泄漏及恶意滥用等风险；最后人工智能放大了

数据要素乘数效应，扩大了数据要素暴露面，数据要素流通风险激增。”针对这些挑战，刘前伟建议，一是企业需要构建纵深防御的内生安全体系；二是通过 AI 赋能数据安全，包括赋能数据安全态势感知、赋能 API 安全、赋能数据分类分级等；三是依托数据可用不可见的隐私计算技术，构建数据要素流通的整体保障。

和前几届论坛一样，本次论坛设置了圆桌对话环节，中国数据要素 50 人论坛发起人兼主席 王春晖教授作为圆桌对话主持人，邀请世界知识产权组织技术与创新支持中心主任，江苏国际知识产权学院院长 戚湧，联合国世界丝路论坛数字经济研究院研究员，深圳竹云科技股份有限公司董事长 董宁，中国科学院深圳先进技术研究院研究员、中国科学院大学博士生导师 曲强，南京领行科技股份有限公司 (T3 出行) 首席执行官 崔大勇，北京邮电大学网络空间安全学院教授、灾备技术国家工程中心常务副主任 辛阳，深圳大学创新发展法治研究院院长，深圳大学校学术委员会副主任 叶卫平，华为技术有限公司全球政务一网通军团研发副总裁 赵猛，人民数据管理有限公司董事长 郑光魁等专家，就“释放数据要素价值 助力新质生产力发展”主题进行了观点碰撞和交流。

全球数字经济大会自 2021 年起至今，成功举办三届，已经成为构建普惠均衡、创新包容、合作共赢、共同繁荣的全球数字经济格局下的国际化、高端化、专业化的交流合作平台。作为全球数字经济大会的专题论坛，中国数据要素 50 人论坛由联合国科学和技术促进发展委员会和全球数字经济大会组委会指导，每年举行一次主论坛和若干平行论坛。该论坛致力于打造数据要素市场创新与发展的学术、产业和国际交流平台，深度分析国际、国内的数据要素市场、人工智能演进、数据治理的政策、法律和规则。安

圆桌对话

第六届智慧能源网络安全论坛在京举行

2024 年 6 月 5 日，2024 北京网络安全大会（BCS2024）期间，第六届智慧能源网络安全论坛在北京国家会议中心举行。论坛由中国能源研究会、中国电机工程学会主办，中国能源研究会网络安全和信息化工作委员会和中国电机工程学会电力信息化专委会协办，奇安信集团承办。中国能源研究会特邀副理事长 陈进行，中国电机工程学会会士、电力信息化专委会副主任委员、国家电网有限公司副总信息师 王继业，全国政协委员、全国工商联副主席、北京网络安全大会主席、奇安信集团董事长 齐向东，国家能源局电力安全监管司原司长 苑舜和来自国家电网、中核集团、中国石油集团、国家能源集团、中国海油集团、中国华能集团、国家电投集团、中国电建等能源行业单位代表共二百余人参加论坛。论坛由中国电机工程学会会士、电力信息化专委会副主任委员刘建明主持。

刘建明

中国电机工程学会会士、中国电机工程学会电力信息化专委会副主任委员

陈进行在致辞中表示，智慧能源推动行业智能化、高效化和可持续发展，网络安全问题随之而来，给智慧能源的发展带来了严峻的挑战。

陈进行

中国能源研究会特邀副理事长

王继业在致辞中详细介绍了电力系统的安全挑战：电力网络的边界更加模糊，终端数量更加扩大，数据由单向变成双向交互，安全防护的难度也进一步增大。

王继业

中国电机工程学会电力信息化专委会副主任委员、国家电网公司副总信息师

齐向东在致辞中提到，我国关基行业面临专业组织和国家级力量两大主力的攻击，给网络防护提出了新课题。要破解能源行业难题之道，除了在原有的安全技术上进行创新外，需要大力推进 AI+ 安全，他建议从建设纵深防御安全体系、做好 AI 的赋能、开展联合创新三个方面推进AI+安全。

齐向东

全国政协委员、全国工商联副主席、奇安信集团董事长

论坛主题演讲环节，中国科学院院士 管晓宏作题为《网络空间安全挑战与应对》的报告。报告指出，新形势下，网络空间安全包括网络安全、信息安全、内容安全、信用安全、CPS综合安全和数据安全六个方面。网络安全管控芯片与系统是网络与智能时代万物互联场景下，解决零信任网络安全互联的新基础路径，为保障信息物理融合系统、物联网、工业智能系统、智能终端的网络安全、信息安全、数据安全提供技术支撑。

管晓宏

（线上）

中国科学院院士

原国家能源局电力安全监管司司长 苑舜 在题为《能源行业网络安全风险》的报告中介绍了我国能源行业发生的主要安全事件。2023年建成的能源行业态势感知系统显示，我国能源系统一天遭受的网络攻击高达1000万次。来自能源企业的安全专家证实，我国能源企业的工业控制系统每天都面临着不断渗透和网络攻击，曾在生产环境的大型工业化控制系统（PLC）发现隐蔽的数据传输通道。

苑舜

原国家能源局电力安全监管司司长

中国电机工程学会电力信息化专委会副主任委员、中核集团科技质量与信息化部主任 尹卫平在题为《数字技术助力核电安全与高质量发展》的报告分享了中国核工业集团公司数字化转型的过程。他表示，中核集团在网络安全方面打造了四保一体系一能力，把网络安全贯穿于数字核工业推进全过程，筑牢安全屏障。

尹卫平

中核集团科技质量与信息化部主任

中国石油网络安全中心高级专家 王静媛作题为《构建数智中国石油网络安全防御体系 迎接新质生产力安全挑战助力品牌价值提升》的报告。报告提到，面对快速数智化、智能物联协同发展、AI快速应用，中石油在考虑重建网络安全防护能力，为此提出了数智安全、数字安全、信息安全、网络安全的安全工作新目标。中石油对于AI在安全工作中的落地和探索，主要在三个方面发力：一是在组织重构的过程中，打造安全数字员工；二是在软件开发的阶段，用AI方式来保证软件开发的质量；三是以AI协同方式，构建整个网络安全运营的能力。

王静媛

中国石油网络安全中心高级专家

国家电网有限公司信息通信分公司总工程师 彭元龙在题为《新形势下网络安全防护体系的完善和提升》的报告中介绍了国网公司提升网络安全防御体系探索和实践。报告提出，AI技术的发展为网络安全防护带来新的机遇，助力网络安全工作迈向智能体的时代。国网公司重点建设了挂图作战，智能安全检测，网络攻击治理、网络安全机器人研究、漏洞自动化检测、防护有效性验证等六类基于AI的典型防御能力。

彭元龙

国家电网公司信息通信分公司总工程师

国家能源集团数据中心副主任 朱志成在题为《国家能源集团网络安全防护实践经验分享》的报告中分享了国能的网络安全思路，即以网络安全管理、技术、运营、人才四大体系为核心，实现网络安全技术全面化、智能化，网络安全运营“一幅图”“一盘棋”，提供全方位的网络安全保障。

奇安信集团副总裁 韩永刚作题为《面向业务的智慧能源网络安全构想》的报告，他表示，现在人工智能还没

朱志成

国家能源集团数据中心副主任

达到把现有安全团队抛弃掉的能力，它更多提供一种辅助的作用。人工智能作为一个装备，最终还要和安全专家结合，打通从检测到发现、再到处置的行动闭环。能源机构可以用内生安全系统工程的方法，面向全局安全能力进行设计，构建网络安全的目标架构；再通过规划建设运行的方式，持续做架构管控，最终通过工程化去落地和建设，进行网络安全能力的建设和生成，并以集约化的安全运营，面向业务保障平稳运行，完成动态综合的网络安全体系的运转。

韩永刚

奇安信集团副总裁

本届论坛围绕“数字能源·安全引领，智慧驱动变革”主题，分享了能源行业数字化转型背景下，电力、石油、核能等能源领域面临的安全挑战，网络安全空间态势变化下的行业影响，以及人工智能如何赋能网络安全防护。与会专家认为，当前在数字化深化、网络空间态势日趋紧张的背景下，能源行业正面临空前的安全挑战，亟需积极拥抱 AI 等新技术，并从业务视角重新思考网络安全，提升全行业的安全防护能力，为智慧能源提供有力的安全保障。安

BCS 第五届金融业网络安全论坛成功举办

——洞察智能化趋势，筑牢金融安全基石

6 月 5 日，2024 年北京网络安全大会第五届金融业网络安全论坛在京成功举办。本届论坛以“洞察智能化趋势，筑牢金融安全基石”为主题，针对金融行业数字化转型面临的安全挑战，尤其是大模型为代表的新型人工智能技术对金融业务带来的机遇、风险以及应对进行了深入探讨。

与会专家表示，金融行业正面临数字化转型的关键时期，这一过程不仅使得网络安全风险变得更加复杂和多变，同时也伴随着法律法规和监管要求的日趋严格。在人工智能技术带来的新机遇和挑战面前，金融行业需要采取双管齐下的策略：一方面，要积极接纳和利用创新技术，充分发挥 AI 的潜能；另一方面，也要对大模型发展可能引发的无边界和穿透式风险保持警觉，平衡发展与安全。

奇安信集团银行军团总经理 徐懿巍 主持论坛

在致辞环节，奇安信集团董事长齐向东表示，“金融行业最近几年面临重大的网络安全挑战，黑客组织为获取经济利益和用户隐私把金融行业作为攻击的重点。”从 2023 年开始，全球很多大型金融机构遭遇勒索攻击，造成巨大损失。因为金融行业不仅掌握重要数据，其业务连续性也非常重要，丢失数据和停止运行对于金融行业都是灾难性的。

齐向东

奇安信集团董事长

信创海河实验室主任、中国新一代人工智能发展战略研究院执行院长龚克在致辞时表示，“推动 AI 和网络安全与金融结合，一定要深度理解 AI

的优势和可能带来的风险。”在优势方面，人工智能凭借其强大的数据处理能力，能够迅速且主动地利用历史数据进行风险预判、行为分析，并做出及时响应。这种能力在金融领域尤其宝贵，能够极大提升风险管理的效率和准确性。但 AI 目前存在着可靠性不足、技术成熟度有待提高，以及可能引发安全隐患和隐私泄露的问题。特别是在金融行业，人工智能带来的隐私问题可能更为严峻，需要我们给予足够的重视并审慎的应对。

龚克

信创海河实验室主任、中国新一代人工智能发展战略研究院执行院长

中国科学院院士 管晓宏在主题演讲《网络空间安全挑战与应对》中表示，网络空间安全包括网络安全、信息安全、内容安全、系统安全、CPS 综合安全和数据安全六个方面。保证网络空间安全应该采取技术与管理相结合的策略。从管理角度，要建立法律法规和国家政策作为安全治理体系的重要一环，强化数据安全监管，构成数据安全的标准体系。从技术角度，数据的全生命周期安全，也就是数据生产、存储、传输、访问、使用、销毁，都应有相应技术手段提供安全保证。

中国工商银行数据中心金融科技专家 顾骏在《金融行业数字化转型背景下的网络安全建设实践》主题演讲中，分享了工商银行应对安全挑战的实践。为应对数字化转型过程中的安全挑战，工商银行对标业界信息安全体系化管理的最佳实践，从管理、运营、技术三个层面建设网络安全的管理框架，并持续优化，为全行高质量发展提供有力的支撑。

管晓宏

（视频形式参会）

中国科学院院士

在大模型技术研究中，工商银行深入分析应用层、模型层、框架层，识别出 15 类安全风险。顾骏指出，大模型虽基于 AI 技术，却同样面临模型窃取、数据投毒等传统风险，同时，其特有的应用模式如提示词等，也带来了新的安全挑战。

顾骏

中国工商银行数据中心金融科技专家

清华大学五道口金融学院金融安全研究中心主任、中国互联网协会金融消费权益保护与教育培训专业委员会主任委员 周道许，精准勾勒了金融智能化的五大发展趋势：质效提升、基础设施完善、人机交互革新、监管科技深化、风险管理能力增强。面对 AI 技术的快速迭代，他指出，“金融智能化发展中伴随着新问题和风险，并提出了针对性的发展建议：利用科技赋能监管，强化消费者权益保护，推动金融机构以客户为中心，提升服务竞争力，并完善立法监督，确保金融智能化的健康发展。”

周道许

清华大学五道口金融学院金融安全研究中心主任

中国邮政储蓄银行数据管理部副总经理 张放在演讲时表示，“随着数字经济的快速迭代和发展，安全问题已经不仅仅是底线和红线的问题，而成为了制约科技能力和业务发展的关键因素。如果安全能力无法突破其‘天花板’，那么科技能力和业务发展都难以跑出加速度。”邮储银行近年来非常重视数据安全工作，搭建了较为完善的数据安全体系，并有条不紊地开展了一系列数据安全工作，如数据分类分级、研发安全工具链建设、数据安全评估等。在未来，邮储银行将落实“做好金融五篇大文章”的号召，借力大模型等新技术，积极面对金融数字化带来的安全挑战，与业内共同铸就数据安全生态。

张放

中国邮政储蓄银行数据管理部副总经理

中央财经大学金融学院院长 张学勇在主题演讲时表示，“金融业正经历全面的数字化转型，数据成为核心

资产，风险管理与决策更加科学化和智能化。然而，数据安全成为金融发展的关键，需在确保安全的同时，有效利用数据资产以提高收益。”张院长指出，源于对金融机构业务发展中安全重要性的深刻认知，中央财经大学金融学院在学科建设中融入了金融安全工程。学院致力于培养掌握金融安全关键知识和技能的人才，以满足金融机构和社会发展的需求。此外，中央财经大学金融学院与奇安信集团紧密合作，建立金融数据安全联合实验室，整合优质资源，期待在未来能成为中国培养金融数据安全人才的阵地，并计划定期发布金融数据安全研究报告，助力行业发展。

张学勇

中央财经大学金融学院院长

中国移动集团信息技术中心架构师 赵永刚发表主题为《人工智能技术在信息安全领域的研究与探索》的演讲，分享了中国移动信息技术中心在大模型领域应用过程中发现的安全问题及应对之道。赵永刚表示，“在 AI 构建大模型应用之时，面临数据侵权、隐私泄露和数据合成伪造的风险，通过在应用、数据和访问三大层面构建核心安全体系，能够有效降低安全风险，提升应用大模型的安全信任感。”赵永刚还提出了三个层面的主要技术手段：在应用侧，研究合成检测，保证应用安全；在数据侧，通过数据水印和一系列数据防护措施，构建数据防护体系；在接入访问侧，通过 5G 专网解决网络安全问题，构建完整的安全访问方案。

赵永刚

中国移动集团信息技术中心架构师

中国联通集团数据安全专家 孙艺发表了主题为《筑牢数据安全防线，护航数字经济发展》的演讲，分享了中国联通在整个数据安全治理体系方面的思考和实践。中国联通始终围绕数据治理、安全防护、常态运营和产业赋能四个方面开展工作，同时还搭建了管理 + 技术 + 组织的数据治理体系，该体系的运用不仅持续强化中国联通在数据安全防护方面的能力，而且通过提高风险发现和处理的效率，有效预防了数据泄露风险，为中国联通在数字经济时代的稳健发展提供了坚实的安全保障。

孙艺

中国联通集团数据安全专家

奇安信集团产品总体部副总经理王月辉发表了题为《重新定义安全服务价值》的主题演讲。他表示：“当前安全厂商提供的安全服务，多数情况下灵活性都很强，安全服务的立项、采购和实施三个阶段都存在着很多不确定性。”王月辉强调，安全服务的未来发展方向应以客户需求为核心驱动力，通过推动供给侧的改革与创新，将安全服务提升为一种标准化、精细化、个性化的工艺品。这种服务模式不仅能够精准对接市场和客户的特定需求，还有助于提高安全行业的服务质量与效率。通过该模式，网络安全服务有望迈入一个全新的发展阶段，实现质的飞跃。

