国盟信息安全通报

2021 年 07 月 31 日第 241 期

全国售后服务中心

国盟信息安全通报

（第 241 期）

国际信息安全学习联盟

2021 年 7 月 31 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 484 个，其中高危漏洞 131 个、中危漏洞 299 个、低危漏洞 54 个。漏洞平均分值为 5.69。本周收录的漏洞中，涉及 0day 漏洞 212 个（占 44%），其中互联网上出现“SourceCodester E-Commerce Website 跨站脚本漏洞、SourceCodester Travel Management System 文件上传漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 4248 个，与上周（4935 个）环比减少 14%。

主要内容

一、概述 4
二、安全漏洞增长数量及种类分布情况 4
➢漏洞产生原因（2021 年 7 月 1 日—2021 年 7 月 31） 4
➢漏洞引发的威胁（2021 年 7 月 1 日—2021 年 7 月 31） 5
➢漏洞影响对象类型（2021 年 7 月 1 日—2021 年 7 月 31） 5
三、安全产业动态 6
➢数据安全关乎国家安全 6
➢不断健全个人信息保护的综合治理体系 10
➢打击网络攻击犯罪应加强国际合作 12
➢斩断电信网络诈骗犯罪链条 14
四、政府之声 16
➢国家网信办《网络安全审查办法（修订草案征求意见稿）》公开征求意见 16
➢商务部、网信办、工信部印发《数字经济对外投资合作工作指引》 17
➢中国人民银行印发《非银行支付机构重大事项报告管理办法》 18
➢最高法发布审理使用人脸识别技术处理个人信息相关民事案件的司法解释 19
五、本期重要漏洞实例 21
➢Microsoft 发布 2021 年 7 月安全更新 21
➢Oracle MySQL Server 拒绝服务漏洞 22
➢Cisco Identity Services Engine 跨站脚本漏洞 23
➢IBM Sterling Secure Proxy 拒绝服务漏洞 23
六、本期网络安全事件 25
➢ 解析“滴滴出行”“BOSS 直聘”等接受网络安全审查，原因是什么？ 25
➢ 四个月内 领英用户个人信息已被兜售三次 28
➢ 厦门某知名快捷酒店被发现摄像头案件告破 29
➢ 伊朗国家铁路遭网络攻击，各地车站大屏传播虚假延误信息 30
➢ 南非主要港口系统遭受黑客攻击 港口货运被迫延迟 31
➢ 离职后心生不满西安某医院前网管“炫技性报复”整个医院系统瘫痪 32

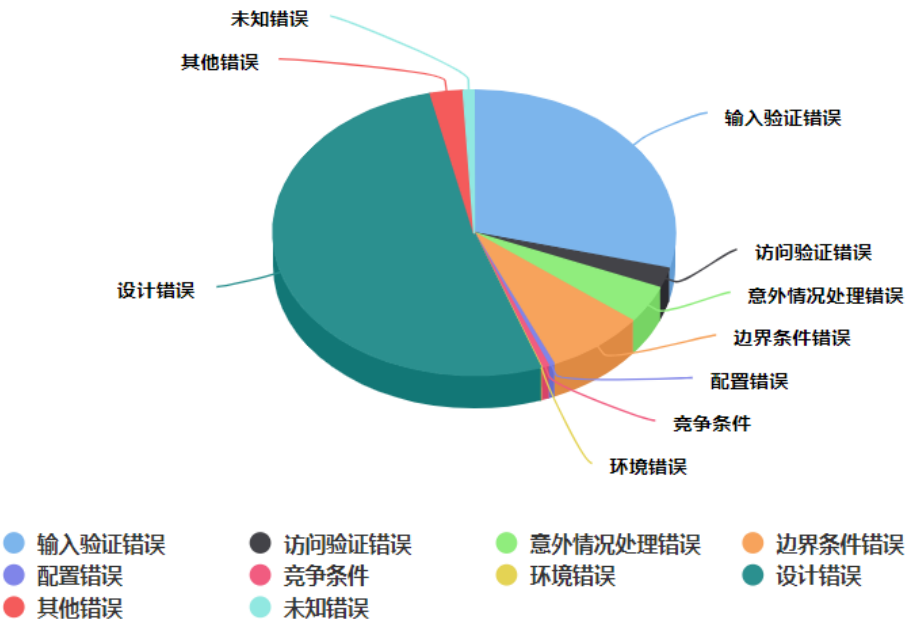
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

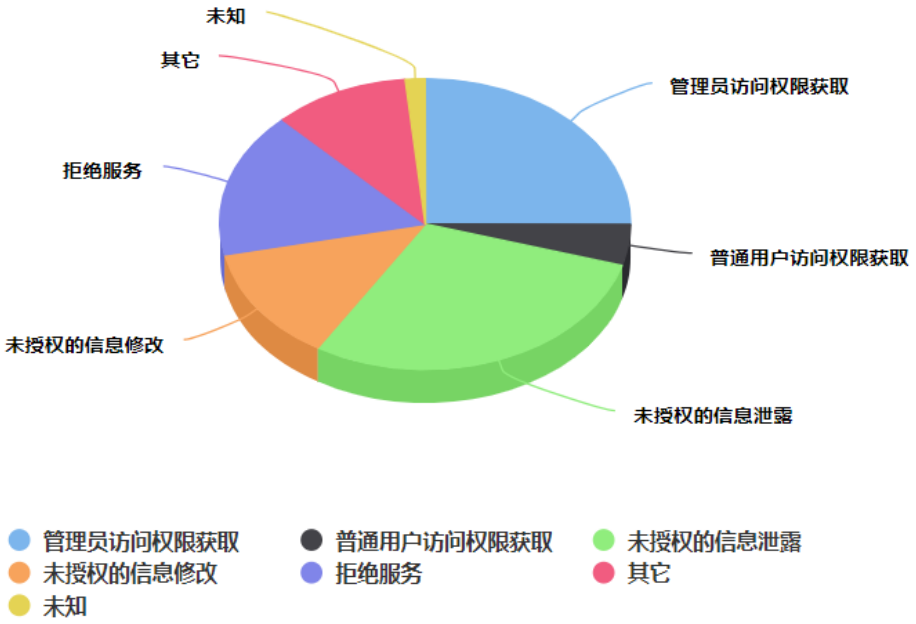
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 484 个，其中高危漏洞 131 个、中危漏洞 299 个、低危漏洞 54 个。漏洞平均分值为 5.69。本周收录的漏洞中，涉及 0day 漏洞 212 个（占 44%），其中互联网上出现“SourceCodester E-Commerce Website 跨站脚本漏洞、SourceCodester Travel Management System 文件上传漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 4248 个，与上周（4935 个）环比减少 14%。

