DOI 10.15302/J-SSCAE-2021.02.010

工业互联网安全公共服务能力提升路径研究

周昊，李俊，王冲华，尹丽波，赵千

（国家工业信息安全发展研究中心，北京 100040）

摘要：工业互联网安全公共服务作为工业互联网安全能力输出的重要表现形式，已成为保障工业互联网健康发展的有效手段之一。通过梳理工业互联网安全公共服务发展现状，本文阐述了工业互联网安全公共服务的重要性，剖析了工业互联网安全公共服务发展面临的挑战；围绕基础资源库建设、信息共享交流、态势感知能力、应急响应机制等提出了工业互联网安全公共服务基础能力提升的思路与建议，从信息技术应用创新的兼容性适配、安全服务能力组合编排、标准与评价机制等方面提出了工业互联网安全创新发展的提升路径。最后从智能化安全服务、服务集成化公共服务平台、新一代信息技术赋能等方面展望了工业互联网安全公共服务的发展前景，以期为新一代工业互联网安全的发展提供参考。

关键词：工业互联网安全；安全公共服务；网络安全；工业信息安全；创新发展

中图分类号：TP393　　**文献标识码：**A

Paths for Improving Public Service Capability Regarding Industrial Internet Security

Zhou Hao, Li Jun, Wang Chonghua, Yin Libo, Zhao Qian

(China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China)

Abstract: Industrial Internet security public service ensures the healthy development of the industrial Internet, as it is an important approach for outputting the industrial Internet security capability. In this article, we elaborate on the importance of industrial Internet security public service while analyzing its development status, and analyze the challenges faced by the development. The path for improving the basic capabilities of the industrial Internet security public service is proposed from the aspects of basic resource database construction, information sharing and exchange, situation awareness capability, and emergency response mechanism. Subsequently, the path for promoting the innovative development of the industrial Internet security is proposed in terms of the compatibility and adaptation of information technology application innovation, combination and arrangement of security service capabilities, as well as standards and evaluation mechanism. Finally, the development of the industrial Internet security public service is prospected from the aspects of intelligent security service, integrated public service platform, and new generation information technology.

Keywords: industrial Internet security; security-related public service; cybersecurity; industrial information security; innovative development

收稿日期：2021-01-13；**修回日期：**2021-02-24

通讯作者：王冲华，国家工业信息安全发展研究中心高级工程师，研究方向为工业互联网安全、网络与系统安全、网络攻防；E-mail: chonghuaw@live.com

资助项目：中国工程院咨询项目“新一代工业互联网安全技术发展战略研究”(2020-XZ-02)

本刊网址：www.engineering.org.cn/ch/journal/sscae

一、前言

工业互联网高度开放、全面互联的特性打破了原有工业控制系统相对封闭的格局，使工业互联网各层次对象暴露于互联网，信息技术（IT）与运营技术（OT）安全风险交织，安全形势颇为严峻 [1]。工业互联网安全作为国家安全的重要组成部分，应与工业互联网同步规划、同步设计、同步推进。我国工业互联网安全建设正处于起步阶段，安全服务能力相关工作的推进较为滞后，存在服务模式体系不够完善、安全技术能力水平较弱等问题，亟待提升整体安全服务能力。

为规范和指导工业互联网发展，我国陆续出台了《关于深化“互联网 + 先进制造业”发展工业互联网的指导意见》《加强工业互联网安全工作的指导意见》《工业互联网创新发展行动计划（2021—2023 年）》等多项政策文件，加快构建工业互联网安全保障体系。2018 年，我国发布了安全信息共享方面的首个国家标准《信息安全技术 网络安全威胁信息格式规范》（GB/T 36643—2018），通过统一、规范的网络安全威胁信息描述，使不同组织间安全信息可以共享与利用 [2]。在学术研究方面，相关研究总结了工业互联网安全的发展趋势和关键技术，给出了安全基本策略和具体防御措施 [3]；加强了对安全情报的搜集、抽取及推理等关键技术的研究与讨论 [4]；从可视、可知、可管、可控、可溯、可预警等方面提出了网络安全态势感知的实现路径 [5]；在网络安全应急方面，从安全监测、总体保障、人才队伍建设等方面给出了应对措施建议 [6]。