王月辉

奇安信集团产品总体部副总经理

奇安信集团战略咨询规划部总经理 邬怡、奇安信集团人工智能研究院负责人王占一做了《从 RSA2024 看 AI 安全趋势》的主题对话。

邬怡认为，人工智能（AI）安全与网络安全在本质上是相通的，治理架构的建立应当先行一步。AI 治理架构与数据安全治理架构有着诸多相似之处，都需要构建一个跨职能的组织，涵盖隐私保护、法律事务、合规性、安全保障及信息技术等多个领域，以实现协同共建。在构建大型 AI 模型的安全框架方面，邬怡提出了四点建议：首先，短期内可以通过评估系统安全性来确保大模型的安全性；其次，建立临时控制措施，对大模型的使用进行有效管控；再次 · ，加强对公司内部 AI 应用的监控，确保其合规性；最后，定期审查并更新现有的安全策略，

以适应不断变化的技术环境和安全需求。

王占一从专业的角度深入剖析了大型 AI 模型的训练与部署应用流程。在训练阶段，对数据进行隐私化处理是至关重要的，包括对数据内容进行安全分析和过滤。针对中间私有数据的处理，王占一强调了两个关键点：首先，要确保数据内容与当前用户的权限相匹配，保障数据访问的合理性；其次，当数据被用于生成回答时，必须对内容进行安全性和合法性的评估，确保其不仅符合法律法规的要求，而且还要与公司的价值观和准则相一致。通过这种机制，在确保 AI 模型提供智能服务的同时，也能够维护用户隐私和数据安全。

圆桌对话环节参与嘉宾

在论坛的圆桌对话环节，来自金融科技领域的多位专家就“金融科技安全：新时代的创新与挑战”这一主题展开了深入的探讨。平安银行金融科技部总经理助理 宋歌、厦门国际银行科技运维部金融科技专家 林建庭、北京航空航天大学计算机学院教授 荣文戈、曙光信息产业股份有限公司金融行业首席架构师 姜永凯，以及奇安信集团副总裁 张卓，分别从不同的角度出发，就大模型人工智能在金融服务领域所带来的深远影响和变革、对人才培养的深远影响，以及人工智能如何赋能网络安全运行等话题，分享了各自的见解和洞见。这次圆桌对话为金融科技安全领域的创新与发展提供了宝贵的思想交流和经验分享。

奇安信集团战略咨询规划部总经理邬怡（左）
奇安信集团人工智能研究院负责人王占一（右）

金融业网络安全论坛作为大会期间举办的重要品牌活动，至今年已经成功举办五届，成为 BCS2024 北京网络安全大会最具影响力的行业论坛之一。安

BCS2024 保险数字安全论坛举行

6 月 5 日，2024 北京网络安全大会“第二届保险数字安全论坛”在国家会议中心举行。论坛由中国太平洋财产保险股份有限公司、奇安信集团主办，厚锋科技（上海）有限公司协办，以“建设数字保险安全生态的挑战与机遇”为主题，邀请了来自科研院所、产业机构的领导嘉宾，共同探讨网络安全保险市场所面临的挑战和机遇，为网络安全保险产业发展建言献策。

李超

中国太平洋财产保险股份有限公司副总经理

保险数字安全生态的建设离不开所有人的共同努力。中国太平洋财产保险股份有限公司副总经理 李超在致辞中表示，“数字保险安全生态的建设，为行业带来新的发展机遇，通过加强数据安全和网络安全，可以为客户提供更加安全可靠的保险服务，增强客户的信任感和满意度，同时通过隐私计算、人工智能等安全的先进技术手段，更好地分析和利用数据，对客户提供更加精准和个性化的保险产品，提高服务效率和质量。”希望通过此次论坛，搭建交流合作平台，汇聚各方智慧，共同推动网络安全生态的建设。

李强

国家工业信息安全发展研究中心信息政策所所长

国家工业信息安全发展研究中心信息政策所所长 李强分析了国内外网络安全保险的发展现状。他指出，“大数据、人工智能、区块链、量子计算等新技术的应用，带来新的网络攻击风险的同时，也能给网络安全保险提供新的技术支撑。”未来，网络安全保险产业发展需要各方共同推动生态构建，建议：一是进一步完善法律法规和标准体系，二是强化网络安全产品的服务创新；三是进一步强化网络安全保险供需对接；四是发展网络安全保险生态。

王建勇

中国人民财产保险股份有限公司科技保险中心副总经理

安全基础设施是风险缓解、防御、防护的主要措施，而网络安全保险是风险转移的最佳选择之一。中国人民财产保险股份有限公司科技保险中心副总经理 王建勇表示，两者的结合将形成企业网络安全高效且有效的防护机制。基于此，人保财险梳理国内保险市场现存网安产品 50 余款，调研客户网络安全风险保障需求，开发制定人保财险网络安全保险产品体系，通过技术合作、风险控制、销售推动等多种形式，在网络安全保险领域积极探索和实践。

谢静

中国人寿财产保险股份有限公司责任意外保险部 / 健康保险部总经理

关于数字生态保险保障体系的构想，中国人寿财产保险股份有限公司责任意外保险部 / 健康保险部总经理谢静提出，“在探索‘保险 + 科技’的融合过程中，需做好‘两手抓’：一方面应更加聚焦产业、聚焦群体，剖析行业风险及痛点；另一方面也要重视与基层政府组织的合作，来做好网络安全保险风险减量。”

中国财产再保险有限责任公司（以下简称“中再产险”）创新业务部资深承保师 谢飞回顾了 2023 年以来的

谢飞

中国财产再保险有限责任公司创新业务部资深承保师

国内外一系列网络安全重大事件，并对比分析了国内外网络安全保险市场的发展差异。针对业界高度关注的工信部试点项目进展及累积风险控制问题，谢飞详细阐述了由中再产险牵头的两个试点方案的具体情况，同时介绍了中再产险当前正在打造的网络安全保险平台和累计风险控制策略。当下，中再产险正积极与各生态合作伙伴共同推动网络安全保险产品和模式的研发与落地，促进我国网络安全水平的提升，服务国家网络强国战略。

吕超

阳光数科人工智能研究院院长

大模型技术快速演进，为保险业带来发展新机遇。阳光数科人工智能研究院院长 吕超分享了大模型技术在保险行业的营销、产品定价、客户服务、数字风控、产业融合等方面的实践成果，以及实践过程中的思考。

王金波

嘉福（北京）保险公估公司中国区总经理

作为外资保险企业代表，嘉福（北京）保险公估公司中国区总经理 王金波分享了网安险理赔全球管理思路，并结合理赔案例分享了网安险项下经营损失的特点和网络安全事故的损失类型和特点。

孟鑫

奇安信集团网络安全保险研究专家

奇安信作为网络安全领军企业，早在 2017 年就战略布局网络安全保险这一新兴领域，先后推出了“零事故”保障险，和针对中小企业防勒索难题的奇安天合安全融合机。本次论坛上，奇安信集团网络安全保险研究专家 孟鑫向与会嘉宾介绍了即将上市的奇安天保网络安全保险服务平台。

圆桌环节，由中厚投资（海南）有限公司董事长兼总经理、苏黎世保险中国原总经理 于璐巍担任主持人，邀请慕尼黑再保险公司大中华区总经理 常青、中意财产保险有限公司总经理 袁颖晖、厚锋科技创始合伙人 曾广旺、华泰财产保险科技保险负责人 陈星、奇安信集团保险行业总经理 邹贵军，从网络安全保险市场、政策及监管环境、市场端客户需求、供给端挑战与机遇等方面进行了深入探讨。

与会嘉宾们普遍认同，尽管当前中国网络安全保险市场尚属发展的萌芽阶段，同时还面临着诸多挑战，但同时也必须清醒地认识到，该市场蕴含着巨大的发展机遇。随着国家对网络安全问题重视程度的日益提升，相关政策法规不断完善，为市场的健康发展提供了有力保障。同时，随着企业数字化转型步伐的加快，网络安全风险也日趋复杂多变，这为网络安全保险市场提供了更为广阔的发展空间和市场需求。

为了充分把握这一市场机遇，与会嘉宾们强调了构建网络安全保险生态的重要性。他们一致认为，应从客户需求、产品供给和技术创新等多个维度出发，全面提升市场服务能力，以更好地满足客户的网络安全风险管理需求。

专家们相信，在政府、企业和社会各方的协同努力下，中国网络安全保险市场必将实现健康、快速的发展，为提升国家网络安全保障能力作出积极贡献。安

BCS2024
互联网创新发展论坛在京召开
——共话互联网安全的革新与实践

6月5日，由中国互联网协会指导、奇安信集团主办的BCS2024互联网创新发展论坛在北京国家会议中心举办。

论坛以“智启安全，赋能未来”为主题，邀请众多知名互联网企业、研究机构、安全专家等业界代表出席，就网络安全技术创新与应用的最新成果与经验进行分享，共同探讨互联网行业新质生产力的实践路径与发展方向。

中国互联网协会副理事长兼常务副秘书长 陈家春在致辞中强调，“今年是我国全功能接入国际互联网30周年，我国互联网事业已经取得历史性成就，探索走出了一条中国特色的互联网发展道路。”如今，在阔步迈向网络强国的过程中，要特别提升安全防护水平，加

陈家春

中国互联网协会副理事长兼常务副秘书长

快提升关键基础设施和大型网络平台的安全防护能力，深入开展数据分类分级保护、重要数据全生命周期的安全管理，加快车联网、人工智能等新兴领域安全建设，持续强化网民权益保护，营造安全有序的网络环境。

曲晓东

奇安信集团首席战略官

对于我国在信息化、数字化、智能化领域的跨越式发展，奇安信集团首席战略官 曲晓东在致辞中表示这得益于互联网的活跃创新和广泛应用。然而，互联网也一直是网络安全攻防的最前沿，正是互联网的发展和普及，让网络安全问题成为经济社会发展最重要的安全挑战之一。奇安信希望能够形成技术创新合力，聚集网络安全

和互联网行业的技术创新资源，共同开展原创性、前沿性和颠覆性技术创新。同时，将网络安全与互联网业务场景相结合，开展面向互联网的安全研究和安全解决方案的研发，并且致力于加快输出既懂安全又懂互联网技术及业务的复合型人才。

Dustin

京东集团基础安全负责人

京东集团基础安全负责人 Dustin 从漏洞、反入侵角度分享了海量资产下的供给面管理方法论。Dustin 介绍，“在整个京东安全防御体系中，基础安全是以漏洞为核心的反入侵，这里的漏洞分为通用漏洞、配置漏送、意识漏洞。为在海量资产且人力有限的情况下去应对这三个挑战，京东利用的是攻击面管理的方式，将漏洞验证的技术融合在攻击面的发现、评估、验证过程中。”未来，京东将从掌握更全的资产及资产标签、更快的漏洞情报及风险评估入手，同时利用大模型应用提升资产标签、资产匹配、漏洞分析等方面的能力。

陈长林

百度研发安全负责人

百度研发安全负责人 陈长林分享了百度智能代码助手 Baidu Comate 的安全实践。生成式 AI 正在为软件研发领域带来前所未有的机遇，大模型的理解、生成、逻辑、记忆能力同软件研发领域相结合，不仅大幅提升代码的开发质量和效率，而且让研发安全转化为切实的交付结果。围绕“AI+ 需求”“AI+ 编码”“AI+ 测试发布”的三大关键流程，陈长林还分享了 Baidu Comate 基于文心大模型，在企业内部推进“安全左移”的实践经验。Comate 不仅能够帮助工程师进行研发提效，还能够帮助工程师发现并快速解决安全问题，让业务代码更加安全。同时通过安全增强模式、数据脱敏保护机制，让 Comate 产品本身更加安全可靠，让用户用的更放心。

仲震宇

蚂蚁集团资深安全算法专家

蚂蚁集团资深安全算法专家 仲震宇在《DKCF 大模型应用可信框架》演讲中介绍了集团安全在大模型应用可信方向的建设工作。作为应用可信框架的组成部分，DKCF 指的是数据、知识、协作、反馈。D 是指充分的数据供给，它决定问题可解的上限；K 是指专业的知识工程，行业数据集需要跟专业知识图谱对接；C 是指协同规划和编排，人力专家及 AI 专家的决策将融合演进到整个大模型的应用中；F 是指高效核验及反馈，目的是让我们推理白盒化、决策可验证，保证知识的高效迭代，最终实现认知可信、决策可信和协同可信。仲震宇强调，以上建设工作是在集团 NbSP 和 OVTP 的安全范式指引下进行的，确保安全底盘，谨防大模型成为新的高危的安全突破问题。

白帆

亚马逊云科技大中华区安全与合规服务总监

亚马逊云科技大中华区安全与合规服务总监 白帆在《用长期主义，做生成式 AI 时代的安全》分享中表示：“不会有一个通用大模型适合所有的业务场景，Amazon Bedrock 服务是一个生成式 AI 的服务，提供众多业界领先的大模型，开发者可以直接调用，也可以构建属于自己的生成式 AI 应用程序。”白帆指出，生成式 AI 真正的差异体现在客户私域数据的应用上，亚马逊云科技做了很多工作确保私域数据的隐私性、安全性。“安全是我们的最高优先级，”白帆说，“亚马逊云科技在做生成式 AI 服务的过程中，始终坚持长期主义，不断对产品进行更新迭代，致力于构建更智能、更安全的生成式 AI 基础性工具。”

张阳

阿里云计算有限公司高级产品专家

阿里云计算有限公司高级产品专

家 张阳结合多年实践提出，云环境中任何的网络攻击都会留下痕迹，阿里云以流量为核心进行应对。为了解决阿里云飞天企业版内东西向、南北向的流量安全风险问题，论坛上，阿里云携手奇安信天眼，隆重发布了“云内全流量威胁监测与分析方案”。这一方案，旨在解决云内网络威胁看不见、看不清的痛点，确保云内威胁无所遁形。此次合作是继阿里云推出云平台网络流量可视化产品“银河安全网关”之后，首次与网络安全企业强强联手。张阳表示，未来阿里云将继续拓展与主流安全合作伙伴、网络合作伙伴的协同合作，共同提高客户业务在云平台中的安全保障水平。

谢兆国

知名互联网公司 AD 安全负责人、《域渗透攻防指南》作者

知名互联网公司 AD 安全负责人、《域渗透攻防指南》作者 谢兆国（谢公子）向与会者分享了 Active Directory（AD）安全建设相关知识。由于 AD 应用广泛、功能齐全，因此 AD 也成为网络攻击的首选目标，据微软统计，每天有超过 9500 万的 AD 账户遭到网络攻击。AD 目前面临着包括凭据窃取、横向渗透、服务配置错误、账号权限滥用、勒索软件等威胁。谢公子提出，需要从漏洞层面、配置层面、管理层面、风控层面构建 AD 安全纵深防御体系予以应对，即在多个层次部署防御策略，有效抵御内外部的威胁，确保组织的线性和业务的连续性。

丁健琮

黑灰产打击专家

论坛特邀黑灰产打击专家 丁健琮揭露了新型虚假流量黑产的手法及入罪路径。互联网企业对用户增长 / 流量投放领域的持续资金投入，吸引了大量黑灰产从事虚假拉新活动，这种虚假流量黑灰产不仅给企业造成了直接的经济损失，由此衍生出来的链条还滋生了其他违法犯罪行为。丁健琮认为，治理虚假流量大概分三步走：第一步，虚假流量情报互通，广告主和广告平台之间搭建黑产情报的互通机制；第二步，通过商业合作的合同约定推动整个行业反作弊技术的升级换代；第三步，通过国家行政和立法层面对流量采买、流量来源平台进行规范化操作。

安永（中国）网络安全与隐私保护咨询高级经理 左超在《生成式 AI 应用背后的数据合规风险与应对》演讲中，着重介绍了人工智能的风险治理建议。左超指出，企业的 AI 安全和合规关注重点在于数据安全、内容安全、内生安全，以及可解释性问题、伦理问题、版权问题等。数据安全方面，安永特别关注跨境数据的数据保密、数据防泄漏工作。

