匡恩网络

2016 年工业控制网络安全态势报告

北京匡恩网络科技有限责任公司

2016 年 12 月

目 / 录

前言

随着物联网技术的迅猛发展，工业控制系统已由原来相对封闭、稳定的环境变得更加开放、多变。乌克兰电网事件后，世界各国已经深刻认识到黑客攻击、网络病毒给工业控制系统、国家关键基础设施带来的危害。且随着互联网在工业领域的不断渗透，以及智能设备在各领域的广泛使用，工业控制系统的脆弱性在物联网世界中暴露无遗，传统工业控制系统的潜在安全性正遭受严重的挑战。

工业控制系统广泛应用于我国电力、水利、污水处理、石油化工、冶金、汽车、航空航天等诸多现代工业，其中超过 80% 的涉及国计民生的关键基础设施（如铁路、城市轨道交通、供排水、邮电通讯等）都依靠工业控制系统来实现自动化作业，随着国务院“中国制造2025”战略提出，中国工业控制领域正在发生重大的变革，两化深度融合是产业结构调整和升级转型的重要支撑，工业控制系统网络安全已经成为两化融合的重要组成部分，深刻地影响着工业控制系统及相关产业的发展，工业控制系统网络安全风险所带来的，不再仅仅是信息泄露、信息系统无法使用等“小”问题，而可能会对社会安全稳定，经济健康发展造成不可估量的影响。

为给政府部门、研究机构提供参考和借鉴，匡恩网络连续第三年撰写和发布工业控制网络安全态势报告。

本报告分为五个章节：第一章为全球工业控制系统使用情况、产品市场规模以及系统存在的漏洞，概述国际工业控制网络安全总体情况、面临的主要威胁和发展趋势；第二章对2016 年国际主要的网络安全事件进行分析总结，从中了解对工业控制系统进行网络攻击的最新手段，黑客的最新的动向；第三章介绍国际及国内工业控制网络安全治理动态，包括欧美国家在 2016 年度在政府管理、行业指导方面的政策动向，国内政府、行业协会、社会联盟及行业内重要厂商的安全动态；第四章对我国工业控制网络安全情况进行总体分析，结合匡恩网络 2016 年的行业研究成果，对影响我国工业生产安全的隐患和问题进行深入分析；第五章重点阐述匡恩网络在解决我国工业控制网络安全问题上的思考和行动，介绍匡恩网络“4+1”的工控网络安全防护理念，打造工业控制网络 PDCA 安全环及匡恩网络提供的工控安全服务等；最后第六章提出推进我国工控网络安全发展的对策和建议。

本报告可供政府部门、合作伙伴及企业客户决策参考使用。

免责声明

本报告分析数据来源于被调查单位，分析结论基于分析数据且仅对分析数据负责，北京匡恩网络科技有限责任公司不承担因以下问题引起的法律责任，具体声明如下：

1. 数据是通过现场座谈交流和被调查单位填写调查问卷两种形式获得的，对数据的准确性引起的结论出入及偏差，北京匡恩网络科技有限责任公司不承担任何法律责任；

2. 本报告严格按照调查数据分析统计结果，不带有任何形式的主观推论；

3. 由于工业控制系统在我国各行各业应用非常广泛，应用场景数量巨大，报告中分析结果可能与实际存在出入，匡恩网络对此不再澄清也不承担任何法律责任；

4. 使用者可以合法地引用本报告数据，并注明出处，但据此数据所作出的任何判断、推论和观点，均属个人行为，北京匡恩网络科技有限责任公司不承担任何法律责任；

5. 使用者在引用本报告内容时，视同完全同意本免责声明。

6. 对于本报告引用的其它文章及数据，著作权属于原版权者所有，若有问题，请与北京匡恩网络科技有限责任公司联系。

免责声明包含但不限于以上内容，北京匡恩网络科技有限责任公司保留对此报告的著作权和追究因滥用此文章内容引起的对北京匡恩网络科技有限责任公司名誉、利益损害等行为的法律责任。

第一章

全球工业控制系统安全概况

全球工业物联网安全态势依然严峻，2015 年美国 ICS-CERT 小组共收集到全球工控安全漏洞数量 427 个，其中能源、关键制造业及水和水处理是工控安全漏洞分布较广泛的行业；因各类工控安全漏洞造成的攻击事件数量达到 295 件，2010-2015 年全球工控领域安全事件呈现逐步增长态势，其中，关键制造业、能源、水处理成为被攻击最多的三个行业，占比分别达到 33%、16%、8%；攻击者的攻击手段多众多，工控设备与物联网的连接使鱼叉式攻击成为 2015 年使用最为广泛的攻击方式，占比达到 37%，给全球的网络安全环境带来了极其严重的灾难。

进入 2016 年，全球工控安全产品市场规模继续保持高速增长，工业控制系统漏洞数量持续增加，工业控制系统安全逐步向工业物联网安全演化。

1.1 工业控制系统区域分布情况

1.1.1 全球联网工控系统地域分布

当前全球各个国家的工控系统数量分布基本与本国的经济发展水平成正比，以美国为代表的西方发达国家拥有世界最先进的工业生产能力，他们所拥有的工业控制系统数量遥遥领先于其他国家和地区。下图为截止 2016 年 3 月全球接入互联网的工控系统地域分布图：

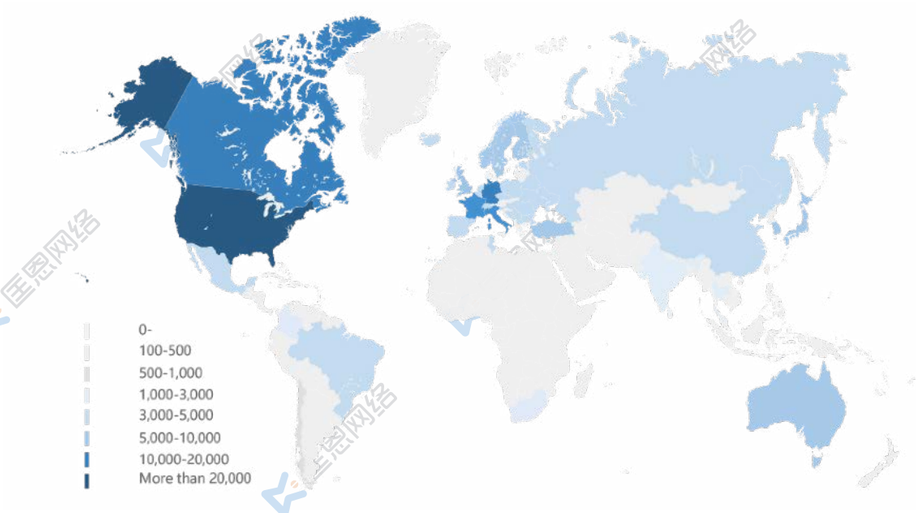


图 1 全球接入互联网的工控系统地域分布图（截止 2016 年 3 月）
数据来源 : POSITIVE TECHNOLOGIES

由上图我们可以看出全球接入互联网的工控系统中，美国的数量最多，其次是加拿大及德国、法国、意大利等欧洲国家。占比较低的地区分布在南美、非洲、亚洲等欠发达地区，部分原因是由于当地工控系统联网水平较低，不易被检测到。

1.1.2 各区域工控系统联网情况

下图显示了截止 2016 年 3 月以国家来分类的工业控制系统有效联网的分布情况。“其他”类别包括工业控制系统有效联网份额小于 1%的国家。以美国为代表的西方发达国家占据了绝对多数的份额，多数亚洲、非洲及美洲等地区的国家均属于“其他”份额中。

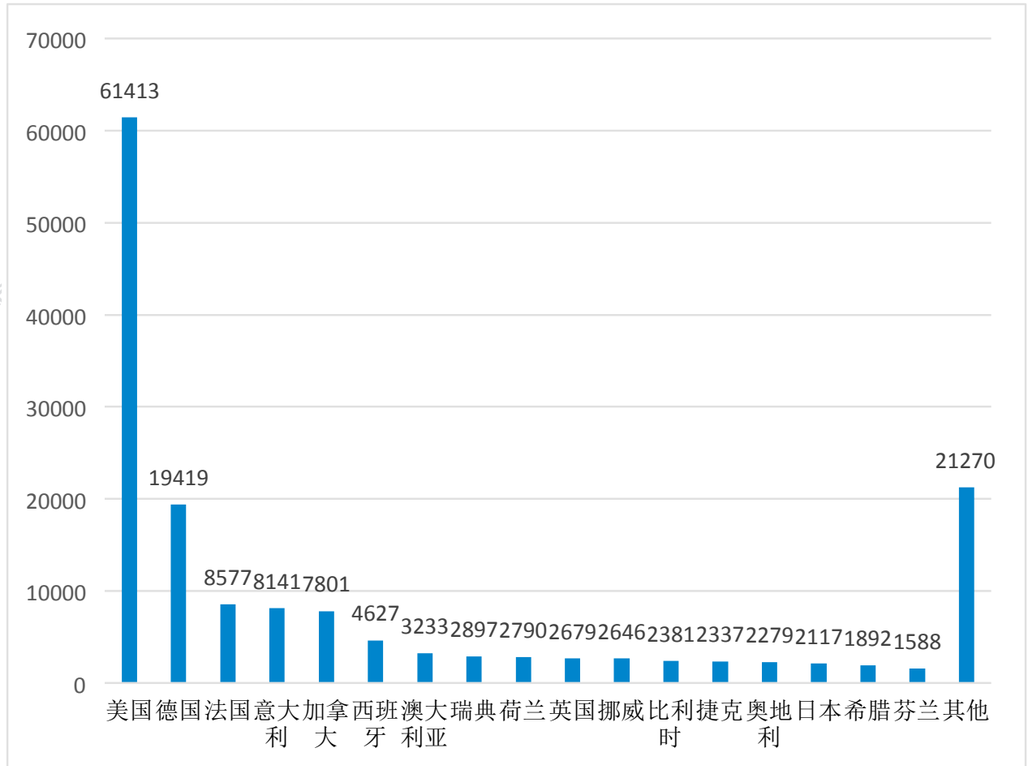


图 2 各国工业控制系统的联网数量（截止 2016 年 3 月）
数据来源：Positive Technologies

联网的工业控制系统在欧洲部分约占总额的一半，大约 40% 的份额集中在美洲，这也为欧美等发达国家工控安全事件频发埋下了隐患。

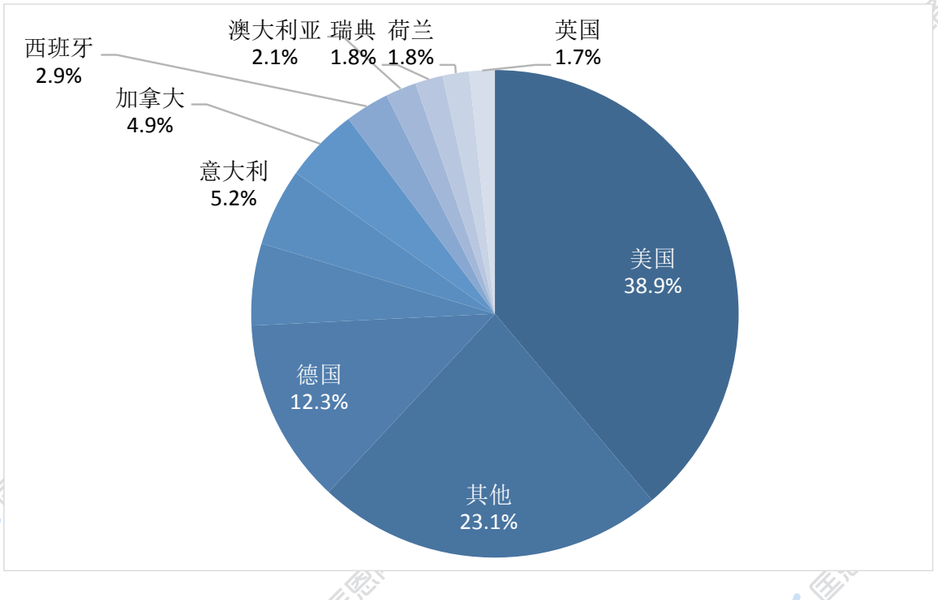


图 3 工控系统联网数量 Top10 的国家（截止 2016 年 3 月）
数据来源：Positive Technologies

1.2 工业控制系统安全市场分析

1.2.1 工控系统安全总体市场规模

研究显示，2016 年全球工业控制安全的市场规模预计将达到 71 亿美元，到 2019 年这一市场规模将达 87.49 亿美元，复合年均增长率将达 7.2%。

随着工业控制系统与互联网的不断融合，工业控制系统不可避免的暴露在网络安全威胁之下，工业控制网络的安全性、稳定性正变得越来越不可控，据惠普公司统计，当前 70% 的联网设备存在安全漏洞；IDC 预计 2016-2017 年接入物联网的软硬件设备 90% 存在一定程度的安全隐患。

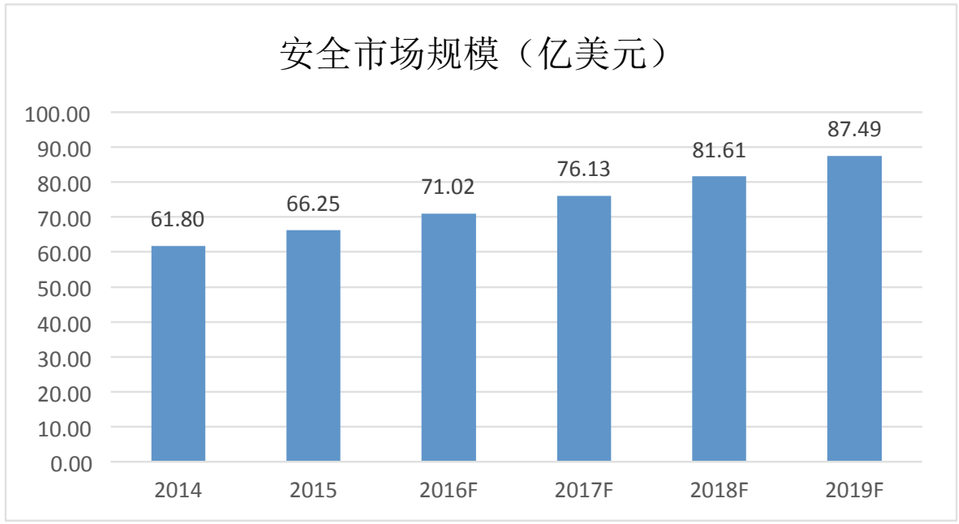


图 4 2014-2019 年全球工控安全市场规模预测
数据来源：MarketsAndMarkets、匡恩网络

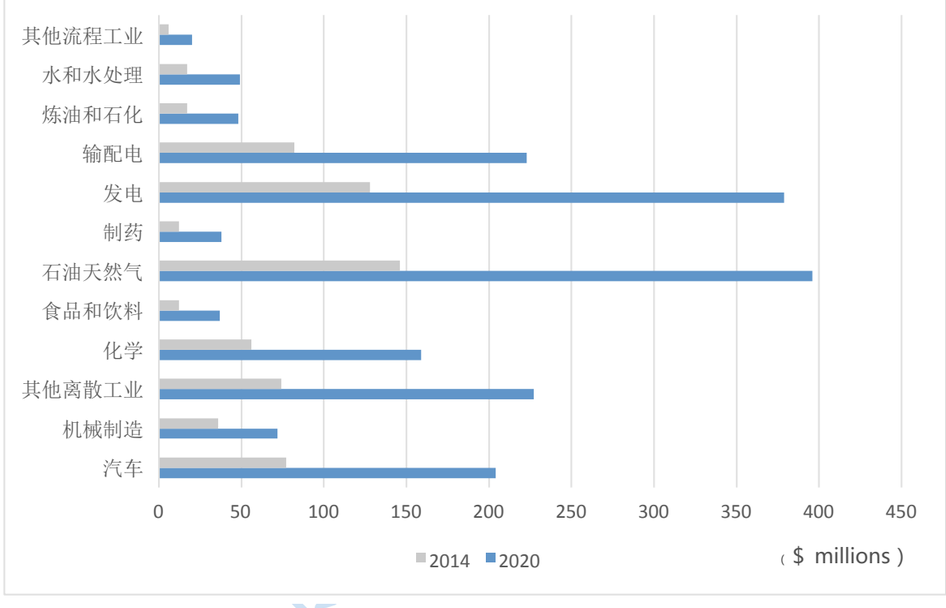


图 5 不同行业工控安全市场规模
数据来源：Positive Technologies、匡恩网络

1.2.2 不同行业工控安全市场规模

根据国外数据服务公司 HIS MARKIT 所提供的数据显示，到 2020 年全球主要工业领域中电力、石化、制造等领域的工控市场规模将大幅增长，其中石油天然气、发电行业的工控安全规模都将接近或达到 4 亿美金。通过对比不难看出，各工业企业对网络需求依赖日益加大，且高端制造业对自身安全的要求更高，一旦发生安全危害，造成的损失和潜在影响也将无法估计。

