极牛网络安全通讯 • 社群期刊

2024 年 10 月 第 40 期

网安观察

第 40 期

2024年10月

CONTEN

目录

安全态势

国际视野

P9 以色列黑入贝鲁特机场塔台，阻止伊朗飞机降落

CONTENTS

专题报道

第40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

政策篇

国内，数据产业发展与安全政策层出不穷，近一个月已发布近十项。国务院公布《网络数据安全管理条例》，两办发布《关于加快公共数据资源开发利用的意见》，国家数据局就促进数据产业高质量发展征求意见，发改委等部门就数据资源开发发布多份文件；

国际上，人工智能安全受关注。美国加州《前沿人工智能模型安全创新法案》未通过签署而流产，法德网络安全机构联合发布人工智能编程助手安全使用指南。

国内

国家发改委《公共数据资源登记管理暂行办法》公开征求意见

10 月 12 日，国家发展改革委会同有关部门起草了《公共数据资源登记管理暂行办法》，现向社会公开征求意见。该文件共 5 章 27 条，包括总则、登记要求、登记程序、登记管理、监督管理。该文件提出，公共数据资源登记应当维护国家安全和公共利益，保护国家秘密、商业秘密、个人隐私和个人信息权益，遵循依法合规、公开透明、标准规范、安全高效的原则。该文件要求，登记机构应建立健全数据资源登记管理责任机制，履行数据安全保护义务，妥善保管登记信息，登记主体在申请登记前应当自行或委托第三方专业服务机构，通过技术手段在保障安全的前提下，对公共数据资源进行存证，确保来源可查、加工可控。

国家数据局《公共数据资源授权运营实施规范（试行）》公开征求意见

10 月 12 日，国家数据局会同有关部门研究起草了《公共数据资源授权运营实施规范（试行）》（公开征求意见稿），现向社会公开征求意见。该文件共 7 章 26 条，包括总则、基本要求、方案编制、协议签订、运营实施、运营管理、附则。该文件提出，公共数据资源授权运营应遵循依法合规、公平透明、公益优先、合理收益、安全可控的原则。该文件要求，实施机构应建立健全管理制度，明确数据分类分级安全保护要求，加强技术支撑保障和数据安全管理；运营机构应履行数据安全主体责任，加强内控管理、技术管理和人员管理，不得超授权范围使用公共数据资源，严防数据加工、处理、运营、服务等环节数据安全风险。实施机构、运营机构应通过管理和技术措施，加强数据关联汇聚风险识别和管控，保障数据安全。

住建部公布《“数字住建”建设整体布局规划》

10 月 12 日，住房和城乡建设部公布《“数字住建”建设整体布局规划》。该文件提出，到 2027 年底，“数字住建”建设取得显著成效，一体化数字基础设施和数据资源体系建成运行，数字化政策标准和安全防护支撑能力明显提升。该文件要求坚持安全可控原则，落实网络和数据安全主体责任，构建制度、管理和技术衔接配套的安全防护体系，强化基础设施、数据资源和应用平台等安全保障能力，守牢网络和数据安全底线。

中共中央办公厅、国务院办公厅发布《关于加快公共数据资源开发利用的意见》

10 月 9 日，中共中央办公厅、国务院办公厅联合发布《关于加快公共数据资源开发利用的意见》。该文件共 6 章 17 条，其中第 12 条要求加强安全管理。具体包括强化数据安全和个人信息保护，加强对数据资源生产、加工使用、产品经营等

开发利用全过程的监督和管理。建立健全分类分级、风险评估、监测预警、应急处置等工作体系，开展公共数据利用的安全风险评估和应用业务规范性审查。运营机构应依据有关法律法规和政策要求，履行数据安全主体责任，采取必要安全措施，保护公共数据安全。加强技术能力建设，提升数据汇聚关联风险识别和管控水平。依法依规予以保密的公共数据不予开放，严格管控未依法依规公开的原始公共数据直接进入市场。

《网络安全技术 办公设备安全规范》等 9 项网络安全国家标准获批发布

10 月 9 日，根据 2024 年 9 月 29 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2024 年第 22 号），全国网络安全标准化技术委员会归口的 9 项国家标准正式发布。具体包括《网络安全技术 信息安全控制》《网络安全技术 网络和终端隔离产品技术规范》《网络安全技术 办公设备安全规范》《网络安全技术 智能门锁网络安全技术规范》《网络安全技术 实体鉴别 第 2 部分：采用鉴别式加密的机制》《网络安全技术 消息鉴别码 第 2 部分：采用专门设计的杂凑函数的机制》《网络安全技术 杂凑函数 第 1 部分：总则》《网络安全技术 杂凑函数 第 2 部分：采用分组密码的杂凑函数》《网络安全技术 杂凑函数 第 3 部分：专门设计的杂凑函数》。

我国工业互联网安全领域首批国家标准发布

10 月 8 日，根据 2024 年 9 月 29 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2024 年第 22 号），全国通信标准化技术委员会归口的《工业互联网企业网络安全 第 1 部分：应用工业互联网的工业企业防护要求》《工业互联网企业网络安全 第 2 部分：平台企业防护要求》《工业互联网企业网络安全 第 3 部分：标识解析企业防护要求》三项工业互联网企业网络安全国家标准发布。这三项标准聚焦三类工业互联网企业网络安全防护需求，提出不同级别企业的网络安全防护要求，为企业实施工业互联网安全分类分级管理工作提供指导，是我国实施工业互联网企业网络安全分类分级管理与防护工作的创新成果与经验总结。

国家发改委等六部门联合印发《国家数据标准体系建设指南》

10 月 8 日，国家发展改革委、国家数据局、中央网信办、工业和信息化部、财政部、国家标准委联合印发《国家数据标准体系建设指南》。该文件提出，到 2026 年年底，基本建成国家数据标准体系。该文件以数据“供得出、流得动、用得好、保安全”为指引，从基础通用、数据基础设施、数据资源、数据技术、数据流通、融合应用、安全保障等 7 个部分，加快构建数据标准体系，全面指导数据标准化工作开展。其中，安全保障部分包括数据基础设施安全、数据要素市场安全、数据流通安全三方面。

国务院公布《网络数据安全管理条例》

9 月 30 日，国务院总理李强签署国务院令，公布《网络数据安全管理条例》，自 2025 年 1 月 1 日起施行。该文件共 9 章 64 条，包括总则、一般规定、个人信息保护、重要数据安全、网络数据跨境安全管理、网络平台服务提供者义务、监督管理、法律责任、附则。该文件主要规定了五方面内容，一是提出网络数据安全管理总体要求和一般规定；二是细化个人信息保护规定；三是完善重要数据安全制度；四是优化网络数据跨境安全管理规定；五是明确网络平台服务提供者义务。

《网络安全技术 统一威胁管理产品（UTM）技术规范》等 15 项国家标准公开征求意见

9 月 30 日，全国网络安全标准化技术委员会归口的 15 项国家标准已形成标准征求意见稿，现公开征求意见。这批标准包括《网络安全技术 公钥密码应用技术体系框架》和 14 项网安产品技术规范标准，分别为《网络安全技术 统一威胁管理产品（UTM）技术规范》《网络安全技术 身份鉴别产品技术规范》《网络安全技术 数据泄露防护产品技术规范》《网络安全技术 终端接入控制产品技术规范》《网络安全技术 负载均衡产品技术规范》《网络安全技术 网络型流量控制产品技术规范》《网络安全技术 USB 移动存储介质管理系统技术规范》《网络安全技术 信息过滤产品技术规范》《网络安

全技术 电子文档安全管理产品技术规范》《网络安全技术 终端安全监测产品技术规范》《网络安全技术 日志分析产品技术规范》《网络安全技术 安全配置检查产品技术规范》《网络安全技术 数据销毁软件产品技术规范》《网络安全技术 抗拒绝服务攻击产品技术规范》。

《网络安全标准实践指南——学术科技服务平台数据安全要求》公开征求意见

9 月 30 日，全国网络安全标准化技术委员会秘书处组织编制了《网络安全标准实践指南——学术科技服务平台数据安全要求（征求意见稿）》，现公开征求意见。该文件规定了学术科技服务平台数据安全保护要求，提出了学术科技服务平台运营者应履行的安全责任和义务，适用于规范学术科技服务平台运营者数据处理活动，也可为有关主管监管部门组织开展相关检查评估提供参考。该文件不适用于涉及国家秘密的数据。

《工业和信息化领域数据安全合规指引》公开征求意见

9 月 29 日，中国钢铁工业协会、中国有色金属工业协会、中国石油和化学工业联合会、中国电子信息行业联合会、中国通信标准化协会、中国通信企业协会等十七家行业组织共同编制《工业和信息化领域数据安全合规指引（征求意见稿）》，现面向成员单位公开征求意见。该文件共 9 章，包括概述、数据分类分级、数据安全管理体系、数据全生命周期保护、数据安全风险监测预警 & 报告 & 处置、数据安全事件应急处置、数据安全风险评估、数据出境、数据交易。该文件聚焦数据处理者在履行数据安全保护义务过程中的难点问题，明确数据安全合规依据，提供实务指引，指导数据处理者开展数据安全合规管理，以提升数据安全保护能力。

国家数据局《关于促进数据产业高质量发展的指导意见》公开征求意见

9 月 27 日，国家数据局会同有关部门研究起草了《关于促进数据产业高质量发展的指导意见》，现向社会公开征求意见。该文件共 9 章，包括总体要求、加强数据产业规划布局、培育多元经营主体、加快数据技术创新、提高数据资源开发利用水平、繁荣数据流通交易市场、强化基础设施支撑、提高数据领域动态安全保障能力、优化产业发展环境。该文件在安全保障部分共两方面。一是创新数据安全产品服务。推动基础设施安全、数据安全、应用安全协同发展，加强身份认证、数据加密、安全传输、合规检测等技术创新，培育壮大适应数据流通特征和人工智能应用的安全服务业态。支持企业创新数据分类分级、隐私保护、安全监测、应急处置等数据安全产品和服务。二是加强动态数据安全保障。扩大数据空间、区块链、隐私计算等可信流通技术及模式应用范围，增强数据可信、可控、可计量开发利用能力。建立健全数据安全风险识别、监测预警、应急处置等相关规范，落实数据流通利用全过程相关主体的安全责任。健全数据分类分级标准，加强对涉及国家安全、商业秘密、个人隐私等数据的保护。

国家数据局《关于促进企业数据资源开发利用的意见》公开征求意见

9 月 27 日，国家数据局会同有关部门研究起草了《关于促进企业数据资源开发利用的意见》，现向社会公开征求意见。该文件共 7 章 16 条，包括总体要求、健全企业数据权益实现机制、培育企业数字化竞争力、赋能产业转型升级、服务经济社会高质量发展、营造开放透明可预期的发展环境、保障措施。该文件要求，落实国家数据分类分级保护制度要求，在防范实质性风险前提下，鼓励企业针对不同敏感级别的数据和数据处理场景，采取差异化的数据安全与合规管理措施，优化对同类型数据处理行为的内部合规审批流程。鼓励企业采用数据空间、区块链、隐私计算、匿名化等技术模式，促进数据安全流动和开发利用。