为探索我国工业互联网安全服务的发展情况，本文在总结工业互联网公共服务发展现状和梳理现阶段发展面临挑战的基础上，从基础能力和创新发展两个维度提出工业互联网安全公共服务能力提升路径，并对未来工业互联网安全公共服务的发展进行展望，以期为新一代工业互联网安全技术的发展提供参考。

二、工业互联网安全公共服务的重要性

（一）正确认识工业互联网安全公共服务

本文将工业互联网安全公共服务定义为：通过国家引导，充分发挥网络安全保障能力，由国家、地方、第三方机构或运营企业面向社会工业互联网用户（含联网工业企业、平台企业、标识解析企业）提供的与工业互联网安全能力相关的各类资源、技术服务的总称。工业互联网安全公共服务贯穿工业互联网安全准备阶段的事前、事中、事后等全流程，覆盖边缘侧的设备接入与安全管控，上层的工业软件运行安全防护，应用侧的漏洞扫描、流量监测、威胁情报、数据取证、泄密溯源、隐私保护等复杂的数据侧安全服务。典型的工业互联网网络安全公共服务包括工业互联网安全基础资源库服务、信息共享服务、态势感知服务、应急响应服务、安全众测服务、攻防演练服务等。

为构建工业互联网安全保障体系，我国多措并举，从政策引导、资金支持等方面全面提升工业互联网安全公共服务能力。自 2018 年起，工业和信息化部通过工业互联网创新发展工程、网络安全试点示范工程等，遴选了一批工业互联网安全平台和网络安全公共服务平台。这些平台基于大数据、云计算、人工智能（AI）、区块链等新一代信息技术，通过远程或在线服务等方式为社会各类单位或群体组织提供包括勒索病毒、木马蠕虫、安全漏洞、恶意攻击等安全威胁在内的实时监测与应急处置，同时利用线上与线下相结合的方式，开展威胁信息共享、数据安全防护、恶意代码检测等网络安全服务 [7]。

（二）公共服务是保障工业互联网安全的重要举措

网络公共服务在促进其他行业发展方面已显现出积极的推动作用。例如，在新型冠状病毒肺炎疫情期间，疫情防控物资紧缺；疫情大数据公共服务平台、国务院物资调度平台等公共服务平台建立起不同领域、不同行业和企业之间的桥梁和纽带，为常态化疫情防控下的复工复产顺利开展提供了支撑。我国的相关安全厂商在不同领域内深耕钻研，不断补填我国工业互联网安全公共服务的短板和弱项，开发了多个安全服务平台，如奇安信科技集团股份有限公司的工业互联网安全公共服务平台、中国电信集团有限公司的电信云堤、成都思维世纪科技有限责任公司的数据安全威胁情报平台等。

安全公共服务对提升工业互联网安全发展水平具有深远的促进意义。一方面，安全公共服务是工业互联网安全保障体系的重要组成部分，公共事业

性质突出，外溢效用和拉动作用明显，仅依靠商业机制很难获得显著提升；需要通过产业政策引导、标准制定实施、项目资金扶持等方式，有效整合市场中的各类安全资源，优化使用效率、提升资源共享程度，使安全产业与工业互联网产业形成良好的交互模式，从而提供更好的服务。另一方面，工业互联网安全公共服务可以助力安全生态形成良好的交互机制及市场模式，能够为工业互联网用户提供更加精准和高效的安全服务，帮助工业互联网企业建立有效的安全防护，减少中小企业的安全投入，降低遭受攻击的风险，提高工业互联网的整体安全能力，全面提升我国的工业互联网安全水平。

