2022

工业控制网络安全态势白皮书

发布时间：2023年01月

东北大学 | 谛听网络安全团队

人工智能产业链联盟

星主： AI产业链盟主

知识星球

微信扫描预览星球详情

目录

1. 前言

关键信息基础设施是指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、国防科技工业等重要行业和领域的，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、公共利益的重要网络设施、信息系统等，对国家的稳定发展发挥着极端重要的作用。工业控制系统是关键信息基础设施的关键核心。随着制造强国、网络强国战略的持续推进，机械、航空、船舶、汽车、轻工、纺织、食品、电子等行业生产设备逐渐步入智能化阶段。与此同时，5G 技术、人工智能、云计算等新一代信息技术与制造技术的加速融合，使得工业控制系统正从封闭独立逐步走向开放互联。工业控制网络正与 IT 网络进行着深度融合，在促进工业进一步发展的同时，传统信息网络中的各种安全威胁已经逐步延伸至工业控制网络中。在党的二十大报告中，习近平总书记着重强调了：“要推进国家安全体系和能力现代化，坚决维护国家安全和社会稳定。”近年来，网络攻击、网络窃密等危及国家安全行为，给社会生产生活带来了不少安全隐患。如何有效保障网络与信息安全，是数字时代的重要课题。

2022 年 4 月，为贯彻落实 2022 年《政府工作报告》关于“加快发展工业互联网”的部署要求，扎实推进《工业互联网创新发展行动计划(2021-2023 年)》任务安排，工信部印发《工业互联网专项工作组 2022 年工作计划》。从夯实基础设施、深化融合应用、强化技术创新、完善要素保障等方面，提出了网络体系强基、标识解析增强、平台体系壮大等 15 大类任务 83 项具体举措。为顺应当前形势，东北大学“谛听”网络安全团队基于自身传统的安全研究优势开发设计并实现了“谛听”网络空间工控设备搜索引擎（http://www.ditecting.com），并根据“谛听”收集的各类安全数据，撰写并发布《2022 年工业控制网络安全态势白皮书》，读者可以通过报告了解 2022 年工控安全相关政策法规报告及典型工控安全事件分析，同时报告对工控系统漏洞、联网工控设备、工控蜜罐、威胁情报数据及工业互联网安全创新发展情况进行了阐释及分析，有助于全面了解工控系统安全现状，多方位感知工控系统安全态势，为研究工控安全相关人员提供参考。

2. 2022 年工控安全相关政策法规报告

随着互联网的快速发展，云计算等新型信息技术开始与传统工业进行融合，工业控制系统逐渐走向智能化。但与此同时，一些网络安全事件层出不穷，工业控制系统在信息安全方面受到了严峻挑战。因此，我国开始逐步完善工业信息安全政策标准，以便于提升工业信息安全保障技术，推动整个安全产业的发展。

通过梳理 2022 年度发布的相关政策法规报告，整理各大工业信息安全研究院及机构针对不同法规所发布的解读文件，现摘选部分重要内容并对其进行简要分析，以供读者进一步了解国家层面关于工控安全领域的政策导向。

2.1 《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》

2022 年 2 月 10 日，工信部再次公开征求对《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）的意见。此次发布的征求意见稿调整了数据定义、监管机构和核心数据目录备案等条款。在工业和信息化领域数据处理者责任方面，征求意见稿明确了其对数据处理活动负安全主体责任，对各类数据实行分级防护，保证数据持续处于有效保护和合法利用的状态。该征求意见稿增加了核心数据跨主体处理以及日志留存条款，要求需要跨主体提供、转移、委托处理核心数据时，应当评估安全风险，采取必要的安全保护措施，并经由地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报工业和信息化部。工业和信息化部严格按照有关规定对其进行审查。

2.2 《信息安全技术 工业控制系统信息安全防护能力成熟度模型》

2022 年 4 月 15 日，根据国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2022 年第 6 号），国家标准 GB/T 41400-2022《信息安全技术 工业控制系统信息安全防护能力成熟度模型》正式发布，并将于 2022 年 11 月进行正式实施。该标准由中国电子技术标准化研究院联合“产学研用测”41 家单位共同研制，意在贯彻落实《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》有关要求、进一步推动工业企业落实《工业控制系统信息安全防护指南》防护要点。

2.3 《电力可靠性管理办法（暂行）》

2022 年 4 月 25 日，国家发改委官网公布了《电力可靠性管理办法（暂行）》，并于 6 月 1 日起开始实施。《办法》第七章对电力网络安全做出了明确要求，其中提出了电力网络安全坚持积极防御和综合防范的方针；电力企业应当落实网络安全保护责任，健全网络安全组织体系；电力企业应当强化电力监控系统安全防护；电力用户应当根据国家有关规定和标准开展网络安全防护，预防网络安全事件，防止对公用电网造成影响；国家能源局依法依规履行电力行业网络安全监督管理职责等具体要求。

2.4 《电力行业网络安全管理办法（修订征求意见稿）》

2022 年 6 月 14 日，国家能源局对《电力行业网络与信息安全管理办法》（国能安全〔2014〕317 号，为加强电力行业网络安全监督管理以及规范电力行业网络安全工作，根据《中华人民共和国网络安全法》《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国计算机信息系统安全保护条例》《关键信息基础设施安全保护条例》及国家有关规定，制定本办法。）、《电力行业信息安全等级保护管理办法》（国能安全〔2014〕318 号，为规范电力行业网络安全等级保护管理，提高电力行业网络安全保障能力和水平，维护国家安全、社会稳定和公共利益，根据《中华人民共和国网络安全法》《中华人民共和国密码法》《中华人民共和国计算机信息系统安全保护条例》《关键信息基础设施安全保护条例》《信息安全等级保护管理办法》等法律法规和规范性文件，制定本办法。）进行修订，形成了《电力行业网络安全管理办法（修订征求意见稿）》《电力行业网络安全等级保护管理办法（修订征求意见稿）》，向社会公开征求意见。

2.5 《数据出境安全评估办法》

2022 年 7 月 7 日，国家互联网信息办公室公布了《数据出境安全评估办法》（以下简称《办法》），并于 2022 年 9 月 1 日起开始施行。出台《办法》是为了更好的落实《网络安全法》、《数据安全法》、《个人信息保护法》的规定，并且有利于保护个人信息的权益，社会公共的利益，规范数据出境的活动以及维护国家的安全。该《办法》

也规定了数据出境安全评估的范围、条件和程序，并具体指明数据出境安全评估工作的方法。

2.6 《关于开展网络安全服务认证工作的实施意见（征求意见稿）》

2022 年 7 月 21 日，市监总局发布《关于开展网络安全服务认证工作的实施意见（征求意见稿）》，公开征求意见至 8 月 21 日。应当依法设立从事网络安全服务认证活动的认证机构，保证其具备从事网络安全服务认证活动的专业能力，并严格经过市场监管总局征求中央网信办、公安部意见后批准取得资质。严格要求网络安全服务认证机构公开认证收费标准和认证证书有效、暂停、注销或者撤销等状态，按照有关规定报送网络安全服务认证实施情况及认证证书信息。

2.7 《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》

2022 年 9 月 14 日，国家互联网信息办公室会同相关部门起草了《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》，并向社会公开征求意见。意见反馈截止时间为 2022 年 9 月 29 日。自 2017 年《中华人民共和国网络安全法》开始实施后，其为维护网络空间主权和国家安全、社会公共利益，保护公民等合法权益，提供了有力法律保障。随着社会形势的发展，拟对《中华人民共和国网络安全法》进行修改，使其法律责任制度能够更加完善，能够更加有效的保障网络的安全。

2.8 《信息安全技术 关键信息基础设施安全保护要求》

2022 年 10 月 12 日，国家标准化管理委员会发布 2022 年第 14 号中华人民共和国国家标准公告，批准发布国家标准 GB/T 39204-2022《信息安全技术 关键信息基础设施安全保护要求》，《信息安全技术 关键信息基础设施安全保护要求》规定了关键信息基础设施运营者在识别分析、安全防护、检测评估等方面的安全要求。此次标准的发布，意味着我国的国家关键信息基础设施（电力，燃气，水力，石化等）工业控制系统的网络安全保护将纳入国家监督成为强制要求，标志着我国关键信息基础设施安全保障体系的建设进一步完善，为运营者开展关键信息基础设施的安全保护工作提供更有效的规范和引领。标准将于 2023 年 5 月 1 日开始实施。

2.9 《工业互联网 总体网络架构》

2022 年 10 月 14 日，国家标准化管理委员会发布 2022 年第 13 号中华人民共和国国家标准公告，批准发布国家标准 GB/T 42021-2022《工业互联网 总体网络架构》。《工业互联网 总体网络架构》是我国首个在工业互联网网络领域中发布的国家标准，其规范了工业互联网工厂内外网络架构的目标架构和功能要求，并且表明了工业互联网网络实施的框架以及对安全方面的要求，相关标准的规定有助于提升全行业全产业的数字化、网络化以及智能化水平，能够进一步促进相关产业向数字化转型。该标准将于 2023 年 5 月 1 日开始实施。

2.10 《网络产品安全漏洞收集平台备案管理办法》

2022 年 10 月 28 日，工业和信息化部近日印发《网络产品安全漏洞收集平台备案管理办法》。《办法》规定，将采取网上备案的形式进行，通过工业和信息化部网络安全威胁和漏洞信息共享平台对漏洞收集平台进行备案。相关参与者需在该共享平台上如实填报网络产品安全漏洞收集平台的备案登记信息。该《办法》将于 2023 年 1 月 1 日起施行。

2.11 《信息安全技术 网络安全服务能力要求》

2022 年 11 月 9 日，全国信息安全标准化技术委员会秘书处发布《信息安全技术 网络安全服务能力要求》（征求意见稿），并向社会公开征求意见，该意见征求截止时间为 12 月 9 日。该文件严格要求了网络安全服务机构所提供的安全服务应该具备的能力水平。该文件能够对网络安全服务机构开展网络安全服务能力建设进行有效指导，同时也可以帮助政务部门以及关键信息基础设施运营者选择合适的网络安全服务机构。

2.12 《信息安全技术 关键信息基础设施网络安全应急体系框架》

2022 年 11 月 17 日，全国信息安全标准化技术委员会秘书处发布《信息安全技术关键信息基础设施网络安全应急体系框架》（征求意见稿），并向社会征求意见，该意见征求截止时间为 2023 年 1 月 16 日。征求意见稿给出了关键信息基础设施网络安全应急体系框架，其中主要包括机构设立、分析识别以及事后恢复与总结等。该文件有助于关

键信息基础设施运营者建立健全网络安全应急体系、开展网络安全应急活动，同时可以为关键信息基础设施安全保护的其他相关方提供参考。

表 2-1 2022 年国内部分出台政策

序号	月份	出台政策
1	2 月	《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）
2	2 月	《工业和信息化部办公厅关于做好工业领域数据安全管理试点工作的通知》
3	2 月	《工业互联网安全标准体系》
4	4 月	《信息安全技术 工业控制系统信息安全防护能力成熟度模型》
5	4 月	《电力可靠性管理办法（暂行）》
6	6 月	《电力行业网络安全管理办法（修订征求意见稿）》
7	7 月	《数据出境安全评估办法》
8	7 月	《关于开展网络安全服务认证工作的实施意见（征求意见稿）》
9	7 月	《信息安全技术 信息安全管理体系 概述和词汇》
10	8 月	《公路水路关键信息基础设施安全保护管理办法（征求意见稿）》
11	9 月	《关于修改（中华人民共和国网络安全法）的决定（征求意见稿）》
12	10 月	《信息安全技术 关键信息基础设施安全保护要求》
13	10 月	《工业互联网 总体网络架构》
14	10 月	《数字化转型 价值效益参考模型》、《供应链数字化管理指南》、《生产设备运行管理规范》、《生产设备运行绩效评价指标集》
15	10 月	《网络产品安全漏洞收集平台备案管理办法》
16	11 月	《信息安全技术 网络安全服务能力要求》（征求意见稿）
17	11 月	《信息安全技术 关键信息基础设施网络安全应急体系框架》（征求意见稿）
18	12 月	《工业互联网企业网络安全 第 4 部分：数据防护要求》（征求意见稿）
19	12 月	《电力行业网络安全管理办法》
20	12 月	《电力行业网络安全等级保护管理办法》
21	12 月	《工业和信息化领域数据安全管理办法（试行）》

3. 2022 年典型工控安全事件分析

时至 2022，全球局势变化风云莫测，工控安全是国家安全保障、社会稳定运行的重要基石。工控网络的应用涉及了社会中的各个重要行业如通信、电力、燃油等。社会中的各个机构、组织、企业在疫情下稳步的复产复工，恢复工作秩序，离不开工控网络的安全。

以下介绍 2022 年发生的一些典型工控安全相关事件，通过以下事件可以了解工业控制网络环境下各种攻击的技术特性和趋势，以此来制定更加有效的相关策略应对未来可能遭受的攻击。

3.1 德国主要燃料储存供应商遭网络攻击

2022 年 1 月 29 日，德国的一家名为 Oiltanking GmbH Group 的石油储存公司遭到了网络攻击。本次攻击主要是针对 Oiltanking 公司以及矿物油贸易公司 Mabanaft，对其造成了一定的影响。Oiltanking 和 Mabanaft 在他们的联合声明中表示他们正在尽力解决该问题，并了解其波及的范围。同时由于受到本次攻击事件的影响，欧洲西北部地区馏分柴油的价格有略微的涨幅。

3.2 FBI 警报：美国关键基础设施正遭受 BLACKBYTE 勒索软件入侵

2022 年 2 月 11 日，美国联邦调查局和美国特勤局联合发布了《联合网络安全咨询公告》。公告中指出：名为 BlackByte 的软件勒索组织在过去的 3 个月期间，入侵了至少 3 个美国关键基础设施组织，尤其是政府设施、金融服务以及食品和农业领域。该组织会将其勒索软件基础设施出租给他人，以此来换取一定比例的勒索收益，该组织自 2021 年 7 月开始开发软件漏洞，全球范围内的企业都可能成为其目标。

3.3 白俄罗斯铁路遭到 ANONYMOU 入侵，所有网络服务中断

2022 年 2 月 27 日，黑客组织 Anonymou 声称已经入侵了白俄罗斯铁路的内部网络，并且攻击并关闭了其内部网络的所有服务。目前网站 pass.rw.by、portal.rw.by、rw.by 都处于无法访问的状态，该国的铁路系统被迫转入手动控制模式，这对白俄罗斯铁路列车

的正常运营以及铁路秩序都造成了极大的影响和破坏。Anonymou 组织还入侵了白俄罗斯的武器制造商 Tetraedr，并窃取了大约 200GB 的电子邮件。

3.4 东欧大型加油站遭勒索攻击，官网、APP 等全部下线

2022 年 3 月 6 日，东欧国家罗马尼亚的一家加油站遭到了勒索软件攻击，该加油站的 Fill&Go 服务以及官方网站都因本次攻击而被迫下线。本次攻击影响到了该公司的大部分业务，导致了官网、APP 都无法正常访问，顾客只能使用现金和刷卡进行支付。

这家公司名为 Rompetrol，是罗马尼亚国内最大的炼油厂 Petromidia Navodari 的配套加油站运营商。攻击者还入侵了 Petromdia 炼油厂内部的网络，但该网络的运营暂未发现受到了影响。

3.5 乌克兰的能源供应商成为 INDUSTROYER2 ICS 恶意软件的目标

2022 年 4 月 12 日，一种新的能够操控工业控制系统造成损害的恶意软件最近将乌克兰的一家能源供应商作为了攻击的目标。该攻击主要针对的是变电站，乌克兰的计算机应急响应小组、网络安全公司和微软公司已经对其进行了分析。经分析发现，该攻击行动与一个威胁组织 Sandworm 有关，该组织据信代表俄罗斯 GRU 军事情报机构运作。根据网络安全公司的说法，该攻击的目的可能是在目标能源设施中执行破坏性的操作进而导致停电，本次安全事件涉及了在 ICS 网络以及运行 Solaris 和 Linux 的系统中部署的几种恶意软件。

