工信安全智库

研判系列报告

报告编号：2019-yp-01

# 2018 年度工业信息安全形势分析



国家工业信息安全发展研究中心

信息政策所

2019 年 1 月

# 编写组

组　长：尹丽波

副组长：黄　鹏　　高晓雨

成　员：孙倩文　　申　畯　　徐　杰　　李　端

李晓婷　　闫　寒

# 序

国家工业信息安全发展研究中心信息政策所成立于 2018 年 9 月，立足深化供给侧结构性改革和加快建设创新型国家战略需求，围绕制造强国和网络强国建设任务，聚焦信息安全、数字经济、信息技术产业等重点领域，开展基础性、战略性、先导性智库研究，为工业和信息化部、中央网信办、国家发展改革委等提供智力支持。

2019 年 1 月起，信息政策所陆续推出“研判”“瞭望”“洞察”“指数”等系列研究报告，围绕党和政府决策急需的相关重大课题和关键问题，开展形势研判、国际跟踪、专题调研和景气测度等方面的持续研究，为主管部门预见走势、把握机遇、应对挑战、谋划战略提供参考。

此次推出的“研判系列报告”含 3 册，分别针对工业信息安全、数字经济和信息技术产业领域，开展了 2018 年基本情况、问题挑战和发展趋势的分析研究。后续“研判系列报告”将每半年发布一次，敬请持续关注。

由于成稿仓促，加之水平有限，报告中难免有疏漏和错误之处，恳请批评指正。

编写组

2019 年 1 月

# 前　言

互联网的迅猛发展深刻改变社会生产生活方式的同时，也对国家安全和经济发展不断提出新挑战。习近平总书记深刻指出，“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题”“没有网络安全就没有国家安全”。当前，我国已开始进入从工业经济向数字经济转型的拐点，制造业正由数字化阶段迈向网络化阶段，工业设备和系统以及生产、管理和服务过程通过映射和具象愈发成为网络空间的重要组成部分，工业信息安全防护的重要性和紧迫性凸显，已经成为网络安全的重中之重。

2018 年，全球范围内针对工业领域的网络攻击有增无减。信息窃取、勒索攻击、病毒感染、网络间谍、黑客入侵等多种攻击手段花样多变，攫取经济利益、盗取知识产权、攻击关键信息基础设施等大规模高强度的安全事件屡有发生，对政治、经济、军事、国家和社会安全等造成直接威胁和现实影响，工业信息安全成为各国政府高度关注的重大安全领域。

2018 年，是我国改革开放 40 周年。40 年来，随着改革开放的不断深入，工业领域社会生产力得以迅猛发展，技术进步扎实推进，两化融合日益深化，工业生产环境从封闭走向开放，生产过程从自动化走向智能化。工业控制系统由单机走向互联，广泛应用于核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输等国家核心领域。2018 年，我国工业信息安全领域出现令人鼓

舞的大好局面，在政策标准、行业技术、平台建设、产业发展、人才培养、机构调整等方面全面发力，部分工作实现突破性进展。

立足现实，放眼未来。我们须清醒地认识到我国工业信息安全发展整体仍处于初级阶段，面对发展初期技术短板、人才紧缺、产业薄弱等现实问题，须以新时代、新担当、新作为的历史责任感，扑下身子，埋头苦干，努力为工业生产安全和两化融合健康发展撑起“保护伞”，为制造强国和网络强国战略实施筑牢“防护墙”。

# 目 录

随着工业数字化、网络化、智能化快速发展，工业信息安全的重要性和紧迫性更加凸显。2018 年，工业信息安全形势复杂严峻，安全风险愈演愈烈，总体态势不容乐观。面对日益严重的安全问题，我国工业信息安全工作稳步推进，政策体系不断完善，安全防护和保障能力建设取得实效。但是，我国在工业信息安全的核心技术、关键产品、服务能力、保障体系、人才培养等领域仍面临诸多问题和挑战。在可预期的未来，工业领域的信息安全风险仍将持续，工业领域仍是网络攻击的主要目标。因此，我们要加快提升工业信息安全保障能力，为实现制造强国和网络强国战略目标奠定坚实基础。

## 一、基本情况

### （一）多国加强网络安全战略部署，高度关注关键信息基础设施安全

**以美国为首的西方发达国家凭借自身优势，进一步完善网络安全战略部署。**美国发布了特朗普政府首份网络安全战略报告——《国家网络战略》，战略部署了美国网络空间发展的四项支柱、十项目标和 42 项优先行动，完善美国网络安全战略体系，增强网络空间综合实力，遏制各类对网络空间发展造成不稳定的行为，为经济增长和激励创新保驾护航。新加坡 7 月发布《网络安全法案》，提出针对关键信息基础设施的监管框架，明确关键信息基础设施的概念及认定程序，建立网络安全事件预警响应机制，赋予网络安全官员对

网络安全事件风险调查的权利。另外，以美国为代表的西方发达国家，通过设立网络司令部、颁布法令等形式，系统提升网络战电子战能力，并将矛头直指中国、俄罗斯、伊朗等国。5 月，美国网络司令部正式升级为一级联合作战司令部，拥有独立执行国家安全任务和作战任务、配合战区实施作战行动、组织与盟军开展联合网络空间作战行动的自主权。8 月，2019 财年《美国国防授权法案》确立多项涉及国防领域重要网络措施，确认了国防部在防范网络攻击和网络作战方面的作用。12 月，美国政府问责局发布的《美国未来四大战略威胁》报告将中国、俄罗斯、伊朗、朝鲜等国列为重要对手，并指出这些国家可能会对美国的关键信息基础设施、军事基础设施、医疗保健系统、航空系统等发起网络攻击，实现对设备、系统的非法控制或破坏其中数据。主要国家和地区 2018 年发布的网络安全战略如表 1 所示。

**主要工业化国家在电力、能源、交通等重要行业，出台政策构建关键信息基础设施保护体系。**2018 年 4 月，美国国家标准与技术研究院发布《提升关键基础设施网络安全框架》（1.1 版），在 2014 年 2 月发布的 1.0 版的基础上进行了升级和补充。5 月，美国能源部发布《能源行业网络安全多年计划》，确定美国能源部未来五年力图实现的目标、计划和具体举措，以降低网络事件给美国能源带来的风险。这也成为了较早在关键信息基础设施单一领域形成安全防

护计划的范例。另外，欧盟颁布行使的“网络与信息安全指令”（NIS）力图通过加强网络防御能力来提升服务安全性与弹性，以保障电力、交通、医疗卫生等关键行业基础设施安全，包含各在线市场、搜索引擎以及关键信息基础设施供应商等。指令要求欧盟成员国建立国家网络安全战略、成立计算机安全事件应急小组（CSIRT），建立国家 NIS 主管部门。

**表 1　2018 年主要国家和地区发布的网络安全战略政策文件**

| 国别 | 时间 | 名称 | 主要内容 |
|---|---|---|---|
| 美国 | 2018.01 | 《网络漏洞公开报告法案》 | 美国众议院通过了《网络漏洞公开报告法案》，要求国土安全部建立公开网络漏洞报告和机密附件的机制和程序。 |
| | 2018.01 | 《外国情报监控法修正案》 | 美国众议院通过了《外国情报监控法修正案》，授权美国国家安全局继续监听境外的外籍人士，并可收集与之相关的美国公民情报。法案待美国总统特朗普签署后，将正式成为法律。 |
| | 2018.03 | 《美军网络司令部愿景：实现并维持网络空间优势》 | 《美军网络司令部愿景：实现并维持网络空间优势》旨在帮助网络司令部实现并维持在网络空间领域的优势，指导和协调网络司令部在网络空间领域的规划和作战，捍卫和推进美国国家利益。 |
| | 2018.05 | 《网络安全战略》 | 美国国土安全部发布《网络安全战略》，致力于使各部门协调一致地开展网络安全工作，以更好地履行网络安全使命，以保护关键基础设施免于遭受网络攻击。 |
| | 2018.05 | 《能源行业网络安全多年计划》 | 美国能源部发布《能源行业网络安全多年计划》，确定了能源部未来五年力图实现的目标和计划，以及实现这些目标和计划将采取的相应举措，以降低网络事件给美国能源带来的风险。 |
| | 2018.08 | 《NIST 小企业网络安全法》 | 美国总统签署《NIST 小企业网络安全法》，要求国家标准与技术研究院提供针对小型企业的网络安全资源和指南，帮助中小企业识别、评估和降低其网络安全风险。 |