综上，鉴于工业互联网安全公共服务的重要性，需要围绕资源跨域共享、全链技术迭代、定制化按需服务、柔性动态重构等需求，进行全面体系化的技术创新；整合工业互联网安全漏洞、威胁信息、通用安全工具、标准规范、解决方案实践等信息资源共享能力，形成在线监测、恶意代码检测、主动加固防护等全流程服务能力；面向工业互联网用户提供安全公共服务，打通网络安全资源跨域共享的技术瓶颈，构建智能、开放的工业互联网安全公共服务体系，提升我国工业信息安全水平，保障工业系统稳定运行和人民群众正常生产生活，切实维护我国工业互联网的安全、可靠运行。

三、我国工业互联网安全公共服务面临的挑战

（一）工业互联网安全基础资源库挑战

工业互联网安全基础资源库主要包括工业资产类型知识、工业 / 网络协议指纹、漏洞、恶意代码样本、网络安全威胁情报、安全评估检查工具等工业互联网安全基础资源，为社会公众提供安全工具和各类资源库的共享，也为工业互联网企业提供资源共享和防护能力调用。2012 年以来，美国着手建设了覆盖轨道交通、能源电力、生产制造等关键领域基础设施的安全基础资源共享体系，已初步形成安全基础资源共享能力。目前，我国在安全漏洞资源库方面建设了国家信息安全漏洞共享平台（CNVD）、中国国家信息安全漏洞库（CNNVD）等国家级漏洞库以及包括补天漏洞库、绿盟科技安全漏洞库等在内的企业漏洞库；2019 年启动国家工业信息安全漏洞库（CICSVD）建设，收集汽车、航空、航天、石油化工等重点工业行业领域的相关漏洞和补丁。在威胁情报方面，2017 年中国科学院信息工程研究所牵头建设国家网络空间威胁情报共享开放平台（CNTIC），通过政府和企业合作共建的方式，加强威胁情报的整合利用；奇安信科技集团股份有限公司、北京微步在线科技有限公司等企业也建设了威胁情报库，为网络攻击追踪溯源、安全事件应急处置等业务提供威胁情报服务支撑。虽然我国工业互联网安全基础资源库建设正在逐步开展，但仍存在一些不足之处。

现有基础资源库在标识、描述、分类、危害等级等方面未统一标准，各个资源库对相同字段的描述方式未统一，不利于不同漏洞库间的数据同步与共享。例如，CNVD 将漏洞成因分为输入验证错误、访问验证错误等 10 个类型，CICSVD 则将漏洞成因分为代码注入、命令注入、跨站脚本等 10 个类型。

基础资源库建设不足，对外依赖程度偏高。目前，我国仅在漏洞库、威胁情报库方面建成了规模化的资源库，形成了以 CNVD、CNNVD、CICSVD、CNTIC 等为主的国家级资源库，但对通用漏洞披露（CVE）的依赖程度高，且主要漏洞信息多来源于美国国家通用漏洞数据库（NVD）、美国工控系统网络应急响应小组（ICS-CERT）等国外漏洞库。受国内漏洞挖掘能力水平、软硬件原理机理认识程度、漏洞上报奖励激励机制等影响，自主提交的漏洞数量较少，存在一定的漏洞资源库供应链安全风险。此外，我国工业互联网安全基础资源种类繁多、数量庞大、汇聚难度高，资产目录库、协议规则库、恶意代码病毒库、安全工具库等其他安全基础资源库也尚未形成国家级的资源平台。

（二）工业互联网安全信息共享挑战

多源异构的安全信息有效提取能力不足。安全信息具有多源、异构、冗余、繁杂等特性，包含各种类型的半结构化及非结构化数据，信息来源可能是网络流量、内外部威胁情报中心、专业机构、行业联盟，甚至是地下黑市等。目前，安全信息的提取已有一些半自动化搜集框架，多通过人工分析、提交、收录的方式进行，效率偏低，易受安全分析人员的能力水平影响；从海量安全数据中准确、高

