国盟信息安全通报

2021 年 01 月 31 日第 233 期

全国售后服务中心

国盟信息安全通报

（第 233 期）

国际信息安全学习联盟

2021 年 1 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 378 个，其中高危漏洞 94 个、中危漏洞 247 个、低危漏洞 37 个。漏洞平均分值为 5.95。本周收录的漏洞中，涉及 0day 漏洞 140 个（占 37%），其中互联网上出现“JIZHICMS 跨站脚本漏洞、ZZCMS SQL 注入漏洞（CNVD-2021-04410）”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 6101 个，与上周（4306 个）环比增加 42%。

主要内容

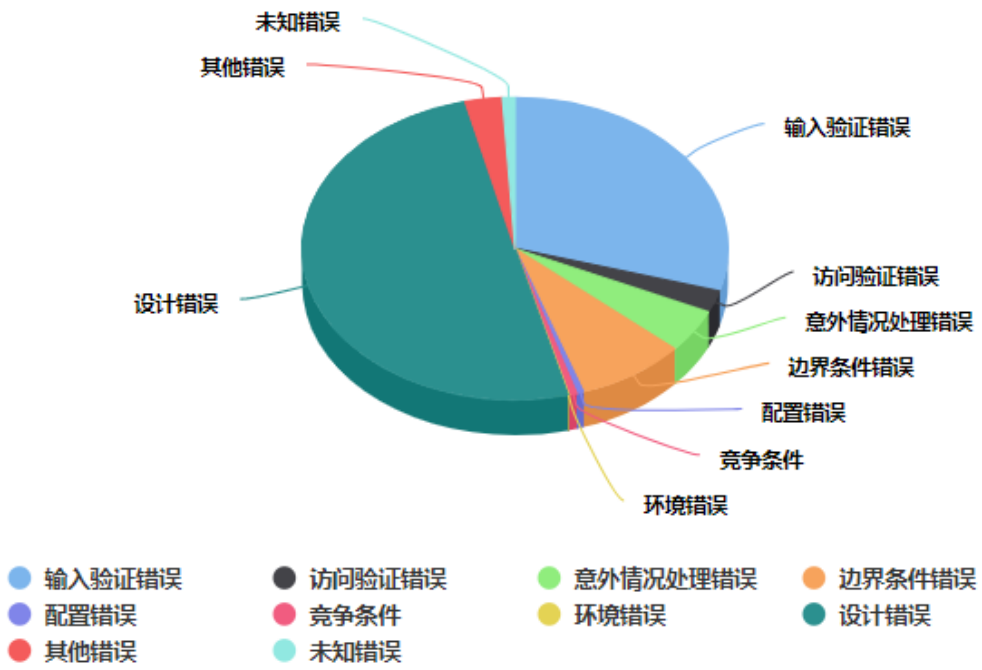
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

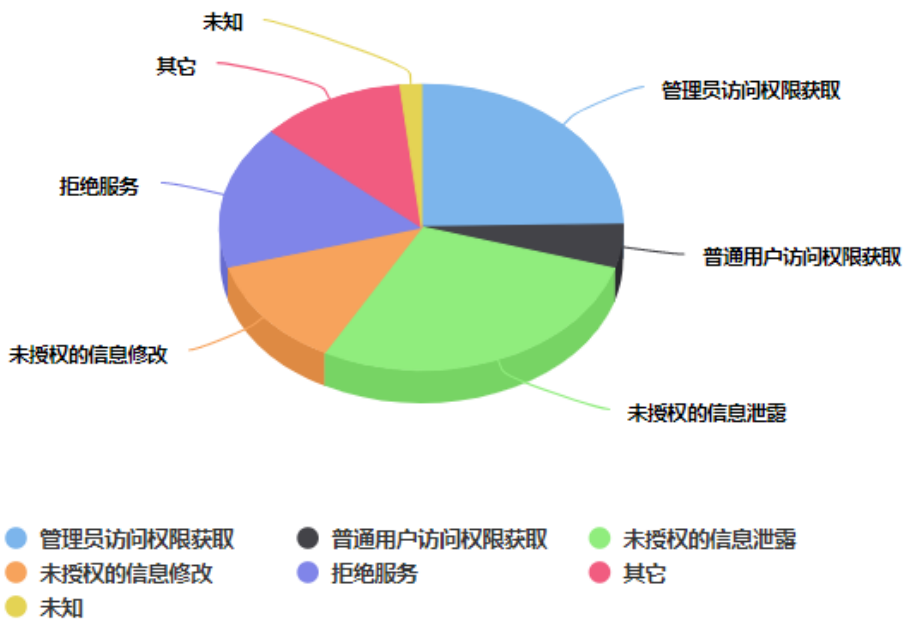
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 378 个，其中高危漏洞 94 个、中危漏洞 247 个、低危漏洞 37 个。漏洞平均分值为 5.95。本周收录的漏洞中，涉及 0day 漏洞 140 个（占 37%），其中互联网上出现“JIZHICMS 跨站脚本漏洞、ZZCMS SQL 注入漏洞（CNVD-2021-04410）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 6101 个，与上周（4306 个）环比增加 42%。

二、安全漏洞增长数量及种类分布情况

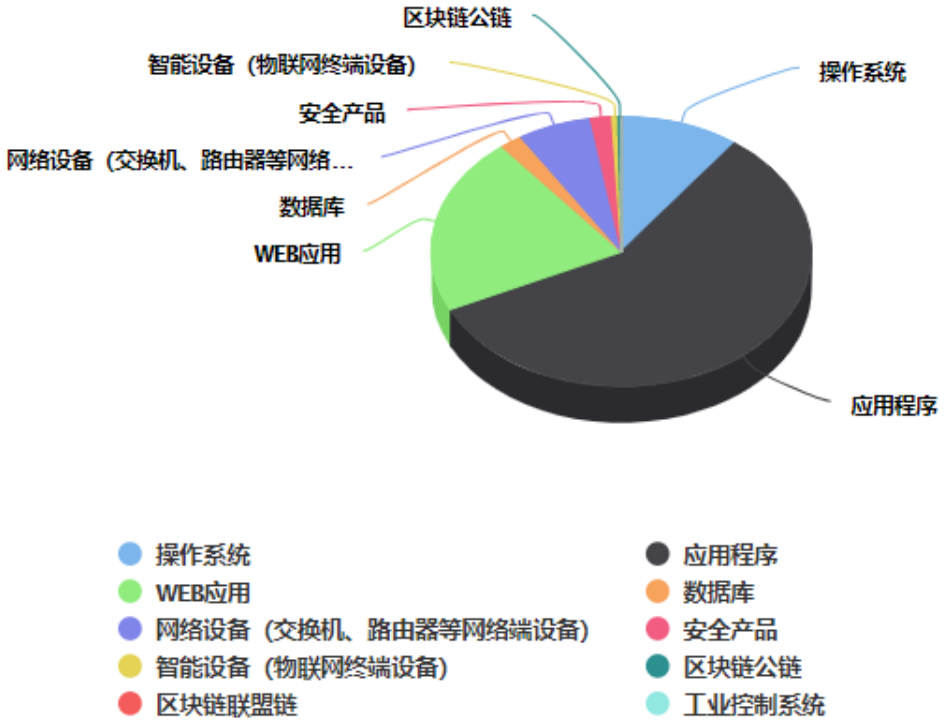
➢ **漏洞产生原因（2021 年 1 月 17 日—2021 年 1 月 31）**



➢ 漏洞引发的威胁（2021 年 1 月 17 日—2021 年 1 月 31）



➢ 漏洞影响对象类型（2021 年 1 月 17 日—2021 年 1 月 31）



三、安全产业动态

➢ 推进网络强国建设 习近平“典”明这些要义

近日，中共中央党史和文献研究院编辑的《习近平关于网络强国论述摘编》一书在全国发行。当今世界，网络信息技术日新月异，全面融入社会生产生活，深刻改变着全球经济格局、利益格局、安全格局。党的十八大以来，以习近平同志为核心的党中央对维护网络安全、培养网络人才、创新网络技术等方面作出一系列重要部署。习近平总书记多次引经据典讲述网络治理的现实意义，妙语频出、发人深省，为网络强国建设指明方向。

谈网络空间 擘画最大同心圆

“知屋漏者在宇下，知政失者在草野。”2016 年 4 月 19 日，习近平总书记主持召开网络安全和信息化工作座谈会并发表重要讲话。他引用东汉哲学家王充之言，提醒各级领导干部要“善于运用网络了解民意、开展工作”，并强调这是“新形势下领导干部做好工作的基本功”。

早在华夏文明诞生之初，民本思想就随之形成。基层工作的重要性，古代先贤们已经给出提示。身处新时代，如何做好基层工作？如何走好党的群众路线？习近平总书记提出要求：

“各级党政机关和领导干部要学会通过网络走群众路线，经常上网看看，潜潜水、聊聊天、发发声，了解群众所思所愿，收集好想法好建议，积极回应网民关切、解疑释惑。”

“国皆有法，而无使法必行之法。”早在 2006 年，习近平就曾在《弘扬法治精神，形成法治风尚》一文引用《商君书·画策第十八》中的这句话来说明法治精神的重要性。2015 年 9 月 22 日，习近平总书记在接受《华尔街日报》的书面采访时指出，互联网这块“新疆域”不是“法外之地”，同样要讲法治。

网络空间风清气正，是人民的共同期待。没有法治精神，再精密的法律条文都难免沦为摆设。因此必须依法加强网络空间治理，培育积极健康、向上向善的网络文化。

“君子务本，本立而道生。”2016 年 11 月 16 日，习近平主席在第三届世界互联网大会开幕式上发表视频讲话指出：“坚持以人类共同福祉为根本，坚持网络主权理念，推动全球互联网治理朝着更加公正合理的方向迈进，推动网络空间实现平等尊重、创新发展、开放共享、安全有序的目标。”

“坚持以人类共同福祉为根本”是中国的一贯主张。互联网是我们这个时代最具发展活力的领域。利用好、发展好、治理好互联网同样需要“务本”。这个根本便是坚持以人类共同福祉为根本，构建网络空间命运共同体。

习近平总书记讲述的这三个典故，有着共同主题：即构建清朗的网络空间，形成网上网下同心圆。如何建好这个“同心圆”？就要凝心聚力，坚持党的领导，团结全国各族人民心往一处想、劲往一处使；知“网事”“网情”坚持群众路线，打造网络舆论新平台；“净网”“护网”弘扬法治精神，扫清网络污染物；参与全球治理，谋求国际共识，构建网络空间命运共同体。