| 国别 | 时间 | 名称 | 主要内容 |
| --- | --- | --- | --- |
| | 2018.09 | 《2018 网络威慑与响应法案》 | 美国众议院通过《2018 网络威慑与响应法案》，旨在阻止和制裁未来国家支持的针对美国的网络攻击，以保护美国的政治、经济和关键信息基础设施免受侵害。 |
| | 2018.09 | 《2018 国防部网络战略》 | 美国国防部公布的《2018 国防部网络战略》指出，美国正与中国和俄罗斯进行长期战略竞争，要综合运用网络能力收集中国和俄罗斯等强敌的情报，为未来冲突做好准备。 |
| | 2018.09 | 《国家网络战略》 | 《国家网络战略》概述了美国网络安全的四项支柱，十项目标与 42 项优先行动，凸显了网络安全在美国国家安全的重要地位。 |
| | 2018.12 | 《网络安全战略报告》 | 美国国防部的《网络安全战略报告》重点点名了中俄等“能够给美国制造战略威胁”的国家，提出了 6 个应对网络安全事件的核心内联概念以及解决网络安全问题的 6 个重点。 |
| 欧盟 | 2018 | 《网络与信息安全指令》 | 欧盟的《网络与信息安全指令》（NIS）于 2018 年开始执行，旨在保障关键行业（电力、交通、医疗卫生等）基础设施安全。 |
| | 2018.05 | 《通用数据保护条例》 | 欧盟的《通用数据保护条例》（GDPR）开始执行，违反 GDPR 的组织将被处罚高达全球年营业额的 4%或 2000 万欧元，两者以较高为准。 |
| 英国 | 2018.03 | 《网络安全出口战略》 | 英国政府为英国的网络安全公司推出了《网络安全出口战略》，旨在帮助英国的网络安全企业进入国际新市场，提升产品和服务的出口规模。 |
| | 2018.06 | 《最低安全标准》 | 英国政府与国家网络安全中心（NCSC）合作推出《最低安全标准》，所有商业组织机构提供了安全框架。英国所有政府机构（包括组织机构和承包商）均被要求强制执行该标准。 |
| 立陶宛、克罗地亚、爱沙尼亚、荷兰、罗马尼亚、西班牙 | 2018.06 | 《网络安全意向联合声明》 | 立陶宛、克罗地亚、爱沙尼亚、荷兰、罗马尼亚、西班牙 6 国签署《意向声明》表示将按照“永久结构化合作”防务机制成立“网络快速响应小组”，应对网络攻击。 |
| 加拿大 | 2018.06 | 《国家网络安全战略》 | 加拿大推出新版《国家网络安全战略》，规划加拿大在网络安全方面的路线图，指导加拿大政府开展网络安全活动，以保护加拿大公民的数字隐私、安全和经济。 |

| 国别 | 时间 | 名称 | 主要内容 |
| --- | --- | --- | --- |
| 澳大利亚 | 2018.02 | 《数据泄露通报法案》 | 《数据通报法案》于 2 月生效，是对澳大利亚隐私法案 1988PartIIIC 的修正案，建立强制性的数据泄露通报制度，要求所有需要遵守澳大利亚隐私法案和隐私原则的机构和团体都需采取措施防止数据泄露事件。 |
| 新加坡 | 2018.02 | 《网络安全法案》 | 新加坡议会正式通过《网络安全法案》，旨在建立关键信息基础设施所有者的监管框架、网络安全事件响应和预防机制、网络安全服务许可机制等，提升网络攻击防范能力。 |

资料来源：国家工业信息安全发展研究中心整理

### （二）全球工业信息安全事件频发，工业企业面临严重威胁

2018 年，全球工业信息安全领域重大安全事件时有发生，**针对工业自动化设备、网络设备和工业控制系统的漏洞攻击、信息窃取、信息探测等恶意攻击行为对工业信息安全造成严重威胁。**1 月，“熔断”（Meltdown）和“幽灵”（Spectre）两大新型漏洞通过攻击获取数据、读取内核内存影响 AMD、ARM、Intel 系统和处理器等设备，思科 800 系列集成多业务路由器和工业以太网 4000 系列交换机以及西门子工业设备已确认受到影响。2 月，接入欧洲废水设施运营技术网络的服务器遭遇加密货币采矿恶意软件入侵，拖垮废水处理设备中的 HMI 服务器 CPU，导致欧洲废水处理设备服务器瘫痪。7 月，包括福特、特斯拉、丰田、大众等在内的 100 余家制造公司的 157GB 含有高度敏感信息的商业和技术文档被曝光。11 月，柬埔寨多家互联网服务商遭到该国历史上最大规模 DDoS 攻击，150Gbps 的 DDoS 攻击造成全国性网络瘫痪，宕机时间超过半天。另据卡巴斯基监测，

勒索软件“永恒之蓝”（WannaCry）仍在孟加拉国等亚洲国家特别活跃。黑客和恶意组织针对特定工业设备、工业软硬件系统中存在的漏洞发起网络攻击，窃取数据信息，干扰工业设备正常运行，影响生产安全。2018 年全球主要工业信息安全重要事件如表 2 所示。

**表 2　2018 年全球工业信息安全重要事件**

| 月份 | 事件 |
|---|---|
| 2 月 | 四台接入欧洲废水处理设施运营技术网络的服务器遭加密货币采矿恶意软件入侵，直接拖垮了废水处理设备中的 HMI 服务器 CPU，致服务器瘫痪。 |
| 4 月 | 美国 4 家天然气输气管道公司遭供应链攻击，导致用于与客户通信的电子系统被关闭。 |
| | 美国国土安全部（DHS）举行 2018“网络风暴”演习，模拟在关键信息基础设施风险加剧的情况下共享信息并响应威胁，参与者包括交通运输和关键制造行业在内的 1000 多人。 |
| 5 月 | 丹麦铁路运营商 DSB 遭遇了大规模的 DDoS 攻击，事件造成约 1.5 万旅客无法通过该公司的应用程序、售票机、网站和商店购票，运营商只得人工售票。 |
| 6 月 | 三一重工泵车失踪案宣判，犯罪分子通过源代码找到远程监控系统的漏洞，得以解锁设备，间接造成企业约 10 亿元的经济损失。 |
| | 法国工程公司 Ingerop 服务器遭受攻击，被窃取共计 11000 多份、65G 的敏感文件，内容涉及法国某监狱的监控摄像头位置、法国东北部规划中的核废料堆信息、有轨电车线路的图纸等十几个项目信息。 |
| 7 月 | 福特、通用、丰田、特斯拉等 100 多家公司发生数据泄露，157GB 含有高度敏感信息的商业和技术文档数据可公开访问。 |
| | 360 披露从 2011 年开始持续至今，高级攻击组织蓝宝菇（APT-C-12）对我国政府、军工、科研、金融等重点单位和部门进行了持续的网络间谍活动。该组织主要关注核工业和科研等相关信息，被攻击目标主要集中在中国大陆境内。 |
| 8 月 | 台湾积体电路制造三大厂区出现电脑大规模勒索病毒事件，约造成 87 亿元新台币（约合人民币 17.6 亿元）的营收损失。 |

| 月份 | 事件 |
| --- | --- |
| 9 月 | 趋势科技发布的调查报告显示，数据采集与监控系统（SCADA）系统 2018 年上半年的漏洞几近于 2017 年上半年的两倍。 |
| | 英国布里斯托机场遭勒索软件袭击，导致航班信息显示系统宕机，机场工作人员只能用白板和记号笔通知航班起降信息。 |
| 12 月 | 安全厂商 Upstream Security 发布的《全球汽车行业网络安全报告》预计，到 2023 年由于网络黑客攻击可导致汽车制造商损失 240 亿美元。 |

资料来源：国家工业信息安全发展研究中心整理

**从区域分布看，工业信息安全攻击事件涉及全球大部分国家和地区，欠发达地区受到的安全威胁更为严重。**能源、电力、精密制造业等关键基础设施遭遇 APT 攻击风险不断加大，APT 攻击活动几乎覆盖全球绝大部分国家和地区。卡巴斯基数据显示，2018 年上半年工业控制系统遭受攻击最多的六个国家分别为越南、阿尔及利亚、摩洛哥、突尼斯、印度尼西亚和中国，非洲、亚洲等欠发达地区遭受攻击数量远高于欧洲、北美和澳大利亚等相对发达的地区。这也反映出针对工业控制系统的网络攻击行为具有明显的国家和地区指向性（表 3、表 4）。上述资料显示，若不局限于工业领域，中国是全球遭受 DDoS 攻击次数最多的国家，受攻击总量多年来占全球总量一半以上，是网络攻击的主要目标国和最大受害国。值得欣慰的是，虽然我国工业信息安全防护体系尚多有不尽人意之处、防护能力尚有很大提升空间，但我国网络整体发展水平、网络安全防护策略和实力在发展中国家仍处于中上水平。这更加坚定了我们加快建设高质量网络安全特别是工业信息安全防护体系的信心和斗志。