二、安全漏洞增长数量及种类分布情况

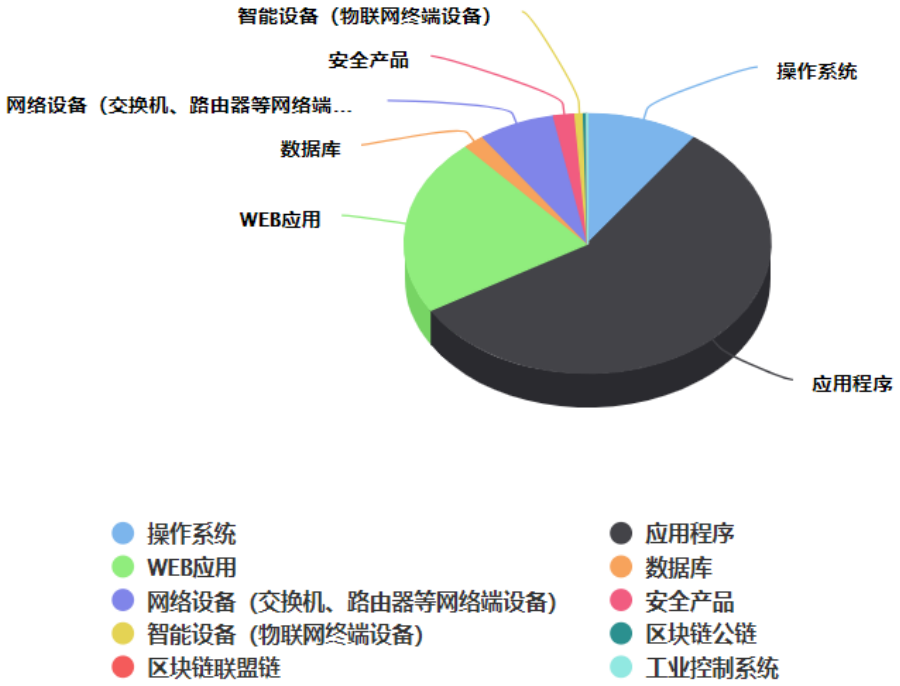
➢ 漏洞产生原因（2021 年 7 月 1 日—2021 年 7 月 31）



➢ 漏洞引发的威胁（2021 年 7 月 1 日—2021 年 7 月 31）



➢ 漏洞影响对象类型（2021 年 7 月 1 日—2021 年 7 月 31）



三、安全产业动态

➢ 数据安全关乎国家安全

2021 年 7 月 6 日，中共中央办公厅、国务院办公厅公开发布《关于依法从严打击证券违法活动的意见》。意见提出，完善数据安全、跨境数据流动、涉密信息管理等相关法律法规。抓紧修订关于加强在境外发行证券与上市相关保密和档案管理工作的规定，压实境外上市公司信息安全主体责任。

近日，国家网信办连续发布了对“滴滴出行”“运满满”“货车帮”“BOSS 直聘”实施网络安全审查的公告。审查期间，以上 APP 均已停止新用户注册。多家互联网企业接受网络安全审查，一时间，数据安全再次成为关注焦点。

接受网络安全审查的几家企业都掌握大量用户隐私数据，并且业务与关键信息基础设施有关

“滴滴一下，美好出行”。作为中国最大的出行平台，“滴滴出行”的下架整改，让这句广告词变了滋味。2021 年 7 月 4 日，国家互联网信息办公室发布公告称，经检测核实，“滴滴出行”APP 存在严重违法违规收集使用个人信息问题。“滴滴出行”随后回应称，将严格按照有关部门的要求下架整改，并积极配合网络安全审查。目前，“滴滴出行”APP 已暂停新用户注册，并下架整改。一天后，网络安全审查办公室发布关于对“运满满”“货车帮”“BOSS 直聘”启动网络安全审查的公告。

对这几家企业启动网络安全审查，原因是什么？

查看“运满满”企业官网时发现，该公司成立于 2013 年，隶属于江苏满运软件科技有限公司，是国内基于云计算、大数据、移动互联网和人工智能技术开发的货运调度平台。官网称,“运满满已经成为全球出类拔萃的整车运力调度平台和智慧物流信息平台”。“货车帮”公司官网则介绍，“货车帮”是中国最大的公路物流互联网信息平台，建立了中国第一张覆盖全国的货源信息网，并为平台货车提供综合服务，致力于做中国公路物流基础设施。

相比于这两家公司，“BOSS 直聘”或许更广为人知。招股书显示，2021 年 3 月，“BOSS 直聘”月活跃用户数达 3060 万，服务 630 万家认证企业，其中 82.6%为中小企业。官网介绍称，该平台应用人工智能、大数据前沿技术，提高雇主与人才的匹配精准度，缩短求职招聘时间，从而提升求职招聘效率。

综合来看,这几家企业都掌握大量用户隐私数据,并且业务与关键信息基础设施有关联。

“上述几家被审查的企业，分别为日常出行、网络货运及大众求职领域的头部平台，至少掌握了所属行业领域 80%以上的深度数据。这些数据可以直接或间接地反映我国各区域人口分布、商业热力、人口流动、货物流动、企业经营等情况。”江苏省大数据交易和流通工程实验室副主任李可顺表示。

被审查企业近期已赴美上市，将不可避免涉及数据出境问题

值得注意的是，这几家被审查的企业有着共同的特点：近期赴美上市。查阅资料发现，2021 年 6 月 11 日，“BOSS 直聘”于美国上市；6 月 22 日，拥有“运满满”和“货车帮”的满帮集团于美国上市；6 月 30 日，国内最大的移动出行平台滴滴于美国上市。滴滴接受网络安全审查的消息，迅速在网络上发酵。

汇业律师事务所高级合伙人李天航认为，滴滴作为一家主要在中国经营的企业，所有数据首先是存储在本地的。但是，在美国上市将不可避免地涉及数据出境问题。

去年 6 月份，美国参议院提出了《外国公司问责法案》，该法案规定，如果外国公司连续三年未能通过美国公众公司会计监督委员会的审计，将被禁止在美国任何交易所上市。而有关信息的披露，可能导致重要数据、个人信息的泄露。今年 3 月份，美国证券交易委员会表示，通过了《外国公司问责法案》最终修正案。

“美国证券市场对于上市公司有很高的信息披露要求,包括必须根据美国公认会计原则编报其财务报表、必须根据美国证券法律规定，对公司重大信息及时披露等，这势必涉及一些该公司在中国境内的经营情况数据是否能够出境的问题。”李天航说。

随着网络安全法、数据安全法等法律的施行，我国网络和数据相关的法律法规体系正在不断完善

我国在网络安全和数据治理方面的立法体系不断构建完善，为开展网络安全和数据治理工作提供了充分的立法保障。”中国信息通信研究院互联网法律研究中心研究员赵淑钰告诉记者。

2017 年 6 月 1 日，《中华人民共和国网络安全法》施行，填补了我国综合性网络信息安全基本大法、核心的网络信息安全法和专门法律的三大空白。

此次几家互联网企业接受审查的依据之一，是 2020 年 6 月 1 日正式实施的《网络安全审查办法》。该办法为开展网络安全审查提供了重要的制度保障和法律依据。

中国人民大学重阳金融研究院副研究员刘典告诉记者，网络安全审查重点评估关键信息基础设施运营者采购网络产品和服务可能带来的国家安全风险，包括：产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险；产品和服务供应中断对关键信息基础设施业务连续性的危害；产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；产品和服务提供者遵守中国法律、行政法规、部门规章情况；其他可能危害关键信息基础设施安全和国家安全的因素。

“通常情况下，网络安全审查在 45 个工作日内完成，情况复杂的会延长 15 个工作日。进入特别审查程序的审查项目，可能还需要 45 个工作日或者更长。”刘典说。

2021 年 3 月，《中华人民共和国个人信息保护法（草案）》提请全国人大常委会审议。目前，该草案已处于审议阶段，业界普遍认为，该法距离面世并生效实施已经为期不远。

2021 年 6 月，《中华人民共和国数据安全法》全文公布，并将于 9 月 1 日起正式实施。“数据安全法明确了由中央国家安全领导机构‘统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制’，这是亮点之一。”刘典告诉记者。

“网络安全法、数据安全法和个人信息保护法这三部法律出台后，中国互联网领域基础性的法律法规框架体系就已完成，其他法律、法规、部门规章、地方性法规等等，都会在这三部法律组成的体系之下，继续细化具体的内容，逐步覆盖互联网、个人信息和数据活动的方方面面。”李天航说。

国家在互联网领域和数据安全领域的主导，符合推动高质量发展的内在要求

近几年，大数据、云计算、物联网等技术和应用高速发展，互联网企业在为人们生活带来便利的同时，跨境数据流动、用户数据泄露等问题，也受到广泛关注。

在赵淑钰看来，随着互联网企业的迅速兴起、发展，其在提升用户黏性、扩展业务生态方面不断强化，巨量数据在互联网企业生成、汇聚、融合，在释放数据价值的同时也带来了

巨大的数据安全风险。

“一方面，造成侵犯用户个人信息的风险，目前过度收集、滥用用户个人信息的情形依然多发高发；另一方面，也会对国家安全产生影响，随着数据分析技术的飞跃发展，互联网企业在运营过程中产生的巨量数据通过大数据分析能够反映出我国整体经济运行情况等涉及国家秘密的信息，对总体国家安全构成重大安全威胁。”赵淑钰说。

“近两年，一些互联网企业在用户个人信息泄露方面发生的问题屡见不鲜，原因之一是我国数据安全保护机制的建设还不是特别完善。”刘典表示，这与互联网行业的高速变化不无关系。“新业态不断推陈出新，监管对象在不停变化，规模不断扩大，给治理带来了一定的难度。”