谈网络安全 要求知己知彼、百战不殆

习近平总书记高度重视网络安全，强调“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”。

如何加强网络安全，打赢网络安全攻坚战？他也提到了三个典故：

“魔高一尺、道高一丈。”出自《初刻拍案惊奇》。习近平总书记将原文中的“道高一尺、魔高一丈”反用为“魔高一尺、道高一丈”，要求网络安全工作者首先要有足够的技术力量来维护网络安全，增强网络安全防御能力和威慑能力。他说：“人家用的是飞机大炮，我们这里还用大刀长矛，那是不行的，攻防力量要对等。”

“知己知彼，才能百战不殆。”出自《孙子兵法·谋攻篇》。在复杂严峻的网络安全态势下，习近平总书记要求网络安全工作者要全天候、全方位感知网络安全态势，知道谁进来了、

是敌是友、干了什么。

“聪者听于无声，明者见于未形。”出自《汉书·伍被传》，习近平总书记用这句古语强调网络安全风险的预见性，要求全面加强网络安全检查。“维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险。”

习近平总书记对防范风险的客观规律有着科学的判断和认识。他强调攻防力量对等，确保在实际对抗中不落下风；要求各领域网络安全工作者要知己知彼，更要听于无声、见于未形，全面掌握网络安全风险，规避网络安全事故，实现不战而屈人之兵。

谈网络技术 强调得人者兴

“得人者兴，失人者崩。”出自《史记·商君列传》，习近平总书记引用此典来强调网络人才的重要性。“念好了人才经，才能事半功倍”，因此要聚天下之英才而用之，为网信事业发展提供有力的人才支撑。

“日日行，不怕千万里；常常做，不怕千万事。”出自《格言联璧·处事》。习近平总书记说：“我国网信领域广大企业家、专家学者、科技人员要树立这个雄心壮志，要争这口气，努力尽快在核心技术上取得新的重大突破。”

互联网核心技术的重要性不言而喻，习近平总书记引用这句古语鼓励网信领域相关工作者，要坚持不懈去探索，脚踏实地去工作，争取尽快在核心技术上取得突破。

随时以举事，因资而立功，用万物之能而获利其上。网信事业代表着新的生产力、新的发展方向。站在新的历史节点，我们必须坚持以习近平总书记关于网络强国的重要思想为指导，抓住互联网发展的关键时机，绘就网上网下同心圆，发挥好网信人才作用，守护住网络安全，不断开创网信工作新局面。（来源：中央广播电视总台央视网）

➢ 加快发展网络信息技术

新冠肺炎疫情防控不仅是我国卫生健康领域的一场战役，也是科学技术领域的一次大考。习近平总书记在全国抗击新冠肺炎疫情表彰大会上的重要讲话中指出：“无论是开展大规模核酸检测、大数据追踪溯源和健康码识别，还是分区分级差异化防控、有序推进复工复产，都是对科学精神的尊崇和弘扬，都为战胜疫情提供了强大科技支撑”。疫情防控取得重大战略成果，包括网络信息技术在内的科技功不可没。

在这场惊心动魄的抗疫大战中，网络信息技术发挥了重要作用：健康码的使用，为阻断

疫情传播路径、防控疫情扩散提供了重要技术支持；借助人工智能技术，机器人能够帮助医疗机构处理前期问询、预诊等许多非紧急工作，还能帮助医生对病人进行远程诊疗，降低医护人员与病患交叉感染的可能性；基于网络信息技术的保障支持，在线购物、网上观剧、视频聊天、网络教育等蓬勃发展；等等。目前，疫情仍在全球蔓延，国内零星散发病例和局部暴发疫情的风险仍然存在，我们要继续毫不放松抓紧抓实抓细各项防控工作。取得抗疫斗争全面胜利，网络信息技术可以再立新功。

继续发挥大数据优势，提供更精准的决策依据。疫情防控需要公安、交通、劳动等管理部门以及电信和互联网企业的数据支撑，需要提升数据整合能力。只有实现数据深度协同，才能更好地发挥大数据的决策支撑作用。要继续发挥网络优势，提供更畅通的远程会诊、远程医疗，最大程度集中优势诊疗资源，发挥各地专家的集体智慧；优化在线教育平台，不断提升在线教育平台的技术水平；保障网络安全，防范利用新冠肺炎疫情实施的网络攻击行为，如网络攻击者将计算机病毒、木马和移动恶意程序等伪装成“肺炎病例”“防护通知”等信息，通过钓鱼邮件、恶意链接等方式进行传播。此外，疫情防控信息的报送流转和大数据利用，容易造成个人信息的泄露，需要网络安全、公安执法等部门联手打击网络犯罪、防范数据泄露。

习近平总书记在统筹推进新冠肺炎疫情防控和经济社会发展工作部署会议上指出：“疫情对产业发展既是挑战也是机遇。一些传统行业受冲击较大，而智能制造、无人配送、在线消费、医疗健康等新兴产业展现出强大成长潜力。要以此为契机，改造提升传统产业，培育壮大新兴产业。”当前，国家 IPv6 部署行动计划到了收官之时，5G 商用步伐不断加快，这为

我国“互联网+”的发展、“人工智能+”的发展提供了重要的信息技术基础。从这个角度看，疫情给我国经济转型升级、网络信息技术发展都带来了机遇。我们要抓住机遇，努力化危为机。比如，在以 IPv6 与 5G 为代表的信息基础设施上加大投入，为长远发展奠定信息基础。同时，可以出台激励与扶持政策，鼓励各个行业与互联网、人工智能深度融合，催生出新的产业和行业。尤为重要的是，要加大关键核心技术创新发展的投入力度。关键核心技术是国之重器，对推动我国经济高质量发展、保障国家安全具有十分重要的意义。应继续加大投入、鼓励创新，力争实现更大突破，彻底改变一些关键核心技术受制于人的局面，为网络强国建设奠定更为坚实的基础。（来源：人民日报　作者为中国工程院院士、清华大学网络科学与网络空间研究院院长）

➢ 央行科技司李伟：做好数据治理，强化个人隐私保护

2021 年 1 月 9 日，在新金融联盟举办的“金融数据治理与个人信息保护”内部研讨会上，中国人民银行科技司司长李伟表示，金融科技的发展始于技术、兴于数据、稳于制度、成于价值观。既不能没有数据让技术空转，也要防止滥用数据造成信息泄露、隐私侵权等问题。做好数据治理、强化信息保护、破解数据安全之困是当前亟待攻关的关键课题。对此，李伟提出四点建议：严防违规滥用数据扰乱市场秩序；推动数据要素规范高效有序流通；强化金融消费者的隐私保护；着力做好金融数据标准化工作。**以下为全文：**

党的十九届四中全会首次将“数据”列为生产要素。五中全会审议通过的十四五规划和

2035 年远景目标的建议提出要推动数据资源开发利用，加强个人信息保护。2020 年中央经济工作会将“强化反垄断和防止资本无序扩张”列为 2021 年八项重点工作之一，并明确提出要完善数据收集使用管理。数据利用和保护已经被提到了很高的层面。

金融和数据天生密不可分，数据价值在金融领域被发现、证实和运用，不断推动金融业务的运行逻辑、经营模式、管理方式的变革和优化。金融科技的发展始于技术、兴于数据、稳于制度、成于价值观。

始于技术，不能没有数据光让技术空转，必须要有生产要素在其中发挥作用；兴于数据，因数据而蓬勃发展的同时也要意识到数据泄露、隐私侵权等问题已经很严重。做好数据治理、强化信息保护、破解数据安全之困是我们亟待解决的关键课题。借今天的机会，我讲几个观点。

第一，严防违规滥用数据扰乱市场秩序。技术是中性的，技术运用善恶完全取决于人，这个结论对数据同样适用。数据应用得当能够提升金融服务精准性、可得性和普惠性，数据应用不当则会引发新的风险。近年来，一些机构违规滥用数据、扰乱市场秩序、侵犯消费者权益，引发一些突出的问题。

一是数据垄断。有的企业凭借电商、社交媒体、游戏等领域积累大量用户群体和渠道优势，把持流量入口，通过一些霸王条款过度采集数据，成为数据寡头、搞赢者通吃。

二是不正当竞争。有的企业有了数据等于有了筹码，就会出现妨碍公平竞争、攫取超额利益等现象。一些金融机构在数据合作中失去话语权，不正当竞争就此形成。

三是数据“绑架”。有的企业没有得到用户授权就肆意开展用户画像，然后进行“大数据杀熟”、过度营销和诱导消费。通过用户画像进行定制推送，侵犯金融消费者的知情权、选择权和隐私权。

当前滥用数据、扰乱市场秩序问题已经非常严重。对此，金融管理部门将研究出台金融业数据应用规划和能力建设的指引，明确数据架构、分级分类、共享应用、隐私保护等相关的标准和管理措施。

第二，推动数据要素规范高效有序流通。资金流通会产生价值，数据流动同样也能产生价值。数据要动起来、用起来且用得多价值才越大。当前在数据利用层面，存在一些难点。

一是数据难以确权。金融机构、电商和互联网公司开展业务活动时收集了大量的数据，包括授权的数据、非授权的数据、行为痕迹数据、关联衍生数据等等。但因为法律制度的缺失，数据确权缺乏法规依据，数据权属难以界定。

二是权属不易分离。数据可复制、易留存，所有权、控制权因为共享使用而发生让渡，

给数据所有方对外共享数据带来顾虑。以前说起数据共享都是“你把数据给我”，很少有人说“我把数据给你”。因为没有法律约定，数据用了多少次不知道，给谁用了也不知道。如何做好权属分离、在不让渡数据所有权前提下实现数据有序流转和融合应用是一个难题。

三是数据的价值难以计量。数据要素有别于传统生产要素，它在形态上具有非实物、高度虚拟化的特点，这增加了数据使用计量的难度。数据的维度多元、内涵不同、结构复杂，它的价值难以单纯体量来进行计量。因此，数据的计量和定价是很大的问题。

解决这些问题，需要在法律、技术和市场等多个层面推动数据要素规范高效有序的流通。

在法律层面，建议有关部门加快完善法律法规，推进数据要素权属立法保护，明确权属判定的准则、主体的范围和权利义务。个人信息保护和数据安全等相关立法已经在规划。

在技术层面，借助多方安全计算、可信区块链、标记化等技术，确保数据可用不可见、可用可计量，做到最小够用、专事专用，消除数据所有方因为所有权让渡而导致事权转移的顾虑，保障各方权益。