左超

安永（中国）网络安全与隐私保护咨询高级经理

鲍坤夫

奇安信云安全首席架构师

论坛的最后，奇安信云安全首席架构师 鲍坤夫提到，在近两年的 RSAC 创新沙盒十强中，云安全一直是受追捧的热点，RSAC2023 有六家产品和云安全相关，RSAC2024 有四家产品和云安全相关。未来云安全将出现集成、整合、平台化趋势，智能化、自动化趋势，业务融合和内容安全趋势。CNAPP 统一安全平台的功能在不断丰富，出现集成整合 DSPM、ASPM、SSPM 及大模型安全的态势。企业整体的安全运行效果在统一入口、策略、风险处理、告警处理之后会有很大的提升。安

2024BCS 信创安全论坛举办

——坚持安全创新，构筑信创基石

6 月 5 日，由中国电子科技委指导，中国电子科技委网络安全专委会和奇安信集团共同主办，自主可控网络安全技术创新中心和中关村网络安全与信息化产业联盟联合承办的 BCS 2024 信创安全论坛在北京国家会议中心举行。

论坛以“坚持安全创新，筑牢信创基石”为主题，吸引了政、产、学、研、用各方面的高度关注，政府领导、顶级专家学者、科研院所、行业组织、安全专家等代表齐聚一堂，共同探讨信创安全行业的前沿技术和发展趋势，分享信创安全的最新成果与成功经验，为信创安全行业发展建言献策，共同培育自主可控的网络安全领域原创技术策源地。

董旭

奇安信集团副总裁、产研与服务 PBG 总经理

奇安信集团副总裁、产研与服务 PBG 总经理 董旭在致辞中表示，“当前世界新质生产力已经成为驱动国家发展的核心动力，网络安全技术不仅本身是新质生产力的组成部分，同时也是维系其他新质生产力安全发展的重要纽带。奇安信集团致力于打造网络安全的核心科技力量，在底层技术、适配标准、产品布局、场景方案、生态融合等各个维度形成了对信创的全面兼容，并且已经在党政、金融、能源、运营商等重要行业开展了广泛的应用。”信息技术应用创新，核心技术是基础，安全是保障，生态是关键，希望通过与会专家意见交融和思想碰撞，为信创安全事业提供源源不断的新认知、新理念、新路径、新模式。

中国工程院院士 倪光南发表了《大力推动中国数据存储产业 掌握数字经济发展主动权》主题演讲。倪光南认为，“随着数据成为关键生产要素，作为数据载体的存储产业应当作为国家战略性、基础性、先导性产业给予大力

倪光南

中国工程院院士

支持，以促进新一轮的科技革命和产业变革。”倪光南院士建议均衡配置算力、存力和运力，推动以先进的固态硬盘 SSD 取代传统机械硬盘 HDD 的“存储革命”，推进制定标准，培养存储产业人才，成立存储国家实验室 / 国家级科创平台等，从而打造优越的体制机制环境及丰富的科技创新资源。

王超

工信部赛迪研究院安全所副所长

工信部赛迪研究院安全所副所长王超分析了当前信创安全的新形势和新挑战，总结了对未来信创安全建设的思考。王超副所长认为，第一，应加强面向互联网新应用的安全技术创新，并通过制定相关计划，推进行业信创安全建设的规模化发展。第二，充分利用人工智能、量子计算等技术，加快实施以智能辅助为核心的网络安全策略。第三，同步防范大模型等新技术、新应用的网络安全风险，做好面向新技术、新应用安全风险的应对预案。第四，围绕数据相关的关键业务场景、环节，做好数据安全的风险评估。

邹冬

中关村网络安全与信息化产业联盟秘书长

中关村网络安全与信息化产业联盟秘书长 邹冬，在论坛正式发布了由中关村网络安全与信息化产业联盟指导、奇安信牵头、自主可控网络安全技术创新中心相关单位编制的 4 项团体标准：T/ZISIA 01-2024《自主创新型网络安全技术 框架》、T/ZISIA 02-2024《自主创新型网络安全技术 安全可信启动设计要求》、T/ZISIA 03-2024《自主创新型网络安全技术 计算基础环境安全要求》、T/ZISIA 04-2024《自主创新型网络安全技术 可信计算技术要求》。邹冬秘书长向与会嘉宾具体介绍了 4 项标准的编制背景、主要内容、重点内容和应用价值，并表示下一步将推动标准的应用，用标准指导工程实践，用实践经验完善标准；继续制订标准，完善“自主创新型网络安全技术”标准体系。

任宇驰

奇安信安全能力中心高级专家

奇安信安全能力中心高级专家 任宇驰在报告中指出，奇安信正在跟国产化操作系统、硬件厂商合作，从而更好地发挥奇安信产品的安全保障效果。任宇驰重点介绍了基于指令流的未知威胁检测产品——奇安信“天狗”，“天狗”基于内存指令调用序列的检测技术，能够在内存指令层检测网络攻击行为，从而有效抵御 0day 漏洞攻击和 APT 攻击，具有极强的高级威胁检测效果。

奇安信与麒麟、统信、中科方德在论坛上举行了签约仪式，奇安信“天

奇安信“天狗”与麒麟、统信、中科方德操作系统签约仪式

狗”与麒麟、统信、中科方德的操作系统强强联合以后，国产化操作系统将深度集成“天狗”的基于指令流未知威胁检测能力，防护层级更深，比对精度更高，且能够还原内存中的更详尽的信息，从而为保障我国信创产业安全发挥更大作用。

李凤华

中国科学院信息工程研究所副总师、北京邮电大学灾备技术国家工程研究中心主任

中国科学院信息工程研究所副总师、北京邮电大学灾备技术国家工程研究中心主任 李凤华做了题为《数据要素流通安全》的专题报告。李凤华副总师讲到，“数据已经成为数字经济的核心生产要素之一，流通是数据要素价值释放的重要途径；当前，数据要素流通与安全保障技术滞后于应用需求，亟需面向数据多轮交易安全服务的体系化解决方案。”报告介绍了数据共享与数据流通的本质差异、数据要素准则，着重从数据要素流通的角度剖析了数据确权、延伸使用控制、低开销监测等概念及学术内涵，数据安全和隐私保护的新挑战及学术边界，并阐述了数据要素流通的关键技术与发展趋势。

中国电子产业规划部副主任 唐路在《数字化转型与网络安全三同步实践》主题演讲中，站在数字化建设与网络安全建设的角度，分享了中国电子在这两方面同步展开的经验成果。唐路副主任表示，“中国电子的数字

唐路

中国电子产业规划部副主任

CEC 建设是和网络安全同步实施、同步规划、同步推进，我们认为网络安全可以成为数字化转型的推手。”中国电子的网络安全建设规划，是以信创底座为基石，打造两大机制支撑、三大体系建设，形成一个一体化的安全运营中心，用以保障数字化业务安全运行。

赵甫

北京计算机技术及应用研究所技术总监

北京计算机技术及应用研究所技术总监 赵甫做专题报告《关键信息基础设施安全保护探索与实践》，提出在装备研制行业推动信创工程面临的任务和当前我国的能力现状；根据北京计算机技术及应用研究所所承担的某技术平台项目的攻关情况，介绍了在某关键信息基础设施行业开展信创工程的成果与经验。

周华涛

奇安信保密信创总体部总经理

奇安信保密信创总体部总经理 周华涛分享了《信创背景下软件开源风险防护的认识和思考》。周华涛总经理介绍说，“开源软件在当前软件开发的作用无可替代，软件供应链问题绕不开开源软件，因此保障开源软件的安全异常重要。”周华涛总经理提出，“我们应该建立纵深防御的安全体系，以体系化的防御措施为基础统筹应对之策，其中要重点守好三关：准入关、过程关、未知风险防范关。”

路轶

蓝信移动总经理

蓝信移动总经理 路轶做了《浅谈移动工作平台与工作秘密》的交流分享。当前，国家主管部门对工作秘密的管理出台了明确的管理规定。蓝信是为安全而生的移动工作平台，具备生产安全、底座安全、业务安全、部署安全、运维安全等全方面的安全保障能力，在长期服务党政军客户过程中积累了非常多的整体的安全能力，可以很好地支持实现主管部门对工作秘密的管理要求。

本次论坛广泛交流了信创安全的技术、产品和解决方案，发布了自主可控网络安全标准和“天狗”产品，举行了奇安信和麒麟、统信、中科方德的签约仪式，论坛嘉宾云集，会场座无虚席，得到了与会人员的积极支持和高度评价。安

BCS2024 举办“灯塔工厂数字安全论坛”

——聚焦灯塔工厂网络安全

2024 年 6 月 5 日 下 午，BCS2024 北京网络安全大会“灯塔工厂数字安全论坛”成功举行。论坛邀请了来自工信部、中国电子科技发展部、全国工商联、联想集团、京东方集团等嘉宾围绕智能工厂安全建设进行分享和探讨。

本次活动汇聚了企业领袖、行业专家和网络安全专业人士，共同分享灯塔工厂在网络安全领域的最佳实践经验，探讨未来发展趋势，推动制造业向更安全、更智能的未来发展。

陈华平

奇安信集团

奇安信集团副总裁陈华平担任活动主持人，在开场中他表示：“新一代信息技术与先进制造技术的深度融合，推动制造业生产模式和发展理念发生了重大而深刻的变革，成为第四次工业革命的核心驱动力。”灯塔工厂作为智能制造领域的标杆典范，引领着整个行业的发展方向。然而，随着数字化转型和智能化改造的推进，原来封闭的网络边界日益模糊，数据的流转突破固定的范围，灯塔工厂面临的网络安全问题日益凸显，一旦安全防线被突破，将可能导致数据泄露、生产中断、质量受损，甚至发生安全生产事故，给企业造成严重的经济和商誉损失。本场论坛以打造智慧工厂的网络安全灯塔为主题，共同分享灯塔工厂在网络安全领域的最佳实践经验，探讨未来发展趋势，推动制造业向更安全、更智能的未来发展。

吴晶

中国电子信息产业集团战略合作部

中国电子信息产业集团战略合作部副主任（主持工作）吴晶对大会的举办表示祝贺，并在致辞中表示：“制造业是国家经济命脉所系，是立国之本、强国之基。加强数字安全防护，确保数据的安全、可靠和完整，已经成为‘灯塔工厂’建设的重要基石。中国电子将牢记职责使命，与大家携

手并进，共同提升智能制造数字安全技术水平，提高制造业人才数字安全意识与素养，深化合作交流、应对数字安全挑战，合力培育和发展新质生产力，构建坚固的网络安全防护体系，打造制造业网络安全产业生态，为我国制造业高质量发展筑基赋能，为实现‘制造强国’战略目标作出新的、更大的贡献。”

乔松

联想集团

在当今全球日益严峻的网络安全形势及政府愈加严格的安全合规监管下，面临极大的数据安全挑战。如何在业务压力和外部安全压力环境下打造成本效益高、适用性广、可持续发展的灯塔工厂数据安全治理体系，联想集团高级副总裁 乔松在分享《灯塔工厂数据安全挑战及应对》中表示：“一个好的工厂的信息体系，一定是有一个特别坚强自身的防护体系，有一个非常完善的供应商合作的生态环境来支撑。”灯塔工厂拥有及其大量的数字化设备，生产制造数据超级离散，多角度协同，且协同复杂度非常大。联想在其科技工厂中不断探索，积极部署，构建了数据安全防护体系，包含技、监、运、管四大维度元素，覆盖数据全生命周期的 IT&OT 安全平台。

京东方集团信息安全中心总监 李楠在分享《数字化工厂网络安全运营实践分享》中，以自身实践为例，分享 BOE 数字化工厂安全如何建设运营，不同工厂应用场景下灵活的不同安全方案。他表示：“京东方从很早开始安全运营中心的建设，在 20 多条产线上，推广数字化可视的‘京东方标准’，也是三个统一：统一标准，统一建设，统一运营。达到统一后强化网络边界、分区域管理。”未来京东方将通过 SCMDB，生成式大模型等方面的研究，提升数字化工厂的安全。

李楠

京东方集团

工业领域关键信息基础设施是国家重要的战略资源，关系国家安全、国计民生和公共利益，具有基础性、支撑性、全局性作用，是国家网络安全工作中的重中之重。IT/OT 安全发展至今，智能工厂逐渐获得关注，并成为制造企业追求的目标。何为智能工厂？它应该是一个柔性系统，能够自行优化整个网络的表现，自行适应并实时或近实时学习新的环境条件，并自动运行整个生产流程。理想中的智能工厂可实现高速可靠运转，在最大程度上降低人工干预和成本。

库卡中国 IT 总监 郭予佳就《库卡智慧工厂》发表演讲。他表示：“库卡对工艺要求非常高，要求每一个数据都能够获取到系统上，跟系统匹配。”因此，必须追溯到每一台设备在工厂的整个生命过程。比起建设，更难的是运营。如何落地到本地数字化团队 / 工厂团队，需要有一个体系平台，将安全的结果更快速地反应，与管理部门联合，使整个过程持续可控。

郭予佳

库卡中国

新一代信息技术与先进制造技术的深度融合，推动制造业生产模式和发展理念发生了重大而深刻的变革，成为第四次工业革命的核心驱动力。灯塔工厂作为智能制造领域的标杆典范，引领着整个行业的发展方向，是推动制造业升级转型的关键力量。灯塔工厂通过数字化、网络化和智能化应用，显著提升了生产效率，降低了运营成本。

徐昕白

中兴通讯

中兴通讯网络安全产品线市场总监 徐昕白在演讲《5G 智慧工厂网络安全解决方案》中表示：“中兴通讯作为 5G+ 智能制造的积极践行者，在南京滨江基地率先提出了‘用 5G 制造 5G’的理念，将 5G 技术运用到 5G 设备的生产环节，基于‘5G 工业现场网 + 数字星云’的架构，实现产

线智能化和园区数字化。”同时，以5G全连接工厂业务发展和安全需求为导向，遵循网络安全等级保护2.0标准，围绕终端、网络、边缘云、业务数据建设端到端全方位5G全连接工厂安全防护体系，纳管24大类、70余种创新5G工业应用，并通过部署5G SIEM系统、5G终端安全卫士、超融合安全网关等安全产品，保障资产和数据安全，提高安全管理效率，实现5G全连接工厂安全工作协同化、可视化，为“5G制造5G”护航，建设可快速复制的5G全连接工厂安全解决方案。

人工智能为网络安全带来的机遇与挑战并存，赛迪顾问网络与数据安全研究中心副总经理 桑元就《智能制造时代下网络与数据安全发展趋势》带

桑元

赛迪顾问

来演讲。她表示：“工业大数据互联互通的特性，对于整个工业生产过程的智能监控、预测，以及提高都有优化和提升的作用，其提升了整个生产过程的效率和治疗。”此外，也为工业企业的决策提供了一个有力的支撑。

奇安信集团副总裁 韩永刚在演讲《面向智能制造的网络安全创新与实践》中分享：“在灯塔工厂，智能制造的基础和保障都运转在现在的数字化和智能化各种核心的技术上，这样

韩永刚

奇安信集团

一来使得原本小范围使用的核心技术，被更广泛得推到了需要生产控制与执行管理的众多一线员工设备上。”在这种情况下的安全问题不是局部损失，对于整个生产、和经济的生命线都会产生非常大的影响。

圆桌环节由北京赛博英杰科技有限公司创始人、董事长 谭晓生主持，联想集团高级副总裁、安管委主任 乔松、库卡中国IT总监松下信息系统（中国）有限公司网络空间安全部经理 徐静雯、浪潮云网络安全事业部总经理 李聪、奇安信集团工业互联网事业部总经理 李小军，分别从各自灯塔工厂（智能工厂）特色、创新、异同、挑战、解决方案及对智能生产与网络安全未来畅想几个角度展开深入探讨。

数字化转型和智能化改造的推进，原来封闭的网络边界日益模糊，数据的流转突破固定的范围，灯塔工厂面临的网络安全问题日益凸显，一旦安全防线被突破，将可能导致数据泄露、生产中断、质量受损，甚至发生安全生产事故，给企业造成严重的经济和商誉损失。为了应对这些新挑战，企业必须将网络安全视为智能制造战略的重要组成部分，通过构建坚固的网络安全防护体系，确保生产系统的稳定运行，免受网络威胁的侵害。安