效且无遗漏地提取高价值安全情报存在一定难度，缺少从开放网络信息中主动化、自动化提取和生成安全信息的能力。

各类资源库之间的关联性不足。各类资源库虽然存在结构化威胁信息表达式（STIX）、信息的可信自动化交换（TAXII）、网络可观察表达式（CybOX）等安全信息描述与共享标准，但现阶段漏洞库、威胁情报库、恶意代码病毒库等发展仍较为独立，导致漏洞、威胁情报、恶意代码等安全信息的离散性分布严重，缺少与协议、资产、依赖软件及解决方案等之间的关联融合分析，未能形成有效的关联知识图谱。即使是同类资源库，不同运营机构之间的关联和共享程度也不高。例如，由安全企业建设的安全漏洞库超过 10 种，但是各企业漏洞库之间并没有设计接口和关联属性信息，也没有统一的第三方共享平台来整合、汇聚漏洞信息，使得安全信息的综合使用率较低，“信息孤岛”现象严重。

安全信息的可信性和隐私保护不足。对安全信息的可信验证和有效的隐私保护是各信息共享方之间建立信任关系的前提，也是推进安全信息共享健康发展的基础。一方面，由于安全信息来源渠道不同及来源可靠程度不一，不同资源库中的安全信息存在相互冲突或虚假安全信息、误导性安全信息、安全信息内容有误等问题，降低了安全信息的可信度，难以充分发挥安全信息资源共享的整体价值。另一方面，在安全信息共享过程中，应注重隐私保护，对共享的安全信息进行匿名或脱敏处理；虽然已有数字水印、差分隐私保护等隐私保护技术，但由于部分企业安全意识不足或对共享方不信任等，致使一些企业对安全信息开放共享产生抵触心理。

（三）工业互联网安全态势感知挑战

近年来，我国工业互联网安全态势感知建设已取得初步进展，在传统互联网的解决方案之上，建立了国家工业互联网安全态势感知与风险预警平台；依托我国特有的国家、省级、企业三级架构，打造了“全国一盘棋”的网络安全全局态势感知平台，基本构建了覆盖安全威胁监测、通报、处置等环节的闭环处理机制。然而，在基于国家平台态势感知能力形成的工业互联网安全公共服务方面，仍然存在一些技术瓶颈。

工业互联网安全态势感知数据的获取难度大。工业互联网运行环境中的设备、交互协议种类繁多，常见的工业协议超过 100 种，加之存在大量无法识别的工业设备和私有协议，导致流量、日志、系统状态等感知数据较难获取。另外，采集获取的网络安全态势感知平台数据质量参差不齐，存在大量空值信息，数据有效性偏弱；不同工业设备、工业协议的数据类型和格式差异较大，处理难度大，需要针对不同的数据类型和格式进行针对性的开发，成本较高。

工业互联网安全态势感知数据的处理分析难。与传统网络安全态势感知相比，工业互联网安全态势感知在数据分析和决策处理方面难度更大，需要额外考虑多类型工业协议分析及多语义数据规格化等特性，从已有安全数据中有效分析出安全攻击事件或潜在的安全风险；需要以恶意行为代码库、威胁情报库等多类型、高精度的专业知识库为依托。受限于安全知识库短缺和对工业互联网安全攻击特征理解不足，现阶段尚未形成高效的安全分析能力。

（四）工业互联网安全应急响应挑战

工业互联网安全应急响应作为技术与管理结合的系统性工作，包括工业互联网安全应急响应流程的构建、安全事件处置、安全响应体系优化重构 3 个部分，最终形成工业互联网安全应急响应工作的闭环 [7]。在技术层面，工业互联网安全应急响应通过自动化或半自动化的方式对工业互联网安全事件进行检测、处置，确保发生安全事件后可以在短时间内恢复可用状态，尽可能避免和预防安全事件发生。现阶段，工业互联网安全应急响应在响应机制和管理机制方面仍存在一些挑战。

工业互联网安全应急响应系统或平台尚未形成规范化、自动化的应急响应预案。工业互联网安全应急响应过程涉及指挥、调度、决策、安全资源库等各方资源或平台，在指导或执行应急响应行为时，非规范化、非自动化的应急预案通常效率低下，受限于应急决策人员的技术能力水平和响应判断时间，影响了工业互联网安全应急响应的速度和效率，使工业互联网安全事件的应急响应处理时间延长。

