2020 年工业信息安全态势报告

国家工业信息安全发展研究中心

2021 年 2 月

编　委　会　主　任　郝志强

副主任　李　丽

成　员　汪礼俊　郭　娴　张　洪

张　格　于　盟　孙　军

陈雪鸿　李　俊　刘　迎

于志成

编　写　组　张慧敏　杨佳宁　黄海波　黄　丹

陈柯宇　杨立宝　孙立立　鞠　远

朱丽娜　赵凯丽　张晓帆　李　莹

樊佳讯　陈大宇　陈　皓　刚占慧

赵　慧　杨　杰　高羽茜　杨　安

版 权 声 明

目录

2020年，全球工业信息安全呈现**技术应用化发展、事件爆发式增长、政策多维度深化、风险弥漫性扩散**等特征。总体来看，**危机中孕育希望，机遇与挑战并存**。放眼技术趋势，围绕威胁诱捕、数据保护、供应链安全、人工智能等的技术应用从理论走向实践；回顾安全事件，新型冠状病毒全球大流行致使利用疫情实施的网络攻击层出不穷，针对工业领域的勒索攻击频发；跟踪政策进展，主要国家围绕工业控制系统安全、工业数据安全、智能制造安全等领域出台一系列法规标准，推动各项措施走向深耕；追溯风险威胁，低防护联网工业控制系统数量激增，高危漏洞占比居高不下，重点行业面临严峻的安全挑战。展望2021，建议秉持**监测、防护、应急“三位一体”理念**，紧密围绕建设态势感知网络、建立防护应急体系、保护工业数据安全、打造专业技术队伍，推进实施“四个一”安全保障措施，切实维护国家工业信息安全。

一、技术趋势

随着工业互联网、智能制造加速发展，海量工业设备泛在互联，工业信息安全呈现风险威胁扩散化、攻击手段智能化等特点，传统信息安全技术在风险识别、威胁发现、安全防护等方面难以有效发挥作用。在此背景下，围绕工控蜜罐、数据保护、供应链、人工智能的安全技术研发日益受到关注，并正以更高效、更可靠的方式走向实践应用。

（一）工控蜜罐技术走向深度应用

“蜜罐”可伪装成有利用价值的设备、系统，吸引网络黑客对其发动攻击。通过对攻击行为进行捕获，分析攻击路径与方法，推测攻击者意图和动机，预判大规模网络攻击事件。“蜜罐”技术直接扭转了网络攻防不对称的局面，越来越多的研究机构与安全企业将蜜罐技术与工控安全相融合，开展了一系列工控蜜罐技术研究与应用，在安全态势感知与主动防御领域涌现出较多成功应用案例。

1. 纯虚拟蜜罐仿真能力逐步提升

纯虚拟蜜罐因部署简单、管理方便等特点被广泛应用。但由于模拟仿真的工业协议种类繁多、运行场景复杂多变，现有的纯虚拟蜜罐无法完全还原工业控制系统设备的真实运行情况，大多局限于对工业协议的简单模拟，易被网络空间搜索引擎或黑客识别，为此，各研究机构纷纷在加强模拟仿真能力上下功夫。2月，英国科学家首次发布了可检测零日漏洞的纯虚拟蜜罐Honware，仅通过软件仿真即可模拟真实物联网设备的硬件运行环境，并借助黑客攻击发现设备零日漏洞，在纯虚拟蜜罐模拟仿真研究方面取得重大突破。

2. 行业级蜜罐网络应用效果显著

近年来，电力、石油石化、智能装备、钢铁、有色等重点行业已成为网络攻击的“重灾区”，黑客组织通过网络攻击意图获得巨大的经济政治利益。基于行业特征，研究部署行

业级蜜罐网络，对于降低设备受攻击风险、提前预警大规模攻击行为十分有效。6 月，以色列安全公司通过部署多个工控蜜罐构建具备电力行业特点的蜜罐网络，成功发现新型勒索软件对电力系统发起的攻击，并及时发布了应对措施。

3. 借助新技术拓展感知溯源范围

工控蜜罐作为主动防御技术，诱捕搜集的攻击数据具有极高的研究价值，在安全监测与态势感知领域发挥着重要作用。2020 年，国家工业信息安全发展研究中心已在全国范围内完成了工控蜜罐网络的一期部署，可精准分析境内外黑客组织的活动趋势，辅助研判我国工业控制系统面临的攻击威胁。下一步将继续通过数据挖掘、人工智能等新技术，对诱捕数据开展深度关联分析及特征提取，加强攻击溯源、威胁感知、预警预判等能力。

（二）数据安全保护技术备受关注

《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》中将数据与土地、劳动力、资本、技术等并列为生产要素，提出要加强数据资源安全保护。近年来，勒索病毒瞄准了工业领域，工业数据成为黑客窃取、篡改的重点目标。针对工业数据安全防护的技术研究方兴未艾，区块链、可信计算、零信任架构等新兴技术引领了新方向。

1. 可信计算保障“新基建”数据安全

在“新基建”背景下，网络攻击从数字空间延伸到物理

空间，新型基础设施以数据和网络为核心，利用主动免疫的可信计算筑牢安全防线。11 月，中国首届可信计算产业峰会暨第五届中国可信计算产业发展论坛以“主动防御 筑牢网安聚力产业”为主题，聚焦推动可信计算产业发展，保障“新基建”数据安全。充分运用可信计算技术，构建安全计算环境和可靠的安全传输数据机制，保证程序运行可信，数据传输、存储和应用可信。

2. 区块链技术保护数据安全共享

基于区块链的数据共享有助于推进跨地域、跨系统、跨主体的数据共享安全，切实促进数据价值的有序流动。区块链技术将数据打包成区块，盖上时间戳，形成一条可溯源而不可篡改的链。数据在受保护的前提下在链上传递，实现“可用不可见”，使企业间数据共享变得安全可控。2 月，美国空军与区块链数据管理公司 Fluree 签署合作协议，共同致力于在军方内部更安全、快速地跟踪和共享信息，并利用分散的数据库来跟踪信息进入系统的过程及访问权限，使空军更易与美军内部和海外盟国的其他军事部门共享情报。

3. 基于零信任架构开发数据安全技术

零信任架构作为一种新兴安全模式，以信任评估为基础，强调动态信任，为网络信任体系的建设应用提供了新的思路。2 月，美国国家标准与技术研究院（NIST）发布《零信任架构》（第 2 版草案），指出零信任架构是一种网络/

数据安全的端到端方法，关注身份、凭证、访问管理、运营、终端、主机环境和互联的基础设施。美国国防部发现零信任架构有可能成功替代 JRSS（联合区域安全栈），承担起国防部网络中间层安全的重任。5 月，美国防承包商宣布与惠普合作开发用于防范勒索软件攻击和数据泄露威胁的数据安全软件平台（BrickStor SP），通过在源头保护非结构化数据，使数据免于被窃取、恶意加密或非法利用，为联邦政府用户提供完整的零信任数据安全解决方案。

（三）供应链安全成为新技术热点

供应链安全是供应链管理的一个重要组成部分，涵盖产品在开发、交付、验收、使用和维护整个生命周期内的安全，其目标是通过识别、评估和确定风险管理的优先级，降低原材料供应、物流管理、运输配送等各环节的安全风险。近年来，复杂多变的国际形势以及新冠肺炎疫情对我国和全球工业领域供应链安全造成了严重冲击，供应链安全防护需求凸显。

1. 汽车行业供应链安全解决方案不断涌现

随着汽车行业供应链全球化程度不断加深，制造商和供应商面对的安全问题也日益复杂，部分汽车厂商、安全服务商开始关注并着手应对供应链安全问题带来的业务中断风险。3 月，宝马集团启动“PartChain”项目，旨在利用区块链技术和云技术提高原材料和零部件在全球供应链中的透