在市场层面，要推动大数据交易市场规范发展，加快征信体系建设，发挥市场机制资源配置作用，促进数据有效流转和高效配置。

第三，强化金融消费者的隐私保护。建议从制度层面出台法律法规，加强金融管理部门与司法、工信、公安等多个部门协同，建立隐私保护联防联控机制，明晰数据应用伦理边界，杜绝随意打开“潘多拉魔盒”的违规行为。此外，还要做好个人金融信息的全生命周期保护自律工作。

第四，着力做好金融数据标准化工作。标准是发挥数据生产要素价值、推动高效融合应用的前提和基础。当前，数据采集标准不一、统计口径各异、机构数量众多。如果没有标准，工作难以开展且成本很高，有了标准不落地实施也于事无补。所以在数据治理上，希望大家做好标准化这件大事，加大金融标准规则供给与实施力度，统一元数据和机构编码、规范数据接口，打造金融数据交换的“通用语言”，提升金融数据工作质量。（作者：中国人民银行科技司司长　李伟）

➢ 关键信息基础设施安全保护技术体系

当前,网络空间与物理空间、社会空间日渐融合,传统安全威胁与新型网络安全威胁相互交织,网络空间安全风险日益突出。网络入侵和攻击行为呈现明显的规模化、精准化、高维化

趋势,传统的安全技术和产品越来越难以满足需求。近年来,全球各地频发严重的网络安全事件,例如,全球最大的网络社交网站 Facebook 明文存储的 6 亿用户密码被泄露;委内瑞拉国家电网干线遭攻击,造成全国大面积停电;南非电力公司遭受勒索病毒攻击,电力系统程序、数据库等被黑客恶意加密导致系统服务瘫痪;黑客组织攻击澳大利亚议会和英国议会,获得大量议员个人数据;我国也发生了如华住集团、万豪酒店数据泄露等影响数亿用户的重大安全事件。其他类似的勒索病毒、工控系统攻击、大规模数据泄露等安全事件层出不穷。

随着大数据、物联网、人工智能、工业控制系统、卫星通信等新型信息应用的发展和普及,能源、交通、通信、金融、医疗等领域与新技术新应用深度融合,越来越多的国家在战略层面向网络空间倾斜。围绕网络空间的技术对抗、压制和博弈也不断加剧,控制网络空间的信息权和话语权成为新的国家战略制高点。国际网络空间安全形势异常严峻,APT 攻击、勒索病毒、分布式拒绝服务攻击等各种网络安全事件造成了巨大危害和损失。关键信息基础设施和智能设备已逐渐成为网络攻击的焦点。

为此,党中央高度重视关键信息基础设施安全保护工作。习近平总书记指出:“要树立正确的网络安全观,加快构建关键信息基础设施安全保障体系,全天候全方位感知网络安全态势,增强网络安全防御能力和威慑能力。”《中华人民共和国网络安全法》规定:国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域,以及其他一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益的关键信息基础设施,在网络安全等级保护制度的基础上,实行重点保护。国家采取措施,监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁,保护关键信息基础设施免受攻击、侵入、干扰和破坏,依法惩治网络违法犯罪活动,维护网络空间安全和秩序。

本文研究如何建立关键信息基础设施安全保护技术体系,落实国家网络安全等级保护和关键信息基础设施保护要求。本文第 1 章介绍国内外技术现状,第 2 章提出建设关键信息基础设施安全保护技术体系的指导思想,第 3 章描述总体技术架构,对数据采集汇聚、数据治理和智慧大脑等关键技术进行详细阐述,最后对全文进行总结展望。

1、网络安全技术现状

1.1 传统网络环境安全防护技术

密码技术是网络安全领域的基础技术,从最初仅能提供机密性保护,逐渐发展到保障完整性、真实性和不可否认性等安全属性。分组密码、公钥密码、摘要密码等算法和系统的出现和发展,为网络安全奠定了基础。公钥基础设施(PKI)是典型的密码应用技术,用于身份认证、鉴别、授权等一系列网络安全技术。近年来,随着 PKI 系统的深入应用,围绕各种应用场景出现了新的研究成果,包括 SSL/TLS 协议安全性研究、电子护照、密钥托管、密钥分发等各个方面。

边界防护技术是目前网络安全领域应用最为广泛的一类技术方法。防火墙、安全网关、网闸等均在网络边界采集流量数据,通过流量还原和规则分析达到网络隔离、安全接入、数据交换的目的。其他如安全审计、入侵防范、恶意代码防范、数据备份恢复等均属于典型的网络安全技术,作为国家网络安全等级保护制度所规定的安全控制措施,在网络与信息系统的安全防护工作中得到了很好的应用。

1.2 新型网络环境安全保护技术

当前,涉及国计民生的基础信息网络、工业控制系统、云计算平台、移动互联网、物联网、大数据平台等关键信息基础设施,以及正在步入千家万户的智能家居、智能汽车等,逐渐成为网络攻击的重要目标。关键信息基础设施和智能设备由于缺乏有效的安全防护措施,而加剧了网络安全风险。此类设备通常具有高带宽、高性能等特点,同时缺少足够的安全审计和责任追溯机制。攻击者隐藏真实身份,利用云平台、物联网设备作为跳板机或控制端发起网络攻击。

为此,国内外研究人员针对新型网络环境的特点,提出了一系列具有针对性的安全保护技术方法。

1）漏洞分析技术。针对工控系统、物联网设备、移动互联设备等新型网络环境的漏洞分析技术,通过研究新型网络环境的网络架构、协议特性、设备操作系统和运维管理模式,采用协议还原、源码扫描、反编译、逆向工程、动态沙箱等技术,分析挖掘可能存在的特殊漏洞,并研究针对性的漏洞修复或隔离措施。

2）威胁情报。为了促进各类新型设备、系统和协议的安全信息分享,研究人员提出了威胁情报的概念。目前工业界和学术界对威胁情报并没有形成统一的定义,常被引用的是 Gartner 公司给出的定义。威胁情报在网络技术厂商、软件厂商、安全厂商之间实现了安全信息的快速分享,如工控设备特有的漏洞信息、木马病毒信息,以及攻击者所使用的恶意攻击 IP 地址、恶意域名等信息,从而形成良好的安全共创模式,对于云平台、物联网、移动互联网等新型网络环境的安全保护起到了重要作用。

3）态势感知技术。新型网络环境通常面临着来自境内外组织化、规模化的高级持续性威胁（APT）,相关漏洞及其加固信息的发布周期越来越短,需要在第一时间迅速发现其攻击趋势并采取措施进行阻断或隔离。因此,研究人员引入军事领域的态势感知理念,通过对网络空间的安全要素进行实时监测,感知网络的脆弱性和威胁、安全状态及发展趋势,提供安全决策支持[8]。

随着新型网络技术和应用模式的不断发展,包括上述技术在内的各类安全保护技术也在不断革新。针对云计算、移动互联网、物联网、工业控制系统,国家网络安全等级保护制度分别提出了安全扩展要求,充分体现对各类新型网络环境保护的能力要求。

1.3 基于人工智能的网络安全新技术

人工智能是研究、开发用于模拟、延伸和扩展人类智能的理论、方法、技术及应用系统的技术科学。人工智能技术诞生较早,但自从谷歌公司研制的 AlphaGo 首次战胜人类围棋世界冠军后,人工智能才受到了社会公众的广泛关注,AlphaGo 所使用的深度学习算法也逐渐为人们所熟知。近年来,人工智能技术逐渐应用到各个领域,包括智能制造、电子商务、交通、教育、医疗等。

人工智能技术具有自学习和知识迭代更新的能力,在不具备先验知识的前提下,能够从数据样本中发现不为人们所了解的隐含关系和规则,突破了传统机器学习技术对于人工专家经验的依赖,逐渐成为解决大数据环境下智能分析、推理、判别和决策问题的有效手段。

在 2000 年前后,国内外研究人员就提出将机器学习算法应用到入侵检测中,包括数据挖掘算法、人工免疫算法等。但由于受限于算法能力和样本数据量,相关方法基本停留在理论研究阶段。近年来,随着人工智能算法的更新换代,以及网络安全大数据汇聚能力的不断提升,基于人工智能的网络安全技术迎来了广阔的发展空间。GRAF 等人引入深度学习算法,分析网络安全威胁情报中的语义信息,实现网络安全事件自动分类。NOOR 等人应用深度学习技术,在网络安全技术报告中实现语义搜索,提取高级威胁指标。卷积神经网络（CNN）、循环神经网络（RNN）、长短时记忆网络（LSTM）等神经网络算法,由于具备强大的自学习能力,逐渐应

用到网络安全入侵检测和行为判别中。

随着网络信息技术在社会经济各个领域的深度融合,人们的网络安全意识不断提升,各类关键信息基础设施和重要信息系统也逐步建立起网络安全管理中心,对各类网络安全数据进行综合处理,实现安全管理决策。网络安全管理中心需要对各类流量数据、日志数据、报警数据进行快速分析和判断。由于网络带宽、网络规模和用户数量的快速提升,传统的统计分析和人工研判已经无法满足需求,迫切需要引入自动化、智能化的分析方法,对大规模网络环境中的安全数据进行快速学习、迭代和智能推理。

同时,在大量的网络安全分析工作中,需要开展数据拼接、补全、攻击链还原和攻击场景重构,以实现攻击行为溯源。由于人工智能技术能够从大量看似无序的数据中挖掘出隐含的关联,因此,引入人工智能技术开展网络安全大数据分析已经成为业界的普遍共识,能够为安全事件的监测发现、行为判别、安全预警、态势感知、攻击趋势预测等提供准确、及时的参考依据。

2、网络安全技术保护能力要求

为有效保障国家关键信息基础设施安全,需要建立关键信息基础设施安全保护技术体系,贯彻“实战化、体系化、常态化”的新理念,采取“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的新举措,形成网络安全数据接入汇聚、大数据治理和威胁数据分析等功能,实现对重要行业网络安全数据的汇聚分析,对关键信息基础设施的态势感知和信息通报,对网络安全事件的联动分析和追踪溯源,实现针对网络违法犯罪活动的“打防管控”一体化综合支撑能力,有效提升国家关键信息基础设施的安全保障水平。