1.3 工业控制系统漏洞分析

1.3.1 工控系统漏洞类型分析

当前世界上大多数工控系统存在的漏洞属于拒绝服务、远程代码执行和缓冲区溢出三个类别。常见漏洞类型的比例如下图所示（其他类型没有被广泛传播，多数占比小于 4%）。

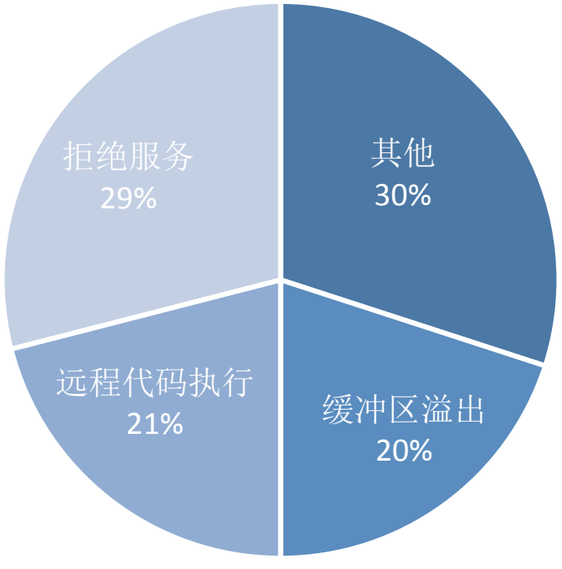


图 6 工业控制系统组件中常见漏洞类型
数据来源：Positive Technologies、匡恩网络

这些漏洞会被入侵者利用引起设备故障或设备未经授权的操作，导致影响可靠性要求和工业控制系统组件的灵敏度。

1.3.2 不同行业工控系统漏洞分布

从行业来看，根据 ICS-CERT 小组的统计数据显示，能源、关键制造业及水处理依然是工控安全漏洞分布较广泛的行业。

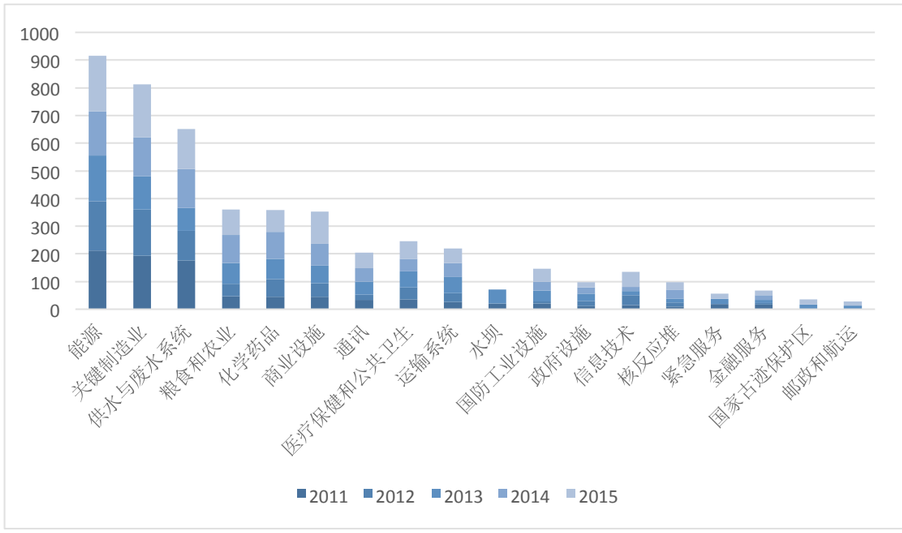


图 7 全球各行业工控安全漏洞数量分布
数据来源：ICS-CERT、匡恩网络

1.4 工业控制系统安全发展趋势

总体来说，2016 年工业控制系统安全的一个重要变化趋势是逐步向工业物联网安全演化。大数据、云计算、物联网、移动互联和软件定义网络、宽带无线等新一代信息通信技术已成为国家关键基础设施领域工控网络的核心技术。同时各类新技术的应用也引入了更多新的风险，给传统防护体系带来严峻挑战，如无人机、机器人、可穿戴设备等智能技术在工业控制系统现场的深化应用，导致物理隔离更加难以实施，使得工控系统一旦存在漏洞后，将“易攻难防”。

例如在电力行业，巡线需要大量的野外作业，用无人机进行低空巡线，是一种高效的巡线方式，它不仅能把部分野外的巡线作业转移到室内来做，还能把肉眼难以发现的、处于萌

芽状态的隐患（如：温度升高，轻微放电等）通过红外、紫外成像显现出来。此外，智能机器人巡检系统是工控系统巡检的新模式。它以智能巡检机器人为平台，整合机器人技术、多传感器融合技术、模式识别技术、导航定位技术以及物联网技术等，实现全天候、全方位、全自主智能巡检和监控。

传统工控安全受互联网及智能设备的影响较小，而物联网的发展促进了工控安全模式的全面升级。第一，物联网促进了工控安全的内涵升级：传统工控安全集中在电力、能源、冶金、烟草、数控等行业，物联网技术引入使得新型工控安全内容包括城市轨道交通、车联网、智能监控、行政基础设施等领域；第二，物联网促进了工控安全的关注点从“系统内”转向系统与外界事物的互联：传统控制设备简单，工控网络主要重视内外网边界防护及物理隔离，物联网时代工控设备与互联网、办公网、控制网、设备网结合更紧密，工控安全成为“网络安全、设备安全、控制安全、应用安全、数据安全”的综合体。因此，工业控制系统安全逐步向工业物联网安全演化的倾向逐渐显现，其具体特征总结如下：

（1）智能设备应用安全问题更突出

如前所述，近年来智能设备在工业控制系统应用日益成熟使得国家关键基础设施面临的网络安全威胁日益严重。2012 年，美国某著名黑客称，他可以在距离目标 50 英尺的范围内侵入心脏起搏器，让起搏器释放出足以致人死亡的 830V 电压 ;2013 年的“防御态势”黑客大会上，美国两位网络安全人员演示了如何通过攻击软件使高速行驶的汽车突然刹车；2014 年乌云安全峰会上黑客指出，360 安全路由、小度路由、小米路由等智能路由器均存在安全漏洞；2015 年的 Geekpwn 大会上，黑客演示了破解智能家居的过程。我国智能设备安全问题同样非常严重，与之形成鲜明对比的是，消费者的安全意识却十分淡薄。调查发现，我国只有 44% 的人知道智能设备可能泄露个人隐私。随着智能设备在医疗、汽车、家居等各大领域深入应用，预计未来，随着物联网技术进一步发展，以智能设备为目标的入侵将越来越多。

（2）云端安全威胁将大量增加

在国家关键基础设施领域，云端业务和数据也在逐步累积，针对云端的基于漏洞、病毒、未知威胁的 APT 攻击、0Day 攻击日益增加，云端的安全事件频频发生。2009 年，Gmail 电子邮箱发生故障，导致业务中断 4 个小时；2010 年，Intuit 基于云连接的服务发生长达 36 小时的断网事故；2011 年，亚马逊的云计算数据中心发生宕机事件，大量企业业务受损；2014 年，UCloud 公司国内云平台发生大规模云服务攻击事件；2015 年，“毒液”漏洞使全球数以百万计的虚拟机处于网络攻击风险之中，严重威胁各大云服务提供商的数据安全。随着云计算的广泛应用于各个领域，2016 年，越来越多的业务在云端开展，越来越多的数据存储在云端，基于漏洞、社工、病毒、未知威胁的 APT 攻击、0Day 攻击越来越频繁，且

已成为企业乃至国际网络空间主要攻击方式。总之，云计算的共享特性和按需定制本质虽然给企业带来效率上提升，也不可避免地引入更多新的安全威胁。

（3）针对关键基础设施的破坏力加大

目前，网络攻击已成为新型武器，敌对势力利用网络攻击成功破坏国家关键基础设施已成为现实，工业控制系统特定攻击一般针对工控系统特有的协议和特定的业务逻辑，具有攻击目标明确、操作隐蔽、潜伏时间长等特点，且一般通过集团式甚至是国家级实施攻击。攻击采用的技术先进，病毒扩散以及破坏隐蔽，现有防病毒软件无法进行查杀。例如，2015 年，以匿名者为代表的黑客团体和以 ISIS 为代表的网络恐怖组织，制造了多起网络安全事件，其影响力和破坏力巨大。3 月，匿名者发布视频称将对以色列发动“电子大屠杀”，进攻政府、军事、金融、公共机构网站，将以色列从网络世界抹去。5 月，匿名者入侵了 WTO 的数据库、攻击以色列武器经销进口商并在 #OpIsrael 计划中泄露大量在线客户端登录的数据。11 月，ISIS 利用互联网组织实施巴黎恐怖袭击。2016 年，以匿名者和 ISIS 组织为代表的黑客团体和网络恐怖组织，频繁地对部分国家的政府网站、国家关键基础设施发动攻击，构成巨大的威胁。

第二章

国际工业控制系统重要安全事件

2015 年美国 ICS-CERT 收集到的工控安全事件中，大多集中在欧美发达国家或地区，且遭受攻击的目标多为国家重要基础设施或重要行业领域工业控制网络。2015 年 12 月底的乌克兰电网事件为代表的网络攻击让全球更加意识到工控网络安全的重要性，此次电网 SCADA 系统遭受攻击造成数小时的停电，受影响人口超过 140 万，其他如波兰航空公司飞机停飞、德国钢厂网络攻击等同样给各国工业企业造成了重大的损失。

2.1 安全事件概述

进入 2016 年，国际工控网络攻击事件仍未停止，相比 2015 年，2016 年所发生的工控安全事件影响越来越大，甚至逐步威胁到国家安全。

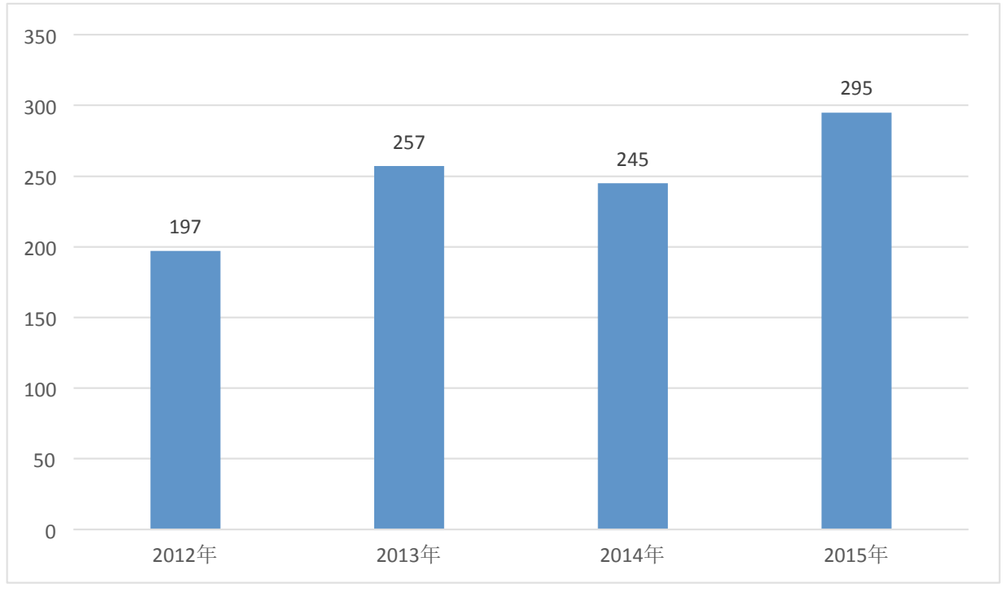


图 8 2012-2015 年全球工控安全事件数量
数据来源：ICS-CERT、匡恩网络

2016 年所发生的工控安全事件中针对国家政府基础设施的攻击开始兴起，同时车联网等热门物联网领域的网络攻击也逐渐成为黑客们的潜在目标。

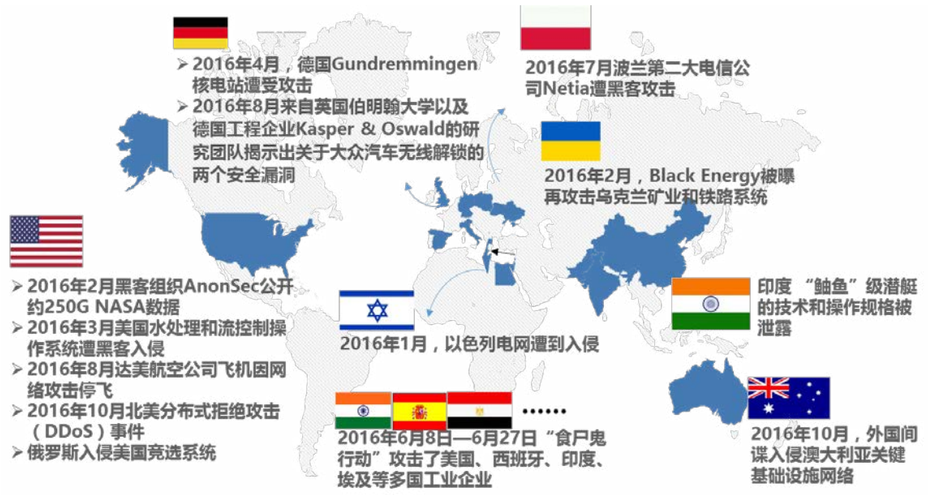


图 9 2016 年全球重要工控安全事件分布图

通过对历年工控安全事件的分析总结，工控入侵表现出了一些鲜明的特点：

- 网络攻击已经从影响虚拟资产向破坏物理世界转变。
- 物联网技术发展直接带来基础设施攻击面的增大，通过物联网设备渗透到工控已成为一种重要途径。
- 传统病毒与工控病毒相互交织，以计算机为跳板的攻击在未来可能发展到直接攻击控制系统上。
- 工控入侵很可能从利用未公开漏洞的高难度攻击方式延伸到常规手段组合式攻击，甚至绕过工控底层知识的壁垒。

2.2 典型安全事件

2.2.1 美国 Kemuri 水务公司系统遭黑客入侵

2016 年 3 月一群黑客攻破了美国 Kemuri 水务公司（KWC）用于水处理和流控制的操作系统。经研究发现该自来水公司系统的安全较为脆弱，许多可以影响到系统的关键漏洞都被公开暴露在互联网上，总体架构也使用了过时的操作技术（OT）系统。

自来水系统所使用的 OT 系统是十多年前计算机运行的操作系统，其中用于控制基础设施的是一个 IBM AS/400 系统，这个系统可以追溯到 1988 年，它需要有操作员来控制每一个不使用的设备（即阀和流量控制应用程序） 和它的功能（即计费）。更令人不安的是，一个雇员，或者攻击者，可以通过访问 IBM AS/400 系统管理整个实用程序。如果 KMC 发生了数据泄露，这里的 SCADA 平台将会是被首先发现的。更令人关注的是，很多重要的功能运行在一台小型机系统上。KMC 小型机系统成为 SCADA 平台，这个系统通过路由器直接连接到几个网络中，包括负责地区的税法和流量控制应用程序、负责处理数以百计的可编程逻辑控制器（PLC）、安置客户的 PII 和相关计费信息。

研究发现 KWC 设施可能成为黑客群体的针对性目标，内部架构中付款应用程序的服务器中存在可被利用的漏洞。一旦服务器被攻破，攻击者可以获得内部 IP 地址信息以及管理员登录 AS/400 的凭证，这些信息可以被用来窃取其中的 250 万条记录，包括客户数据和付款信息。幸运的是，攻击者还没有利用这些数据进行欺诈活动。通过访问 AS/400 系统，攻击者也可以完全控制水流和用于净化水的化学物质。在为期 60 天的评估期间，专家们发现了四个自来水连接系统，攻击者可以通过这些修改系统设置，幸运的是，要做到这些需要相关专业领域的知识（供水领域）才能够造成破坏。

黑客可以通过预先了解自来水系统，发起针对供水系统发起网络攻击从而影响到民族国家的日常生活。因此，相关部门需要加强这类系统的安全性。

2.2.2 北美遭受分布式拒绝服务攻击

美国当地时间 2016 年 10 月 21 日，黑客组织 NewWorldHackers 和 Anonymous 通过互联网控制了美国大量的网络摄像头和相关的 DVR 录像机，然后操纵这些“肉鸡”攻击了为美国众多公司提供域名解析网络服务的 DYN 公司，影响到的服务厂商包括：Twitter、Etsy、Github、Soundcloud、Spotify、Heroku、PagerDuty、Shopify、Intercom 等。该攻击事件一直持续到当地时间 13 点 45 分左右。

据分析，黑客们使用了一种被称作“物联网破坏者”的 Mirai 病毒来进行“肉鸡”搜索。更为致命的是，Mirai 病毒的源代码在 2016 年 9 月的时候被公开发布，大量黑客对该病毒进行了升级，升级后版本的传染性、危害性比前代更高（Mirai 日语的意思是“未来”，研究人员将新变种命名为“Hajime”，日语的意思是“起点”）。Mirai 病毒是一种通过互联网搜索物联网设备的病毒，当它扫描到一台物联网设备（如网络摄像头、DVR 设备等）后会尝试使用弱口令进行登陆（Mirai 病毒自带 60 个通用密码），如果登陆成功，这台物联网设备就会进入“肉鸡”名单，并被黑客操控攻击其他网络设备。

据悉，此次 DDoS 攻击事件涉及的 IP 数量达到千万量级，共有超过百万台物联网设备参与了此次 DDoS 攻击。Mirai 感染分布如下图所示，感染国家 top10 如下表所示。