3.6 农业机械巨头爱科遭勒索攻击，美国种植季拖拉机供应受影响

2022 年 5 月 7 日，美国农业机械巨头爱科遭到了勒索软件的攻击，对部分生产设施的运营造成了影响，并且该影响可能会持续多天。本次事件中，爱科公司并没有提供任何关于业务中断的细节信息，为了阻止攻势蔓延该公司可能会关闭部分系统。有经销商表示，这导致拖拉机销售在美国最重要的种植季节停滞不前。近一年来已经有多家农业供应链企业遭到攻击，可见农业逐渐成为了勒索攻击的重点目标。同时受到紧张的国际政治局势的影响，部分网络攻击可能还具有报复性动机，目的是破坏美国关键基础设施企业的生产活动。

3.7 得克萨斯州一家液化天然气厂遭黑客攻击导致爆炸

2022 年 6 月 8 日，德克萨斯州一家液化天然气厂发生爆炸。爆炸发生在德克萨斯州金塔纳岛的自由港液化天然气液化厂（名为 Freeport LNG 公司）和出口码头。华盛顿时报一国家安全作家 Rogan 证实：德克萨斯州的液化天然气设施爆炸与 APT 组织进行的黑客活动一致。Freeport LNG 拥有运营技术以及工业控制系统网络检测系统，但否认了将网络攻击视为事件发生的根本原因。除非 Freeport LNG 适当部署了 OT/ICS 网络检测系统并完成了取证调查，否则不能排除网络攻击。此次爆炸事故将对自由港液化天然气的运营产生持久的影响。

3.8 伊朗 LYCAEUM APT 组织利用新的 DNS 后门攻击能源行业

2022 年 6 月 10 日，伊朗 Lycaeum APT 黑客组织使用新的基于.NET 的 DNS 后门，以对能源和电信行业的公司进行攻击。Lyceum 曾使用 DNS 隧道后门瞄准中东的通信服务提供商。Zscaler 最近的一项分析提出了一种新的 DNS 后门，该后门基于 DIG.net 开源工具可以执行“DNS 劫持”攻击、执行命令、丢弃更多有效负载并泄露数据。DNS 劫持是一种重定向攻击，它依赖于 DNS 查询操作，将尝试访问合法站点的用户带到威胁参与者控制下的服务器上托管的恶意克隆。

3.9 德国建材巨头 KNAUF 被 BLACK BASTA 勒索软件团伙袭击

2022 年 7 月 19 日消息，德国建材巨头 Knauf 集团表示它已成为网络攻击的目标，该攻击扰乱了其业务运营。据悉，网络攻击发生在 6 月 29 日晚上，目前，可耐夫仍在进行调查取证、事件处理和补救工作。虽然 Knauf 没有公布他们所遭受的网络攻击的类型，但根据恢复正常运营的时间、影响和难度可以推断这大概率是一起勒索软件事件。名为 Black Basta 的勒索软件团伙已经在其勒索网站上发布公告宣布对这次攻击负责，并于 7 月 16 日将 Knauf 列为受害者。勒索软件团伙目前已经泄露了 20%的被盗文件，超过 350 名访问者访问了这些文件。并非所有文件都已在线泄露的事实表明，威胁行为者仍有希望获得成功的谈判结果并获得赎金。

3.10 希腊天然气分销商 DESFA 部分基础设施遭受网络袭击

2022 年 8 月 20 日，希腊最大的天然气分销商 DESFA 表示在其部分基础设施上遭受了网络攻击，攻击者试图非法访问电子数据，并可能泄露了许多目录和文件。8 月 19 日，Ragnar Locker 勒索软件组织在其暗网数据泄露网站上泄露了 DESFA 的数据样本及被盗数据列表，这也证实了此次攻击。泄露的数据样本不包含机密信息。Ragnar Locker 在其暗网上表示，DESFA 的系统中存在多个安全漏洞，会导致公司的敏感数据受到损害。Ragnar Locker 已将此类漏洞通知了 DESFA，然而并没有收到回应。因此 Ragnar Locker 发布了从 DESFA 网络下载的数据列表，并威胁如果 DESFA 没有在规定时间内采取行动，也没有联系威胁行为者以解决安全问题，将发布文件列表中包含的所有文件。

3.11 黑客组织 GHOSTSEC 入侵以色列各地的 55 个 PLC

2022 年 9 月 12 日，巴勒斯坦的黑客组织 GhostSec 声称他们破坏了多达 55 个 Berghof 可编程逻辑控制器（PLC），这些 PLC 被以色列组织用作“Free Palestine”运动的一部分。GhostSec 于 2015 年首次被发现，自称治安组织，最初成立的目的是针对宣扬伊斯兰极端主义的 ISIS 网站。9 月 4 日，GhostSec 在其 Telegram 频道上分享了一段视频，展示了成功登录 PLC 管理面板的过程，此外还转储了被黑客入侵控制器的数据。同时，GhostSec 发布了更多的截图，声称已经获得了另一个控制面板的权限，可以用来改变水中的氯含量和 PH 值。工业网络安全公司 OTORIO 对此事进行了更深入的调查后表示，发生此次入侵的原因可能是因为 PLC 可以通过互联网访问，而且使用的是可以轻易猜到的凭证。

3.12 黑客组织 KILLNET 对美国机场网站发起分布式拒绝服务(DDOS)攻击

2022 年 10 月 10 日，亲俄黑客组织 KillNet 声称对美国几个主要机场的网站进行了大规模分布式拒绝服务(DDoS)攻击，导致其无法访问。DDoS 攻击通过垃圾请求使托管这些网站的服务器无法运作，使旅客无法连接并获取有关其定期航班或预订机场服务的更新。被攻击的机场包括芝加哥奥黑尔国际机场(ORD)、奥兰多国际机场(MCO)、丹佛国际机场(DIA)、凤凰城天港国际机场(PHX)，以及肯塔基州、密西西比州和夏威夷的一些机场。虽然 DDoS 攻击不会影响航班，但仍然对关键经济部门的运作产生了不利影响，

可能将会造成相关服务的暂缓甚至是瘫痪。KillNet 的创始人 KillMilk 还表示，他们正在计划进一步的攻击，涉及更严重的技术，包括旨在破坏数据的擦除器攻击。

3.13 网络攻击导致丹麦最大铁路公司火车全部停运

2022 年 11 月 5 日，由于遭受了网络攻击导致服务器关闭，丹麦最大的铁路运营公司 DSB 旗下所有列车均陷入停运，且连续数个小时未能恢复。遭受攻击的是丹麦公司 Supeo，该公司是一家专为铁路、交通基础设施和公共客运提供资产管理解决方案的外包供应商。Supeo 可能经受了一次勒索软件攻击，但该公司并未披露任何信息。Supeo 公司提供了一款移动应用，可供火车司机访问各项关键运营信息，例如限速指标和铁路运行信息。由于服务器关闭，导致该应用停止工作，司机们只能被迫停车，最终引发了列车运营中断事件。

3.14 乌克兰政府机构和国家铁路遭受新一波网络钓鱼攻击

2022 年 12 月 8 日，乌克兰计算机应急响应小组报道，乌克兰政府机构和国家铁路遭受网络钓鱼攻击。攻击者被响应小组追踪为 UAC-0140，他们使用电子邮件分发由 Delphi 编程语言开发的名为 DolphinCape 恶意软件。这种恶意软件可以采集被攻击电脑的信息，包括主机名、用户名、比特率和操作系统版本等等，该软件还会运行可执行文件、提取其他关键数据、并对目标设备进行屏幕截图等操作，严重影响被攻击者的电脑的运行安全。乌克兰安全官员认为，俄罗斯黑客是大多数攻击的幕后黑手。

表 3-1 2022 年部分安全事件

序号	时间	国家/地区	行业	方式	影响
1	1 月	德国	制造业	未知	欧洲北部地区柴油涨价
2	1 月	荷兰	能源业	勒索软件	石油装卸和转运受阻
3	2 月	美国	农业	勒索软件	勒索高额赎金
4	2 月	白俄罗斯	运输业	未知	铁路运营秩序受影响，资料泄露
5	2 月	瑞士	运输业	勒索软件	运营受到干扰
6	3 月	罗马尼亚	能源业	勒索软件	油站官网、APP 无法访问

7	3 月	德国	能源业	勒索软件	近 6000 台风力发电机失去远程控制
8	4 月	乌克兰	能源业	恶意软件	变电站停电
9	4 月	德国	制造业	网络攻击	被迫关闭多个业务部门的系统
10	4 月	加拿大	制造业	网络攻击	航班延误，大量旅客滞留机场
11	5 月	美国	农业	勒索软件	公司被迫关闭系统、销售停滞
12	5 月	印度	航空业	勒索软件	航班延误、旅客滞留机场
13	6 月	美国	建筑业	恶意流量混合	探测到更多新的恶意软件变种和与攻击者相关的 TTP
14	6 月	土耳其	航空业	未知	严重的数据泄露
15	6 月	美国	能源业	网络攻击	液化天然气厂的运营产生了持久影响
16	7 月	德国	制造业	勒索软件	文件泄露、被索要高额赎金
17	7 月	伊朗	制造业	网络攻击	严重扰乱工厂运营
18	7 月	西班牙	工业	网络攻击	辐射警报网络无法响应辐射激增事件
19	8 月	希腊	能源业	勒索软件	大量数据遭到泄露
20	8 月	英国	医疗业	网络攻击	急救热线持续性中断
21	9 月	巴勒斯坦	工业	网络入侵	多个 PLC 可以被攻击者控制
22	10 月	美国	航空业	DDoS 攻击	航空公司网站的服务器无法运作
23	10 月	德国	新闻业	勒索软件	系统陷入瘫痪，电子版文件无法访问
24	11 月	乌克兰	互联网	勒索软件	恶意脚本入侵网络
25	11 月	德国	制造业	网络攻击	数据泄露，被索要赎金
26	12 月	乌克兰	运输业	网络钓鱼攻击	电脑被恶意操控、数据泄露
27	12 月	哥伦比亚	能源业	勒索软件	大量数据泄露
28	12 月	德国	制造业	网络攻击	有可能造成数据泄露

4. 工控系统安全漏洞概况

随着工业 4.0、智能制造、工业互联网等概念的产生和发展，全球工控产业体系迅速扩大，工控系统的独立性日益降低，理论上来说对工控系统的攻击实现将更加简单，例如 PLC 等 ICS 的核心构成将面对更多样的攻击手段、更隐蔽的攻击形式等。相关数据显示，2022 年西门子（Siemens）、施耐德（Schneider）、北京亚控科技发展有限公司（WellinTech）、三菱（Mitsubishi）、欧姆龙（Omron）等工业控制系统厂商也均被发现包含各种信息安全漏洞。然而本团队从采集到的工控漏洞数据中注意到，近两年的工控安全漏洞数量呈逐年下降的趋势。

图 4-1 2012-2022 年工控漏洞走势图（数据来源 CNVD、“谛听”）

根据 CNVD（国家信息安全漏洞共享平台）[1][2]和“谛听”的数据，2012-2022 年工控漏洞走势如图 4-1 所示。从图中可以看出，2015 年到 2020 年期间工控漏洞数量呈显著的逐年增长趋势，出现这种情况的主要原因，本团队分析认为是：2015 年后，技术融合加速工控产业发展的同时破坏了传统工控系统的体系结构，在产业标准、政策尚不成熟的情况下攻击者可能会采取更加丰富的攻击手段攻击工控系统，导致工控漏洞的数量逐年上升。然而从 2021 年开始，工控漏洞数量呈逐年下降的趋势，与 2020 年的 568 条漏

洞信息相比，2021 年减少了 416 条，漏洞数量大幅降低，减少数量占 2020 年的 73%，2022 年的漏洞数量降幅虽不及 2021 年的 73%，但仍达到了 37%，本团队猜测出现的原因是：一方面，由于新冠疫情在全球反复暴发，大量从业人员线上办公，工控产业活力低下，导致工控攻击目标的数量与类型较往年有所减少，工控漏洞的产生和发现可能会因此减少；另一方面，随着工控信息安全政策、体系、法规的不断完善，工控安全方面的产品体系和解决方案愈发健全，客观上的漏洞数量下降应在情理之中。

图 4-2 2022 年工控系统行业漏洞危险等级饼状图（数据来源 CNVD、“谛听”）

如图 4-2 所示，2022 年工控系统行业漏洞危险等级饼状图，截至 2022 年 12 月 31 日，2022 年新增工控系统行业漏洞 96 个，其中高危漏洞 35 个，中危漏洞 51 个，低危漏洞 10 个。与去年相比，漏洞数量减少了 56 个，高危、中危和低危漏洞数量均有一定减少，其中，中高危漏洞数量减少了 54 个，占 2021 年中高危漏洞总数的 39%。2022 全年高危工控安全漏洞占全年漏洞总数量中的 36%，与 2021 年相比相差不大。由此可见，今年的全球工控安全体系建设更加完备，工控产业相关厂商、企业的研究更加深入，情况较为乐观，但同时高危漏洞数量占比仍然较大，需要持续完善工控方面的协议、政策，增加对工控信息安全产业的投入。

以上数据表明，在 2022 年，虽然工控漏洞数量的降幅较 2021 年有所降低，但全球工控系统的安全维护水平依然持续提升；同时我们注意到高危漏洞数量占比变化不大，理想情况下，风险等级被标记为“高危”的漏洞数量应当在工控相关协议、设备设计之初尽量避免，或在被工控系统安全人员发现时及时解决，其相比中低危漏洞具有更高的处理优先级，故工控系统所遭受攻击数量虽然在近两年逐年减少，但工控系统所遭受的攻击强度可能并没有降低，或者说工控系统方面设计缺陷可能并没有得到及时完善，同时工控产业相关单位有必要进一步加强对工业漏洞的防范，并持续增加对工控系统安全建设的投入。