BCS2024 中国首届国际关键信息基础设施网络安全论坛成功举办

6 月 5 日，中国首届国际关键信息基础设施网络安全论坛（CIICS 2024 ）在北京国家会议中心盛大开幕。本次论坛聚焦于数字时代下关键信息基础设施的网络安全挑战与对策。论坛汇聚了全球网络安全领域的领导者、技术专家及学者，共同探讨了交通、金融和电信等关键行业的网络安全问题。

随着数字化技术的飞速发展，关键信息基础设施的安全性问题日益凸显，APT 攻击、勒索软件、供应链安全漏洞，以及国家级网络间谍活动等新型威胁层出不穷。论坛特别强调了新兴领域，如人工智能和通信卫星系统的网络安全，呼吁全球共同努力，构建更加安全、高效的网络防护体系。

论坛旨在通过知识分享、政策研讨、技术创新和国际合作，推动网络安全领域的发展。会议强调了建立公私合作关系、培养网络安全人才，以及制定全球网络安全标准的重要性。与会者积极交流各自的见解和经验，共同为构建一个更加安全的网络世界贡献力量。

何瑞

奇安信集团副总裁、国际部负责人

作为论坛主持人，奇安信集团副总裁、国际部负责人何瑞，在论坛上强调了数字连接在现代社会中的基础性作用，并提出了关键信息基础设施面临的网络安全威胁，他特别提到了 AI 和低轨道通信卫星等新兴领域，呼吁全球共同努力，促进知识交流和政策发展，以建立一个更加安全和可信赖的网络环境。他倡导应加强国际合作，共同面对网络安全的挑战、推动数字经济的健康发展。

孙耀达

联想电讯盈科企业方案副行政总裁

联想电讯盈科企业方案副行政总裁孙耀达，在论坛上探论了如何保护关键基础设施免受数据泄露和系统故障的威胁，并分享了他曾经作为港铁公司 CIO 的经验。他强调了铁路系统中安全信号、通信和企业系统的重要性，并提出了网络分割、可见性和威胁情报等六大网络安全原则，以应对不断变化的网络安全挑战。孙博士的经验表明，通过实践这些原则，可以有效地提高关键基础设施的安全性和抵御网络攻击的能力。

Charles Lim

瑞士德国大学信息技术专业研究生副院长

瑞士德国大学信息技术专业研究生副院长 Charles Lim，在论坛上讨论了协作维护网络安全的重要性，并分享了印尼在建立公私合作关系方面的经验。他强调了信任建立、研究合作、人才培养和社区在网络安全中的作用，并提出了通过共享威胁情报和学术研究来提高公众对网络安全的认识。他的经验表明，通过跨部门合作和知识共享，可以更有效地应对网络安全挑战。

宫一鸣

XLab 创始人

XLab 创始人宫一鸣，在论坛中讨论了国家层面安全框架设计时，对数据收集和利用的策略，以及 DNS 数据在提供国家级别可见性和可扩展性方面的重要性。同时，他强调了数据和平台在基础设施安全框架中的作用，

通过实例说明了高价值数据对于即使是基本工具的性能提升至关重要。宫老师的观点是，通过合理收集和利用数据，可以构建更为有效的网络安全防御体系。

周万雷

澳门城市大学副校长、数据科学学院院长

澳门城市大学副校长、数据科学学院院长周万雷，在论坛上探讨了关键信息基础设施的攻击与防御，包括 DDoS 攻击、恶意软件和 APT 攻击。他分享了在这些领域的研究成果，并讨论了使用 AI 工具进行流量监控和异常检测的方法，以及如何通过游戏理论和机器学习来提高防御能力。周教授的见解为如何利用先进技术来增强网络安全提供了宝贵的思路。

Chris Miller

G4S Hill & Associates 大中华及北亚区咨询经理

G4S Hill & Associates 大中华及北亚区咨询经理 Chris Miller，从政策风险和地缘政治风险的角度分析了网络安全政策的发展。他讨论了政府监督与企业私人安全之间的平衡、数据的集中与分割，以及国际合作在标准设定、规则制定和联合执法中的潜在作用。他的发言强调了在全球化背景下，国际合作对于应对网络安全挑战的重要性。

黄迪奇

新世界集团科技风险主管

新世界集团科技风险主管黄迪奇，分享了如何利用 AI 构建下一代网络安全中心，以保护关键基础设施。他提出了网络安全人才短缺的问题，并给出使用 AI 进行数据分析、威胁检测和响应的策略。Dicky 强调，在组织内部建立正确的网络安全文化和治理结构的重要性。他的见解表达了技术创新在提升网络安全中的关键作用，以及人才培养在维护网络安全中的必要性。

在最后的圆桌对话环节，与会者一致认为，随着技术的不断进步，关键信息基础设施面临着日益复杂的网络安全挑战。专家们呼吁，加强国际合作，共享情报，制定统一的安全标准，并建立有效的应急响应机制。此外，该对话亦着重于人才培育的核心地位，并倡导在机构内部塑造和弘扬正确的网络安全理念。安

BCS2024 网络安全人才合作与发展论坛成功举办

鲁昕

中国职业技术教育学会会长、教育部原副部长

宋敏

中国职业技术教育学会副会长

2024 年 6 月 5 日下午，由中国职业技术教育学会和奇安信集团联合主办的 BCS2024 北京网络安全大会“网络安全人才合作与发展论坛”召开，中国职业技术教育学会会长、教育部原副部长鲁昕作题为《网络安全建设：现代职业教育使命担当》的主旨报告，并为网络空间安全产教融合实践示范基地揭牌。

鲁昕指出，产教融合、科教融汇的本质是生产要素的创新性配置，是知识、产业、技术、劳动等要素的创新性配置，要培养大批熟练掌握新质生产资料的新型劳动者队伍。领导强调，网络安全、信息安全、数字安全是发展新质生产力、服务推进新型工业化的数字基础设施和安全基座。职业院校要担当使命，着力培养高水平、实战型网络安全技术技能人才，适配国家安全人才新结构，服务构筑国家新安全格局。同时，职业院校要把网络安全作为基础必修课程。

论坛由学会副会长宋敏主持。学会副会长、全国工商联副主席、奇安信集团董事长齐向东致辞。中国工程院沈昌祥院士作专家报告。北京理工大学网络空间安全学院副院长嵩天，重庆电子科技职业大学校长聂强，广东技术师范大学校长戴青云，嘉兴职业技术学院网络空间安全学院院长陈双喜作网络安全人才培养案例分享。来自全国 170 多所职业院校、网安企业等 200 多名代表现场参会。

论坛现场观众认真听取专家汇报

沈昌祥

中国工程院院士

在专家报告中，中国工程院院士沈昌祥表示：网络空间安全一级学科建设，必须解决三大问题。一是创新理论基础，要解决图灵机计算原理的问题；二是解决体系结构问题，体系结构一定要完善起来；三是工程建设怎么搞，信息系统数据化、网络化是现代社会数字化的映射，计算环境一定要健康、可信。

论坛上，中国职业技术教育学会会长鲁昕与奇安信集团副总裁吴侃还共同为“网络空间安全产教融合实践示范基地”（简称“示范基地”）揭牌。北京理工大学、北京市信息管理学校、重庆电子科技职业大学、广东技术师范大学、国家开放大学、暨南大学、嘉兴职业技术学院、上海电子信息职业技术学院这 8 所院校，成为示范基地首批示范院校。

示范基地是由职教学会、全国网络空间安全行业产教融合共同体和奇安信集团共同发起的。据奇安信高校合作中心主任林雪纲介绍：示范基地专项计划，是在职教学会指导下，通过运营网络安全产教融合课程资源共享平台、人才供需对接服务平台，面向课程资源、双师队伍、人才供需对接、实验室共建及职教出海这五个目标，在共同体成员单位中协同发展，做出示范、树立样板。

中国职业技术教育学会会长鲁昕与奇安信集团副总裁吴侃共同为示范基地揭牌

网络空间安全产教融合实践示范基地 8 家首批示范校授牌仪式

林雪纲

奇安信高校合作中心主任

嵩天

北京理工大学网络空间安全学院副院长

本次论坛，邀请了部分院校的校长、院长做了主题报告。北京理工大学网络空间安全学院副院长嵩天指出：网络空间安全领域的竞争，归根到底是人才的竞争。要素不能够做有效配置，我们的人才培养就会出现问题。应当通过产教融合共同体，进行产教互助和产教深度融合。应当积极通过数字化平台建立全国范围内的网络安全实践智慧教育平台，通过产教互助的模式来深化产教融合。

重庆电子科技职业大学校长聂强认为：新质生产力一定会带来教育体系的变革、教育观念的变革、教育内容的变革和人才培养目标的变革。通

聂强

重庆电子科技职业大学校长

过培养高级数字技术人才，夯实“新质生产力”发展的人才根基，是非常重要的。要高度关注和重视专业群对接产业群，形成同频共振的格局。

戴青云

广东技术师范大学校长

广东技术师范大学校长戴青云指出，所有的老师、所有的学生都要实现“一个创新、两个转化”。一个创新就是说围绕国家战略、围绕国家中心和区域的重大发展战略，坚持科技自立自强，坚持原始创新。两个转化，一个是科技成果向外转化，要服务区域、服务产业、服务行业。一个是科技成果的向内转化，创新完成以后要转化成为教育教学的资源。但是向内转化，很多时候都被忽视了。

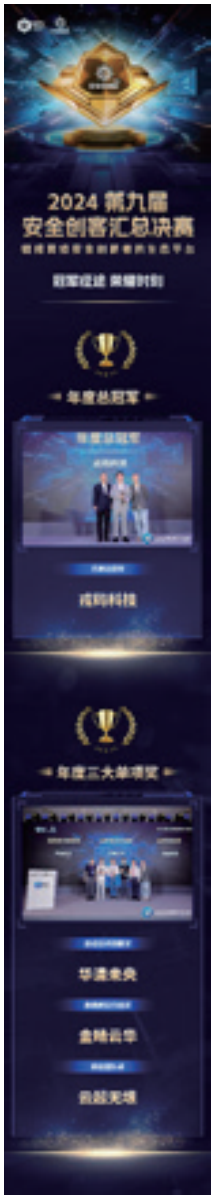
陈双喜

嘉兴职业技术学院互联网学院、网络空间安全学院院长

嘉兴职业技术学院互联网学院、网络空间安全学院院长陈双喜分享了嘉兴职业技术学院在网络安全实战化人才培养方面的特色：学校所有的教学都是围绕实战化开展的；一是结合实战化建设网络攻防的工具库；二是通过实战经验的沉淀建设网络安全的战例库；三是通过向相关单位输送专业人才就业，在正常教学师资库之外，建设一批实践教学师资库；通过前辈带后辈，形成实战化能力的不断传承。

在本次论坛的最后，由奇安信行业安全研究中心主任裴智勇主持，北京市信息管理学校信息技术系主任胡志齐，北京信息科技大学计算机学院副教授马利民，暨南大学网络空间安全系主任夏志华，沈阳格微软件有限责任公司董事长、沈阳北软信息职业技术学院院长张桂平，国开在线教育科技有限公司职业教育科创中心总监陈松，共同参与了圆桌对话。对话主题为：应用型人才培养的探索与实践。安

第九届安全创客汇冠军出炉 戎码科技获全国总冠军



6 月 6 日，由奇安信集团、北京网络安全大会（BCS）、中国网络空间新兴技术安全创新论坛、奇安投资、网络信息安全创业投资服务联盟（筹）联合主办的第九届安全创客汇决赛在国家会议中心落幕。经过激烈的角逐，戎码科技获得全国总冠军，并现场与奇安投资签订了 2000 万元投资意向书。华清未央获年度最佳技术创新奖，金睛云华获年度最具商业价值奖，云起无垠获年度最佳团队奖。

齐向东

全国政协委员、全国工商联副主席、奇安信集团董事长

“资本的支持对于网络安全初创企业而言，不仅是生存的血液，更是发展的加速器。”全国政协委员、全国工商联副主席、奇安信集团董事长 齐向东在致辞中表示，“网络安全作为一个技术密集型行业，高昂的研发成本和持续的技术更新需求，使得资金尤为重要。资本的注入不仅是对网络安全初创企业财务上的支持，更是对其发展战略、市场定位、技术创新等多方面能力的强化，是推动企业从概念走向成熟的关键力量。”安全创客汇始终致力于促成产业界与资本市场的互利共赢，希望在这个平台上，各方都能有所收获。

陈华平

安全创客汇评委会主任、奇安信集团副总裁

“创新创业是一场‘马拉松’，需要正确的方向、聪明的人、好的生态系统，以及恰到好处的资源。”总结盘点参赛企业特点及行业现状，安全创客汇评委会主任、奇安信集团副总裁 陈华平认为，我国网安产业进入了新起点。

他表示，从创新创业企业视角来看，我国 AI 安全创新创业紧跟国际趋势，在 2024 年迎来爆发式发展，今年创客汇十强企业半数主打 AI 安全，优秀创企纷纷加强 AI 赋能；从资本市场来看，中国投资基金的增加和国有资本的加速布局，凸显了网络安全的刚需属性；从产业生态来看，人工智能与大数据的结合，为网络安全行业带来了新的场景和机遇，预示着产业发展的新篇章正在开启。

作为国内首个聚焦网络安全领域的专业创投平台和信息安全行业技术创新风向标，安全创客汇已连续举办九届，通过搭建平台，将政府、产业园区、资本、大企业和创新企业深入连接，已挖掘和扶植了一批国内外优秀的安全创新企业。据统计，进入总决赛的企业在赛后获得的融资总额超过 55 亿元。越来越多的安全创新企业将安全创客汇视为寻求行业认可和获取资本助力的有效平台。安

BCS2024 京津冀数字化产业协作与网络安全创新论坛成功举办

戴键

京津冀企业家联盟秘书长、中关村社会组织联合会常务副会长兼秘书长

6 月 6 日，2024 北京网络安全大会京津冀数字化产业协作与网络安全创新论坛在国家会议中心举行。论坛由京津冀企业家联盟、中关村社会组织联合会主办，奇安信集团承办，北京市朝阳区企业联合会支持，聚焦“护航企业数字化转型，助力新质生产力发展”主题，汇聚京津冀政府部门、企业、社会组织代表 90 余名嘉宾，共话跨区域数字安全产业合作议题。本次论坛由京津冀企业家联盟秘书长、中关村社会组织联合会常务副会长兼秘书长 戴键主持。

李兆前

全国工商联原副主席、中国民营经济研究会会长

全国工商联原副主席、中国民营经济研究会会长 李兆前在致辞中表示，“京津冀地区在推进跨区域数字协作方面，有无可比拟的条件和优势。”京津冀地区在数字经济新时代打好新技术、发掘新动能，要做好三点：一是要打破区域分割和信息孤岛，强化跨区域数字协作；二是要进一步营造数字化产业协作发展的良好环境；三是要更加重视数字安全，构建一个安全、可靠、稳定、高效的网络环境，为数字化协同发展提供安全可靠的保障。

京津冀联合办规划政策组副组长、河北省协同办综合三处副处长（主持工作）刘静琨在致辞中表示，“作为全国一体化算力网络国家枢纽节点，京津冀数字化转型技术良好，目前正在努力发展数字经济生态，将为网络安全产业发展提供新的空间。”希望企业家联盟切实发挥平台机制作用，

刘静琨

京津冀联合办规划政策组副组长、河北省协同办综合三处副处长（主持工作）

围绕企业需求构筑连心桥，开展京津冀城市行等系列推介活动，提供政策解读，融资上市等专业化设计服务，积极开展协同创新和产业协作，依托成立三个重点产业链联盟，发挥产业链主带动作用，加快相关产业图谱成果转化推动三地重点产业强链补链，全力展现联盟企业风采。