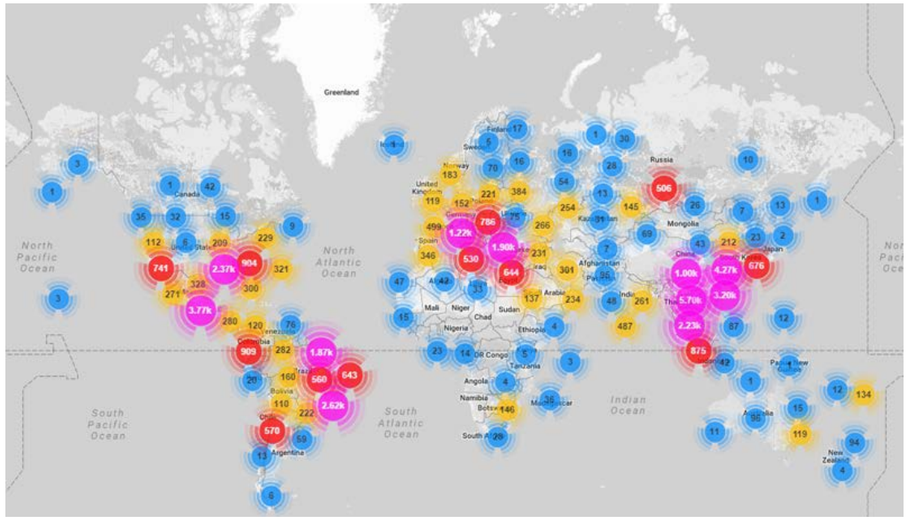


图 10 Mirai 感染分布

表 1 Mirai 感染国家分布 Top 10

国家	% of Mirai botnet IPs
越南	12.8
巴西	11.8
美国	10.9
中国	8.8
墨西哥	8.4
韩国	6.2
台湾	4.9
俄罗斯	4.0
罗马尼亚	2.3
哥伦比亚	1.5

其中，这些设备中有大量的 DVR（数字录像机，一般用来记录监控录像，用户可联网查看）和网络摄像头（通过 Wifi 来联网，用户可以使用 App 进行实时查看的摄像头）。而数据显示，参与本次 DDoS 攻击的设备中，主要来自于中国杭州雄迈科技生产的设备。这家公司生产的摄像模组被许多网络摄像头、DVR 解决方案厂家采用，在美国大量销售。

此次北美的 DDOS 事件是物联网领域的又一安全事件，安防监控产品本身作为维护国家公共安全的重要工具，遍布国家重要机构和群众生活的各个领域，里面存储的信息包含了从国家机密到普通百姓日常生活隐私的各个方面。一旦信息泄露，造成的损失和未来潜在的威胁难以估量。目前发现的安全隐患主要是由于设备生产厂商出场预置的登陆口令在用户使用过程中未强制要求修改、使用者自身安全意识薄弱导致。

物联感知设备如传感器、摄像头等肩负着采集现实世界信息的职责，为保证此类安防系统的安全，我们应注意：

- IOT 设备（含安防监控设备）开发商应加强安全审核，避免出现弱口令或安全绕过漏洞，避免出现口令硬编码无法修改的漏洞；
- 用户在使用时，应停止使用默认 / 通用密码，及时修改登录密码；
- 使用时禁用对设备的所有远程（WAN）访问。要验证设备是否未打开以进行远程访问，可以使用工具扫描以下端口：SSH（22），Telnet（23）和 HTTP /HTTPS（80/443）；
- 使用时尽可能避免该摄像头在公网上直接访问，如果无法避免，使用路由器或边界访问控制设备限制公网用户直接访问摄像机或探测设备。

2.2.3 BlackEnergy 被曝再攻击乌克兰矿业和铁路系统

继 2015 年 12 月乌克兰电网遭受攻击后，BlackEnergy 备受关注。近日，趋势科技公司宣布，其在乌克兰一家矿业公司和铁路运营商的系统上发现了 BlackEnergy 和 KillDisk 样本。

趋势科技发现的数个样本变种与当初感染乌克兰电力公司的 BlackEnergy 类似，这个恶意软件使用同样的指挥和控制（C&C）服务器。安全研究人员认为，幕后的攻击者与当初攻击乌克兰电力公司系同一伙人。研究人员注意到样本、命名约定、控制基础设施和攻击时机等方面存在着许多相似之处。

专家们对这起攻击的几种原因进行了阐释。一种可能是，攻击者可能想通过持续地破坏电力、矿业和交通运输等设施，破坏乌克兰的稳定性；另一种可能是，他们将恶意软件植入到不同的关键基础设施系统，确定哪一种基础设施系统最容易被渗透，从而获得控制权。其他相关的说法是，矿业和铁路公司的感染可能只是初步的感染，攻击者只是企图测试代码库。

无论是哪种情况，针对关键基础设施的网络攻击都会给任何国家和政府构成严重威胁。

2.2.4 德国 Gundremmingen 核电站计算机系统发现恶意程序

2016 年 4 月 24 日，德国 Gundremmingen 核电站计算机系统在常规安全检测中发现了恶意程序，核电站的操作员 RWE 为防不测，关闭了发电厂。

分析显示此恶意程序是在核电站负责燃料装卸系统的 Block B IT 网络中发现的，当时该恶意程序仅感染了计算机的 IT 系统，而没有涉及到与核燃料交互的 ICS/SCADA 设备。

核电站表示该 IT 系统并未连接至互联网，应是有人通过 USB 驱动设备意外将恶意程序带进来，可能是从家中，或者核电站内的计算机中。德国相关部门将整个事故分级为“N”（表示 Normal）。

然而通过此次事件，业界认识到当前工业控制系统和其他连接至互联网的系统一样脆弱，时刻处在各种计算机病毒的威胁之中。

2.2.5 大众汽车被曝存在无线解锁漏洞

2016 年 8 月，来自英国伯明翰大学以及德国工程企业 Kasper & Oswald 的研究团队揭示出关于大众汽车的两个安全漏洞，该漏洞对自 1995 年起开始售卖的所有大众汽车都有效。预计两个系统的漏洞将影响到近 1 亿台汽车的无钥匙进入系统。其中之一，能让黑客无线解锁大众集团这 20 年来售出的所有车辆，包括奥迪和斯柯达。另一个，影响范围更广，阿尔法罗密欧、雪铁龙、菲亚特、福特、三菱、日产、欧宝和标致都未能幸免。

图 11 用来截获车辆遥控钥匙信号的 Arduino 开源无线电设备

针对两种漏洞的攻击都用到了一款无线电硬件，来截获受害汽车遥控钥匙的信号，然后利用这些信号来克隆钥匙。两种攻击都可用连到笔记本电脑的软件定义无线电来操作，或者用更便宜更隐秘的工具包——40 美元就能做出的连上无线电接收器的 Auduino 开发板。硬件花销很小，攻击流程普通，但却能产生跟原版遥控钥匙一样的效果。

通过对大众车内部网络某组件的艰难逆向，研究人员抽取到了一个上百万辆大众汽车共享的加密密钥值。然后通过利用无线电硬件，截获目标车辆特有的，包含在遥控钥匙每次按钮发出信号中的另一个值，他们就能将这两个本应保密的数字结合到一起，打开车门，只需要窃听一次，就能克隆原版遥控。

但该攻击也非易事，无线电窃听需要将窃听设备放置在目标车辆方圆 90 米之内。而且虽然共享密钥可从某辆大众车内部组件中抽取出来，却并非完全通用。大众车出品年份和车型不同，该共享密钥也不一样，且存放的内部组件也并非完全相同。最近出品的高尔夫 7 和搭载同样锁定系统的其他车型，被设计成使用各自唯一的密钥，因而对此攻击免疫。

汽车公司想要修复该漏洞并不简单，车辆软件开发周期非常漫长，响应新设计速度较慢。但这一研究应提起汽车制造商注意所有系统都需要进行多维度安全审查，以免更多漏洞被用到更关键的驾驶系统上。

2.2.6 以色列电网遭受入侵

2016 年 01 月 28 日，以色列能源与水力基础设施部部长 Yuval Steinitz 披露称，该国电力供应系统受到重大网络攻击侵袭，且已经有多份报告表明勒索软件正是造成事故的直接原因。此次攻击是以色列有史以来出现过的规模最大的网络攻击。

尽管以色列官方称此次攻击所使用的病毒已经被查明，且采取了应急措施，如中止以色列电力设施当中大量计算机的运行，但目前尚不清楚到底是谁策划并实施了此次攻击。

据推测以达伊沙、真主党、哈马斯以及基地组织为代表的各恐怖组织能够通过网络攻击手段对目标国家造成巨大破坏，很有可能是此次攻击事件的幕后主导者。

针对关键性基础设施的攻击活动正日益受到重视。去年 12 月 23 日乌克兰电网遭遇的攻击活动被视为出现的首例针对电网体系的攻击行为，当时成千上万乌克兰民众陷入无电可用的窘境。

从 15 年底的乌克兰电网事件到 16 年初的以色列电网被攻击事件我们认识到关键性基础设施正越来越多地成为安全威胁的指向目标，黑客攻击的手段正变得越来越复杂，且业界普遍认为这类状况正有愈演愈烈之势。

2.2.7 “食尸鬼行动”事件

自 2015 年 3 月以来，一个组织严密的网络犯罪团伙对超过 30 个国家逾 130 家企业开展工业间谍活动。绝大多数受害者为工业领域的中小型企业（30-300 员工）。

卡巴斯基实验室表示，他们将该行动称之为“食尸鬼行动”（Operation Ghoul），行动集中在 2016 年 6 月 8 日—6 月 27 日。

- 攻击者以工业领域的企业为目标

大多数目标企业活跃在工业领域，比如石油化工、海军、军事、航空航天、重型机械、太阳能、刚铁等行业。该间谍组织还针对其它领域，包括工程、航运、医药、制造、贸易、教育、旅游、IT 等。

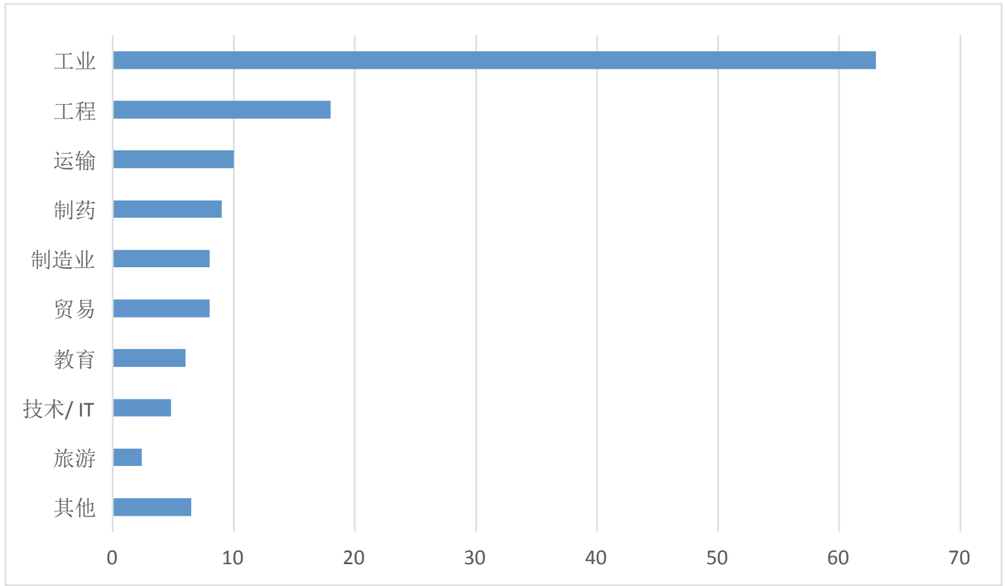


图 12 受食尸鬼行动影响的行业分布

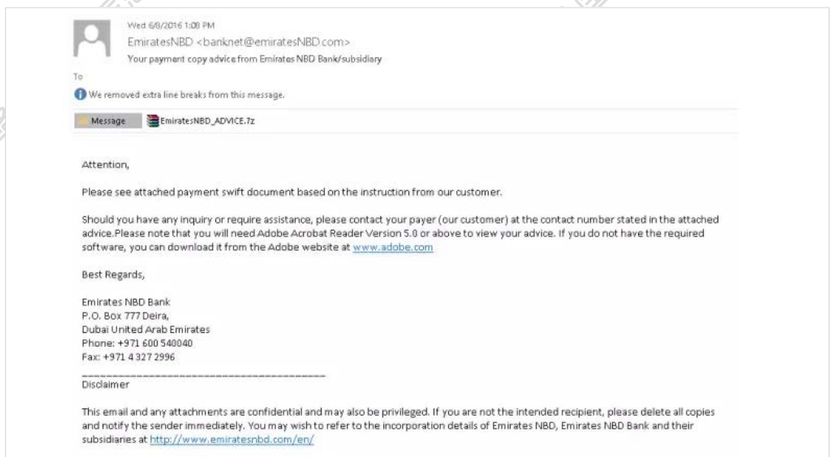
该组织主要将目标局限在活跃于工业领域的企业，但不具体针对一个国家。攻击范围遍布全球：西班牙（25 起）、巴基斯坦（22 起）、阿联酋（19 起）、印度（17 起）、埃及（16 起）等。

图 13 全球受食尸鬼行动攻击的国家分布

其它被攻击国家包括英国、德国、南非、葡萄牙、卡塔尔、瑞士直布罗陀、美国、瑞典、中国、法哥、阿塞拜疆、伊拉克、土耳其、罗马尼亚、伊朗、伊拉克和意大利。

- 攻击者使用“鹰眼”（HawkEye）RAT 感染企业高管

“食尸鬼”黑客使用 HawkEye RAT（远程访问木马），也被称为 KeyBase 攻击。


Wed 6/8/2016 1:08 PM
EmiratesNBD <banknet@emiratesNBD.com>
Your payment copy advice from Emirates NBD Bank/subsidiary

To

We removed extra line breaks from this message.

Message EmiratesNBD_ADVICE.7z

Attention,

Please see attached payment swift document based on the instruction from our customer.

Should you have any inquiry or require assistance, please contact your payer (our customer) at the contact number stated in the attached advice.Please note that you will need Adobe Acrobat Reader Version 5.0 or above to view your advice. If you do not have the required software, you can download it from the Adobe website at www.adobe.com

Best Regards,

Emirates NBD Bank
P.O. Box 777 Deira,
Dubai United Arab Emirates
Phone: +971 600 540040
Fax: +971 4 327 2996

Disclaimer

This email and any attachments are confidential and may also be privileged. If you are not the intended recipient, please delete all copies and notify the sender immediately. You may wish to refer to the incorporation details of Emirates NBD, Emirates NBD Bank and their subsidiaries at http://www.emiratesnbd.com/en/

图 14 被感染的高管邮件

在 2016 年 6 月，研究人员发现大量鱼叉式网络钓鱼电子邮件中包含的恶意软件。附件中的恶意软件基于在暗网公开售卖的“鹰眼”商业间谍软件，为攻击者提供大量黑客工具。一旦安装，它会收集受害者 PC 的数据，包括：击键、剪贴板数据、FTP 服务器凭证、浏览器的账户数据、消息客户端的账户数据（Paltalk、Google talk、AIM）、电子邮件客户端的账户数据（Outlook、Windows Live 邮件）、已安装应用程序信息（Microsoft Office）。攻击者在 EXE 文件中打包他们的 RAT，放在 ZIP 文件内通过鱼叉式钓鱼邮件发送给目标企业的高管。卡巴斯基研究显示，这些邮件发送给了首席执行官、首席运营官、经理、工程师、主管、销售等，很大程度上是因为攻击者希望获取核心情报、其它有趣的信息以及控制账号。

对于这类攻击，“鹰眼”收集目标数据并通过 HTTP 以非加密的方式发送至两个服务器中的一个，这两个服务器属于过去被劫持的合法企业所有。

2.2.8 伊朗多个重要石化工厂被恶意软件攻击

伊朗近期发现一个恶意软件，并将其从两大重要的石化公司删除。值得注意的是，最近，伊朗声称其石化公司起火是网络攻击所致。

伊朗民防部门负责人 Gholamreza Jalali 周六向路透社透露，在“定期检查石化单位”的时候发现了该恶意软件，确实属于工业恶意软件。伊朗国防部自然将事情揽到自己身上并采取了必要的措施。Jalali 与伊朗国家新闻机构 IRNA 之间的谈话揭露了这一事件。

Jalali 也借此机会澄清近期伊朗石化工厂起火的谣言。他指出，在两大石化工厂发现该恶意软件，但称恶意软件处于非活动状态与火灾毫无关联。

尽管如此，这样的新闻报道是意料之中的事。因为，伊朗一直怀疑是外国攻击，包括美国和以色列。2009 年和 2010 年，美国和以色列通过震网（Stuxnet）病毒秘密攻击伊朗核电项目，Stuxnet 渗透至伊朗核电项目的计算机系统并破坏了伊朗铀浓缩离心机。

伊朗国家网络空间委员会（National Cyberspace Council）正在调查近期的网络攻击。该委员会还将分析网络罪犯引起失火的概率。

许多伊朗石化设备遭受大火侵袭，比如上月的 Bu Ali Sina 炼油厂。但是，Jalali 已经排除了近期火灾因网络攻击或恶意软件而起的可能性。伊朗石油部长也表示，石化工厂遭遇火灾是由于私有石化公司缩减安全健康检查预算而致。

2.2.9 美国西海岸遭受每秒 400G 新型僵尸网络攻击

美国免费 CDN 服务商 CloudFlare 发布的一篇博文指出美国西海岸遭到一波大规模 DDoS 攻击。

图 15 美国西海岸遭受大规模网络攻击

该公司大约两周前就观测到流量溢出现象，攻击方首先利用朝九晚五式攻击模式进行自身能力测试，随后将攻击模式转为 24 小时全天候侵扰，经过观察，其中高强度攻击流量的峰值可达到 172 MBps，这意味着每秒发送约 100 万个数据包或者每秒 400Gb 数据。CloudFlare 观察到这套僵尸网络应该是由某些朝九晚五工作制的攻击者所操纵，并在此时间段内定时开启与关闭。