《网络安全标准实践指南——敏感个人信息识别指南》发布

9 月 18 日，全国网络安全标准化技术委员会秘书处组织编制了《网络安全标准实践指南——敏感个人信息识别指南》。该文件给出了敏感个人信息识别规则及常见敏感个人信息类

别和示例，可用于指导各组织识别敏感个人信息，也可为敏感个人信息处理和保护工作提供参考。

国际

法德网络安全机构联合发布 AI 编程助手安全使用指南

10 月 4 日，法国网络安全局（ANSSI）和德国联邦信息安全办公室（BSI）共同编制发布了《AI 编程助手》，为开发人员安全使用 AI 编码助手提供了风险和安全建议。该文件提出，在软件开发中使用 AI 编程助手可能面临敏感信息通过用户输入泄露、输出低质量或不安全的代码、供应链攻击、被攻击者滥用等风险。该文件指出，AI 编程助手无法替代经验丰富的开发人员，无节制使用此类工具，将带来严重安全隐患。该文件建议，引入 AI 工具应进行系统的风险分析，并加强质量管理。

九国网络安全机构联合发布《运营技术网络安全原则》

10 月 2 日，澳大利亚信号局网络安全中心与五眼联盟、德国、荷兰、日本、韩国的网络安全机构联合发布《运营技术（OT）网络安全原则》，阐述了指导创建和维护安全、可靠的关键基础设施 OT 环境的六项原则，包括安全至上（确保系统安全）；了解业务至关重要（了解并保护关键系统）；OT 数据极其宝贵且需要保护（保护 OT 数据）；将 OT 与其他所有网络进行隔离和分段（守好边界关紧后门）；供应链必须安全（确保网络安全供应链）；人员在 OT 网络安全中至关重要（人员是第一道防线）。

欧盟发布《数据治理法案》指导文件，进一步明确非个人数据跨境流动规则

9 月 24 日，在《数据治理法案》推出一周年后，欧盟委员会发布了一份关于实施《数据治理法案》的指导文件。该文件明确指出，《数据治理法案》的适用范围包括个人数据和非个人数据。对于个人数据，《通用数据保护条例》和《电子隐私条例》将同时适用。该文件重申，《数据治理法案》不会修改《通用数据保护条例》，也不涉及《通用数据保护条例》中监管机构的作用。该文件还指出，在非个人数据跨境流动规则方面，《数据治理法案》仅为非个人数据的跨境转移设定规则，个人数据的跨境转移仍受《通用数据保护条例》第五章规定的约束。

美国拟禁用中国、俄罗斯智能网联汽车软硬件

9 月 23 日，美国商务部工业与安全局发布《保障信息和通信技术及服务供应链：网联汽车》的拟议规则通知，并于 9 月 26 日正式公布了文本，面向公众征求意见。该文件提出了一项规则，旨在解决由于某些外国对手（如中国和俄罗斯）设计、开发、制造或供应的信息和通信技术及服务用于网联汽车而带来的国家安全风险。该文件重点关注集成到车辆连接系统（VCS）中的硬件和软件（如蓝牙、卫星、蜂窝和 Wi-Fi 模块）及集成到自动驾驶系统（ADS）中的软件。这些关键系统通过特定的硬件和软件，可以在网联汽车中实现外部连接和自动驾驶功能。该文件将禁止 2027 年款的车辆进口 VCS、ADS 软件，以及 2030 年款的车辆进口硬件。小规模生产者可能会获得豁免，以防止行业混乱。

美国 CISA 发布《联邦民事行政部门运营网络安全协调计划》

9 月 16 日，美国网络安全与基础设施安全局（CISA）发布《联邦民事行政部门（FCEB）运营网络安全协调计划》，以指导对各 FCEB 的协调支持和服务，推动优先事项有效开展，协调集体运营防御能力。该计划包括五个优先事项，资产管理、漏洞管理、可防御架构、网络供应链风险管理、事件检测与响应。该计划并非一份全面清单，而是旨在将资源集中在可实质推动运营网络安全改进和协调目标的行动上。CISA 表示，通过与各 FCEB 合作共同推进计划，将实现美国联邦机构网络安全现代化。

事件篇

网络物理战迈向新范式，颠覆了传统的网络战认知。黎巴嫩寻呼机遭远程攻击大规模爆炸，致使 9 人死亡数千人受伤；以色列黑入贝鲁特机场塔台，阻止伊朗飞机降落；多个政府机密系统遭 APT 组织攻破，物理隔离不等于绝对安全。

广东省教育厅短信平台遭入侵，向师生家长群发非法链接短信

10 月 12 日综合消息，广东省教育厅发布声明称，发现有不法分子入侵该部门短信平台，以“广东省教育厅”的名义向师生和家长发送包含非法链接的短信。该部门已第一时间向公安机关报案，并配合开展调查。请广大师生和家长提高警惕，切勿点击短信中的非法链接，避免个人信息泄露或遭受财产损失。此前，社交媒体上有多位用户表示，收到一条来自“广东省教育厅”的短信，写着“深夜必备成人电影戳链接”与非法内容链接。

南昌市某企业 IP 疑被黑客远控并滥用，当地网信办罚款 5 万元

9 月 30 日网信南昌公众号消息，南昌市网信办在日常的网络安全监测中发现，属地企业所属 IP 疑似被黑客远控，频繁对外发起网络爆破攻击。经过立案调查、现场勘验、远程勘验（采样技术分析）、笔录问询等工作，查明：1. 该企业未履行网络安全保护义务，未对运营的网络及信息系统开展网络安全等级保护测评等相关工作，并采取防范计算机病毒和网络攻击等危害网络安全行为的技术措施；2. 该企业未及时处置计算机病毒、网络攻击等安全风险，所属终端感染木马病毒，持续对外发起网络攻击，导致产生危害网络安全的后果。相关行为违反了《中华人民共和国网络安全法》第二十一条、第二十五条的规定。9 月 29 日，南昌市网信办依据《中华人民共和国网络安全法》第五十九条的规定，对该企业作出罚款 5 万元、对直接负责的主管人员罚款 1 万元的行政处罚。

打破物理隔离！多个政府机密系统遭 APT 组织攻破

10 月 8 日 BleepingComputer 消息，欧洲网络安全厂商 ESET 发布报告称，名为 GoldenJackal 的 APT 组织成功攻破了欧洲政府机构的气隙隔离系统。该组织至少成功实施了两起攻击行动，第一起发生在 2019 年 9 月和 2021 年 7 月，目标是某南亚国家驻白俄罗斯大使馆。第二起针对的是一个欧洲政府机构，发生在 2022 年 5 月至 2024 年 3 月之间。黑客使用了两套自定义工具集窃取了大量敏感数据，包括电子邮件、加密密钥、图像、档案及文件。此前 2023 年 5 月，卡巴斯基发布关于 GoldenJackal 组织攻击活动的报告，指出该组织专注于政府和外交机构，主要目的是进行间谍活动。

美国水务巨头遭网络攻击：水计费系统瘫痪，上千万人无法处理账单

10 月 8 日 The Record 消息，美国水务公司（American Water Works）7 日发布 SEC 文件称，其供水和废水设施未受到上周发生的网络攻击影响。该公司管理层在网站上警告，为遏制此次攻击采取了停用和隔离措施，客户目前无法访问用于管理个人账户和支付水费的门户网站。目前公司的 MyWater 账户系统已瘫痪，所有客户预约的服务将被重新安排。所有账单处理已暂停，直至另行通知。但是，系统恢复上线之前，不会产生逾期费用或停止服务。该公司的呼叫中心也无法正常运作。美国水务公司是美国最大的受监管水务公共事业公司。

科威特卫生部被黑，致使国内多个医疗服务中断

9 月 27 日 The Record 消息，中东国家科威特的卫生部日前遭遇网络攻击，导致该国多家医院的系统瘫痪，国家医疗应用 Sahel 也因此下线。截至 9 月 26 日下午，卫生部官网仍处于瘫痪状态。该部门通过科威特通讯社发布声明称，政府通过备份数据，已经成功恢复了科威特癌症控制中心的系统，以及国家健康保险和外籍人员体检管理办公室的相关系统。声明还称，黑客未能攻入“核心数据库”，但为进行必要的安全更新，卫生部不得不暂时关闭部分系统。卫生部没有提供系统全面恢复的确切时间表，仅表示恢复工作将很快完成。目前尚无任何勒索软件组织对这次攻击事件宣称负责。

以色列黑入贝鲁特机场塔台，阻止伊朗飞机降落

9 月 28 日 Middle East Monitor 消息，黎巴嫩贝鲁特国际机场的控制塔台疑似遭以色列网络攻击，导致一架伊朗民航班机未能降落，被迫返回德黑兰。黎巴嫩交通部长阿里 · 哈米向黎巴嫩媒体《An-Nahar》透露，以色列国防军拦截了贝鲁特机场控制塔的无线电通信，并威胁称，如果这架伊朗飞机降落，将攻击机场基础设施。以色列媒体《耶路撒冷邮报》也报道称，以色列军方入侵了贝鲁特控制塔的通信系统，警告一架来自“卡西姆航空”的货运飞机，航班号为 QFZ9964，在其准备降落时发出警告。以色列军方声称，贝鲁特国际机场被用作向真主党输送武器的入口，但黎巴嫩当局对此予以否认，强调机场是完全用于民用的基础设施。

英国主要火车站紧急关停公共 Wi-Fi：因被黑后传播恐怖主义信息

9 月 26 日英国卫报消息，由于发生“网络安全事件”，英国境内 19 个主要火车站宣布暂停提供 Wi-Fi 服务，其中伦敦有 10 个车站受到影响。有乘客在皮卡迪利站连接 Wi-Fi 时，被引导到一个标题为“我们爱你，欧洲”的网页。该网页包含了反伊斯兰的信息，以及关于英国和欧洲几起恐怖袭击的详细内容。英国铁路网公司（Network Rail）的发言人表示，“我们正在应对影响铁路网公司管理的车站公共 Wi-Fi 的网络安全事件。由于 Wi-Fi 服务由第三方提供，调查期间该服务已被暂停。”为该公司提供 Wi-Fi 服务的 Telent 公司表示，Wi-Fi 登录页面遭遇“未经授权的更改”，该更改是通过该网页供应商 Global Reach 公司的“合法管理员账号”进行的。稍晚时候，英国交通警察局表示，一名受雇于 Global Reach 的男子已因涉嫌违反《1990 年计算机滥用法》被捕。

美国汇款巨头速汇金遭网络攻击，支付服务中断约 5 天

9 月 24 日 BleepingComputer 消息，全球第二大汇款公司速汇金（MoneyGram）23 日发布公告称，自 9 月 20 日以来，该公司由于遭受网络攻击，导致系统故障和支付服务中断。公告中指出：“速汇金近期发现了一个影响我们部分系统的网络安全问题。我们在发现问题后，立即展开调查，并采取了保护措施应对此次事件，其中包括主动下线部分系统，这对网络连接产生了影响。”该公司此前一直声称这是一次“网络故障”，直到 23 日才披露是一次“网络安全事件”，但并未披露攻击细节，媒体认为该事件的特征与勒索软件攻击极为类似。25 日下午，速汇金在 X 平台上称，许多代理合作伙伴的汇款和收款服务已经恢复，待处理的交易正在陆续完成，公司将继续恢复剩余的其他服务，包括官方网站。