明度，在防篡改基础上实现数据共享和所有组件的全流程追溯。7 月，专注于汽车行业安全解决方案的以色列网络安全初创公司 Cybellum 获得 1200 万美元融资，资金重点用于车辆组件中的软件漏洞分析，以确保汽车供应链安全，有效防范供应链安全问题给汽车制造商带来的风险。

2. 基于威胁信息共享方案确保供应链安全

为保护供应链安全，一些技术机构和厂商联手构建漏洞信息共享渠道，帮助用户及时获取和处理供应链中的潜在漏洞，以应对可能存在的安全风险。2 月，北美电力可靠性委员会（NERC）宣布与美国电力信息共享和分析中心、网络安全风险信息共享计划工作者合作，共同应对电力等公用事业供应链中的潜在漏洞威胁。9 月，施耐德电气加入美国能源部的“具有恢复力的工业控制系统网络测试”（CyTRICS）项目，旨在通过漏洞测试和组件枚举来确保工业控制系统软件和固件的安全性，重点通过研究成果和测试结果的分享运用，来增强能源行业供应链的恢复力。

（四）人工智能技术助力安全防护

人工智能技术可增强网络安全人员应对威胁的能力，在安全防护领域的应用日益普及。印度市场研究机构 Meticulous Research 报告显示，2020 年到 2027 年，人工智能技术用于网络安全所形成的市场规模预计将以 23.6％的复合年增长率增长，到 2027 年将达到 463 亿美元。美国企业策

略小组（ESG）与信息系统安全协会（ISSA）8 月发布的研究报告显示，70％的组织正在受到网络安全技能短缺的影响，这种严重的人员缺口为人工智能解决方案创造了机遇，人工智能有助于实现安全防护技术的自动化，在提升防护效果的同时减轻安全从业人员的负担。

1. 人工智能增强自动风险识别能力

2020 年，国家工业信息安全漏洞库共收集整理工业信息安全漏洞 2138 个，较去年上升 22.2%，漏洞数量的快速递增与安全人员的短缺激发了以机器代替人工开展自动化风险识别的需求。10 月，阿肯色州大学开发的基于人工智能的 AVIRA 工具可以根据电力公司的运营环境自动执行更有效的风险评估流程。同月，康奈尔大学的研究人员与保险公司 Axa 合作开发基于人工智能的工具，用于对海事数据区块链系统的保险设计和地理信息进行分析，以识别其中的漏洞并采取防护措施。

2. 人工智能促进威胁检测技术发展

传统的网络安全工具仅能抵抗已知的恶意代码，而基于人工智能的工具可通过训练来检测更广泛的网络异常活动，从而提供更全面、更动态性的安全保障。6 月，西门子和 Spark Cognition 宣布合作开发基于人工智能的网络安全系统 DeepArmor Industrial，该系统采用下一代防病毒、威胁检测、应用程序控制和零日攻击防护技术，为能源行业提供安全监

控和保护功能。11 月，美国网络安全公司 Palo Alto Networks 发布报告称 Windows XP 和 Windows Server 2003 源代码泄漏，对大量应用这些操作系统的制造业企业造成严重威胁，提出使用基于人工智能的网络行为监控和流量分析工具进行安全保护，以应对上述情况带来的安全风险，充分体现出人工智能在威胁检测领域的巨大作用和应用前景。

3. 人工智能成为恶意邮件检测有力手段

近年来，邮箱地址泄露事件和通过邮件进行欺诈的案例层出不穷。9 月，卡巴斯基发布《2020 年上半年工业自动化系统的威胁态势报告》，指出电子邮件攻击仍然是工业控制系统面临的主要威胁之一，并提出基于人工智能的恶意邮件检测技术可为解决上述问题提供有力支持。防欺诈和可信身份服务商 Kount 发布的检测工具 Email Insights 运用人工智能技术对其全球信任网络产品中的用户交互信息和欺诈信号进行分析，实时阻止欺诈事件的发生。电子邮件安全解决方案提供商 Abnormal security 在新一轮融资后计划将人工智能团队规模扩大一倍，致力于通过人工智能技术分析人员、关系和业务流程数据，以识别安全威胁、防御电子邮件欺诈等恶意行为。

二、事件分析

2020 年，国家工业信息安全发展研究中心共跟踪公开发布的工业信息安全事件 274 件，其中勒索软件攻击共 92 件，

占比33.6%，涉及20余个国家的多个重点行业。在新冠疫情全球大流行的背景下，攻击者大量使用“COVID-19”等疫情相关内容作为钓鱼诱饵发起网络攻击。物联网设备、智能联网设备因其低成本、低安全等特征，逐步取代IT设备成为攻击者的重要攻击武器。

（一）勒索病毒已成头号安全威胁

自2017年5月WannaCry勒索病毒爆发以来，勒索软件的热度持续飙升。工业领域因其运营成本高、数据价值大、社会影响广，成为攻击者开展勒索攻击的首选目标，索要赎金翻倍增长。近年来出现的多个新型勒索软件将攻击目标精准定位于工业控制系统。

1. 工业领域勒索攻击快速增长

2020年，公开发布的针对工业领域的勒索攻击事件共计33起，较2019年增长超3倍，事件数量远超2017-2019年的累计之和。安全公司Dragos和研究团队X-Force发布的《针对工业控制系统的勒索软件攻击评估报告》显示，过去两年针对工业实体的勒索攻击暴增了500%以上，其中，制造业是发生勒索软件攻击事件最多的行业，攻击数量占比高达36%。

2. 新型勒索软件直指工业控制系统

2020年，勒索软件组织开始致力于研发新型变种软件，并定向针对工业领域实施攻击。与传统勒索软件泄露知识产

权和采取对关键数据的破坏性操作相比，新型勒索软件可终止工业控制系统关键进程，对工业生产造成严重影响和损失。安全公司FireEye发布报告显示，2020年共发现EKANS、DoppelPaymer、LockerGoga、Maze、MegaCortex、Nefilim、CLOP等7个勒索软件家族将数千个工业软件进程列入“黑名单”，涉及西门子、GE等多个品牌工业控制系统。安全公司Dragos发布的《制造业网络威胁展望》报告显示，黑客组织XENOTIME和ELECTRUM可利用针对工业控制系统的恶意软件TRISIS和CRASHOVERRIDE,对制造业企业发起定向勒索攻击。

3. 工业领域勒索软件赎金翻倍增长

获取经济利益一直是勒索团伙发起攻击的主要目的。2020年,越来越多的勒索攻击受害者选择支付赎金以恢复其系统及数据。研究机构CyberEdge Group的报告显示，2018年有39％的勒索攻击受害者支付了赎金，2019年提高到45％，而2020年则达到58％。安全公司BlackFog的研究显示，2019年第四季度，勒索攻击受害者平均支付4.5万美元赎金，而到2020年第二季度，这一数值猛增4倍，达到18万美元。钢铁制造商EVRAZ、葡萄牙跨国能源公司EDP、巴西电力公司Light S.A均被索要超过1000万美元赎金。勒索组织的频频得手进一步助推了勒索赎金的节节攀升。安全公司Group-IB在《2020/2021年度高科技犯罪网络威胁趋势报告》中保守估计，2020年勒索攻击造成的经济损失总计超

过 10 亿美元。

（二）利用新冠疫情攻击活动频多

在新型冠状病毒全球大流行的背景下，攻击者利用新冠疫情实施网络攻击事件层出不穷，医疗、制药等行业成为网络攻击的重点目标。在众多的攻击手法中，钓鱼邮件使用频率最高，多数攻击意在窃取数据。

1. 钓鱼邮件成网络攻击常用手段

受疫情影响，众多企业和机构将业务转至线上，视频会议、远程运维等办公模式为攻击者提供了可乘之机，安全公司 Lookout 研究发现，2020 年针对制药企业发起的移动网络钓鱼攻击较 2019 年增长超过 1 倍。FortiGuard 实验室监测发现，恶意攻击者以“COVID-19”或“冠状病毒大流行”等标题为诱饵，向医疗设备制造商发起钓鱼邮件攻击。阿塞拜疆能源基础设施遭以新型冠状病毒为主题网络钓鱼攻击，工业控制系统、特别是数据采集与监控系统（SCADA）被植入远程木马病毒 PoetRAT。