我国工业互联网安全应急响应管理的各类主体合作不紧密。在发生工业互联网安全事件时，受网

络划分、地域归属、管理职责等因素影响，工业互联网安全应急响应各类主体合作零散，难以形成工业互联网安全应急联动机制。

四、工业互联网安全公共服务的基础能力提升路径

（一）完善工业互联网安全基础资源库建设

完善的工业互联网安全基础资源库应具备良好的扩展性和兼容性，拥有丰富、全面、有价值的安全数据及工具。为此，工业互联网安全基础资源库建设的提升路径应从以下几方面来开展。

采用政府授权或委托第三方机构授权的方式，建立健全工业互联网资产、工业 / 网络协议指纹、漏洞、恶意代码样本、网络安全威胁情报、安全评估检查工具等基础资源库；在持续加强对现有安全基础资源库建设的同时，补全缺失的安全基础资源库，不断扩充面向典型行业的工业互联网安全取证、风险评估、应急处置等工具集；在提交、上报、分享等方面实行激励机制，使工业互联网安全基础资源的储备量不断增加、丰富度不断提升。

强化工业互联网企业、安全企业、工业软件企业、安全研究机构与各类资源库建设、运营方的合作深度与广度，形成合作密切、各有优势、互为补充的良好局面；完善工业互联网安全基础资源库在收集、验证、发布和修复等方面的流程管理，对出现的重大安全事件能够及时预警与修复。

鼓励科研机构和安全企业加强工业互联网安全漏洞挖掘、恶意代码分析、软件逆向等关键技术攻关，提高对工业互联网安全软硬件、固件等基础要素的研究深度和广度；支持开展工业互联网安全众测，鼓励安全企业或个人主动提交“零日漏洞”。

（二）增强工业互联网安全信息共享交流

信息共享是连通、赋能工业互联网安全基础资源库的有效手段，是建设安全基础资源库后自然形成的需求。

明确并不断更新完善工业互联网安全信息共享的参与主体、共享范围、格式规范、接口标准、隐私保护等内容，整合政府、科研院所、高校、企业等在工业互联网漏洞挖掘、威胁情报、测评工具研发和协议分析等方面的资源和技术优势，逐步建立起内容较为完备、体系较为清晰、具有长期性和连续性的工业互联网安全信息共享机制。

在行业主管部门的统一管理和协调下，依托国家级、省级、行业级、企业级 4 个层级，分层次构建工业互联网安全信息共享平台，分领域、分行业、分地域汇聚安全信息，基于区块链、隐私计算、安全多方计算等方式保护共享信息的隐私性与可信性；研究制定安全信息共享数据、格式、协议等相关标准规范，通过标准化方式，实现工业互联网安全信息的互联、互通、共享。

（三）重点提升工业互联网安全态势获取、理解、预测能力

态势感知主要用于为安全人员提供数据分析结果和网络安全风险预警，辅助管理者做出安全战略决策。然而在态势获取、态势理解、态势预测等方面，亟需提升对多源异构数据的聚合、分析能力，改进态势预测模型，全面度量态势感知应用场景。

增强工业互联网安全态势获取能力。基于多种数据来源，获取和感知工业互联网环境中的各类安全信息；突破海量多源异构数据的融合汇聚技术，通过属性融合、相关性分析、图聚类等方式挖掘数据间的潜在关联，为下一步态势理解提供数据支撑。

提升工业互联网安全态势理解能力。以工业互联网安全数据为驱动，对网络流量数据、系统日志数据、威胁情报数据等安全数据进行进一步融合和分析，挖掘隐含在数据中的安全知识；建立全面的安全数据感知模型、算法模型、推理模型、检测模型，构建关联知识图谱与安全态势知识库，将机器数据转换为人类可读、可认知、可理解的安全态势数据。