齐向东

全国政协委员、全国工商联副主席、奇安信集团董事长

“数字化转型是一场深刻的变革，它要求我们不仅要追求效率和创新，更要确保安全和可靠。”全国政协委员、全国工商联副主席、奇安信集团董事长 齐向东在致辞中表示，“作为我国经济发展的重要引擎，京津冀地区要抓住新技术带来的新机遇，也要应对好新形势带来的新风险，统筹好发展和安全两篇大文章。”一是推动产学研跨区域融合，架起三地“政产学研用”的协同“立交桥”；二是以点带链、以链带面，以重点企业和产业链条发展为主线，强化产业链供应链安全水平；三是加快人才培养，促进科教融合、产教融合，为京津冀协同创新发展构建多元化、多层次的人才体系。

王建伟

中国电子信息行业联合会副会长、原工业和信息化部信息技术发展司副司长、一级巡视员

在主旨演讲环节，中国电子信息行业联合会副会长、原工业和信息化部信息技术发展司副司长、一级巡视员 王建伟认为，“工业互联网发展存在工控网络先天脆弱、新技术与工业系统深度融合导致安全问题加剧、工控系统漏洞数量居高不下、攻击呈现多样性等问题，需要通过完善政策保障体系、强化核心技术攻关、构建安全产品体系、加强重点标准供给、开展监测评估服务、深化重点场景应用手段，共同推动制造业数字化转型安全稳步发展。”

刘娟

赛迪顾问网络与数据安全研究中心总经理

赛迪顾问网络与数据安全研究中心总经理 刘娟认为，“京津冀企业的数字化转型过程中应该将网络安全作为重要事项同步推进，并充分考虑监管、业务、技术、运营要求。”具体来说，企业需要基于数字化转型丰富场景构建以业务为中心的安全建设、构建以数据流转为视角的数据全防护体系、通过平台进一步整合碎片化的安全产品、构建满足常态化和实战化的网络安全运营，并加深 AI 技术在网络安全领域的应用。

王胜彪

砹立方（北京）科技服务有限公司创始人、董事长

砹立方（北京）科技服务有限公司创始人、董事长 王胜彪总结了高效实现跨区域数字化产业协作的 8 个途径：强化顶层设计与规划、推进数字化基础设施建设、深化跨界合作与资源整合、推广数字技术及应用创新、培养数字化人才与团队、加强政策支持与标准制定、搭建数字化平台与生态、强化安全保障与风险管理。其中，“人”是跨界合作与资源整合的核心难点与痛点，如何培养懂产业、懂政策、懂投资、懂服务的“四懂新人”，是当前需要重点解决的问题之一。

尹智清

奇安信集团首席架构师

针对京津冀企业数字化转型协同发展的网络安全需求，奇安信集团首席架构师 尹智清从全球勒索攻击态势、勒索攻击案例出发，为与会嘉宾分享了企业防范勒索攻击的要点——体系化与常态化。他认为，要以底线思维

和极限思维体系化布局防勒索工作：做好架构管控、加强基础结构安全、构建贯穿端网云的大纵深防御，并通过实战化运行落实安全工作。

刘贵

北京市科委、中关村管委会重大专项处二级调研员

为进一步推动京津冀地区产业协同、统筹安全发展，推动大数据、网络安全等新兴领域技术转化为国防科技力量，北京市科委、中关村管委会重大专项处二级调研员 刘贵在会上详细介绍了中关村新兴领域专题赛赛事情况及政策支持，并重点强调专题赛的需求内容新、背景实等特点，号召京津冀地区企业积极参赛，借助专题赛平台寻找合作机会。

圆桌环节，北京易安睿龙科技有限公司 王睿，北京柏睿数据技术股份有限公司总经办主任兼市场总监 唐可可，北京鸥兔智能健康科技有限公司 CEO 马懿宏，围绕“跨区域数字协作与产业链安全构建”和“政策支持与企业可持续发展”两个话题，展开了深入交流。

最后，京津冀企业家联盟秘书处、中关村社会组织联合会副会长兼秘书长戴键作总结发言，他表示：“京津冀协同发展是政府企业社会组织等多方主体参与的共同事业，是一项系统工程，希望通过此次论坛，促进各方发挥优势、形成合力，推动京津冀协同发展走深走实，为京津冀地区打造成为世界级先进制造业集群贡献智慧和力量，共同推动京津冀协同发展，迈向更高的台阶！”安

智能网联新能源汽车安全论坛成功举办

——智驭未来，安行天下

6 月 6 日，由奇安信集团主办的智能网联新能源汽车安全论坛在北京网络安全大会（BCS）期间成功举办。来自国家智能网联汽车创新中心、赛迪研究院、德勤、上海大学、智能汽车创新发展平台、长安汽车、奇安信集团等机构的汽车行业专家、学者、政策制定者、企业领袖及技术创新者，共同探讨智能网联汽车信息安全防护、跨行业协同与法规政策等核心议题。

统计显示，2025 年全球网联汽车达到 7400 万辆，中国将超过 2800 万辆，汽车行业正在进入智能网联时代。随着汽车智能化、网联化的快速发展，车联网网络安全与数据安全的外部威胁加剧。与会专家认为，当前，数据安全、网络安全、自动驾驶系统可靠性、车辆与基础设施的协同安全性等问题日益凸显，成为制约行业健康发展的重要因素。特别是在全球范围内频发的数据泄露事件背景下，如何保障智能网联新能源汽车的信息安全，防止黑客攻击，保护用户隐私，成为业界亟待解决的关键问题。

智能网联新能源汽车安全论坛嘉宾

吕韬

论坛主持人 奇安信集团副总裁

全国政协委员、全国工商联副主席、奇安信集团董事长 齐向东在致辞时表示，“智能网联高速发展带来网络安全和数据安全的挑战。智能网联车安全事关人身安全，一定要注重网络安全，让消费者能够放心地使用新能源车。”此外，智能网联车靠数据驱动，数据安全也成了智能网联车的大问题。

齐向东

全国政协委员、全国工商联副主席、奇安信集团董事长

中国工程院院士、国家智能网联汽车创新中心首席科学家 李克强在演讲时介绍，国家相关部委发布的智能汽车发展顶层战略，现在已部署二十项重点任务，其中特别强调网络安全、信息安全、数据治理网络等。

李克强表示，未来智能网联汽车需要在智能化基础之上运行，需要联网运行，更需要信息安全管理体系提供保障，支撑满足条件的新架构车辆。针对智能网联汽车的安全挑战，李克强建议，建立覆盖车路云网图全要素的系统性安全防护体系，通过共性技术的安全系统为智能网联汽车方案提供全面支撑。所构建的智能网联汽车信息安全基础平台架构，包括基础资源层、基础平台层，支撑所需的安全系统层，这包括态势感知、安全监控、安全监管、安全诊断、资产管理、应急响应等，真正能够形成数据融合、共性技术、应用系统等相应关键能力，为行业提供有力保障服务。

中国工程院院士、国家智能网联汽车创新中心首席科学家李克强

赛迪研究院智能网联汽车研究测评事业部主任、工业和信息化部重点实验室副主任 邹博松总结了汽车网联化智能化后的信息安全挑战。他认为，构建基于国密的汽车网络安全分层的纵深防御体系是需要解决的话题。

邹博松强调，随着汽车智能网化的发展，软件逐渐成为重要的角色。软件占有量会增加直接到功能安全，特别是软件质量对功能安全的质量慢慢在凸显。

邹博松

赛迪研究院智能网联汽车研究测评事业部主任、工业和信息化部重点实验室副主任

德勤中国合伙人 张震分享了《中国车企在全球化面临的合规与安全的挑战》。他认为，合规类风险已成为中国车企高层至少是 Top3 的重大风险。中国车企走向全球化过程并非坦途，在全球化、多国家市场上面临的合规风险远远超过现在的单一市场。

张震

德勤中国合伙人

张震认为，中国车企在合规方面存在五个方面的问题：合规法律分散跟踪与管理；监管地区性差异问题；合规权责问题；合规监控问题；合规人才不足问题。在张震看来，中国车企的安全合规最大挑战在于权责的问题，即网络安全和数据安全合规，谁来牵头、责任边界如何去界定的问题。

张震建议，对中国车企各个业务单元的网络安全责任，需要整体统筹，建立以品牌为导向的网络安全数据合规主体。此外，针对当前以被动式、应对式合规来实施的专项合规，他建议，车企在识别完整合规要求的基础上，采取平台化、融合化的方式去构建合规体系。

上海市智能网联汽车网络安全产业协同创新中心主任、上海市智能网联汽车网络安全重点实验室执行主任、紫金山实验室、上海大学车联网安全方向学术带头人 李玉峰发表题为《智能网联汽车网络安全检测前移的思考和实践》的演讲。他强调，“软件定义汽车新趋势下，漏洞已经成为智能网联汽车的公害。”

针对网联车的漏洞安全风险，李玉峰介绍了两大实践方向：事前检测和内生安全防御。他认为，事前检测、事中体系化防御，以及事后应急处理是网络安全常见的工作链条，自然也适用于智能网联汽车。他强调，就事前检测而言，考虑到汽车的复杂长供应链特性，应该提倡网络安全检测从整车向零部件“前移”。这样的“前移”可以使网络安全责任在供应链上横向到边、纵向到底、层层压实，带来早发现、易实施、低成本、高效益的效果，成为整体提升汽车网络安全基线水平，扎实落实相关法规和标准要求的一个重要“抓手”。

李玉峰

上海市智能网联汽车网络安全产业协同创新中心主任，紫金山实验室、上海大学车联网安全方向带头人

智能汽车创新发展平台首席架构师 梁健在演讲时表示，单车智能加网联赋能是中国的特色路线。梁健认为，车路云一体化目前迎来了重要的时机，目前全国有 17 个国家级的示范区，全国试点城市也在不断扩大。AI 大模型、区块链隐私计算及相关技术，将会在车路云一体化中创造更多机遇。

梁健

智能汽车创新发展平台首席架构师

梁健还认为，建设车路云一体化平台，带来的新技术、新业务依赖于整体网络基础设施建设，这种多组网方式对网络安全防护带来很高的挑战。需要配合网络的现代化改造，完善网络安全的防护体系建设，强化网络边界的防护，增加网络防御的纵深，提升安全结构的安全性，提升运行效率的管理，要作为保障车路云业务的安全有序运转的机构，采用集约化的模式，构建网络纵深的体系。

长安汽车前瞻院信息安全负责人、智能汽车安全技术全国重点实验室高级副总工 刘岱总结了智能网联汽车的六大安全特点：人身安全强相关；高实时性，且需要高安全可靠；多网融合风险暴露面很广；端点资源争夺非常激烈；数据量庞大；各方安全互相关联。

基于这些挑战，长安汽车提出构建一体化安全技术架构与多个重点研究方向，包括抗量子密码迁移、下一代数据安全隐私计算、虚实结合智能车安全检测、AI 融合安全 Safety 与 Security 等技术领域。

刘岱

长安汽车前瞻院信息安全负责人、智能汽车安全技术全国重点实验室高级副总工

奇安信集团副总裁 孔德亮在主题演讲中，从安全防护和威胁发现的角度，探讨了智能网联汽车产业发展过程中的数据安全问题。他认为，数据安全监管应贯穿整车的生产设计阶段、行驶阶段和未来产业发展的演进阶段。针对智能网联汽车的数据安全防护问题，孔德亮认为，应该围绕保护数据资产为中心，从管理、技术、运营进行数据安全体系设计，去明确数据安全战略和组织，制定数据安全工作机制和流程，梳理数据安全能力现状，理清数据安全建设的任务和实施路径，逐步开展数据安全体系的建设。

与会专家也强求，智能网联汽车领域的竞争形式已经从技术产品竞争升级到体系竞争、生态竞争，生态建设成为应对严峻竞争形式的迫切要求，成为抢占制高点的关键举措和重大依

孔德亮
奇安信集团副总裁

托。

在智能网联新能源汽车安全论坛上，网络安全企业和车企宣布了多项合作，展示出车联网信息安全平台生态建设的最新成果。西部智联和奇安信签署了战略合作协议；此外，赛力斯和奇安信联合实验室揭牌。安

西部智联和奇安信签署战略合作协议

赛力斯和奇安信联合实验室揭牌

BCS 2024 数据安全论坛成功举办

——保障数据要素安全，构建可信数据流通生态

6 月 6 日，在 2024 北京网络安全大会产业日上，由 CCF 数据安全工作组、奇安信集团共同举办的数据安全论坛顺利召开，论坛以“保障数据要素安全，构建可信数据流通生态”为主题。汇聚了行业专家、学者、政策制定者及技术开发者，共同探讨数据流通安全的最新趋势、技术创新与实践，促进一个更加安全、高效、可信的数据流通生态的建立。

计算机安全专委会常务副主任 于锐致辞表示，“数据安全仍然存在着许多亟待解决的技术、管理和应用问题，涉及数据的确权、授权、交易、隐私保护、系统安全等方方面面，因此要全面落实党和国家的部署，统筹发展与安全，建立良好的数据安全产业生态，提升数据安全治理和安全的保障能力。”

于锐

计算机安全专委会常务副主任

齐向东

全国政协委员、全国工商联副主席、奇安信集团董事长

全国政协委员、全国工商联副主席、奇安信集团董事长 齐向东在致辞中表示：“数据促进各行各业发展的大前提，一定是安全。我们要把加快数据安全建设、提升数据安全保障能力当成重点任务。”奇安信一直以促进发展为最终目标，打造整体性的数据安全合规保障体系。奇安信还坚持

“AI 驱动安全”，通过打造人工智能安全大模型、推出 AI 安全整体应对方案，进一步加强安全建设。

闫树

中国信息通信研究院云大所副总工

中国信息通信研究院云大所副总工 闫树分享了政策与技术共同推动数据安全高效流动的思考。他指出，“数据已成为数字经济时代的关键生产要素，具有高流动性、可复制性等特点，推动数据价值释放的规章制度和技术手段需要进一步重塑。”闫树先生详细介绍了国家在数据安全方面的政策更新，特别是《促进和规范数据跨境流动规定》，对于平衡数据出境需求与跨境数据安全保护要求的新尝试。在此基础上，探讨了数据流通技术的体系架构，分享了重点技术的发展情况与应用前景。

李爱君

法学博士、中国政法大学教授博士生导师、中国政法大学互联网金融法律研究院院长

法学博士、中国政法大学教授博士生导师、中国政法大学互联网金融法律研究院院长 李爱君在演讲中深入探讨了数据产权制度的重要性，她认为，“数据产权制度是数据流通和安全的基础。”李教授提出，要充分发挥数据的自然属性价值，科学认知数据与信息的区别，尊重数据的双重结构特征，并充分保护数据承载的多元主体合法权益。她强调，数据产权制度的构建需要围绕这些方面进行，以确保数据的安全和高效利用。

周辉

中国社科院法学所网络与信息法室副主任（主持工作），中国法学会网络与信息法学研究会常务副秘书长

中国社科院法学所网络与信息法室副主任（主持工作），中国法学会网络与信息法学研究会常务副秘书长 周辉在演讲中聚焦人工智能时代下的数据合规和数据安全问题。他从五个方面展开讨论，包括人工智能发展背景下数据的特殊价值、数据合规的挑战、数据安全的风险及如何在保障安全的同时促进人工智能的发展。周辉先生提出，“数据安全不仅是技术问题，也是法律和政策问题，需要从多维度进行综合考虑和制度设计。”

刘国伟

北京市政务服务和数据管理局数据标准与安全处处长

北京市政务服务和数据管理局数据标准与安全处处长 刘国伟从政府视角出发，分享了对数据要素流通安全管理的思考。他提出，“数据安全工作应与数据发展紧密结合，为促进数据要素流通发展保驾护航。”刘处长强调，应充分认识数据安全相比传统网络安全的新变化和新内涵，构建涵盖管理、责任、技术、措施等多层面全方位的数据安全防护体系。