**表 3　2018 上半年工业控制系统遭受攻击比例最高的 10 个国家或地区**

| 序号 | 国家或地区 | 占比 |
|---|---|---|
| 1 | 越南 | 75.1% |
| 2 | 阿尔及利亚 | 71.6% |
| 3 | 摩洛哥 | 64.8% |
| 4 | 突尼斯 | 64.6% |
| 5 | 印度尼西亚 | 64.0% |
| 6 | 中国 | 57.4% |
| 7 | 印度 | 55.2% |
| 8 | 伊朗 | 55.2% |
| 9 | 埃及 | 55.1% |
| 10 | 沙特阿拉伯 | 55.0% |

资料来源：卡巴斯基实验室

**表 4　2018 上半年工业控制系统遭受攻击比例最低的 10 个国家或地区**

| 序号 | 国家或地区 | 占比 |
|---|---|---|
| 1 | 丹麦 | 14.0% |
| 2 | 爱尔兰 | 14.4% |
| 3 | 瑞士 | 15.9% |
| 4 | 荷兰 | 15.9% |
| 5 | 瑞典 | 16.1% |
| 6 | 英国 | 17.3% |
| 7 | 奥地利 | 17.6% |
| 8 | 中国香港 | 19.4% |
| 9 | 以色列 | 20.1% |
| 10 | 美国 | 21.4% |

资料来源：卡巴斯基实验室

### （三）全球工控系统安全漏洞居高不下，制造业和能源行业风险加剧

工控系统的开放互联，使自身安全风险不断增多、安全漏洞出现蔓延。国家工业信息安全发展研究中心监测发现，已连接互联网的工业控制系统覆盖数据采集与监测控制系统（SCADA）、分布式控制系统（DCS）、过程控制系统（PCS）、可编程逻辑控制器（PLC）及现场总线控制系统（FCS）等多个门类，涉及西门子、罗克韦尔、施耐德、ABB、台达、研华科技等工业控制系统厂商，广泛应用于制造业、商业设施、能源、农业、水利、通信等重点工业领域，其中能源、关键制造及水处理是工控安全漏洞分布较广的行业。

美国工业控制系统网络紧急响应小组（ICS-CERT）公布的工业控制系统漏洞信息显示，自 2015 年以来全球工业控制系统、智能设备、物联网等领域安全漏洞总数出现大幅上升且一直保持在较高水平（图 1）。2018 年漏洞总数为 426 个，同比增长 11.5%，其中高危漏洞 270 个，中危漏洞 148 个，中高危漏洞占比高达 95%（图 2）。

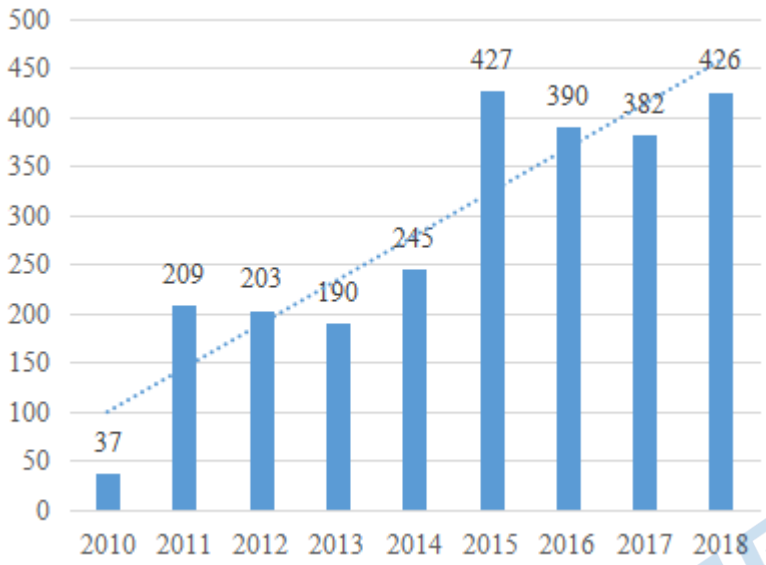


**图 1　2010-2018 年全球工控系统漏洞数量**

资料来源：美国 ICS-CERT

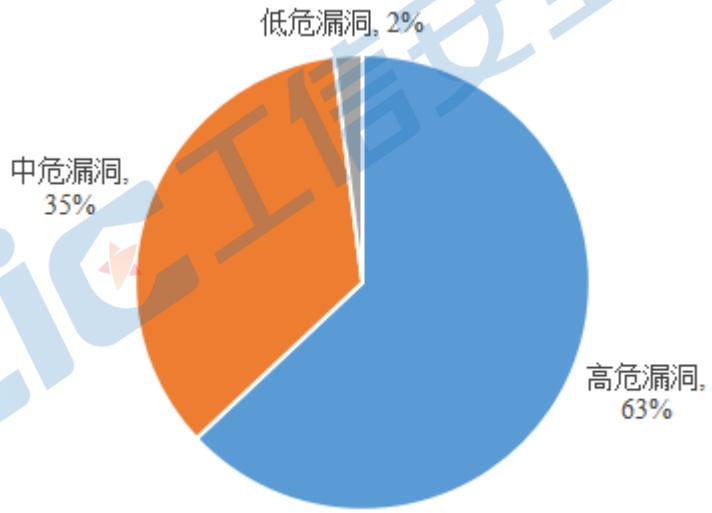


**图 2　2018 年全球工业控制系统漏洞分布**

资料来源：美国 ICS-CERT

**工业领域安全漏洞影响面巨大。**2018 年，瑞士工业技术公司 ABB 生产的部分 PLC 网关中存在两个未修复的高危漏洞。思科公开披露

存在于其自适应安全设备（ASA）软件和 Firepower 威胁防御（FTD）软件中的会话启动协议（SIP）检查引擎中的严重安全漏洞，可能导致设备重启和崩溃。福州维控电子广泛应用于制造、冶金、化工、能源、污水处理等领域的 PI Studio HMI 软件中发现多个安全漏洞。电网防护公司施瓦茨工程实验室管理和配置工具中出现多个高危漏洞，可导致信息泄露、任意代码执行等严重后果。

**（四）针对工业领域网络攻击方式多元，传统威胁加速向工业系统渗透**

**来自互联网的传统网络威胁成为工业控制系统感染的主要来源。**2018 年，恶意软件、病毒、钓鱼邮件、僵尸网络等传统网络威胁进一步向工业领域渗透。思科公司调查数据显示，31%的安全专业人员表示，其所在组织遭受过针对 OT 基础设施的网络攻击。据卡巴斯基统计，2018 年上半年工业系统三大网络威胁分别来自互联网网络威胁、可移动存储介质和邮件客户端。2018 年，针对工业领域网络攻击呈现出以下特点，**一是更精准、更擅伪装的勒索软件不断出现。**欧洲刑警组织 2018 年《互联网有组织犯罪威胁评估》显示，在大多数欧盟成员国中，勒索软件仍位列恶意软件威胁之首。3 月，黑客攻占印度一家电力公司的计算机系统并窃取客户账单数据，索要 1000 万卢比（约合 15.2 万美元）作为归还条件。8 月，WannaCry 卷土重来，造成台积电三大基地生产线停摆。12 月，莫斯科新缆车系