提高工业互联网安全态势预测能力。基于安全数据，对工业互联网安全环境信息进行全面分析；结合安全基础资源库、安全知识库、大数据分析等，开展工业互联网安全事件的追踪溯源工作，复盘工业互联网安全事件的攻击路径，为工业互联网安全取证及反制提供依据。

（四）完善工业互联网安全应急响应体系

应急响应作为保障工业互联网安全可靠运行的

最后壁垒，是网络安全公共服务基础能力的重要体现，是确保工业互联网安全的有力支撑。

完善工业互联网安全应急响应机制，构建专业化、自动化、全面化的工业互联网安全事件应急响应预案体系。基于完善的工业互联网应急响应机制，实现各类资源调配的网络化和智能化，提升应急响应协调能力。

推进工业互联网安全应急响应技术手段建设。整合包括数据、平台和系统等在内的现有工业互联网安全应急响应资源，形成跨行业、跨部门、跨层级、跨地域的工业互联网安全应急响应能力；同步提升对工业信息安全漏洞库的收集、分析能力。

推动建立常态化工业互联网安全应急演练机制。以实战的方式提升工业互联网企业应急响应能力，丰富工业互联网安全从业人员的应急处置经验；研发应急响应能力评估模型和工具集，在实战过程中同步测试和完善，全面评估应急响应能力的有效性和充分性。

五、工业互联网安全公共服务的创新发展提升路径

（一）基于信息技术创新应用进行交叉性兼容适配，同步提升供应链创新水平

一方面，基于飞腾、鲲泰、鲲鹏等信息技术创新应用产品，开展工业互联网安全公共服务系统、平台的交叉性兼容适配，覆盖关键芯片、操作系统、数据库、核心软件等，形成组合运行、适配调优能力。另一方面，改善工业互联网安全技术创新发展环境，重点解决工业互联网安全关键产品、核心技术攻关等工业互联网供应链“命门”问题；集中国家优势力量和资源，加大核心电子器件、高端通用芯片、基础软件产品等研发投入力度，为工业互联网安全公共服务基础软硬件和供应链带来基础底层技术的变革，切实提升我国工业互联网安全公共服务创新发展能力。

（二）组合编排安全服务能力，形成创新发展的安全服务按需提供能力

工业互联网安全创新发展需要逐步具备自主研制关键芯片、操作系统、数据库、软件、网络设备的能力，从根本上摆脱对进口技术和产品的依赖。工业互联网安全公共服务需要摒弃堆砌加密机、防火墙、入侵检测、身份认证等“护城河”式安全产品的现状，积极探索主动化、智能化的安全服务技术；对已有的安全服务能力进行重新组合编排，重点突破行为分析、服务编排、自动化响应等关键安全技术，不断改善工业互联网安全服务机制，形成创新发展的安全服务按需提供能力。

（三）探索公共服务标准与评价机制，形成可持续发展产业链条

从工业互联网安全需求侧出发，研究提出工业互联网公共服务能力标准体系与评价体系。标准体系是评价体系建立的前提和依据，没有标准体系及相关标准的建立，评价体系的推进就会遭遇瓶颈。应在国家主管部门的引导下，建立能力范围广、服务能力强、流程规范的工业互联网安全公共服务标准体系，促进标准与评价的良性互动闭环，自上向下有序推进；探索建立工业互联网安全公共服务效果评价机制，从体系建设入手，落实关键实用标准和评价工作，避免无序发展。

六、结语

随着工业互联网与新一代信息技术的高度融合与快速发展，未来工业互联网安全公共服务将朝智能化、集成化、专业化方向发展。

基于 AI 的安全服务将得到高速发展。随着工业互联网数据量的爆发式增长、深度学习算法的优化改进、平台计算能力的大幅提升，工业互联网安全技术将呈现更高效、更精确、更智能的发展趋势。基于 AI 强大的自我学习和自我演进能力，构建全面智能化的工业互联网安全识别、检测、响应和恢复能力，辅以安全基础资源库进行关联性安全态势分析，推动安全防御体系向全面感知、智能协同方向发展，有效抵御不断演变的高级威胁。