互联网企业的数据安全问题也可能从不同方面影响国家安全。类似地图数据、位置数据等重要数据，同样需要保护。

“从国家层面来说，监管互联网企业的数据安全问题需要平衡一个内在矛盾，即大型科技公司跨境数据流动的业务需求和跨境数据流动带来的安全风险的矛盾。”刘典表示。

在刘典看来，当前国家在互联网领域和数据安全领域的主导，符合推动高质量发展的内在要求。“过去一些互联网企业在野蛮高速增长的状态下，主要从商业利益的角度出发进行数据的开发利用，对数据合规的投入相对较小。随着数据保护问题成为一个社会焦点，国家开始不断加强对于数据监管和数据安全合规的监管。虽然从短期来看，会对互联网企业的发展模式带来一定冲击，但这也是由高速发展转向高质量发展的必由之路。”刘典说。

在李天航看来，将来所有企业的所有经营行为，都必须受到国家安全法、网络安全法、数据安全法和个人信息保护法这四部法律为纲的立体法律框架体系的规范。他建议，企业要有前瞻性，调整自己的经营、运维和治理理念，甚至重塑自身业务模式。“这不但能够预防很多行政甚至刑事处罚风险，而且某种程度上来说，合规能够成为企业的最大竞争力。”

数据安全已被提升至国家安全的层面，充分体现我国维护数据主权和国家安全的决心

“6 月 10 日，十三届全国人大常委会第二十九次会议表决通过数据安全法，将数据安全提升到了国家安全的层面，同时对重要数据出境安全管理也提出了相应要求。”李可顺表示。

数据安全法第三十一条明确了重要数据出境安全管理制度，“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。”

此外，数据安全法还严格规制面向境外司法或者执法机构的数据出境活动。该法第三十六条规定，“非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。”

“这一条款制定的背景是近年来数据管辖权冲突日益激烈的国际环境。”中伦律师事务所顾问贾申刊文指出，在这一背景下，数据安全法的规定再度明确了我国对境内数据的管辖权，充分体现了我国维护数据主权和国家安全的决心。

“值得一提的是，数据安全法还特别明确了未经主管机关批准向境外的司法或者执法机构提供数据的法律责任，包括对企业和直接负责的主管人员的罚款，以及责令企业暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照等。这一明确的法律责任形式，不仅意味着第三十六条的规定是企业应严格履行的一项数据合规义务，也使得企业在对抗境外执法或司法机构可能的数据调取要求时，拥有了可援引的有力的法律规则。”贾申表示。

没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。要树立正确的网络安全观，加强信息基础设施网络安全防护，加强网络安全信息统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然。要落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任，主管部门履行好监管责任。

“目前来看，围绕这家企业（滴滴）的跨境数据流动问题，数据出境当中涉及的国家网络安全审查问题，以及 APP 对于个体用户隐私信息的过度搜集问题，中国网信的治理实践迎来了一个跃迁的契机。”复旦大学国际关系学院教授沈逸在专栏中写道。沈逸还表示，个人在关注企业的跨境数据流动问题时，应该避免“走极端”，“要么就是认为它应该绝对地遵循技术市场的内生需求，要求最小化的监管，要么将它视作洪水猛兽，对它进行过度监管”。“对最后的政策出台，目前从实践来看，大家可以抱有充分的信心。保障人民的福祉，最大限度地为人民服务，是我国网信部门在推动相应监管落实过程当中已经确立起来的坚定不移的目标。我们应该对网信部门保持坚定的信心。”沈逸说。（来源：中央纪委国家监委网站）

➢ 不断健全个人信息保护的综合治理体系

个人信息是宝贵的数字资产，加强个人信息保护，规范个人信息获取及使用，不仅事关个人权益的维护，也关系到数字经济健康发展

如今，随着互联网的发展，各种类型的移动互联网应用程序（APP）层出不穷，极大满足了人们在社交、购物、娱乐、办公等多方面的需求。但这些程序在给人们生活带来便利的同时，也给个人信息安全带来威胁。比如，想要下载某个 APP，先得授权大量个人信息，否则无法使用；闲聊中提到某个商品，不久就会收到精准推送的广告；手机上收到一张礼服照片，购物软件就开始推送各款礼服……不经意间，人们的隐私信息、“网络足迹”等就被“偷走”甚至滥用了。

万物皆可联的现代信息社会，个人信息不可避免地被各类网络服务平台大量留痕。而各种基于大数据的新产业新业态新模式的发展，让个人数据变得越来越有价值。个人信息是宝贵的数字资产，加强个人信息保护，规范个人信息获取及使用，不仅事关个人权益的维护，也关系到数字经济健康发展。

近年来，我国不断加大个人信息保护力度。网络安全法、民法典、消费者权益保护法等从法律层面对个人信息权益进行了保护，如规定 APP 运营商的信息处理活动应当遵循“合法、正当、必要”的原则，且不得收集与其提供的服务无关的个人信息。有关部门也相继出台了《APP 违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》等，明确了地图导航、即时通信、网络购物等常见类型 APP 的必要个人信息范围。

“十四五”规划纲要中对加快数字化发展、建设数字中国做出了全面部署。要营造良好数字生态，其中的重要一环就是进一步加强个人信息保护，不断健全个人信息保护的综合治理体系。

不以规矩，不能成方圆。应加快完善个人信息保护相关法律法规，规范个人信息收集和

使用。大数据、人工智能产业的发展需要对相关数据进行分析与共享，一些 APP 基于提供服务、提升体验的需要，要求一定权限、收集相关信息也是合理的，但应有边界，不能侵犯个人权益。近年来我国陆续出台了保护个人信息的法律法规，规范政府、企业和个人在使用个人信息方面的行为，但这些法规较为分散，迫切需要加快个人信息保护法立法进程。要加快推进数据安全、个人信息保护等领域基础性立法。通过专门立法，进一步明确网络运营者收集用户信息的原则、程序，明确其对收集到的信息的保密和保护义务，不当使用、保护不力应当承担的责任以及监督检查和评估措施等。

监管部门应当严格执法、统一执法，强化对 APP 超范围收集用户个人信息的监管力度。日前，针对人们反映强烈的 APP 非法获取、超范围收集、过度索权等侵害个人权益现象，国家互联网信息办公室依据相关法律法规，通报了 105 款 APP 违法违规收集使用个人信息情况，并责令限期整改。工信部近年来也持续开展了 APP 侵害用户权益专项整治行动。这些举措都取得了积极成效，消费者拍手称赞。人们期待监管能够更加有力，如加大对个人信息保护相关违法行为查处和处罚力度，提高违法成本和法律震慑效应等。同时，也要善用人工智能、大数据等新技术新手段来加强对 APP 收集个人信息的监管与检测，优化消费者的举报投诉服务，形成常态化监管体系。

此外，用户个人也应当提升自己的个人信息安全意识。网民在注册 APP 时，要养成浏览用户协议、隐私保护协议等内容的习惯，谨慎填写个人信息，及时关闭不必要的 APP 权限。当发现个人信息被违法违规使用等情况时，也要勇敢地站出来，通过投诉、举报和诉讼等方式维护自己的个人信息权益，保护好我们的“网络足迹”。（来源：人民日报）

➢ 打击网络攻击犯罪应加强国际合作

2021 年 7 月 19 日，美国纠集其盟友英国、澳大利亚、加拿大、新西兰、日本、挪威、欧盟和北约等，在没有证据的情况下，无端指责中国搞“网络安全攻击”，并将今年稍早时候披露的针对微软的大规模攻击归咎于中国，污称中国政府“极有可能”支持了这一“网络攻击”行为。西方的这种抹黑行径完全不符合其所标榜的法治精神和所推崇的国际关系基本准则。

西方对中国政府的无端指责已经不是什么新闻了。2014 年 5 月，美国司法部以所谓“网络窃密”为由，起诉 5 名中国军官，指控他们侵入美国企业窃取商业秘密。2018 年 12 月，