背调公司发生超大规模数据泄漏，一亿美国人隐私信息暴露

9 月 23 日 Cybernews 消息，网络安全研究机构 Cybernews 发现，美国背景调查和公共记录服务公司 MC2 Data 发生了大规模数据泄露事件，由于数据库没有设置密码保护，暴露了该公司 2.2TB 的敏感数据。这些数据中包含超过 1 亿美国公民的个人信息，涉及姓名、电

子邮箱、电话号码、家庭住址、加密的密码、部分支付信息、房产记录、法律记录、就业经历、家庭亲戚及邻居信息等，严重威胁了个人隐私与信息安全。这是 Facebook（2019 年 5 亿）和 Linkedin（2021 年 7 亿）之后，近年来美国发生的最严重的数据泄漏事件。MC2 Data 旗下运营的网站包括 PrivateRecords.net、PrivateReports、PeopleSearcher、ThePeopleSearchers 及 PeopleSearchUSA。这些网站通过汇集公开数据，如犯罪记录、就业历史、家庭信息和联系方式，提供背景调查服务，广泛应用于雇主、房东等作出决策时的参考。

国家安全部发文披露“台独”网军“匿名者 64”

9 月 23 日国家安全部消息，国家安全部公众号发布文章《起底“台独”网军“匿名者 64”》称，今年以来，一个名为“匿名者 64”的黑客组织，针对中国大陆和港澳地区，频繁开展网络攻击，试图获取有关门户网站、户外电子屏幕、网络电视等控制权限，进而非法上传、插播诋毁大陆政治制度和大政方针的内容，颠倒黑白，散布谣言。对此，国家安全机关立即行动，采取有效措施，处置危害隐患，消除不良影响。深入调查确认，“匿名者 64”组织并非普通黑客，而是由“台独”势力豢养的一支网军。目前，国家安全机关锁定了实施相关网络攻击活动的台湾人员身份信息，其中包括台湾资通电军现役人员罗俊铭、洪莉棋、廖韦纶。国家安全机关已依法对三人立案侦查。

供应商泄露用户数据，美国电信巨头 AT&T 被罚超 9000 万元

9 月 17 日 CyberScoop 消息，美国联邦通信委员会（FCC）与 AT&T 就 2023 年 1 月发生的重大数据泄露事件达成了一项 1300 万美元（约合人民币 9181 万元）的和解协议，该事件导致 AT&T 超过 890 万名移动客户的信息被窃取。根据和解协议，AT&T 向一家提供用于营销、账单处理和生成个性化视频内容服务的供应商共享了大量客户数据，双方签署合同明确了数据保护和删除要求，此前多年评估均显示该供应商遵循了数据删除政策，但本该被删除的数据却在 2023 年 1 月被泄露。FCC 最终认定，AT&T 对这一失误负有不可推卸的最终责任，并要求其实施安全改进计划。FCC 执法局局长 Loyaan Egal 指出，这份和解协议提醒企业，FCC 正对企业在供应链中如何确保客户数据安全进行更为严格的审查。

黎巴嫩寻呼机遭远程攻击大规模爆炸，致使 9 人死亡数千人受伤

9 月 17 日综合消息，黎巴嫩真主党 17 日发表声明，该组织多名成员携带的寻呼机当天下午发生爆炸，已造成多名黎巴嫩真主党成员死亡，并在全国范围内造成大量人员受伤。黎巴嫩公共卫生部长阿卜亚德称，爆炸已造成 9 人死亡，约有 2800 人受伤，其中约 200 人伤情危重。据悉，黎巴嫩真主党武装人员近来较为普遍地使用寻呼机，以通过这种技术含量较低的通信设备，避免以色列追踪他们的位置。此次发生寻呼机爆炸的地点主要集中在贝鲁特南郊、黎巴嫩南部及贝卡谷地等地，这些都被认为是黎巴嫩真主党据点所在地。多方消息显示，可能是真主党采购的某批次寻呼机被以色列截获篡改植入炸药，真主党未发现继续分发使用。纽约时报称，这些寻呼机在当天下午同时收到一条看似来自真主党领导层的消息，发出振动 / 蜂鸣声几秒后发生爆炸，尚不确定引爆指令是这条消息还是其他信号。

因勒索攻击泄露患者敏感数据，美国医疗巨头赔偿超 4.6 亿元

9 月 12 日 The Register 消息，美国宾夕法尼亚州大型初级医疗集团利哈伊谷健康网络（Lehigh Valley Health Network，LVHN）将支付 6500 万美元（约合人民币 4.6 亿元），以了结其患者发起的集体诉讼，此次和解金额按每人计算或为医疗数据泄露案件最高。该机构于 2023 年 2 月 6 日发现其 IT 系统遭受入侵，随后确认 ALPHV（又称 BlackCat）团伙是这次攻击的幕后黑手。攻击者共窃取了 13.4 万名患者和员工的相关数据，数据量达数 GB。被窃取的数据包括姓名、地址、社会安全号码、州 ID 信息、医疗记录和手术照片等，甚至还有未经授权拍摄留存的患者裸露照片，并且部分已被公开发布到网上。

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...

漏洞篇

微软本月共发布了 117 个漏洞的补丁程序，经研判有 13 个重要漏洞值得关注，包括 3 个紧急漏洞、9 个重要漏洞、1 个中危漏洞。鉴于这些漏洞危害较大，建议客户尽快安装更新补丁。

Oracle 10 月补丁日多个产品高危漏洞安全风险通告

10 月 16 日，Oracle 官方发布了 2024 年 10 月的关键安全补丁集合更新 CPU（Critical Patch Update），修复了多个漏洞。其中 Oracle WebLogic Server T3/IIOP 远程命令执行漏洞 (CVE-2024-21216)、Oracle WebLogic Server T3/IIOP 未授权数据访问漏洞 (CVE-2024-21234) 影响相对较大。奇安信 CERT 建议客户尽快自查，并应用本次关键安全补丁集合（CPU）。

CVE 编号	影响组件	协议	可否远程未授权利用	CVSS	受影响版本
CVE-2024-21216	Oracle WebLogic Server (Core)	T3/IIOP	可	9.8	12.2.1.4.0, 14.1.1.0.0
CVE-2024-21274	Oracle WebLogic Server (Console)	HTTP	可	7.5	12.2.1.4.0, 14.1.1.0.0
CVE-2024-21215	Oracle WebLogic Server (Core)	HTTP	可	7.5	12.2.1.4.0, 14.1.1.0.0
CVE-2024-21234	Oracle WebLogic Server (Core)	T3/IIOP	可	7.5	12.2.1.4.0, 14.1.1.0.0
CVE-2024-21260	Oracle WebLogic Server (Core)	T3/IIOP	可	7.5	12.2.1.4.0, 14.1.1.0.0
CVE-2024-5535	MySQL Connectors: Connectors: Connector/C++ (OpenSSL)	MySQL Protocol	可	9.1	8.0.39 and prior, 8.4.2 and prior, 9.0.1 and prior
CVE-2024-21272	MySQL Connectors: Connector/Python	MySQL Protocol	否	7.5	9.0.0 and prior

Mozilla Firefox 释放后重用漏洞安全风险通告

10 月 12 日，奇安信 CERT 监测到 Mozilla 发布公告称 Mozilla Firefox Animation timelines 释放后重用漏洞 (CVE-2024-9680) 存在在野利用，远程攻击者能够通过利用 Animation timelines 中的释放后使用漏洞在内容进程中实现代码执行。目前，此漏洞已发现在野利用。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

GitLab EE 权限绕过漏洞安全风险通告

10 月 10 日，奇安信 CERT 监测到官方修复 GitLab EE 权限绕过漏洞 (CVE-2024-9164)，攻击者可以在某些情况下，以其他用户的身份利用该漏洞在 GitLab 的任意分支上执行管道，从而可能执行恶意代码或泄露敏感信息。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 1,500,205 个，关联 IP 总数为 27,508 个。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

cups-browsed 远程代码执行漏洞安全风险通告

9 月 27 日，奇安信 CERT 监测到官方修复 cups-browsed 远程代码执行漏洞 (CVE-2024-47176)，该漏洞是由于 cups-browsed 服务在处理网络打印任务时，会绑定到 UDP 端口 631 的 INADDR_ANY 地址，从而信任来自任何来源的数据包。这会导致未经身份验证的远程攻击

者可以利用该漏洞发送特制的数据包，触发恶意请求到攻击者控制的 URL，从而在目标系统上执行任意命令。利用此漏洞需要启用 cups-browsed 服务（Ubuntu Desktop 环境下默认启用），且需要受害者主动使用该恶意 IPP 服务器配置的打印机设备进行打印操作。目前该漏洞技术细节和 PoC 已公开，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

微软 10 月补丁日多个产品安全漏洞风险通告

10 月 9 日，微软本月共发布了 117 个漏洞的补丁程序，修复了 Microsoft Management Console、Windows MSHTML Platform、Microsoft Configuration Manager 等产品中的漏洞。经研判，以下 13 个重要漏洞值得关注（包括 3 个紧急漏洞、9 个重要漏洞、1 个中等漏洞），如下表所示。鉴于这些漏洞危害较大，建议客户尽快安装更新补丁。

编号	漏洞名称	风险等级	公开状态	利用可能
CVE-2024-43572	Microsoft Management Console 远程代码执行漏洞	重要	已公开	在野利用
CVE-2024-43573	Windows MSHTML Platform 欺骗漏洞	中	已公开	在野利用
CVE-2024-43582	Windows 远程桌面协议服务器远程代码执行漏洞	紧急	未公开	较小
CVE-2024-43488	Visual Studio Code extension for Arduino 远程代码执行漏洞	紧急	未公开	较小
CVE-2024-43468	Microsoft Configuration Manager 远程代码执行漏洞	紧急	未公开	较小
CVE-2024-43583	Winlogon 权限提升漏洞	重要	已公开	较大
CVE-2024-43560	Microsoft Windows 存储端口驱动程序权限提升漏洞	重要	未公开	较大
CVE-2024-43556	Windows 图形组件权限提升漏洞	重要	未公开	较大
CVE-2024-43509	Windows 图形组件权限提升漏洞	重要	未公开	较大
CVE-2024-43615	Microsoft OpenSSH for Windows 远程代码执行漏洞	重要	未公开	较大
CVE-2024-43609	Microsoft Office 欺骗漏洞	重要	未公开	较大
CVE-2024-43581	Microsoft OpenSSH for Windows 远程代码执行漏洞	重要	未公开	较大
CVE-2024-43502	Windows 内核权限提升漏洞	重要	未公开	较大