这一攻击流量并非源自 Mirai 僵尸网络，攻击者们使用的是完全不同的软件以及实施方法，即“在 TCP 协议上发送大规模 L3/L4 洪流”。

该公司同时指出，此轮攻击目前主要针对美国西海岸管辖范围内较为集中的区间。就在这一消息公布前不久，美国白宫网络安全特别委员会刚刚发布建议并向总统递交了相关论文。在这份建议中，网络安全特别委员会要求通过行之有效的行动以减少或消除威胁性僵尸网络。

2.2.10 施耐德工业防火墙被爆严重安全漏洞

根据国外媒体的最新报道，安全研究专家在 2016 年工业控制系统（ICS）网络安全大会上披露了好几个严重的安全漏洞，其中就包括一个存在于施耐德工业防火墙中的严重漏洞。该漏洞将会影响施耐德公司 ConneXium 工业级以太网防火墙的安全性，该系列的防火墙产品主要用于保护工业环境下的数据采集与监视控制系统（SCADA 系统）、自动化控制系统、工业网络、以及其他的一些关键设施。

安全研究专家在对施耐德 ConneXium 工业级以太网防火墙进行安全检测时，在该系列防火墙产品的 Web 管理接口中发现了一个缓冲区溢出漏洞，如果能够成功利用该漏洞的话，那么攻击者将可以在目标设备中远程执行任意代码。除此之外，攻击者还可以干扰正常的网络通信。

根据安全公司透露的信息，施耐德电气目前已经开发出了能够修复该漏洞的更新补丁，但是厂商目前由于种种原因还未能向用户推送这个修复补丁。除了上述这个漏洞之外，安全研究人员还报告了七个存在于 PLC 控制系统中的 0day 漏洞。

第三章

国际工业控制网络安全治理动态

2015 年是世界各国网络安全法律法规密集出台的一年，美国、日本、欧洲等地区在工控网络安全方面走在了世界前列。美国 2015 年在工控网络安全管理方面主要工作包括出台网络和信息安全法规、调整组建网络安全机构、修订完善网络和信息安全标准、强化网络空间军事能力、开展网络安全多方合作、研发信息安全关键技术等；欧盟 2015 年在网络和信息安全方面的政策、举措主要包括完善网络安全法规、严格网络空间监管、打击网络恐怖主义、保护儿童上网安全、研发网络安全技术、加强网络安全国际合作等；其他国家和地区在工控安全管理中投入的精力虽不及美国及欧盟诸国，但在网络安全法规、网络空间监管、开展网络安全合作等方面均采取了相关行动。

进入 2016 年，受 2015 年各类工控网络安全事件的影响，世界各国纷纷加大了对国内网络安全的投入，除制定各项法律法规外，在网络安全演练，网络安全人才的培养等方面也在不断进行投入。以美国为首的西方国家更是不断扩大网络安全资金预算，甚至成立专门的网络安全部门保障以各大工业控制系统为代表的关键基础设施的安全。

3.1 美国安全治理动态

2016 年，受年前全球爆发的多起工控安全事件影响，美国率先响应，奥巴马政府从更广泛的物联网安全的角度提高对网络安全的重视。首先是在 2016 财年新增 140 亿美元的网络安全发展预算；其次，更新并新增了多项网络安全政策，包括《保障物联网安全战略》、《网络安全研发战略规划》、《网络安全国家行动计划》以及《制造业与工业控制系统安全保障能力评估》草案；除此之外，还设立了专门的网络安全管理机构，并建立网络安全部队。

3.1.1 新增 140 亿美元用于网络安全发展战略

美国 2016 财年预算报告要求联邦政府斥资 140 亿美元用于支持政府层面的网络安全发展战略，较 2015 财年总额增长 11%。联邦部分部门及机构预算投入如下：

美国国土安全部 (14 亿美元，较 2015 财年增长 7%)：美国国土安全部（简称 DHS）2016 财年预算支持面向各类必要领域的关键性投入，旨在改善网络安全水平并保护政府网络免受恶意网络攻击之侵害。

美国司法部 (6.36 亿美元，较 2015 财年增长 14%)：美国司法部 2016 财年预算额度被要求主要用于进一步支持网络检测与响应能力。

美国国防部 (95 亿美元，较 2015 财年增长 11%)：其中包括用于保护高价值资产及国防部网络防御之专项资金；改进防御与进攻两方面的网络空间运作能力；同时继续推进国防部网络技术人才的保留、招聘以及培训工作。

美国国内收入署 (2.42 亿美元，较 2015 财年增长 72%)：美国国内收入署 (简称 IRS) 负责维护来自数以百万计的个人及企业纳税人的收入数据，旨在提升网络安全水平并保护美国国内收入署所管理的纳税人信息。

健康与人类服务部 (2.62 亿美元，较 2015 财年增长 23%)：其需要强化控制与威胁管理策略，同时建立起成熟的网络安全技术团队——包括为其配备妥善的培训、教育以及技能组合，从而切实对不断演进的安全威胁加以管理，并利用必要控制手段保护相关 IT 资产。

美国商务部 (1.87 亿美元，与 2015 财年持平)：包括开发政府及私营部门所使用的安全标准，同时对美国人口普查局代表自身及其它联邦统计机构收集到的人口与经济数据进行维护。

退伍军人事务部 (简称 VA， 1.803 亿美元，较 2015 财年增长 15.5%)：退伍军人事务部斥资 1.803 亿美元以确保事务部信息与网络安全，其中包括普及持续安全监控、运营连续性以及一系列小规模网络安全项目。

图 16 美国网络安全治理动态

3.1.2 发布《网络安全研发战略规划》

2016 年 2 月 5 日，美国白宫国家科技委员会（NSTC）网络和信息技术研发分委会发布《网络安全研发战略规划》。更新和扩大了 2011 年 12 月发布的《可信网络空间：联邦网络安全研发项目战略规划》。

规划确定了三个研发目标，近期目标（1 ～ 3 年），通过有效和高效的风险管理，抵抗对手的非对称优势；中期目标（3 ～ 7 年），通过可持续安全系统的开发和运行，逆转对手的非对称威胁；长期目标（7 ～ 15 年），通过结果和可能因素的制衡，有效和高效地威慑恶意网络活动。

重点关注四项防御能力的开发：一是威慑，衡量并增加对手实施相关活动的成本、减少活动造成的破坏、增加潜在对手的风险和不确定，以有效地阻止恶意网络活动；二是保护，使组件、系统、用户和关键基础设施有效地抵御恶意网络活动，确保机密性、完整性、可用性和可追究性；三是有效地侦察甚至预测对手的行为；四是适应，通过有效地响应破坏、从损毁中恢复运行、调整以挫败未来类似活动，防御者可动态地适应恶意网络活动。

确定开展网络安全研发六个关键方面：科学基础、强化风险管理、人的因素、研究成果转化、人员开发和加强研究的基础设施。

3.1.3 公布《网络安全国家行动计划》

2016 年 2 月 9 日，美国总统奥巴马公布《网络安全国家行动计划》，将从提升网络基础设施水平、加强专业人才队伍建设、增进与企业的合作等五个方面入手，全面提高美国在数字空间的安全。主要包含：

建立“国家网络安全促进委员会”——由顶尖的企业与技术专家组成，部分人员由国会任命，共同勾勒出一份为期十年、涵盖公私两方面的网络安全技术、政策发展路线图，以推广各类最佳实践。

专门分配 31 亿美元的信息技术现代化基金，用于升级已过时或难维护的政府 IT 和网络安全管理基础设施。

加强在线账户的保护，通过“国家网络安全联盟”发起新的国家网络安全宣传行动，专注多重认证，以提升、培育信息消费者的网络安全意识。

提议在 2017 财年预算中，网络安全总体支出达 190 亿美元，较 2016 财年增长 35%。

3.1.4 发布《制造业与工业控制系统安全保障能力评估》草案

2016 年 11 月，美国国家标准与技术研究所（简称 NIST）发布了《制造业与工业控制系统安全保障能力评估》草案。这份草案的评估工作为其规划的四项实施流程中的第一部分，其中将涵盖的四大议题包括：

- 行为异常检测——用于监控计算机网络，查找其中的异常流量或者其它可疑现象；
- ICS 应用程序白名单——仅允许经过授权的应用程序在 ICS 系统之上运行；
- 恶意软件检测与缓解——发现并阻止恶意程序；
- ICS 数据完整性——确保由 ICS 设备生成的数据能够准确反映机器内部的实际情况。

3.1.5 发布《保障物联网安全战略原则》

2016 年 11 月 15 日，美国国土安全部（DHS）发布《保障物联网安全战略原则》，该战略原则指出，未在最初设计阶段构建安全并采取基本安全措施“可能会造成制造商的经济成本、声誉成本或产品召回成本损失。虽然还没有建立解决物联网问题的判例法体系，但传统的产品责任侵权原则可以适用。”以下为物联网安全战略原则的部分总结内容：

- 在设计阶段结合安全：“经济驱动力使得企业将设备推入市场时很少考虑安全。这给恶意攻击者创造大量机会操控联网设备的信息流”。
- 启用安全更新和漏洞管理：即使安全从一开就内置存在，但在产品部署后发现产品漏洞很常见。这些漏洞能通过补丁、安全更新和漏洞管理策略缓解。
- 建立在可靠的安全最佳实践之上：传统网络安全中许多经过验证的实践可以作为提升物联网安全的出发点。
- 根据影响优先考虑安全措施：数据泄露的风险和后果大不相同，这取决于联网设备。因此，专注破坏、泄露或恶意活动的潜在后果对决定物联网生态系统的安全方向尤为重要。
- 提升透明度：在可能的情况下，开发人员和制造商需要了解供应链，因此他们能识别软件和硬件组件，并了解任何相关漏洞。增强意识能帮助制造商和工业消费者识别安全措施应用的位置和具体方法。
- 连接需仔细谨慎：考虑物联网的使用和物联网被破坏相关风险，物联网消费者尤其工业企业应该仔细并谨慎考虑是否需持续连网。

3.1.6 设立网络安全监管机构

美国总统奥巴马 2016 年 2 月 17 日宣布任命前白宫国家安全事务助理多尼隆担任网络安全促进委员会主席，新委员会的主要任务是帮助联邦政府、私营企业和公民个人改善网络安全环境，为提升美国长期网络安全提供一份“路线图”。

美国海军陆战队 3 月 25 日宣布新成立了一个新的部门，开展网络空间防御行动名称为“Marine Corps Cyberspace Warefare Group”(MCCYWG)，现在的环境下，网络安全不容忽视，这引起了美国政府和军事部门在网络领域的投资兴趣，通过投资来增强网络安全性。

2016 年 7 月 27 日，美国总统奥巴马发布总统行政令，规定美国司法部直接负责响应美国的网络威胁。同时，美国国土安全部将应要求立即帮助机构和企业平息网络或“资产”威胁。美国司法部将带头负责“威胁响应”或调查系统攻击，确认网络罪犯并摧毁攻击行动，因为外国对手常涉足其中。

3.1.7 强调军事部署，将关键基础设施网络攻击作为第五战场

网络神盾演练：最近举行的网络神盾 2016（Cyber Shield 2016）演习活动中的一大关注重点是基础设施的潜在威胁，而这场国家级的网络战演习亦获得了美国国民警卫队、美国陆军、预备役以及海军陆战队网络作战人员们的共同参与。

“网络神盾是一场立足于国家层面的事件响应演习活动，旨在加强行业合作伙伴与国民警卫队间的协作，允许各合作伙伴利用警卫队的响应技术应对自身环境内的各类网络入侵状况”陆军网络司令部通过发布在 YouTube 频道上的一段公开视频解释称。

提前部署网络部队：美国安局和网络司令部（USCYBERCOM）相关负责人表示，由于当前国家层面的紧急状态，和对网络安全的迫切需求，美军某些网络部队已处于战备待命状态。其中，网络司令部下属网络任务部队（Cyber Mission Force,CMF）已在 9 月 30 日前完成初始作战能力建设。

为了提高网络作战能力，美国国防部从 2012 年就开始组建网络任务部队 CMF，以整合协调军方网络作战任务。CMF 包含 133 个小组共 6200 余人，是美国计算机网络行动的最大专门单位，致力于保护或攻击世界各地的计算机系统。

美军网络任务部队 CMF 共 133 个分队，有四个组成部分：

- 13 个网络保护分队（Cyber Protection Teams），分队加强传统防御措施，优先保卫军方网络系统免遭入侵破坏威胁；
- 68 个国家任务分队（National Mission Teams），分队保护美国国家关键基础设施及相关国家利益免遭网络攻击；
- 27 个战斗任务分队（Combat Mission Teams），分队响应网络空间作战任务并支持作战计划和应急行动；
- 支持分队（Support Teams），分队负责给国家任务分队和作战任务分队提供分析和计划支持。

3.2 欧洲地区安全治理动态

2016 年，受恐怖主义活动的影响，欧洲地区一直处在恐慌与不安之中，虽然欧洲自身具备较强的网络安全防护能力，但来自各方的网络安全威胁尤其是来自恐怖主义的网络安全威胁不可不防。除了通过全欧洲地区性的网络安全监管法，采用新的网络安全规则，以及开展相关专题研讨会之外，欧洲各国政府对本国内部的网络安全情况也愈加重视。英国政府开始扶持本国网络安全企业的成长，意大利政府借鉴美国的做法引入了网络安全框架与情报模型，丹麦政府成立了专门的黑客学院，以培养网络安全人才。

图 17 欧洲地区网络安全治理动态

3.2.1 通过首套网络安全监管法

欧洲议会全体会议 2016 年 7 月 6 日通过《欧盟网络与信息系统安全指令》，以加强欧盟各成员国之间在网络与信息安全方面的合作，提高欧盟应对处理网络信息技术故障的能力，提升欧盟打击黑客恶意攻击特别是跨国网络犯罪的力度。

其主要内容是，要求欧盟各成员国加强跨境管理与合作，制定本国的网络信息安全战略，建立事故应急机制，对各自在能源、银行、交通运输和饮用水供应等公共服务重点领域的企业进行梳理，强制这些企业加强其网络信息系统的安全，增强防范风险和处理事故的能力。

此外，该指令还明确要求在线市场、搜索引擎和云计算等数字服务提供商必须采取确保其设施安全的必要措施，在发现和发生重大事故后，及时向本国相关管理机构汇报。

据悉，在获得欧洲议会批准后，这项指令将很快由欧盟官方进行权威发布，并在发布之日 20 天后正式生效。欧盟各成员国需在指令生效 21 个月内将指令内容纳入国家法律，并在 27 个月内完成对指令涉及公共服务重点领域企业的梳理。

3.2.2 采用新的网络安全规则

欧洲理事会已经采纳一系列新的网络安全规则，旨在确保欧盟区内各网络与信息服务方案实现物理及虚拟层面的安全性提升。这项网络与信息安全（简称 NIS）命令将要求重要服务供应方（例如能源、交通、医疗与金融等）及“数字化服务供应商”（在线交易市场、搜索引擎与云服务等）采取相应措施以降低网络攻击风险并报告任何已经发生的重大安全事故。欧盟各成员国将识别出重要服务供应方，制定严格的安全规则加以约束。数字服务供应商需要遵守的规则相当较为宽松，且规则条款适用于除小型企业外的任何特定领域从业厂商。

与此同时，各国还将共同建立一支新的安全合作小组以及一套新的国家计算机安全事件响应小组（简称 CSIRT）协同网络。该项协议仍然需要由欧盟各成员国进行正式确认。最终批准日期为今年 12 月 18 日，而后还将由欧洲理事会与议会正式通过。一旦生效，各欧盟成员国将有 21 个月的时间推进措施，且可另外延长 6 个月用于确定关键服务运营方。这意味着到 2019 年，随着各项举措的成功实施，欧洲的整体网络安全将显著得到提升。

3.2.3 拿出 18 亿欧元用于网络安全公司合作

欧盟委员会已经启动了一个在网络安全方向的公私合作伙伴关系并计划在 2020 年前投资 18 亿欧元（约 20 亿美元）。欧盟已经答应前期投入的 4.5 亿欧元（约合 5.02 亿美元）并将其用于激发参与此项目私有企业人员的创新力，包括相关调研以及创新项目“地平线 2020”。代表欧洲网络安全组织（ECSO）的安全厂商们则希望欧盟能在这个项目上有三倍以上的投入。

合作伙伴关系同样会包括国家、地域和当地的公共行政机构、调研中心以及高等院校。这个伙伴关系设计之初是为了培养仍处于初期的网络安全调研和发展的合作，并希望这个计划可以催生出更多满足能源、健康、交通和金融这些特别领域需求的信息安全产品和服务。

3.2.3 组织网络安全专题研讨会

欧洲网络与信息安全局于柏林的“#hub15 大会”组织了网络安全专题研讨会。其目的是增强对当前网络安全挑战的意识。该大会聚集了两千名关注信息和通信技术的参与者。

大会当天，欧洲网络与信息安全局通过组织与公共和私营部门专家以及注册参与者的焦点讨论，提升了欧洲网络安全的需求。欧洲网络与信息安全局和特邀专家们都意识到，数字化单一市场是使欧洲更加安全的关键点。

3.2.4 英国开始实施“网络安全早期加速项目”

