极牛网络安全通讯 • 社群期刊
2024 年 6 月 第 36 期

网安观察



P10
AI 驱动：网络安全进入智能新纪元

P5
欧洲理事会正式批准《人工智能法案》

P17 人工智能是先进生产力，不发展是最大的不安全
P20 大型语言模型正彻底改变网络安全形势
P23 AI 的安全问题要通过 AI 来解决

第36期
2024年6月

CONTEN

目录



安全态势

P4 | 国家能源局印发《电力网络安全事件应急预案》
P4 | 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
P4 | 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）》
P5 | 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》
P5 | 美国家情报总监办公室发布情报界 IT 能力建设路线图
P5 | 美国防部发布《零信任覆盖》政策指南
P6 | 美国政府发布 2023 网络安全年报披露 11 起重大事件
P6 | 云存储巨头 Snowflake 被黑，165 家知名企业遭殃 勒
P6 | 索攻击迫使越南国家邮政服务瘫痪超 3 天
P7 | 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
P7 | 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
P8 | 美国发生超大规模电信网络攻击，60 万台路由器集体变砖
P8 | SolarWinds Serv-U 目录遍历漏洞 (CVE-2024-28995) 安全风险通告
P8 | PHP CGI Windows 平台远程代码执行漏洞安全风险
P8 | 通告
P8 | Apache OFBiz 路径遍历漏洞安全风险通告
Check Point 安全网关任意文件读取漏洞安全风险通告
P9 | Google Chrome V8 类型混淆漏洞
P9 | (CVE-2024-5274) 安全风险通告
Atlassian Confluence 远程代码执行漏洞安全风险通
P9 | 告GitHub Enterprise Server 身份认证绕过漏洞安全
P9 | 风险通告
P9 | Zabbix Server SQL 注入漏洞安全风险通告
Git 远程代码执行漏洞安全风险通告
P10 | Google Chrome V8 类型混淆漏洞
(CVE-2024-4947) 安全风险通告



国际视野

P6 美国政府发布 2023 网络安全年报披露 11 起重大事件

ONTENTS



P10
AI驱动：网络安全进入智能新纪元

专题报道

P17
龚克：人工智能是先进生产力，不发展是最大的不安全

P18
高文：打造大规模 AI 模型训练的强大底座

P23
蒋楠：AI 的安全问题要通过 AI 来解决



第 3 6 期

《网安观察》编辑部

主办　极牛网

总　　编　　辑：陈鑫杰
总　　顾　　问：叶绍琛
副　　总　　编：王文彦
威胁情报主编：陈艇鑫
移动安全主编：蔡国兆
网安人才主编：林俊濠
涉网犯罪主编：胡铭凯
网安产业主编：张九史
网安态势主编：郑泽彬

公众号　小程序　网站

电子版请访问 www.geeknb.com 阅读或下载索阅、投稿、建议和意见反馈，请联系极牛网期刊编辑部。

E m a i l：hi@geeknb.com
地　　址：深圳市龙岗区天安云谷2栋2层
邮　　编：518000
电　　话：0755-33228862
印刷数量：1000 本
印刷单位：深圳彩虹印刷有限公司

版权所有 ©2021 极牛网，保留一切权利。
非经极牛网书面同意，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，极牛网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，极牛网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。



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。

红帽人才工程

Cyber Crime Governance Talent Training Project

工程简介

在“全国网络警察培训基地”的指导下，中国下一代网络安全联盟牵头发起「红帽人才工程」，联合华云信安、美亚柏科、高联通信等知名网络安全企业，围绕“网络犯罪治理、涉网犯罪打击”等相关网络安全课题，持续挖掘、培养、资助、赋能网络安全人才，构建红色基因的网络空间安全人才防线。

申报流程

课题征集 → 课题公示 → 立项评审

研究课题计划征集

研究课题信息公示

研究课题立项评审

申报说明

项目资讯

培养对象

政企单位在职人员、高校全日制在校生（含研究生）、互联网企业技术人员、网络安全企业技术人员以及社会网络安全人才...

核心课题

内网攻防、社工钓鱼、远控木马、免杀加壳、情报甄别、资金分析、调证溯源、取证固证、远程勘验、APP反编译、二进制逆向...