潘进杰

CIMC 中集集团 CIO

CIMC 中集集团 CIO 潘进杰分享了中集集团在数据安全和数字化转型方面的丰富经验。他强调了数据资产保护的重要性，并介绍了集团从查缺补漏到主动防御，再到持续提升安全运维能力的三个发展阶段。潘进杰先生特别提到了通过与奇安信等合作伙伴建立的 7×24 小时安全运维体系，以及利用人工智能技术进行威胁识别和处理的创新实践。他指出，尽管已经采取了多种安全措施，数据安全仍然是一个需要持续关注和改进的领域。

徐权佐

平安银行数据安全专家

平安银行数据安全专家 徐权佐发表了关于金融业数据安全风险运营

实践的演讲。他提出，“数据安全运营的核心目的和困难是实现‘风险可控、相对便利、过程可量’，并强调了‘持续合规’在数据安全管理中的重要性。徐权佐先生从合规风险、泄露风险两方面分别举例了平安银行在客户授权、内外部威胁防护、第三方数据交换的实践案例，并在最后简要介绍了基于 IPDRR 模型的网络与数据安全风险运营体系。

刘前伟

奇安信集团副总裁、首席数据安全科学家

奇安信集团副总裁、首席数据安全科学家 刘前伟从国家数字经济发展的顶层设计出发，在“人工智能 +”和“数据要素”的时代背景下，指出安全与合规对数据要素及数字经济发展至关重要。

刘前伟认为，筑牢数据安全屏障，需要数据资源安全保护与数据要素流通安全合规并重。在数据资源安全保护上要以数据资源本身为核心，关注数据流转的层面，构建面向数据全生命周期和全流程的保护体系，做到数据安全看得清、管得住、防得好；当数据要素流通起来，应该构建分类流通和分级保护体系，明确哪些数据应该充分流通，哪些数据应该受控流通，哪些数据应该合规流通，并通过技术手段进行保障。以“公共数据授权运营”和“大模型训练”两个场景讲解了从业务的视角去出发，找出来那些重点要保护的数据资产，找出关键的环节，并进行适度防护的实践经验。

在最后的圆桌对话上，与会者一致认为，数据作为新型生产要素，其安全性和流通性是实现数字经济高质量发展的关键。嘉宾们呼吁各方共同努力，构建可信的数据流动生态系统，实现数据要素的安全和高效利用。安

BCS 云原生安全论坛在京召开

——原生融合 安全随行

近日，2024 年 BCS 北京网络安全大会—云原生安全论坛在京召开，论坛以“原生融合 安全随行”为主题，共同探讨云原生环境下的安全实践与建设思路，以新技术解决新安全问题，护航在数字经济浪潮下云原生产业的健康发展。

随着企业上云、用云的进程加快，云原生技术快速普及，凭借敏捷、高可用、可弹性扩展等优点，云原生已经成为当前 IT 基础设施优先采用的云计算技术，成为推动 AI、新质生产力发展的重要力量。然而，随着云原生业务的快速发展，诸多安全问题随之而来，如云原生的到来让安全可观测性变的更加困难；旁挂式的安全工具各自为阵，缺乏统一管理和协作能力，给安全运营带来了巨大挑战。针对这些云原生环境产生的新型安全问题，参会嘉宾分别表达了自己的观点。

杜岚

中国信息通信研究院云大所高级业务主管

“我们需要构建一个原生化、平台化、智能化的云原生安全防护体系，包括：云原生和安全的深度融合、全生命周期一体化防护、AI 赋能自动化，以及云原生安全运营水平提升。”中国信息通信研究院云大所高级业务主管 杜岚表示，“国内的云原生安全进入了快发展期，构建云原生安全防护体系是目前市场关注的热点。”

周凯

联通数科安全事业部 CTO

“联通云原生安全产品、安全的能力生于云、长于云、用于云，跟联通云做深度融合，成为一个 PaaS 化的能力对外提供。”联通数科安全事业部 CTO 周凯表示，“联通云正在推进云安全能力的统一编排、云安全产品的原生化、云安全运营的原生化工作，为客户提供更好的云原生安全产品和真正体系化、精细化的安全运营服务。”

朱志强

亚马逊云科技资深安全专家

“我们认为云安全是一个洋葱型的防护，我们希望客户建立多层次的防护，这样能够让黑客每递进一层都会付出很大的代价，当这个代价已经让攻击者无法承受时，进一步的攻击会停止。”亚马逊云科技资深安全专家 朱志强表示，“客户需要做多层级的保护、提高攻击成本，最大限度降低黑客攻击带来的危害。”

任一林

火山引擎终端安全攻防研究专家

“当前，供应链安全问题及漏洞、后门等可以给攻击者带来初始入侵入口的问题非常受关注，这些问题会进一步导致容器逃逸或者其他隔离性问题，最后威胁到其他集群的安全。”火山引擎终端安全攻防研究专家 任一林表示，“云原生安全需要左移，在应用层入口利用上就可以检测到攻击者的存在，目前 RASP 是保护云原生应用运行时安全的有效手段，未来会进一步加强对抗手法检测、加强同集群侧的检测研判联动，从而实现更好的防御效果。”

王强

中国科学院大学

“云原生的资产拓扑高复杂性，由于伸缩及业务部署的弹性要求，我们可能对资产的底层管理是偏弱的，在云原生的条件下，容器和虚拟化都让我们对底层的掌控越来越缺失，这个缺失带来了观测性的减弱。”中国科学院大学 王强表示，“网络防御现在已经进入到深水区，可以从云上去建立多维度卡点，去规避流量旁路的观测盲区，建立无缝的应用安全感知平面。”

范维博

奇安信云安全事业部负责人

“数字经济驱动企业数字化创新，云原生成为技术新趋势，随之而来的云原生安全也是被关注的热点，云原生环境普遍存在代码缺陷、错误配置、供应链安全、云原生制品安全等诸多安全问题。”奇安信云安全事业部负责人 范维博表示，“现阶段要从全局视角，对云原生资产、风险、威胁的全生命周期做安全管理，奇安信 CNAPP 云原生安全管理系统正是针对云原生安全需求开发的，其安全能力覆盖整个云原生架构及云原生应用的全生命周期。”其中，纵向从下到上覆盖云原生应用运行的基础设施，包括 IaaS 平台、PaaS 平台、主机及容器工作负载，以及应用自身对应的微服务，横向从左到右覆盖云原生应用的整个生命周期，包括开发、部署和运行时阶段，将安全融于 Devops，成功实现“安全左移”，帮助客户实现云原生安全的可视、可管、可控。

薛庆伟

奇安信网络安全部安全专家

“云原生技术的快速发展为企业带来了灵活性和可扩展性，但同时也带来了新的安全挑战。”奇安信网络安全部安全专家 薛庆伟，以奇安信内部实践为基础，向参会嘉宾介绍了云原生环境下的攻击和异常检测方法，以及云原生安全运营的实践思考。

BCS 云原生安全论坛迄今已经连续举办两届，汇集了来自云原生领域的众多业界专家学者、甲方客户及安全企业，对提升云原生安全领域的理论建设与实践水平产生了积极影响，为数字经济浪潮下的云原生产业健康发展保驾护航。安

企业安全运营论坛顺利召开

——共探智能化时代企业安全运营新思路

6 月 6 日，由奇安信集团主办的 BCS2024 企业安全运营论坛在北京国家会议中心顺利举行。论坛就“智能化时代的企业安全运营”主题，邀请多位网络安全行业知名的一线实战管理者与安全专家进行分享和讨论，吸引了线下、线上 1500 余位大会听众，现场 200 余人座无虚席，场面热烈。

论坛共设四个演讲单元，分别是：安全运营体系建设、终端安全运营、供应链管理和 AI 助力企业安全运营。同时，为与会者提供三个听众提问环节，促进知识的分享和观点的碰撞。

林培旺

中兴通讯信息安全资深专家

中兴通讯信息安全资深专家 林培旺介绍了公司内信息安全体系管理的相关经验，对为什么要建信息安全管理体系、体系如何构建、如何推进落地进行了详细分享。林培旺表示，“中兴通讯之所以建设信息安全管理体系，是因为需要用体系化方法解决安全管理中的痛点和难点问题。”整体体系框架通过强化总则、通则到业务细则的分级管理，在制度层面明确业务谁管理，安全谁负责，把安全规则嵌入业务流程；并采用组织、定、管、查的闭环管理方法推动体系落地。建立职责清晰、分工明确的组织机制确保工作高效推进；通过精准定密识别核心信息，聚焦绝密，平衡数据保密与共享；全面管控信息流及其涉及的人、事、物等相关要素，压实归口管理责任，识别核心资产，在业务流程的关键节点进行安全规则嵌入；并通过体系运行符合性检查与安全事件响应处置，完成体系闭环，进行负反馈并推动优化改进。同时，中兴通讯

也会将自身信息安全体系化管理的实践通过咨询服务等方式对外共享，更好地为各行各业赋能。

李鹏

兴业证券安全经理

兴业证券安全经理 李鹏在《自动化安全运营实践》主题演讲中分享了兴业证券在安全自动化运营方面的实践和经验，总结了兴业证券在自动化运营体系建设过程中的重要心得。第一，制度先行，一定要有完善的信息安全管理制度，并从上自下推动安全管理。第二，信息资产管理，整个自动化运营的体系，需要基于精确的信息资产。第三，安全场景，需要有一个平台和安全人员定义这个安全场景，设计和不断优化安全场景。第四，闭环运营，需要持续跟踪每个工单的完成情况，保障运营的效果。

刘海庆

多氟多智能信息部部长

作为场内唯一一家做实体制造的公司，多氟多智能信息部部长 刘海庆带来了新材料行业信息安全要素的建设实践分享。刘海庆解释道，“我们流程制造业做信息安全，保护的就是企业的核心数据。”多氟多已经从传统的业务数字化转向数据驱动业务，数据安全的重要性尤为重要。在安全建设方面，多氟多定义了五个一，即一眼看全、一眼看穿、一眼看透，一目了然、一竿子到底，通过洞察全流程、全场景，看透安全攻击的背后逻辑，将安全风险降到最低。

孙诚

奇安信终端安全技术总监

奇安信终端安全技术总监 孙诚，通过天擎的云端数据，展示了当前勒索攻击的技术趋势，给出终端对抗思路。孙诚指出，“勒索攻击是一套链条式的攻击，攻击过程越长，越能充分发现企业关键数据。而 0~30 分钟是勒索病毒攻击应急响应的‘黄金救援期’，90% 的攻击都可以被有效遏制。”奇安信通过入口防御技术、过程防御、勒索加密防御技术等体系化防御措施，能够尽早发现攻击痕迹及攻击线索，大大降低勒索成功概率。

王萌

北京银行系统运营中心安全管理室室经理

北京银行系统运营中心安全管理室室经理 王萌在《网络资产攻击面管理运营实践》中，介绍了北京银行以往安全运营领域的实践和过程成果，从资产、风险及如何对资产和风险开展持续运营进行分享。王萌认识到，为实现银行资产的有效汇总，做好资产的识别策略，必须要同时结合 IT 运维管理和安全运营技术和策略。

胡文友

金睛云华联合创始人

金睛云华联合创始人胡文友发表了《AI 大模型赋能威胁检测 & 安全运营》的主题演讲。胡文友引用 IDC 的一个大模型调研，显示大模型的能力被用到安全行业，才是最具颠复性的。他强调，“大模型本身是一种能力，类似于发动机，不能直接卖给客户，必须得把大模型作为一个核心组件，置于成品中卖给客户。”如今，金睛云华已经发布了一系列应用大模型的产品，在攻防演练、重保活动等场景中表现突出，广受赞誉。

印钰

奇安信安全攻防专家

奇安信安全攻防专家 印钰从智能红队的研究和实践，展开《自动化渗透测试与智能红队实践》分享。印钰认为，“自动化渗透测试就是一个加强版的扫描，功能更强、覆盖面更多，但始终是自动化工具，工作流程是固

定的。”目前，红队在大模型加持之下，加强的是分析环节、决策环节。奇安信正在基于整个技术做新的产品、策略研究，包括平台建设等，为实现智能红队的完全全流程自动化。

陈然

奇安信网络安全部安全运营经理

奇安信网络安全部安全运营经理陈然分享了《Q-GPT 重塑安全运营探索》。陈然指出，“安全运营人员通常的工作内容繁琐、细碎且量大，亟需利用 AI 解决安全运营过程中的困难和困境。”去年，奇安信发布了安全大模型 Q-GPT，“Q-GPT 在安全运营上的应用，解放了运营人员大量精力，对我们来说，现在的职责就是把大模型用好”。预计未来，可帮广大客户实现 95% 的自动化安全运营，重塑传统安全运营模式，定义智能安全运营新标准。

论坛圆桌讨论环节中，嘉宾结合自身实践，针对安全运营落地大模型技术的最佳途径给出了各自的看法，并对大会“AI 驱动安全”的发展理念表示一致认可。奇安信安全运营专家富源表示，未来的安全运营工作将离不开 AI 的加持和助力，目前，奇安信安全大模型 Q-GPT 已与 NGSOC 平台完美融合，在自动遏制高频事件、量化安全运营指标、预防通报等方面表现突出，未来有望在智慧交通、智慧医疗、金融风控、智能制造等领域快速落地。安

圆桌对话环节

BCS 2024 融合安全论坛召开

——揭秘网安行业最大赛道的增长密码

“作为网络安全的第一道防线，以防火墙为代表的边界安全是网络安全行业迄今已有 30 多年，始终是最大的细分市场，被誉为行业‘常青树’。”全国政协委员、全国工商联副主席、奇安信集团董事长 齐向东在北京网络安全大会融合安全论坛上表示，“边界安全之所以经久不衰，是因为它在能力融合的路线上不断创新演进，持续推动市场增长。”

2024 北京网络安全大会融合安全论坛

2024 年 6 月 6 日，2024 北京网络安全大会（BCS2024）“融合安全论坛”在北京国际会议中心举办。奇安信集团董事长 齐向东，奇安信集团高级副总裁 吴登峰，奇安信集团副总裁、首席架构师 吴亚东，国家信息中心办公室副主任 吕欣，国家信息中心信息与网络安全部处长 刘蓓，中国石化工程建设有限公司高级安全专家 郭放，乐信集团信息安全中心总监 刘志诚，南凌科技股份有限公司首席技术官 鲁子奕，飞腾信息副总裁兼行业解决方案总经理 杨威，企业 IT 自媒体“老韩一米九”创始人 韩勋；思博伦通信科技产品总监 任红波等领导、专家和业界嘉宾出席了本次论坛，就融合趋势下的边界创新进行了探索交流和观点碰撞。

网络安全硬件市场达 225 亿，技术融合成驱动引擎

齐向东

全国政协委员、全国工商联副主席、奇安信集团董事长

齐向东引用了 IDC 的一组数据，

2023 年，中国网络安全硬件产品的市场规模达到了 225 亿人民币，到 2027 年，中国网络安全硬件市场规模将达到 364 亿人民币。这其中，边界安全是占比最大的主力产品，也是广大政企客户安全建设的刚需，长期占据着网络安全投资的主要比重。

对此，齐向东表示，能力融合是推动边界安全持续创新和市场增长的核心引擎，尤其是企业对网络安全需求的持续升级，包括混合环境的兴起、零信任的普及，都加速了边界安全的能力融合趋势。从 Gartner 提出的“网络安全网格架构 (CSMA)”的理念，到今年 RSAC 大会越来越多的厂商推出了平台集成解决方案，都验证了融合是行业发展的大势所趋。

吕欣

国家信息中心办公室副主任

“数字经济的崛起与繁荣，赋予经济社会发展‘新领域、新赛道’，形成‘新动能、新优势’，正在成为引领我国经济增长和社会发展的‘新力量’”。国家信息中心办公室副主任 吕欣表示，“数字经济高速发展，网络安全屏障作用更为重要，在网络系统的跨层级、跨地域、跨系统、跨部门、跨业务的协同管理和服务越来越普遍的情况下，技术融合、数据融合、业务融合成为趋势，推定网安行业尤其是融合安全技术创新和升级迭代变得更为迫切。”