统遭遇勒索软件感染，同月我国爆发新型勒索病毒要求受害者使用微信支付赎金并窃取软件密码。**二是典型的网络钓鱼在制造业领域活动频繁**。2018 年上半年，卡巴斯基实验室发现新一轮网络钓鱼电子邮件攻击事件。虽然攻击主要针对俄罗斯境内工业企业，但其策略和工具可用于攻击世界任何国家的工业企业。8 月，从制造业企业窃取资金的网络钓鱼活动频繁出现，至少有 400 个组织的 800 台计算机感染，涉及制造业、石油、天然气、冶金、工程、能源、建筑、采矿和物流行业，该钓鱼活动从 2017 年 7 月已露踪迹。11 月，一起针对美国核工业、国防、能源、金融企业的黑客攻击出现，神枪手（Sharpshooter）通过伪装成招聘机构向目标人物发送寻求英语应聘者的电子邮件传播。**三是工业领域 USB 恶意软件风险严重程度超过预期**。霍尼韦尔在其针对炼油厂、化工长、纸浆厂及造纸厂等 50 个工业站点扫描结果显示，近一半（44%）USB 设备存在恶意软件，其中 9%被设计为直接利用 USB 协议或接口漏洞，使 USB 传输更加有效，特别是在较旧或配置较差计算机上；2%与常见的人机接口设备（HID）攻击有关，使 USB 主机控制器误认为存在键盘连接，允许恶意软件键入命令并操纵应用程序。USB 威胁对于工业运营商而言真实存在，工业控制环境中 USB 安全使用环境堪忧。**四是专门针对工业控制系统的恶意攻击与日俱增**。鉴于工控网络的相对封闭性，目前针对工控系统的攻击以恶意软件为载体，以病毒、木马等恶意

程序为主，恶意程序通过自我复制、主动探测、自动传播等方式，在工业网络内扩散传播，对工业企业安全生产构成极大威胁。1 月，一个名为 Hide'N Seek（HNS）的新僵尸网络在世界各地不断增长，受感染的物联网设备数量达 2 万。12 月，全球最大水下工程和建筑企业之一意大利萨伊佩姆钻探公司声明，其在印度和中东地区等地的计算机设备遭到“沙蒙”（Shamoon）病毒变体攻击，致使数百台服务器和电脑瘫痪。

**（五）我国工业信息安全政策体系框架基本形成，安全标准覆盖范围不断扩大**

2016 年以来，为贯彻《国务院关于深化制造业与互联网融合发展的指导意见》《深化“互联网+先进制造业”发展工业互联网的指导意见》等文件，在国家层面，工业和信息化部先后发布了《工业控制系统信息安全防护指南》《工业控制系统信息安全事件应急管理工作指南》《工业控制系统信息安全防护能力评估工作管理办法》《工业控制系统信息安全行动计划（2018-2020 年）》等政策文件，初步形成了集工业信息安全防护、评估、应急等为一体的顶层指导体系框架。在地方层面，有省市着手建立本地区的的防护策略体系。例如，上海市经信委于 2018 年 4 月印发《上海市工业控制系统信息安全行动计划（2018-2020）》，以提升工业互联网安全防护能力，促进上海市工业信息安全产业发展，全力支撑和服务于打响“上海

制造”品牌。

**多项工业信息安全领域相关标准出台。**2018 年，国家市场监督管理总局和中国国家标准化管理委员会发布《信息安全技术 工业控制系统安全管理基本要求》（GB/T 36323-2018）、《信息安全技术 工业控制系统信息安全分级规范》（GB/T 36324-2018）、《信息安全 技术工业控制系统风险评估实施指南》（GB/T 36466-2018）三项国家标准。GB/T 36323-2018 对包括安全控制措施、安全评估和授权、系统和服务获取、人员安全、风险评估、应急规划、物理和环境安全等在内的 17 项工业控制系统安全管理基本措施进行规定，界定了工业控制系统安全管理基本框架和关键活动，为实现对工业控制系统适度、有效的安全管理控制提供遵循。GB/T 36324-2018 明确了工业控制系统安全等级划分模型、安全定级要素和安全定级方法，确定工业控制系统资产重要程度、受侵害后的潜在影响程度、需抵御的信息安全威胁程度，为加强工业控制系统安全管理提供了依据。GB/T 36466-2018 规定了工业控制系统风险评估实施方法和过程，适用于指导第三方安全检测评估机构对工业控制系统的风险评估，也可供工业控制系统业主单位进行自评估时执行。

**（六）我国工业信息安全防护体系建设稳步推进，安全防护能力明显提升**

**工控安全防护体系有序建设。**《工业控制系统信息安全行动计

划（2018-2020）》对工业控制系统信息安全方面未来 3 年重点工作提出要求，特别明确了建立多级联防联动的工控安全工作机制，打造“一网一库三平台”（国家在线监测网络，应急资源库，仿真测试、信息共享、信息通报平台）的技术保障体系和监管机制。2018 年，国家级“一网一库三平台”建设和各地技术分平台建设有序推进，态势感知、安全防护、应急处置能力得到提升。工业和信息化部推动建设工业控制系统信息安全应急资源库。国家级工业控制应急指挥通信系统建设完成，实现对工控安全动态、风险、事件信息汇聚和预处理，及时发布预警信息，支撑工业信息安全日常信息报送与通报工作。工业信息安全检查有序进行，针对平台企业、工业企业、工业 APP 和联网设备安全进行检查评估，督促企业加强自身安全防护，健全“以查促建、以查促改、以查促防”的工作机制。

**工业互联网安全保障体系建设稳步推进**。目前已初步形成以健全制度机制、建设技术手段、促进产业发展、强化人才培育四大领域为基本内容的体系架构。国家、地方、企业三级协同的安全技术保障体系也正在加快构建。工业互联网创新发展工程项目（安全方向）建设有序进行（表 5），支持企事业单位开展综合保障、监测和态势感知、应急协作指挥、数据安全防护、测试验证环境等建设，部分项目已初见成效。工业互联网安全监测平台初步具备工业互联网安全风险监测发现、预警通知、处置支撑能力。

表 5　2018 年支持的工业互联网创新发展工程项目（安全方向）

| 重点任务 | 序号 | 项目名称 | 牵头单位 |
|---|---|---|---|
| 工业互联网安全技术保障体系建设 | 1 | 面向电子行业工业互联网企业级集中化安全监测平台建设 | 中国电子信息产业集团有限公司第六研究所 |
| | 2 | 航空工业工业互联网安全监测平台 | 金航数码科技有限责任公司 |
| | 3 | 典型行业工业网企业级集中化安全监测平台建设 | 上海工业自动化仪表研究院有限公司 |
| | 4 | 典型行业工业互联网企业级集中化安全监测平台建设（电子行业） | 珠海格力电器股份有限公司 |
| | 5 | 昆钢工业互联网企业级集中化安全监测平台建设 | 昆明钢铁控股有限公司 |
| | 6 | 工业信息安全综合保障系统建设 | 国家工业信息安全发展研究中心 |
| | 7 | 国家级工业互联网安全监测与态势感知平台建设 | 中国信息通信研究院 |
| | 8 | 工业互联网安全监测与态势感知技术手段建设 | 国家工业信息安全发展研究中心 |
| | 9 | 面向关键信息基础设施的工业互联网安全监测与态势感知系统 | 北京天融信网络安全技术有限公司 |
| | 10 | 河南省工业互联网安全监测与态势感知技术手段建设 | 河南省信息咨询设计研究有限公司 |
| | 11 | 湖南省级工业互联网安全监测与态势感知管理平台 | 创发科技有限责任公司 |
| | 12 | 广东省工业互联网安全监测与态势感知技术手段建设 | 广州泰尔智信科技有限公司 |
| | 13 | 工业互联网数据安全防护监测平台建设 | 国家工业信息安全发展研究中心 |
| | 14 | 工业互联网数据流动监测平台建设 | 国家计算机网络与信息安全管理中心 |
| | 15 | 工业互联网数据安全防护及评估技术研究与能力建设 | 中国电子技术标准化研究院 |

| 重点任务 | 序号 | 项目名称 | 牵头单位 |
|---|---|---|---|
| | 16 | 工业互联网威胁信息共享与突发事件应急协作指挥平台建设与应用 | 中国信息通信研究院 |
| 工业互联网安全评估测试与试验验证环境建设 | 17 | 工业互联网安全标准体系与试验验证环境建设 | 机械工业仪器仪表综合技术经济研究所 |
| | 18 | 工业互联网安全核心标准研制与重点行业试验验证环境建设及应用推广 | 中国信息通信研究院 |
| | 19 | 工业控制系统内建安全核心技术能力提升及应用 | 浙江中控技术股份有限公司 |
| | 20 | 面向船舶行业的工业控制系统主动安全防护技术集成与推广 | 中国船舶重工集团公司第七二二研究所 |
| | 21 | 船舶行业内置信息安全功能工业控制设备推广应用 | 中国船舶重工集团公司第七一六研究所 |
| | 22 | 工业互联网安全攻防测试环境联合管控能力建设 | 国家工业信息安全发展研究中心 |
| | 23 | 面向重点行业的工业互联网攻防管控平台建设 | 上海华东电信研究院 |
| 工业互联网安全共性服务能力建设与推广应用 | 24 | 新兴领域中小企业工业互联网安全公共服务能力建设 | 北京奇安信科技有限公司 |
| | 25 | 基于 SaaS 模式的中小企业工业互联网安全预警监测防御服务能力建设项目 | 恒安嘉新（北京）科技股份公司 |
| | 26 | 工业互联网安全服务平台建设及运营项目 | 工业互联网创新中心（上海）有限公司 |
| | 27 | 面向智能装备的工业互联网安全技术典型应用推广 | 上海振华重工（集团）股份有限公司 |
| | 28 | 面向电子行业安全技术典型应用推广项目 | 南京中电熊猫平板显示科技有限公司 |