CTFWAR.ORG

网络安全的本质是攻防对抗
讲百遍不如打一遍

---习近平

CTFWAR介绍

CTFWAR攻防战争平台是CTFWAR网络安全攻防对抗联赛的官方平台，是由中国网络安全攻防大咖联合发起的创新型学习平台，以游戏的形式融入多种网络攻防场景进行答题、竞赛、互动。CTFWAR攻防靶场分为初级新手区、中级进阶区、高级挑战区，同学们可根据自身技术能力及技术方向进行筛选，整个学习过程将有全面的数据化呈现。

攻防答题模式

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

积分等级体系

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

AI 驱动：网络安全进入智能新纪元

2014 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。



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
联合国副秘书长

李军华：人工智能和机器学习的监管问题亟待解决

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
北京市经济和信息化局副局长

顾瑾栩：北京市未来将积极培育数字安全核心能力

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。

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。



圆桌对话

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。



极牛技术社群

网络安全技术社群

Cyber Security Technology Community

PLATFORM

网络安全技术社群

极牛网旗下面向网络安全工程师的社群平台，汇聚行业中网安工程师的知识和社交平台，围绕『技术』『管理』和『圈子』三个核心能力，将前沿的技术内容、技术管理成长感悟、技术圈子社群平台等向优质的网安工程师开放，每月定期组织社群会员线下活动，强调内容分享的体系化和活动内容的多样性，为中国网络安全工程师打造专属的全方位综合赋能的社群平台。

技术

聚焦前沿技术、热点技术、难点技术，提升网安在企业架构中的决策能力和迭代能力。

管理

专注在帮助网安工程师在职业发展中，建立体系化的管理知识和技术管理转型路径。

圈子

建立精准的技术方向圈子，针对不同的职业发展阶段，组成技术成长小组一起结伴同行。

极牛技术站

以沙龙、峰会、圆桌论坛等深度学习的形式进行，满足知识获取与社交需求。

管理加油站

面向管理者的闭门活动，前瞻性的思维和观点，成熟的管理模式与领导模型。

极牛知识变现

通过帮助工程师打造个人品牌，从出书、录课、企培等形式帮助知识变现。

极牛训练营

面向社群成员的线下课程，技术架构、团队管理、商业模式、塑造个人品牌等。

极牛众星计划

社群中优秀的工程师将会被受邀签约极牛众星计划，平台辅助进行品牌孵化。

更多内容敬请期待

华云信安

以人才梯队为依托，以自主创新为核心，深耕网络空间安全产业

华云信安(深圳)科技有限公司（简称 华云信安™ ）成立于2016年，是一家深耕于网络空间安全领域，拥有自主研发能力及核心知识产权，提供网络安全解决方案与技术服务的高新技术企业。华云信安™总部位于深圳，在广州、上海、武汉设有分支机构，公司核心团队来自奇安信、网易、华为、绿盟、思科等国际知名科技企业，具有深厚的网络安全技术实力和管理经验。

华云信安™目前拥有数十项计算机软件著作权和十余款自主研发产品，具备“风险评估类”和“安全工程类”两项信息安全服务资质，通过ISO9001质量管理体系认证，现为深圳市信息安全行业协会理事单位和深圳市信息网络安全管理协会会员单位。

华云信安™凭借创新的网络安全产品体系、深厚的网络安全服务能力以及丰富的服务经验，为互联网、金融、能源、制造、交通、医疗、政务等领域的广大客户，提供专业优质的网络安全产品、网络安全解决方案和网络安全技术服务。

网络犯罪研究中心

华云信安·网络犯罪研究中心，是专注于打击网络犯罪的安全服务部门，致力于打击涉网新型犯罪领域的安全技术研究与产品研发，包括涉网犯罪案件技术支撑、网络诈骗案件技术支撑、涉众型经济犯罪案件技术支撑等，以攻防实验室和极牛技术社群组成创新型的安全研究团队，为国家及各省市公安机关提供高效专业的打击涉网犯罪情报分析服务和实战解决方案。

极牛攻防实验室

华云信安·极牛攻防实验室，由内部成员及外部知名技术专家团队组成，致力于最前沿网络安全技术的研究和调研，以指导技术研发路径和产品发展方向。其职责除开展传统的网络安全技术研究外，还跟踪国内外网络安全技术趋势并进行相关技术研究。现已协助国家互联网应急中心(CNcert)发现并修复数百个安全漏洞，获得数十张高危原创漏洞证明证书。

涉网犯罪对抗　护网重保服务　安全咨询服务　安全保障服务　安全培训服务

丰富的解决方案

我们提供卓越、丰富的信息安全产品及各行业解决方案、信息安全技术服务和基础架构咨询服务。

专业的团队服务

我们拥有资深、专业的服务团队，按需为用户提供多元化、多级别的咨询规划服务和技术实施服务。

众多的行业案例

我们拥有众多行业应用案例，包括制造、快消、航空、金融、物流、建筑、服务、互联网等行业。

深入的厂商合作

我们与多家国内外知名厂商建立战略合作关系，共同致力于优质解决方案及相关服务的推广落地。

全国范围的服务

我们公司总部在深圳，同时在上海、广州、武汉等设有分支机构，具有全国范围内的业务服务能力。

公众号 小程序 官网

网安观察

没有网络安全就没有国家安全



7436084028