边界安全的发展史，就是能力的融合史

吴亚东

奇安信集团副总裁、首席架构师

“边界安全的发展史就是能力的融合史。”奇安信集团副总裁、首席架构师吴亚东就边界安全的创新实践进行了分享。他表示，“防火墙的演进是边界安全发展的缩影，从最早具备简单 ACL 功能的路由器，到融入基础安全接入、NAT、VPN 的传统防火墙，再到融入了应用识别、URL、IPS、反恶意软件的 UTM（统一威胁管理），以及当前市场主流的融入 WAF、SDWAN、ZTNA、物联网、协同联动等功能的下一代防火墙。不难发现，融合是始终不变的关键词。”

在边界安全朝着融合趋势演进的过程中，先后创造了全球网络安全市值领先的两家公司，分别是开创 UTM 品类的飞塔公司（Fortinet），以及引领 NGFW 浪潮的派拓网络（PaloAlto Networks），其市值分别为 456 亿美元和 958 亿美元，这也充分验证了这个技术趋势。

吴亚东表示，从技术路线上说，融合分为两种，一种是功能组件级的融合，核心是把各种模块作为内部的一个功能组件，形成融合网关；另一种是 uCPE，通过虚拟化的方式把各种安全能力融合进来，目前在国外比较普遍。

吴亚东认为，未来融合的长期目标就是简化边界，代表产品是流量解密编排平台，它通过简化边界安全架构、安全设备资源池化、软件定义服务链、灵活的引流策略、软件定义 bypass 等技术，让网络维护化繁为简，实现了安全、高性能、易管理的完美平衡。

刘蓓

国家信息中心信息与网络安全部处长

“当前，企业数字化业务的形态已经发生变化，技术发展日新月异，安全要应对这种多变复杂的网络安全威胁，光靠单台设备、单一功能和单点防护，很难做到安全保障的效果，所以，融合安全成了一个非常急迫的需求。”刘蓓表示，“数字政府发展呈现几个特征，一是更加开放互联；二是特征就是融合协同；三是加强平台支撑和集约化建设；四是数据更加开放共享；五是新技术的广泛应用。这些趋势都需要加速推动融合的技术创新，包括数据的共享、 互联互通的标准化、多场景的覆盖等。

“传统边界安全架构存在多个问题，分别是业务连续性降低，安全建设压力剧增，投入产出比降低、安全投入关注点，安全能力固化、安全设备切割影响面广，尤其是加密流量增多，导致原有安全设备失效，安全威

郭放

中国石化工程建设有限公司高级安全专家

刘志诚

乐信集团信息安全中心总监

胁愈发严峻。”中国石化工程建设有限公司高级安全专家 郭放就大型能源央企对网络新边界的探索进行了分享。他认为，“原有串糖葫芦的网络部署架构，存在性能瓶颈、单个故障影响整体等弊病。未来需要对边界安全架构进行重塑，实现安全能力的池化部署。

郭放以流量解密编排器举例，描绘了融合安全趋势下的新部署模式。首先在编排方面，安全能力基于意图或业务进行按需编排，从而提升出口部署的可靠性、灵活性，简化出口运维，将原来冗余的一个糖葫芦串的边界防护体系，打造成为灵活、适应不同业务场景和需求的体系，让不同安全设备发挥出最大价值。结合业务、不同场景和需求的体系让不同安全设备发挥其最大价值。其次在流量解密方面，通过高性能流量解密，赋能不同的安全设备，提升其处理能力，最终实现降本增效的网络安全架构。郭放建议，对于大型企业机构，可以通过一拖 N 的流量编排器，将流量分流按需给流量平台，实现安全能力的全局化。

“边界的定义随着时代在不断变化，网络边界的定义是内外网的分界，应用边界的定义是账号和身份验证，我们理解的边界是对检测点的可验证控制。”乐信集团信息安全中心总监 刘志诚在《从零信任到无边界——我的数字安全边界观》中表示，“数字安全分企业安全、运营安全、产品安全三个层面，其边界定义也有所不同。”企业安全边界的定义是内网、零信任、CASB、SASE；运营安全边界包括消费者边界、运营边界、供应链边界、监管边界等；产品安全的边界是安全性和舒适度。解决边界的核心，在要素层面，需围绕身份、终端和访问策略，在能力层面，围绕数据驱动、关联分析、安全中台来推动。未来，一方面，从零信任到无边界是数字安全的必然趋势；另一方面，无边界的安全防线需要依托可验证控制的安全检测点。

鲁子奕

南凌科技股份有限公司首席技术官

南凌科技股份有限公司首席技术官 鲁子奕就从《SDWAN 到 SASE 的演进：探索和实践》进行了分享。他表示，“SASE 是一个集成了云安全、SD-WAN、边缘计算等多个元素的综合解决方案，其并非简单地将现有安全组件云化或整合，而是需要在边缘计算、云原生安全网元、灵活接入方式及持续的安全策略动态调整等方面实现深度融合。”南凌科技通过一系列创新措施，如混合云策略，将 SSE 功能部署在 POP 点 和 CPE（Customer Premises Equipment）上，以及构建统一管理平台，以提高安全策略配置与响应效率，并通过集成奇安信等多家安全伙伴的技术，实现了从资产统计到防御、检测、响应的全链条安全服务。

融合趋势推动算力平台、测试平台持续演进

杨威

飞腾信息副总裁兼行业解决方案总经理

“融合在各个领域成为趋势，包括技术的融合、端边云的融合等。”飞腾信息副总裁兼行业解决方案总经理 杨威表示，“飞腾芯片作为中国电子集团旗下的 CPU 设计国家队，致力于为技术创新提供高性能、高安全、高可靠的通用算力底座。”凭借 20 多年的研发历程，飞腾遵循“从端到云、安全定制、安全可信、开放合作”的研发路线，已拥有从端到云的全谱系通用智能和专用算力芯片，广泛应

用于各类设备，特别是在安全领域展现出显著优势，从而为网络安全的融合创新提供强大的算力底座。

韩勛

企业级 IT 自媒体“老韩一米九”创始人

作为专注企业级 IT 自媒体“老韩一米九”创始人 韩勛就《从企业业务 AI 化浪潮看安全发展趋势》进行了分享。他表示，“尽管 AI 应用在企业中日益普及，旨在提升效率降低成本，但很多企业在追求 AI 与业务融合时，并未充分意识到对现有网络和安全架构的潜在挑战，导致安全配置普遍薄弱，南北向与东西向均面临大量安全威胁。”韩勛表示，行业市场与商业市场需求的不同，导致产品在应用识别、互通与联动、部署形态等方面存在显著差异，因此需要更灵活的产品形态和商业模式，以适应快速变化的商业市场。他认为，目前网络和安全都已经走向融合，未来多个安全能力的整合，甚至单一供应商全家桶式方案可能成为未来发展方向。

任红波

思博伦通信科技公司产品总监

“随着网络架构的演变，传统的城堡与护城河安全模型已无法满足现代企业复杂多变的需求。如今，云服务、远程办公与分支网络的兴起，使得企业网络边界变得模糊，安全测试与性能评估面临全新挑战”。思博伦通信科技公司产品总监 任红波表示，传统测试集中于单一设备的性能，如吞吐量、时延等，而今需要转向整体网络效能与用户体验的评估。随着 SD-WAN、零信任等技术的应用，安全测试需要纳入新指标，如攻击识别准确性、负载均衡与智能选路能力等，测试对象由单台设备扩展到整体网络，考虑不同部署位置的安全策略与流量路径优化，避免重复分析，确保高性能与低时延。同时，软硬结合，线下和云端结合将是安全工具的发展方向。

2024 北京网络安全大会以“AI 驱动安全”为主题，共举办了 2 场峰会、20 多场分论坛，2 场大赛，邀请来自 10 多个国家和地区的专家学者，来自金融、能源、交通、政务等 10 多个行业领域代表参会。其中，融合安全论坛聚焦融合趋势下的边界安全演进和创新，邀请政府机构、行业客户、上下游合作伙伴等共同探索“如何拥抱技术趋势，共同推动产业升级，为数字经济筑牢安全基石”。 安

2024 年 InForSec@BCS 网络空间安全国际学术研究交流会在北京成功召开

6 月 6 日，2024 年 InForSec@BCS 网络空间安全国际学术研究交流会在北京国家会议中心成功举办，线上、线下近千人参加了本次研讨会。

本次学术研究交流会主题为“网络安全技术创新与应用前沿”，邀请了国内从事人工智能安全、互联网基础设施安全、电磁安全、物联网安全等领域研究的专家、学者，分享国际前沿的研究成果。

交流会上半场由 IEEE Fellow、浙江大学教授、系统科学与工程系系主任 徐文渊主持；下半场由清华大学助理教授 刘保君主持。

徐文渊

IEEE Fellow、浙江大学教授、系统科学与工程系系主任

刘保君

清华大学助理教授

邹德清

长江学者特聘教授、华中科技大学网络空间安全学院常务副院长

长江学者特聘教授、华中科技大学网络空间安全学院常务副院长 邹德清在会上作特邀报告——《开源社区中克隆代码管理与安全漏洞检测》。随着开源代码的规模不断扩大且开源代码的语义不断丰富，面向开源社区的代码克隆检测技术成为一项迫切的需求。邹德清教授分别从语法克隆与语义入手，介绍了团队近年来取得的六项代表性成果。

李冰雨

北京航空航天大学副教授

北京航空航天大学副教授 李冰雨发表题为《重新审视证书透明化：公众对第三方 Monitor 的监督》的报告。他结合实际经验，介绍团队如何

重新审视 CT 设计，引入 CT 框架新组件——CT Watcher，借助该组件，任何利益相关方均可充当，协同参与检查多个第三方 Monitor 的证书检索服务，检测返回结果一致性，从而发现在证书签发过程中的不当行为。

刘明烜

中关村实验室助理研究员

中关村实验室助理研究员 刘明烜发表题为《数据驱动的域名基础设施新型滥用行为研究》的报告。她从数据驱动的角度出发，结合主动探测和被动数据分析，介绍了基于域名威胁情报的防护型域名解析服务相关安全研究，以及基于海量域名解析日志的新型域名滥用形式的大规模识别和分析结果。

闫琛

浙江大学副研究员

浙江大学副研究员 闫琛发表题为《传感器电磁安全与隐私问题研究》的报告。传感器不仅是电子信息系统与物理世界交互的入口，还是收集用户位置信息、行为模式、健康数据等敏感数据的重要来源，他从传感器电磁漏洞机理分析、电磁攻击技术、防护方案等方面介绍团队的研究成果，分享了在后续传感器安全与隐私设计方面的思考。

吴豪奇

蚂蚁集团隐语算法专家

蚂蚁集团隐语算法专家 吴豪奇发表题为《基于隐语 SPU 框架实现高效大模型密态推理》的报告。大模型研究如火如荼，在对话领域取得了显著进展，然而其实际落地，如提供推理服务和对话接口（如 ChatGPT），存在潜在的数据泄露风险。对此，他在会上分享了如何基于 SPU 实现大模型安全推理，无缝地由明文推理切换为密态推理，并介绍了结合量化的性能优化方法。

华中科技大学副研究员 周满发表题为《基于手指摩擦声感知的指纹推断研究》的报告。他介绍了一种针对指纹识别的新型侧信道攻击——PrintListener。它利用用户在屏幕上的指尖滑动产生的细微摩擦声，经过背景噪声隔离、信号补偿、摩擦事件检测、数据增强等预处理，提取可解释的音频特征，通过加权联合预测推断一级指纹特征，然后利用随机重启爬坡算法，合成更具有针对性的万能指纹。

周满

华中科技大学副研究员

会议同期还举行了大数据安全分析竞赛 DataCon 专家委员会及技术委员会聘书颁发仪式。DataCon 专家委员会主任、清华大学教授 段海新为西安交通大学教授 王伟、北京大学计算中心网络安全室主任 周昌令等专家学者代表颁发证书。安

BCS2024 举办威胁情报技术论坛
——威胁情报多场景下的实战技术落地

2024 年 6 月 6 日下午，威胁情报技术论坛亮相 2024 北京网络安全大会。论坛以“威胁情报多场景下的实战技术落地”为主题，邀请了多位业界资深专家，共同探讨网络威胁情报技术的最新进展、发展趋势及应用实践，分享威胁情报的有效利用案例及经验。

刘宸宇

数世咨询合伙人

威胁情报作为一种非常有效的检测赋能技术，自 2014 年开始流行，经过十年的发展，技术日趋成熟，应用场景日益丰富。数世咨询合伙人 刘宸宇作为本论坛主持人表示：“据数世咨询观察，威胁情报近年来呈现数据化、要素化的趋势，在 AI 大模型出现后，对于情报处置的泛化能力也越来越凸显。”作为整个安全生态中很重要的基础要素，威胁情报在用户网络安全体系中的基础地位也越来越重要。

中国信息安全测评中心 梁智溢的主题演讲围绕“威胁情报情报的共享和协同”展开。他表示：“目前 APT 网络活动呈现高级别、持续性、波及广、影响大及单一视角的现状，威胁狩猎是通过一块拼图看到事件全貌的过程，而威胁情报共享可以从及时性、准确性方面给企业提供更好的研判思路。”安全行业应该尽可能地在一定范围内开展情报共享和技术共享，协同验证，共筑网络安全防线。

梁智溢

中国信息安全测评中心

王宇

零零信安 CEO

“数据泄露是‘事后’安全，核心是‘监控’和‘处置’。”零零信安 CEO 王宇指出，大量的暗网玩家涌向了深网和明网，由于技术瓶颈变低，非法数据买卖越来越猖狂，但同时也为威胁情报提供了宝贵的来源。对于需要更高重视度的 LOG 数据泄露

而言，除采用双因素认证方式外，还可针对已知泄露的大量数据进行清洗，并作为威胁情报源，将可能涉及泄露的用户关停，用户再次登录时必须重新认证。而对于影响内容和范围巨大的非结构化数据，同时可采用 AI 技术使数据处理效率提高近百倍。

代皓

知道创宇 APT 威胁情报团队负责人

传统的威胁情报狩猎存在覆盖率低、部署难、滞后性、效率低等多种问题，部分 APT 组织还会针对网络安全设备漏洞进行攻击。知道创宇 APT 威胁情报团队负责人 代皓表示：“除基础的测绘数据外，还可以通过定向测绘、主动测绘的手段，掌握多个资产与新 IP 域名的明确关联信息，可实现 APT 威胁狩猎的追踪，做到高效率、低依赖获取威胁情报，并在攻击者进行攻击之前掌握其资产。”将威胁情报与网络空间测绘技术相结合，帮助用户有效抵御网络风险，提高资产管理、攻击面发现，以及漏洞事件应急响应等能力。

孙朝晖

北京派网软件有限公司 CEO

现代网络结构的变化，给传统威胁检测带来了新的挑战。北京派网软件有限公司 CEO 孙朝晖聚焦于多分支网络的威胁情报前置检测的实际问题和应用经验，强调了在分布式网络环境中，威胁情报是有效应对分支潜在安全问题的必需能力，并从技术实践角度讲解如何有效地部署和利用威胁情报，来增强各分支节点的安全性。

汪列军

奇安信威胁情报中心负责人

奇安信威胁情报中心负责人 汪列军在会上介绍了 AI 技术在威胁检测与分类、恶意代码分析、情报收集处理、漏洞挖掘分析及信息整合、应急响应等方面的能力，并介绍了 AI 技术在奇安信的威胁情报运营中的应用实践。值得注意的是，大模型技术虽然可以极大地提升安全分析和威胁情报的运营效率，但在实践过程中，仍需要警惕存在依赖特定输入和可能出现的误导性输出等风险问题，应该正确且有效地利用 AI 技术来增强而非替代人工分析，以实现更高效的网络安全防护。

信息技术飞速发展，网络环境日益复杂，网络威胁态势也呈现出多样化、复杂化的特点。勒索软件、物联网安全等问题层出不穷，人才储备不足，企业成本受限等问题，给企业带来前所未有的挑战。因此，加强网络威胁情报技术的研究与应用，在威胁情报应用及威胁发现中，集合多种类 AI 技术及应用，提升网络安全防护能力，已成为当前亟待解决的重要课题。安