资料来源：工业和信息化部

### （七）我国工业互联网安全风险尤为突出，平台和设备成为主要攻击目标

**工业互联网平台安全防护处于初级阶段。**我国工业互联网仍处于发展初期，技术尚未成熟，大规模成熟应用尚需时日，安全防护体系还需进一步完善。截至 2018 年 12 月，我国有一定行业区域影响力的区域平台超过 50 家，工业设备连接数量超过 10 万台（套），既包括航天科工、中船工业、三一重工、海尔、美的、富士康等制造行业龙头企业建设的大规模平台，也包括一些新兴较小规模平台。但目前我国企业推出的工业互联网平台仍难以与通用电气、西门子为代表的跨国寡头相抗衡，国外平台在我国的大规模部署直接加剧安全可控风险。工业互联网平台作为工业互联网的核心，一旦受到木马病毒感染、拒绝服务攻击、有组织针对性的网络攻击等，将严重危害生产稳定运行，甚至导致生产事故，威胁人身和国家安全。

**工业互联网平台和联网设备成为网络攻击主要目标。**工业互联网安全包含设备、控制、网络、平台、数据安全等方面，安全防护流程复杂，防护难度大。2018 年，境内工业互联网平台联网设备频繁遭受扫描探测和恶意程序监测，重要敏感数据时有泄露。存在漏洞的联网设备和平台比例较高，且大部分都是中高危漏洞。工业和信息化部开展 2018 年度针对国内工业互联网平台的安全检查，对我国重点行业、重点领域工业互联网平台、企业、应用等安全现状情

况进行摸底调查。结果显示，仅针对 20 个相关机构的排查就发现超过 2000 处安全风险点，平台面临的安全风险突出，弱口令、权限绕过、远程命令执行、信息泄露、模块安全等安全漏洞较为普遍。

**（八）我国工业信息安全产业潜力巨大，投融资总量大幅提升**

**工业信息安全产业规模大幅增长。**近两年，我国网络安全产业工业信息细分领域呈现多样化发展趋势，工控安全、工业互联网安全、物联网安全、车联网安全、云安全、数据库安全等细分领域的新兴安全技术开始落地。随着工业互联网发展提速、工业信息安全成为国家安全体系有机组成，我国工业信息安全产业发展进入快速增长期。国家工业信息安全发展研究中心统计与调研结果显示，2018 年我国工业信息安全市场规模达到 8.42 亿元，与 2017 年的 5.57 亿元相比，年增长率超过 50%。从产业总量和市场情况看，工业信息安全目前虽产业规模较小，成熟的商业市场还未形成，但已成为安全厂商重点关注及投入研究的新兴领域，涌现出中安工控、长扬科技、威努特、天地和兴、安点科技、安恒信息、力控华康、启明星辰等一批专注于工业信息安全的企业。

**工业信息安全大规模投融资开始出现。**2018 年我国网络安全领域融资额高达 60 亿元人民币，同比增长率约为 71%。从投资并购情况看（表 6），工业信息安全领域企业威努特、博智软件、天地和兴、长阳科技等大规模投资并购事件开始涌现，国内排名领先的工控安

全厂商威努特获超亿元 C 轮人民币投资，天地和兴完成超亿元 B 轮融资用于工控安全人才培养储备、产品研发及市场推广等，长扬科技完成数千万 A 轮融资推动人才队伍组建及市场拓展等。目前，我国工业信息安全政策和需求两方面关键驱动力量巨大，国内工业信息安全厂商看好工业信息安全市场巨大潜力，加快产业布局。

**表 6　2018 年我国网络安全企业融资并购情况**

| 公司名称 | 阶段 | 日期 | 万元 | 领域 |
|---|---|---|---|---|
| 白山云科技 | C | 2018.01 | 33000 | 业务安全 |
| 芯盾时代 | B+ | 2018.01 | 12000 | 身份安全 |
| 安赛科技 | A | 2018.01 | 10000 | 下一代 IDS |
| 顶象技术 | 二轮 | 2018.02 | 亿级 | 在线业务安全 |
| 青藤云安全 | B | 2018.02 | 20000 | 云主机防护 |
| 瀚思科技 | B+ | 2018.03 | 千万级 | 大数据安全 |
| 威努特 | C | 2018.03 | 10000 | 工控安全 |
| 安百科技 | A | 2018.03 | 6000 | 应用安全 |
| 信安世纪 | 二轮 | 2018.03 | 5209.68 | 身份认证 |
| 恒安嘉新 | D | 2018.04 | 3986.7 | 移动安全/流量分析 |
| 华顺信安 | 二轮 | 2018.04 | 千万级 | 网络空间测绘 |
| 观安信息 | B | 2018.04 | 13000 | 大数据安全 |
| 天际友盟 | A | 2018.04 | 千万级 | 威胁情报 |
| 博智软件 | B+ | 2018.05 | 4000 | 工控安全 |
| 江民网安 | 天使 | 2018.05 | 1000 | 端点安全 |
| 威胁猎人 | 天使 | 2018.05 | 2500 | 在线业务安全 |
| 派盾 | 天使 | 2018.05 | 2000 | 区块链安全 |
| 深信服 | IPO | 2018.05 | 120000 | 网络安全、云安全 |
| 白山云科技 | C+ | 2018.06 | 240000 | 云 WAF |
| 中安威士 | A+ | 2018.06 | 1000 | 数据库安全 |

| 公司名称 | 阶段 | 日期 | 万元 | 领域 |
|---|---|---|---|---|
| 中安威士 | B | 2018.06 | 2000 | 数据库安全 |
| 杰思安全 | 战投 | 2018.06 | 2000 | 端点安全 |
| 天地和兴 | B | 2018.07 | 8000 | 工控安全 |
| 丁牛科技 | 天使 | 2018.07 | 千万级 | 漏洞检测 |
| 中睿天下 | A+ | 2018.07 | 8000 | 攻击溯源 |
| 长亭科技 | B | 2018.07 | 亿级 | 应用安全 |
| 安华金和 | C1 | 2018.08 | 大千万级 | 数据库安全 |
| 上元信安 | A+ | 2018.08 | 千万级 | 云 WAF |
| 几维安全 | Pre-A+ | 2018.08 | 千万级 | 代码安全 |
| 云屏科技 | 天使 | 2018.08 | 2000 | 数据安全 |
| 壹进制 | 被购 | 2018.08 | 27000 | 容灾备份/数据安全 |
| 墨云科技 | A | 2018.08 | 千万级 | 黑客攻防模拟 |
| 青莲云 | A | 2018.08 | 2000 | 物联网安全 |
| 红芯 | C | 2018.08 | 25000 | 安全浏览器 |
| 赛宁网安 | A | 2018.09 | 千万级 | 攻防平台 |
| 椒图科技 | A | 2018.09 | 8000 | 主机加固 |
| 威胁猎人 | Pre-A | 2018.09 | 600 | 在线业务安全 |
| 美创科技 | C | 2018.09 | 近亿级 | 数据库安全 |
| 数蓬科技 | Pre-A | 2018.09 | 3500 | 自适应可信平台 |
| 云杉网络 | B+ | 2018.09 | 1100 | 流量分析 |
| 光通天下 | B | 2018.10 | 10000 | 抗 D |
| 长扬科技 | A | 2018.10 | 千万级 | 工业互联网安全 |
| 指掌易 | B | 2018.10 | 20000 | 移动安全 |
| 易安联 | A | 2018.10 | 千万级 | 云安全 |
| 极御云安全 | A | 2018.11 | 14000 | 云安全 |
| 中安威士 | B+ | 2018.11 | 6000 | 数据库安全 |
| 杰思安全 | A+ | 2018.11 | 千万级 | 端点安全 |
| 360 企业安全 | Pre-B | 2018.11 | 125000 | 全安全行业 |
| 爱加密 | - | 2018.12 | 3000 | 移动应用加固 |

| 公司名称 | 阶段 | 日期 | 万元 | 领域 |
| --- | --- | --- | --- | --- |
| 威胁猎人 | Pre-A+ | 2018.12 | 3000 | 在线业务安全 |