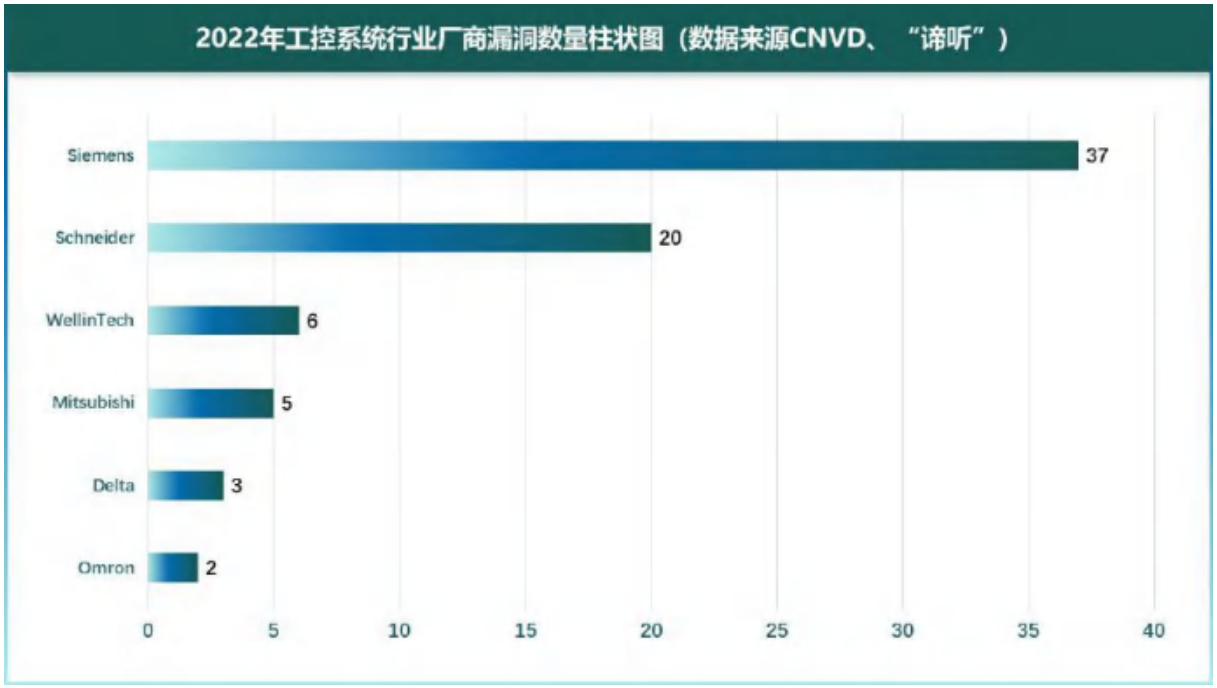

图 4-3 2022 年工控系统行业厂商漏洞数量柱状图（数据来源 CNVD、“谛听”）

如图 4-3 是 2022 年工控系统行业厂商漏洞数量柱状图，由图中可知，西门子（Siemens）厂商具有的漏洞数量最多，多达 37 个。漏洞数量排在其后的厂商分别是：施耐德（Schneider）、亚控科技（WellinTech）、三菱（Mitsubishi）、台达（Delta）、欧姆龙（Omron），这些厂商也存在着一定数量的工控系统行业漏洞。由此可见，各个厂商应该密切关注工控系统行业漏洞，通过部署终端安全防护组件、部署防火墙、入侵检测系统、入侵防护系统或安全监测系统等方式进一步提升系统防护水平，确保工控系统信息安全。

5. 联网工控设备分布

“谛听”网络空间工控设备搜索引擎共支持 31 种服务的协议识别，表 5-1 展示了“谛听”网络安全团队识别的工控协议等的相关信息。如想了解这些协议的详细信息请参照“谛听”网络安全团队之前发布的工控网络安全态势分析白皮书。

表 5-1 “谛听”网络空间工控设备搜索引擎支持的协议

工控协议	端口	概述
Modbus	502/503	应用于电子控制器上的一种通用语言
Tridium Niagara Fox	1911	Tridium 公司专用协议，用于智能电网等领域
SSL/ Niagara Fox	4911	智能建筑、基础设置管理、安防系统的网络协议
BACnet	47808	智能建筑的通信协议
ATGs Devices	10001	工控协议
Moxa Nport	4800	虚拟串口协议
EtherNet/IP	44818	以太网协议
Siemens S7	102	西门子通信协议
DNP3	20000	分布式网络协议
Codesys	2455	PLC 协议
ilon Smartserver	1628/1629	智能服务器协议
Redlion Crimson3	789	工控协议
IEC 60870-5-104	2404	IEC 系列协议
OMRON FINS	9600	欧姆龙工业控制协议
CSPV4	2222	工控协议
GE SRTP	18245	美国通用电器产品协议
PCWorx	1962	菲尼克斯电气产品协议
ProConOs	20547	科维公司操作系统协议
MELSEC-Q	5006/5007	三菱通信协议

opc-ua	4840	OPC UA 接口协议
DDP	5002	用于数据的传输和 DTU 管理
Profinet	80	基于工业以太网技术的自动化总线标准
IEC 61850-8-1	102	IEC 系列协议
Lantronix	30718	专为工业应用而设计，解决串口和以太网通信问题
物联网协议	**端口**	**概述**
AMQP	5672	提供统一消息服务的应用层标准高级消息队列协议
XMPP	5222	基于 XML 的可扩展通讯和表示协议
SOAP	8089	基于 XML 简单对象访问协议
ONVIF	3702	开放型网络视频接口标准协议
MQTT	1883	基于客户端-服务器的消息发布/订阅传输协议
摄像头协议	**端口**	**概述**
Dahua Dvr	37777	大华摄像头与服务器通信协议
hikvision	81-90	海康威视摄像头与服务器通信协议

“谛听”官方网站（www.ditecting.com）公布的数据为 2017 年以前的历史数据，若需要最新版的数据请与东北大学“谛听”网络安全团队直接联系获取。根据“谛听”网络空间工控设备搜索引擎收集的内部数据，经“谛听”网络安全团队分析，得出如图 5-1 的可视化展示，下面做简要说明。

图 5-1 为 2022 年全球工控设备暴露 Top-10 国家。在图中可以看到，国家排名较 2021 年基本没有发生太大变化。在全球范围内，美国作为世界上最发达的工业化国家暴露出的工控设备仍然保持第一；中国继续大力发展先进制造业，推动新型基础设施建设，工业产值大幅增加，位居第二；2022 年波兰的 GDP 有所增长，暴露的工控设备也有所增长，位居第三。以下着重介绍国内及美国、波兰的工控设备暴露情况。

图 5-1 全球工控设备暴露 Top10 柱状图（数据来源“谛听”）

5.1 国际工控设备暴露情况

国际工控设备的暴露情况以美国和波兰为例进行简要介绍。

美国是世界上工业化程度最高的国家之一，同时也是 2022 年全球工控设备暴露最多的国家，如图 5-2 所示为美国 2022 年工控协议暴露数量和占比。自 2012 年美国通用电气公司（GE）提出工业互联网的概念以来，美国政府就十分重视工业控制领域。依托互联网技术的发展优势，大力推动工控相关技术的发展，以应对经济全球化可能带来的机遇与挑战。在推动工业互联网革命的同时，美国政府也关注到了由于缺乏监管而泄露的数据可能带来的一系列互联网安全问题。2022 年 9 月，美国网络安全和基础设施安全局（CISA）发布了《2023 年至 2025 年战略规划》（2023-2025 Strategic Plan），该规划是 CISA 自 2018 年成立以来发布的首个综合性战略规划，规划中明确了美国未来三年网络防御、减少风险和增强恢复能力、业务协作、统一机构 4 个总的网络安全目标。

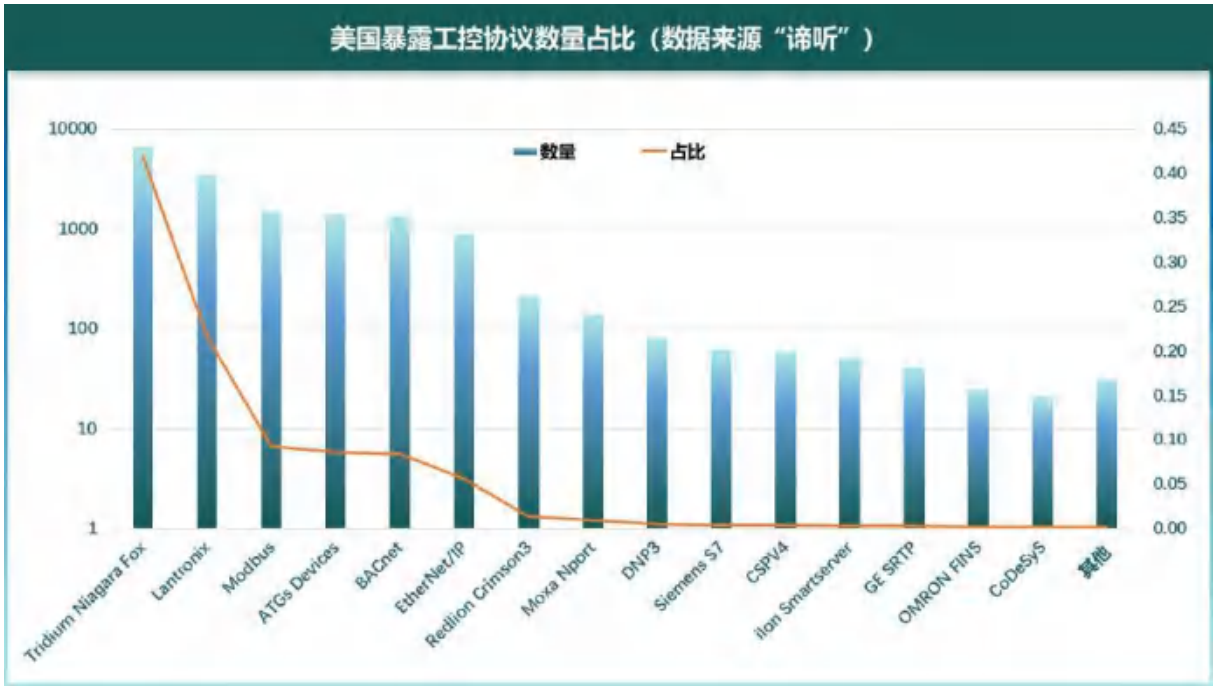

图 5-2 美国工控协议暴露数量和占比（数据来源“谛听”）

虽然美国是最早投身网络安全建设的国家之一，但在工业控制系统网络安全方面的表现仍然有待提高。与 2021 年相比，美国 2022 年暴露的工控设备数有所减少。可能是受俄乌战争的影响，美国政府认识到工控设备及其之上运行的大量关键基础设施的重要性，因此更加重视工控领域的安全问题。2022 年的全球网络空间安全形势愈发复杂，美国政府愈发重视工业控制系统安全。

2022 年波兰工控设备暴露数量位居全球第三。波兰地处欧洲中部，属于发展中国家，但其人均 GDP 基本接近末流发达国家的水平。波兰的工业化程度很高，是欧盟第六大工业强国，在波兰的诸多工业产业中，以制造业的表现最为突出。据波兰中央统计局发布的数据，自 2022 年年初，波兰的工业产值一直以每月两位数的速度在增长。通过图 5-3 可以看到，在波兰所暴露的协议中，Modbus 协议的数量居于首位。Modbus 协议由于其公开免费，部署较为简单，自问世以来受到了诸多供应商的青睐，但由于其缺乏认证加密等机制，Modbus 协议被广泛使用的同时，也为波兰工业控制系统的安全性带来了巨大的风险。

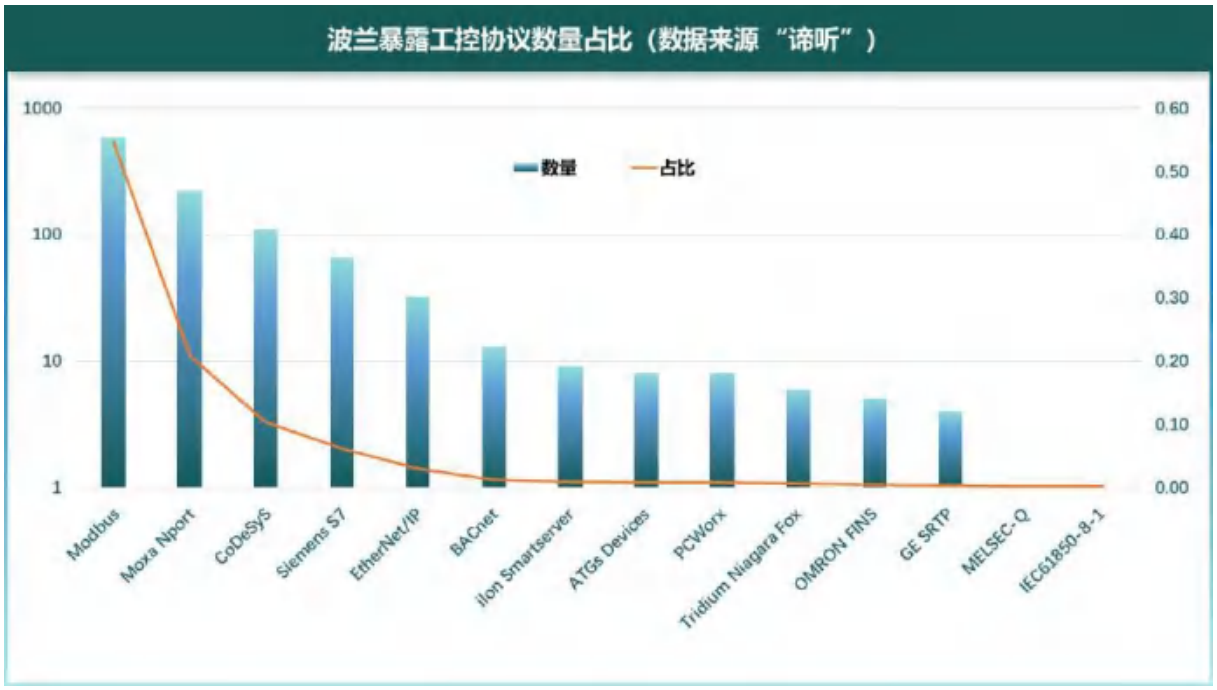

图 5-3 波兰工控协议暴露数量和占比（数据来源“谛听”）

综上，相较于 2021 年，美国政府在发展工业的同时，更加重视国家工控系统安全性的问题，2022 年暴露的工控设备数量略有下降。而波兰由于汽车制造业的繁荣发展，国家 GDP 增长的同时暴露的工控设备数量也大幅增长，这势必会给国家的后续健康发展埋下一定的隐患。

5.2 国内工控设备暴露情况

2022 年中国暴露的工控设备数量排全球第二。近几年来，中国的产业结构不断优化升级，工业互联网发展迅速，实体经济也在逐步转型升级中。下面详细分析一下国内工控设备暴露情况。

在全国暴露工控设备数量的条形图 5-4 中可以直观的看出江苏省的工控设备暴露数量跻身至全国首位，与去年相比，多省的工控设备暴露数量都有了很大程度的增长。2021 年由于新冠疫情的肆虐，全国很多地方停工停产，国内工控设备暴露数量也随之减少。2022 年在政策稳步推动、经济企稳复苏及企业数字转型需求增加等因素交织影响下，中国工业互联网市场继续保持稳定增长，工业化与信息化在高层次进行了深度融合，国内工控设备暴露数量相比 2021 年有了爆发式增长。

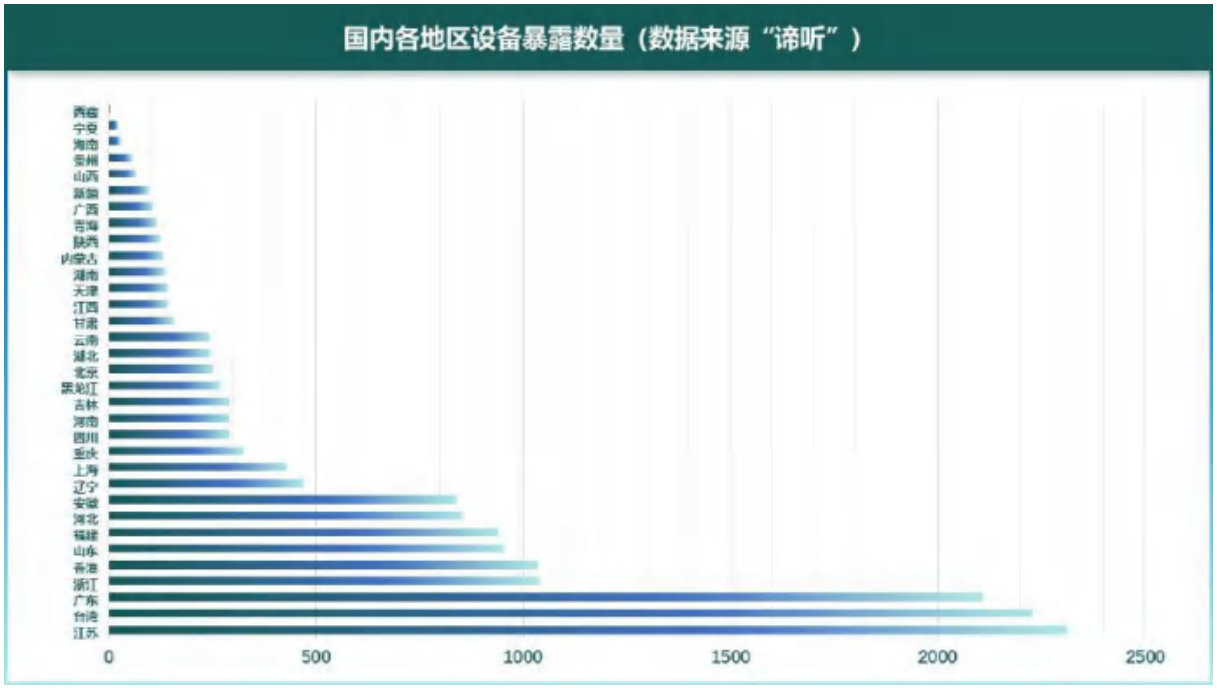

图 5-4 国内各地区工控设备暴露数量（数据来源“谛听”）

2022 年，江苏省是暴露工控设备数量最多的省份。据中国经济新闻网报道，江苏省 2022 年信息化和工业化融合发展水平指数达到 66.4，年平均增速 3%左右，较 2022 年全国平均水平 59.6 高出 11.4%。发达的工业体系是江苏省实现信息化和工业化的基础。近年来，江苏立足制造业优势，坚持“实体强基”，先后出台《关于深化“互联网+先进制造业”发展工业互联网的实施意见》《江苏省制造业智能化改造和数字化转型三年行动计划》等文件，把工业互联网创新工程作为战略性任务，融入到制造业数字化转型全过程。制定实施《江苏省加快推进工业互联网创新发展三年行动计划（2021—2023 年）》等文件，推进“数实融合”发展[3]。江苏省多年来一直以两化(信息化、工业化)融合为行为指南，实现了多个行业智能化改造以及数字化转型，其正以工业互联网、大数据中心、5G 基站等新基建夯实数据基底，着力打造领先世界的工业互联生态圈。