英国今年开始实施“网络安全早期加速项目”，旨在为本国的安全初创企业提供建议和支持。该项目将由“伦敦网络”和贝尔法斯特女王大学安全信息科技中心联合管理。截至目前，已获得 25 万英镑资金，资金将从 3 月开始对外发放。

3.2.5 意大利引入网络安全框架与情报模型

意大利网络安全框架由 On.Minniti 与 Baldoni 教授于 2016 年 2 月发布，作为国家网络安全战略规划的推动机制，意大利引入一套创新型参考模型，要求国内全部企业及政府机构都加入进来。此网络安全框架借鉴了美国的 NIST 框架，从而帮助意大利关键性基础设施网络安全性提升，包含以下五项主要功能：

- 资产识别与业务流程认知功能，能够识别关键性业务流程及其相关风险。
- 保护功能，用于实现对业务及企业资产流程的安全保护，且无关乎其数字化特性。
- 检测功能，涵盖检测举措的定义与实现方式，旨在及时对各类计算机安全事故进行识别。
- 响应功能，发现企业安全事件时做出的针对性举措。
- 恢复功能，对受事故影响的各流程与服务的恢复规划与举措。

3.2.6 丹麦政府成立丹麦黑客学院

2016 年 3 月丹麦国家情报机构 PET（Politiets Efterretningstjeneste）宣布计划成立一个丹麦黑客学院，旨在提升本国网络安全能力以及对抗外来的网络威胁。

PET 担心网络空间会演变成一个军事化的场地，外国政府可能会使用网络工具发动网络

间谍和破坏性攻击。丹麦安全情报机构 PET 将会招募一些有天赋的 IT 人员，支持丹麦政府在网络空间中的活动。拟计划从 2016 年 8 月 1 日开始培训出一些攻防型黑帽黑客。

在为期四个半月的培训中，丹麦黑客学院为学员设定了三个学习模块：第一个模块是基础模块，提升学员的网络和电脑安全能力；第二个模块是防御技术培训；第三个模块是攻击技术培训与演练。

3.3 其它国家或地区安全治理动态

在以欧美为代表的发达国家和地区纷纷加强国内网络安全之际，其他国家也开始对国内的网络安全重视起来。以色列作为世界上网络安全产业较为发达的国家，在 2013 年的时候就已推出了名为“前进计划”的网络安全产业研发计划，在 2016 年又在此基础上推出了“前进 2.0”；日本此前已在网络安全领域颁布了一系列政策法规，2016 年又成立了专门的网络安全促进机构——工业网络安全促进机构（ICPA）来抵御针对关键基础设施的网络攻击；其他国家如澳大利亚、俄罗斯、韩国、新加坡等也在网络安全上采取了相关政策措施。

图 18 其他国家或地区网络安全治理动态

3.3.1 以色列推出“前进 2.0”网络安全产业计划

2013 年，以色列国家网络局和首席科学家办公室推出了促进网络安全研发计划，即“前进计划”。这是以色列国家网络局成立 18 个月后推出的首个促进网络安全产业化发展计划，旨在促进研发与产业结合，加快技术转移，培育本土企业。随着该计划于 2015 年 6 月结束，首席科学家办公室对计划进行了专业评估，发现网络安全行业出现了新困难，面临新挑战。要继续推动以色列网络安全产业健康发展，解决新问题，迎接新挑战，重组“前进计划”、增加新的政策工具成为必然选择，“前进 2.0”版应运而生。升级版“前进计划”有三个资助重点：

一是资助突破性和颠覆性技术研发：突破性和颠覆性技术是大型网络安全公司的立足发展之本，就像以色列检查哨公司独有的防火墙技术，有全球市场影响力。

二是资助优秀网络安全企业产品创新和概念验证：这类资助主要帮助解决产品和技术市场化道路末端的障碍，如适应法规、用户体验、本土制造集成、产品推广应用等，创造一个真正的市场化产品。

三是促进产业合作：这类资助鼓励多家有技术优势的企业联合，共同研发针对特定网络安全问题的解决方案，或者打造技术企业产业集群，共同实现商业目标。

3.3.2 日本成立工业网络安全促进机构

日本正在考虑成立一个新的政府机构，专门抵御针对关键基础设施的网络攻击。这个新机构名为工业网络安全促进机构（ICPA），将于 2017 年正式运营，日本政府希望借此能够在 2020 年东京奥运会期间保护关键基础设施的安全。ICPA 的保护目标包括电力、天然气、石油、化学和核设施等。此外，小型国防私营企业也将在保护的范围内。从公布的情况来看，日本政府将组建的 ICPA 包括两个处室，一个是研究处，另一个是主动响应处。

研究处将会跟本地大学和海外机构如美国国土安全局等开展联合研究和真实的网络演练；而主动响应处会执行相应措施，如对专家、白帽进行入侵技术训练，阻止网络攻击的实施，对已有的网络威胁采取行动。

ICPA 的唯一任务是保护关键基础设施和所有政府机构的网络安全。日本政府创建 ICPA 的原因是为避免日本遭遇像乌克兰电网系统、美国电网和大坝系统那样的网络攻击。

3.3.3 澳大利亚发布《澳大利亚网络安全战略》

澳大利亚总理特恩布尔于 4 月 21 日在位于悉尼的澳洲科技园发布了《澳大利亚网络安全战略》。此安全战略的重点在于澳大利亚人如何在网络环境中保护自己，以及如何提高对

恶意网络行为的抵抗力。

网络安全战略将通过 33 项新举措保障国家的网络安全，政府 4 年内计划花费近 2.3 亿澳元在国家重要基础设施的攻击防护上，并承认他们具有极强的发动网络攻击的能力。这个战略非常的完善，有对国有行业和私人行业的防护， 还为 5000 家中型企业和信息分享活动所做的安全测试提供了资金支持。政府将计划拿出 2.3 亿澳元用于网络安全方面，包括成立网络威胁中心，建立网络安全中心，在重要城市建立情报分享中心等。根据网络安全战略，政府还将花费 4100 万澳元用于提高国家计算机应急响应中心（澳大利亚 CERT）的能力，并为战略型政府部门（包括澳大利亚联邦警署、犯罪委员会、澳大利亚通信局）聘请新的网络安全专家。

3.3.4 俄罗斯将通过新反恐法案支持网络监控

俄罗斯新反恐法案涉及大量网络监控相关问题。电信和网络公司必须记录和存储所有客户半年的通信数据，潜在成本高达数万亿美元。互联网公司将必须将所有通信元数据保存一年，而电信公司将必须保存三年。

法案通过后，电信运营商和互联网公司将必须将所有客户的通信保存半年，这就意味着这些公司将面临数万亿美元的额外成本，以遵守新反恐法。

众所周知，俄罗斯政府正严格监控国家互联网。俄罗斯政府开发了一个名为“SORM-2”的系统代码监控俄罗斯公民。政府迫使国家网络服务提供商（ISP）购买并安装 SORM-2 系统使用的探头。SORM-2 系统允许联邦安全服务（FSB）监控互联网流量，包括网上通信。

3.3.5 卡巴斯基发布物联网安全操作系统 KasperskyOS

卡巴斯基实验室在长达四年的低调研发之后，正式推出了新的安全操作系统：Kaspersky OS。这款操作系统是一套从零开始打造的方案，旨在保护工业控制系统。该系统为了实现安全保障，操作系统完全自主开发，同时对系统中的模块进行安全控制。通过内置的安全系统来控制应用程序操作和 OS 模块。这款操作系统需要有多种不同的应用。首先，需要为工控系统防护开发提供基础；其次需要为嵌入式设备，包括 IoT 设备防护开发提供基础。

其设计目标在于保护电站、输电网络以及通信网络等基础设施。工业控制系统提出的实际安全需求意味着从业者需要从零开始构建一套操作系统，且实现以下几项关键目标：

- 这款操作系统不可基于现有计算机代码；因此，其必须从头进行编写。
- 为了实现安全保障，其内核中不可存在任何错误或者安全漏洞，从而对系统中的其余模块进行安全控制。这意味着其内核必须 100% 正确无误，即不允许出现代码漏洞或者两用情况。
- 出于同样的理由，这套内核需要包含最低程度代码量，意味着尽可能提高代码质量，且需要由内核控制并以低级访问权限执行。
- 在这样的环境下，亦需要一套强大而可靠的保护系统用于支持不同安全模式。
- 这是一套经过强化的操作系统，允许用户在工业控制系统、医疗设备及物联网装置内控制进程执行级别。

卡巴斯基强调 Kaspersky OS 不管是 SCADA、ICS 还是 IoT 设备，都可以得到保护。因为这些攻击都是利用了 Mirai 僵尸网络来进行 DDoS 攻击的，Kaspersky 强调他们的 OS 会强制保护 IoT 和关键基础设施如工业、运输和通信等方面免于威胁。

3.3.6 韩国政府公布“韩国 ICT 2020”五年战略

2016 年 6 月，韩国政府公布了名为“韩国 ICT 2020”（K-ICT 2020）的五年战略规划，旨在将韩国打造成为全球信息安全行业领导者。在“韩国 ICT 2020”战略的指导下，政府将扩大在 ICT 领域的投资，使其成为韩国创新经济推动下的新“蓝海”。

战略指出，政府计划推动 ICT 初创企业发展，并加强国际合作，将信息安全相关程序和设备的出口额从目前的 1.6 万亿韩元（约合 13 亿美元）扩大至 2020 年的 4.5 万亿韩元（约合 36 亿美元）。韩国政府将着重实现网络安全和信息保护技术的全球化，把韩国网络安全品牌影响力扩大至全球，打破集中于国内需求的市场结构。在此战略的引领下，到 2020 年，网络安全产业预计将产生 1.9 万个相关工作岗位。同时，韩国正积极加强国际合作，推动“网络安全互助联盟”（CAMP）的成立，以建立全球网络安全的合作伙伴关系。CAMP 预计于 2016 年 7 月正式成立，届时将有 24 个国家参与。

3.3.7 新加坡正式公布国家网络安全策略

10 月 10 日，在为期 3 天的新加坡国际网络周（SICW）开幕式上，新加坡总理李显龙正式宣布了该国的网络安全策略报告。网络安全是新加坡数字经济社会发展的关键，该策略提出了新加坡网络安全的愿景、目标和要点。主要包括以下四个方面：

（1）建立强健的基础设施网络：政府将与运营商和网络安全团体等相关部门加强合作，共同保护国家关键设施网络；政府将在所有关键单位建立一个统一协调的网络风险管理和应急响应流程。同时，采用基于供应链的安全建设也是报告提到的重点。

（2）创造更加安全的网络空间：策略阐述了政府部门应对网络犯罪和推动新加坡成为可信数据中心的相关措施。策略还指出，政府不能完全解决网络安全威胁，社会企业和相关各方应加强促进交流并提供好的实践方法，共同为网络安全尽力。

（3）发展具有活力的网络安全生态系统：政府将与社会企业和高校合作，通过奖学金项目和特殊课程培养网络安全人才，并在社会层面加强网络安全就业和相关的技能培训。

（4）加强国际合作：与其他国家加强网络安全方面的合作，特别是深化与东盟国家在该领域的合作。在网络安全全球治理方面，新加坡将积极开展网络规范、政策和立法工作。

2015 年 2 月，美网络安全公司 FireEye 与新加坡电信合作，在新加坡成立了运营中心。2014 年 9 月，波音公司宣布在新加坡开设美国本土外首个网络安全中心。为了应对日益严重的全球网络安全问题，2015 年 4 月 1 日，新加坡网络安全局 (CSA) 正式成立。该机构除了监督新加坡网络安全政策外，还负责监管全国日益发展的网络安全产业。

3.4 我国网络安全治理动态

3.4.1 国家各部委颁布各项政策并积极采取行动

3.4.1.1《中华人民共和国网络安全法》经表决通过

2016 年 11 月 7 日上午，十二届全国人大常委会第二十四次会议经表决，通过了《中华人民共和国网络安全法》。这是我国网络领域的基础性法律，明确加强对个人信息保护，打击网络诈骗。该法自 2017 年 6 月 1 日起施行。

网络安全法共有 7 章 79 条，内容上有 6 方面突出亮点：第一，明确了网络空间主权的原则；第二，明确了网络产品和服务提供者的安全义务；第三，明确了网络运营者的安全义务；第四，进一步完善了个人信息保护规则；第五，建立了关键信息基础设施安全等级保护制度；第六，确立了关键信息基础设施重要数据跨境传输的规则。

对当前我国网络安全方面存在的热点难点问题，该法都有明确规定。针对个人信息泄露问题，网络安全法规定：网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；网络运营者不得泄露、篡改、毁损其收集的个人信息；任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息，并规定了相应法律责任。

针对网络诈骗多发态势，网络安全法规定，任何个人和组织不得设立用于实施诈骗，传

授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。并规定了相应法律责任。

此外，网络安全法在关键信息基础设施的运行安全、建立网络安全监测预警与应急处置制度等方面都作出了明确规定。

3.4.1.2 网信办开展关键信息基础设施网络安全检查

2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上对关键信息基础设施保护和网络安全检查工作做了精辟论述，指出：“金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标”，要求“要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改”。

经中央网络安全和信息化领导小组批准，首次全国范围的关键信息基础设施网络安全检查工作于 7 月底启动，至 12 月底结束。此次检查由中央网信办牵头组织，各省（区、市）网络安全和信息化领导小组与中央和国家机关将统一领导本地区、本部门的网络安全检查工作，各省（区、市）网信办统筹组织本地区检查工作。除中央和国家机关及其直属机构外，党政机关、企事业单位主管的关键信息基础设施，根据党政机关、企事业单位的注册登记地，纳入所在省（区、市）检查范围。

3.4.1.3 公安部开展全国工业控制系统安全大检查

2016 年 6 月至 10 月，公安部成立了专门领导机构和由各地公安厅（局）领导挂帅的检查工作领导小组，明确工作职责、任务和流程，采取单位自查、远程技术检测和现场安全检查相结合的方式，对全国范围内电力、通信、铁路、航空、航天、交通、石油、石化、核工业、矿山、冶金、水利、烟草、制造、邮电通讯、环保、医疗、市政（轨道交通、城市燃气、热网、排水、污水处理）等 18 个重点领域的工控系统进行了全面检查。

在现场检查阶段，借助北京匡恩网络科技有限责任公司提供的技术支撑，对全国 28 个省（自治区、直辖市）所辖 104 个地市的 451 家单位的工控系统安全状况进行了现场抽查。通过对检查数据的深入分析，陆续发现了西门子等国外知名工控设备存在大量漏洞，占比高达 93%，其中危急和高危漏洞占比达到 50% 以上，其中发现工控系统漏洞约 1 万 5 千个（次），操作系统漏洞 4 万 7 千个（次），并发现了近 20 起以混合程序攻击、病毒木马以及漏洞攻击等为主的网络安全威胁事件，全面、客观、准确地掌握了被检查单位工业控制网络安全状况，为完善我国工控系统信息安全法律、法规和标准体系提供了科学依据，为国家相关部门提高监管针对性提供了重要技术支撑。

3.4.1.4 工业和信息化部印发《工业控制系统信息安全防护指南》

2011 年 9 月，工信部印发《关于加强工业控制系统信息安全管理的通知》工信部协 [2011] 451 号文（简称 451 号文），掀开了工业控制系统安全的“面纱”，通过规范管理等要求，使各工业企业单位，理解工业控制系统安全的重要性。时隔 5 年，2016 年 11 月工信部印发《工业控制系统信息安全防护指南》（简称指南），从 11 项 30 个要点详细明确安全防护工作的指导方针。并且《指南》所列 11 项要求充分体现了《国家网络安全法》中网络安全支持与促进、网络运行安全、网络信息安全、监测预警与应急处置等法规在工控安全领域的要求，是《国家网络安全法》在工业领域的具体应用。

3.4.1.5 工信部发布《关于开展工业控制系统信息安全管理体系建设》试点工作函

2016 年 5 月，工业和信息化部电子工业标准化研究院信息安全中心和工业控制系统信息安全产业联盟向一些中大型智能制造企业发布了《关于开展工业控制系统信息安全管理体系建设》试点工作函。工业和信息化部电子工业标准化研究院信息安全中心和工业控制系统信息安全产业联盟希望借鉴一些企业 2015 年智能制造试点示范项目中取得的成功经验，共同开展工业控制系统信息安全管理体系建设试点工作。该项目的目标是为了验证国家标准《工业控制系统安全控制应用指南》、国家标准《工业控制系统安全管理基本要求》在轨道交通行业和企业应用的可行性；同时，建立工业控制系统信息安全管理配套制度，形成符合自身安全需求的工业控制系统信息安全管理体系。

3.4.1.6 中央网信办等六部门共同举办网络安全宣传周活动

2016 年 3 月 17 日，中央网信办发布《关于印发国家网络安全宣传周活动方案的通知》。

今年的网络安全宣传周在 9 月 19 日 -25 日举行，主题是“网络安全为人民，网络安全靠人民”，由中央网信办、教育部、工信部、公安部、新闻出版广电总局、共青团中央等六部门共同举办。根据《国家网络安全宣传周活动方案》关于宣传周开幕式等重要活动可根据地方实际情况安排在省会城市举行的精神，今年宣传周的开幕式、网络安全博览会、网络安全技术高峰论坛、网络安全电视知识竞赛等重要活动在武汉市举行。中央领导、有关部门负责同志，湖北省和武汉市负责同志，以及企业专家代表将出席开幕式等活动。