GitLab SAML 认证绕过漏洞安全风险通告

9 月 19 日，奇安信 CERT 监测到官方修复 GitLab SAML 认证绕过漏洞（QVD-2024-40180），由于 GitLab 对 SAML 响应的不当处理，使得攻击者可以插入任意值，攻击者从而通过构造特定的 SAML 响应，绕过 GitLab 实例的身份验证机制，无需正确的凭证即可访问受保护的资源。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 1,372,328 个，关联 IP 总数为 24,944 个。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Ivanti Cloud Service Appliance 命令注入漏洞在野利用风险通告

9 月 19 日，奇安信 CERT 监测到 Ivanti Cloud Service Appliance 命令注入漏洞（CVE-2024-8190）技术细节与 EXP 已公开，该漏洞是由于后台未对传入的 TIMEZONE 参数做校验，而是直接传给 exec() 函数执行，从而导致拥有管理员权限的攻击者执行任意命令。奇安信鹰图资产测绘平台数据显示，该漏洞关联的全球风险资产总数为 11,321 个，关联 IP 总数为 2,249 个。奇安信威胁情报中心安全研究员已成功复现漏洞，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

VMware vCenter Server 堆溢出漏洞安全风险通告

9 月 18 日，奇安信 CERT 监测到官方修复 VMware vCenter Server 堆溢出漏洞（CVE-2024-38812），VMware vCenter Server 在 DCERPC 协议实施过程中存在堆溢出漏洞，攻击者可发送特制的网络数据包来触发此漏洞，从而导致远程代码执行。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 13,314 个，关联 IP 总数为 3,017 个。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

夺命寻呼机

黎巴嫩系列爆炸事件还原与解析

黎巴嫩寻呼机爆炸，是一场精心策划、利用各种技术实施的攻击行动，它是首个硬件篡改攻击，凸显供应链武器化的灾难后果，预示着“一切武器化”正成为现实。同时，这一事件使网络战和物理战争在冲突中深度融合，开启了网络战的新篇章，其影响可能将会极其深远。

事件还原：以色列如何打造现代特洛伊木马

黎巴嫩时间 9 月 17 日（星期二）下午 3 点 30 分左右，黎巴嫩真主党成员的寻呼机发出嘟嘟声，提醒其领导层有消息传来。

但这不是真主党领导人的信息，而是由真主党的死敌发出的。寻呼机信息提醒声发出几秒钟后，黎巴嫩贝鲁特南郊和其他真主党据点的数千台寻呼机同时发生爆炸。一时间，爆炸声和痛苦与恐慌的哭喊声，充斥着真主党据点的街道。

当天结束时，至少有十余人死亡，2800 多人受伤，其中许多人眼睛受伤、手指被炸断或腹部严重受伤而致残。

在寻呼机爆炸后的第二天，黎巴嫩再次发生爆炸，不过，这次爆炸的是真主党使用的对讲机，直接造成 20 余人死亡、600 多人受伤。

据路透社 10 月中旬披露，寻呼机和对讲机两次爆炸事件，在黎巴嫩共造成 39 人死亡、3400 多人受伤，其中包括真主党战士和伊朗驻贝鲁特特使。

据西方安全部门消息人士称，以色列情报机构摩萨德主导了此次寻呼机和对讲机爆炸事件。以色列既没有否认也没有证实其参与了袭击。袭击发生后的第二天，以色列国防部长约阿夫 · 加兰特称赞摩萨德取得了“非常令人印象深刻”的成果，以色列国内普遍将此解读为以色列承认该机构参与了袭击。

为何可能是以色列?

尽管以色列官员对相关指控不予置评，但大多数分析人士都认为，以色列很可能是此次袭击的幕后黑手。实际上，以色列也是少数拥有以这种方式渗透供应链的国家之一。

长期以来，真主党等伊朗支持的相关武装组织，一直受到以色列先进技术的攻击。

例如，2020 年，以色列使用通过卫星远程控制的人工智能辅助机器人，暗杀了伊朗顶级核科学家。此外，以色列还利用黑客手段阻止伊朗的核技术发展。2009 年和 2010 年，以色列与美国部署利用名为“震网”（ Stuxnet ）的计算机病毒 ，摧毁了伊朗核设施的大量离心机。

针对此次连环爆炸事件，美国国家安全局前情报分析员戴维 · 肯尼迪表示，这是其亲眼见过的规模最大、

> 以色列前军事情报部门负责人、著名战略专家阿莫斯 · 亚德林表示，此次袭击展示了“非常令人印象深刻的渗透能力、技术和情报”。

最有组织性的袭击之一。实施这一袭击所需的复杂性令人难以置信。人工情报(HUMINT) 是实现这一攻击的主要方法，同时还需要拦截硬件供应链，对寻呼机进行篡改。

以色列前军事情报部门负责人、该国著名战略专家之一阿莫斯 · 亚德林表示，此次袭击展示了“非常令人印象深刻的渗透能力、技术和情报”。

评论人士认为，袭击行动可能是为了在真主党成员中制造高度恐慌，削弱其招募人员的能力，并削弱人们对真主党领导层的信心，以及他们确保行动和人员安全的能力。

为何是寻呼机?

真主党长期以来一直宣称保密是其军事战略的基石，因此一直放弃使用高科技设备以避免以色列和美国间谍软件的渗透。与中东其他非国家组织不同，真主党部队据信通过内部通信网络进行交流。这被认为是该强大组织的关键组成部分之一，因此，长期以来该组织一直被视为国中之国。

根据美国情报评估，多年来，真主党领导人哈桑 · 纳斯鲁拉一直敦促真主党使用寻呼机。寻呼机功能有限，但可以接收数据却不会泄露用户的位置或其他信息。

据路透社报道，真主党组织在意识到手机通信遭以色列窃听后，于今年年初改用寻呼机。真主党领导人哈桑 · 纳斯鲁拉要求黎巴嫩南部的真主党成员及其家人交出手机，因为他认为以色列可以通过这些设备追踪到真主党成员的动向。

纳斯鲁拉的忧虑部分源于其盟友的报告。相关报告称以色列已经掌握了入侵手机的新手段，可以远程激活手机麦克风和摄像头来监视手机用户。真主党及其盟友之间流传着这样一种传言：任何手机通信，甚至加密短信应用，都已经不再安全。

据前以色列情报官员和中东分析师阿维 · 梅拉梅德称，正是在这样的背景下，真主党转而使用寻呼机等低端设备，认为这些设备比可能被具有 GPS 功能的手机更安全。

据两名美国情报官员透露，2024 年夏天，运往黎巴嫩的寻呼机数量有所增加，数千台寻呼机运抵黎巴嫩，分发给真主党军官及其战士。

对于真主党来说，这是一种防御措施，但以色列情报人员则将寻呼机称为可以在时机成熟时按下的“按钮”。

寻呼机是如何躲过检测的?

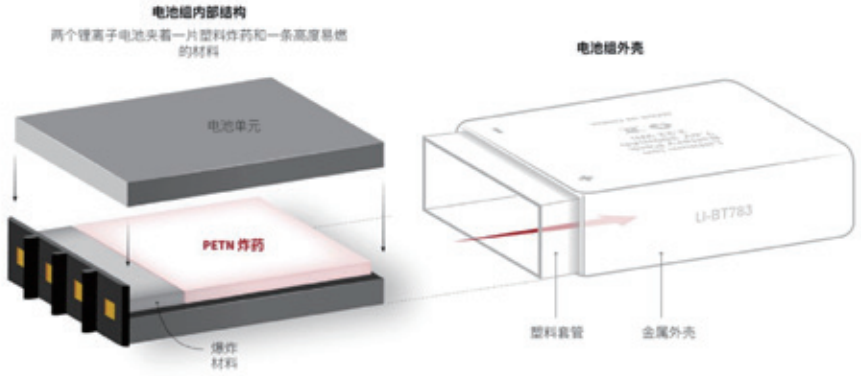
随着黎巴嫩遭受系列爆炸袭击，各界开始猜测，这些低端通信设备是如何躲过安全检测的。寻呼机炸弹和电池的秘密设计和精心策划表明，这是一次执行长达数年的长期行动。

据路透社报道，在真主党领导人纳斯鲁拉决定扩大寻呼机的使用范围之前，以色列就已开始实施这一计划。在真主党领导人要求其成员改用寻呼机之后，以色列特工看到了机会。

根据路透社发布的电池组拆卸照片，制造寻呼机的特工设计了一种电池：两个矩形电池之间暗藏了少量（6 克）但威力巨大的薄方形塑料炸药，以及一条高度易燃的物质作为雷管。由于不含任何金属成分，这种用于引爆的材料有一个优势：就像塑料炸药一样，无法用 X 光机检测出来。

据知情人士透露，在今年 2 月收到寻呼机后，真主党立即检查是否有爆炸物，并将其放入机场安检扫描仪中，看是否会触发警报。但并未发现任何可疑情况。

据电池专家表示，由于炸药和包装物占据约三分之一的体积，因此，电池



组的电量有所降低。消息人士称，真主党注意到寻呼机的电池耗电速度比预期的要快。不过，这个问题似乎并未引起重大安全担忧——真主党组织在爆炸前数小时，仍在向其成员分发寻呼机。

内部调查遭遇挫折

从外观来看，这款讯寻呼机的电源与消费电子产品中使用的普通锂离子电池组类似。然而，这种标有 LI-BT783 的电池在市场上并不存在，就像这款寻呼机本身一样。

据媒体报道，真主党的采购审查非常严格，以色列特工必须确保他们制造的寻呼机能够通过检查。

为了掩盖问题，即为这个新产品编造一个难以令人信服的故事，以色列特工建立了空壳公司，冒充寻呼机生产商，同时还创建了虚假的网上商店和页面，以欺骗真主党的检查。

为特工行动编造故事一直是间谍机构的核心技能。寻呼机的故事之所以不同寻常，是因为这些技能被运用到了无处不在的消费电子产品上。

为了欺骗真主党，以色列特工决定以合法品牌台湾金波罗公司的名义销售定制的 AR-924 型号寻呼机。爆炸事件发生后，金波罗董事长对外称，该公司是这一阴谋的受害者，对寻呼机的杀伤力及袭击真主党的行动一无所知。

该公司在声明中表示，AR294 型号寻呼机“由 BAC 咨询公司生产和销售。金波罗仅提供品牌商标授权，不参与该产品的设计或制造。”

从表面上看，BAC 咨询公司是一家总部位于匈牙利的公司，依据合同代表台湾公司金波罗生产这些通信设备。据情报官员称，事实上，该公司只是以色列特工的幌子。此外，至少还创办了两家空壳公司，以掩盖制造寻呼机者的以色列情报官员身份。

为此，BAC 咨询公司生产了一系列寻呼机。但它唯一真正重要的客户是真主党。这种暗藏 PETN 塑料炸药的寻呼机，于 2022 年夏天开始少量运往黎巴嫩，在 2024 年后产量迅速增加。

真主党领导人曾表示后悔购买了寻呼机，并展开内部调查，以了解安全漏洞是如何发生的，并找出可能的内奸。

这一仍在进行的内部调查遭遇挫折：寻呼机袭击发生 11 天后，即 9 月 28 日，负责领导采购调查的真主党高级官员纳比勒 · 卡奥克 (Nabil Kaouk) 本人在以色列空袭中丧生。