资料来源：安全牛

## 二、问题挑战

### （一）工业信息安全具有独特的更高标准的安全防护需求

与传统网络安全内容相比较，工业信息安全具有十分鲜明的特性。工业信息安全涵盖工业运行全过程，不仅涉及传统计算机网络信息系统安全，还涉及工业软硬件设备、控制系统、工业协议、生产数据等的安全。工业信息安全的保障对象是各种各样的工业生产系统、工业软硬件、工业设备等，工业控制系统与互联网是异构的，这就要求加强跨界融合。工业设备的设计重点在于高效率完成生产动作，数据采集、存储、传输、分析能力无法与商用计算设备比拟，不能使用安全可靠性高但计算资源消耗大的复杂加密算法、防护软件等产品。工业信息安全面临的场景更复杂，生产环境软硬件种类与技术手段繁多，协议通用性低，而且更加强调生产或运行过程的可靠性、连续性、实时性要求。

此外，工业信息系统一旦发生安全问题，其修复难度更大。工业设备和系统通常依照生产需求进行定制，供应体系较为封闭，出现问题需要特定设备提供商、系统集成商等进行安全维护，无法像处理传统网络安全问题一样高频次地进行漏洞修复，威胁容易集聚。可见，工业信息安全更加关注持续的可操作性、稳定的系统性能、

数据的安全保密和全生命周期的安全支持。这些都是区别于传统的互联网安全保障体系的，因此，需要针对其特性建立起专门的工业信息安全技术防护体系。

**（二）软硬件依赖国外技术产品的状况加剧工业信息安全风险**

目前，我国工业软硬件自主研发实力不足，在高端装备、工业控制系统、工业网络和软件领域的技术产业实力难以满足安全防护需求，工业控制系统及工业软硬件依赖国外技术产品。工业控制系统方面，工控 MCU、DSP、FPGA 等核心元器件技术与国外差距较大，SCADA、PLC、DCS、PCS 等系统国外产品占领大部分国内市场。PLC 绝大部分是法国施耐德、德国西门子等品牌，DCS 的首选品牌则包括瑞典 ABB、美国罗克韦尔等传统品牌。工业软硬件方面，超高精度机床主要来自日本、德国和瑞士。国外厂商凭借其全球品牌影响力，进入中国市场较早，已经形成持续性的产品服务生态和利益链，具备较强的市场竞争优势。例如，在城市地铁领域，通信和机电系统中的工业交换机、传感器等主要工业控制设备以及网络系统中的核心交换机一般都采用国外产品。依赖国外工控和网络产品会面临不可预知的安全隐患，进一步加剧了我国工业信息安全风险。

**（三）国内厂商安全服务能力难以满足现实需求**

目前，我国专注于工业信息安全领域的厂商普遍规模较小，布

局工业信息安全业务的传统信息安全厂商、自动化厂商和 IT 系统集成商进入市场的时间多数不足五年，缺乏工业信息安全龙头企业、行业集中度不高，产业规模尚小，产品竞争力不强。根据全球网络安全产业分布图，目前全球前 100 的安全供应商中没有中国厂商，前 500 名中仅有 9 家入围（表 7、表 8），我国工业信息安全领域的安全技术和产品主要依赖于国外厂商，尚未形成完整的安全服务产业生态体系。非自主产品具有封闭性强、操作复杂、技术资料短缺、持续升级维护能力差等特点，国内用户很难组织二次开发或者自主生产。

**表 7　全球排名前 10 位的网络安全企业**

| 序号 | 企业名称 | 国家 |
|---|---|---|
| 1 | Herjavec Group | 加拿大 |
| 2 | KnowBe4 | 美国 |
| 3 | CyberArk | 以色列 |
| 4 | Raytheon Cyber | 美国 |
| 5 | Cisco | 美国 |
| 6 | IBM Security | 美国 |
| 7 | Microsoft | 美国 |
| 8 | Amazon Web Services | 美国 |
| 9 | FireEye | 美国 |
| 10 | Lockheed Martin | 美国 |

资料来源：全球网络安全产业分布图

**表 8　进入全球排名前 500 位的中国网络安全企业**

| 排名 | 企业名称 |
|---|---|
| 104 | 安天实验室 |

| | |
|---|---|
| 186 | 奇虎 360 |
| 223 | 安恒信息 |
| 345 | 山石网科 |
| 348 | 耐誉斯凯 |
| 409 | 翰思 |
| 489 | 绿盟科技 |
| 499 | 深信服 |
| 500 | 微步在线 |

资料来源：全球网络安全产业分布图

近几年，一批国内厂商致力于工业控制系统安全产品和服务发展，提出了一些工控安全解决方案（表 9）。例如，绿盟科技工控安全威胁防御整体解决方案 NGTP、三零卫士提高攻击早期预警响应能力的“固隔监”、中科网威的“时空防御模型”、威努特的“工控主机卫士”等。但是，赛门铁克、迈克菲、思科以及传统工控厂商罗克韦尔、通用电气在工业控制系统的安全产品和服务提供方面处于大幅领先地位，在有限时间内，国内初具规模的安全企业与国外行业巨头无法抗衡。

**表 9　我国主要工控安全企业及产品**

| 企业名称 | 工控安全产品 |
|---|---|
| 威努特 | 防火墙、主机卫士、监测审计平台、漏洞挖掘平台、漏洞扫描平台、统一安全管理平台、工业互联网雷达、攻防演练平台、单向隔离网闸、安全隔离与信息交换系统、安全运维管理系统、入侵检测系统、主机安全加固系统、日志审计与分析系统、生产安全集中监测平台、安全配置核查系统、检查工具箱、网络威胁感知系统等 |
| 绿盟科技 | 抗拒绝服务系统、防火墙、入侵检测系统、安全网关、漏洞扫描系统、远程安全评估系统、安全审计系统等 |
| 三零卫士 | 防火墙、漏洞扫描系统、隔离网关、集中管理平台、安全监控系统、态势感知系统等 |
| 中科网威 | 防火墙、漏洞扫描系统、入侵检测系统、集中管理平台、安全 |

| 企业名称 | 工控安全产品 |
| --- | --- |
| | 隔离与单向导入系统等 |
| 安天实验室 | 威胁检测分析系统、终端防御系统、应急处置工具箱等 |
| 立思辰 | 安全监测审计、安全管理平台、防火墙、内外网隔离设备、数据库审计平台、安全监控系统、终端防护应用程序白名单系统等 |
| 启明星辰 | 防火墙、网络流秩序分析、审计系统、脆弱性扫描、工业互联网信息安全管理系统、工业网闸、安全检查工具箱等 |
| 安恒信息 | 安全监测审计平台、防火墙等 |
| 安点科技 | 工业网闸、防火墙、主机安全防护系统、工业远动网关、网络威胁感知系统、安全审计系统、漏洞扫描系统、安全检查工具集、对战平台等 |
| 天地和兴 | 主机安全防护系统、防火墙、安全隔离与信息交换系统、威胁检测系统、入侵检测系统、安全审计平台、安全监管与分析平台等 |
| 力控华康 | 安全网关、防火墙、嵌入式工业通信网关等 |
| 圣博润 | 防火墙、安全隔离与信息导入系统、安全监测与审计系统、安全合规工具箱、终端安全卫士等 |
| 网藤科技 | 行为追溯系统、安全审计系统、USB 安全隔离装置、隔离网关、防火墙、预警系统等 |
| 长扬科技 | 防火墙、工业网闸、安全隔离与信息单向导入系统、主机卫士、工业监测审计系统、安全评估系统、统一安全管理平台等 |
| 木链科技 | 安全审计平台、防火墙、主机卫士、综合管理平台、攻防演练平台、威胁感知平台等 |
| 恒安嘉新 | 工业互联网安全态势感知平台、物联网安全监控平台、企业安全威胁感知系统、威胁情报分析平台、跨境数据通信与接入信息安全系统等 |
| 山石网科 | 防火墙、入侵检测和防御、漏洞扫描、威胁感知系统、安全审计平台、渗透测试等 |
| 东软 | 防火墙、安全网关、入侵检测系统、安全运维管理平台、统一身份管控系统、审计系统等 |
| 天融信 | 防火墙、安全隔离与单向导入系统、病毒过滤网关系统、安全隔离与信息交换系统、入侵防御系统、入侵检测系统、僵木蠕监测系统、异常流量管理与抗拒绝服务系统、网络审计系统、数据库审计系统、安全准入系统、主机监控与审计系统等 |
| 中睿天下 | 溯源系统、资产统一监管平台、智能安全运营中心等 |
| 蓝盾 | 防火墙、审计系统、主机卫士、统一安全管控平台等 |
| 迪普科技 | 防火墙、入侵防御系统、异常流量清洗系统、物联网应用安全控制系统、DPI 流量分析设备、漏洞扫描系统等 |