2.1 立体化监测发现能力

建立针对关键信息基础设施安全保护的协同联动机制,基于主动探测、引接、报送、代理、对接、汇聚的多来源、多方向、多品类、结构各异的网络安全多源异构数据,形成跨行业、跨部门、跨地区的立体化网络安全监测体系,监测发现网络攻击、安全威胁和网络违法活动,支撑网络安全事件通报处置,打击网络违法犯罪活动。

2.2 智能化分析挖掘能力

引入大数据和人工智能技术,构建关键信息基础设施安全保护智慧大脑,形成机器学习与专家研判的交互启发和交叉验证环境,突破隐含知识发掘、深度关联信息发掘、威胁情报智能推理等关键技术,形成针对网络安全大数据的智能分析、挖掘、决策支持能力,感知未知网络风险,预警重大安全威胁。

2.3 可视化综合防控能力

绘制网络空间地图,打通网络空间、物理空间和社会空间的屏障,实现网络空间要素可视化表达、网络空间关系可视化描述和网络安全事件可视化分析,支撑网络安全挂图作战,形成条块结合、纵横联通、协同联动的综合防控格局,落实常态化、实战化措施,提升网络安全突发事件的应对处置能力和重大风险的防控能力。

3、安全保护技术架构

基于前文给出的指导思想,本章提出面向关键信息基础设施的安全保护技术体系,阐述关键技术的核心内容。如图 1 所示,技术体系总体分为 4 层架构：采集汇聚层、数据治理层、智慧大脑层和业务应用层。标准规范和安全保障贯穿技术体系的各个层次。同时,技术体系与外部的各级资源进行联动交互,为关键信息基础设施的安全保护工作提供数据协同、能力协同和业务协同的支撑。

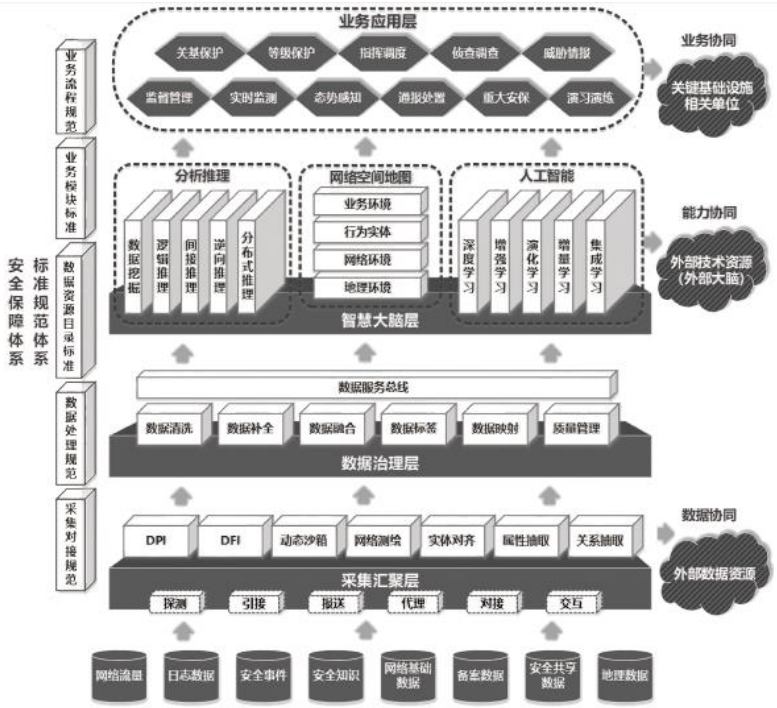


图 1 关键信息基础设施安全保护技术体系架构

3.1 采集汇聚层

关键信息基础设施涉及的安全数据来自网络空间、物理空间、社会空间多个领域,如关键信息基础设施的备案数据、网络流量、日志数据、安全事件、安全知识、网络基础数据、安全共享数据、地理空间数据等。数据来源方式多种多样,包括主动探测、引接、报送、数据代理、平台对接等,并支持交互式查询。采集汇聚层也包括与外部数据资源（如第三方威胁情报库）之间的数据协同。

针对上述网络安全多源异构数据存在的结构复杂、更新频繁、语义不明、内容散落、关

键数据项缺失等问题,需要研究利用高效精准和可扩展的知识抽取方法,围绕上层数据治理和智能分析需求,从网络空间的实体、属性、关系入手,提取网络空间安全数据要素。采集汇聚层综合运用各类数据提取方法,包括：

1）深度包检测技术（DPI）。DPI 是一种典型的网络安全技术,对网络中传输的数据包进行检查,识别应用层协议,恢复连接记录,检查是否包含攻击或异常行为。DPI 技术的特点是可以识别完整的协议交互过程,除了协议头部数据外,还会检查应用载荷内容。DPI 技术通常采用旁路部署,满足高效率和高准确性的检测要求。

2）深度流检测技术（DFI）。DFI 采用基于流量行为的应用识别技术,即不同的应用类型体现在会话连接或数据流上的状态各有不同。数据流状态包括流时长分布、报文到达间隔分布、报文长度分布等。对于加密协议流量而言,由于应用流的状态行为特征不会因加密而根本改变,因此 DFI 技术有助于发现加密流量中的威胁行为。DPI 和 DFI 技术都能够产生关键基础设施安全保护所需的事件告警数据。

3）动态沙箱技术。沙箱是一种按照安全策略限制程序行为的执行环境,用以测试不受信任的文件或应用程序行为的技术。经典的沙箱系统一般是通过构造虚拟运行环境,拦截系统调用和资源访问（如修改注册表、访问磁盘等）,从而监视分析程序行为。沙箱技术已广泛应用于包括 APT 攻击在内的软件样本动态分析技术,能够为关键基础设施安全保护提供木马、病毒等恶意样本的行为分析结果。

4）网络测绘技术。网络测绘是探测互联网空间的节点分布情况和网络关系索引,也包括探测网络节点的类型、版本、配置以及漏洞等安全信息,构建全面、精准的网络空间图谱,以支撑与威胁信息的关联分析等工作目标。网络测绘能够提供关键基础设施安全保护相关的网络资产图谱,掌握网络节点信息和关联关系。

5）实体对齐技术。实体对齐技术也称作实体匹配,是指对于异构数据源中的各个实体,利用属性和关系信息,判定其是否属于现实世界中的同一实体。实体对齐在网络安全保护中尤为重要,可以实现网络空间实体（虚拟身份）和物理空间实体（真实身份）的映射,支撑关键基础设施安全保卫中的固证溯源、攻击者画像、安全预警等业务。

6）属性抽取技术。属性抽取的目标是从异构数据源中采集相同实体的属性信息,从而完成对实体属性的完整刻画。属性抽取本质上也是一种关系抽取。网络安全的属性抽取能够全面反映攻击者、保护目标、网络资源的全要素信息,支撑重点目标画像、关联碰撞、扩线分析等工作。

7）关系抽取技术。关系抽取技术用于发现网络安全实体间的关联关系,形成网状的知识

结构。实体间的关系多种多样,例如攻击者之间的协作关系、地下黑产之间的上下游关系、病毒工具之间的同源关系、服务器与应用程序之间的承载关系等。关系抽取技术从多源异构数据源中抽取上述实体间的相互关系,针对关键基础设施安全保护,支撑情报分析挖掘、事件处置和违法活动打击。

3.2 数据治理层

数据治理层负责针对采集汇聚层提取的网络安全多源异构数据,根据数据资源目录标准进行治理,形成标准范式下的关键信息基础设施安全保护数据资源,具体包括数据清洗、数据补全、数据融合、数据标签、数据映射和数据质量管理。

1）数据资源目录（Data Resources Directory）。数据资源目录是对数据存储对象的描述,让数据分析处理系统或分析人员能够方便、快速地找到所需要的数据。建立网络安全数据资源目录,是开展网络安全大数据治理的依据,也是实现关键信息基础设施安全保护的基础。基于数据资源目录,各类多源异构数据能够对网络安全工作涉及的各类实体、属性及其关系进行统一维度、统一语境下的描述、分析和处理。

2）数据清洗。数据清洗是对多源异构数据进行检查和校验的过程,目的在于归并重复数据,规范数据格式,纠正数据错误,并保证数据一致性。例如,安全设备产生的大量攻击告警需要进行归并去重,以提高分析效率;通过网络测绘或报送获取的网站后门和漏洞隐患,需要进行后门及隐患的有效性验证,仅保留真实存在的此类数据,以免对后端数据分析造成误导。

3）数据补全。数据补全针对不同渠道和来源获取的数据,根据其关联的实体进行数据补全,以完善数据内容。以网络空间数据为主,适当融合物理空间和社会空间数据进行多维补全,从组织、人员、设备、事件、行为、资源、时间、空间等维度支撑构建知识图谱。

4）数据融合。数据融合针对已抽取的网络空间安全要素（包括实体、属性和关系）,通过本体映射、实体消歧、共指消解等操作进行知识融合,形成知识图谱。例如,对于典型的后门攻击,由于多方渠道汇聚的安全数据对其表述存在差异,需要采用共指消解技术,对各类安全数据中使用“远控攻击”“后门植入”“网站后门”“Webshell”等术语描述的事件进行融合,以判断其是否归属于同一类实体,从而形成实体共指链（Coreference Chain）,以利于从各类数据中提取实体的关键信息,从而实现安全数据融合。

5）数据映射。数据映射主要用于反映在关键信息基础设施安全保护中各类实体在网络空间、地理空间和社会空间要素之间的相互映射关系,实现实体在多维空间中的定位,支持多场景多源异构的知识映射。例如,通过跨空间数据映射,对黑客组织发动网络攻击所使用的网络资源进行地理空间映射,定位网络资源的地理位置,从而为公安机关打击网络违法活动提供

支撑。

6）数据标签。标签是一种用来描述实体特征的数据形式。通过标签对实体进行刻画,从多角度反映实体的特征。标签之间相互独立又彼此关联,通过对不同标签的简单操作,便可进行网络安全数据的筛选和分析。关键信息基础设施安全保护的数据标签分为技术标签（如缓冲区溢出、struts2 漏洞等技术手段）、场景标签（如地区、行业、单位、系统等场景维度）、业务标签（如侦查调查、通报处置、演习演练等业务应用）和组合标签。