质量类似为 35 克的电池的预期能量容量约为 8.75Wh，而不是 2.22Wh。

解读：寻呼机爆炸事件颠覆了哪些网络战传统认知？

黎巴嫩 9 月 17 日、18 日连续发生寻呼机和对讲机爆炸事件，至少造成 39 人死亡，数千人受伤。黎巴嫩真主党指责对手以色列发动了这些攻击，称其已越过“所有红线”，并誓言将会实施“正义的惩罚”。外界分析普遍认为，以色列是此次爆炸行动的幕后主使，但以色列至今仍未承认对爆炸事件负责。

目前，公开来源信息还远未能揭示事件的全部真相，有关此次事件的内情可能需要有关情况解密或曝光才能完全为外界所知。本文尝试基于已经掌握的情况，从军事、政治、技术和法律角度出发，剖析事件疑点和谜题，分析攻击活动的创新性和颠覆性，并提出对新时代网络攻防态势的启示和思考。

一、事件疑点剖析

（一）爆炸物载体是什么？

目前，关于此次事件的爆炸起因，媒体、学者和专家众说纷纭、说法不一。有多种方式可以导致寻呼机、对讲机爆炸，外界对爆炸载体分析主要集中在预置微型爆炸物和通信设备本身电池上。电池爆炸的原因有多种，主要包括内部压力过大、外部加热、化学反应过快等。有观点认为，袭击者可能设法通过化学反应使设备电池过热，从而引发爆炸。

笔者认为这种观点可能性不大，原因有三：

一是曝光的爆炸视频显示，爆炸的破坏范围和烈度显然超出了电池爆炸的威力。英国前陆军军官、爆炸物处理专家肖恩 · 穆尔豪斯表示，“从视频来看，爆炸的规模与单独使用电雷管或使用含有极小高爆炸药的电雷管引起的爆炸规模相似。”

二是电池过热爆炸前应该有过渡时间，会引起大量通信设备使用者的警觉，而此次事件造成大量人员伤亡，表明爆炸的启动时间较短，使用者没有时间做出反应。

三是通信设备电池通常都具有过

热自保护措施，包括嵌入保护板等，外因诱发化学反应导致的电池过热爆炸成功率不高，与事件的实际情况明显不符。英国陆军某退役拆弹人员表示，“爆炸装置主要有五个组成部分：容器、电池、引爆装置、雷管和炸药，寻呼机上已经有三个组成部分，你只需要加上雷管和炸药。”

综合分析认为，事件中的通信设备爆炸极有可能源于设备中被预先暗藏的微型炸弹。

（二）是否源于网络攻击？

目前曝光情况反映，真主党成员使用的寻呼机几乎同时于当地时间 9 月 17 日 15 时 30 分发生爆炸。针对通信设备爆炸物的引爆机制分析集中在两个方面：一是预先设置的定时炸弹；二是网电信号指令引发的爆炸。笔者认为定时炸弹的可能性不大，原因有二：

一是从地区冲突局势上看，自事件的嫌疑幕后主使以色列与哈马斯冲突 2023 年 10 月爆发冲突以来，其与跟哈马斯站在同一战线的真主党暴力冲突不断。此次事件的通信设备约于 5 个月前购置，而事件主使不太可能未来局势不明朗的情况下选择设置定时爆炸，更可能会选择“把引线留在手中”，将装置设定为收到特定指令时才会爆炸，从而掌握主动性并避免失控态势。

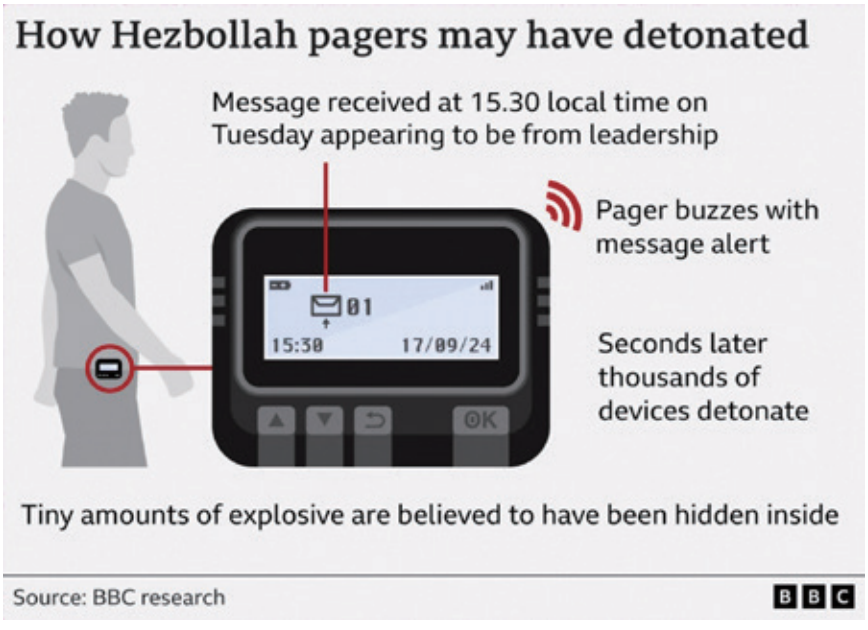
二是从技术原理上看，寻呼机、对讲机均可接收网电信息，为择时引爆内置炸药提供了方便途径和渠道。情况反映，携带寻呼机的人员听到传呼机发出提示音，收到被认为来自真主党领导人发来的信息，当他们正在阅读这些信息时，寻呼机发生爆炸。

综合分析认为，事件中的通信设备爆炸促发机制很可能源于传呼机和对讲机的通信网络遭渗透，设备在接收到特定的信号或代码后发生爆炸，即“由比特数字触发的 PETN 爆炸”。

（三）是否违反国际人道法？

国际人道法基本准则涉及，“失去战斗能力、已退出战斗及未直接参与战斗的人士，其生命及身心健全均有权受到尊重。在任何情况下，他们都应受到不加任何不利区别的保护与人道对待。”“冲突各方及其武装部队成员选择战争的方法与手段均受到限制。使用具有造成不必要损失或过度伤害性质的武器或战争方法，均受禁止。”“冲突各方在任何时候均应将平民居民与战斗员加以区分，以避免平民居民及平民财产受到伤害。不论是平民居民还是平民个人，都不应成为攻击的目标。攻击应只针对军事目标。”

黎巴嫩真主党是伊朗资助成立的什



叶派黎巴嫩伊斯兰政治和军事组织，其宗旨是消灭以色列，并将西方势力逐出国内。该组织性质极具争议，其自创立以来即于国内属合法政党，但其同时被美国、英国、以色列、澳大利亚、加拿大、德国、欧盟、海湾阿拉伯国家合作委员会等国列为恐怖组织。

从结果事件影响来看，此次攻击行动显然违背了国际人道法，原因在于：此次攻击爆炸针对是真主党订购的数千台寻呼机、数百台对讲机的拥有者，行动的针对性只能说是“相对集中和精准”，体现出控制范围和烈度意图，但未充分考虑设备拥有者的身份（是否战斗人员）、所在位置（住宅、汽车、杂货店或咖啡馆）和周围环境（周围是否有平民人员或目标），在动用武力手段实现军事目标过程中未区分平民目标和军事目标，也未采取有可行措施预防平民伤害，不符合国际人道法规定的攻击中的“区分”“相称”“预防”等关键原则。

联合国人权事务高级专员福尔克尔·蒂尔克表示，国际人道法禁止使用诱杀装置，这种装置是看似无害的便携式物体，经过专门设计和制造，可以装载爆炸材料。其中，所指的“诱杀装置”是指其设计、制造或改装旨在致死或致伤，而且在有人扰动或趋近一个外表无害的物体或进行一项看似安全的行动时出乎意料地发生作用的装置或材料。

综合分析认为，此次行动针对数千台设备持有目标人员实施无差别爆炸攻击，导致非战斗人员甚至平民伤亡及平民财产损失，在适用情况下违反了国际人道法。

二、此次特别网络行动的创新性和颠覆性

（一）从行动方式来看，通过软硬供应链攻击，实现现代“特洛伊木马”计划

此次行动极有可能是某种供应链攻击，即在制造或运输过程中对寻呼机和对讲机进行篡改。供应链攻击涉及使用第三方工具或服务（统称为“供

应链”）来渗透目标系统或网络，可能针对由第三方管理的硬件、软件、应用程序或设备。

供应链攻击在网络安全领域日益受到关注，最近很多重大网络安全事件都是黑客在产品研发过程中获得访问权限导致的，如 SolarWinds 攻击、Kaseya 勒索软件攻击等。但此类攻击通常局限于软件，硬件供应链攻击则相对少见，因为这涉及对设备的人工物理接触。

美国智库“新美国安全中心”的高级研究员维韦克·奇尔库里表示，“两轮攻击都可能起源于所谓的供应链攻击：在寻呼机和对讲机的生产节点，就被渗透了。少量的爆炸性物质被添加到这两种设备中，让它们在特定时间被远程引爆。”前英国军队弹药专家表示，这些设备可能在假电子元件中隐藏了 10~20 克的军用级高爆炸药。1996 年和 2000 年，哈马斯的主要炸弹制造者叶海亚 · 阿亚什及法塔赫活动家萨米赫 · 马拉比均死于“手机炸弹”，以色列军事和情报机构被认为是事件的幕后策划者。上述两次猎杀行动可被视为此次爆炸事件的“先锋”，而此次爆炸袭击的不同之处在于其规模更庞大。

除硬件篡改外，此次行动还可能涉及对设备应用程序的操纵及通信渠道的入侵。

综合来看，此次爆炸事件可被视为基于供应链渗透和设备武器化的成功网电攻击行动，其行动方式新颖且大胆，具有与“震网”攻击、“手机炸弹”攻击相类似的元素，如人力介入、硬件接触和设备篡改等，符合以色列军情和情报机构的行事风络，也反映出以色列网电攻击手段的创新和发展。

（二）从毁伤效果来看，通过动能与非动能打击相结合实现“目标斩伤”

从历史来看，军事战争主要是通过使用物理力量来破坏或摧毁物质资产，所使用主要是动能武器。进入现代信息化战争时代，网络战、电子战、定向能和信息战等非动能效应手段也在不断发展，并为动能攻击手段提供了补充。网络攻击通常造成的影响是非动能数字损害，包括系统停转、信息被资、数据泄露，以及由此衍生的服务停顿、物理损害、经济损失、名誉受损等，鲜见由网络攻击直接引发的人员伤亡和财产物理损失。美军联合出版物 JP 3-0 号《联合作战》认为，网络空间攻击是一种可产生非致命效果的能力，能产生这种效果的还包括电子攻击、军事信息支援作战及非致命武器。

对比来看，动能攻击与网络攻击的主要区别包括：

一是动能攻击的介入和效果具有瞬时性（如发射导弹并摧毁目标），而非动能网络攻击手段则具有跨时性，如需要长时间来对目标开展情报侦察、研制网络攻击武器、获取目标访问权限、渗透并植入攻击载体、实施攻击行动等；