2022 年，台湾地区工控设备暴露数量依然名列前茅，位列全国第二。台湾工业体系发展完善且依然在全国各地区中处于领先的位置，其与大陆的交流合作也十分密切。2022 年九月，两岸工业互联网融合发展研讨会在昆山举办，会上聚焦“产业升级”展开交流，助力双方合作共赢。近年来，大陆在工业互联网、大数据以及 5G 基站等新基建方面有着坚实的基底，而台湾在集成电路等领域也积攒了雄厚的实力，双方的交流合作有

利于社会数字化转型和智能化改造，推动工业互联网在更广范围、更深程度、更高水平上融合创新。

广东 2022 年工控设备暴露数量排全国第三。近年来，广东深化工业互联网国家示范区建设，推进工业化和信息化深度融合成效显著，工业互联网相关企业数量也位居全国前列。据羊城新闻晚报报道，截至 2022 年 6 月底，广东省累计推动 2.25 万家规上工业企业运用工业互联网数字化转型，带动 65 万家中小企业“上云用云”。从制造业强省到数字化强省，广东一直走在全国前面，广东的工业互联网企业也在加快全球化布局，输出积累的数字化转型经验。

长江三角洲地区工控设备暴露数量的排名变动不大。随着经济的逐步复苏，长三角地区（江苏、安徽、浙江和上海）正利用区位和资源优势，加速推进长三角工业互联网一体化发展，为全国国际化、区域联动发展等方面进行了前沿探索。2022 年 11 月，为加快构建长三角工业互联网体系，促进长三角产业转型升级，长三角工业互联网峰会在合肥市奥体中心隆重召开。此次大会全面展示了长三角区域工业互联网的最新发展成果，推动长三角工业互联网一体化发展再升级、再提速。把握重大战略机遇，加快发展工业互联网，是长三角实现制造业高质量发展、构筑工业竞争新优势的必然选择[4]。

北京今年排名相较去年有所下降，作为中国首都，北京经转人流量过多，疫情时常反复，对工业互联网的发展还是产生了一定的影响。并且现阶段的北京，绿色发展是基础，工业产业大量转移出去，使暴露的工控设备数量与其他地区相比显得相对较少。

与 2021 年工控设备暴露数量相比，辽宁 2022 年工控设备暴露的数量反超黑龙江和吉林，成为东北地区工控设备暴露数量最多的省份。东北地区（辽宁、吉林、黑龙江）作为中国工业的摇篮，在我国发展史上写下了光辉灿烂的篇章。辽宁省于 2022 年 11 月举办了全球工业互联网大会，此次大会对于加快工业互联网创新发展、推动数字辽宁智造强省建设取得新突破，具有重大意义。据辽宁省政府新闻办报道，辽宁省认真贯彻习近平总书记关于工业互联网创新发展的重要指示精神，把工业互联网创新发展作为助推经济高质量发展的重要力量，出台了《工业互联网创新发展三年行动计划》等政策文件，设立了省级专项资金，加快推动制造业数字化转型，使得辽宁省工业互联网进入了新的发展阶段[5]。中国工业互联网研究院院长鲁春丛于此次大会上发表了《全球工业互联网

创新发展报告》讲话，他指出，未来五年将是工业互联网从起步探索转向快速发展的重要阶段，也是我国推进新型工业化，加快建设制造强国、网络强国、数字中国的关键时期[6]。当前，随着技术的不断发展，实现工业化和信息化高水平融合已是中国特色新型工业化道路的集中体现，工业互联网为产业数字化、网络化以及智能化发展提供了新的机遇。

2022 年，香港排名虽然较去年有所下降，但暴露设备数量却上升了将近三倍。香港以往是一个主要以服务业为主的经济体，所以香港的工控设备暴露数量并不能与广东以及台湾等地相比。但近年来，随着 5G 专网工业模组成本的降低，香港积极资助 5G 技术应用，多方面推动 5G 发展，完善 5G 网络覆盖，开展 5G 企业网络以及 5G 工业互联网的融合应用以及部署，推动香港新型工业化的发展。香港抓住机遇，积极融入国家发展大局，为中国独立自主建设工业互联网络起到了表率作用。

5.3 国内工控协议暴露数量统计情况

图 5-5 国内工控协议暴露数量和占比（数据来源“谛听”）

“谛听”团队统计了国内暴露的各协议总量，从图 5-5 中可以看出 Modbus 协议在网络中暴露的数量最多，领先于第二位的 Moxa Nport。Modbus 是一种串行通信协议，是

Modicon 公司（现在的 Schneider Electric）于 1979 年为使用可编程逻辑控制器（PLC）通信所发行的。在我国，Modbus 协议已经被纳入国家标准 GB/T19582-2008。虽然 Modbus 协议支持多个设备在同一网络中的透明通信，帧格式紧凑、简洁，兼容多种电气接口。且 Modbus 凭借易部署、限制少、门槛低的优点，成为工业领域通信协议的业界标准，是国内工业电子设备之间最常用的连接方式。然而该协议缺乏有效的认证和加密手段，亦缺少对功能码的有效管理，因此造成许多安全问题，可见该协议排在国内暴露协议第一位属情理之中。

Moxa Nport，Moxa 串口服务器专为工业应用而设计，Moxa Nport 是其中的一个串口服务器系列，在世界范围内具有广泛的应用。不同配置和组合的服务器能满足多种工业场景的需要，因此适用性强。

Tridium Niagara Fox，Tridium Niagara Fox 被广泛应用于国家的智能建筑、设施管理、安防、电力、空调设备等领域。Tridium 是 Honeywell 旗下独立品牌运作的子公司，开发了软件框架“Niagara Framework”。基于 Niagara 框架，客户可以开发专有产品和应用，也可以集成、连接各种智能设备和系统，不受生产厂家和协议的影响，在实现设备互联的同时可以通过网络进行实时控制和管理。NiagaraAX 平台时至今日已经整合了多种系统，例如建筑、园区的基础硬件设施、安防系统、访客管理、电网系统、设施管理等。NiagaraAX 把这些设备和系统进行连接，使用 Tridium Niagara Fox 协议通信，具有极高的使用价值，因此排在第三位亦在意料之中。

EtherNet/IP 是由 ODVA（Open DeviceNet Vendor Association）指定的工业以太网协议，它使用 ODVA 已知的应用层“通用工业协议”（CIP™）。CIP 是一种由 ODVA 支持的开放工业协议，它被使用在例如 EtherNet/IP 等串行通信协议中。美国的工控设备制造商 Rockwell/Allen-Bradley 对 EtherNet/IP 进行了标准化处理，其他的厂商也在其设备上支持了 EtherNet/IP 协议。当前，EtherNet/IP 的使用已经十分广泛，然而协议层面的安全问题仍值得我们重视。

BACnet 是用于楼宇自动化和控制网络的简短形式的数据通信协议，亦是主要行业供应商产品中常用的自动化和控制协议之一，其目的是提高服务供应商之间的互操作性，减少因设备厂商的专有系统所造成的使用限制问题。此协议的泄露往往是由用户缺乏安

全意识导致，意味着该 IP 对应的行业供应商的产品设备已经暴露，因此容易造成用户的网络安全隐患和财产损失。

5.4 俄乌冲突以来暴露设备数量变化

俄乌冲突开始于 2022 年三月份，目前俄罗斯和乌克兰的紧张局势依然在持续中，近期的冲突仍然在加剧。发动网络战能够削弱一个国家的通信能力以及战场感知能力，而且随着军队依靠软件，利用获取的情报在战场上进行部署，这场竞赛变得越来越重要。为了能够了解俄罗斯和乌克兰的工控领域的相关状况，“谛听”网络安全团队对此进行了持续关注。表 5-2 列举了俄罗斯、乌克兰暴露工控设备的相关协议。

表 5-2 俄罗斯、乌克兰暴露工控设备相关协议

探测发现协议	探测端口	协议概述
Siemens S7	102	西门子通信协议
Modbus	502	应用于电子控制器上的一种通用语言
ilon Smartserver	1628	智能服务器协议
Moxa Nport	4800	Moxa 专用的虚拟串口协议
XMPP	5222	基于 XML 的可扩展通讯和表示协议
AMQP	5672	提供统一消息服务的应用层标准高级消息队列协议
IEC 60870-5-104	2404	IEC 系列协议

同时，“谛听”网络安全团队每月都会收集俄乌暴露的设备数量情况，根据收集的数据，得到了俄罗斯和乌克兰自冲突爆发以来暴露的设备的数量变化情况。

从图 5-6 冲突前后俄罗斯各协议暴露设备数量来看，AMQP 协议从冲突前到冲突开始持续到 8 月份变化幅度较大，总体呈现先降后升的趋势，后续趋于平缓；Siemens S7 协议从冲突前至 3 月份呈现下降趋势，之后整体趋势呈现先升后降；IEC 60870-5-104 协议整体变化趋势与 Siemens S7 协议相同，但在 11 月至 12 月份突然呈现迅速上升的趋

势，猜测与 11 月发生了工控事件有关；ilon Smart -server 协议在 5 月份变化较大，10 月份之后呈现下降趋势；其它协议整体的变化幅度不大。

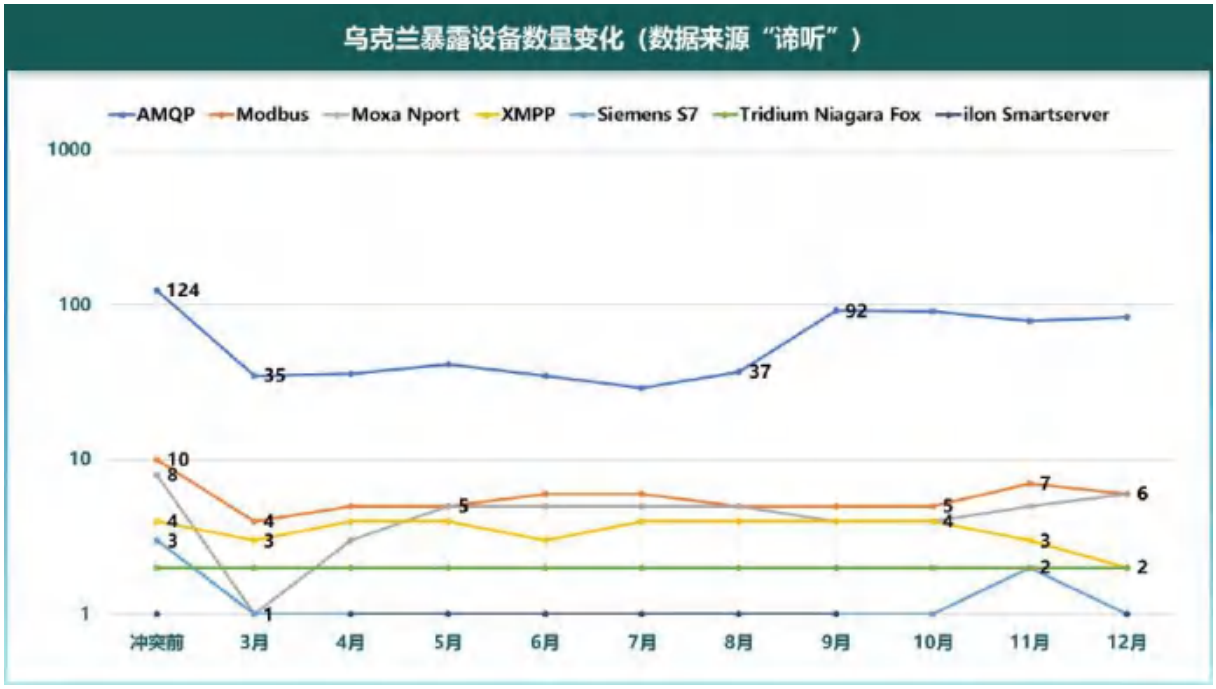

图 5-6 俄罗斯暴露设备数量变化（数据来源“谛听”）

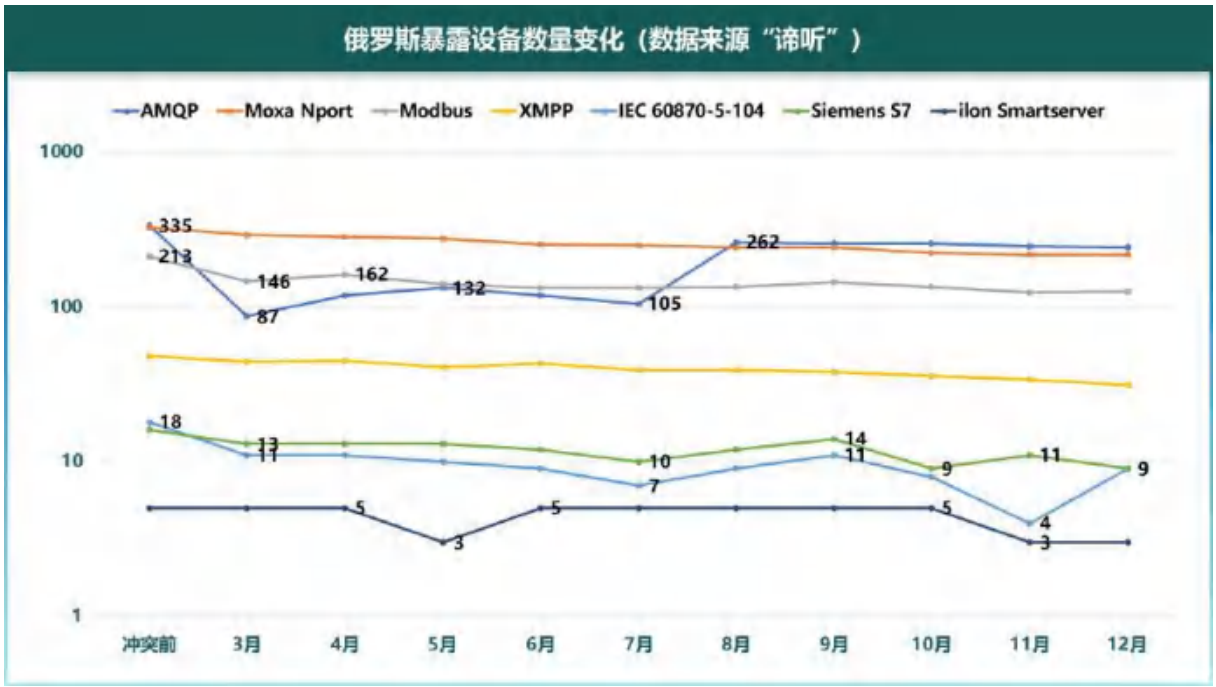

图 5-7 乌克兰暴露设备数量变化（数据来源“谛听”）

从图 5-7 冲突前后乌克兰各协议暴露设备数量变化情况中我们可以看到，首先 AMQP、Modbus、Moxa Nport、XMPP 以及 Siemens S7 等协议从冲突前到 4 月份变化较大，猜测是期间发生了重大的工控事件导致的。随后，除 AMQP 以外的四种协议在 10 月到 12 月份发生了小幅度的变化；其它两种协议没有变化。