7）数据质量管理。数据质量管理是指对数据生命周期的各阶段可能出现的各类数据质量问题,进行监测、评估、度量、反馈等一系列管理活动,以促使数据质量持续提高。关键信息基础设施安全保护数据重点关注 5 个方面的质量问题：一是数据完整性,即数据对于重点要素内容的涵盖完整程度;二是数据一致性,即数据对于不同时间、空间或其他维度方面描述结果的一致程度;三是数据准确性,即数据对于对应实体、属性或关系在语义描述方面的准确程度;四是数据关联性,即数据与其他来源或渠道数据之间的可关联程度;五是数据规范性,即数据与资源目录中统一规范的吻合程度。

数据质量的优劣,直接决定了后端开展关键信息基础设施安全保护的准确性、有效性和效率。通过上述环节的数据治理,形成统一规范下的高质量安全数据,经由数据服务总线,向上层提供数据服务,支撑安全保护业务驱动下的数据分析。

3.3 智慧大脑层

智慧大脑是关键信息基础设施安全保护的核心中枢,负责对通过大数据治理形成的统一规范性数据进行智能化的分析、挖掘和推理,建立支撑各类安全保护业务的知识图谱和分析结果。智慧大脑层支持与外部技术资源（外部大脑）的能力协同,例如重点地区、重要行业、重点机构、技术支持单位的网络安全大数据平台、安全分析中心等,充分利用各级网络安全机构的技术资源能力。

3.3.1 人工智能

以关键信息基础设施的安全保护实战为业务驱动,引入深度学习、增强学习、演化学习、增量学习和集成学习,实现对网络安全行为的多轮次动态评估和演绎分析,充分适应网络实战中普遍存在的全局知识不完备、攻防态势快速演变、情报关键要素缺失、攻击方逆向反制、最优策略决策等难题,增强安全保护工作的前瞻性和预判性,掌握网络空间的主动权。

1）深度学习。深度学习是机器学习的一种,通过组合低层特征形成更加抽象的高层表示属性类别或特征。典型的深度学习模型有卷积神经网络、深度置信网络和堆栈自编码网络模型等。作为深度学习的最新发展领域,图神经网络技术近年来引起了广泛重视。图神经网络

具有强大的表征能力,在挖掘图的未知关系方面具有较强的表现力,尤其适用于对非结构化数据的推理工作,更为接近于人脑的推理过程。针对关键信息基础设施安全保护工作,利用图神经网络的深度学习能力,在一定程度上发掘出未知的潜在关系,例如 APT 攻击活动与区域政治关系的关联性,或是关键基础设施安全隐患与 IT 行业供应链之间的隐含关系。针对此类潜在关系训练形成网络空间目标实体、属性及关系的提取模型,为我们揭示网络空间攻防的深层次内涵,有助于支撑全局性和前瞻性的安全决策。

2）增强学习。增强学习是人工智能组件以“试错”的方式进行学习,通过与环境进行交互获得的奖赏指导行为来获取知识。增强学习不同于传统的有监督学习或无监督学习,尤其适用于复杂的网络安全场景,如大范围、大规模、多维度的网络对抗。在关键信息基础设施的网络对抗场景中,各方存在复杂的攻击、防护、协作、对抗、利用和反制关系,此类场景中即便是专业的技术人员也无法清晰掌握场景全貌,通过增强学习能够充分利用人工智能组件的自我优化能力,构建出在一定程度上超越个体人脑判断能力的智慧组件,从而在关键信息基础设施的网络攻防场景中掌握主动权。

3）演化学习。演化学习是基于演化算法提供的优化工具来设计机器学习的算法。演化学习是实现机器学习自我调优的技术手段。由于机器学习任务中存在大量有待解决的复杂优化问题,这就使得机器学习与演化算法的结合（即演化学习）有了自然的动机和天然的条件。例如,上述深度学习和增强学习的过程中,可能会出现大量的推理分支,需要利用演化学习来选择在实际攻防场景下的最优分支。演化学习已成功运用于数据挖掘和人工智能等诸多领域,实现参数选择和算法优化。

4）增量学习。增量学习是机器学习应用在大数据场景中必须采用的机制。增量学习对于关键信息基础设施的安全保护尤为重要。大量的安全事件告警、日志和威胁情报数据实时地汇聚到安全保护平台,在数据总量达到 PB 级甚至 EB 级的情况下,增量学习能够保证数据在海量实时更新的前提下,无需对全数据集进行重复学习,即可实现知识的动态进化和实时更新。

5）集成学习。集成学习通过构建并结合多个机器学习组件来完成学习任务,通过将多个机器学习组件进行结合,获得比单一组件更加显著的泛化性能。由于不同的机器学习组件（如深度学习、增强学习等）受训练数据和表征模型的限制而不可避免地存在局限性,通过集成学习的方式可以进行二次学习,有助于在各类网络安全实战场景下实现最优结果的选择。

利用上述人工智能方法,针对关键信息基础设施中的网络安全实体、属性及其关系数据进行建模、分析、预测,实现实体分析、关系分析、属性分析、行为分析和态势分析,采用多种人工智能方法,进行多轮迭代学习和最优选择,支撑安全保护业务驱动的分析推理。

3.3.2 分析推理

分析推理既包括传统的基于数理统计的数据挖掘和逻辑推理方法,也包括基于人工智能的间接推理和复杂推理方法。

1）数据挖掘：采用分类、回归、聚类、关联分析等数据挖掘方法,挖掘多来源、多形态的网络空间安全数据,实现网络安全行为和态势的高精度机器拟合,保证面向关键信息基础设施安全态势的感知能力、拟合能力和推演能力。

2）逻辑推理：包括时间推理、空间推理、案例推理和本体推理等,其推理得到的知识置信度高,对于网络空间行为能够做到精确定位、快速发现,但缺点是推理规则不易生成,对未知威胁行为无能为力。

3）间接推理：利用网络空间中身份、行为、工具、资产、部位、场所、IP、域名等实体内部或相互之间的结构联系进行间接推理,能够发现网络空间目标之间的隐含关联关系。间接推理对于关键信息基础设施的安全保护具有重要作用。由于网络安全原始监测数据存在数据链缺失,无法覆盖完整的行为过程,通过间接推理技术对缺失环节进行重现,以恢复完整行为过程,这对于网络安全事件的研判、分析和处置等工作具有重要意义。

4）逆向推理：类比于人类大脑对知识的存储和读写,利用共享记忆组件或外部存储矩阵来存储推理所需结果或必要信息。通过读写操作来模拟人脑对新知识的获取和旧知识的遗忘过程,能够适应动态变化的网络空间结构和目标图谱,便于推理过程获取隐含信息,实现针对重大网络威胁的预警预判。

5）分布式推理：针对低维向量表示的图谱,将推理预测转化为基于表示模型的向量操作,以提高推理的计算效率。分布式推理适用于针对网络安全案件进行快速应对处理的应用场景,但需要解决图谱事实元组约束和组合语义信息引起的级联误差问题,避免推理结果的局限性。

针对关键信息基础设施安全保护,为了兼顾推理的效率和准确性,需要在更深层次上融合多种推理方法,利用逻辑推理的高准确率、分布式推理的强计算能力和智能推理的强学习能力和泛化能力,实现优势互补,挖掘提取网络安全实体的逻辑关系及转移概率,掌控重点目标的行为模式、关联关系和演化规律,实现态势推演、行为预测和意图分析,理解网络空间安全动向,构建网络空间对抗态势图景,支撑安全保护实战业务。

3.3.3 网络空间地图

网络空间地图是实现网络空间可视化表达和分析推理的基础。在“人-地-网”纽带关系的理论指导下,网络空间要素已拓展到地理空间和社会空间。针对关键信息基础设施安全保护工作,网络空间地图的要素划分为以下 4 个层次。

1）地理环境层：各类网络空间要素依附的地理载体,强调网络空间要素的地理属性。地理环境层包括网络空间实体的行政区划、道路、设施等基础地理信息,交通管理设施、治安管理设施等公共安全地理信息,图像、音视频、建筑物三维模型等信息,主要涉及关键信息基础设施及相关实体的距离、尺度、区域、物理边界、空间映射等概念。

2）网络环境层：各类网络空间要素形成的节点和链路,即网络逻辑拓扑关系。网络环境层包括楼层、机房、机柜等物理环境,网络拓扑、网络接入等逻辑环境,电商平台、网络论坛等网络环境,以及 IP 地址、域名、网络服务等网络资源。

3）行为主体层：各类网络实体角色的真实身份和网络身份。行为主体层包括关键信息基础设施所属的行业、运营使用单位、人员组织角色以及人员组织对应的邮箱、社交账号、联系方式等。行为主体层主要关注网络实体的交互行为及其社会关系。

4）业务环境层：业务部门重点关注的安全保护业务对象。包括等级保护/关基保护业务关注的信息系统、关键信息基础设施、测评机构,通报处置业务所关注的安全事件、涉事单位、处置人员等,重大安保业务关注的重保单位、保护目标、人员组织等。

通过在地理环境层、网络环境层、行为主体层和业务环境层中对实体、属性及其关系进行交叉映射和融合,充分反映出网络安全实体间多层次、多维度、跨空间的关联关系,形成关键信息基础设施网络空间地图。

3.4 业务应用层

面向关键信息基础设施安全保护的业务工作包括等级保护、关基保护、指挥调度、实时监测、态势感知、通报处置、重大安保、侦查调查、威胁情报、演习演练和监督管理。相关业务工作在上述智慧大脑层各类分析功能的支撑下,形成支撑关键信息基础设施安全保护的业务闭环。业务应用层与关键信息基础设施的行业监管机构、运营使用单位实现业务协同,保证及时、有效应对重大网络安全威胁和风险。

4、结束语

本文阐述了面向关键信息基础设施安全保护的指导思想,提出了涵盖采集汇聚层、数据治理层、智慧大脑层、业务应用层和配套标准规范及安全保障的技术体系,为国家网络安全监管部门和重要行业开展关键信息基础设施安全保护工作提供支持。

网络空间安全覆盖面广,技术性强,针对关键信息基础设施的安全保护工作任重而道远,需要依托大数据和人工智能技术,构建网络空间地图,实现智能化、精准化、动态化的目标画像、行为推理、情报挖掘、态势推演和预测预警,支撑面向关键信息基础设施的“实战化、体系化、常态化”安全保护工作。（来源：信息安全网络　作者：郭启全，张海霞）