| 企业名称 | 工控安全产品 |
| --- | --- |
| 亚信安全 | IP 网络管理、综合监控、安全监测、终端管理、接入控制、APT 治理、安全网关、超级 DPI 等 |
| 新华三 | 防火墙、负载均衡产品、统一威胁管理、安全管理中心、入侵防御系统等 |
| 盛邦安全 | 漏洞评估系统、入侵检测系统、态势感知系统、应用防护系统、事件收集系统、云监测防御平台等 |
| 中新网安 | 抗拒绝服务系统、防火墙、漏洞扫描系统、威胁防御平台、审计系统等 |
| 深信服 | 安全感知平台、安全审计系统、安全网关等 |
| 锐捷网络 | 防火墙、安全网关、监控预警平台、统一安全认证与运维审计系统等 |
| 观安信息 | 应用安全防护、安全运维管理平台、车联网安全系统等 |

资料来源：国家工业信息安全发展研究中心整理

### （四）工业互联网平台安全策略构建相对滞后

我国工业互联网平台已从理论走向实践，工业互联网发展顶层架构已经具备，但工业互联网安全技术防护体系和安全管理体系尚未建立，相关政策文件和标准指南主要集中于工业控制系统安全领域，针对工业互联网平台安全接入、数据保护、平台防护等方面的标准尚属空白，平台分级分类管理体制和方法尚未统一，针对设备、网络、控制、应用和数据的防护措施尚未到位，对风险的识别、抵御和化解能力尚未形成，上线平台基本处于“裸奔”状态。

在工业企业自身防护能力普遍较弱的情况下，国家级管理体系和技术防护平台的重要性和优先级更为凸显。企业对工业互联网安全防护整体解决方案了解不足，对安全防护架构、措施、技术、产品最佳实践知之甚少，亟待依托国家级的防护平台、解决方案和最

佳实践，开展相关试点示范工作，推动工业互联网平台安全防护体系建设。

### （五）企业安全意识和主体责任感仍显薄弱

从现状看，工业企业对工业信息安全的重视程度仍有相当差距，往往管理主体更关注生产过程安全，存在重发展、轻安全的现象，对工业信息安全事故造成的灾难性、毁灭性后果估计不足。在信息安全领域投入的资金也很有限，尤其是实力薄弱的中小企业更是缺乏配套资金及人力部署安全措施，工业信息安全防护能力滞后于工业发展能力、工业信息安全防护意识不到位等问题比较突出。在企业内部管理方面，企业信息安全部门往往担心承担影响企业生产效率的责任，而未按规定设置相应级别的安全策略，导致安全管理制度和实际安全防护工作“两张皮”，没有真正发挥安全防护的职能作用。国家、地方及行业的工业信息安全监督责任、管理责任和主体责任虽有明确要求，但不少企业安全主体责任落实不到位。主要表现在，一方面，对恶意网络攻击行为可能造成的生产事故、损害或伤亡不了解；另一方面，工业信息安全事故发生时，责任认定、信息上报、应急处置等工作不成体系，往往造成难以挽回的灾难性后果。另外，有关部门对企业安全防护能力建设的督促和监督效果也不理想，安全职责不到位甚至缺位。

### （六）从业人员数量质量与现实需求矛盾突出

工业信息安全涉及计算机、自动化、通信、管理、经济、行为科学等多个学科，对工业生产自动化控制技术、计算机技术、网络与通信技术、信息安全防护技术有综合性要求。在学科建设上，目前国内高校只设立传统信息安全和网络安全学科，尚未设置关于工业信息安全领域的专门学科。从人才培养来看，由于至今距网络空间安全成为国家一级学科仅三年，网络安全专业人才数量尚无法满足行业需求。根据猎聘等机构联合发布人才研究报告，国内网络安全人才存在较大缺口，且高度集中在北京、广州、上海等一线城市，在安全需求分析和体系设计、安全态势分析以及战略法规制定方面的人才最为紧缺。而工业信息安全从业人员在数量和质量上与现实需求差距更大，服务支撑能力不足，相当一部分在企业端负责信息安全的管理人员是非专业出身，对工业控制系统的系统知识不甚了解，负责操作和维护工业控制系统的工程人员是其它相关专业转行，对工业信息安全掌握不系统不到位。大多数工业企业现有安全领域从业人员不具备分析和解决工业信息安全问题的能力，在专业性上亟待提高。

## 三、发展趋势

### （一）开放互联和技术进步是“双刃剑”，工业信息系统安全风险随之加剧

高德纳（Gartner）、美国技术工业协会（CompTIA）等多个机

构和组织均对包括工业设备在内的全球联网设备数量增长趋势保持乐观。卡巴斯基也认为未来一段时间越来越多的自动化系统和工业控制设备将连接互联网。由于越来越多的生产组件和服务直接或间接与互联网连接，攻击者从研发、生产、管理、服务等各环节都可能实现对工业系统的网络攻击和病毒传播，受攻击面和攻击路径将大大增多。加之 5G 商用步伐加快，与 4G 的 1Gbps 相比，其峰值数据速率高达 10Gbps。向 5G 的转变将催生新的运营模式、新架构以及难以避免的产生新漏洞，成为网络攻击的新目标。

另外，针对先前处于独立状态的工控设备的远程监控、远程控制、信息通信等技术和渠道不断出现并逐渐成熟，易接触性和易获得性也逐步提高，具备直接或远程访问工业自动化系统能力的组织、甚至个人的数量也将不断增加，这都扩大了网络罪犯计划和实施攻击的机会。同时，在传统网络攻击领域，针对传统受害者的网络攻击利润降低，而攻击风险增加，网络罪犯必然会寻找新的、性价比更高的新目标，将会更多地瞄准事关国家工业发展、涉及国计民生的公共系统和关键信息基础设施实施攻击。这些攻击威胁技术性更强，烈度更大，将以常态化的形式每时每刻危害着国家利益、经济建设、工业运行、以及公民隐私。当前，针对工业领域网络攻击数量的不断增加从侧面印证了网络罪犯对工业领域特别是新兴技术领域的兴趣不断增长，位于工业组织内的联网系统和设备正成为黑客

组织的更易选择的目标群体。

**（二）针对关键信息基础设施的预谋性攻击或增加，网络攻击军事化意味浓厚**

据统计，2018 年俄罗斯重要信息基础设施遭受网络攻击超过 43 亿次，仅在举办世界杯期间其关键信息基础设施和设备就受到超过 2500 多万次攻击。在 WannaCry 大规模爆发后一年，其仍然位居传播最广泛的加密恶意软件排行榜首位，与上一年度相比攻击次数仍保持增加态势。与攻击普通联网工控设备相比，针对关键信息基础设施的网络攻击后果更为严重。民间黑客组织也可利用军用级网络攻击武器进行攻击，如 WannaCry 病毒等，具备对联网重要设备和基础设施产生不可恢复的破坏能力，造成政府、企业、社会相关运行系统的瘫痪。

鉴于大部分关键信息基础设施在信息技术和生产系统之间缺少整体统一的安全防护策略，黑客团体或组织针对关键信息基础设施的干扰和破坏行为或增多。赛门铁克预计，未来一段时间内针对控制关键信息基础设施的物联网设备将出现越来越多新型、专门性攻击。美国网络安全厂商火眼预测，2019 年针对关键信息基础设施的威胁将有所上升，攻击者或许有意通过恶意行为干扰技术网络、扰乱商业行为或获取赎金，以政治为由发动攻击，甚至仅仅只是为了证实自身网络攻击实力。火眼同时预测在 2020 年前后针对东京奥运

基础设施的攻击或明显增加。在特定时期针对关键信息基础设施发起网络攻击，等同于直接扼住国家咽喉，有意造成国家功能和基本行动能力丧失，相当于变相宣战。随着网络发达国家网络空间攻防体系和综合实力的发展，以国家组织为背景的针对关键信息基础设施的高强度、精准式攻击很可能更趋常态，如果在敏感时间、关键节点、攻击了要害设施，触犯了对方国家的核心利益，不排除升级为网络战甚至演变成热战的可能。从这个意义上说，针对关键信息基础设施攻击行为带有相当浓厚的军事化意味。