总之，从上面两幅图可以看出，俄乌暴露设备的数量变化较大的月份主要集中在 3 月至 5 月以及 10 月至 12 月这几个月份，猜测其变化趋势与当时发生的工控事件有直接或间接的关系，表 5-3 列举自俄乌冲突以来与之相关的主要的工控事件。

表 5-3 俄乌冲突相关的主要的工控事件

时间	主要工控事件
2022 年 3 月	俄罗斯联邦储蓄银行（Sberbank）和莫斯科交易所的网站遭到乌克兰 IT 军攻击 黑客组织“匿名者”入侵并泄漏了俄罗斯经济发展部等政府单位以及俄罗斯国家原子能公司 Rosatom 数据，攻击了包括俄罗斯航空公司 PegasusFly、俄国防产品出口公司（Rosoboronexport）、俄罗斯紧急情况部、俄罗斯能源巨头 Rosneft 位于德国的子公司以及俄罗斯管道巨头 Transneft 内部研发部门 Omega 公司等相关网站 黑客组织 AnonGh0st 入侵俄罗斯 SCADA 系统并共享了与供水系统相关的数据 俄罗斯黑客组织攻击了覆盖乌克兰地区的美国卫星运营商 Viasat 俄罗斯有关 APT 组织 InvisiMole 主要针对乌克兰国家机构发起攻击 未知组织攻击了乌克兰互联网服务提供商 Triolan 以及主要的通信运营商 Ukrtelecom，导致网络严重中断 未知组织入侵了包括乌克兰政府机构、智囊团、国防军招募和金融等相关网站
2022 年 4 月	乌克兰某能源公司遭恶意软件攻击 俄罗斯石油巨头 Gazprom Neft 网站遭黑客攻击
2022 年 10 月	亲俄黑客组织对美国关键基础设施发起大规模攻击
2022 年 11 月	黑客成功入侵乌军战场指挥系统，战场数据泄露
2022 年 12 月	俄罗斯黑客试图入侵北约某国的大型炼油厂未遂

6. 工控蜜罐数据相关分析

如今，工业互联网的蓬勃发展给工业控制领域带来了新的发展机遇，与此同时也带来了新的网络安全问题。蜜罐技术是增强工控系统网络安全防护能力的有效方法，东北大学“谛听”网络安全团队对工控蜜罐技术展开了研究。经过多年努力，“谛听”网络安全团队研发出了可以模拟多种工控协议和工控设备并且全面捕获攻击者流量的“谛听”工控蜜罐。目前，“谛听”蜜罐支持 11 种协议，且已经部署在多个国家和地区。“谛听”网络安全团队在 2021 年进一步改进了基于 ICS 蜜网的攻击流量指纹识别方法（以下简称“识别方法”），有效地提高了识别各类针对工控网络的攻击流量的效率，并根据不同类型的攻击流量制定出更加有效的工控系统防御措施。

6.1 工控蜜罐全球捕获流量概况

“谛听”工控蜜罐可支持 ATGs Devices、DNP3、Modbus、EGD 等 11 种协议，其中，EGD 协议是今年新增的协议。目前“谛听”工控蜜罐已经部署在了中国华北地区、中国华南地区、东欧地区、东南亚地区、美国东北部等国内外多个地区。截止到 2022 年 12 月 31 日，“谛听”蜜罐收集到大量攻击数据。图 6-1、6-2 和 6-3 中展示了经过统计和分析后的数据。下面将对各个图表进行简要解释说明。

图 6-1 蜜罐各协议攻击量（数据来源“谛听”）

图 6-1 展示了不同协议下各蜜罐受到的攻击量。从图中可以看出，ATGs Devices、DNP3 和 Modbus 协议下蜜罐所受攻击量仍然保持在前三名。但与 2021 年相比，曾大幅领先的 Modbus 协议被 ATGs Devices 协议和 DNP3 协议超越，降至第三名，ATGs Devices 协议从第二名跃居第一，这表明 ATGs Devices 协议受到的关注大幅度增加。另外，今年新增的 EGD 协议具有简便高效的特性，其所受攻击量位于第六位。这些变化表明工控系统协议在不断发展，攻击者的攻击方向也在不断调整和变化。前四种协议所受的攻击量总计占比接近 70%，这表明这些协议比较受攻击者的关注，因此工控网络安全研究人员应根据需求情况，加强这些协议下设备的网络安全防护。

“谛听”网络安全团队对收集到的攻击数据的 IP 来源进行分析，得到了来自不同国家和地区攻击源的数量统计，图 6-2 仅展示攻击量最多的 10 个国家。从图中可以看到，美国的攻击量遥遥领先，甚至超过了其他 9 个国家攻击量的总和；排在第二的国家是荷兰，其攻击量虽远少于美国但也处于较高的数量水平，这在一定程度上表明两国攻击者对本国工控设备的高度关注。英国、俄罗斯和德国的攻击量相差不大，分别位于第三到五位。从排名第六位的斯洛伐克开始，攻击量显著减少。

图 6-2 其他各国对蜜罐的攻击量 TOP10（数据来源“谛听”）

对中国国内流量来源的 IP 地址进行相关分析，列出了 IP 流量的省份排名，如图 6-3 所示，这里仅展示前十名。可以看到，来自中国华北地区的 IP 流量较多，北京同去年一样排在了第一位，体现出其作为首都在网络安全支撑工作方面的领先地位。山西省跃升至第二位，浙江省由去年的第五名上升至第三名，由此可见山西省和浙江省在网络安全方面做出的努力。

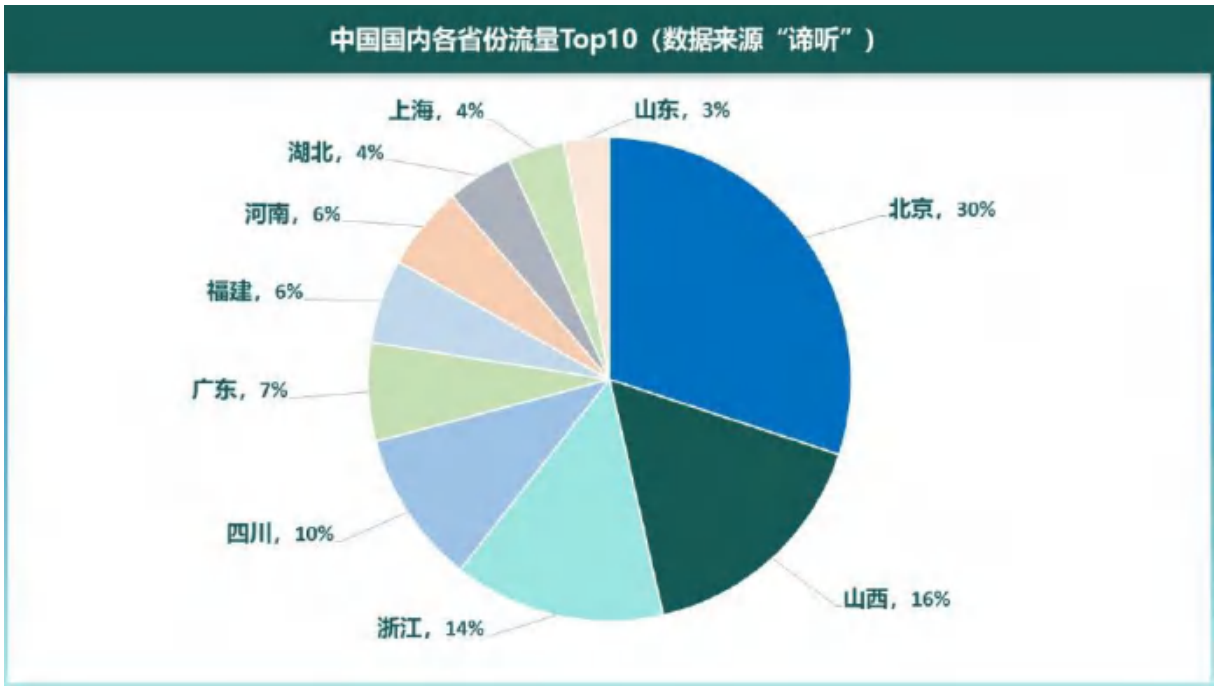

图 6-3 中国国内各省份流量（top10）（数据来源“谛听”）

2022 年，“谛听”网络安全团队调整了已部署的蜜罐，拓展了蜜罐可支持协议的范围，未来将会与更多高新技术应用进行融合，相关的研究将会持续推进。

6.2 工控系统攻击流量分析

“谛听”团队首先对来自不同地区的蜜罐捕获的攻击流量数据进行初步分析，然后使用识别方法对 Modbus、Ethernet/IP 两个应用范围较广的协议进行攻击流量检测，并从每个协议在不同地区部署的蜜罐中选择最具代表性的两个地区进行攻击流量数据统计。

针对 Modbus 协议，我们选择了中国华东地区和美国东海岸地区部署的蜜罐，统计结果如表 6-1、6-2 所示。

表 6-1 中国华东地区 Modbus 协议蜜罐捕获攻击总量来源 TOP10（数据来源“谛听”）

攻击源	攻击总量	攻击 IP 数量	IP 平均攻击数
Netherlands	5422	85	63.8
United States	2008	401	5.0
China	573	59	9.7
United Kingdom	395	8	49.4
Germany	72	10	7.2
Japan	62	3	20.7
Russia	61	14	4.4
Belgium	48	34	1.4
Canada	34	21	1.6
Greece	15	12	1.3

表 6-2 美国东海岸地区 Modbus 协议蜜罐捕获攻击总量来源 TOP10（数据来源“谛听”）

攻击源	攻击总量	攻击 IP 数量	IP 平均攻击数
United States	865	243	3.6
Netherlands	282	11	25.6
Germany	183	19	9.6
China	85	12	7.1
United Kingdom	74	7	10.6
Singapore	42	3	14.0
Belgium	38	28	1.4
Canada	22	18	1.2
Ukraine	9	1	9.0

Japan	8	1	8.0

由表 6-1、6-2 可知，在攻击总量来源方面，荷兰在中国华东地区的攻击总量显著高于其他国家，且远高于去年同期数据。在美国东海岸地区 Modbus 协议蜜罐捕获攻击总量中，美国仍然保持第一位，且与去年相比呈现上升趋势。在攻击 IP 数量方面，美国仍在两个地区中均排名第一，并远超于其他国家。以表 6-2 为例，美国在美国东海岸地区的攻击 IP 数量约是排名第二的比利时的 8.7 倍。在 IP 平均攻击数方面，荷兰在两个地区中均处于第一位。

针对 Ethernet/IP 协议，我们选择的是中国华南地区和美国西海岸地区部署的蜜罐，统计结果如表 6-3、6-4 所示。

表 6-3 中国华南地区 Ethernet/IP 协议蜜罐捕获攻击总量来源 TOP10（数据来源“谛听”）

攻击源	攻击总量	攻击 IP 数量	IP 平均攻击数
United States	452	119	3.8
China	89	29	3.1
Kazakhstan	55	3	18.3
Netherlands	19	6	3.2
Germany	8	6	1.3
Japan	6	1	6.0
India	2	1	2.0
Ukraine	1	1	1.0
United Kingdom	1	1	1.0
Vienna	2	1	2.0

表 6-4 美国西海岸地区 Ethernet/IP 协议蜜罐捕获攻击总量来源 TOP5（数据来源“谛听”）

攻击源	攻击总量	攻击 IP 数量	IP 平均攻击数
United States	333	69	4.8
China	17	11	1.5
Germany	8	5	1.6
Netherlands	8	7	1.1
Japan	4	2	2.0

由表 6-3、6-4 分析可知，在攻击总量来源和攻击 IP 数量方面，美国在两个地区中均位列第一，且远超其他国家。在 IP 平均攻击数方面，哈萨克斯坦在中国华南地区排名第一，是排名第二的日本的 3.05 倍。美国在美国西海岸地区的 IP 平均攻击数最高。

通过上述统计的 Modbus 协议蜜罐和 Ethernet/IP 协议蜜罐捕获的攻击总量来源数据，可以看出 Modbus 协议蜜罐受攻击的总次数远大于 Ethernet/IP 协议蜜罐，推测其原因为 Modbus 协议具有公开免费、开源工具多、部署和维护简单等特点，从而当前应用范围更广泛，因此所受攻击更多。此外，在确定攻击源的情况下，排名前三的国家的攻击方来源数占总数的近 90%，可能的原因包括：一是由于这些国家的公司提供的云服务器被租赁用于长期扫描；二是由于这些国家的安全行业从业者及研究人员较多，相关研究行为较活跃；三是由于这些国家存在大量恶意攻击团队，其对互联网进行的恶意攻击被谛听部署的蜜罐有效诱捕。

6.3 工控系统攻击类型识别

“谛听”网络安全团队提出一种基于 ICS 蜜网的攻击流量指纹识别方法，针对 Modbus、Ethernet/IP 协议蜜罐捕获的流量数据进行了攻击类型识别。图 6-4 和图 6-5 分别显示了对 Modbus 和 Ethernet/IP 协议蜜罐捕获的攻击流量的攻击类型识别结果。其中的“E”表示 Ethernet/IP 协议，其中的“M”表示 Modbus 协议，由于国内和国外的蜜罐程序不同，“E”和“E"”同一编号表示不同的攻击类型，“M”和“M"”同一编号表示不同的攻击类型，环形图中各部分为不同的攻击类型。