四、政府之声

➢ 国家网信办修订《互联网用户公众账号信息服务管理规定》发布施行

2021 年 1 月 22 日，国家互联网信息办公室发布新修订的《互联网用户公众账号信息服务管理规定》（以下简称《规定》）。《规定》自 2021 年 2 月 22 日起施行。国家互联网信息办公室有关负责人表示，发布《规定》旨在进一步加强互联网用户公众账号的依法监管，促进公众账号信息服务健康有序发展。

国家互联网信息办公室有关负责人介绍：原《规定》自 2017 年 10 月 8 日施行以来，对依法规范公众账号信息传播秩序发挥了积极作用。随着移动互联网快速发展，公众账号信息服务呈现出专业化、组织化、商业化等诸多特点，原《规定》在施行过程中面临新情况新问题，需要适应形势发展进行修订完善。国家互联网信息办公室依据《中华人民共和国网络安全法》等相关法律法规修订原《规定》。《规定》共 23 条，包括公众账号信息服务平台信息内容和公众账号管理主体责任、公众账号生产运营者信息内容生产和公众账号运营管理主体责任、真实身份信息认证、分级分类管理、行业自律、社会监督及行政管理等条款。

《规定》强调，公众账号信息服务平台和公众账号生产运营者要严格遵守法律法规，积极履行社会责任，自觉遵守公序良俗，坚持正确舆论导向、价值取向，大力弘扬和践行社会主义核心价值观，为用户提供向上向善的优质信息内容，发展积极健康网络文化。《规定》鼓励各级党政机关、企事业单位等组织机构注册运营公众账号，生产发布高质量政务和服务信息，满足公众信息需求，推动经济社会发展。

《规定》要求，公众账号信息服务平台要履行企业主体责任，建立公众账号分级分类管理、生态治理、著作权保护、信用评价等制度，健全公众账号注册认证、资质审核、主体公示、动态核验、运营推广等管理措施，完善网络谣言等违法违规信息预警发现和处置机制，全面加强平台公众账号信息服务行为的基础管理和过程管理，切实维护平台内容安全、账号安全、数据安全和个人信息安全。

《规定》提出，公众账号生产运营者应当履行用户主体责任，建立健全内容和账号安全审核机制，加强内容导向性、真实性、合法性把关，依法依规管理运营账号，以优质信息内容吸引公众关注订阅和互动分享，不得从事恶意注册账号、编造虚假信息、煽动极端情绪、剽窃原创作品、实施网络暴力、进行敲诈勒索、买卖交易账号等违法违规行为，维护账号内容安全和清朗网络空间。国家互联网信息办公室有关负责人强调，公众账号信息服务平台和公众账号生产运营者应当按照《规定》要求，切实履行责任和义务，依照相关法律法规加强自身管理，主动接受社会监督，积极营造清朗的网络空间。（来源：国家互联网信息办公室）

- **《互联网用户公众账号信息服务管理规定》**
- **全文：**http://www.cac.gov.cn/2021-01/22/c_1612887880656609.htm

➢ 中国银保监会印发监管数据安全管理办法（试行）的通知

2021 年 1 月 15 日，中国银保监会关于印发监管数据安全管理办法（试行）的通知。其中，中国银保监会监管数据安全管理办法所称监管数据是指：银保监会在履行监管职责过程中，依法定期采集,经监管信息系统记录、生成和存储的，或经银保监会各业务部门认定的数字、指标、报表、文字等各类信息。

本办法所称监管信息系统是指以满足监管需求为目的开发建设的，具有数据采集、处理、存储等功能的信息系统。同时，开展监管数据活动，必须遵守相关法律和行政法规。任何单位和个人对在监管数据活动中知悉的国家秘密、工作秘密、商业秘密和个人信息，应当依照相关规定予以保密。（来源：中国银行保险监督管理委员会）

- **中国银保监会监管数据安全管理办法（试行）**
- **全文：**http://www.cbirc.gov.cn/cn/view/pages/govermentDetail.html?docId=959801

➢ 最高检印发《人民检察院办理网络犯罪案件规定》

2021 年 1 月 25 日，最高人民检察院召开的“充分发挥检察职能 推进网络空间治理”新闻发布会上发布了《人民检察院办理网络犯罪案件规定》，通报了当前检察机关惩治网络犯罪、促进网络空间依法治理情况。

规定共 7 章 65 条，包括一般规定、引导取证和案件审查、电子数据的审查、出庭支持公诉等内容，以办案流程为脉络，以事实证据审查为主线，对检察机关办理网络犯罪案件提出了规范指引，对办案技术融合、一体协作办案等机制建设提出了具体要求。

近年来，全国检察机关依法严厉打击和有效防范网络犯罪，积极参与网络综合治理。针对电信网络诈骗、网络赌博等严重危害网络安全犯罪持续多发高发的情况，积极参与“断卡”“打击治理跨境赌博”等专项行动，会同有关部门，坚持惩防并举、惩治结合，坚决遏制相关犯罪高发蔓延势头；注重全面履行公益诉讼、民事、行政检察职能，形成对网络空间的全方位司法保护；主动加强与执法司法部门、企业、科研院校的沟通协作，形成治理合力。（来源：人民警察网）

- **《人民检察院办理网络犯罪案件规定》**
- **全文：**https://www.spp.gov.cn/spp/xwfbh/wsfbh/202101/t20210125_507446.shtml

➢ 《涉密信息系统集成资质管理办法》2021 年 3 月 1 日施行

2021 年 1 月 25 日，国家保密局发布 2020 年第 1 号令：《涉密信息系统集成资质管理办法》已经国家保密局 2020 年 11 月 13 日局务会议通过，现予公布，自 2021 年 3 月 1 日起施行。

同时，国家保密局发布的《涉密信息系统集成资质管理办法》（国保发〔2013〕7 号，国保发〔2019〕13 号修订）同时废止。（来源：国家保密局）

- **《涉密信息系统集成资质管理办法》**
- **全文：**http://www.gjbmj.gov.cn/n1/2021/0125/c409089-32010949.html

五、本期重要漏洞实例

➢ Mozilla Firefox 内存破坏漏洞

发布日期：2021-1-21
更新日期：2021-1-21
受影响系统：
Mozilla Firefox <82
Mozilla Firefox ESR <78.4
Mozilla Thunderbird <78.4
描述：

CVE(CAN) ID: CVE-2020-15683
Mozilla Firefox 是一款流行的 WEB 浏览器。Mozilla Firefox 处理 WEB 页内容存在内存破坏漏洞，远程攻击者可利用该漏洞提交特殊的 WEB 请求，诱使用户解析，可使应用程序崩溃或可以应用程序上下文执行任意代码。
建议：

厂商补丁：
Mozilla
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://www.mozilla.org/en-US/security/advisories/mfsa2020-45/

➢ Linux kernel 任意代码执行漏洞

发布日期：2021-1-18
更新日期：2021-1-18
受影响系统：
Linux Linux kernel <=5.10.4
描述：

CVE(CAN) ID: CVE-2020-36158
Linux kernel 是一种计算机操作系统内核，以 C 语言和汇编语言写成，符合 POSIX 标准，按 GNU 通用公共许可证发行。Linux kernel 5.10.4 及更早版本中的 drivers/net/wireless/marvell/mwifiex/join.c 中的 mwifiex_cmd_802_11_ad_hoc_start 存在任意代码执行漏洞。攻击者可通过长 SSID 值利用该漏洞执行任意代码。
建议：

厂商补丁：
Linux

厂商已发布了漏洞修复程序，请及时关注更新：
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=5c455c5ab332773464d02ba17015acdca198f03d

➢ Oracle 发布 2021 年 1 月的安全公告

发布日期：2021-1-19
更新日期：2021-1-19
描述：2021 年 1 月 19 日，Oracle 发布了 2021 年 1 月份的安全更新，修复了其多款产品存在的 329 个安全漏洞。受影响的产品包括：Oracle Database Server 数据库（8 个）、Oracle Communications Applications（8 个）、OracleCommunications（12 个）、Oracle Construction and Engineering（7 个）、电子商务套装软件 OracleE-Business Suite（31 个）、Oracle Enterprise Manager（8 个）、Oracle Financial Services Applications（50 个）、OracleFood and Beverage Applications（2 个）、中间件产品 Fusion Middleware（60 个）、Oracle GraalVM（2 个）、Oracle Health Sciences Applications（5 个）、OracleHyperion（7 个）、Oracle Insurance Applications（3 个）、OracleJava SE（1 个）、Oracle JD Edwards(5 个)、Oracle MySQL 数据库(43 个)、Oracle PeopleSoft(8 个)、Oracle Retail Applications（32 个）、Oracle Siebel CRM（4 个）、Oracle Supply Chain（11 个）、Oracle Systems（4 个）、Oracle Utilities Applications（1 个）和 OracleVirtualization（17 个）。本次安全更新提供了针对 179 个高危漏洞的补丁，有 293 个漏洞可被远程利用。提醒广大 Oracle 用户，请及时下载补丁更新，避免引发漏洞相关的安全事件。

CVE 编号	公告标题和摘要	最高严重等级	受影响的软件
CVE-2021-2047	**Oracle WebLogic Server 产品存在漏洞** 未经身份验证的攻击者通过 IIOP、T3 进行网络访问，从而危害 Oracle WebLogic Server。成功攻击此漏洞可导致接管 Oracle WebLogic Server。	严重	WebLogic Server 10.3.6.0.0 WebLogic Server 12.1.3.0.0 WebLogic Server 12.2.1.3.0 WebLogic Server 12.2.1.4.0 WebLogic Server 14.1.1.0.0
CVE-2021-2075	**Oracle WebLogic Server 产品存在漏洞** 未经身份验证的攻击者通过 IIOP、T3 进行网络访问，从而危害 Oracle WebLogic Server。成功攻击此漏洞可导致接管 Oracle WebLogic Server。	严重	WebLogic Server 10.3.6.0.0 WebLogic Server 12.1.3.0.0 WebLogic Server 12.2.1.3.0 WebLogic Server 12.2.1.4.0 WebLogic Server 14.1.1.0.0
CVE-2021-2064	**Oracle WebLogic Server 产品存在漏洞** 未经身份验证的攻击者通过 IIOP、T3 进行网络访问，从而危害 Oracle WebLogic Server。成功攻击此漏洞可导致接管 Oracle WebLogic Server。	严重	WebLogic Server 12.1.3.0.0
CVE-2021-2108	**Oracle WebLogic Server 产品存在漏洞** 未经身份验证的攻击者通过 IIOP、T3 进行网络访问，从而危害 Oracle WebLogic Server。成功攻击此漏洞可导致接管 Oracle WebLogic Server。	严重	WebLogic Server 12.1.3.0.0