2. 数据窃取为网络攻击主要目的

随着全球各行业加快数字化转型，数据价值进一步凸显，数据也日益成为攻击者的重点目标。2020 年，攻击者针对疫情防控发起一系列特定目标的数据窃取活动。美国医疗临床试验软件供应商 ERT 的医疗临床源数据被窃取，影响了施贵宝、辉瑞、强生等公司的多个新冠肺炎疫苗研究项目。

美国麦哲伦医疗公司遭网络攻击，大量患者个人信息及信息系统数据被窃取，影响多个医疗计划及多家护理组织、工会、军事和政府机构。攻击者试图入侵英国制药商阿斯利康公司的系统，以窃取该公司正在研制的新冠肺炎疫苗相关数据。

（三）联网设备成为重要攻击武器

疫情改变了人们的日常工作与生活方式，居家办公、远程运维、无人化管理推动着各行业联网设备数量迅猛增长，随着联网设备安全问题的不断暴露，遭受攻击利用的风险也随之增加。

1. 物联网设备漏洞隐患频现

广泛用于制造、能源、交通、医疗等重点行业领域的物联网设备安全漏洞频遭曝光。Fibaro Home Center Lite、Homematic中央控制单元（CCU2）及eLAN-RF-003等智能家居集线器、Thales通信模块、Treck TCP/IP软件库等物联网设备被曝存在严重漏洞，涉及全球汽车、能源、电信、制造业、医疗保健和运输系统中的数百万个物联网设备，利用上述漏洞可劫持设备或访问内部网络，甚至用以发动中间人（MitM）或拒绝服务（DoS）攻击，对生产进程、物资运输、电力供应、医疗服务等造成严重影响。

2. 智能联网设备易被劫持利用

随着云计算、大数据、物联网、人工智能等技术的发展，智能联网设备大幅增加。经验证，攻击者可利用设计缺陷、

弱口令等安全漏洞劫持智能门锁、楼宇门禁、LED 灯控制台、智能监控设备及系统，变更配置参数、篡改控制指令、中断正常运行。美国联邦调查局 FBI 发布警告称，攻击者意图劫持安全性较低的智能联网设备，如具有视频和音频功能的家庭监控设备作为攻击工具，对全球实施分布式拒绝服务（DDoS）攻击。

三、政策动向

2020 年，中、美、欧等各国围绕工业控制系统防护、工业数据安全、智能制造安全等，出台了多项战略、法规与标准，将强化安全保障作为重要内容，有序指导重点行业落实政策要求、加强安全防护。

（一）加强控制系统安全防护

1. 基于最佳实践提供防护指导

美、英等国家高度重视关键基础设施、重点行业的工业控制系统网络安全，出台了多项政策措施。美国发布五年战略《保护工业控制系统：一体化倡议 2019-2023》，从公私合作、整体防御、威胁预知、资金投入四个方面，提出了指导关键基础设施领域、重点行业开展工业控制系统网络安全保护工作的基本原则，强调提升工业控制系统网络防御能力、确保工业控制设备和网络的设计安全、提高工业控制系统网络安全工具和服务的易用性。

美、英联合发布《工业控制系统网络安全最佳实践》，

从风险管理和网络安全治理、物理安全、工业控制系统网络体系结构、工业控制系统网络边界安全、主机安全、安全监测、供应链管理、人为因素等八方面提供了保障工业控制系统网络安全的最佳做法，并将维护工业控制系统资产清单、制定和实施事件响应计划、加强漏洞管理、配置入侵检测系统等措施作为重要内容。

2. 制定指南保护行业基础设施

随着美国能源行业智能电网的大规模推广应用，自动控制系统和大数据等新技术被广泛用于提高电网的运行效率和可靠性，与此同时也为能源行业引入了新的网络安全风险。在此背景下，美国围绕电力基础设施网络安全出台了多项标准规范，以指导能源行业应对安全风险、加强安全防护。美国联邦能源监管委员会（FERC）和北美电力可靠性委员会（NERC）共同发布电力企业网络事件响应报告，围绕网络安全事件准备、检测和分析、遏制和消除及事后活动等应急响应流程，提出电力企业网络事件响应和恢复的最佳做法，包括使用安全基准检测潜在事件、使用决策树或流程图快速评估风险、全面考虑采取响应措施可能产生的影响、依据事件和演习经验持续改进完善应急响应计划等。

NERC与美国NIST对《NERC关键基础设施保护可靠性标准》与《NIST网络安全框架》的对应关系进行了更新，围绕电子安全边界、电力系统网络资产保护、人员培训、安全管

理等方面，指导行业开展网络安全风险识别、风险评估及风险管理，以消减北美大型电力系统面临的网络安全风险。NIST还发布《智能电网互操作性标准的框架和路线图4.0版》（草案），旨在完善智能电网网络安全风险管理方法，进一步明确特定接口的特性及安全要求。

（二）强化工业数据安全保护

1. 明确工业数据作为生产要素的保护要求

党的十八大以来，党中央高度重视大数据发展，在十九大报告、中共中央政治局第二次集体学习、十九届四中全会等中央会议上逐步明确数据的生产要素属性。2020年4月9日，中共中央、国务院正式发布《中共中央、国务院关于构建更加完善的要素市场化配置体制机制的意见》，首次将数据与土地、劳动力、资本、技术等传统要素并列为生产要素，提出要围绕推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护等3方面加快培育数据要素市场。其中，在释放工业数据潜在价值方面提出支持构建工业等领域规范化数据开发利用的场景，在加强数据安全保护方面强调“推动完善适用于大数据环境下的数据分类分级安全保护制度”，为工业数据作为生产要素的安全保护要求提供了政策依据。

为应对日益泛滥的勒索攻击导致的企业关键数据遭破坏、更改和窃取状况，美国NIST发布《数据完整性恢复指

南（SP）1800-11》，围绕安全存储、损坏测试、备份恢复、虚拟架构、日志记录等5方面，指导重点行业企业制定保护数据完整性的策略，帮助企业实现关键数据的安全保护。

2. 工业数据分类分级管理取得阶段性进展

为全面提升我国工业数据管理能力，释放数据潜在价值，保证数据安全，工信部印发《工业数据分类分级指南（试行）》，提出构建我国工业数据分类分级的基本框架，与《数据管理能力成熟度评估模型》互为补充、相互衔接，引导企业通过防护技术应用、管理流程优化、组织体系变革，有效应对工业数据遭篡改、破坏、泄露或非法利用，强化数据安全防护。为切实贯彻指南要求，推动工业数据安全管理走向实践深耕，工信部组织开展了工业数据分类分级应用试点工作，在北京、江苏、江西、广东、四川等5个地区，以及钢铁、烟草、电力等9个行业的150家企业完成试点工作，在引导企业开展工业数据分类分级、指导行业加强宣贯培训、检验指南内容等方面取得了实效。

（三）着力保障智能制造安全

1. 智能制造安全纳入战略法规

随着人工智能等技术的进一步成熟，推进智能制造、加速制造业数字化转型已经成为全球制造业变革的主要方向。中、美等国家纷纷将加大人工智能技术在智能制造领域安全应用的研究力度，强调建立覆盖智能制造全生命周期的网络

安全保障体系。

美国发布《国家人工智能倡议法案》，授权成立国家人工智能研究所，并投入为期 5 年、金额高达 1.4 亿美元的资金，重点支持合成制造、精准农业、机器学习等领域的人工智能技术安全应用研发工作。同时，美国出台第 13960 号行政命令《在联邦政府中推行可信赖人工智能》，强调围绕“安全可靠”的原则，在联邦政府设计、开发、获取和应用人工智能时确保应用安全，有效应对系统漏洞、对抗性攻击和其他恶意利用行为。