美国司法部起诉中国两名黑客，指控他们受雇于中国黑客组织，专门入侵协助政府机关和私营企业管理资讯科技系统的“托管服务提供商”，盗取机密资料，并称这是中国政府指挥的一项行动的一部分。2020 年 2 月，美国司法部指控 4 名中国军人侵入美国征信机构 Equifax 公司，窃取 1.45 亿个人信息及商业秘密。凡此种种，其基本套路都是：受到来自中国的黑客攻击，必是中国政府支持，但拒绝提供充分的证据，以“猜测”开始，以“抹黑”结束，搞有罪推定，扣帽子、打棍子，完全无视正当程序和法治精神。可以说，这种不提供充分证据的指责，就是耍流氓。

我们都知道，当前拥有最先进的信息通信技术的是美国，拥有最先进的网络监听技术和最强网络战能力的也是美国。2013 年披露的棱镜门事件、2020 年曝光的瑞士加密机事件、一个多月前曝光的丹麦海底电缆窃听事件，都已充分表明美国在无时无刻监听着全世界，连其亲密盟友国家也不放过。对此，美国都是只言片语轻轻带过。前总统奥巴马说，这是“为了更好地认识世界”。前国务卿克里辩称，监控是出于国家利益考虑，“各种各样的情报对维护国家安全都有好处”。这是典型的为了自己的安全，而不顾其他国家的安全；牺牲他国的安全而谋求自身的所谓绝对安全。

网络的开放性必然带来风险性。网络黑客攻击是当今网络时代的毒瘤，是全球性的问题。各国都是网络攻击的受害者，中国也不例外。根据中国国家互联网应急中心报告，2020 年共有位于境外的约 5.2 万个计算机恶意程序控制服务器控制了中国境内约 531 万台主机；今年 2 月，中国境内多达 83 万个 IP 地址受到不明的网络攻击，七成以上来自境外，对中国国家安全、经济社会发展和人民正常生产生活造成了严重危害。网络攻击溯源是复杂的技术问题，在定性网络事件的时候应基于充分的证据，而不是无端猜测指责，更不应该不负责任

地将网络攻击直接与一国政府相关联。

实际上，中国已经建立起了比较完善的打击网络攻击等犯罪行为的法律体系。中国《刑法》规定了非法侵入计算机信息系统罪，非法获取计算机信息系统数据、非法控制计算机信息系统罪，提供侵入、非法控制计算机信息系统程序、工具罪，破坏计算机信息系统罪，非法利用信息网络罪等犯罪行为。《网络安全法》明确规定，任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具。最高人民法院、最高人民检察院也发布了一系列打击网络犯罪的司法解释。2019 年以来，检察机关共起诉网络犯罪案件 5 万余件 14 万余人。在国际上，中国提出《全球数据安全倡议》，明确倡议各国反对利用信息技术破坏他国关键基础设施或窃取重要数据，反对滥用信息技术从事针对他国的大规模监控、非法采集他国公民个人信息等。

道高一尺，魔高一丈。面对无孔不入的跨国网络攻击，当前最需要做的是进一步加强国际合作，全世界联合起来共同打击网络攻击、网络恐怖主义等网络犯罪行为，实现共同安全。为实现共同的数字安全，我们呼吁拥有先进信息通信技术和网络攻击溯源技术的国家，分享相关技术，支持其他国家应对网络威胁的能力建设，积极开展国际协作，共同打击网络攻击和网络窃密行为，真正为实现网络空间共同安全做出应有的贡献。（来源：环球网）

➢ 斩断电信网络诈骗犯罪链条

日前，最高法、最高检、公安部联合发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见(二)》，对于电信网络诈骗犯罪以及涉手机卡、信用卡犯罪等关联犯罪，提出更加明确具体的适用法律依据，对电信网络诈骗犯罪实行全链条、全方位打击。

电信网络诈骗已经成为严重损害人民利益的刑事犯罪，仅 2020 年，全国电信网络诈骗案件涉及财产损失达 353.7 亿元。从政法机关执法办案情况来看，非法开办贩卖电话卡、银行卡(以下简称“两卡”)是电信网络诈骗案件持续高发的重要根源之一，犯罪分子多利用非法收贩来的电话卡、银行卡进行收取、转移赃款，逃避公安机关追查，导致诈骗资金迅速流转、拆解、混同，极大地增加了打击犯罪和追赃挽损的难度。

有效惩治电信网络诈骗犯罪，就要瞄准关键环节。依法严厉打击涉“两卡”违法犯罪，就是斩断电信网络诈骗犯罪帮助链条、遏制电信网络诈骗犯罪高发态势、加强源头治理的关

键环节。从去年 10 月起，全国公安机关会同检察、法院、通信、金融等部门联合开展“断卡”行动，以斩断电信网络诈骗违法犯罪的信息流和资金链，从源头上全力遏制电信网络诈骗犯罪高发态势，取得了积极成效。此次《意见(二)》在总结“断卡”行动经验的基础上规定，为他人利用信息网络实施犯罪而收购、出售、出租信用卡、银行账户、他人手机卡、流量卡等的，可认定为刑法规定的“帮助”行为，打击“两卡”犯罪的法律依据进一步完善，法律标准更加全面。

由于电信网络诈骗犯罪分子不断变换形式、使用多种技术手段，增加了查处追溯的难度，这就要求相关部门切实履行好主体责任，强化源头治理和行业治理，不断加大监管工作力度。当前，相关部门在集中清理整治涉诈电话卡、涉诈银行账户的同时，持续加强技术反制工作，拦截诈骗电话、诈骗短信，封堵诈骗网址，强力清除涉诈黑灰产业链，铲除诈骗犯罪土壤。一些地方还探索对手机卡、银行卡的失信用户实行信用惩戒，例如在通信方面对失信用户实施 5 年内只保留 1 张电话卡且不得新增移动电话业务功能的惩戒，通过行业治理净化网络生态空间，形成了综合治理合力。

电信网络诈骗是可防性犯罪，坚持打防并举、防范为先，才能最低限度减少发案，最大限度为群众避免损失。下发预警指令、加强受骗资金紧急拦截，这些都是防范电信网络诈骗的有力举措。值得关注的是，司法实践中发现，部分在校学生在寻找实习机会、社会兼职过程中，容易被贩卡团伙拉拢、利诱。这也提醒我们打击治理电信网络诈骗，既要靠政府部门的重拳出击，也需要网络平台和全社会的共同努力。唯有打防结合、多措并举、综合治理，才能遏制电信网络诈骗的高发态势，守护好广大人民群众的钱袋子。（来源：人民日报）

四、政府之声

➢ 国家网信办《网络安全审查办法（修订草案征求意见稿）》公开征求意见

2021 年 7 月 10 日，国家互联网信息办公室会同有关部门修订的《网络安全审查办法（修订草案征求意见稿）》（以下简称《办法》向社会公开征求意见，征求意见截止日期为 2021 年 7 月 25 日。

《办法》旨在确保关键信息基础设施供应链安全，维护国家安全。明确网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务安全性、可能带来的国家安全风险等方面进行审查。

《办法》提出，运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

《办法》规定，网络安全审查重点评估采购活动、数据处理活动以及国外上市可能带来的国家安全风险，主要考虑以下因素：产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏的风险；产品和服务供应中断对关键信息基础设施业务连续性的危害；产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；产品和服务提供者遵守中国法律、行政法规、部门规章情况；核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险；国外上市后关键信息基础设施，核心数据、重要数据或大量个人信息被国外政府影响、

控制、恶意利用的风险；其他可能危害关键信息基础设施安全和国家数据安全的因素。

《办法》明确，运营者应当督促产品和服务提供者履行网络安全审查中作出的承诺。网络安全审查办公室通过接受举报等形式加强事前事中事后监督。此外，运营者违反本办法规定的，依照《中华人民共和国网络安全法》《中华人民共和国数据安全法》的规定处理。（来源：中国网信网）

- **国家互联网信息办公室《网络安全审查办法（修订草案征求意见稿）》**
- **全文：**http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm

➢ 商务部、网信办、工信部印发《数字经济对外投资合作工作指引》

2021 年 7 月 23 日，商务部网站消息，近日，商务部、中央网信办、工信部联合印发《数字经济对外投资合作工作指引》（附后）。《工作指引》提出，完善对外投资备案报告制度，用好境外企业和对外投资联络服务平台，加强监测与分析，做好风险预警。提升对外投资合作数字化管理水平，加强部门间信息共享和协同监管。