二是动能攻击产生的物理损伤效果几乎是不可逆的（如射杀人员、炸毁建筑物等），而网络攻击的效果则可以产生完全可逆的效果（如恢复系统运转等），可逆性既是网络武器的优势、也是其局限性；

三是动能攻击影响具有局限性，通常限定于一定范围的物理区域内，而网络攻击则具有广泛性和衍射性，可对广域分布式目标实施攻击并产生级联效应；

四是动能攻击的效果具有量化可预测性（如导弹的毁伤半径等），而网络攻击的效果可能因目标软件、硬件和用户配置的变化而具有不确定性。

此次爆炸行动开创了动能攻击与网络攻击深度融合的先河，展现出俄乌网络战争从未呈现的新型网络技战术，并取得了“先发制人”式闪击效果，除造成大量真主党成员伤亡外，还破坏了真主党指挥通信网络，是一次现代战争的成功网络战战例。

此次爆炸行动还彰显出网络攻击在现代战争中的威力还远未得到挖掘释放，其不仅是军事行动的一种火力形式，在与动能攻击相结合的情况下，还能产生“互相补充、力量倍增”的效果，在保留动能攻击效果不可逆、量化可预测的基础上，还能突破时空限制，瞬时对广泛、大量目标实施打击，以达到最大作战效果。

未来，动能与网络攻击手段的结合可能在常规战争冲突的重要军事战略工具，为国家实现军事目标提供新的渠道。

（三）从资源统筹来看，通过情报、人力和技术相结合实现缜密部署

此次通信设备爆炸行动是一次特种作战行动，事先必然经过长期和缜密的策划，并对情报、人力和技术等大量资源进行综合性、精准性统筹和调度。专家认为，此次爆炸的策划准备可能需要数月到数年的时间，需要动用大量人力、物力资源。前美国网络司令部司令保罗·中曾根表示，此次爆炸行动展示“令人震惊”的情报收集能力，肇事者“拥有令人难以置信的情报定位能力，能够真正了解这些号码，知道谁拥有这些号码，并且知道他们使用这些号码的频率”；对真主党的秘密袭击表明了对其成员的“透彻了解”，并且对目标“非常熟悉”。纽约大学学者尼古拉斯·里斯认为，此次攻击的复杂程度表明，肇事者长期以来一直在收集情报。英国皇家国际事务研究所的莉娜·哈提卜表示，此次袭击表明，以色列已经“深度渗透”了真主党的通信网络。

从攻击的规模来看，策划实施此次攻击需要几个方面：

一是精确的情报信息。需要获取目标人员使用的设备信息（型号、配置等）、采购设备的渠道，以及通信设备操作机制和所运行网络，开发能够确认目标携带设备的情报来源。

二是成功的人力介入。需要建立必要的人力关系和渠道，获得寻呼机、对讲机的物理访问权限，并对设备进行物理篡改及在设备系统中建立立足点。

三是可行的技术操作。需要对目标设备开展技术分析，开发将爆炸物

嵌入设备的技术及通过网信手段引爆爆炸物的技术，具备在执行前不被发现地渗透和操纵该通信设备网络的能力，且极可能提前对整体行动进行了技术测试和验证。

此次复杂爆炸攻击行动涉及环节众多，资源协调统筹及相互配合的难度极大，任何环节或要素出错都可能导致行动失败，在部分要素上完全可以与“震网”攻击行动相媲美，是一次网络战、渗透战和情报战的成功结合。网信攻击手段可能只是此次爆炸行动的“最后扳机”，由人力、情报手段支撑的设备改造、行动决策、部署实施则为行动成功实施奠定了基础。

此次行动体现出，现代网络战并非单纯的技术战，还必须要有精确的情报作为支撑，并在适用的情况下结合人力特种行动，才能保障网络行动的成功实施。

（四）从行动影响来看，通过热战、网战和心战相结合实现跨域辐射。

两轮爆炸袭击粉碎了真主党煞费苦心建立的低技术通信网络，而以色列在事件前就已经破坏了真主党其他形式的现代通信网络。此次爆炸行动既削弱了真主党力量，也对该组织士气造成极大打击。事件不仅让真主党感到危机四伏，也让黎巴嫩民众人人自危，担心任何电子设备都可能被外敌动了手脚。有报道称，爆炸开始后的最初时刻，众多黎巴嫩民众惊慌失措，拔掉了家里的路由器甚至电视机的插头，担心爆炸物可能已经渗透到家用电器。

网络风险咨询公司 SecDev Group 联合创始人罗布·穆加表示，“这次史无前例的袭击，削弱了真主党对其通信电子设备和更广泛的第三方供应链的信心。这也严重削弱了真主党的沟通能力。”美国智库“新美国安全中心”的高级研究员维韦克·奇尔库里表示，“我认为以色列发出的信息是，即使真主党试图转向技术含量较低、本以为更安全的通信替代品，也仍然很容易受到攻击。‘我们仍然可以在你的口袋里找到你，无论你在哪里。’这对真主党的安全感产生了巨大的心理影响。”美国东北大学国际安全问题专家麦克斯·亚伯拉罕表示，“以色列的寻呼机袭击是一次非常有效的心理作战。它传达了一个信息：‘我们比你聪明。我们可以以你甚至没有意识到、甚至不理解的方式攻击你。如果你越界，你会以闻所未闻的方式付出代价，悔恨不已’。”

可见，此次爆炸行动集成了动能战、网络战和心理战，攻击发生在网信域，作用发生在物理域，影响发生在认知域。行动在物理域、信息域和认知域均对真主党造成了破坏性影响，达到了“一举三得”的效果。

在物理域，通过动能爆炸杀伤了真主党成员并破坏了其所用通信设备，影响了该组织的组织动员能力和指挥控制网络；

在网信域，渗透了真主党通信渠道，并瓦解了其通信网络，造成其内部互相猜疑，并迫使其另行布建新的通信网络；

在认知域，打击了真主党的士气，并干预了真主党成员的感知、认知、情绪、情感、观念、信念等意识活动，影响了真主党高层的决策权衡。

三、启示与思考

（一）网络攻击形式创新性或将开启网络战新篇章

此次爆炸行动可以被视为网络战争和物理战争原则在当今冲突中融合的经典创新案例，或将开辟网络战的新致命前沿，开启网络战争的新篇章，并预示着网络战争将发展成为比黑客攻击和间谍活动更致命的战争活动。

此次行动还标志着军事战略的一个重要转折点，表明现实世界和虚拟世界间不再有明确的界限，网络和物理元素在战争中可以无缝集成，为更致命的混合威胁敲响了警钟。此次袭击行动不仅仅是一次战术打击，还代表了战争模式的深刻转变，数字和物理领域不仅相互联系，而且融合成一个单一的、强大的战线。先前的网络战例通常破坏性较低，用于实现非关键性的动能目标，主要涉及间谍活动、数据盗窃或基础设施破坏。但能够造成物理伤害的网络攻击的能力则完全将破坏性提升至更高层次，源自数字世界的攻击威胁不再像以前那样是虚拟的、跨时的、可逆的，而是有能力对现实世界造成实际的、即时的、不可逆的影响。

此次事件体现了网络物理系统的巨大潜力和固有风险，为未来的军事行动提供了蓝图，表明网络能力不仅可用于间谍活动或破坏，还可以用作直接动能武器；或将打开网络战的“潘多拉魔盒”，启示民族国家开发新的网络战技战术，进一步推动网络空间军事化程度。

（二）国家网络安全防线建设需要树立体系化思维

此次事件将促使全球重新思考国防和安全战略，凸显强有力的网络安全措施的迫切需要，以及在数字和物理基础设施界限日益模糊的时代，不断创新以保护相互连接的数字和物理基础设施的紧迫性。

在新的时代，网络安全威胁的来源将不再局限于单个漏洞、系统或设备，构成最严重网络威胁的主体将是国家级对手。与普通黑客组织或个人相比，国家级对手能够安排、调动、整合国内人力和资源，甚至可能联合利用国际盟友力量，来实现“数字军火的大融合”。其技术能力强大，拥有成熟的网络攻击技战术，且渗透渠道多样、手法更加隐蔽。尤其是国家级对手还能动用间谍情报机关，通过对目标开展侦察获取敏感信息，通过拉扰策反等手段打入目标内部，甚至派遣特工直接实施人工操作，导致网络安全威胁更趋严峻复杂。

因此，要应对国家级对手构成的严峻威胁，必须树立体系化网络安全建设思维，变“单打独斗”为“联合作战”，集成和发挥政产学研军等各方力量，构建实战化网络安全防御体系，筑牢数字时代安全基石。

此次爆炸行动可以被视为
网络战争和物理战争原则在当今冲突中融合的
经典创新案例，
或将开辟网络战的新致命前沿，
开启网络战争的新篇章。

（三）网络安全防护需要跳出“重软轻硬”传统误区

此次攻击可能会催生一个防御创新的新时代，重点是保护供应链和通信设备免受复杂的网络物理威胁。

相比于保护网络系统、软件应用、信息数据等的复杂网络安全机制相比，终端硬件的供应链物理安全获得的关注较少。此次事件告诉我们几方面信息：

一是高科技设备和低科技设备都可能被此类袭击破坏，即使是寻呼机、对讲机等已过时的通信设备经过篡改后也可能成为发动网络攻击的致命武器；

二是电子设备遭物理入侵可能会为间谍活动、破坏行动和网络攻击打开方便大门，对国家安全造成潜在的灾难性影响；

三是网络安全防护不仅仅要保护网络、软件和信息，还要保护通信设备中的物理系统，尤其需要加强设备供应链的监察和保护。

供应链风险无法通过单一措施来消除，但多种策略相结合可以大大降低风险，包括加强国内制造业、减少外国设备依赖、强化进口检验和测试规程、采用尖端安全技术（如基于区块链的跟踪系统）、实施硬件完整性检测等，确保从原材料到生产和运输的每个阶段都受到保护，以免受到渗透。

（四）万物互联时代需扩大网络安全的内涵和外延

当今社会已进入万物互联时代，大量智能设备和基础设施都与互联网紧密相连，智能手机、无人机、物联网设备已经成为当今社会不可分隔的一部分。上述设备如果遭受攻击，可能引发更大的灾难，对军队和平民都可能造成严重致命的影响。本次黎巴嫩爆炸事件表明，网络物理攻击领域的威胁较以前认知的更加多样化，汽车、家用电器、智能手环、耳机、智能门禁、医疗设备、军用电台、关键基础设施、太空飞行器都是潜在的攻击对象。相比于应用范围较小的传统的寻呼机、对讲机，对未来更先进、更复杂、更广泛应用的技术设备的网络物理攻击，在未来网络战争中具有潜在的更大破坏性。

可以预见，万物互联将催生更多前所未有的安全问题，把网络攻击面扩大到新维度，使网络攻击场景更加多样化，导致网络安全风险程度也将上升到新高度。伴着新风险、新隐患，需要并行探索和扩展网络安全的内涵和外延，不断丰富和创新安全理念和思维，加快推动网络安全技术的研发和实践落地，构建全方位、多维度的网络安全监测与防御体系。