3.4.1.7 《工业自动化和控制系统网络安全》等 6 项国家标准正式发布

2016 年 10 月 13 日，国家质检总局、国家标准委联合召开新闻发布会宣布，《工业自动化和控制系统网络安全》等 6 项重要国家标准，由国家质量监督检验检疫总局、国家标准化管理委员会于 2016 年 10 月 13 日正式批准发布，将陆续实施。这批 6 项推荐性国家标准分别是：

- GB/T 33007-2016《工业通信网络　网络和系统安全　建立工业自动化和控制系统安全程序》；
- GB/T 33008.1-2016《工业自动化和控制系统网络安全　可编程序控制器（PLC）》；
- GB/T 33009.1-2016《工业自动化和控制系统网络安全　集散控制系统（DCS）　第 1 部分：防护要求》；
- GB/T 33009.2-2016《工业自动化和控制系统网络安全　集散控制系统（DCS）　第 2 部分：管理要求》；
- GB/T 33009.3-2016《工业自动化和控制系统网络安全　集散控制系统（DCS）　第 3 部分：评估指南》；
- GB/T 33009.4-2016《工业自动化和控制系统网络安全　集散控制系统（DCS）　第 4 部分：风险与脆弱性检测要求》。

3.4.2 行业协会、联盟等社会组织积极参与

3.4.2.1 成立关键基础设施保护工作委员会

2016 年 7 月 16 日，在京召开的首届中国网络安全产业大会暨关键基础设施保护高峰论坛上，中国网络安全产业联盟宣布，旗下第一个工作委员会——关键基础设施保护工作委员会正式成立。该委员会旨在促进我国关键基础设施重点行业以及建设、运营企业对于网络安全的认知和重视，集合各方力量，整合资源，促进跨行业的技术联合与创新，提高我国关键基础设施网络安全的防护水平。

该委员会由北京匡恩网络科技有限责任公司、中电长城网际系统应用有限公司及北京创原天地科技有限公司等数十家企业联合发起成立。主要职责包括：协助相关部门制定相关国家标准及行业标准；连接关键基础设施保护上下游企业、整合产学研相关机构，共同推动行业创新与发展；加强与涉及基础设施的重点行业和建设、运营企业的沟通、协调和合作，大力推进对网络安全的认知和重视；积极拓展与国内外企业及行业间技术交流，促进国内企业的国际化视野，力争赶上国际先进国家的防护水平；积极开展行业人才培养，建立专家人才库，建立分层级、专业化的人才培训体系等。

3.4.2.2 召开“2016 中国（杭州）网络安全和信息化高峰论坛”

9 月 21 日经中央网络安全和信息化领导小组批准，由中央网信办网络安全协调局、中共浙江省委网络安全和信息化领导小组办公室、浙江省经济和信息化委员会指导，中国网络空间安全协会、浙江省信息经济联合会主办，杭州安恒信息技术有限公司承办，阿里云计算有

限公司、杭州海康威视数字技术股份有限公司、浙江省计算机信息系统安全协会协办。论坛主题是“弘扬网信精神，共筑安全防线”。在峰会上，多所国内高校以及众多企业就网络空间安全多个议题展开讨论，其中，网信人才培养成为讨论焦点。

3.4.2.3 全国首个关键基础设施控制网络防护技术工程实验室批复成立

匡恩网络于 2016 年 1 月经北京市发改委批准成立了“关键基础设施控制网络安全防护技术北京市工控实验室”。本工程实验室面向关键基础设施网络互联互通急需解决的控制网络安全问题，开展工业控制网络安全检测、安全防护和态势感知等技术研发和工程平台建设。本工程实验室旨在建立一个关键基础设施控制网络安全防护前沿创新技术研究和防护产品的研究、验证、仿真、测试综合平台，面向大规模关键基础设施控制网络应用的分布式防护产品关键技术研究和产品开发，开展广泛第三方合作，为多个目标行业客户提供安全运维、风险评估、安全检测服务，为我国重点产业领域关键基础设施控制网络运行提供技术支撑和安全保障，成为我国关键基础设施控制网络安全共性技术和产品研发基地、产业化技术中心、人才培养中心以及国家和行业相关标准的研究制定机构。

3.4.2.4 云安全联盟 CSA 发布物联网安全指南

云安全联盟于 10 月 7 日发布的长达 80 页的指南，指出物联网安全的必要性。

随着关键国家基础设施逐渐依赖物联网，汽车日益联网，物联网能被用来发起 DDoS 攻击。此外，无人机正“迈入”主流地位，并被作为侦察平台，物联网产品一般会“影响隐私”。

云安全联盟在新的物联网建议中指出，以安全开发方法起步是关键。这就意味着开发人员必须从一开始就满足联网设备的安全要求和过程。开发人员应该谨慎。物联网时常物理暴露在不完全的环境中，这就意味着不应只在通信层面实现安全。设备会被物理窃取，共享密钥被解除。

3.4.2.5 召开第五届工业控制系统信息安全峰会

工业控制系统信息安全峰会至 2016 年已成功举办五届，峰会由工业控制系统信息安全产业联盟（ICSISIA）主办，ICSISIA 秘书处及控制网（kongzhi.net）&《自动化博览》承办。

第五届工业控制系统信息安全峰会目前已完成第一站、第二站及第三站的举办。第一站及第三站的举办地均在北京，第二站的举办地为杭州。此次峰会（即第三站）共邀请来自电力、石化、冶金、核电、水利、航天等领域的行业用户单位、系统集成商、产品供应商、设计院、大专院校及科研单位的 120 多位代表出席，共同深入交流当前工业控制系统信息安全政策、标准、技术、应用等多方面的最新研究进展，探讨远程测控系统的未来发展趋势。

3.4.2.6 成立可信工控网络安全专委会

2016 年 11 月 03 日——中关村可信计算产业联盟中国可信计算技术创新与产业化论坛“可信工控网络安全分论坛”在京隆重开幕，可信工控网络安全专委会（以下简称专委会）同期宣布成立，北京匡恩网络科技有限责任公司任主任单位。

随着快速的网络化趋势，工业控制系统网络安全已成为国家关键基础设施安全，城市运行安全，工业生产安全重要有机组成部分和重要保障。在技术驱动、需求拉动和市场开放的共同作用下，在中关村可信计算产业联盟支持下，北京匡恩网络科技有限责任公司发起倡议，联合北京工业大学、北信源、立思辰等 27 家优秀企业建立可信工控网络安全专委会，共同推动可信计算在工控领域的推广和发展。

可信工控网络安全专委会的成立，赋予了各成员单位更多的责任和义务。匡恩网络倡议专委会着力从六个方面推动并确保可信工控网络安全的全面发展，具体而言就是：进一步推广可信工控网络安全理念，丰富我国可信工控网络安全系列产品及整体解决方案，推动可信在工控领域的行业创新与发展，推动可信工控网络安全产品标准的制定和可信工控网络安全人才培养，全面配合联盟及做好技术支撑工作。

3.4.3 行业内重要安全厂商积极布局

3.4.3.1 专业工控安全厂商活动

专业工控安全厂商成立时间都较短，但他们 100% 专注于工控安全业务，工控安全业务的成败决定了公司的生死存亡，因此能够全力投入。专业工控安全厂商中目前北京匡恩网络科技有限责任公司所占市场份额最大，实力最强。

匡恩网络成立以来一直专注于工控网络安全领域的安全研究。从 2016 年 6 月 30 日至 9 月 6 日，匡恩网络作为杭州二十国集团峰会（以下简称“G20”峰会）网络安全保卫技术支持单位，全程参与了公安系统检查，经历了重点单位检查、重点单位复查、各分区初查、各分区复查等阶段，圆满完成了大会安保服务工作，收到来自 G20 峰会网络安全保卫组和浙江省公安厅的感谢信，获得公安部和浙江省厅的高度肯定，确保了峰会期间工业控制系统持续、稳定运行，为 G20 峰会的成功召开做出了重要贡献。

目前，随着互联网的长尾效应在工业领域正在凸显，数以千万计的工业设备开始接入互联网形成工业物联网。随着“中国制造 2025”国家战略的深入发展，工业物联网成为我国探求生产力变革，助推生产效率提升的关键。但同时，工业物联网安全面临着严峻挑战。高速发展必须有安全守望，安全性是工业物联网健康发展的重中之重。如何摆脱在“在别人地基上盖房子”的尴尬与无奈，避免重蹈互联网安全滞后于应用的覆辙，是中国工业物联网安

全领域致力于解决的迫切问题。工业物联网安全正在快速成长为一个战略新兴产业，我国有能力成为该领域的先进国家，并主导该领域的发展，建立全球影响力。因此，匡恩网络逐渐由工控安全扩展到工业物联网安全。对于工业物联网安全的产业化发展，一个系统化安全保障体系将是其实践运营的核心支柱。匡恩网络对国内外各个行业的工业物联网系统进行大量深入调研，全面了解工业物联网的安全特性。并以此为起点，总结更多行业存在共性特点，充分考量细分行业特点和特定属性，为更多行业提供定制级解决方案，快速广泛应用与实施。这是促进工业物联网安全规模化应用和产业发展的有效路径。

在工业生产的实践中，匡恩网络将“4+1 安全保障体系”作为有效方法论，将其与集合人工智能算法、工业协议深度分析、模式匹配、智能感知等前沿技术的多系列近二十款产品深度结合应用，为涉及关键基础设施、智能制造、智慧城市、军民融合四个领域的十多个重要行业提供定制级的一体化解决方案。

在 2016 年 9 月的国家网络安全周，匡恩网络重磅发布两款针对工业物联网安全的双子星新品：威胁态势感知平台和漏洞挖掘云服务平台，深度发力工业物联网感知与服务，有效解决工业物联网安全应用中存在的痛点和盲点，与跨行业、跨领域的解决方案深度融合，实现从感知到应用到服务的纵向整合。目前，匡恩网络已构建了丰富的产品体系，已完成包含检测、保护、审计、终端、管理、实训、E 能互联及其他等 8 大系列、20 多条产品线，成为国内首家以全产品线和服务覆盖智能工业安全企业务领域的公司。

从技术创新到管理模式创新，从单一产品到纵深联动，匡恩网络自主可控工业物联网安全解决方案改变了传统安全产品简单堆砌的被动防御模式，实现了风险提前预知、设备纵深联动、管理精准及时的主动防御方案，从网络安全、主机安全、应用安全、数据安全四个层面全面保障控制系统网络安全和设备安全。匡恩网络工业物联网安全解决方案广泛在水利、电力、交通、燃气、供水等关键基础设施保护，以及石油化工、冶金、烟草、智能汽车、智能制造等国家重点行业和领域成功应用，并深受好评。

同时，匡恩网络吸收工业互联网的威胁态势感知平台，构建基于云技术和大数据技术的工业物联网安全态势中心，为大中型企业、地方政府、行业监管部门的工业物联网各层面网络提供全方位安全监测与防护，实现早期预警、态势感知、攻击溯源和有效应对。

经过近三年时间的深耕，从创建方法论，到产品和解决方案深度应用，再到构建工业物联网安全态势中心，匡恩网络“点面结合”纵深推进工业物联网安全的产业发展。2016 年，匡恩网络在工业物联网安全领域的深耕，迎来蝶变，在工控网络安全领域的规模和市场份额均居榜首，成为中国工业物联网安全领域的创新先锋和重要支撑力量，得到中央网信办、公安部、工信部等中央和政府部门的高度认可；并作为第一第二单位负责牵头制定“工控漏洞挖掘”、“智慧城市安全”、“数控安全”、“工控网络监测”、“工控网络安全隔离与信

息交换”等多项国家标准。

3.4.3.2 自动化背景厂商的安全活动

自动化背景厂商原从事自动化相关业务，由于看好工控安全的市场机遇，或者本身产品就涉及到工控安全，因此成立工控安全部门或子公司进入工控安全领域。这类公司的特点是对工控系统有比较深刻的理解，有现成的客户资源。当前在工控安全领域影响力较大的如国外的施耐德、西门子等，国内的如北京和利时，浙大中控等。

以施耐德电气为例，2016 年 10 月 24 日，施耐德电气与国家计算机网络应急技术处理协调中心（简称“CNCERT”）于北京签署工业网络安全技术与服务合作备忘录。双方将在网络安全领域建立战略合作伙伴关系，并在工业控制系统安全领域开展联合技术研究、设备检测认证和安全事件应急等方面的合作。

双方将从以下四大方面着手保障工业信息安全：

- 工业控制信息安全解决方案的共同开发：针对工业控制领域信息安全的解决方案进行合作开发，提高企业信息安全设计水平。

- 工业控制信息安全标准制定工作的共同推进：就国际工业控制信息安全标准如何落地中国共同开展调研、交流等，推进中国工业控制信息安全标准的制定推广工作，尽早落实权威性标准发布。

- 共建工业控制系统网络安全应急技术工信部重点实验室：实验室将聚焦工业控制系统网络安全态势感知、工控安全事件应急处置和工控设备安全检测等领域开展研究工作。在此基础上，共建工控系统网络安全仿真实验平台。以此推进工业信息安全建设并打造示范性案例。

- 形成工控安全事件共享通报处置机制：围绕工业控制系统网络安全应急体系的事前预警、事中发现、事后处置等环节，建立施耐德电气相关工业产品的漏洞及安全事件共享、通报及处置机制。完善当下技术、管理上对风险的预警和应急处置预案。

由此可见，国外自动化厂商为了更好的进入中国市场并且扩大其在中国市场的占有份额，开始寻求加强与中国政府及安全企业的多方面的合作，从而更有效地提高其产品及服务的安全性。

3.4.3.3 IT 安全厂商的安全活动

IT 安全厂商在信息安全领域的技术积累较多，但对工控系统缺乏深刻的理解，在工控安全方面的投入较小，但都已成立相关的工控安全部门或子公司来进入工控安全领域，其中部

分互联网企业通过在物联网安全领域的投入，涉猎到工控安全防护的部分内容，如：阿里巴巴、华为、中国电信等。

其中，阿里巴巴的阿里云在物联网安全领域投入较大，2016 年阿里云分别发布了《数据安全白皮书》及《智能物联安全白皮书》。

（1）《数据安全白皮书》

2016 年 7 月阿里云在云栖大会成都峰会发布《数据安全白皮书》（以下简称白皮书），首次公开了阿里云在保障 230 万用户数据安全方面建立的流程、机制以及具体实践办法。

阿里云邀请全球顶尖安全技术专家持续进行“红蓝军”攻防对抗，并将对抗结果与生产环境中所遭受的威胁结合，更新跌代威胁分析工具、安全评估方法论，让数据安全防御形成一个持续迭代更新的良性循环系统。白皮书介绍，所有开发、维护、客服以及其他可能接触到阿里云内部系统的人员，他们的每次登陆都有严密的身份识别，确保帐号与生产设备“不会误用”、“不被盗用”、“不能乱用”。

当前，阿里云保护着全国 35% 的网站。2015 年，阿里云安全团队共监控到 DDoS 攻击事件超过 10 万次，其中流量达到 300Gbps 以上的攻击次数有 66 次，最大攻击峰值流量达到 477Gbps。

（2）《阿里智能物联安全白皮书》

近日，阿里巴巴安全部集团标准化团队、OS 事业群 - 阿里智能联合发布了《阿里智能物联安全白皮书》。

阿里智能物联是阿里巴巴集团自主创新的物联网服务产品，旨在为厂商和用户提供一站式的设备智能化解决方案。

图 19 阿里智能物联系统架构

阿里智能物联通过“服务平台”为厂商设备提供统一接入与管理服务。同时，“阿里智能 APP”为用户提供智能家居管理服务。设备和 APP 通过接口协议（Alink 协议）与服务平台进行交互。

阿里智能物联在产品研发流程中引入 SDL，控制产品整体的安全风险，并通过“阿里云盾”保障云端服务平台的安全，使用“阿里聚安全”为移动客户端提供安全保障，同时结合物联网业务的安全需求，为物联网智能业务信息安全提供全方位的安全保障。

综上，传统的 IT 安全厂商由于普遍缺乏对工业控制系统的深入了解，因此其在工控安全的投入尚不足。而“互联网”背景的厂商（如阿里、腾讯等）已经开始关注物联网安全，并且开始加大人力、物力及财力方面的投入。

第四章

我国工业控制网络安全态势分析

随着“两化融合”逐步深入，工业控制系统安全隐患和风险不断涌现。面对日益严峻的工控安全问题，我国各地方政府积极探索建立健全工控网络安全管理体系，不断增强政府部门工控网络安全监管力度。

目前，工业控制系统重点应用在炼油、石化、电力、冶金、建材、交通、电网、水网、气网、国防等关系到国家和社会稳定、经济正常运行的重要领域。随着我国大力推进信息化建设，工业控制系统在我国各行业的应用范围和部署规模快速增长，工业控制系统已成为国家关键基础设施的“中枢神经”。其中，公用事业行业，大中型城市的燃气输配、供电、供水、供暖、排水、污水处理等均采用了智能工业控制系统；以石油石化天然气为代表的能源行业，从大型油气田到数万公里的原油、天然气和成品油输送管线，大规模采用工业控制系统；电力行业，发电、调度、变电、配电和用电等各个环节都离不开工业控制系统；以铁路为代表的公共交通行业，远程监控系统已具规模，若干铁路局采用了先进的工控系统实现调车作业自动化；水利行业，国家防汛指挥系统采用工控系统进行区域和全国联网。

我国近几年工业控制系统的安全事件屡有发生，如钢厂异常停机、石化工厂蠕虫泛滥等等，这些层出不穷的安全事件，为我国关键基础设施核心要害系统安全问题敲响了警钟。分析工控系统所遭受的漏洞和攻击，可以看出工业控制系统漏洞攻击正向着简单控制器受攻击增大、利用网络协议进行攻击、专业攻击人员进行攻击、利用病毒进行攻击、工控信息系统漏洞挖掘与发布同时增长的趋势发展。