CVE-2020-14756	**Oracle Coherence 产品存在漏洞** 未经身份验证的攻击者通过 IIOP、T3 访问网络，从而危害 Oracle Coherence。成功攻击此漏洞可导致接管 Oracle Coherence。	严重	Oracle Coherence3.7.1.0 Oracle Coherence12.1.3.0.0 Oracle Coherence12.2.1.3.0 Oracle Coherence12.2.1.4.0 Oracle Coherence14.1.1.0.0

来源：
https://www.oracle.com/security-alerts/cpujan2021.html

➢ Cisco Smart Software Manager Satellite 信息泄露漏洞

发布日期：2021-01-20
更新日期：2021-01-25
受影响系统：
Cisco Smart Software Manager Satellite <= 5.1.0
描述：

CVE(CAN) ID: CVE-2021-1219
Cisco Smart Software Manager 是美国思科（Cisco）公司的一个为用于提供许可证智能管理功能的软件。该软件消除了繁琐的产品激活密钥（PAK）和许可证文件管理，使许可证节点不再锁定到设备，可以支持再任何兼容的设备上使用许可证。
Cisco Smart Software Manager Satellite 5.1.0 及之前版本存在信息泄露漏洞。该漏洞源于程序未对静态凭据设置充分保护。经过身份认证的本地攻击者可通过访问本地设备上的静态凭据利用该漏洞访问受影响系统上的敏感信息。
链 接： https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-sc-Jd42D4Tq
建议：

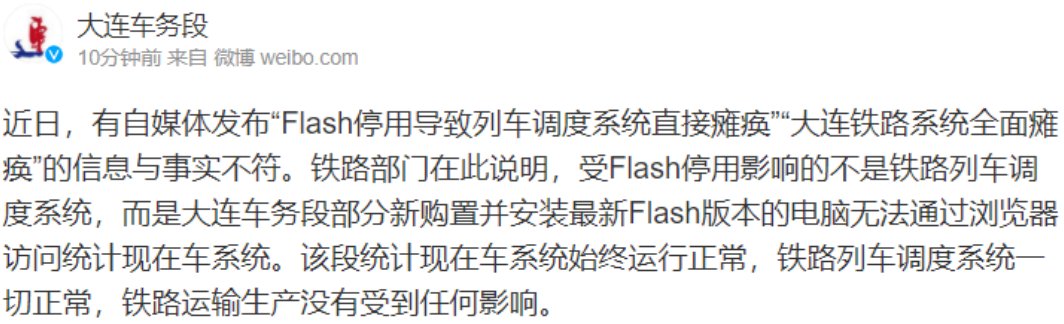
厂商补丁：
Cisco
Cisco 已经为此发布了一个安全公告（cisco-sa-cssm-sc-Jd42D4Tq）以及相应补丁：
cisco-sa-cssm-sc-Jd42D4Tq：Cisco Smart Software Manager Satellite Static Credential Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-sc-Jd42D4Tq

六、本期网络安全事件

➢ 因 Adobe Flash 停用 大连铁路系统瘫痪逾 20 小时

2021 年 1 月 15 日，针对“Flash 停用导致列车调度系统直接瘫痪”事件大连车务端在 15 日在官方微博进行了回应表示，受 Flash 停用影响的不是铁路列车调度系统，而是大连车务段部分新购置并安装最新 Flash 版本的电脑无法通过浏览器访问统计现在车系统。大连车务段表示，铁路列车调度系统一切正常，铁路运输生产没有受到任何影响。

官方原文如下：


大连车务段
10分钟前 来自 微博 weibo.com

近日，有自媒体发布“Flash停用导致列车调度系统直接瘫痪”“大连铁路系统全面瘫痪”的信息与事实不符。铁路部门在此说明，受Flash停用影响的不是铁路列车调度系统，而是大连车务段部分新购置并安装最新Flash版本的电脑无法通过浏览器访问统计现在车系统。该段统计现在车系统始终运行正常，铁路列车调度系统一切正常，铁路运输生产没有受到任何影响。

美国电脑软件公司 Adobe，于去年 12 月 30 日起终止支援 Flash，并于周二（1 月 12 日）起禁止所有 Flash 内容运行。辽宁沈阳铁路局下属大连车务段，近日因未及时停用 Flash，部分车站无法编排调车计划和制定列车编组顺序表，职员亦未能查看列车运行图，导致铁路系统瘫痪逾 20 小时。车务段最终要降低软件版本才能停止混乱情况。

大连车务段官方微信指，职员在上周二（12 日）接报指行车系统页面无法显示，令他们无法查看列车运行图。在 30 分钟后，几乎全段运输生产电脑都出现故障，令铁路运输管理信息系统瘫痪，铁路局与车站之间的讯息共享中断。经调查后，事故原因与 Adobe 公司全面禁止 Flash 运行有关。大连车务段立即採取应急措施，实施降级调试、启动备用设备、硬件更换等，尝试恢复 flash 运作，终在 1 日后重启服务。

惟该车务段在周五（15 日）更正称，故障并未造成铁路系统全面瘫痪，受 Flash 停用影响的不是铁路调度系统，而是部分新购置并安装最新 Flash 版本的电脑，不能通过浏览器访问统计现时的车系统，强调铁路运输生产未受此次故障的任何影响。

另外，大连车务段亦在微信发表彰文，表扬此次紧急"攻关"表现精彩，铁路局更称讚车务段"人人都是高手"，但相关发文遭网民讽刺，指"Flash 停用已不是新闻，早就应该更新铁路系统了"、"最后的办法是降级，又不是连夜开发新软件，有值得宣传的地方吗"。该车务段

受网民抨击后，目前已删除相关文章。（来源：互联网综合整理）

➢ 30 人贩卖 6 亿条个人信息获利 800 余万 通过区块链虚拟货币收付款

2021 年 1 月 25 日，近日，江苏丹阳警方成功侦破一起公安部督办的侵犯公民个人信息案，涉及 10 多个省市，抓获犯罪嫌疑人 30 名。该团伙采用境外聊天工具和区块链虚拟货币收付款，共贩卖个人信息 6 亿余条，违法所得 800 余万元。犯罪嫌疑人已被移送检察机关。

2020 年 5 月，丹阳市公安局网安大队在网上巡查时，发现有一专门利用境外聊天软件（Telegram）贩卖公民个人信息的犯罪团伙，且资金大多通过区块链虚拟货币进行收付款的犯罪线索。该团伙贩卖公民信息数量巨大，且贩卖信息中包含数据种类繁多，涉及姓名、身份证号、联系方式、家庭住址、银行流水等众多信息。由于该案件侵犯对象广，犯罪嫌疑人摒弃传统的网络通信工具和银行卡转账的收付款方式，采用境外聊天工具和区块链虚拟货币，犯罪手段新颖，社会危害严重，该案被公安部挂牌督办。

经查，涉嫌侵犯公民个人信息罪的 30 名犯罪嫌疑人共贩卖公民个人信息 6 亿余条，违法所得 800 余万元。其中同时涉嫌诈骗罪的王某胜、王某超、赵某新还供述，利用架设的虚假“蚂蚁金融”网贷平台和公民个人信息对 200 余名受害人进行诈骗，诈骗金额达 20 余万元。

为了维护社会的稳定，丹阳市公安局立即组织精干警力，成立专案组展开侦查工作。经过深入侦查研判，专案组民警最终锁定了犯罪嫌疑人李某某以及范某某，并顺藤摸瓜掌握了

涉案的 30 余名犯罪嫌疑人。至此，一条源头收集贩卖公民信息、 中介倒卖公民信息、底层购买信息电销、诈骗分子购买信息进行诈骗的全链条犯罪团伙被丹阳警方成功摧毁。（来源：新华社）

➢ WhatsApp 因违反 GDPR 面临最高 5000 万欧元罚款

2021 年 1 月 25 日，根据爱尔兰数据保护监管机构做出的初步判决，WhatsApp 因违反 GDPR 规定将面临最高 5000 万欧元（约合 4400 万英镑）的罚款。

根据爱尔兰数据保护委员会（DPC）的调查结果，WhatsApp 未能正确告知欧盟用户其如何与 Facebook 共享数据，在透明性要求上未达标。该判决于 2020 年 12 月确定，然后发送给欧洲其他数据监管机构进行评估。

Politico 网站表示，WhatsApp 可能会受到迄今为止最大的 GDPR 处罚之一，罚款可能在 3000 万至 5000 万欧元之间，而 WhatsApp 可能需要更改其处理用户数据的方式。针对 WhatsApp 的调查是爱尔兰数据保护委员会当前正在进行的多项调查之一。截至 2020 年 2 月，爱尔兰数据保护委员会正在调查包括 Facebook、Google 和 Tinder 在内的跨国科技公司的 21 种潜在违规行为。

此外，近期在线约会应用 Grindr 因与第三方广告商共享用户个人数据而未征得其充分同意，被挪威数据监管机构处以 1 亿瑞典克朗（约合 860 万英镑）的罚款。经过长时间调查，挪威数据保护局（Datatilsynet）得出结论，Grindr 出于营销目的与第三方共享用户数据，