发改委、工信部、科技部等 11 个部委联合印发《智能汽车创新发展战略》，明确提出到 2025 年基本形成中国标准智能汽车的网络安全体系的目标，强调围绕完善安全管理联动机制、提升网络安全防护能力和加强数据安全监督管理 3 方面加快构建全面高效的智能汽车网络安全体系，包括建立风险评估、等级测评、监测预警、应急响应等机制，搭建多层纵深防御、软硬件结合的安全防护体系等。

2. 智能制造安全标准取得进展

在智能制造发展战略和政策的引领下，主要国家着力建设与智能制造发展相适应的网络安全标准体系，加快推进人工智能技术应用于制造领域的相关标准研制，明确提出智能制造安全防护基本原则，指导行业落实网络安全防护要求。我国五部委联合印发《国家新一代人工智能标准体系建设指

南》，明确提出“到 2023 年，初步建立人工智能标准体系”的建设目标，将智能制造作为人工智能标准化重点行业应用领域之一，规范人工智能技术用于工业制造过程中的信息感知、自主控制、系统协同、个性化定制、检测维护、过程优化等方面的技术要求，提出从基础安全，数据、算法和模型安全，技术和系统安全，安全管理和服务，安全测试评估，产品和应用安全等 6 方面，推进人工智能技术安全标准研制。

为落实第 13859 号行政令《维持美国在人工智能方面的领导地位》有关要求，特别是减少人工智能技术在智能制造、智慧医疗等领域的应用障碍，美国发布《人工智能应用监管指南》，从监管和非监管层面对非联邦政府机构开发和部署人工智能提出了 10 项管理原则，其中“安全保障”原则强调在智能制造等领域的人工智能设计、开发、部署和运行全流程中必须考虑安全问题，确保人工智能系统处理、存储和传输信息的保密性、完整性和可用性，并要求进一步提升相关应用系统抵御网络攻击的能力。

四、监测情况

2020 年，国家工业信息安全发展研究中心联合 31 家支撑机构初步建成国家工业信息安全监测预警网络。从年度监测数据分析，我国低防护联网工业控制系统和设备数量呈现激增态势，市政、制造、交通等行业风险较高，工业信息安全漏洞数量持续增长。

（一）低防护联网设备监测情况

低防护联网设备是指暴露于公共互联网，自身防护水平差，可被识别、监测，存在极大被远程入侵风险的设备。国家工业信息安全发展研究中心自2014年起开展针对低防护联网工业控制系统的在线监测工作，目前可识别种类已从工业控制系统扩展至物联网终端、工业信息系统及工业互联网设备等，共计500余种。经对比分析多轮次在线监测数据，各类低防护联网设备数量相比去年均有较大幅度增长。

1. 我国低防护联网设备数量已超500万，其中工业控制系统已突破2.5万

2020年12月最新监测数据显示，**我国各类低防护联网设备数量总计超过500万，**其中，摄像头、车载模块、打印机等终端设备占比超过80%。可编程逻辑控制器（PLC）、数据采集与监视控制系统（SCADA）、数据传输单元（DTU）等**工业控制系统数量已超过2.5万**，相比2019年增加近4倍。从地域分布来看，低防护联网工业控制系统分布于全国31个省（区、市）（见图1），其中，山东、辽宁、北京排名前3，数量均超过2000台/套。

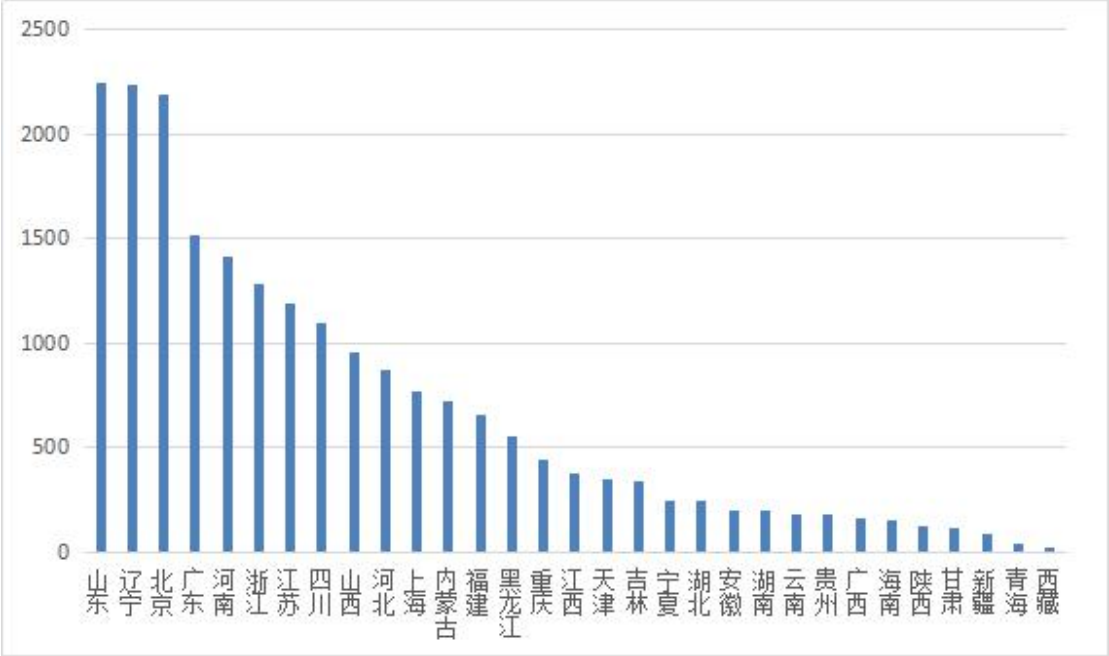

图 1　低防护联网工业控制系统数量（单位：台/套）

2. 低防护联网工业控制系统中，电力系统、Modbus 协议设备、DTU 数据采集终端占比最高

据 2020 年 12 月监测数据显示，DLT698 电能采集主站、Modbus 协议设备、DTU 数据采集终端占比分别为 31.60%、20.52%和 20.03%（见图 2）。其中，Modbus 协议设备涉及施耐德、和利时、通用电气、罗克韦尔、浙江中控等国内外主流工业控制系统厂商，在智能制造、能源、化工等多个重点行业领域应用广泛，由于 Modbus 协议自身安全性不足，存在加密手段缺失、授权认证不足等固有问题，导致此类低防护联网设备存在较大安全隐患。

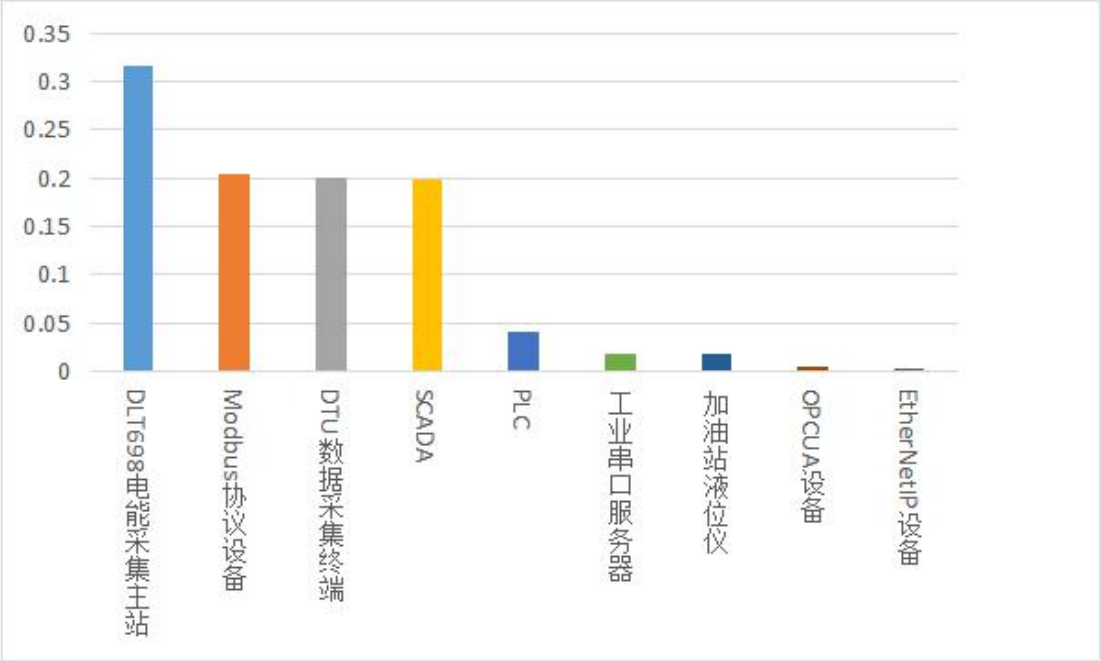

图 2　各类低防护联网工业控制系统占比情况

3. 低防护联网工业控制系统数量激增原因分析

从近年监测统计数据看，低防护联网工业控制系统数量持续攀升。2018 年 12 月为 3000 余台/套，2019 年底数量增至 5000 余台/套，2020 年相比 2019 年同期增长了 375%。（见图 3）