此外，《工作指引》还提出，鼓励企业抓住海外数字基础设施市场机遇，投资建设陆海光缆、宽带网络、卫星通信等通信网络基础设施，大数据中心、云计算等算力基础设施，人工智能、5G 网络等智慧基础设施，在全球范围内提供数字服务。挖掘传统基础设施升级改

造市场潜力，积极参与东道国市政、交通、能源、电力、水利等传统基础设施数字化、网络化、智能化升级改造。

同时，《工作指引》中还提到，要做好数字经济走出去风险防范。鼓励数字经济企业完善内部合规制度，严格落实我国法律法规有关数据出境安全管理的规定，遵守东道国法律法规及国际通行规则，妥善应对数字经济领域审查和监管措施。提高知识产权保护意识，健全数据安全管理制度，采取必要技术措施，保护数据安全和个人信息，支持企业通过法律手段维权。密切跟踪全球数字经济反垄断及加征数字税最新政策动向，做好应对准备。

在营造数字经济国际合作良好环境方面，《工作指引》明确，完善数字经济领域多双边交流合作机制，发挥投资合作工作组作用，加强与有关国家数字经济发展战略对接和政策沟通。鼓励数字经济企业、研究机构、行业协会加强与国际同行交流合作。鼓励数字经济企业积极参与东道国复工复产和民生项目，履行社会责任，培养当地数字经济人才，树立良好口碑。扩大正面宣传，营造数字经济企业良好国 际形象，做好舆情应对工作。（来源：中华人民共和国商务部）

- **《数字经济对外投资合作工作指引》**
- **全文：**http://www.ltcjzx.org.cn/article/cq/202107/20210703180522.shtml

➢ 中国人民银行印发《非银行支付机构重大事项报告管理办法》

2021 年 7 月 23 日，中国人民银行发布《非银行支付机构重大事项报告管理办法》（以下称《管理办法》），针对非银行支付机构重大事项报告行为作出了详细要求，并将于 2021 年 9 月 1 日起正式施行。

根据该《管理办法》中的要求，非银行支付机构报告重大事项应当一事一报，做到及时、真实、准确、完整，不得迟报、漏报、瞒报、谎报、错报，不得有误导性陈述或者重大遗漏。

支付机构发生风险事件或者突发情况，要求及时上报。根据该《管理办法》中的要求，支付机构“发生客户个人信息泄露等信息安全事件一次性涉及客户信息数据超过 5000 条或者客户数量超过 500 户的”，属于一类事项，应当在事项发生后 2 小时内通过电话、传真或者电子邮件等形式向所在地中国人民银行分支机构及时报告，并在事项发生后 2 个工作日内向所在地中国人民银行分支机构提交书面报告。

如发生《管理办法》中所提到的二类事项，如“发生客户个人信息泄露等信息安全事件

一次性涉及客户信息数据不超过 5000 条，且涉及客户数量不超过 500 户的”，支付机构应当在事项发生后 24 小时内通过电话、传真或者电子邮件等形式向所在地中国人民银行分支机构及时报告，并在事项发生后 5 个工作日内向所在地中国人民银行分支机构提交书面报告。

《管理办法》指出，中国人民银行分支机构应当将支付机构重大事项报告执行情况纳入支付机构年度分类评级考核。未按本办法规定建立重大事项报告、风险事件防控、处置等工作机制或者报告重大事项的，中国人民银行及其分支机构责令其限期整改，可以采取约谈等监管措施，并可以依据《非金融机构支付服务管理办法》有关规定予以处罚。（来源：最高人民检察院）

- **《非银行支付机构重大事项报告管理办法》（银发〔2021〕198 号）**
- **全文：**http://www.pbc.gov.cn/tiaofasi/144941/3581332/4301558/index.html

➢ 最高法发布审理使用人脸识别技术处理个人信息相关民事案件的司法解释

2021 年 7 月 28 日，最高人民法院发布《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》，对滥用人脸识别说“不”。这一司法解释，对各级人民法院正确审理相关案件、统一裁判标准、维护法律统一正确实施、实现高质量司法，具有重要的现实意义。

近年来，随着信息技术飞速发展，人脸识别逐步渗透到人们生活的方方面面。但由于信息泄露风险大、安全漏洞难消除等问题，人脸识别技术带来的个人信息保护问题也日益凸显，强化人脸信息保护的呼声日益高涨。百姓有所呼，司法有所应。从今年“人脸识别第一案”的宣判，到此次最高法发布司法解释，都彰显了遏制人脸识别技术滥用趋势的司法努力。

然而，在人工智能发展的风口上，强化用户人脸信息保护，会不会影响数字经济发展？此次司法解释，很好地实现了两者平衡。一方面，在依法保护自然人人脸信息的同时，明确规定了使用人脸识别不承担民事责任的情形，实现了个人利益和公共利益的平衡。另一方面，充分考量人脸识别技术的积极作用，明确不溯及既往的基本规则，以规范促应用，实现惩戒侵权和鼓励数字科技发展之间的平衡。可以说，这一司法解释既保护了当事人合法权益，又有利于数字经济健康发展。

繁荣数字经济，是为了共享数字红利。依法应对新技术带来的新挑战，让人脸识别应用规范起来，实现技术运用与商业伦理、社会价值的良性互动，用户体验必将更加便利，数字经济也必将拥有健康发展的新助力。（来源：最高人民法院）

- **《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》**
- **全文：**https://mp.weixin.qq.com/s/kSX19JbG3w8crfiSoeNq7A

五、本期重要漏洞实例

➢ Microsoft 发布 2021 年 7 月安全更新

发布日期：2021-07-14

更新日期：2021-07-14

描述：7 月 14 日，微软发布了 2021 年 7 月份的月度例行安全公告，修复了其多款产品存在的 117 个安全漏洞。受影响的产品包括：Windows 10 21H1 (68 个)、Windows 10 20H2 & Windows Server v20H2（75 个）、Windows 10 2004 & Windows Server v2004（75 个）、Windows 8.1 & Server 2012 R2（50 个）、Windows Server 2012（44 个）、Windows RT 8.1（39 个）和 Microsoft Office-related software（10 个）。利用上述漏洞，攻击者可以绕过安全功能限制，获取敏感信息，提升权限，执行远程代码，或发起拒绝服务攻击等。提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

CVE 编号	公告标题	最高严重等级和漏洞影响	受影响的软件
CVE-2021-34458	**Windows Kernel 远程代码执行漏洞**	严重 远程代码执行	Server, version 20H2 Server, version 2004 Server 2019 Server 2016
CVE-2021-31979/33771	**Windows Kernel 权限提升漏洞**	重要 特权提升	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-34450	**Windows Hyper-V 远程代码执行漏洞**	严重 远程代码执行	Server, version 20H2 Windows 10 Server, version 2004 Server 2019
CVE-2021-34494	**Windows DNS Server 远程代码执行漏洞**	严重 远程代码执行	Server, version 20H2 Server, version 2004 Server 2019 Server 2016 Server 2012 R2 Server 2012
CVE-2021-34527	**Windows Print Spooler 远程代码执行漏洞**	严重 远程代码执行	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2

			Server 2012 Windows 8.1
CVE-2021-34448	**Scripting Engine 内存破坏漏洞**	严重 远程代码执行	Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-34501	**Microsoft Excel 远程代码执行漏洞**	重要 远程代码执行	365 Apps Enterprise Excel 2016 Excel 2013 Office 2019 Office 2019 for Mac Office Online Server
CVE-2021-34452	**Microsoft Word 远程代码执行漏洞**	重要 远程代码执行	Word 2016 365 Apps Enterprise Office 2019
CVE-2021-34520	**Microsoft Share Point Server 远程代码执行漏洞**	重要 远程代码执行	SharePoint Foundation 2013 SharePoint Server 2019 SharePoint Enterprise Server 2016

来源：https://msrc.microsoft.com/update-guide/releaseNote/2021-Jul

➢ Oracle MySQL Server 拒绝服务漏洞

发布日期：2021-07-26
更新日期：2021-07-26
受影响系统：
Oracle MySQL Server <=8.0.25
描述：

CVE(CAN) ID: CVE-2021-2383
Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。Oracle MySQL Server 8.0.25 及更早版本中的 Server: Optimizer 组件存在拒绝服务漏洞。攻击者可利用该漏洞导致 MySQL 服务器挂起或频繁重复崩溃（完全拒绝服务）。
建议：