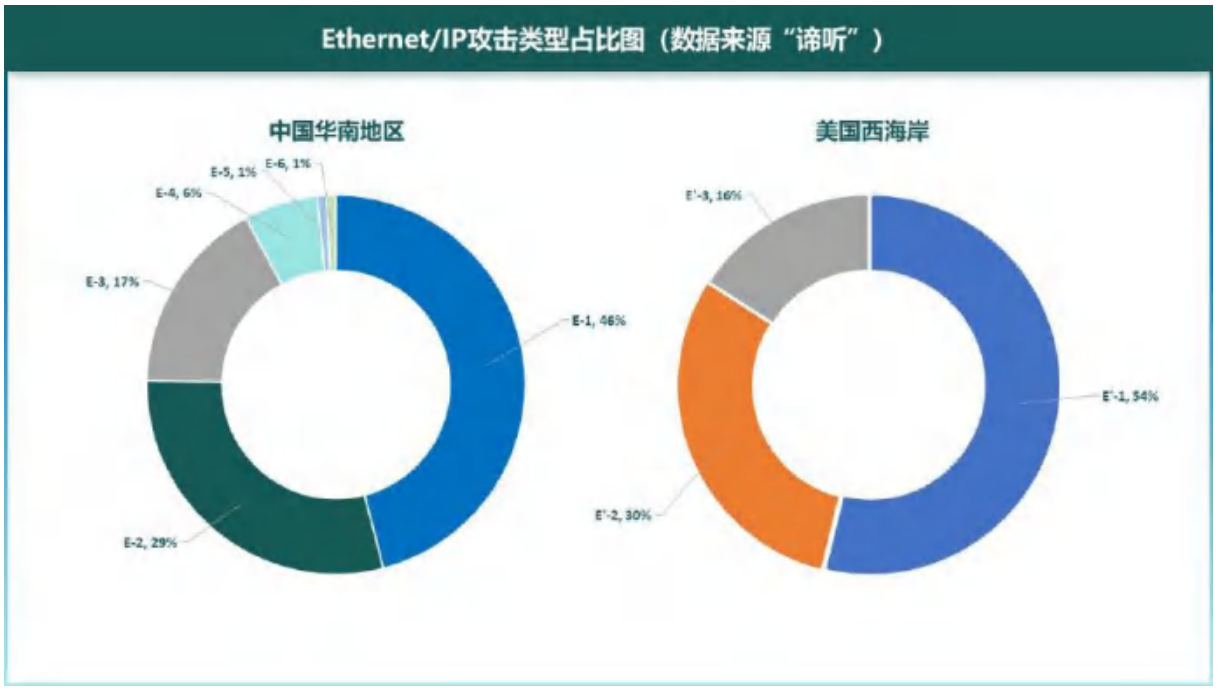

图 6-4 Ethernet/IP 协议攻击类型占比图（数据来源“谛听”）

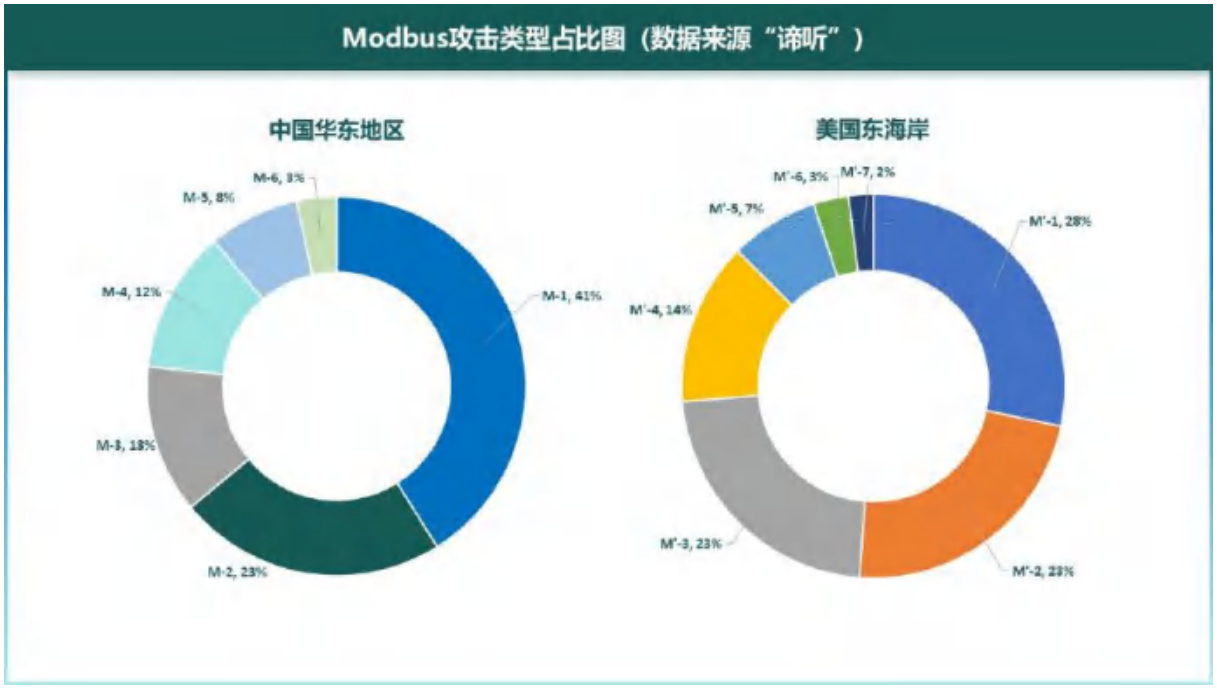

图 6-5 Modbus 协议攻击类型占比图（数据来源“谛听”）

Ethernet/IP 协议蜜罐部署地区为中国华南地区和美国西海岸，两地区的经济发展迅速，高新技术产业发达，各种网络活动较频繁。蜜罐部署在经济科技发达地区，便于收

集更多、更详细的攻击信息。由图 6-4 可知，中国华南地区的 Ethernet/IP 协议蜜罐捕获的攻击流量主要采用的攻击类型为 E-1、E-2、E-3，其中 E-1 约占所捕获总流量的一半。美国西海岸地区的 Ethernet/IP 协议蜜罐捕获的攻击流量采用 E'-1、E'-2、E'-3 三种攻击类型，其中，E'-1 以 54%的高占比成为该地区 Ethernet/IP 协议蜜罐捕获的攻击流量的主要攻击类型。由此可见以上攻击类型是对 Ethernet/IP 协议蜜罐进行攻击的主要手段。

Modbus 协议蜜罐部署地区为中国华东地区和美国东海岸，二者均为工业发达地区，蜜罐部署在该地区便于伪装隐藏，且易于收集更多的攻击信息。由图 6-5 可知，中国华东地区的 Modbus 协议蜜罐捕获的攻击流量主要采用的攻击类型为 M-1、M-2，其中 M-1 占到了 41%。美国东海岸 Modbus 协议蜜罐捕获的攻击流量主要采用的攻击类型为 M'-1、M'-2、M'-3，且相互之间占比差距较小。由此可见以上攻击类型是对 Modbus 协议蜜罐进行攻击的主要手段。本团队对 Ethernet/IP 和 Modbus 的 ICS 网络流量进行了解析、建模、评估，但其中还存在部分未知的攻击类型，针对未知的攻击类型还需进一步的研究，以便提供有效的 ICS 流量检测与攻击预警，评估其潜在的攻击意图，制定针对性的防御措施。

6.4 工控蜜罐与威胁情报数据关联分析

近年来，网络安全风险持续向工业控制领域扩散，工控网络也逐渐成为网络安全的重要一环。当前工控攻击具有类型丰富、途径泛滥、追踪困难等特点，传统的被动式防御手段“老三样”——防火墙、查杀病毒、入侵检测以及针对单点的攻击取证与溯源技术难以应对高级持续性威胁（APT）、新型高危漏洞等复杂安全威胁，而以威胁情报（TI）为基础的分析技术能够收集整合全球范围内的分散攻击与威胁，进而采取智能化的攻击响应措施，实现大规模网络攻击的防护与对抗，本团队也对 2022 全年采集到的大量威胁情报及蜜罐数据进行了关联分析。

由“谛听”网络安全团队开发并于 2021 年 2 月上线的威胁情报搜索引擎（https://www.TItecting.com）是基于“谛听”威胁情报中心而研发的应用服务。威胁情报中心存有海量威胁情报数据，提供全面准确、内容详细的相关决策支持信息，为行业系统安全提供保障。面对复杂的攻击形式和不断迭代的攻击手段，建立完善的威胁情报搜

索引擎刻不容缓，旨在为工业、企业、组织以及个人提供更加全面的情报信息，打造以威胁情报平台为基石的网络安全空间。

2022 年“谛听”蜜罐和威胁情报中心均采集到大量新数据，为探寻数据间潜在的相关性，“谛听”团队计算威胁情报数据和蜜罐数据的重叠部分，并根据攻击类型的不同将数据分为 5 类。其中包括代理 IP（proxy）、命令执行与控制攻击（command execution and control attacks）、恶意 IP（reputation）、垃圾邮件（spamming）和洋葱路由（tor）。每种类型数据与蜜罐数据重叠部分在二者中的占比如图 6-6，本团队对该图的分析如下。

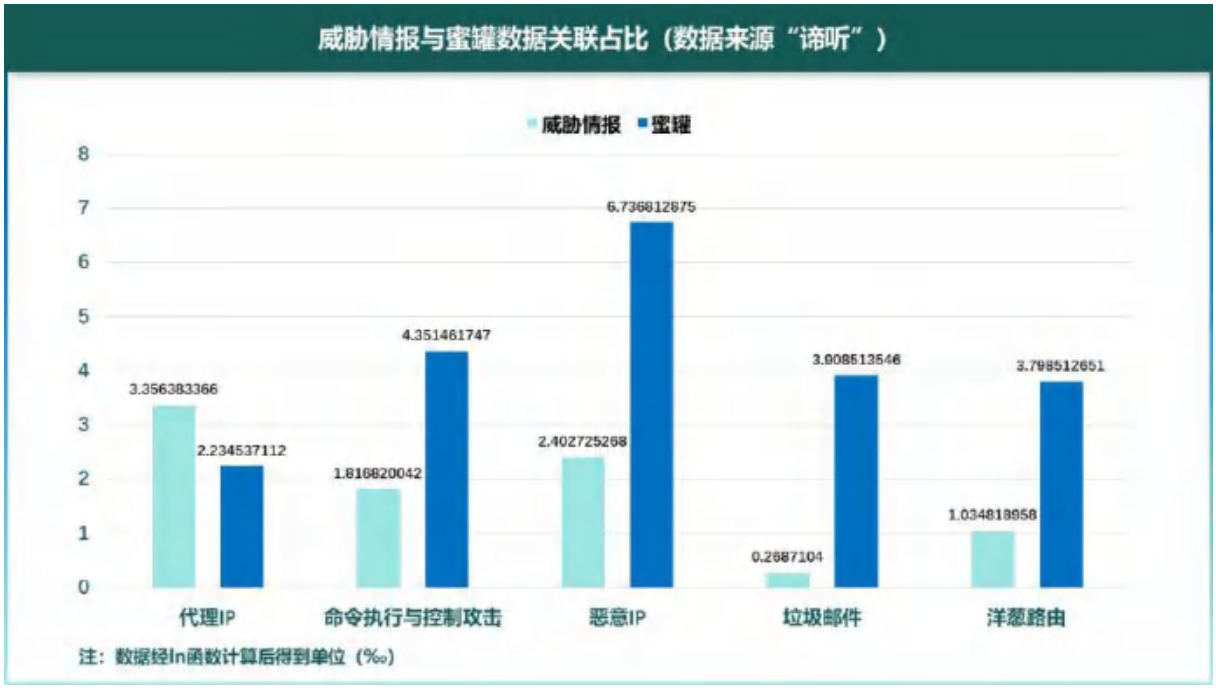

图 6-6 威胁情报与蜜罐数据关联占比（数据来源“谛听”）

图 6-6 中威胁情报数据来源于“谛听”威胁情报中心，该系统所记录的数据为安全网站或安全数据库中的情报数据，本团队根据情报数据攻击类型不同分别记录在不同的数据表中。而直接在部署在国内外网络节点上的工控蜜罐通过模拟暴露在互联网上的工业控制设备，开放设备对应工业网络协议端口吸引攻击者，在记录每一次攻击者的攻击信息的同时，监听捕捉流经此节点的网络流量，以保证攻击信息的真实性与可用性。因此，图中威胁情报数据与工控蜜罐数据有重叠的部分表示情报中心收集到的 IP 地址确实发生了工控攻击，这可以让系统更有针对性的对攻击进行防御。下面对具体的数据进行分析。

首先，与 2021 年类似，2022 年占蜜罐数据最多的攻击类型依然是“恶意 IP”，达到了 6.737‰（经过 ln 函数计算后），本团队认为发起代理 IP、命令执行与控制攻击、垃圾邮件和洋葱路由攻击的攻击者 IP 在主观上均可以标识为“恶意 IP”，这可能是“恶意 IP”的关联占比最高的原因，未来工控产业可能需要更加严格地细分“恶意 IP”的认证标准，将工控网络中的“恶意 IP”概念与其他网络作准确的区别。

其次，与 2021 年仅“洋葱路由”在蜜罐数据中的关联占比排名第二不同的是，今年“命令执行与控制攻击”、“垃圾邮件”与“洋葱路由”的关联占比相差不大，可以视为紧随“恶意 IP”之后均排名第二。本团队猜测，基于 Tor 网络协议内部固有的脆弱性特征且目前相关研究并不成熟的现状，工控系统在设计时可能就会避免部署 Tor 网络结构，这就使得工控攻击者失去攻击目标而采取其他类型的攻击方式，其中可能就包括“命令执行与控制攻击”与“垃圾邮件”，当然工控系统安全人员也不能对“洋葱路由”攻击掉以轻心。

最后，通过“代理 IP”进行攻击的情报数量在蜜罐数据中占比最小，本团队猜想：代理 IP 是一种特定的 IP 地址，用户购买代理 IP 并不代表可以随意使用，一般情况下会有特定的管理人员对代理 IP 进行管理，一旦发现某用户频繁通过该 IP 进行攻击，管理人员会对该 IP 进行回收，不再授予使用权；同时目前针对“代理 IP”攻击的防护方案较为成熟，攻击者倾向于使用多种方式对工控系统进行立体攻击。

6.5 工控网络探针

6.5.1 数据处理之 Honeyeye

随着网络信息技术的飞速发展，互联网与工业融合创新不断推进，通信、金融、交通、能源等基础行业设施日益依赖于网络，并逐步与公共互联网连接。随之而来的是工业领域逐渐成为网络攻击重灾区，工业互联网安全防护急需加强与提升。

网络探针是一个用于捕获、分析网络数据包的组件，在确保网络信息产业的安全可控中有着重要的意义。由“谛听”网络安全团队研发的 Honeyeye 工控网络探针支持对 30 余种工控协议解析的同时，亦可进行数据预处理。

分析网络特征与行为是实现工控安全中一个重要的环节，因此获得有效且易于分析的数据至关重要。PCAP 文件被广泛应用于网络流量存储，但因其文件格式是二进制格

式，可读性较差。相较于现有的网络流量捕获系统（如 TCPDump、Windump 和 Wireshark）只将捕获的原始二进制数据保存在 PCAP 文件中，Honeyeye 能够将捕获的数据转换为所需格式对外输出。

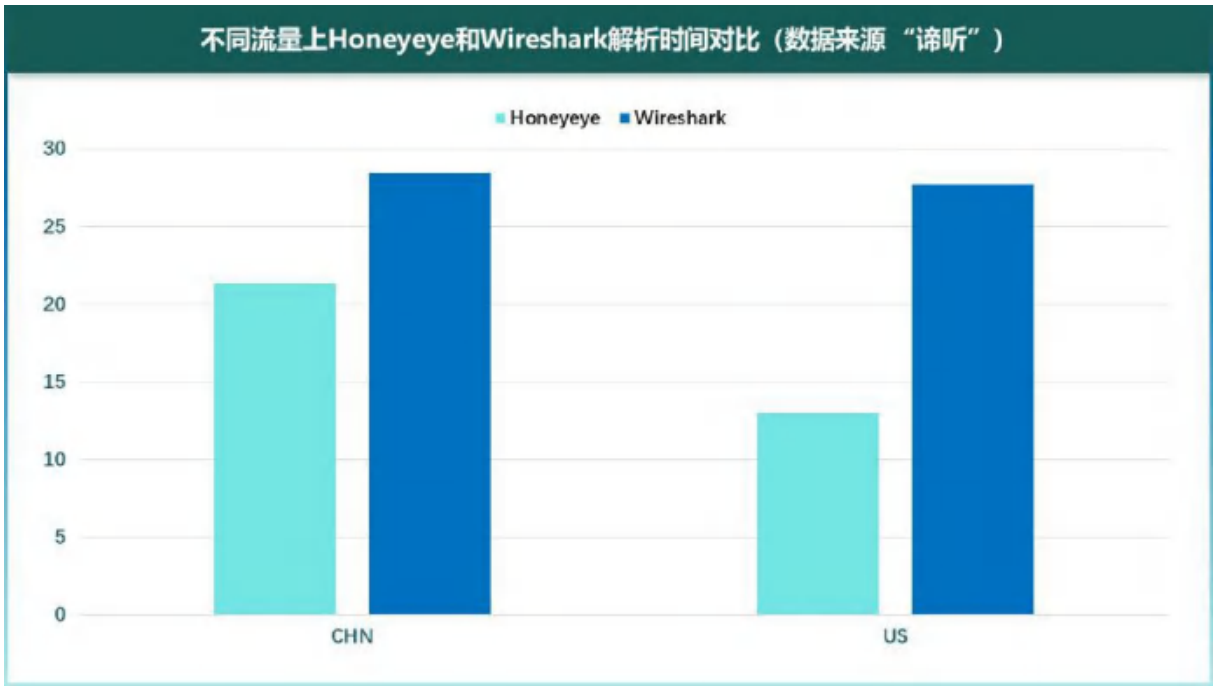

图 6-7 不同流量上 Honeyeye 和 Wireshark 解析时间对比（数据来源“谛听”）

从图 6-7 可以看出，相较与主流的网络流量解析工具 Wireshark，本团队所研发的探针 Honeyeye 解析速度更快。Honeyeye 可以捕获流量以及导入 PCAP 文件作为输入进行解析，输出结果以 Json 格式保存及传输到远端服务器，从而易于人阅读和编写，同时也易于机器解析，为下一步分析提供支撑。此外，Honeyeye 可以作为插件被其他框架所整合，从而提高 Honeyeye 的可用性。