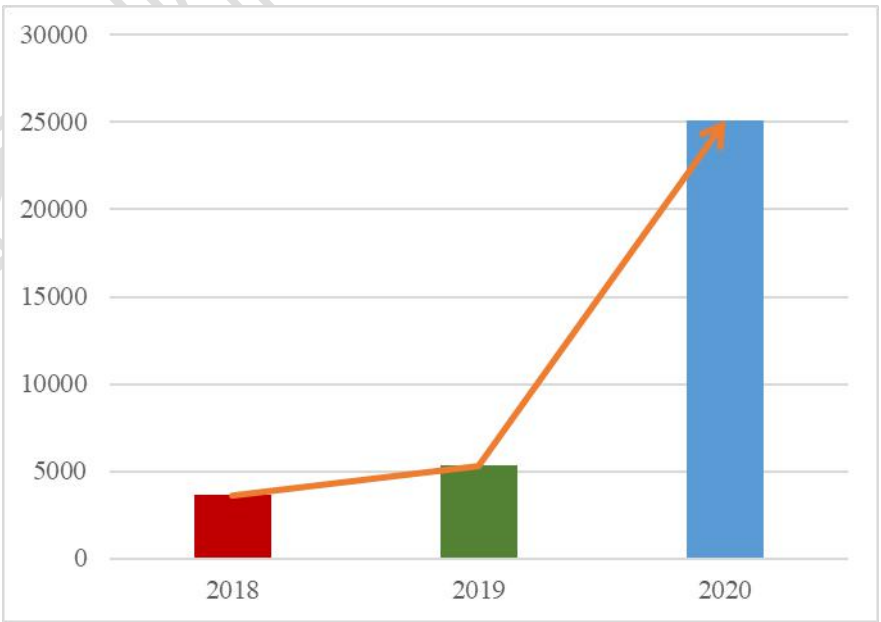

图 3 2018-2020 年低防护联网工业控制系统数量（（单位：台/套））

主要原因有：**一是工业数字化转型的推动作用。**工业数字化转型推动着工业企业向智能化、数字化、网络化生产服务模式转变，工业设备“上云”“上平台”，风险面快速扩大。**二是监测技术水平提升。**通过深耕工控指纹识别、工业协议解析、高交互仿真、安全大数据分析等核心技术，国家工业信息安全监测预警网络在2020年完成第3轮技术更新，监测范围、探测能力、节点覆盖量等均有大幅提升。**三是工业企业安全防护仍不到位。**经研判分析，部分工业企业仍存在设备固件更新和系统漏洞修复不及时、使用默认口令或弱口令、开放非必要远程服务端口等情况，安全意识和防护水平亟待提高。

（二）风险研判情况

2020年，国家工业信息安全发展研究中心抽样研判工业信息安全风险近800个，涉及制造、交通、市政等多个重点行业，研判发现工业控制系统、工业信息系统存在受攻击面大、漏洞利用难度低等问题。

1. 市政、制造、交通等行业安全风险偏高

在研判的工业信息安全风险中，35%集中于热力、环境监测、给排水等市政领域，上述领域均采用管网监控，工业控制系统联网比例高，若缺乏有效安全防护，极易被攻击者入侵，致使关键数据泄露，控制指令篡改、生产运行停滞。另有16%的安全风险源于制造业，制造业的工业控制系统、

工业信息系统应用基数大，在环境参数采集、仪表信息配置等环节多采用远程操作，风险暴露面较大。此外，交通、电力、石油等行业领域也面临着严峻的安全挑战（见图 4）。

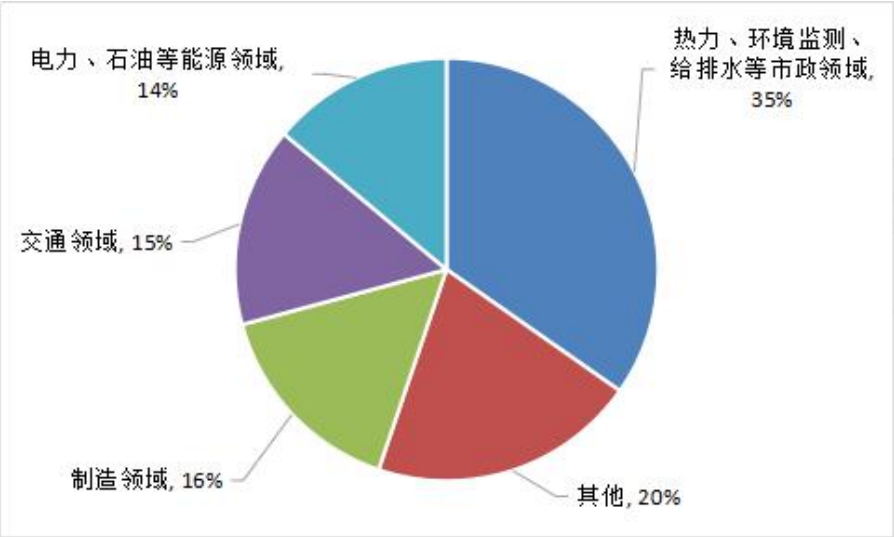

图 4　工业信息安全风险行业分布图

2. 弱口令漏洞、未授权访问漏洞普遍

在研判的工业信息安全风险中，主要存在弱口令漏洞、未授权访问漏洞、目录遍历漏洞、SQL 注入漏洞等，其中，弱口令漏洞占比 61%、未授权访问漏洞占比 11%、目录遍历漏洞占比 9%，三类漏洞总计占比达 81%（见图 5）。这三类漏洞利用门槛低，影响范围广，存在较大风险隐患。受影响系统及设备多为 SCADA、工业信息系统、串口服务器等。

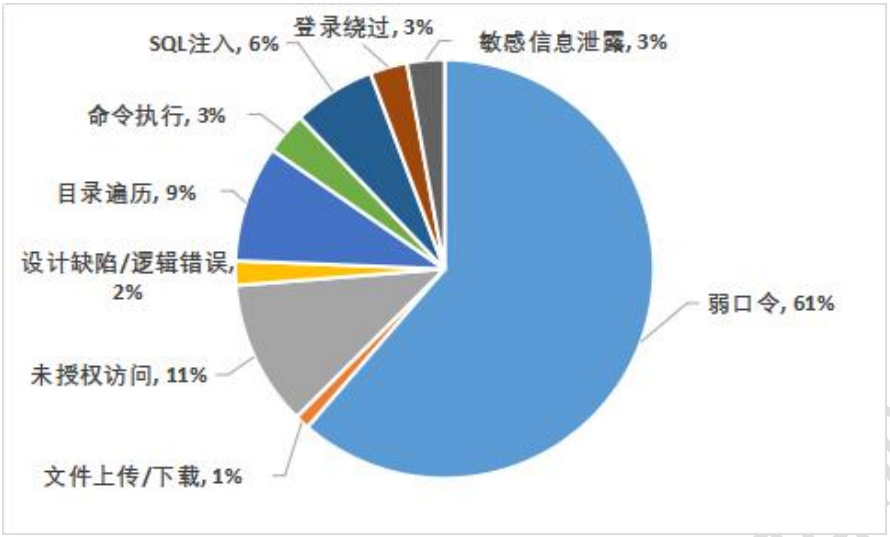

图 5　工业信息安全风险类型统计图

（三）安全威胁情况

依托国家工业信息安全监测预警网络，对 S7Comm、Modbus、OmronFINS、DNP3 等 10 余种工业专属协议进行高交互仿真，研发并实施了工控蜜罐网络一期部署，全年捕获来自境外的恶意网络攻击累计 200 余万次，平均每个蜜罐每日捕获攻击 50 余次。