厂商补丁：
Oracle
厂商已发布了漏洞修复程序，请及时关注更新：
https://www.oracle.com/security-alerts/cpujul2021.html

➢ Cisco Identity Services Engine 跨站脚本漏洞

发布日期：2021-07-07
更新日期：2021-07-26
受影响系统：
Cisco Identity Services Engine < 3.0 Patch 3
Cisco Identity Services Engine < 2.7 Patch 4
Cisco Identity Services Engine < 2.6 Patch 9
描述：

CVE(CAN) ID: CVE-2021-1607
Cisco Identity Services Engine（ISE）是美国思科（Cisco）公司的一款基于身份的环境感知平台（ISE 身份服务引擎）。该平台通过收集网络、用户和设备中的实时信息，制定并实施相应策略来监管网络。
Cisco Identity Services Engine (ISE) 2.6 Patch 9 之前版本、2.7 Patch 4 之前版本和 3.0 Patch 3 之前版本存在跨站脚本漏洞。该漏洞源于 web 管理界面未对用户输入进行正确验证。攻击者可利用该漏洞通过说服受影响界面的用户单击特制的链接从而执行任意脚本代码或访问敏感信息。
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stored-xss-TWwjVP
建议：

厂商补丁：
Cisco

Cisco 已经为此发布了一个安全公告（cisco-sa-ise-stored-xss-TWwjVPdL）以及相应补丁:
cisco-sa-ise-stored-xss-TWwjVPdL：Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerabilities
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stored-xss-TWwjVPdL

➢ IBM Sterling Secure Proxy 拒绝服务漏洞

发布日期：2021-07-15
更新日期：2021-08-05
受影响系统：
IBM Secure External Authentication Server 6.0.2
IBM Secure External Authentication Server 6.0.1
IBM Secure External Authentication Server 2.4.3.2
IBM Secure Proxy 6.0.2
IBM Secure Proxy 6.0.1
IBM Secure Proxy 3.4.3.2
描述：

CVE(CAN) ID: CVE-2021-29725

IBM Sterling Secure Proxy 是美国国际商业机器公司（IBM）的一个用于确保组织非保护区(DMZ)中文件安全传输的应用程序代理。

IBM Secure External Authentication Server 2.4.3.2、6.0.1 和 6.0.2 版本以及 IBM Secure Proxy 3.4.3.2、6.0.1 和 6.0.2 版本存在拒绝服务漏洞。远程攻击者可利用该漏洞消耗资源，从而导致拒绝服务。

链接：https://www.ibm.com/support/pages/node/6471615

建议：

厂商补丁：

IBM

IBM 已经为此发布了一个安全公告（6471615）以及相应补丁：

6471615：Security Bulletin: Multiple Vulnerabilities were detected in IBM Secure External Authentication Server

链接：https://www.ibm.com/support/pages/node/6471615

六、本期网络安全事件

➢ 解析 “滴滴出行”“BOSS 直聘”等接受网络安全审查，原因是什么？

2021 年 7 月 2 日，为防范国家数据安全风险，维护国家安全，保障公共利益，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》，网络安全审查办公室按照《网络安全审查办法》，对“滴滴出行”实施网络安全审查。为配合网络安全审查工作，防范风险扩大，审查期间“滴滴出行”停止新用户注册。 7 月 4 日，国家互联网信息办公室通知应用商店下架“滴滴出行”App，要求滴滴出行科技有限公司严格按照法律要求，参照国家有关标准，认真整改存在的问题，切实保障广大用户个人信息安全。7 月 5 日，网络安全审查办公室关于对“运满满”“货车帮”“BOSS 直聘”启动网络安全审查的公告。7 月 16 日，国家网信办会同公安部、国家安全部、自然资源部、交通运输部、税务总局、市场监管总局等部门联合进驻滴滴出行科技有限公司，开展网络安全审查。

对此，滴滴回应称，滴滴将积极配合网络安全审查。审查期间，我们将在相关部门的监督指导下，全面梳理和排查网络安全风险，持续完善网络安全体系和技术能力。受此消息影响，滴滴（NYSE：DIDI）盘前转跌，截至发稿跌 6.1%，报 15.91 美元。

“运满满”官网称，“运满满已经成为全球出类拔萃的整车运力调度平台和智慧物流信息平台”。“货车帮”公司官网则介绍，“货车帮”是中国最大的公路物流互联网信息平台，建立了中国第一张覆盖全国的货源信息网，并为平台货车提供综合服务，致力于做中国公路物流基础设施。“BOSS 直聘”官网介绍称，该平台应用人工智能、大数据前沿技术，提高雇主与人才的匹配精准度，缩短求职招聘时间，从而提升求职招聘效率。

综合来看，这几家企业都掌握大量用户隐私数据，并且业务与关键信息基础设施有关联。

“上述几家被审查的企业，分别为日常出行、网络货运及大众求职领域的头部平台，至少掌握了所属行业领域 80%以上的深度数据。这些数据可以直接或间接地反映我国各区域人口分布、商业热力、人口流动、货物流动、企业经营等情况。”江苏省大数据交易和流通工程实验室副主任李可顺表示。

值得注意的是，这几家被审查的企业有着共同的特点：近期赴美上市。

经查阅资料发现，2021 年 6 月 11 日，“BOSS 直聘”于美国上市；6 月 22 日，拥有“运满满”和“货车帮”的满帮集团于美国上市；6 月 30 日，国内最大的移动出行平台滴滴于美国上市。

滴滴作为一家主要在中国经营的企业，所有数据首先是存储在本地的。但是，在美国上市将不可避免地涉及数据出境问题。去年 6 月份，美国参议院提出了《外国公司问责法案》，该法案规定，如果外国公司连续三年未能通过美国公众公司会计监督委员会的审计，将被禁止在美国任何交易所上市。而有关信息的披露，可能导致重要数据、个人信息的泄露。今年 3 月份，美国证券交易委员会表示，通过了《外国公司问责法案》最终修正案。

据了解，美国证券市场对于上市公司有很高的信息披露要求，包括必须根据美国公认会计原则编报其财务报表、必须根据美国证券法律规定，对公司重大信息及时披露等，这势必涉及一些该公司在中国境内的经营情况数据是否能够出境的问题。

数据安全，关乎国家安全

近几年，大数据、云计算、物联网等技术和应用高速发展，互联网企业在为人们生活带来便利的同时，跨境数据流动、用户数据泄露等问题，也受到广泛关注。

中国人民大学信息学院教授孟小峰在《人民论坛》刊文表示，随着数据的累积，不同科技企业在数据资源的储备量上的差异也愈加明显，数据垄断逐渐形成，并催生了“堰塞湖”，各企业间的数据难以互通，并且由于数据本身与个人隐私的密切关系，用户隐私泄露问题亦随之凸显。

孟小峰指出，各类 APP 中，工具类、社交类和游戏类为数据垄断的重灾区。工具类、社交类和游戏类的前 0.1%数据收集者收集了约 80%的权限数据，前 1%的数据收集者收集了约 95%的权限数据，而前 5%的数据收集者就收集了约 99%的权限数据。对数据进行有效治理迫在眉睫。

不难看出，大量数据在互联网企业生成、汇聚、融合，在释放数据价值的同时也带来了

巨大的数据安全风险。

中国信息通信研究院互联网法律研究中心研究员赵淑钰指出，“一方面，造成侵犯用户个人信息的风险，目前过度收集、滥用用户个人信息的情形依然多发高发；另一方面，也会对国家安全产生影响，随着数据分析技术的飞跃发展，互联网企业在运营过程中产生的巨量数据通过大数据分析能够反映出我国整体经济运行情况等涉及国家秘密的信息，对总体国家安全构成重大安全威胁。”互联网企业的数据安全问题也可能从不同方面影响国家安全。类似地图数据、位置数据等重要数据，同样需要保护。

如何维护数据主权和国家安全？

习近平总书记指出：“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。”要统筹推进网络安全工作，坚持网络安全为人民、网络安全靠人民，坚持网络安全教育、技术、产业融合发展，坚持促进发展和依法管理相统一，坚持安全可控和开放创新并重，切实保障国家网络安全和公民个人信息安全。