包括特殊类别的个人数据。（来源：ITPro）

➢ 特斯拉起诉前员工窃取 26000 份机密文件，该员工表示只是无意中犯错

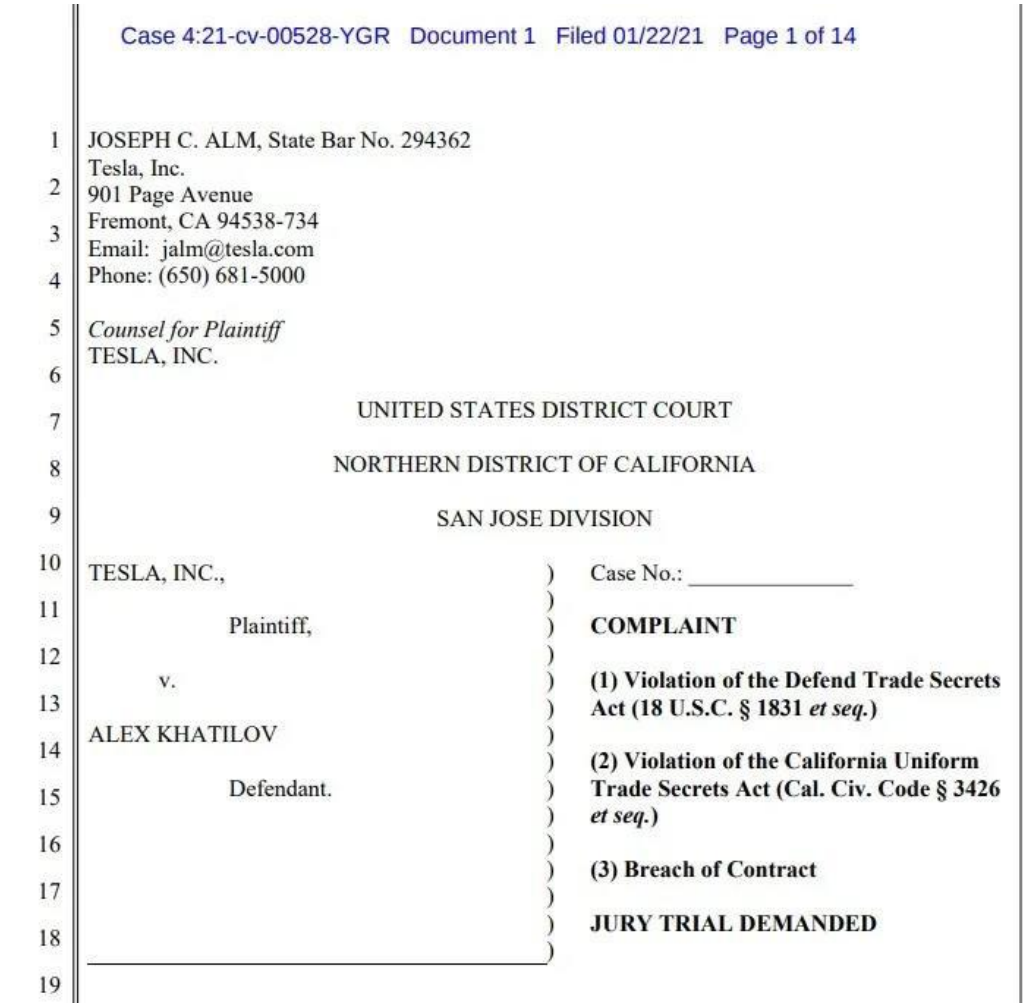
2021 年 1 月 25 日报道，据外媒报道，特斯拉正在起诉一名前员工，指控其窃取公司信息。特斯拉表示，软件工程师亚历克斯哈提洛夫(Alex Khatilov)从特斯拉内部网络中窃取了与 WARP Drive 软件相关的文件，该软件用于自动化公司的许多业务流程。

特斯拉在诉讼文件中写道：“2020 年 12 月 28 日，特斯拉雇佣被告为公司软件自动化工程师。在三天内，被告从特斯拉的安全内部网络中盗取了数千份高度机密的软件文件，并将其转移到他的个人 Dropbox 云存储账户中，特斯拉无法访问或查看。这些文件含有特斯拉花费多年工程时间所开发的专用软件代码“脚本”。这些脚本在执行的时候，可以自动完成特斯拉业务中的各种功能。只有少数特斯拉员工可以访问这些文件，而作为其中一员，被告利用其访问权下载了与其工作无关的文件。”

特斯拉还表示：Khatilov 试图掩盖其行为。报道称，在接受调查人员的盘问时，他谎称自己只是转移了个人文件。另外，当他允许调查人员查看其 Dropbox 储存空间时，又称自己“忘记了”曾转移这些文件。特斯拉表示，在调查开始时，这位工程师甚至还曾试图删除 Dropbox 应用和其他文件。

特斯拉没有透露是否认为 Khatilov 有其他同伙。但是该公司警告说，他们“并未完全发现” Khatilov 的所有行动，他有可能依然在分享特斯拉的文件。受疫情影响，这位员工不得不远程工作，因此很难核实他是否已经删除了这些盗取的文件。

不过，Alex Khatilov 在接受采访时表示：自己是无意中把文件上传到个人 Dropbox 账户的。他表示，当时自己正试图备份自己电脑上的一个文件夹，无意中把这些文件移到了 Dropbox 上。而且在《纽约邮报》联系他之前，他一直不知道特斯拉已经对他提起了诉讼。Khatilov 告诉纽约邮报，直到星期五报纸上刊登了他的名字，他才知道自己被起诉了，而且他也在同一天被解雇。“我真的很震惊竟然会发生这种事情，”他说。“我真的没有撒谎，我说的都是事实。



Case 4:21-cv-00528-YGR Document 1 Filed 01/22/21 Page 1 of 14

JOSEPH C. ALM, State Bar No. 294362
Tesla, Inc.
901 Page Avenue
Fremont, CA 94538-734
Email: jalm@tesla.com
Phone: (650) 681-5000

Counsel for Plaintiff
TESLA, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

TESLA, INC.,

Plaintiff,

v.

ALEX KHATILOV

Defendant.

Case No.: _____

COMPLAINT

(1) Violation of the Defend Trade Secrets Act (18 U.S.C. § 1831 *et seq.*)

(2) Violation of the California Uniform Trade Secrets Act (Cal. Civ. Code § 3426 *et seq.*)

(3) Breach of Contract

JURY TRIAL DEMANDED

这并不是特斯拉第一次因保护公司数据起诉前员工了

一直以来，特斯拉都非常注重保护自己的技术，该公司曾起诉 Rivian 和 Zoox，因为这两家公司涉嫌雇佣了持有特斯拉机密的员工。除此之外，特斯拉还起诉过 Martin Tripp，特斯拉 CEO 埃隆·马斯克(Elon Musk)将其称为“破坏者”。如果 Khatilov 的案件属实，只会加剧特斯拉对商业机密盗窃的担忧，如果人们加入该公司只是为了盗取其自动化工具，那么特斯拉有理由去保护其重要的电动汽车和自动驾驶技术。（来源：互联网综合整理）

➢ 中国农业因重要信息系统突发事件未报告等 6 项原因被罚 420 万元

2021 年 1 月 29 日，银保监会开出 2021 年第一张罚单，中国农业银行因涉及发生重要信息系统突发事件未报告、互联网门户网站泄露敏感信息等六项问题，被罚 420 万人民币。

具体来看，农业银行涉及的违法违规行为包括：

（一）发生重要信息系统突发事件未报告

（二）制卡数据违规明文留存

（三）生产网络、分行无线互联网络保护不当

（四）数据安全管理较粗放，存在数据泄露风险

（五）网络信息系统存在较多漏洞

（六）互联网门户网站泄露敏感信息

中国银行保险监督管理委员会行政处罚信息公开表
（银保监罚决字〔2021〕1号）

（中国农业银行股份有限公司）

行政处罚决定书文号			银保监罚决字〔2021〕1号
被处罚当事人	单位	名称	中国农业银行股份有限公司
		法定代表人姓名	周慕冰
主要违法违规事实（案由）			（一）发生重要信息系统突发事件未报告 （二）制卡数据违规明文留存 （三）生产网络、分行无线互联网络保护不当 （四）数据安全管理较粗放，存在数据泄露风险 （五）网络信息系统存在较多漏洞 （六）互联网门户网站泄露敏感信息
行政处罚依据			《中华人民共和国银行业监督管理法》第二十一条、第四十六条第五项和相关审慎经营规则
行政处罚决定			罚款420万元
作出处罚决定的机关名称			中国银行保险监督管理委员会
作出处罚决定的日期			2021年1月19日

可以看出，农行“六宗罪”主要涉及到两个问题：数据安全与网络安全。

《网络安全法》第三十一条规定，国家对金融等重要行业和领域，在网络安全等级保护制度的基础上，实行重点保护。根据《关键信息基础设施确定指南（试行）》要求，银行运营为金融行业中的关键业务。

因此，银行一般应被认定为关键信息基础设施运营者，在履行网络运营者的一般安全保

护义务的基础上，还需履行关键信息基础设施运营者的特殊义务。

从这个角度出发，银行需承担网络安全义务非常重，而相关的规范规定更是数不胜数，在今年就发布有《个人金融信息保护技术规范》、《网上银行系统信息安全通用规范》、《商业银行应用程序接口安全管理规范》等等多个规范。

除了网络安全，数据安全是银行安全合规的另一个重点，特别是个人金融信息保护。对于金融行业来说，数据对业务的开展情况影响深远，优质的数据内容将极大的提升金融机构的服务能力。数据保护对金融行业来说也具有较强的特殊性，一方面，金融机构基于业务需求，需要收集、利用客户的个人金融信息；另一方面，从金融创新发展的大局出发，金融机构需要把数据作为核心资产管好、用好，促进数据资产的流动和增值。

此外，在数字化转型形势下，当前中国经济发展呈现全要素数字化特征，新经济催生数字化融资模式，新需求驱动多元化金融服务，新技术促进智能化金融创新，这都需要数据的支撑。（来源：安全学习那些事）

➢ 拒不履行信息网络安全管理义务，嫌疑人被依法刑事拘留

2021 年 1 月 22 日报道，2020 年 8 月，浙江省金华市武义县网安大队接上级部门的涉网诈骗线索通报称：外省多起电信诈骗案件中的作案微信号、QQ 号登录的宽带装机地址，均为一个名为玉环谊诚的公司在武义电信所租赁。于是立即启动“一案双查”工作机制，成立专案组进行调查。

掌握了充分证据后，武义网安部门于 2021 年 1 月 5 日收网，扣押该公司主机 70 余台、服务器 10 余台、光猫 120 余套，犯罪嫌疑人王某因涉嫌拒不履行信息网络安全管理义务罪被依法刑事拘留。经查，犯罪嫌疑人王某于 2017 年 10 月成立玉环谊诚服务器租赁有限公司并担任法人，从事租赁服务器业务。该公司经常在一些 QQ 群和购物平台上发布关于动态 IP 出租的信息，联系到业务后，便通过向对方发送某远程操作软件和对应的账号密码提供动态 IP，以此获利。

经调取宽带安装数据后又发现，嫌疑人王某还分别以个人名义和公司名义在浙江省内绍兴、金华、丽水、温州、衢州等地设置了机房，涉及宽带账号 344 个。在抓获王某后，民警即赶赴以上地点将机房内的设备一并扣押。目前，案件还在进一步侦办中。

在侦查过程中发现，王某曾经多次因未履行网络安全管理义务被予以行政处罚。（来源：互联网综合整理）

信息安全意识产品服务

021-33663299