1. 通用型工业协议遭受攻击次数高于特定行业专属协议

从攻击协议分析，S7Comm 和 Modbus 两种主流通用协议遭受攻击次数最多，占比近 40%。DNP3、IEC104 等特定行业专属协议遭受的攻击次数相对较少（见图 6）。

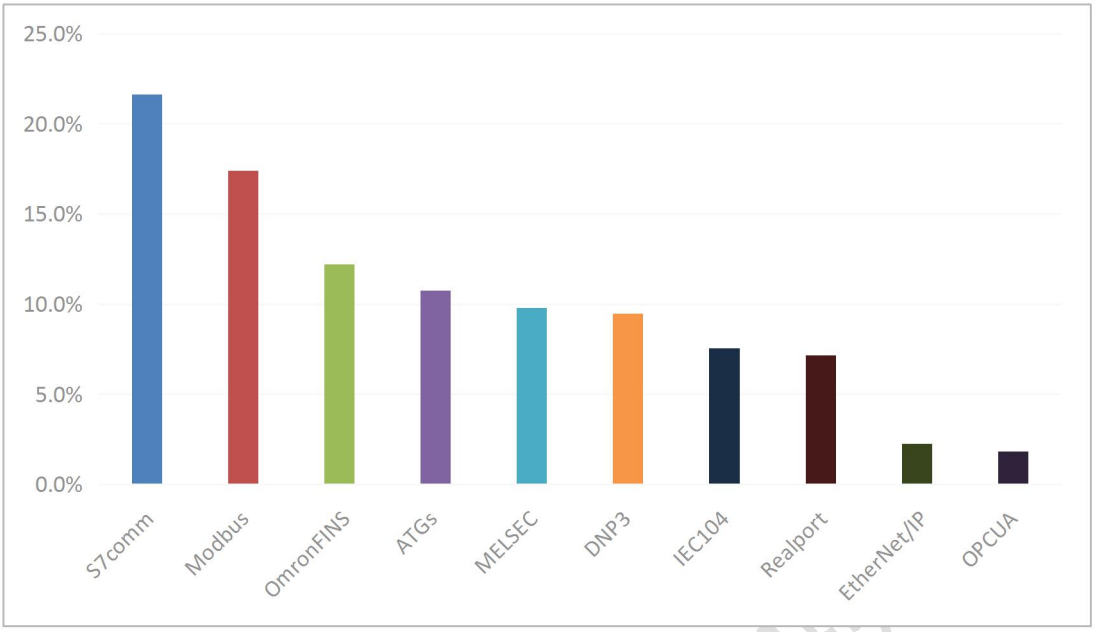

图 6　不同协议的工控蜜罐捕获攻击占比情况

2. 东部沿海地区遭受攻击次数高于内陆地区

从我国遭受攻击的区域情况看，东部沿海地区遭受攻击次数相对较多，其中，浙江、江苏、上海排名前三（见图 7）。

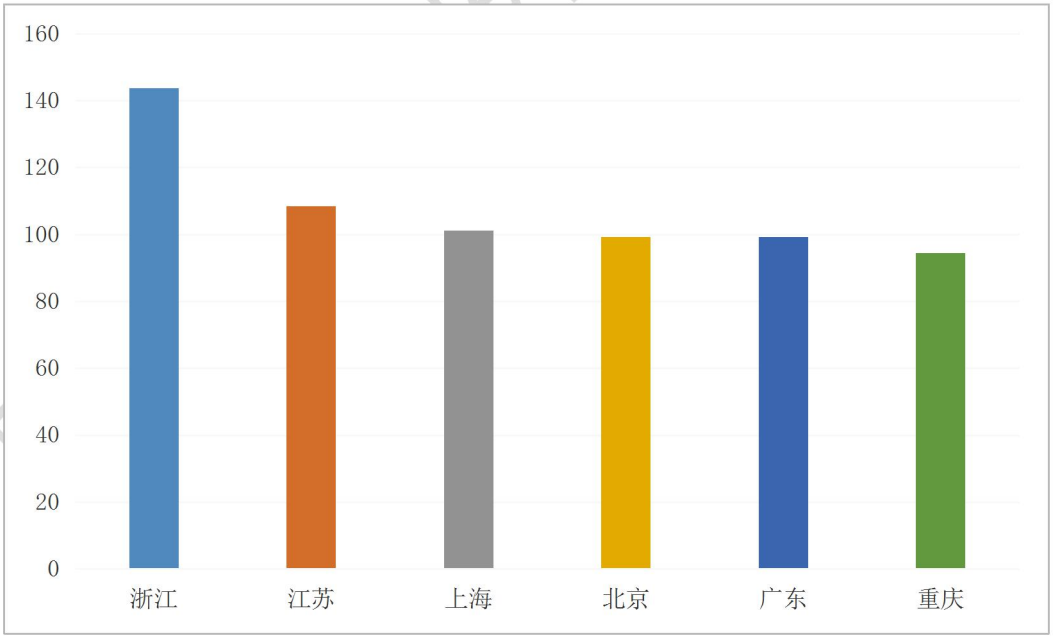

图 7　我国每个蜜罐每天遭受攻击数量省份排名 TOP6（单位：次）

（四）漏洞跟踪情况

国家工业信息安全漏洞库（CICSVD）在 25 家成员单位

的支持下，持续开展工业信息安全漏洞收集整理工作，逐步完善工业信息安全漏洞发现和应急处置生态。整体来看，2020 年工业信息安全漏洞保持高速增长，呈现危害等级高、分布范围广、成因多样的特点。

1. 漏洞数量高速增长

2020 年，CICSVD 共收录工业信息安全漏洞 2138 个，较 2019 年上升 22.2%，其中通用型漏洞 2045 个，事件型漏洞 93 个，保持了较高的增长态势。每月漏洞收录情况如图 8 所示。