第一，强化关键信息基础设施防护。关键信息基础设施是经济社会运行的神经中枢，涉及国家安全、国计民生以及公共利益，对于国家网络安全和信息化建设意义重大。要严格落实《中华人民共和国网络安全法》、网络安全工作责任制要求，夯实关键信息基础设施防护责任，强化不同地区、不同行业、不同领域关键信息基础设施之间的威胁信息共享和协同应对，建立完善关键信息基础设施安全保障体系。加强网络安全检查，明确保护范围和对象，及时发现隐患、修补漏洞，做到关口前移，防患于未然。

第二，强化数据安全管理。在积极开发利用数据资源、充分释放数据效能的同时，切实保障数据安全，强化关键数据资源保护能力。健全管理和运用数据资源的法律制度和政策措施，依法保护数据资源。加大个人信息保护力度，规范个人信息的收集、处理和利用，完善保护机制，依法坚决打击各种形式的网络诈骗、侵犯知识产权、侵犯公民隐私等网络违法犯罪活动。督促企业加强数据安全风险评估，加强对大数据企业的监督管理和责任追究，打造安全可靠的数据生态环境。

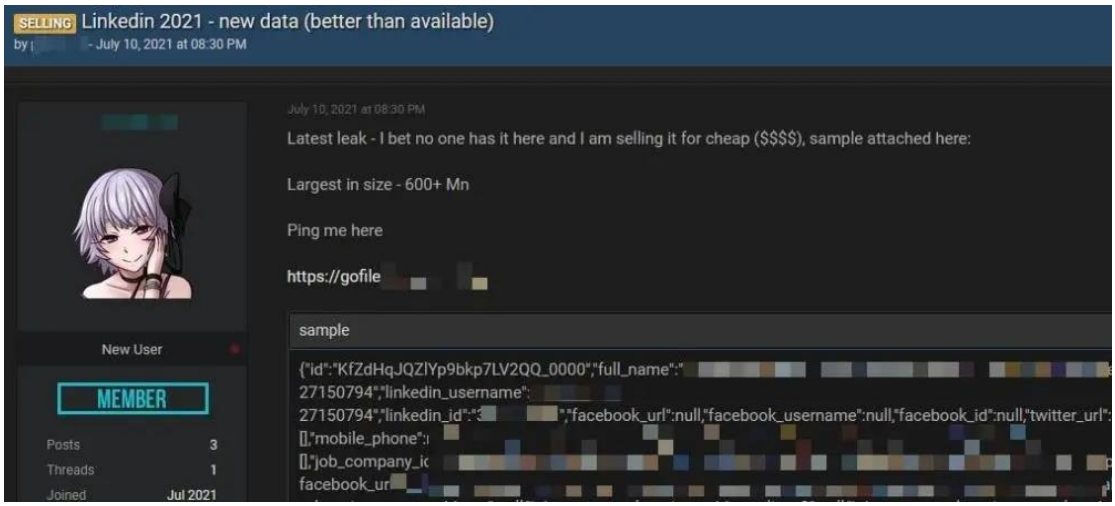
第三，强化网络安全应急处置能力。加强网络安全信息统筹机制、手段、平台建设，实时监测预警网络安全重大事件，既掌握网络空间当前状态，又分析下一步动态，为科学决策指挥提供依据。加强网络安全事件应急指挥能力建设，健全完善网络安全监测预警响应机制，提升网络安全态势感知、事件分析、追踪溯源以及遭受攻击后的快速恢复能力。

第四，强化网络安全工作基础。大力发展网络安全产业，加强网络安全产业统筹规划和整体布局，培育扶持一批具有国际竞争力的网络安全企业。加强网络安全教育，加快推进国

家网络安全人才与创新基地建设，积极开展一流网络安全学院建设示范项目。深入开展网络安全知识技能宣传普及，办好国家网络安全宣传周，不断提高广大人民群众网络安全意识和防护技能。（来源：互联网综合整理）

➢ 四个月内 领英用户个人信息已被兜售三次

2021 年 7 月 13 日，继领英（LinkedIn）5 亿用户信息被出售的两个月后，近日，7 亿条领英用户信息再次出现在黑客论坛上被售卖。领英系微软旗下的拥有 7 亿多用户的职场社交平台，许多用户在此平台上公开自己的教育背景、从业经历等信息。据外媒报道，名为“GOD User”的卖家在一黑客论坛上发帖称，他们在 2021 年 6 月 22 日获得 7 亿条领英用户信息，并提供了 100 万条用户信息样本作为证明。具体而言，被出售的领英用户信息包括：用户全名、性别、电子邮件地址、电话号码和行业信息等。



当地时间 6 月 26 日，领英回复媒体称，“虽然我们仍在调查这个问题，但我们的初步分析表明，此数据集包括了从领英抓取的用户信息以及其他渠道获得的信息。这并非领英的数据泄露事件，我们的调查已经确定，领英私人会员用户数据没有遭到泄露。从领英抓取数据违反了我们的服务条款，我们一直在努力保护我们会员的隐私。”领英在上述回应中强调，数据集包括了“从领英抓取的用户数据”。与两个月前的“5 亿领英用户简历被抛售”事件类似的是，或都与“数据抓取”相关。

今年 4 月，据媒体报道，某知名黑客论坛有黑客发帖出售 5 亿领英用户数据，具体信息包括：全名、邮件地址、手机号码、工作地址等。

当地时间 4 月 8 日，领英在其官网发布声明称，“我们调查了一组涉嫌出售的 LinkedIn

数据，并确定它实际上是来自许多网站和公司的数据的聚合。它确实包括可公开查看的会员个人资料数据，这些数据似乎是从领英上抓取的，其中在我们能够审查的内容中，并没有发现来自领英的私人会员帐户数据。”实际上，领英的用户数据被抓取已非首次引发关注。据此前报道，早在 4 年前，因反对数据抓取，领英就曾将竞争对手 hiQ Labs 告上法庭。

领英方面表示，hiQ Labs 对用户数据的大规模自动抓取，违反了领英用户协议中的访问和使用限制，等同于黑客行为，威胁到用户的隐私。

hiQ Labs 辩称，公共数据必须保持公开，大公司不应以垄断的方式囤积公共数据，领英的诉求会影响互联网的开放和创新。而且，hiQ Labs 只将抓取的信息用于宏观分析，并未售卖用户的个人资料。

从 2017 年至今，领英的反数据抓取诉讼未有结论。搜索引擎作为互联网非常重要的一部分，其对网页的抓取正是利用爬虫工具。如果禁止爬取数据，搜索引擎也许将不能使用。另外，进入大数据时代，非法的数据爬取带来的数据泄露等负面影响正不断显现。就在前不久，6 月 14 日，美国最高法院要求下级法院重审 hiQ Labs 抓取领英用户数据一案。（来源：隐私护卫队）

➢ 厦门某知名快捷酒店被发现摄像头案件告破

2021 年 7 月 12 日，最近，厦门“长青路某酒店房间发现微型摄像头案”备受关注。7 月 12 日下午，厦门警方发布最新通报，这起案件告破，犯罪嫌疑人已被刑拘。通报全文如下：“长青路某酒店房间发现微型摄像头案”告破，犯罪嫌疑人被刑拘！我市警方接到关于长青路某酒店房间发现微型摄像头的报警后，立即组织刑侦支队、思明分局及相关部门全力开展侦查。

经技术检验鉴定、深入研判分析和缜密侦查，我市警方于 7 月 10 日奔赴泉州，在某住宅小区抓获案件嫌疑人刘某煌（男，29 岁，泉州人），并在其住处电脑和手机缴获其偷拍视频，目前未发现外传。