未来，本团队将继续致力于 Honeyeye 的改进，包括但不限于改进框架跨不同系统和网络运行的能力，以及收集防火墙日志和攻击者击键操作等其他信息的能力。

6.5.2 网络安全态势可视化

利用 Honeyeye 输出的数据进行网络安全态势可视化为用户监控网络环境、发现网络异常、定位故障节点等提供了便利。

本团队所开发的网络安全态势可视化系统中主要包括设备监测、流量统计以及带宽变化等模块。其中设备监测对 CPU 和内存使用率、设备 IP 以及部署时间等信息进行展示，能够帮助用户掌握系统运行状态，减少突发事件，一定程度上提高运维效率。流量统计中的总体流量统计有助于用户从宏观上了解近期流量变化；而实时流量统计能够展示每秒的流量变化趋势，并显示上下限之外的异常流量，以便定位异常。重要网络设备的带宽变化可以有效检测可疑网络活动，进而为网络安全提供保障。

目前，网络安全态势可视化还是一项刚刚发展的技术，通过可视化图形方式将网络中蕴含的态势展示给用户，方便用户对网络异常的检测、预防及处理。未来，基于大数据和人工智能的网络安全态势需要进一步探索，从而获得并展示更多、更深层次的数据，最终协助网络安全管理人员实现网络安全智能化管理。

7. 工业互联网安全创新发展

随着近年来技术的发展，工业互联网的应用越来越广泛。工业互联网（Industrial Internet）是新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业生态，通过对人、机、物、系统等的全面连接，构建起覆盖全产业链、全价值链的全新制造和服务体系，为工业乃至产业数字化、网络化、智能化发展提供了实现途径，是第四次工业革命的重要基石。工业互联网不是互联网在工业的简单应用，而是具有更为丰富的内涵和外延。它以网络为基础、平台为中枢、数据为要素、安全为保障，既是工业数字化、网络化、智能化转型的基础设施，也是互联网、大数据、人工智能与实体经济深度融合的应用模式，同时也是一种新业态、新产业，将重塑企业形态、供应链和产业链[7]。

近年来，工业化与信息化的深度融合使得互联网与工业控制系统相结合，改变了传统工业控制系统封闭的环境。在享受互联网便利的同时，工业领域也同样开始面临互联网的安全威胁。远在千里之外的黑客可以通过互联网，攻击原本封闭的工业控制系统，这使得网络型攻击可以直达生产现场，造成生产中断甚至威胁工作人员的生命安全。例如 2022 年 1 月 29 日，位于荷兰阿姆斯特丹和鹿特丹、比利时安特卫普的几处港口因遭到勒索软件的攻击，石油装卸和转运受阻，至少有 7 艘油轮被迫在安特卫普港外等候，无法靠港。同月，黑客组织勒索攻击铁路相关基础设施，试图谋求政治诉求。网络攻击带来的巨大利益诉求让工业领域面临严峻的安全挑战。

目前的工业互联网安全技术大体分为安全防护技术、安全评测技术、安全监测技术。首先，工业互联网安全防护技术是对工业互联网各层级部署边界控制、身份鉴别与访问控制等的技术措施，是工业互联网安全技术的核心。工业互联网安全评测技术是采取技术手段对工业互联网各层级的安全防护对象进行测试和评价，了解其安全状态，从而增强防护能力，主要包括漏洞扫描、漏洞挖掘、渗透测试等技术。工业互联网安全监测技术就是通过技术手段实现对各层级的安全威胁的发现识别、理解分析、响应处置，主要包括安全监测审计、安全态势感知等关键技术。随着相关安全技术的发展，未来工业互联网行业的安全性会愈来愈好。

据目前情况来看，我国发展工业互联网有优势也有缺点，可以说是机遇与困难并存。从优势上来讲，一是我国有着一定的工业基础，自 19 世纪第一个五年计划起，我国就开始了工业化建设，这也让我国工业门类齐全；二是市场需求充足，我国作为世界第二大经济体，有着极大的市场需求，很多东西都能自产自销；三是拥有相应的网络配置以及政策倾向，我国 5G 的研发处于世界领先水平，5G 的覆盖率使得我们拥有很好的网络配置。与此同时，我国政策一直都是科技导向，发展以工业互联网为基础的高新技术产业。四是我国人口众多，14 亿的人口基数能让我们拥有庞大的人才资源储备。相应的，有优势就有缺点，一是思想观念上的挑战，当今社会科学技术日新月异，这要求我们从业者有破釜沉舟的勇气，有敢为天下先的担当，从业者要敢于走出舒适圈，将互联网融于传统工业企业中，积极响应国家号召，适应当前飞速发展的时代。二是商业模式的挑战，工业互联网相对于传统工业还是小众行业，国内目前还没形成统一的评价标准，社会各界认知不统一；三是关键技术的挑战，我国工业互联网平台产业空心化问题是一道迈不过的难关，目前国内很多工业互联网平台都是基于国外基础产业体系而建立的。虽然我国很多技术已实现弯道超车，但仍有许多被卡脖子的技术需要攻克。核心技术必须掌握在自己手里，这是不可退步的原则问题。

7.1 工业互联网与智能制造

智能制造与工业互联网二者密不可分，相辅相成。根据工业互联网产业联盟（Allianceof Industrial Internet，AII）发布的《工业互联网术语与定义》，智能制造（Intelligent Manufacturing，IM）包含了智能制造技术和智能制造系统两方面。而智能制造的实现主要依托两个基础能力，一个是工业制造技术，主要包括了先进装备、先进材料和先进工艺等，工业制造技术是决定制造边界与制造能力的根本；另一个就是工业互联网。工业互联网包括智能传感控制软硬件、新型工业网络、工业互联网平台等，是充分发挥工业装备、工艺和材料潜能，提高生产效率、优化资源配置效率、创造差异化产品和实现服务增值的关键[8]。

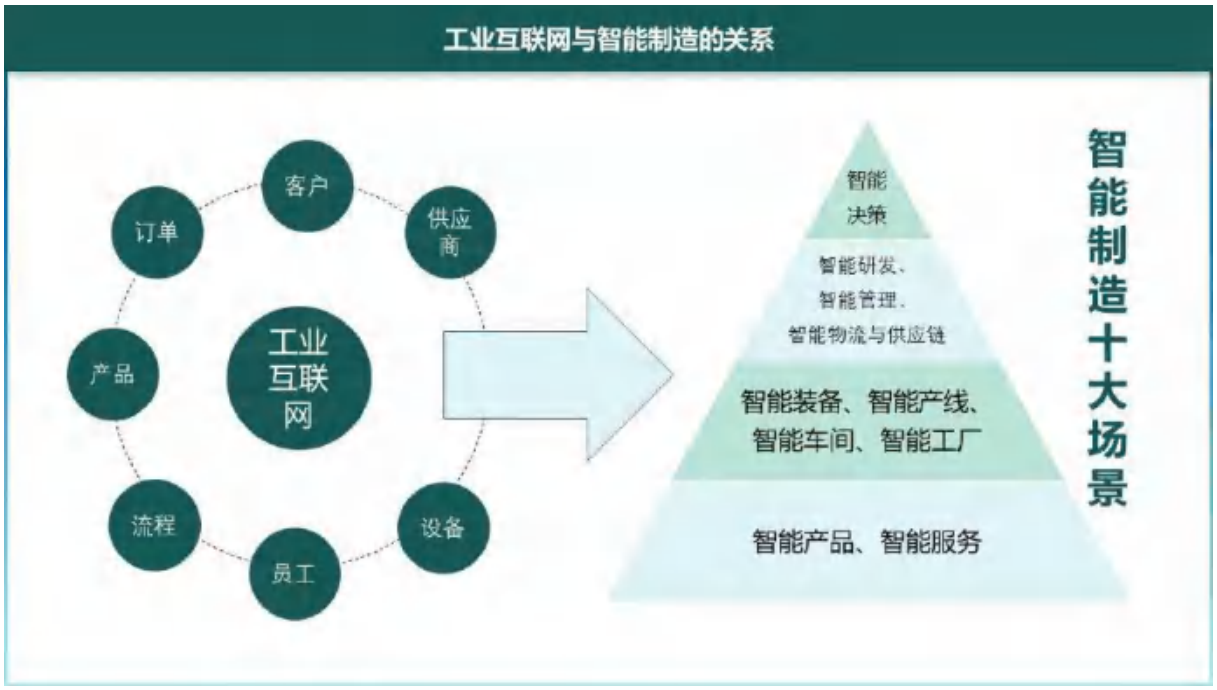

图 7-1 工业互联网与智能制造的关系[9]

工业互联网是实现智能制造的基础，工业互联网主要通过五大技术来支持实现智能制造，包括工业软件技术、工业网络技术、工业平台技术、工业安全技术、工业智能技术[9]。智能制造依托工业互联网发展的同时，反过来也推动着工业互联网的改造与升级。制造自动化、智能化的宏伟目标，也在不断促进着工业互联网朝高速度、低延迟的方向发展。

自工业互联网相关概念被提出以来，实现智能制造就一直是人们谈论的热点话题。而如今随着人工智能、大数据等新兴互联网技术的突破，更是为智能制造的实现提供了新的可能性。2021 年 12 月，工业和信息化部、国家发展改革委、教育部、科技部、财政部、人力资源社会保障部、市场监管总局、国资委等八部门联合发布了《“十四五”智能制造发展规划》，《“十四五”智能制造发展规划》中对我国智能制造的现状与形势、未来发展的重点任务等方面进行了详细的阐述，其中更是提出到 2035 年相关国家重点骨干企业基本实现智能化的宏伟目标。

7.2 工业互联网与产业数字化转型

产业数字化转型是利用数字技术进行全方位、多角度、全链条的改造过程，是利用数字技术破解企业、产业发展中的难题，重新定义、设计产品和服务，实现业务的转型、创新和增长[10]。产业数字化转型对推动我国经济高质量发展具有重要意义。

十九大以来，我国不断推动工业互联网创新战略走深走实，与我国的产业发展相互适应、齐头并进。《工业互联网创新发展行动计划（2021-2023 年）》确立了未来三年我国工业互联网发展目标：到 2023 年，新型基础设施进一步完善，融合应用成效进一步彰显，技术创新能力进一步提升，产业发展生态进一步健全，安全保障能力进一步增强[11]。目前，工业互联网创新进入高速发展阶段，我国正加快工业互联网与制造业融合的脚步，充分发挥我国的人才优势、市场优势及制造业优势，深化工业互联网与重点企业、集团的合作。产学研紧密结合，工业互联网新技术相继落地，在企业维护、工厂监管、生产技术、销售渠道等方面为企业提供优秀的数字化转型方案。工信部最新统计数据显示，截至 2022 年上半年，工业互联网高质量外网覆盖全国 300 多个城市。“5G+工业互联网”全国建设项目 2022 年第二季度新增 700 个，累计已超过 3100 个。(数据来源[12])

如今，工业互联网平台已经成为产业升级的关键组成、数据交互的集散地、政府与产业的沟通桥梁、拓展市场的重要途径。近年来，工业互联网带动国民经济迅猛发展，影响力显著提高。至 2022 年 8 月，工业互联网已经全面融入 45 个国民经济大类(数据来源[12])，工业互联网实现了产业的增速增效，也助推了全产业链的协同高效运转，是实现产业链数字化和智能化的基础。工业互联网创新逐渐成为我国产业数字化转型升级、建设制造强国和构建发展新格局的主要切入点，为推动经济高质量发展提供动力。

现阶段，工业互联网还需要融入更多行业，巩固跨界合作，提高深度与广度，为其他行业提供技术、方案支持，推进产业数字化全面向好发展。在未来，工业互联网创新将会继续带动我国产业的迭代创新，提升我国产业的核心竞争力。

7.3 工业互联网与典型工业环境

7.3.1 工业互联网与电力行业

电力系统作为重要的工业基础设施之一，便利了人民日常生活，也对社会稳定起到重大作用，由于电网系统的脆弱性和低攻击容忍性，一旦电力系统受到攻击，会对国家安全，人民安全产生巨大威胁。一些不法分子通过网络攻击来损害电网系统达到扰乱社会的目的。2019 年 3 月，黑客组织利用电力系统漏洞对美国可再生能源电力 SPower 公司发动 DDos 攻击，攻击导致控制系统与太阳能和风力发电设备之间通讯中断。2020 年，巴西电力公司 Light S.A 遭黑客入侵系统，并被勒索 1400 万美元的赎金。

随着信息化电网的建设，各种电力设备以网络为媒介互联互通，工业控制系统的开放程度越来越高，在为工业生产带来极大推动的同时，也减弱了电力工业控制系统与外界的隔离，致使外界攻击者可以通过互联网来攻击电网。

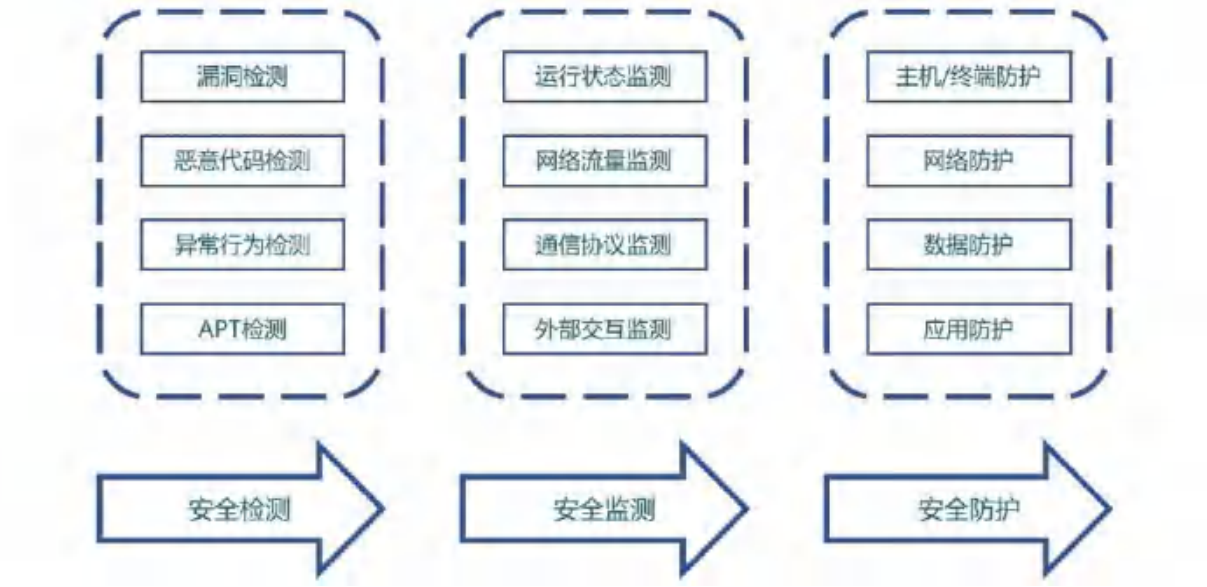

图 7-2 电力工业控制系统的安全防护体系[13]