随着信息化与工业化深度融合，工业控制系统正趋于使用通用协议、通用操作系统、通用硬件和软件，现在以太网、无线设备无处不在，整个控制系统都可以和远程终端进行互连，网络安全问题直接延伸到工业控制系统，使得工业控制系统固有漏洞和攻击面不断增加。兴趣索然或金钱驱动的黑客、一不留神误操作或蓄意报复的业内人士、愤世嫉俗恐怖分子、政治意图明确组织使得我国工业控制系统信息安全内忧外患。

4.1 我国工控网络安全概述

我国工控系统中大量存在漏洞和隐患，包括：系统体系结构存在共性安全隐患、工控系统自身存在安全漏洞、工控系统运行所处的系统和环境存在安全漏洞和隐患。工业控制系统组件漏洞的数量并没有逐年减少，而近一半的已识别漏洞是高风险的，大多数漏洞在最知名的供应商的产品中被发现，SCADA 系统最脆弱，同时也很常见。随着信息化建设深入，工控系统开始同生产管理、ERP 系统、电子商务系统等相连并逐渐纳入到统一的信息系统中，但在此过程中相关分区隔离等信息安全问题并未得到充分认识和重视。

近年，我国对工业控制系统网络安全的重视也上升到国家层面，从中央网络安全与信息

化领导小组的成立，到各政府部门设立专职岗位管理；从“互联网 +”“中国制造 2025”等国家战略方针的推出，到各地开展针对工业控制系统网络安全工作；从工信部发布《关于加强工业控制网络安全管理的通知》，到《国家网络安全法》的颁布；从首个国家工控安全技术国家工程实验室的成立，到网络空间一级学科的正式成立，都预示了工控安全在我国也将进入国家战略层次。

4.1.1 工控网络设备安全概况

随着工业 4.0 的高速发展，工业自动化程度越来越高，工控设备暴露在公网的情况也越发明显，其安全问题也日趋严重，据匡恩网络工业控制威胁情报中心统计，截至 2016 年底，中国境内暴露在互联网的工控设备高达 1143 个，以下为联网工控设备区域分布图（信息敏感，下图仅为示意图）。

图 20 全国接入互联网的工控设备区域分布图
数据来源：匡恩网络

从工控设备类型的角度看，此次在线监测采集到的数据中，可编程逻辑控制器（PLC）为接入互联网数量最多的设备，其次为远程控制终端（RTU），这些设备的来源多为国外厂商，其安全性不可控，国内工业企业在使用中尤其需要注意此类设备的安全问题。

从设备厂商来源的角度看，此次工控设备在线监测发现：暴露在互联网上的工业控制系统涉及到国内外多家控制系统厂商（信息敏感，内容有删减），相关单位应给予高度重视。

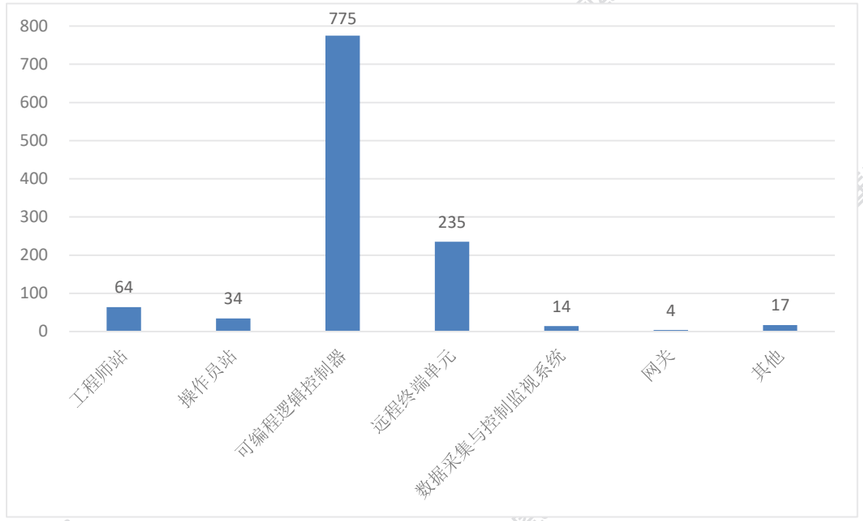


图 21 全国接入互联网的工控设备按类型统计图
数据来源：匡恩网络

4.1.2 工控网络安全漏洞概况

截至 2016 年底，根据中国国家信息安全漏洞共享平台 [CNVD] 所发布的 2016 年新增工业控制系统漏洞信息，并经过匡恩网络的统计分析，2016 年新增公开工控漏洞数量达 141 个。

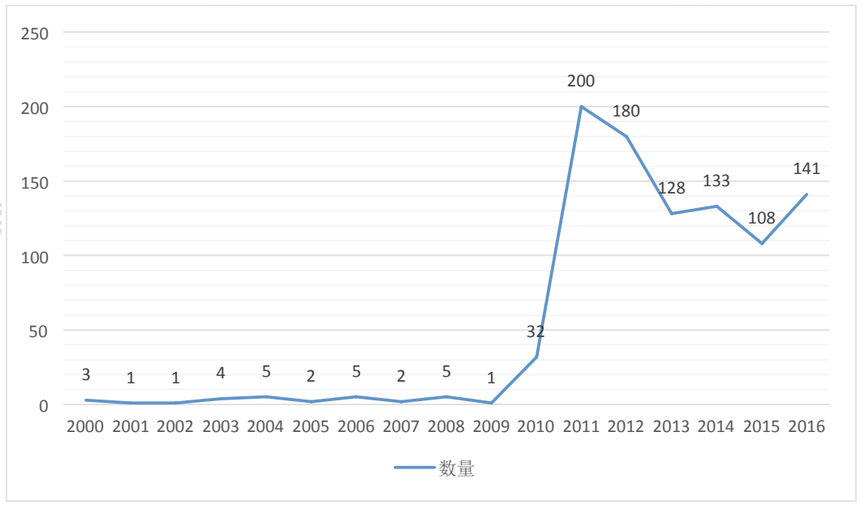


图 22 2000-2016 年公开工控漏洞趋势图
数据来源：CNVD、匡恩网络

从上图可以看出，2000 年以来公开发布的工控系统新增漏洞数量大幅增长，2010 年前，公开的工控系统漏洞数量相对较少，每年新增不超过 5 个。2010 年以后快速增长，2011 年公开工控系统漏洞多达 200 个，此后几年均超过 100 多个，截止到 2016 年底，累计漏洞总数已超过 900 多个，工控系统面临的安全问题愈加严峻。

- 工控系统漏洞涉及的厂商较为集中

根据匡恩网络工业控制网络威胁情报中心研究发现：工控系统漏洞涉及的厂商较为集中，而且多为在我国工控领域所占市场份额较大的厂商（信息敏感，内容有删减）。

- 工控系统漏洞危害性集中于服务器系统和工控数据

根据本次对 2000 年以来新增漏洞危害性分析，缓冲区溢出、信息泄露、输入验证、跨站脚本等类型的工控漏洞数量居多，对工控系统的危害主要集中在服务器的系统和数据中。

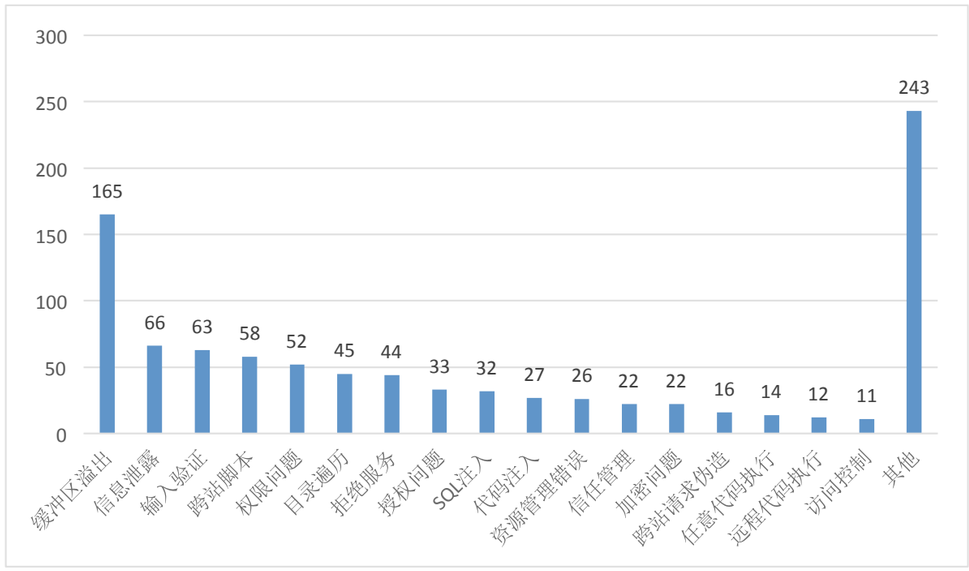


图 23 2000-2016 年公开工控漏洞主要类型统计
数据来源：CNVD、匡恩网络

如上图所示，从已公开的工控系统漏洞类型来看，缓冲区溢出类型的漏洞高居榜首，漏洞数量达到 165 个，其次分别为信息泄露、输入验证、跨站脚本、权限问题类型的漏洞，数量分别达到 66、63、58、52 个。由于以上五种漏洞类型都能够造成工控系统服务中断、系统停机、信息泄露，甚至是物理性破坏，因此常常被黑客、病毒及恶意程序所利用，危害性

十分巨大。利用缓冲区溢出攻击，可以导致程序运行失败、系统宕机、重新启动等后果，甚至可以利用它执行非授权指令，对工业现场的智能设备下发非法指令（例如修改运行参数、关闭阀门开关等），以达到其攻击目的。

信息泄露方面的漏洞对工控系统的影响主要体现在两个方面：一方面企业内部的工艺流程、图纸、排产计划等关键信息容易成为攻击者窃取的对象，所以对这些关键数据的保护构成严重威胁；另一方面信息泄露的漏洞经常被攻击者利用间谍工具来收集被攻击目标各种信息，为真正的网络攻击方式、工具的使用提供情报。

另外，值得一提的是输入验证类漏洞明显增多（该类漏洞在信息网的漏洞中已经并不多见），身份验证类漏洞允许攻击者利用漏洞绕过某些安全限制，让攻击者很容易就能够在系统中执行任意代码。

- 工控系统漏洞影响的工控系统产品类型较为集中

由于 PLC、DCS 等工控系统在工业领域的大规模应用，其受工控漏洞的潜在威胁也最为严重，如下图所示：

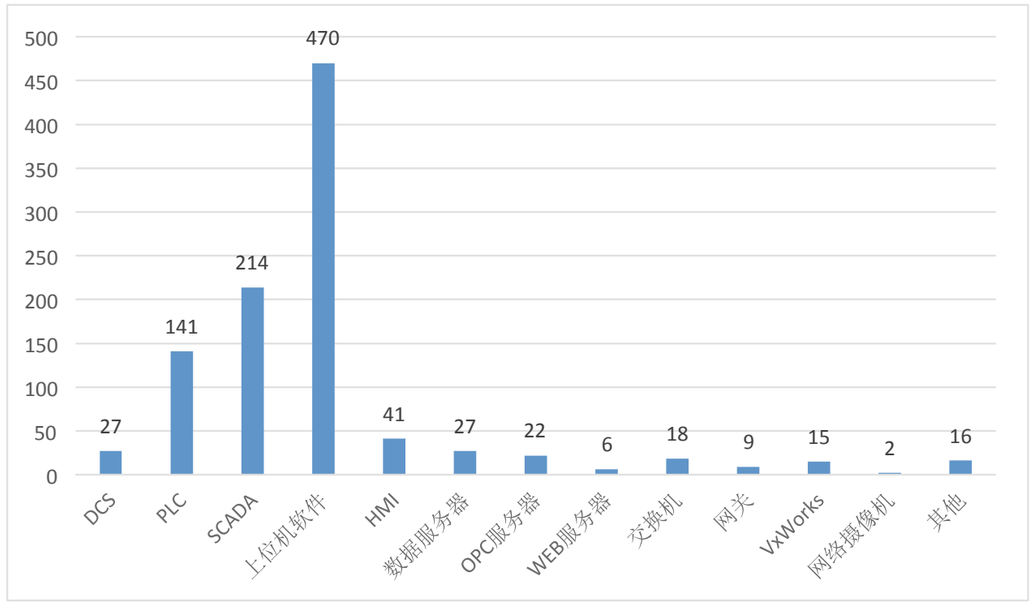


图 24 2000-2016 年公开工控漏洞影响产品统计
数据来源：CNVD、匡恩网络

根据上图中展示的 2000-2016 年公开工控漏洞影响产品统计数据，其中上位机、SCADA、PLC 历年累计已公开的工控系统漏洞数量分别达到了 470、214、141，成为了工控系统产品中最“脆弱”的产品组件。这三类产品在我国电力、水利、污水处理、石油化工等国家关键基础设施和冶金、汽车、航空航天等制造业工业领域应用十分广泛，属于无法替代的关键角色。因此，就工控系统而言，三类产品的健康状况也决定了工控系统本身的“免疫”能力。

4.1.3 各区域工控网络安全概况

近三年来，匡恩网络作为核心技术支持力量，在国家相关部委的统一部署下，出色地完成了多次全国性的安全检查任务；同时匡恩网络广泛与工业企业、科研院所等单位合作，开展了多种形式的安全研究和项目实践，积累了大量一手材料；在此基础上，匡恩网络搭建了工业物联网安全大数据分析平台，接下来我们从工控安全组织建设、核心设备和资产管理、安全经费和风险统计、等级测评、网络边界管理、日志及安全审计管理、恶意代码防范管理、安全漏洞管理、安全事件处置与追责、应急预案和演练、运维服务、教育培训情况等 12 项指标对我国 7 个不同区域的工控网络安全状况进行总体评估，得出各区域工控网络安全综合指数（如下图所示）。

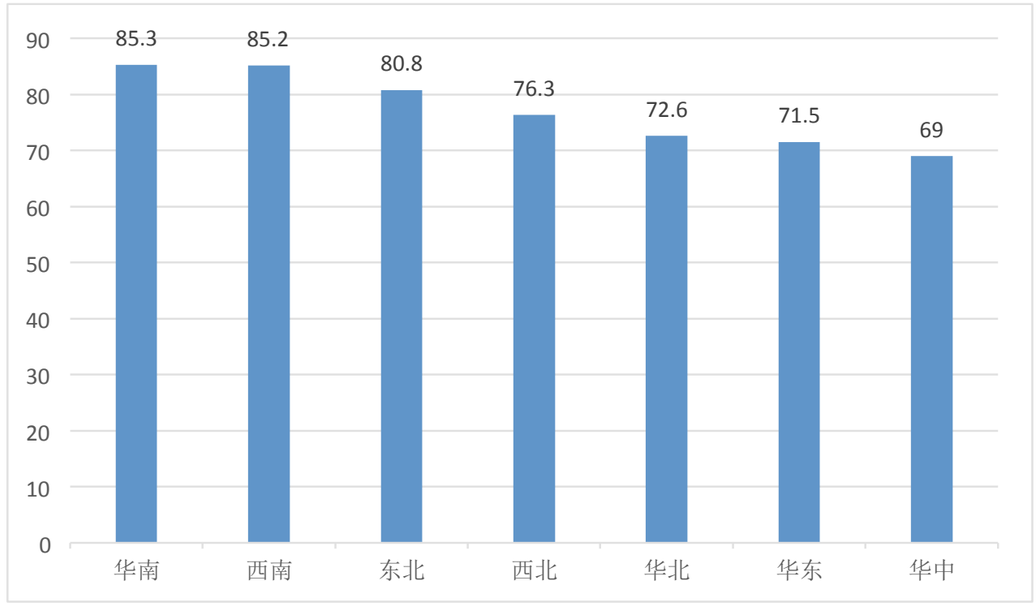


图 25 各区域工控网络安全综合指数统计
数据来源：匡恩网络

可以看出，我国各区域工控网络安全水平总体水平偏低（平均 76）、各区域参差不齐，华南、西南较好，华北、华东较低，华中最低。我国华东、华北等发达地区工业、公共设施相对其他区域发达，工业控制系统应用范围广、数量大、发展速度快，漏洞、病毒木马等网络威胁及基层防护薄弱等问题反而更加突出，因此，工控网络安全综合指数相对较低。

匡恩网络工业控制网络威胁情报中心深入研究发现，全国各省市工控网络安全状况参差不齐，整体状况令人堪忧（信息敏感，内容有删减）。

4.1.4 重点行业工控安全概况

通过匡恩网络对我国电力、通信、铁路、航空、航天、交通、石油、石化、核工业、矿山、冶金、水利、烟草、制造、邮电通讯、环保、医疗、市政等 18 个重点行业的工控系统安全调查，发现各行业的工控安全情况不尽相同。根据调查的结果依据工控安全组织建设、核心设备和资产管理、安全经费和风险统计、等级测评等 12 项指标进行综合打分，得出每个行业的综合分数（即综合指数），如下图所示。