分析：黎巴嫩寻呼机爆炸三个特点

黎巴嫩寻呼机爆炸事件，可能是一场精心策划、利用各种技术实施的攻击行动，包括硬件供应链攻击、软件漏洞和数据窃取，显示网络攻击将发展成为比黑客攻击和间谍窃密更致命的形式。

随着网络空间和传统物理领域的战场越来越模糊，网络安全防护除了保护传统的网络、信息和隐私安全，还需要考虑保护硬件供应链的完整性。

“一切武器化”正成为现实

此前，以色列曾被指控使用篡改通信设备实施暗杀，包括 1996 年通过装有炸药的手机杀害哈马斯炸弹制造者叶海亚 · 阿亚什 (Yahya Ayyash)，但此次袭击的规模之大是前所未有的：数千部设备同时引爆。

因此，分析人士预计，以色列实施的真主党通信设备爆炸，可能开启网络空间地缘政治竞争的新阶段。

在过去数十年里，以色列经常通过利用非常规的战术和先进技术来攻击对手。2009 年，以色列和美国利用震网病毒（Stuxnet ）恶意软件针对伊朗核计划实施网络攻击。根据国际原子能机构的数据，震网病毒造成严重的破坏，2009 年至 2010 年年初，伊朗因震网病毒造成的破坏而被迫更换约 1,000 台离心机，严重打击了伊朗的核计划发展。这一事件在全球首次展示了网络武器对物理空间的重大影响。

随后，以色列国防军于 2019 年 5 月轰炸加沙地带的哈马斯技术部门，以阻止潜在的网络攻击。以色列的反应开创了先例，成为地区冲突中首个以军队实时应对网络攻击的案例。

此外，以色列还被指责针对伊朗科学家实施了长达数十年的秘密行动。据报道，以色列情报机构于 2021 年使用人工智能遥控狙击机枪杀死了顶级核科学家 Mohsen Fakhrizadeh。这是首次有记录的远程遥控此类设备。

这次攻击事件所展示的战略创新应该引起更多人的关注。它提出了一个令人不安的问题：只需要跳出固有的思维模式，像寻呼机这样简单的东西都可以武器化。长期以来，真主党一直依赖过时但安全的寻呼机通信系统，来保护敏感信息免受现代黑客技术的攻击。当这

> 爆炸事件证实了许多人猜测即将发生的事件：21 世纪冲突将出现日常物品的武器化。“一切武器化”，这种好莱坞电影惊悚片的情节，正在成为现实。

些曾用于协调军事行动的设备成为毁灭性武器时，这种看似安全的局面被打破了。信号很明确：无论多么过时或看似安全，没有哪个系统能够免受网络操纵。

可以说，黎巴嫩寻呼机和对讲机爆炸是许多人猜测即将发生的事件之一：21 世纪冲突中日常物品的武器化。“一切武器化”，这种好莱坞电影惊悚片的情节，正在成为现实。

奇安信观星实验室负责人龚玉山认为，寻呼机爆炸事件可能是未来时代战争的先兆。因为从理论上来说，所有的智能硬件设备，都能通过生产链大规模预先安装爆炸装置。

智能手机、无人机、物联网 (IoT) 设备已成为当今社会的一部分。相比寻呼机，智能手机要复杂几个数量级、电池更大、电路更复杂、传感器也更多，完全可能作为未来网络战的攻击途径。试想一下，如果所有这些更高级、更复杂的设备受到攻击，可能造成什么样的灾难?

因此，降低物联网设备、智能电子和通信设备的攻击可能性，将成为网络安全面临的一大挑战。

首个硬件篡改攻击，凸显供应链武器化的灾难后果

在网络空间，敌对各方会一直试图破坏对方的关键基础设施，包括通信网络。

尽管近年来各国互相指控对方在设备中植入后门漏洞，但黎巴嫩真主党寻呼机遭篡改，是已知的第一起在生产层面篡改硬件的案例。这暴露出供应链漏洞被武器化后将会灾难性的后果。武器和弹药情报专家、咨询公司 Armament Research Services 主任任詹森·琼斯(Jenzen-Jones)表示:“事件的规模表明，这是一次复杂的供应链攻击，而不是设备在运输过程中遭拦截和修改的场景。”

供应链攻击在网络安全领域越来越常见，但通常以软件为目标；针对硬件的攻击则少见得多，因为需要能够实现对设备的物理访问。对于缺乏国家背景的攻击组织，可能难以获得对设备制造阶段的深入访问权限，但具有国家背景的攻击者则可以通过适当的资源实现这一目标。

利用供应链漏洞的战略利益尚待商榷。但鉴于其可能造成的巨大破坏和损失，至少在短期内，将会导致更多的攻击者试图利用供应链漏洞来攻击对手。考虑到硬件供应链遍布全球各地，且缺乏严格监管，其不透明性显示了供应链的脆弱性，无意会加剧相关担忧。

科技行业和供应链分析师表示，科技公司可能会将此次攻击视为一次强烈的提醒，提醒他们确保供应链安全的重要性，而公众对科技的信任也可能受到打击。

加州州立理工大学伦理与新兴科学组主任帕特里克·林（Patrick Lin）表示，不知何时，数千个装置被制成武器，却无人察觉。这些爆炸装置分布有多广? 爆炸物是如何进入装置或装置供应链的? 这次袭击引发出了一些以前从未考虑过的可怕问题。

牛津大学数字伦理与防御技术教授马里亚罗萨里亚·塔德奥表示，攻击开创了一个令人担忧的先例，因为其中对供应链的干扰“不是出于特定的破坏行为，而是为了进行分布式、影响深远的攻击”。

迪拜科技公司 Ombori 首席执行官安德烈亚斯·哈塞洛夫 (Andreas Hassellof) 表示，爆炸事件为我们敲响警钟，“提醒我们需要彻底改革应对供应链安全的方法。”

阿布扎比网络安全公司 Cypherleak 的首席执行官穆罕默德·贝拉比 (Mohamed Belarbi) 表示：“如果一部手机或设备在到达你手中之前，在制造商或供应链层面遭到篡改，你什么也做不了。因为即使打开了一部 iPhone 或三星手机，你也难以发现问题。”

与保护当代设备的复杂机制相比，终端硬件安全却鲜受关注。美国康奈尔科技大学数字和信息法教授詹姆斯·格里梅尔曼表示：“每家生产或销售数字设备的公司都会担心其供应链的完整性。”“他们可能会考虑增加额外的保障措施和验证措施，以便能够更好地检测和阻止此类举动。”

惠普公司发布的一项全球调查显示，针对硬件供应链的攻击和设备篡改预计会增加，研究强调，企业需要关注设备硬件和固件的完整性。

安全专家认为，要减轻终端硬件安全风险，需要进一步加强电子设备的反破坏措施、确保供应链安全、建立更严格的敏感技术转让出口管制措施，并加强对网络空间负责任行为的问责制。

帕特里克·林（Patrick Lin）则认为，攻击事件会进一步加速“在一国境内自主研发技术，以加强对供应链安全控制的努力”。 澳大利亚新南威

尔士大学供应链专家米拉德·哈加尼(Milad Haghani)预计，（数字设备）将会看到一场“广泛的清算”，导致制造企业加强其供应链安全协议。 对于整个科技公司来说，这种情况的规模是前所未有的，许多公司以前可能没有如此重视其生产流程的安全性。因为许多公司可能还没有完全配备应对此类威胁的设备。

网络攻击和物理战深度融合的经典案例

寻呼机爆炸事件表明，网络战争将发展成为比传统黑客攻击和间谍窃密更致命的战争。这次攻击可以被视为网络战争和物理战争在冲突中融合的经典案例，开启了网络战争的新篇章，其影响可能远远超出当前事件。

黎巴嫩真主党通信设备爆炸，将网络战的后果带到物理领域。如果引发其他攻击者效仿，将对网络空间的稳定产生更广泛的影响。

网络战主要被定义为窃取机密信息、进行间谍活动或使主要设施失灵。这一事件以物理形态的影响展现出网络攻击的巨大威胁，表明数字世界的威胁不再像以前那样是虚拟的——它们非常有能力对现实世界造成巨大影响。此外，现实世界和虚拟世界之间不再有明确的界限，这次袭击可能是对更致命混合威胁的警告。

更令人难以置信的是，这些爆炸是通过一种越来越被视为过时的通信设备实施的。将寻呼机改装成简易爆炸装置的案例表明，即使有人认为这些装置已经过时，它们也可能具有未知的负面能力。

在大多数关于网络安全的讨论中，我们经常听到保护新的复杂系统——在此次事件中，攻击者却成功破解和利用了古老的系统，将一种简单而无害的工具变成了致命武器。真主党维护和使用这种原始系统是为了避免复杂网络攻击，但这样做却正好落入了为其设置的陷阱。

寻呼机爆炸事件表明，网络攻击的威胁比以前考虑的更加多样化。在这个几乎所有设备都相互关联的时代，通信设备故障的影响不仅对军队，而且对平民都可能造成严重致命的影响。

安全专家警告称，我们正面临一种新的威胁，这种威胁模糊了数字和物理漏洞之间的界限。信息很明确：要么适应，要么成为攻击目标。坚持使用过时安全模式的组织不仅落后，而且还会面临灾难性的后果。

（本期黎巴嫩系列爆炸事件专题由奇安信威胁情报中心、网络空间安全军民融合创新中心、奇安信观星实验室等联合供稿。）

> 这次攻击可以被视为网络战争和物理战争在冲突中融合的经典案例，开启了网络战争的新篇章，其影响可能远远超出当前事件。

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。

加拿大建立武装部队网络司令部以整合军事网络能力

编者按：9 月 26 日加拿大正式宣布成立加拿大武装部队网络司令部，从而将武装部队的网络能力整合为一个统一的专门实体，提高军队应对网络领域威胁的准备程度。

加拿大武装部队网络司令部的成立对加拿大国防部和加拿大武装部队来说是一个重要的里程碑，体现了加拿大建立专门的网络作战架构的承诺，凸显了网络能力在现代军事行动中日益增长的重要性。该司令部将成为加拿大国防部和武装部队网络行动的唯一管理机构，负责网络部队的维持、管理和发展，通过集中资源来推进与行动、人员、政策和能力相关的网络空间现有活动；包括信号情报和联合电子战，能够执行和支持一系列网络任务；除对保卫加拿大和推进其利益至关重要外，还将帮助国防团队履行北约承诺及加拿大印度－太平洋战略的网络和防御部分，如虚拟网络事件支持能力和盟国自愿提供的主权网络效应；将支持加拿大武装部队过渡到全域战场，具有更高的灵活性和对恶意网络活动的响应能力。