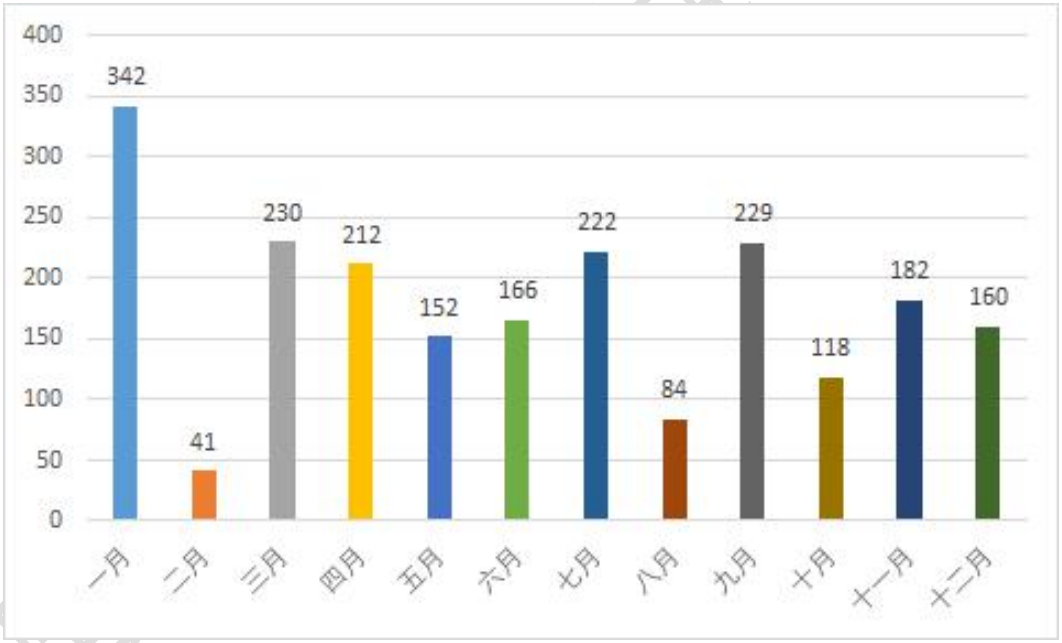

图 8　CICSVD 收录漏洞月度分布情况（单位：个）

2. 高危漏洞占比居高不下

2020 年，CICSVD 收录的通用型漏洞中，高危及以上漏洞占比高达 62.5%。具体来看，超危漏洞 379 个（占比 18.5%），高危漏洞 899 个（占比 44%），中危漏洞 716 个（占比 35%），

低危漏洞 51 个（占比 2.5%）（见图 9）。危害等级较高的漏洞包括 Treck TCP/IP 软件库漏洞、法国施耐德电气公司 Easergy T300 认证绕过漏洞、德国 WAGO 公司 I/O-CHECK 工业软件缓冲区错误漏洞、瑞士 ABB 公司 Relion 670 Series 目录遍历漏洞等。

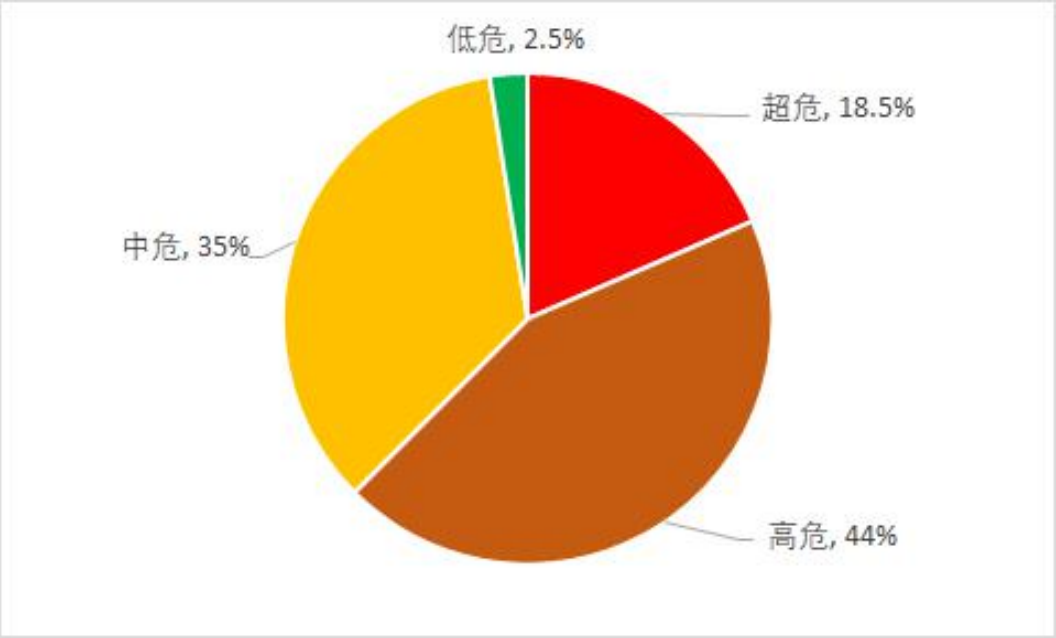

图 9　CICSVD 收录漏洞按危害等级分布

3. 漏洞分布范围广泛

在 CICSVD 收录的通用型漏洞中，受影响产品共涉及 10 个大类、66 个小类。其中，工业主机设备和软件类、工业生产控制设备类和工业网络通信设备类产品是收录漏洞数量最多的产品大类，合计占比 72.8%（见图 10）。从产品小类来看，PLC、组态软件、工业路由器、SCADA、工业软件是收录漏洞数量最多的 5 类产品，合计占比 83%（见图 11）。漏洞基本涵盖国内外主流设备厂商，涉及德国西门子公司、