**（三）新技术融合应用步伐加快，呼唤新的防护措施防护产品和服务模式**

从全球看，各类新技术在工业领域应用，以及融合应用的案例增多，将对工业信息安全防护带来更高标准、更复杂化的新要求。5G、人工智能等可预期的新技术在工业领域应用的趋势已经显现。例如，美国高通为专用工业物联网开发 5G NR 技术、意大利电信与工业技术公司 Robopac 合作致力于在圣马力诺共和国建立第一个 5G 智能工厂。从国内看，云计算、大数据与工业互联网融合应用步伐加快，互联网龙头企业在工业互联网领域加快布局。腾讯将工业互联网作为其战略重点之一；网易布局“产业数字化”，全年扶持 2000 余家企业；用友云打造工业互联网智能云平台，注册企业达 44 万家；浪潮工业互联网平台“1+N”战略发布，浪潮云广东节点正式落地；

华为通过云企业智能服务企业数字化转型。互联网行业巨头将工业互联网作为其战略重点，必将对工业信息安全投入更多力量。

工业信息安全厂商的动作也呼应了这一预测。例如，以色列工业物联网和工业控制系统安全公司 CyberX 宣布，将参与通用电气数字联盟项目；美国工业网络安全厂商 Dragos 和通用电气合作，以加强工业控制系统安全。现阶段的网络安全包括工业信息安全防护，往往是安全漏洞暴露后打补丁修复，但从网络安全龙头企业近期产品动向来看，未来网络安全服务理念有望呈现出从被动弥补向主动预防转变的趋势。12 月，赛门铁克推出面向工业控制系统安全的神经网络解决方案 ICSP Neural，该方案利用人工智能技术，对 USB 设备进行针对恶意软件的扫描检测，拦截潜在攻击威胁。未来工业信息安全防护理念和产品将呈现出化被动为主动的技术策略方向，漏洞发现、攻击利用和应急响应将成为攻防双方角力的主战场。

**（四）政策红利有待释放，工业信息安全产业市场处于爆发临界阶段**

2016 下半年来，随着相关政策、法规、指南、标准的密集推出，相信会对机械制造、航空、石化、煤矿、轨道交通等行业的工业信息安全建设和产业发展掀起一轮带动效应。《工业控制系统信息安全行动计划（2018-2020 年）》明确指出将培育龙头骨干企业、创建国家新型工业化产业示范基地（工业信息安全）作为主要任务。一

方面，传统工业企业生产业务需求逐渐将包含网络安全能力部署，必然将会在细分领域上出现新公司、产品及服务形态。另一方面，随着重点企业用户工控安全产品和服务口碑效应的形成，更多企业将在工控安全产品和服务的选择方面有更清晰的范围。以启明星辰为例，目前其推出的工控安全产品基本处于试用期，客户付费较低，随着产品正式进入收费期，客户付费将成倍增长。随着以其为代表的工控安全产品和服务提供商打造的工控安全用户案例成型推广，将有更多对工控安全概念尚不清晰的企业逐步使用安全产品、购买安全服务。

目前，启明星辰、绿盟科技、安控科技、北信源、华北工控等企业已全面布局工控安全产品和服务，威努特、天地和等工控领先企业获超亿元融资。同时，以腾讯、阿里为代表的互联网龙头企业纷纷将工业互联网作为未来重要发展战略，安全问题必然会成为其重要战略组成。未来随着各项国家法规政策的稳步推进，工业信息安全产业环境将持续优化，产业聚集效应将逐渐形成。因此，2019 年工业信息安全产业市场规模在多种力量驱动下有望实现数倍放大，预计 2018-2020 年将成为工控安全合规性需求持续爆发的阶段。

**（五）人才培训和意识宣贯需求猛增，有望成为工业信息安全行业重点**

网络安全本质是人与人的攻防对抗，安全防护效果与防护技术

体系和人工应急响应能力密切相关。与美国、日本、欧盟等在工业信息安全领域布局较早的国家或地区相比较，我国网络安全人才培养战略和工业信息安全防护工作起步较晚，整体水平存在一定差距。目前面临企业工业信息安全防护意识薄弱、专业人才紧缺的现实情况，工信部组织国家工业信息安全发展研究中心在 2017 和 2018 年度以《工业控制系统信息安全防护指南》和《工业控制系统信息安全行动计划（2018-2020 年）》为核心开展宣贯培训，覆盖全国 31 个省（市、自治区）多地工信主管部门和重点企业。未来一段时间，在顶层设计落实的不断推动下，省级宣贯培训工作的示范效应有望进一步显现，并逐步推动工业信息安全防护意识宣贯和人才需求下沉到市、县级。以企业为主体的针对工业信息安全领域专业型、技能型、复合型人才的多元化市场化培训有望增加，将会有越来越多资源投入到网络安全人才培养和专业团队建设中，工业信息安全意识宣贯和人才培养有望成为下一阶段行业重点。

各类工业信息安全竞赛将成为选拔优秀实战人才的途径之一。2018 年我国科研机构、企业、行业社团等举办多场各类工业信息安全竞赛，如工业信息安全技能大赛、“赛博地球杯”工业互联网安全竞赛、“护网杯”网络安全防护赛、工业互联网安全精英邀请赛等。竞赛成为网络安全人才发掘、培养、和储备重要途径。预期在未来一段时期，各类工业信息安全竞赛将继续开展，并呈现竞赛与

培训教育融合发展的趋势，对推动行业领域技术和经验共享、提升关键部门、重点企业以及关键信息基础设施相关单位的实战能力产生积极作用。

**（六）工业领域网络攻击与政治博弈相勾连，或催化网络空间国际规则制定**

从 2010 年“震网”到 2017 年 WannaCry，工业信息安全重大事件导致的连锁反应威胁性巨大，其潜在毁灭性、极端破坏性、深度威慑性对国家经济和社会的打击程度不可预期，越来越多国家和地区已充分了解工业信息安全事故可能直接导致现实威胁、社会动荡等严重后果，认识到工业信息安全防护的极端重要性。一方面，各国通过出台政策、制定标准、设立机构等举措进一步增强对关键信息基础设施安全防护力度；另一方面，各国不断加强网络空间战备建设，以提升网络攻防实力、形成网络威慑能力。

考虑到当前国际政治环境的复杂性，需高度警惕有组织有预谋的团体采取以发起工业信息安全重大事件这一高性价比手段来谋求某些政治或经济利益。卡巴斯基研究报告显示，许多国家特种服务以及其他组织团体或许以政治利益和经济利益为动机，积极参与到研究技术开发，以实施针对工业企业的间谍活动和恐怖主义袭击。目前，相当一部分国家处于工业控制系统的迅速普及以及向新型管理流程和生产模型以及经济活动模式过渡的重要时期，这种持续增

长的现实威胁或催化网络空间国际规则制定，以约束特种服务组织或团体行为，将针对工业领域网络安全威胁限制在可控程度，以保证各国工业及经济正常稳定发展。

# 参考文献


1. Fire Eye, “Facing Forward, Cyber Security in 2019 and Beyond”, 2018.
2. U.S. Department of Energy, “Multiyear Plan for Energy Sector Cybersecurity, 2018.
3. The White House, “National Cyber Strategy of the United States of America”, 2018.
4. Kaspersky Lab ICS-CERT, “Threat Landscape for Industrial Automation Systems, H1 2018”, 2018.
5. Kaspersky Lab ICS-CERT, “Threats posed by using RATs in ICS”, 2018.
6. 中国信息安全测评中心等，《2018 网络安全人才发展白皮书》，2018 年 9 月.
7. 国家能源局，《国家能源局关于加强电力行业网络安全工作的指导意见》，2018 年 9 月.
8. 肖建荣，《工业控制系统信息安全》，2015 年 9 月.
9. 姚羽、祝烈煌、武传坤.《工业控制网络安全技术与实践》，2018 年 11 月.

# 2019 年系列研究报告

| 报告编号 | 报告名称 | 发布时间 |
| --- | --- | --- |
| 2019-yp-01 | 2018 年度工业信息安全发展形势分析 | 2019 年 1 月 |
| 2019-yp-02 | 2018 年度数字经济发展形势分析 | 2019 年 1 月 |
| 2019-yp-03 | 2018 年度信息技术产业发展形势分析 | 2019 年 1 月 |



联系人：王丁冉　　15801304403