新司令部的成立与加拿大在北美防空司令部、“五眼”联盟和北约的主要合作伙伴和盟友的类似投资相一致。通过增强其网络能力，加拿大正在支持与其盟友的更大互操作性，更好地应对各种网络威胁，并正在推进北约的任务目标和目的。加拿大国防部长比尔·布莱尔表示，新司令部的成立向盟友、合作伙伴和对手展示了加拿大持续致力于在充满挑战的网络领域开展行动的承诺，将通过加强加拿大在网络领域的工作并推进与合作伙伴和盟友合作，来发现、阻止和防御针对加拿大和利益关切的网络威胁和恶意行为者。加拿大国防参谋长珍妮·卡里尼昂表示，加拿大国防部和武装部队将通过网络司令部继续与通信安全局密切合作，开发和扩大进攻性和防御性网络行动能力，支持战术和战略层面的网络行动。加拿大武装部队网络司令部首任司令戴夫·雅克表示，在网络领域建立决定性优势需要速度、信任、敏捷和团结的努力。

奇安网情局编译有关情况，供读者参考。

加拿大国防部长比尔·布莱尔和国防参谋长珍妮·卡里尼昂 9 月 26 日正式宣布成立加拿大武装部队网络司令部（CAFCYBERCOM）。该新司令部将把加拿大武装部队的网络能力整合为一个统一的专门实体，这将提高军队应对网络领域威胁的准备程度。

加拿大武装部队网络司令部（CAFCYBERCOM）的成立对加拿大国防部和加拿大武装部队来说是一个

重要的里程碑。该司令部体现了加拿大在“强大、安全、参与”战略中提出的建立专门的网络作战架构的承诺，凸显了网络能力在现代军事行动中日益增长的重要性。

该新司令部将由戴夫·雅克少将领导，负责网络行动及网络部队的维持、管理和发展。戴夫·雅克将利用他担任联合网络部队指挥官和通信安全局（CSE）顾问的经验，利用他的专业知识指导该机构在网络领域取得新的战略进步。

通过加拿大武装部队网络司令部（CAFCYBERCOM），加拿大武装部队继续与加拿大通信安全局（CSE）密切合作，开发和扩大其进攻性和防御性网络行动能力。加拿大武装部队和加拿大通信安全局（CSE）长期合作，开发先进的技术和专业能力，为军事行动提供情报。在过去十年中，双方的伙伴关系不断发展，包括网络安全、防御性和进攻性网络行动领域的合作。

新的加拿大武装部队网络司令部还使加拿大能够履行对北约的承诺，如虚拟网络事件支持能力和盟国自愿提供的主权网络效应。新司令部的成立与加拿大在北美防空司令部、“五眼”联盟和北约的主要合作伙伴和盟友的类似投资相一致。通过增强其网络能力，加拿大正在支持与其盟友的更大互操作性，更好地应对各种网络威胁，并正在推进北约的任务目标和目的。

高官言述

加拿大国防部长比尔·布莱尔表示，“加拿大武装部队网络司令部的成立向我们的盟友、合作伙伴和对手展示了加拿大持续致力于在充满挑战的网络领域开展行动的承诺。通过加强我们在网络领域的工作，并继续与我们的合作伙伴和盟友合作，我们可以发现、阻止和防御针对加拿大和我们利益的网络威胁和恶意行为者。”

加拿大国防参谋长珍妮·卡里尼昂表示，“通过加拿大武装部队网络司令部，加拿大国防部和武装部队将继续与通信安全局密切合作，开发和扩大进攻性和防御性网络行动能力。这一举措支持战术和战略层面的网络行动。新机构将集中资源，以便我们能够推进与行动、人员、政策和能力相关的网络空间现有活动。”

加拿大国防部副部长斯蒂芬妮·贝克表示，“我向雅克少将表示祝贺，祝贺他担任加拿大武装部队网络司令部司令。他为司令部、国防团队和所有加拿大人带来了丰富的知识、经验和领导才能。”

加拿大武装部队网络司令部司令戴夫·雅克少将表示，“在网络领域建立决定性优势需要速度、信任、敏捷和团结的努力，我很自豪被任命为致力于实现这一目标的组织的负责人。”

加拿大通信安全局局长卡罗琳·泽维尔表示，“自成立以来，加拿大通信安全局一直是加拿大武装部队的重要合作伙伴。合作对我们来说是自然而然的事情，加拿大武装部队网络司令部也不例外。这就是为什么我们要联合我们已经世界一流的外国网络作战能力，以在复杂的世界中保护加拿大。即使在和平时期，我们也面临网络战，这种伙伴关系将使加拿大人民及加拿大的盟友受益，并让我们所有人更好地了解我们每天面对的不断变化的威胁形势。”

简要事实

- 加拿大武装部队网络司令部（CAFCYBERCOM）将成为加拿大国防部 / 武装部队网络行动的唯一管理机构，负责网络部队的维持、管理和发展。
- 加拿大武装网络司令部包括信号情报和联合电子战，能够执行和支持一系列网络任务。
- 加拿大武装部队网络司令部的建立除了对保卫加拿大和推进其利益至关重要，还将帮助国防团队履行北约承诺及加拿大印度 – 太平洋战略的网络和防御部分。
- 加拿大武装部队网络司令部将支持加拿大武装部队过渡到全域战场，具有更高的灵活性和对恶意网络活动的响应能力。
- 自 2010 年以来，戴夫·雅克少将一直担任盟友和合作机构的关键参谋和联络职位，以及部队和编队级别的指挥职位。戴夫·雅克于 2022 年被任命为联合部队网络部分指挥官。

关于作者

赵慧杰

虎符智库专家、网络空间安全军民融合创新中心高级研究员。长期从事网络安全、互联网发展等领域研究工作，对外军网络战、国际网络安全态势、全球网络空间竞合及新技术新应用发展等具有深厚研究造诣，先后获得军内成果奖七项。

“定期更换密码”是最愚蠢的密码规则?

数十年来，消费者和企业员工经常被灌输一些“强密码规则”，如定期更换密码，在密码中使用特殊字符等。虽然，近年来此类密码规则的有效性遭到安全专家的广泛质疑，但是新一代密码规则（如用长度换强度、非必要不更新等）由于企业界的强大惯性和阻力（如大多数互联网服务和企业系统都不支持 64 位长密码）而难以普及推广。

近日，美国国家标准与技术研究院（NIST）发布了最新的数字身份指南草案（SP800-63-4 第二版），彻底颠覆了人们对密码安全的认知。指南提议取消一些最流行的、同时也是“最荒谬”的常识性做法，例如：

- 强制用户定期更改密码
- 强制或限制用特定字符
- 强制要求混合多种类型字符
- 使用安全问题作为验证手段

美国国家标准与技术研究院（NIST）指出，
许多传统密码管理规则不仅没有增强安全性，
反而适得其反。
最典型的例子是强制用户定期更改密码的要求。

破除密码安全的陈规陋习

在数字时代，密码是保护用户隐私和数据安全的关键要素。然而，NIST 指出，许多传统密码管理规则不仅没有增强安全性，反而适得其反。最典型的例子是强制用户定期更改密码的要求。

几十年前，密码安全性认知尚未普及，人们往往选择容易被破解的常见词汇或简单字符组合，因此定期更改密码被认为是防止被盗用的一种策略。但是，随着密码管理技术的进步和随机生成密码的普及，强制更改密码的做法不仅增加了用户的负担，还可能导致密码复杂性下降。

NIST 给验证服务和管理者的“颠覆性”密码建议如下：

- 密码长度至少为 8 个字符，建议不少于 15 个字符。
- 应允许最大密码长度至少为 64 个字符。
- 应该接受所有打印 ASCII（RFC20）字符，或在密码中添加空格字符。
- 应接受密码中的 Unicode（ISO/ISC 10646）字符。评估密码长度时，每个 Unicode 代码点应计为一个字符。
- 不得对密码施加其他组合要求（如要求混合不同类型的字符）。
- 不得要求用户定期更改密码，

除非有证据表明账户被盗用。

• 不得允许订阅者存储未经身份验证的用户可访问的提示。

• 不得提示订阅者在选择密码时使用基于知识的身份验证 (KBA)（如“您的第一只宠物的名字是什么？”）或安全问题。

• 验证者应当完整验证所提交的密码（即，不要截断它）。

特殊字符与安全问题是一对“卧龙凤雏”

NIST 还质疑另一项广受诟病的规则——要求密码必须包含大小写字母、数字和特殊字符。NIST 认为，在密码足够长且复杂的情况下，这类字符组合规则并没有实质上的安全提升作用，反而会导致用户选择更容易记忆且相对脆弱的密码。

许多用户为了满足这些复杂的规则，往往倾向于使用重复的字符或常见组合，如“Password123!”之类的“伪强密码”。

同样，NIST 建议废除使用安全问题（如“您的第一只宠物叫什么？”）作为密码验证手段。研究表明，安全问题容易被破解或通过社交工程攻击获取答案，难以真正保障用户隐私（有时反而会导致隐私泄漏）。

用长度换取强度

NIST 在新指南中建议，密码验证系统应接受至少 64 个字符长度的密码，并支持所有 ASCII 字符和 Unicode 字符的使用。这意味着用户不仅可以设置更长的密码（如 wo xihuan chi gobelieve baozi），还可以使用更广泛的字符集，进一步增强密码的复杂性与安全性。

同时，NIST 强调，密码验证应当检查用户输入的完整密码，而非截断处理，确保密码的每一个字符都被考虑在内。

密码安全新趋势：回归常识与用户体验

NIST 的最新指南草案不仅在技术层面上进行了优化，更重要的是，它体现了密码安全领域的一种回归——回归常识、回归用户体验。正如 NIST 在声明中指出的，许多密码管理规则之所以存在，是因为早期网络安全认知不足，然而，随着技术的进步和攻击手段的复杂化，许多看似“安全”的做法其实已经不再适用，甚至成为安全隐患的源头。

以密码长度为例，NIST 建议的 8~15 字符的最低密码长度既确保了密码的基本安全性，又避免了过度复杂的字符组合规则，让用户可以在增强安全性的同时减少记忆负担。这一理念与近年来密码管理软件（如密码管理器）和生物识别技术的普及相呼应，进一步提升了整体用户体验。

未来展望：安全管理需要以人为本

尽管近年来不少专家一再批评现行密码规则的弊端，但银行、互联网平台和政府机构大多依然固守这些过时、无效甚至有害的规则。NIST（美国国家标准与技术研究院）发布的新指南草案尽管并不具备强制性，但被业界广泛看作是终结“无效”密码规则的一个标志性历史事件，也是全球密码安全标准演进的重要一环，有望在更广泛的领域内被采纳和应用，带动密码安全领域的深层变革。

未来，随着量子计算等新技术的发展，密码学的基础原理也可能发生变革。目前来看，这一提议对于密码管理和用户安全的提升是显而易见的，但其最终效果仍有待观察和验证。

“人的因素”是网络安全最重要的环节，NIST 密码新规的提出代表了一个重要的网络安全趋势——有效的安全管理需要更多地依赖技术创新和用户友好的安全设计，而不是机械地强制用户遵循陈规陋习。

关于作者

GoUpSec

以国际化视野服务于网络安全决策者人群，致力于成为国际一流的调研、分析、媒体、智库机构。

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