法国施耐德电气公司、瑞士 ABB 公司等 335 家厂商，影响关键制造、能源、化工、医疗、安防等重点领域。

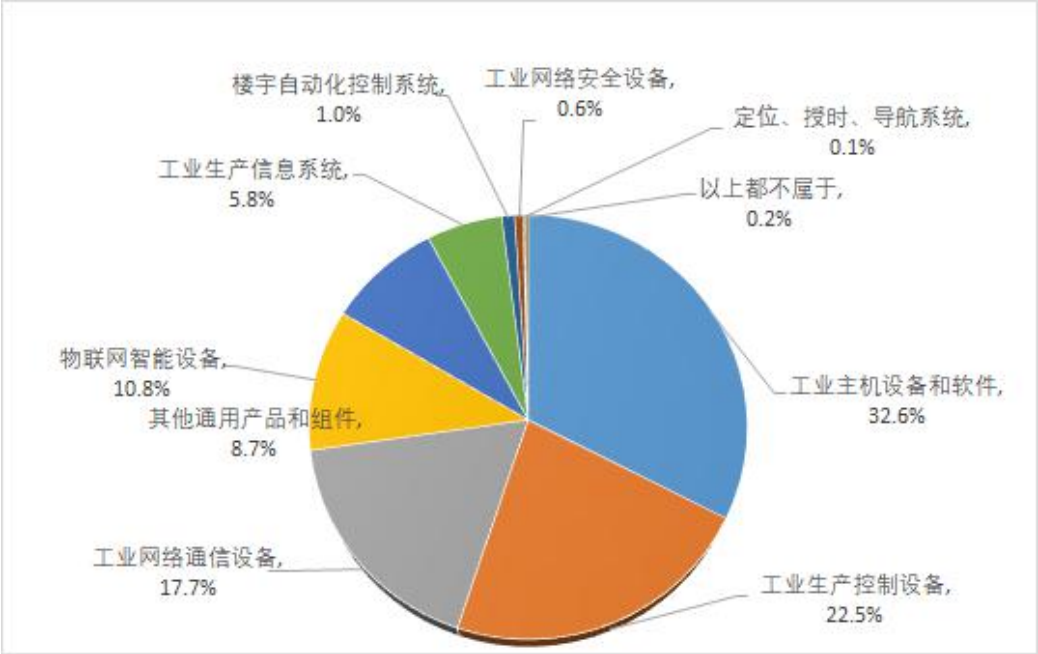

图 10　CICSVD 收录漏洞按受影响产品大类分布

图 11　CICSVD 收录漏洞按受影响产品小类分布

4. 漏洞类型多样

按照漏洞成因分类，2020 年 CICSVD 收录的漏洞中共涉及 31 种漏洞类型。其中，缓冲区错误漏洞数量最多，为 337

个（占比 16.5%），输入验证错误、授权问题、资源管理错误漏洞分别占比 7.4%、7.2%和 6.9%。（见图 12）。

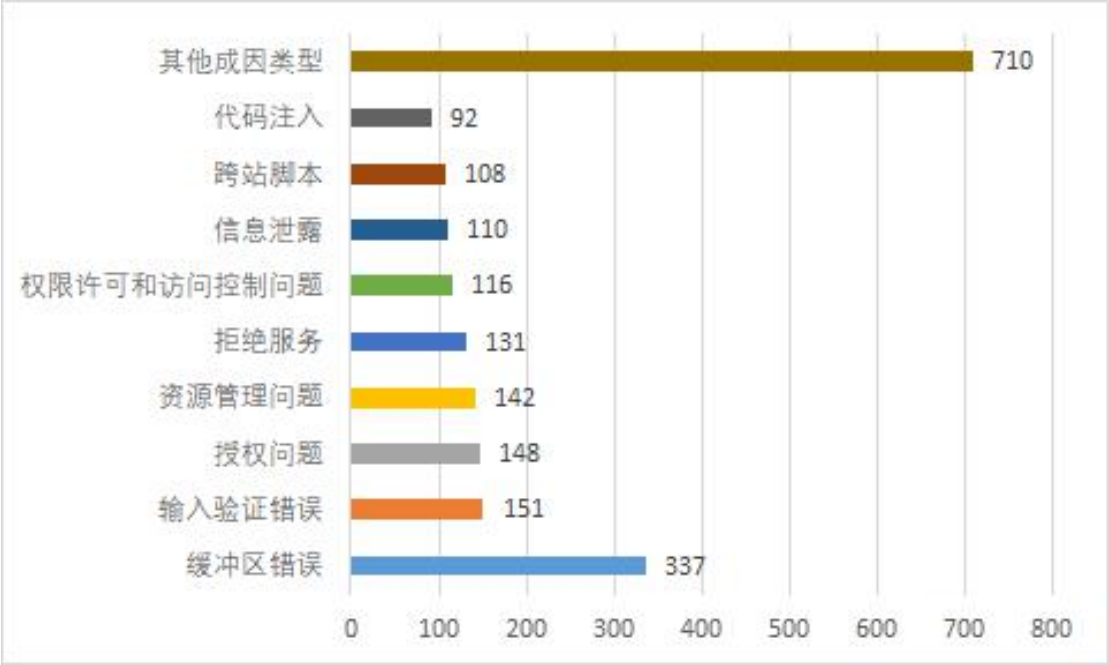

图 12　CICSVD 收录漏洞类型（单位：个）

五、对策建议

随着工业企业数字化、智能化程度进一步提高，工业企业联网、“上云”已成大势，传统工业信息安全风险隐患在网上的“暴露”日益增多，面临的安全威胁愈发严峻。建议紧密围绕“一网络”“一体系”“一核心”“一队伍”，强化态势感知、提升响应能力、保护数据安全、建设基础力量，切实保障国家工业信息安全。

（一）依托“一网络”，强化整体安全态势感知

依托以国家级工业信息安全态势感知平台为核心、国家、省/行业、企业三级联动的“纵横网络”，密切跟踪工业信息安全风险与威胁，加强技术手段建设，稳步提升整体

安全态势感知能力。

1. 持续发挥国家平台作用

加强主动监测、资产识别、风险研判、威胁诱捕、流量分析、协议解析、数据分析等技术研究，丰富技术工具，持续增强国家级工业信息安全态势感知平台技术手段和能力。把握国家工业信息安全风险态势，开展威胁分析、风险研判、预警通报，切实发挥国家级工业信息安全态势感知平台作用。

2. 着力加快地方平台建设

加快省级、市级工业信息安全态势感知平台建设，实现对地方辖区内低防护联网设备的识别与监测，开展地方工业信息安全风险发现、威胁分析、攻击溯源，提升地方工业信息安全态势感知能力，鼓励地方平台与国家平台实现数据交互与对接，丰富国家工业信息安全监测预警网络，形成上下联动工作模式，为国家整体安全态势感知提供支持。

3. 提升企业风险发现能力

依托国家级、地方级工业信息安全态势感知平台技术资源，支持重点工业企业建立安全监测系统，运用流量监控、安全检测等技术，及时发现设备非法接入、恶意探测攻击等行为，实现对工业企业设备资产的动态管控、系统异常操作监控、网络威胁实时告警，提升工业企业风险发现与感知能力。

（二）建立“一体系”，提升防护处置综合能力

加强对工业企业信息安全防护工作的指导督促，推动工业企业筑牢自身安全防护基础，同时做好应急资源储备，定期开展应急演练，稳步提高工业信息安全事件应急指挥决策、分析研判、资源调度、处置实施的效率和能力。

1. 守牢安全防护底线

针对当前工业领域仍普遍存在的防护责任不清晰、防护意识不够强、防护措施不到位的问题，指导督促企业按照《工业控制系统信息安全防护指南》要求，确立工业企业安全防护主体责任，持续强化安全风险监测、安全软件管理、配置补丁管理、边界安全防护、物理安全防护等措施，从管理和技术两个方面，牢牢守住工业信息安全防护底线。

2. 完善应急基础资源

完善国家工业信息安全应急资源库，健全国家工业信息安全漏洞库功能，持续汇聚工业信息安全漏洞风险、解决方案、应急预案等基础资源，持续发挥国家工业信息安全应急资源库在工业信息安全资源储备、分析决策、应急指挥、事件处置等方面对国家、行业、地方的基础性、支撑性作用。

3. 提高响应处置能力

健全国家、地方、企业三级应急联动机制，协同推进工业信息安全信息共享、预警通报、事件处置。定期组织工业信息安全应急管理培训，帮助行业、地方、企业把握政策标

准，掌握风险监测、预警通报、应急处置技术，提高工业信息安全知识与技能水平。开展覆盖国家、地方、企业层面工业信息安全事件应急演练，提升应对工业信息安全事件的组织指挥和快速处置能力。

（三）围绕“一核心”，确保工业数据资源安全

为保护工业数据“核心资产”，必须进一步贯彻《工业数据分类分级指南（试行）》，制定工业数据安全保护标准规范，管理和技术“双管齐下”，确保工业数据采集、传输、存储、处理等全生命周期安全。

1. 推进数据分类分级管理

落实《工业数据分类分级指南（试行）》要求，继续按照“企业点突破、行业线贯通、地方面推广”的工作思路，进一步加强宣贯培训，推广优秀企业案例，打造标杆示范效应，立足行业特征细化数据分类目录和分级量化指标，指导更多企业建立工业数据分类分级管理体系，为工业数据安全使用和有序共享奠定基础。

2. 制定工业数据安全标准

围绕工业数据分类分级管理要求，研究制定工业数据分类分级安全防护标准，明确针对不同类别、不同级别工业数据的安全保护要求，为重点行业、工业企业提供可对照、可诊断、可评价的工业数据安全规范，确保工业数据分类分级管理措施具有可操作性，将工业数据安全保护落到实处。

3. 确保数据全生命周期安全

以工业数据为核心，在理清数据资产、掌握数据用途、了解数据风险的基础上，遵循最小化授权、分类分级保护、可审计等原则，构建覆盖数据采集、数据传输、数据存储、数据使用和数据销毁等工业数据生命周期各个环节的安全保护机制、流程与策略，确保工业数据异常情况的及时发现和快速应对。

（四）打造“一队伍”，建设坚实安全保障力量

在全国范围内开展工业信息安全技术队伍选拔评价，培育一支覆盖国家、行业、地方的技术实力强、综合素质好的工业信息安全队伍力量，形成相互协同、有效配合的格局，为国家工业信息安全保障奠定坚实基础。

1. 建立专业队伍选评机制

面向全国范围内的技术机构、安全企业，遴选一批有资质、有条件、有能力、有素质的专业队伍，形成以国家队为核心、以地方队为协同的工业信息安全专业队伍力量，通过科学的选拔和评价机制，形成进退有序、优胜劣汰的良性循环，为保障国家工业信息安全提供专业力量支持。

2. 充分发挥专业队伍作用

建立国家和地方工业信息安全专业队伍协同机制，围绕风险发现、威胁共享、态势感知、应急处置等方面，构建“上下联动、多方协同”的工作机制，实现全天候风险发现、全

方位态势感知、全流程应急响应，发挥专业队伍合力，共同保障国家工业信息安全。

国家工业信息安全发展研究中心

地　　址：北京市石景山区鲁谷路 35 号

邮政编码：100040

联系电话：010-88686332　010-88686273

电子邮箱：zhanghuimin@cics-cert.org.cn

网　　址：http://www.cics-cert.org.cn/