电子取证分论坛成功举办

——揭示 AI 挑战，引领取证新时代

2024 年 6 月 6 日，北京网络安全大会（BCS2024）“电子取证分论坛”成功举行。

论坛以“AI 时代电子取证的新技术、新场景、新趋势”为主题，聚焦深度伪造技术、自动生成内容的真伪鉴定等新兴取证场景，探讨应对人工智能恶意使用的技术挑战，旨在引领电子取证技术的前沿发展，为司法实践提供有力支持。

蒋丽华

北京市刑事侦查学研究会常务理事

北京市刑事侦查学研究会常务理事 蒋丽华代表指导单位对论坛的召开表示祝贺。她指出，“AI 时代的网络非接触式犯罪打防难度不断增加，给公安刑侦实战带来了技术和法治治理上的挑战。”她强调，“要紧扣实战热点，坚持问题导向，在 AI 深伪识别和反诈等领域取得突破；强化结果导向，做到‘打一仗，胜一仗’；推进警企合作，调动全社会的科技力量为刑侦工作服务。”

赵峰

北京司法鉴定业协会秘书长

北京司法鉴定业协会秘书长 赵峰，在致辞中表示：“面对 AI 技术带来的挑战，北京司法鉴定业协会将坚定信念，积极作为，推动 AI 技术在司法鉴定领域的健康发展。协会将深入研究司法鉴定的新情况和新问题，确保数据安全和隐私得到严格保护，同时加强人才培养和科技支撑，提升从业人员的专业素养，全面提升司法鉴定行业的服务质量。”

韩争光

奇安信集团副总裁

奇安信集团副总裁 韩争光代表奇安信集团对论坛召开表示祝贺，并对各位嘉宾和参会者表示欢迎和感谢。他指出，“随着大数据、云计算和物

联网的发展，取证对象和需求日益多样化，技术也日趋成熟。奇安信集团始终秉承‘安全赋能取证’的理念，为客户提供高效、精准的解决方案，以应对不断变化的攻防态势。”面对AI时代的挑战与机遇，奇安信集团将不断创新，推动技术研究与应用，同时共建开放、协同的取证生态圈，推动行业整体进步。

张皓斐

北京市人民检察院声像资料鉴定人

正式演讲环节，演讲嘉宾们分别从政产学研用多个角度探讨了在AI时代，电子取证领域的新技术、新场景、新趋势。

北京市人民检察院声像资料鉴定人 张皓斐带来分享《人工智能时代下伪造图像与声音的技术审查及未来应对路径探讨》，他强调，“近3年来，深度学习算法迭代升级速度明显加快，深度伪造的音视频对取证、鉴证工作也带来检测技术难度的提升。”一是用AI打败AI。在利用传统标准和技术应对同时，要积极尝试以AI技术为基础的新技术进行辅助审查判断；二是产学研用互动。国内AI研究机构、高校、厂商应加快对接侦查机关等相关技术部门，组织行业技术研讨，多维度展示产品的可用性和有效性；三是加快人才培训。组织开展深度伪造检测技术一体化培训，适时邀请司法机关技术人员参与。

陈龙

重庆邮电大学教授

重庆邮电大学网络空间安全与信息法学院教授 陈龙老师带来主题分享《面向生成图像滥用侵权的图像归因取证方法》。陈教授指出，“生成对抗网络（GAN）生成图像带来了滥用和侵权的挑战，迫切需要有效的应对方法。”他介绍了图像水印、伪造检测和图像重建等技术，并强调了这些方法在不同应用场景中的重要性。通过基于迭代优化和编码器预学习的重建图像方法，陈教授展示了如何通过比较待检图像与重建图像的相似性，实现对图像生成方式和来源的归因分析，以满足司法鉴定的需求。

萧子豪

瑞莱智慧联合创始人

瑞莱智慧RealAI联合创始人、算法科学家 萧子豪基于瑞莱智慧多年来在AIGC检测领域的前沿研究和实践经验，包括AI伪造音视图文的特点、检测方法和案例，分享了《AIGC鉴伪取证技术的研究和实践》。他表示，“随着AIGC技术的发展，生成效果越来越逼真，滥用门槛大幅降低，严重干扰了案件的研判，亟需升级鉴伪技术，开发面向多模态AIGC的反制技术。”他强调，AI伪造反制技术需注重“攻防一体”，综合考量伪造技术、鉴伪技术及对抗样本攻击和防御技术，从而提升整体能力。

谢春磊

奇安信司法鉴定技术总监

奇安信司法鉴定技术总监 谢春磊从产业方向带来演讲《智能化犯罪的取证挑战：人工智能恶意使用的识别与应对》。他指出，“人工智能技术的发展导致智能化犯罪爆发式增长，呈现出复杂性高、成本低、破坏性强和隐蔽性高的特点，目前尚无成熟的应对方案。”谢春磊建议，多管齐下应对智能化犯罪：加强AI技术监控与行为分析，利用数据挖掘和机器学习提升识别能力；应用深度伪造检测和主动防御技术，搭建预警平台；完善法律法规，明确AI使用的法律界限；提高公众意识，构建全社会防范体系。通过这些措施，可有效提升对智能化犯罪的识别与应对能力。

奇安信盘古事业部副总经理 段继平在论坛中发布了奇安信司法鉴定的全新品牌“洞鉴”。他指出，“经济利益驱使下，新型网络犯罪形态不断涌现，鉴定需求日益增长，而目前的鉴定机构普遍存在“小、慢、乱”的现状，难以满足市场需求。为此，奇安信司法鉴定致力于打造一个全国范围内统

段继平

奇安信盘古事业部副总经理

一标准、高品质、高效率的司法鉴定网络，为客户提供全链条专业服务。”段继平强调，“洞鉴”的使命是洞观虚实、鉴辨真伪，通过整合先进技术和专业团队，奇安信将为客户带来更领先、更高效、更权威、更全面的新一代数字司法服务。

吴汉迪

奇安信盘古事业部产品总监

奇安信盘古事业部产品总监 吴汉迪发布“盘古石取证：引领变革，数字时代取证产品的变与不变”的演说。

电子数据取证行业从萌芽初生到同质同构，面对数字时代多变的网络犯罪技术趋势，同质化发展、创新积极性降低等问题凸显，作为打击网络犯罪的最后一道“防线”其面临的挑战在不断增加。时有所需，必有所为，奇安信盘古石取证多年来坚守“安全赋能取证”的核心理念，致力于高强度对抗环境下的技术创新、产品研发与服务支撑，同时倡导行业内加强合作与交流，实现多元化、专精化发展，共创取证新时代。

会上进行了构建新基座：业务安全生态联盟签约仪式。此次签约仪式代表着奇安信业务安全以取证鉴定为基础转型迈向事前、事中、事后提供全链条支撑服务的关键一步，同时也是奇安信首次创新性地以生态合作的模式推动行业发展的重要里程碑。来自四川效率源信息安全技术股份有限公司、上海硕煜智能科技有限公司、上海歆仁信息科技有限公司、成都链安科技有限公司、滁州天邈电子科技有限公司的嘉宾一起参加了签约仪式。安

奇安信

奇安信威胁情报中心

中国威胁情报行业领军者

奇安信威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，以业界领先的安全大数据资源为基础，基于奇安信长期积累的威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

威胁情报中心

威胁研判分析平台ALPHA： 一站式云端SaaS服务的威胁分析工具平台。是安全分析师为同行打造的利器，针对IOC查询、线索关联、事件溯源、样本行为检测和同源分析等威胁分析场景提供全面的解决方案。

高对抗云沙箱分析平台： 提供多种动静态检测、分析技术，展现文件各方面特征，帮助分析师快速判别、并掌握恶意软件的详情。

威胁分析武器库： 服务于安服、安运、安全分析师及各类企业用户。支持IOC自动化数据流检测、失陷情报、恶意IP批量查询；支持邮件批量自动化检测；支持WEB应急日志、主机应急日志分析。

威胁情报系统QAX TIP： 威胁情报平台是情报收集、维护、使用的综合性平台。可帮助企业在安全运营中，利用威胁情报快速检测、响应、分析和预防各类网络攻击威胁，并分析产生行业威胁情报。

威胁雷达： 利用大数据和威胁情报监测技术，整合了奇安信的高、中位威胁情报能力，提供指定区域内网络威胁高位监控、案件拓线分析、样本深度分析等多种能力。

样本同源分析系统： 奇安信威胁情报中心红雨滴团队基于样本基因深度解析，使用机器学习算法用于APT数字武器追踪的可视化分析系统。

高级威胁分析服务： 为网络安全主管单位，政府机构、行业客户及高校科研机构提供情报线索拓线和威胁分析服务，输出深度分析报告供其决策参考。

奇安信威胁情报中心：
ALPHA网址：https://ti.qianxin.com
雷达网址：https://r.ti.qianxin.com
扫描关注我们的微信公众号
邮箱：ti_support@qianxin.com

▶ 2024 全球数字经济大会数字安全高层论坛暨北京网络安全大会战略峰会现场。

▲ 6 月 5 日，国家会议中心，第六届北京网络安全大会签到台。

▲ 全国工商联副主席、中国民间商会副会长 汪鸿雁，中国电子信息产业集团有限公司总经理 李立功，中国职业技术教育学会会长、教育部原副部长 鲁昕，中国友谊促进会理事长、国家网信办原副主任 陈智敏，中国工程院院士、鹏城实验室主任 高文，中国工程院院士 蒋昌俊，中央网信办网络安全协调局副局长 王营康，全国政协委员、全国工商联副主席、奇安信集团董事长 齐向东共同宣布大会启动。

▲ 全国政协委员、全国工商联副主席、奇安信集团董事长 齐向东接受媒体采访。

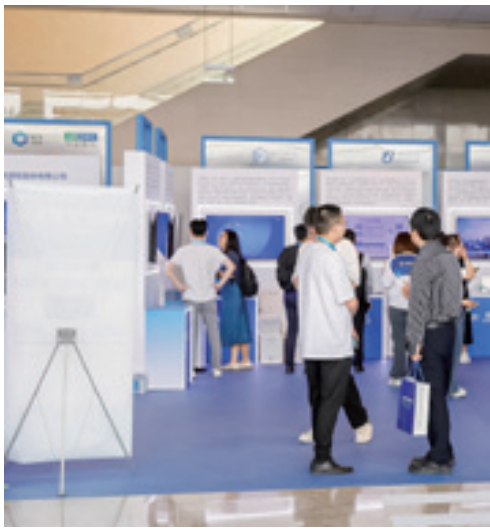
▲ 第九届安全创客汇决赛集体合影。

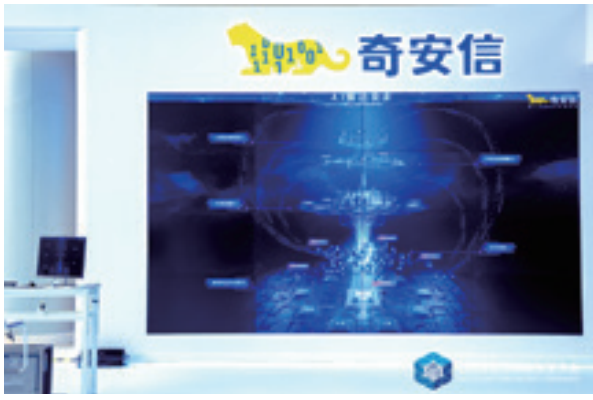
▶ 中国数据要素 50 人论坛是全球数字经济大会旗下的专题论坛。

今年BCS2024奇安信集团展区，主要展示了围绕本次大会主题“AI驱动安全”的全新可视化展示内容，以及QAX-GPT安全机器人的最新版本的亮相，集中呈现了奇安信集团AI能力在网络安全领域的实战应用。

同时，现场聚焦客户的实际使用场景，有针对性的将奇安信集团在数据安全、终端安全、边界安全、云安全、工业互联网安全等方面的实际解决方案展示出来。更是通过标杆案例内容的呈现展示产品能力。

除此之外，针对勒索病毒攻击及AI换脸的风险现场演示讲解，将网络安全领域真实存在的风险通过互动体验的方式呈现给现场观众，起到了真实的警示作用。





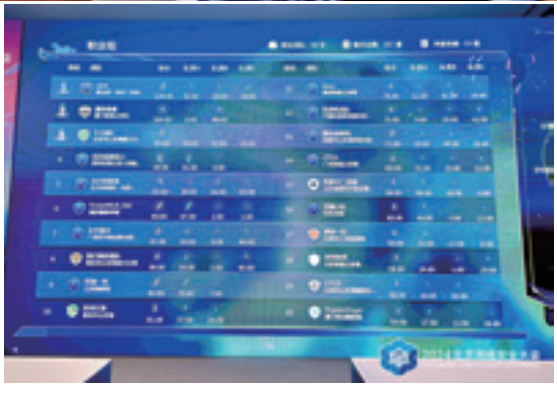

奇安信
2024北京网络安全大会


奇安天信×宁德时代
奇安信
2024北京网络安全大会


奇安信
2024北京网络安全大会


奇安信
2024北京网络安全大会

6 月 6 日，第二届“盘古石杯”全国电子数据取证大赛在国家会议中心圆满落幕。自 4 月 3 日启动报名至 5 月 11 日的线上晋级赛，再到 6 月 5 日的总决赛，这场历时 63 天的盛会，汇集了来自公安、检察院、企业、银行、海事局、高校、警校、政法院校及职业院校等众多领域的精英团队。大赛不仅展示了电子数据取证技术的广泛应用，更为专业人士提供了一个高水平的交流与展示平台。




E-07
2024北京网络安全大会


A-05
2024北京网络安全大会
2024 BEIJING CYBER SECURITY CONFERENCE


第二届
盘古石杯
全国电子数据取证大赛
2024北京网络安全大会


盘古石杯
全国电子数据取证大赛
总决赛


2024北京网络安全大会

奇安信

敏感信息泄露情报服务

- 攻击队视角的全网敏感信息情报
- 急需补上的防守盲点
- 供应链安全的管控抓手
- 预防性进攻反制利器

纵深防御的马奇诺防线，为什么会被攻破？

- 完整的防御体系，既要考虑正面防御，侧翼的情报收集和对抗也必不可少！
- 忽视全网视角的情报，是防守的重大盲点！

服务定位 SERVICE POSITIONING

- **攻击队视角**：使用渗透专家交付，不是简单的信息收集。
- **全网视角**：核心功能是从外部探测全互联网第三方应用中的敏感泄露数据；而非只关心自己的网络和应用。
- **情报级**：专家梳理的情报级信息，而不是简单数据抓取：给出利用思路和可能的攻击链，更有详细的整改建议。

奇安信安服团队

奇安信

新一代网络安全领军者

「零事故」安服团队重磅力作

900余次实战攻防演练的经验总结

从红队、蓝队、紫队视角全面解读攻防演练

扫码购买

奇安信连续三年位居
“中国网安产业竞争力50强”
第一名

6月20日，中国网络安全产业联盟（CCIA）
公布“2023年中国网安产业竞争力50强”榜单，
凭借扎实的技术实力和领先的市场表现，
奇安信连续三年高居榜单第一名。

“2022年中国网安产业竞争力50强”榜单

TOP15	公司名称
	奇安信科技集团股份有限公司
	深信服科技股份有限公司
	启明星辰信息技术集团股份有限公司
④	华为技术有限公司
⑤	天融信科技集团股份有限公司
⑥	绿盟科技集团股份有限公司
⑦	腾讯云计算（北京）有限责任公司
⑧	新华三技术有限公司
⑨	阿里云计算有限公司
⑩	杭州安恒信息技术股份有限公司
⑪	三六零数字安全科技集团有限公司
⑫	亚信安全科技股份有限公司
⑬	中电科网络安全科技股份有限公司
⑭	杭州迪普科技股份有限公司
⑮	山石网科通信技术股份有限公司