2009 年我国正式提出“智能电网”的概念，意图建设信息化，自动化的坚强智能电网，近年来已经成为了国家电网的主要发展方向。2022 年 7 月，发改委、住建部印发《“十四五”全国城市基础设施建设规划》，其中提到开展城市韧性电网和智能电网建设。

智能电网也被称作“电网 2.0”，是电网的智能化，是世界电力产业发展的体现，也是新能源发展实施的重要基础，具有智能化的信息架构，通过先进的测量技术、控制方法、决策系统，可以为人民提供安全、经济、环保的电力服务，其应具有高度的可自愈性，抵御攻击以及满足所有用户的用电需求。

随着工业互联网和传统电力系统的发展融合，需要加大对电网安全问题的注意，时刻防范针对电网的恶意攻击，守护国家安全。

7.3.2 工业互联网与能源行业

能源产业是国民经济的重要基础工业，关系到国家战略储备，百姓日常生活。“重资产、资源型”的特点决定了其实践工业互联网的必要性和创新性。能源行业在自动化、信息化等方面已经有了一定程度的普及，PLC、传感器、DCS 等较为完善[14]。

能源行业连续生产需要设备高可靠、安全运行，通过技术手段优化运行效率、实现节能降耗更是核心的工业需求[14]。工业互联网能够有效地满足上述需求，通过实时监测设备状态从而保证设备的可靠性、易控制性，设备不间断运行产生海量的工业时序数据在分析故障、分析产能以及分析能耗等方面起到重要的作用。

石油被称为工业血液，是国家生存和发展必不可少的资源。从当前形势来看，石油行业在满足其他行业对于石油需求的同时，得到的经济效益是有限的。此外，在“双碳”背景下，如何在石油开发中减少碳排放实现绿色开发，也是一个值得考虑的问题。工业互联网的引入能够有效地节约石油行业中的物耗成本、人员成本、时间成本，进而提高石油行业的经济效益。同时，对于设备的实时监测可以实现排污主动处理，从源头上解决部分的污染问题。因此，与工业互联网结合是越来越多石油企业的必然选择。

工业互联网的高速发展推动煤炭行业生产管理方式改革，并为煤炭行业发展助力。我国煤炭行业的变革已经从机械化走向了今天的自动化，但这并不意味着我国煤炭行业已无发展空间，各系统间协同合作程度低，不同技术难以整合等问题的解决需要工业互联网的支持。工业互联网的应用可实现实时掌控作业环境情况、提高设备工作效率、保障矿井工人安全等。但就目前来看，我国煤炭工业互联网还处于前期，未来技术创新、与煤炭行业适配任重而道远。

在新能源迅速发展的背景下，工业互联网的价值得到进一步地体现。构建新能源体系不仅是社会主义现代化强国的必然要求，同时对实现“双碳”目标意义重大[15]。然而，新能源开发利用仍存在一些制约因素，比如新能源各类设备种类杂、多系统间存在数据壁垒等问题[16]，这与工业互联网的主攻方向恰恰契合。工业互联网的应用能够通过设备的自我监测和报备，将以往设备定期维护和检修转向预防为主的维护方式，从而降低了设备突发宕机的概率。此外，当设备发生故障时，工业互联网能够通过实时数据上报，快速定位告警、故障节点，达到缩短维修周期的效果。

纵观整个能源行业，工业互联网在实现降低能耗、智能管理、提高效率，最终达到降本增效的过程中起到至关重要的作用。但也因此，能源行业成为网络攻击重灾区，随着与工业互联网合作的持续深入，越来越多的网络安全问题也会接踵而至。所以，在能源行业应用工业互联网的过程中，需要考虑可能存在的网络安全问题以及注重网络安全防护。

7.3.3 工业互联网与交通行业

工业互联网快速发展，逐渐与传统工业行业进行融合旨在推动传统工业向数字化与智能化方向转化，在交通基础设施建设行业也有所体现。在工业互联网的辅助下，交通基建企业可以设计协同管理等应用来提高施工质量、生产安全水平等，将工业互联网融合至工业生产过程以及运行管理模块，利用新型信息技术弥补传统工业模式上的不足，提高企业整个生产的效率并保障生产过程的安全。

在城市交通的地铁领域中，工业互联网已应用于地铁综合监控系统的搭建，该系统包含中央综合监控系统以及车站综合监控系统，并由综合监控系统骨干网连接而成。中央综合监控系统致力于保证交通各线路上的各车站的各个子系统都能够处于正确的运行状态并正确实现中心级下达的操作控制功能指令，该系统被安装于线路控制中心处；车站级监控网则是具有双冗余高速交换特点的以太网，其数据传输速率可以高达100Mbit/s 或 1000Mbit/s。图 7-3 则为一个典型的综合监控系统架构示例图，该系统构建在广域网上，也是地理分散的大型 SCADA 系统。

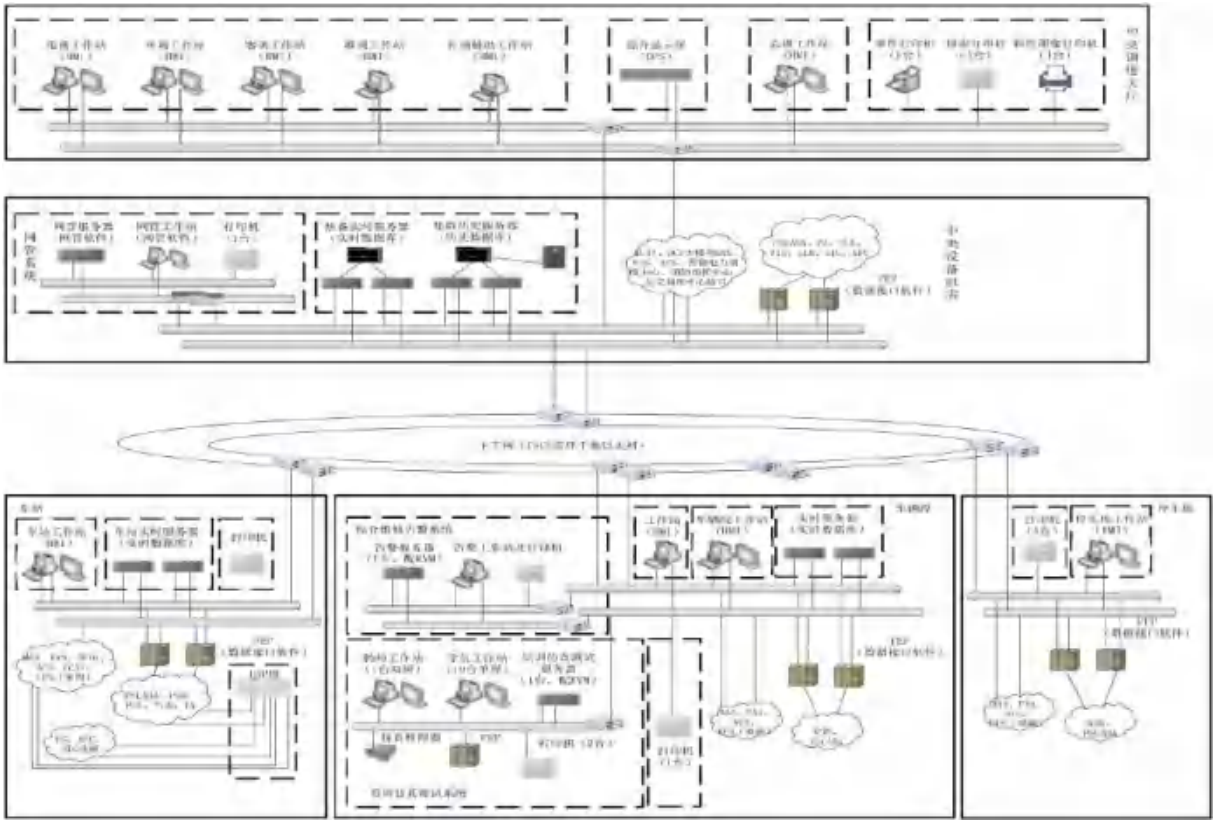

图 7-3 典型的综合监控系统架构图[17]

随着工业互联网在交通领域的快速发展，其也存在着安全责任边界模糊、安全防护意识不足等问题。因此在交通工业环境中，解决城市轨道交通信息系统、地铁综合监控系统以及公交管家系统等的安全问题的意识在不断增强，解决措施也在不断完善。以城市轨道交通信息系统为例，在工业互联网的介入后，该系统需要着重对防病毒软件以及防火墙这两个安全设备进行加强防护，并注意及时升级防病毒软件的病毒库，以防出现恶意病毒入侵、系统外的非授权访问等一系列网络安全问题。

工业互联网应用在交通领域后，可以实现行业数据共享交换、地铁运行自动化以及智能化等，推动了这个领域的发展以及进步。与此同时，使得该领域也面临一定的信息安全风险，例如网络安全责任边界不清晰、信息泄露以及数据窃取风险增加、工业互联网设备长期遭受恶意攻击、工业互联网软件设备更新慢以及漏洞无法及时修补等安全风险。因此，在提高网络安全意识以及技术的基础上，也需要不断根据实际情况来拟定和出台相关战略或有针对性的信息安全政策来辅助解决一系列潜在或待解决的信息安全的问题。

8. 总结

2022 年党的二十大报告对推进新型工业化、构建现代化基础设施体系做出重大战略部署。工业互联网作为构建工业环境下人、机、物全面互联的关键基础设施[18]，已经连续五年写入政府工作报告，被明确为重点发展的任务之一，加强工业互联网安全防护的重要性日益凸显。为贯彻落实《中华人民共和国网络安全法》等法律法规，国家标准化管理委员会发布了《信息安全技术 关键信息基础设施安全保护要求》。同时，我国在 2022 年相继推出了一大批工业互联网信息安全相关的政策法规及报告，以保证工业互联网高质量发展。

随着工业互联网应用范围的不断扩大，工控领域面临的安全风险不断增加。2022 年工控安全事件频发，各类网络攻击威胁持续上升。这些攻击行为涉及到各行各业，给个人、企业、国家带来了不同程度的损失。值得注意的是，针对关键基础设施的攻击呈现上升态势，加强关键基础设施安全工作刻不容缓。基于以往的工控安全形势，工控系统行业漏洞数量呈逐年下降的趋势。相比于 2021 年，全球在工控设备暴露数量方面的排名除前两名外发生了较为明显的变化，各国工控设备暴露数量有所回升。通过威胁情报和蜜罐数据的关联分析，进一步体现了威胁情报在工控网络安全领域中具备极高的应用价值。

万物互联时代，工业互联网的发展与普及无论从政策制定层面还是实际落地层面都得到了国家的大力支持。建立安全保障体系，提高安全防护水平，对工业互联网的创新发展具有重要意义。在未来，工业互联网将持续为智能制造与产业数字化转型赋能，促进与各行业的融合创新应用，为推进新型工业化、构建现代化基础设施体系提供强劲动力。

人工智能产业链联盟

星主： AI产业链盟主

知识星球

微信扫描预览星球详情

参考文献

[1] 国家信息安全漏洞共享平台工业控制系统漏洞列表[EB/OL].https://www.cnvd.org.cn/flaw/typelist?typeId=38.

[2] 国家信息安全漏洞共享平台工控漏洞子库[EB/OL].https://ics.cnvd.org.cn/index.

[3] 《中国工业经济发展形势展望（2022年）》发布：重点行业运行稳健,表现出较强韧性[EB/OL].https://m.gmw.cn/baijia/2022-11/25/36188775.html.

[4] 长三角工业互联网峰会在合肥举行，专家代表共话工业互联网发展新趋势[EB/OL].https://baijiahao.baidu.com/s?id=1750020167651651422&wfr=spider&for=pc.

[5] 辽宁工业互联网进入新发展阶段[EB/OL].https://baijiahao.baidu.com/s?id=1747904920330529308&wfr=spider&for=pc.

[6] 2022全球工业互联网大会在沈阳盛大开幕[EB/OL].https://baijiahao.baidu.com/s?id=1748985030614262442&wfr=spider&for=pc.

[7] 工业互联网（概念）[EB/OL]. https://baike.baidu.com/item/%E5%B7%A5%E4%B8%9A%E4%BA%92%E8%81%94%E7%BD%91/8413475?fr=aladdin.

[8] 中华人民共和国国家互联网信息办公室.工业互联网你知道多少.[EB/OL].http://www.cac.gov.cn/2018-03/28/c_1122602167.htm?from=singlemessage.2018-3-28.

[9] 工云智慧.一文读懂智能制造与工业互联网的区别.[EB/OL]. https://zhuanlan.zhihu.com/p/353753658.

[10] 产业数字化转型是什么意思[EB/OL].https://worktile.com/blog/know-1293/

[11] 《工业互联网创新发展行动计划（2021-2023年）》解读[EB/OL].http://www.gov.cn/zhengce/2021-02/18/content_5587565.htm.

[12] 工业互联网：制造业数字化转型重要力量[EB/OL].https://www.ncsti.gov.cn/kjdt/ztbd/xzjj/szjjrc/gyhlw/202208/t20220818_94146.html.

[13] 应欢,刘松华,韩丽芳,缪思薇,周亮.电力工业控制系统安全技术综述[J].电力信息与通信技术,2018,16(03):56-63.DOI:10.16543/j.2095-641x.electric.power.ict.2018.03.009.

[14] 毛旭初.能源行业工业互联网发展的核心是工业智能化[EB/OL].http://iiot.cechina.cn/21/0408/08/20210408085918.htm.2021-4-8.

[15] 陈洪波.构建新型能源体系的战略意义[J].上海企业,2022(12):84.

[16] 顾维玺,王为民.构建国家级新能源工业互联网平台[EB/OL].https://paper.cnii.com.cn/article/rmydb_16240_312934.htm

[17] 典型工业领域的工业控制网络[EB/OL].https://www.jianshu.com/p/dbfa1925109f?ivk_sa=1024320u.

[18] 工业互联网网络建设及推广指南[Z]. 工业和信息化部, 2021.

“谛听”网络安全团队简介

“谛听”网络安全团队，由东北大学姚羽教授带领课题组师生组建，依托复杂网络系统安全保障技术教育部工程研究中心，被辽宁省工信委授予“辽宁省工业信息安全支撑单位（首批）”，包括 3 名博士，7 名博士研究生，23 名硕士研究生。团队的研究方向为工业互联网安全，重点研究内容主要包括工业互联网安全测绘、工业流量探针、工业流量异常检测、工控蜜罐/蜜网、威胁情报、工业安全态势感知等。课题组发表学术论文 50 余篇，专利 8 项，软件著作权 2 项，主编国内首部工业信息安全专著《工控网络安全技术与实践》，获省部级以上科技奖励二项、中国国际互联网+大学生创新创业大赛国奖及省级金奖、“挑战杯”辽宁省大学生创业计划竞赛金奖、中国高校计算机大赛网络技术挑战赛特等奖、ChinaVis 数据可视化分析挑战赛一等奖等，制定国家、地方标准 3 项，连续 6 年发布《工业控制网络安全态势白皮书》。

东北大学 | 谛听网络安全团队