经审查，刘某煌供认其为满足个人偷窥欲望，从网上购买微型摄像头，入住长青路某酒店房间时，将微型摄像头安装到房间筒灯内，用于偷拍他人隐私。

目前，犯罪嫌疑人刘某煌因涉嫌非法使用窃听、窃照专用器材罪已被警方依法刑事拘留，案件正在进一步审查中。警方同时敦促涉事酒店进行彻查整改。

厦门警方表示：对侵犯他人隐私的违法犯罪行为，将坚决依法惩处，绝不姑息！7 月 7 日，福建厦门警方通报长青路某知名快捷酒店被曝藏摄像头事件。厦门思明区警方第一时间受案调查，对可疑灯筒、微型摄像头送检鉴定。6 月底一名网友入住该知名酒店，在房间内发现微型摄像头。酒店负责人称已配合警方调查，排查其他房间并未发现摄像头。（来源：环球时报）

➢ 伊朗国家铁路遭网络攻击，各地车站大屏传播虚假延误信息

2021 年 7 月 10 日，据伊朗国内的法尔斯通讯社报道，伊朗铁路系统在当地时间 7 月 9 日遭遇网络攻击，攻击者在全国各地车站的显示屏上大肆发布关于火车延误或取消的虚假信息。显示屏上的通报信息提到，火车“因网络攻击而长时间延误”或“取消”，并敦促乘客拨打电话查询更多详细信息。而这里留下的，恰恰是伊朗最高领导人阿亚图拉·阿里·哈梅内伊办公室的座机号码。

网络攻击导致伊朗火车站爆发出“前所未有的混乱局面”。不过法尔斯社称，攻击活动并未引发运力中断，希望尽量淡化事件影响。

ABC News 报道称，“法尔斯社后来删除了报道，转而引用国家铁路公司发言人萨德·塞克里的的解释，即「中断」并未对火车乘运服务造成任何影响。”

截至本文发布时，仍不清楚这次攻击的幕后黑手是谁，也没有任何团伙宣称对此次事件负责。

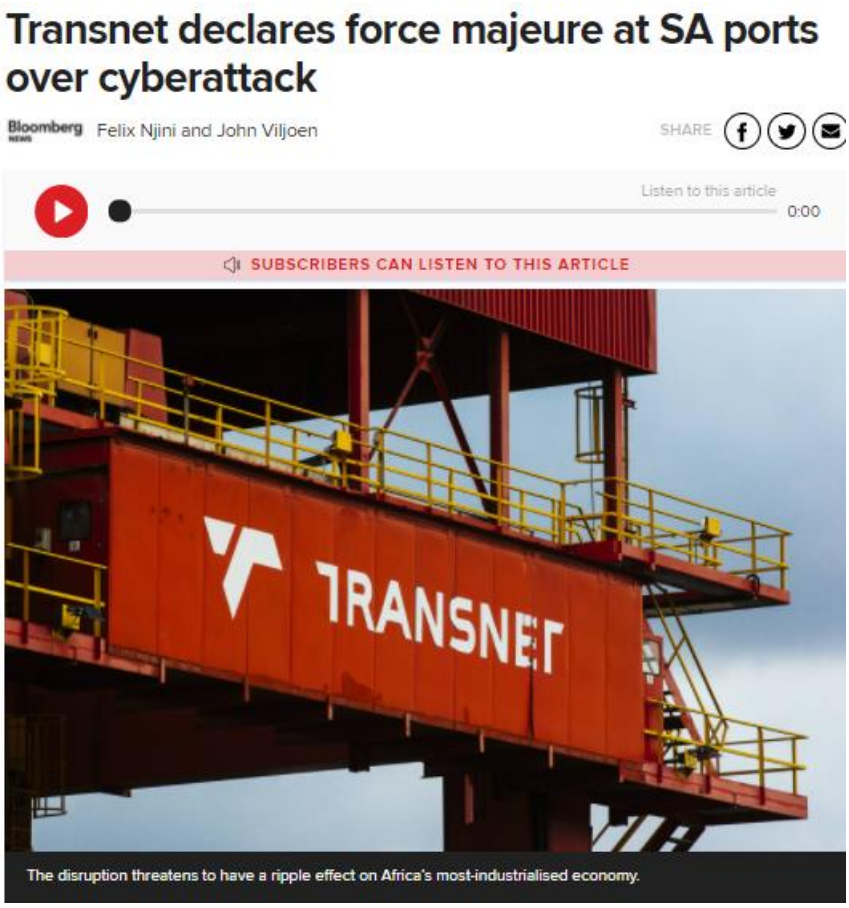
但伊朗铁路系统当前的麻烦还不止于此。同一天早些时候，伊朗各地火车突然爆发电子跟踪系统失灵。目前还不清楚二者是否有所关联。

当地时间 7 月 10 日，伊朗国家电视台报道，伊朗道路和城市发展部的内部计算机系统 10 日遭到网络攻击，使得该部网站和旗下其他网站中断服务。报道没说怀疑对象和黑客是否索要赎金。（来源：央视新闻）

➢ 南非主要港口系统遭受黑客攻击 港口货运被迫延迟

2021 年 7 月 28 日，据南非媒体当地时间 7 月 27 日报道，南非国有物流公司（Transnet）表示，其主要港口的 IT 系统近一周来遭受网络攻击，对港口集装箱运输产生了巨大影响。目前部分原定停靠开普敦和德班的集装箱船已转移到周边国家港口装卸货物，如南非邻国莫桑比克的港口等。

这将导致集装箱船上的货主需要等待很长时间才能收到订购的货物。未来南非市场因骚乱导致的部分商品短缺现象将进一步加剧，同时大量出口矿产也将无法运出。南非国有物流公司 27 日表示，相关港口码头问题预计将很快解决，但没有提供时间表或原因细节。



刚刚结束的骚乱已让南非多个港口停止运行，此次的系统瘫痪不仅将加大南非目前部分商品短缺的状况，还将进一步打击该国疫情下的经济复苏。（来源：央视网）

➢ 离职后心生不满西安某医院前网管“炫技性报复”整个医院系统瘫痪

2021 年 7 月 30 日华商报报道，因对医院不满遂产生报复念头西安某医院网络管理员离职后利用自学网络知识非法入侵医院内网服务器远程进行破坏性操作致使该院诊疗系统瘫痪无法正常诊治

今年 3 月起，西安市莲湖区一家医院的网络系统持续出现故障，导医台、诊室、药房和病历系统等网络设备无法正常联网，医院诊疗秩序受到破坏。据医院负责人介绍，有时候是打印机连不上网，药也开不出来，有时候是 CT 机无法使用，还有 B 超机用不成……从 3 月中旬到 5 月中旬，这样的情况陆陆续续出现，直到医院的诊疗系统全面瘫痪。

经医院网络工程师初步排查，医院网络系统重要文件疑似被人为更改，连病人的病历也被删除，诊疗系统全面瘫痪。5 月 15 日，医院负责人向公安莲湖分局报警。

公安莲湖分局网络安全保卫大队接到报警后，迅速联合属地红庙坡派出所成立专案组

进行案件侦破，第一时间对受破坏网络系统开展电子证据数据侦查、取证工作，收集攻击日志近 10 万条，提取电子证据 1.2TB。

经过连续月余技术攻关，分析海量服务器数据后，发现多条可疑 IP 地址先后十余次非法登录该院计算机系统，并更改、删除、重置重要文件的记录。通过进一步侦查，最终锁定医院前系统管理员、41 岁的男子白某某有重大作案嫌疑。

在掌握白某某犯罪证据后，专案组抽调精干力量对其实施抓捕，当场查获作案用电脑 1 台、手机 1 部、硬盘 1 个及用于作案的软件 1 款。

经审查，犯罪嫌疑人白某某系医院前网络系统管理员。其在办理离职手续时，听到院方一位领导说其岗位不重要的话，遂产生报复心理。为了证明自己的实力，白某某利用自学网络知识，非法入侵医院内网服务器，远程进行破坏性操作。

办案民警说，白某某此举实际上就是一种炫技性的报复，他对医院的网络系统非常熟悉，因为他参与了早期医院诊疗系统的建设，所以知道什么是核心内容，非法入侵时有针对性地进行破坏。此案也是西安公安莲湖分局侦破的首例破坏医院计算机信息系统案。

目前，犯罪嫌疑人白某某对其破坏计算机系统的犯罪事实供认不讳，白某某因涉嫌破坏计算机信息系统罪被莲湖公安依法刑事拘留，莲湖区检察院已对其批准逮捕，案件正在进一步侦查中。（来源：华商报）

信息安全意识产品服务

021-33663299