安全技术集成化催生功能紧密耦合的公共服务平台。未来工业互联网安全公共服务平台将进一步整合安全信息与事件管理、用户行为分析和其他安全分析功能，成为紧密耦合、可扩展的安全运营和分析平台；服务形式也将由提供单一的安全功能服务朝着多种功能融合的集成化服务方向发展，威胁情报库、安全漏洞库、恶意代码病毒库等将被紧密

关联或整合形成统一的安全基础资源库。安全诊断评估、安全咨询、数据保护、代码检查、系统加固、云端防护等安全服务将以微服务或其他方式，通过工业互联网安全公共服务平台的形式统一对外提供服务。

新一代信息技术进一步赋能工业互联网安全公共服务，不断提升融合创新能力，增强工业互联网安全服务的专业化水平。随着工业互联网快速发展，第五代移动通信、云计算、大数据、区块链、可信计算等先进技术将在工业互联网安全中逐步应用与落地，推动形成面向工业互联网安全公共服务的专业化服务平台、综合性服务平台、共性技术平台；促进和引导工业互联网企业及用户在风险识别、威胁检测、安全加固、运营管理等流程中开展探索性应用，从而催生面向工业互联网安全公共服务的专业化咨询服务商、解决方案提供商。

参考文献

[1] 王冲华, 周昊. 工业互联网安全技术的思考 [EB/OL]. (2020-03-02) [2020-12-25]. https://mp.weixin.qq.com/s/5tvsJ_wdlJtnCf57tf-8DQQ.
Wang C H, Zhou H. Research on industrial Internet security technology. [EB/OL]. (2020-03-02) [2020-12-25]. https://mp.weixin.qq.com/s/5tvsJ_wdlJtnCf57tf8DQQ.

[2] 国家市场监督管理总局, 中国国家标准化管理委员会. 信息安全技术 网络安全威胁信息格式规范: GB/T 36643—2018 [S]. 2018.
State Administration for Market Regulation, Standardization Administration of the People's Republic of China. Information security technology—Cyber security threat information format: GB/T 36643—2018 [S]. 2018.

[3] 邢黎闻. 何积丰院士: 工业互联网安全发展趋势与关键技术 [J]. 信息化建设, 2016 (11): 38–40.
Xing L W. He Jifeng: Development trend and key technologies of industrial Internet security [J]. Information Construction, 2016 (11): 38–40.

[4] 董聪, 姜波, 卢志刚, 等. 面向网络空间安全情报的知识图谱综述 [J]. 信息安全学报, 2020, 5(5): 56–76.
Dong C, Jiang B, Lu Z G, et al. Knowledge graph for cyberspace security intelligence: A survey [J]. Journal of Information Security, 2020, 5(5): 56–76.

[5] 陶源, 黄涛, 张墨涵, 等. 网络安全态势感知关键技术研究及发展趋势分析 [J]. 信息网络安全, 2018 (8): 79–85.
Tao Y, Huang T, Zhang M H, et al. Research and development trend analysis of key technologies for cyberspace security situation awareness [J]. Netinfo Security, 2018 (8): 79–85.

[6] 于全, 杨丽凤, 高贵军, 等. 网络空间安全应急与应对 [J]. 中国工程科学, 2016, 18(6): 79–82.
Yu Q, Yang L F, Gao G J, et al. Emergency and response for cyberspace security [J]. Strategic Study of CAE, 2016, 18(6): 79–82.

[7] 国家工业信息安全发展研究中心, 工业信息安全产业发展联盟. 工业互联网平台安全白皮书（2020）[R]. 北京: 国家工业信息安全发展研究中心, 工业信息安全产业发展联盟, 2020.
China Industrial Control Systems Cyber Emergency Response Team, National Industrial Security Industry Alliance. White paper on industrial Internet platform security (2020) [R]. Beijing: China Industrial Control Systems Cyber Emergency Response Team, National Industrial Security Industry Alliance, 2020.