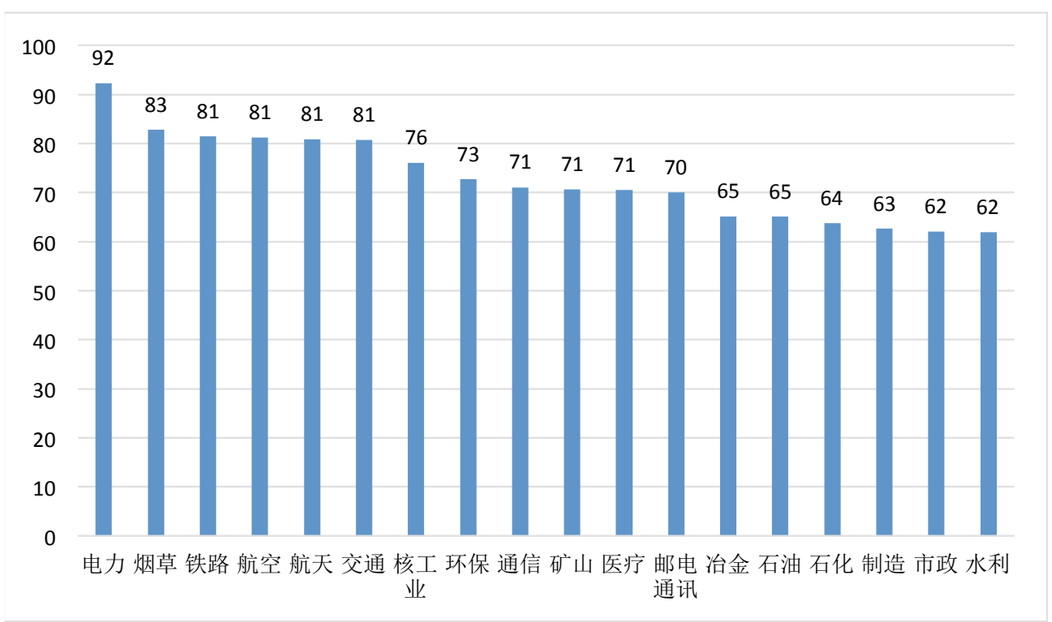


图 26 重点行业工控安全综合指数统计
数据来源：匡恩网络

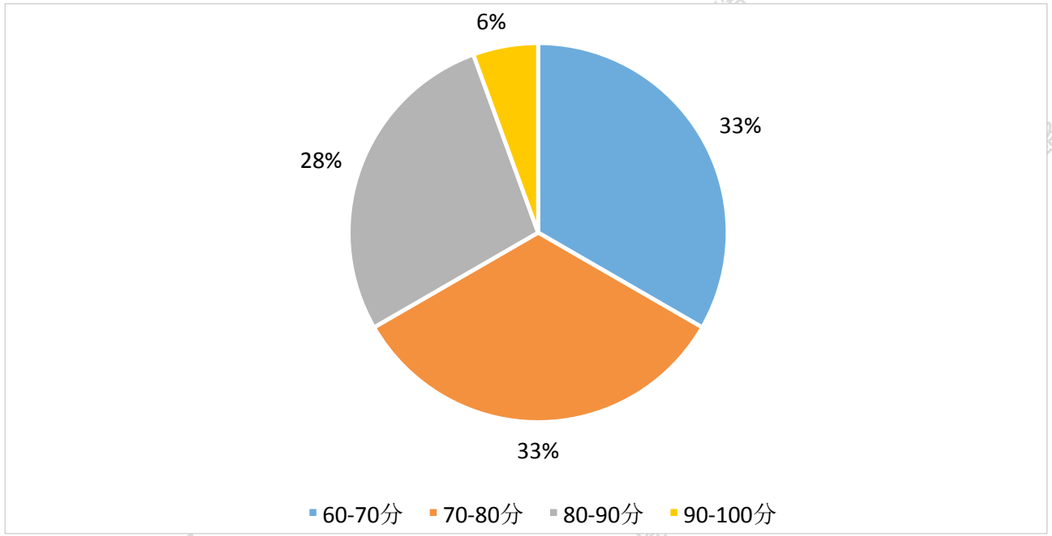


图 27 重点行业等级统计
数据来源：匡恩网络

从上面两幅图可以看出，在这 18 个行业中，只有电力 1 个行业综合指数最高，分数在 90-100 分数段，占比为 6%；其次是烟草、铁路、航空、航天、交通等 5 个行业综合分数在 80-90 分数段，占比 28%；综合指数最低的是冶金、石油、石化、制造、市政、水利等 6 个行业，占比为 33%。

（1）综合指数在 90-100 分的行业工控安全情况

在此分数段的只有电力行业，该行业的工控情况较好。该行业有明确的部门、岗位和人员以及责任和义务；有较多的安全经费年度预算；定期对工控系统开展等级保护测评工作；安全事件处置机制较完善；对不同的安全事件备有不同的应急预案与演练；定期开展安全教育培训。但是，在恶意代码防范方面和终端设备、核心资产保护方面存在不足。

（2）综合指数在 80-90 分的行业工控安全情况

在此分数段的有烟草、铁路、航空、航天、交通等 5 个行业，这些行业的工控安全情况是在强化组织建设方面有相对较明确的部门、岗位和人员以及责任和义务；在安全经费预算方面基本能按照国家和行业监管部门有关要求落实专项资金，专款专用；在系统定级备案、等级评测方面能定期对工控系统开展等级保护测评，形成常态化工作机制。但是，在安全事件处置、应急预案与演练方面存在没有制定安全事件报告和处置管理制度以及应急处理流

程、系统恢复流程、事后教育和培训等落实较差等问题；在日志及安全审计、组态权限设置、USB 防护方面存在较严重的问题。

（3）综合指数在 70-80 分的行业工控安全情况

在此分数段的有核工业、环保、通信、矿山、医疗、邮电通讯等 6 个行业，这些行业的工控安全问题主要在网络安全管理和技术防护方面突出。由于技术力量、人员配备、资金等方面的限制，工控系统网络安全防护方面较为薄弱，存在一些问题，如工控安全教育培训较薄弱、办公网与生产网网络边界划分不清晰等，工控安全体系的建设落后，没有制定网络安全管理制度，没有采取网络安全防护措施。在国产化方面，大部分的设备、软件、数据库都是国外进口，其中 90% 以上的核心控制器都是来自西门子、施耐德、ABB 等国外品牌。在终端设备、核心资产方面只有部分系统部署了专门的工控安全设备，如核工业、矿山行业。

（4）综合指数在 60-70 分的行业工控安全情况

在此分数段的行业有冶金、石油、石化、制造、市政、水利等 6 个行业，这些行业的安全问题突出。主要由于在强化组织建设方面没有明确的部门、岗位和人员，责任划分不清，追责不到位；在安全经费方面没有足够的资金预算；系统定级备案、等级评测工作落实不到位；对安全管理活动中重要的管理内容没有建立安全管理制度，对安全管理人员或操作人员执行的重要管理操作没有建立操作规程。在安全事件处置方面没有制定安全事件报告和处置管理制度；在工控安全教育培训方面落实较差，没有定期组织开展信息安全政策宣贯培训，提高领导层的认识，提高员工信息安全防范意识。在日志安全审计、防恶意代码、数据保护以及漏洞管理方面没有明确的有效措施实施。

通过以上分析，我国工业控制系统的安全应该引起足够的重视，需要提高工业控制系统的安全意识，从系统层面和网络层面加强针对性的防护措施。国家更要建立健全的应急响应机制，各方联动，提供更有价值的威胁情报信息，建立更有实用性的威胁情报库，为政府机构、安全厂商、企事业用户提供更好的支持。同时需要积极发展信息技术，做好整个防护体系的“供应链”安全，特别是在国家工业领域一些关键基础设施和重要信息系统新建项目上，必须要强化项目规划和设计阶段的信息安全风险评估，整体考虑工业控制系统安全体系，加大投资，大力发展具有自主知识产权的安全防护技术和产品。

4.2 我国工业企业控制网络安全问题分析

工业控制系统的安全可靠运行一直是工业控制各相关行业最为关注和重视的方面，但传统的工业控制安全技术主要是针对系统的功能安全，主要考虑由于随机软硬件故障所导致的

组件或系统失效对健康、安全或环境的影响。而在信息安全领域中，要从全方位去考虑整个网络系统的信息安全，既要考虑随机工控系统软硬件功能故障等技术安全问题，还需要进一步考虑结构安全、本体安全、行为安全、基因安全问题及信息安全管理问题。我国针对工业控制系统信息安全领域的研究目前尚处在起步阶段，同美国等西方发达国家早在十多年前就已开展国家级工业控制系统信息安全研究相比，我国在工业控制网络系统信息安全技术和管理制度、标准、实践等方面都存在很大差距。

4.2.1 技术方面

大量现场调研发现我国各单位工控网络安全隐患和问题主要表现在整个工控网络系统的结构安全、本体安全、行为安全、基因安全四个层面。

- 结构安全上的隐患和问题

我们在工业企业工控网络现场发现铁路、水利、造纸、卷烟、冶金、制造、航空、核工业、医疗、港口、交通、矿业、石油等板块的工业企业的工业控制系统网络内部能够采取一些安全隔离或者访问认证的措施，但在工控网络结构上仍然缺乏全面地有效地网络边界防护、安全区域内防护、访问加密认证防护等安全防护措施及策略，同时没有风险评估。

部分电力企业生产控制网与管理信息网，基层单位网与上级主管单位网直接连接；部分煤炭企业的办公网可以直连访问生产控制网络；部分风电、矿业、铁路、港口、航空、卷烟等工业企业的外部用户可以通过 VPN 直接访问 SCADA 系统；冶金、矿业、铁路、造纸等部分工业企业使用传统防火墙进行边界防护；冶金、矿业、等部分工业企业生产控制网与管理信息网在同一网段。

- 本体安全上的隐患和问题

在工业企业工控网络现场发现铁路、水利、造纸、卷烟、冶金、制造、航空、核工业、医疗、港口、交通、矿业、石油等板块的工业企业系统主机、工控设备和移动介质、网络设备普遍采用国外品牌，因协议和配置缺陷导致工业控制系统存在大量漏洞且未修复或者未能及时修复，无法自主可控同时缺乏必要补偿性控制措施进行防护。

大多数漏洞属于拒绝服务、远程代码执行和缓冲区溢出的类别，这样的漏洞会被入侵者利用，引起设备故障或设备未经授权的操作，导致影响工控系统和组件的灵敏度和可靠性要求。

同时依据前述对工控系统漏洞危害等级的统计分析，高危与中危漏洞数量占比 93%，存在如此大量的高危漏洞隐患致使工控系统安全指数较低，同时设备的安装和维护严重依赖于国外厂商；多数工业企业工控系统上位机未能及时开展安全加固工作，存在使用过期操作系统，缺乏补丁更新；80% 以上的工业企业缺乏工控系统漏洞风险管理能力及对工控系统的

漏洞分析与评估的技术能力，不能准确掌握工控设备的漏洞和后门情况，工业控制系统组件漏洞的数量呈逐年增加态势。

- 行为安全上的隐患和问题

匡恩网络在工业企业工控网络现场发现铁路、水利、造纸、卷烟、冶金、制造、航空、核工业、医疗、港口、交通、矿业、石油等板块的工业企业工控系统普遍缺乏必要的技术手段对网络行为进行监控和审计。

电力、煤矿、化工、铁路、水利、造纸、卷烟等工业企业内部工控网络主机存在使用公网 IP 现象，未对工控系统关键设备进行信息安全审计设置，未部署必要的监控审计设备，不能及时监控网络中的攻击和异常行为，未对工控系统账户进行定期审计且缺乏对违规操作、越权访问行为的审计能力，无法有效对设备维护时的行为进行审计；多数工业企业工控系统的部署、策略配置等主要依赖厂商或系统集成商，对第三方人员缺乏严格的管控措施，部分工业企业开放工控系统的远程维护，但缺乏监控审计，在发生故障后不能快速、有效地对关键设备的操作进行溯源以及无法及时对故障进行定位。

匡恩网络通过对以上板块的工业企业异常流量威胁事件行为审计分析，发现我国重点领域工业控制系统中存在较大网络安全威胁，其中以黑客入侵、病毒木马及其他类型的威胁事件数量较多，已成为对工控系统网络进行攻击的主要形式。

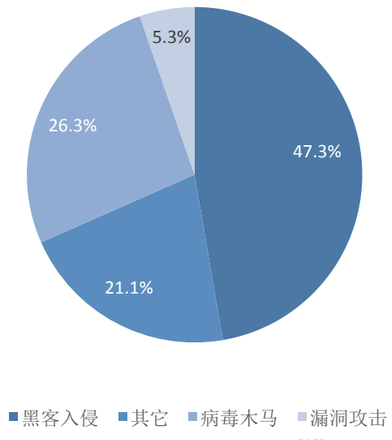


图 28 威胁事件总体分布图
数据来源：匡恩网络

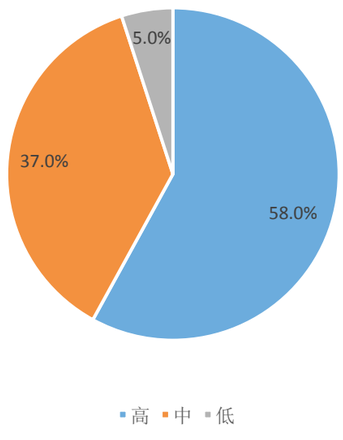


图 29 威胁事件等级分类统计图
数据来源：匡恩网络

把异常流量威胁事件的威胁按照等级进行分类，可划分为高、中、低三类，高等级威胁事件数量占比已接近 60%，以黑客入侵等为主导的网络攻击威胁事件已成为我国重点领域工控系统网络面临的严重安全威胁。

- 基因安全上的隐患和问题

匡恩网络在工业企业工控网络现场发现铁路、水利、造纸、卷烟、冶金、制造、航空、核工业、医疗、港口、交通、矿业、石油等板块的工业企业工控系统普遍缺乏基因安全的手段对工控系统进行防护，而大部分工控系统的设备、软件及工控安全产品及服务由外国主导，无法在基因安全层面实现自主可控。

目前在所有板块的工业企业中，只有电力工业企业提出的可信计算技术，其它板块的工业企业对基因安全还没有意识。在工控系统的软硬件产品应用层、内核层、硬件层等设计、生产阶段加入可信软件模块、可信芯片等核心组件，建立系统主动免疫机制，提升对未知恶意代码攻击的免疫能力，实现计算环境和网络环境的全程可测可控和安全可信。

4.2.2 管理方面

工业控制网络安全除了技术层面的问题外，在不同层级管理上也存在诸多不足，主要表现在：

一是管理体制机制不健全。基层单位注重工业控制系统的功能安全而忽视信息安全，普遍缺乏完善的系统风险评估、运行维护、安全审计、突发事件处理等管理体制机制，现场操作人员安全意识淡泊且缺乏专业培训，违规操作现象普遍。

二是系统维护行为不可控。我国 80% 以上的单位设备运维升级依赖厂商，要求工控厂商提供整改方案或转向第三方厂商购买安全解决方案，对其行为无法进行有效监管。例如操作员站和工程师站的组态软件就存在较多远程维护端口和后门，有的组态软件全部被厂商加密，上述行为过程不可控，很容易导致生产、工艺数据及配方等机密信息泄露。

三是安全维护费用投入不足。据统计，我国绝大多数单位年度实际投入工控系统安全经费远低于预算费用，投入费用难以满足设备设施运维、日常管理、教育培训、等级测评和安全建设整改等工控网络安全维护费用的需求。

四是行业标准体系不健完善，缺乏监管依据。随着《工业自动化和控制系统网络安全集散控制系统（DCS）第 1 部分：防护要求》等 6 项工控网络安全相关标准陆续发布实施，标志着我国工控网络安全防护标准建立工作步伐明显加快，但距离形成完善的标准体系尚有很大差距，各部门在进行行业监管和执法检查时缺乏相应的政策和法律依据，工控网络安全防护工作难以引起基层单位的重视，也阻碍了我国工控网络安全服务产业的快速发展。

第五章

匡恩网络“4+1”工控网络安全防护理念与实践

5.1 工控网络安全防护理念的发展沿革

自工控网络安全被业界人士提出以来，国内外工业控制系统网络安全防护理念经历了一系列发展演变过程，总体来说可以划分为以下四个阶段。

图 30 国际工业控制网络安全防护理念经历四个阶段

第一个阶段是以隔离为手段的安全防护理念。在我国“工业化”与“信息化”两化融合伊始，隔离就成为了企业用户、集成商、供应商应对工控系统网络安全的“庇护伞”。工业控制系统是一个“信息孤岛”成为了行业内根深蒂固的思想，直至 2010 年“震网”病毒爆发，人们才开始意识到隔离在整个工控系统网络安全防护中只是一种手段，并非解决一切问题的方法。隔离手段在工控系统内有各种实现方式，比较常用的有物理隔离或在系统边界部署网闸进行隔离，以隔离为手段的防护理念其风险在于：一旦隔离被连通后，其系统内部的脆弱性就会被一览无遗。因此，仅凭隔离进行工控系统网络安全防护是治标不治本的。

第二个阶段是纵深防御的安全防护体系。纵深防御这一概念是由 IT 厂商提出的，近年来在学术界、工业界也一直被提及用于工控系统网络安全防护。这个理念从信息安全领域自然延伸，有其在网络安全防护上的功效与成果，但在工控系统网络安全防护实施过程中，设备供应商、安全供应商并未解决实际问题。首先，设备供应商推卸责任。工控设备供应商出于自身利益，缺乏工控安全的基因与动力。其次，安全供应商偷换概念。其为工厂用户所建立的纵深防御体系往往会变成信息安全产品的简单堆砌。工业控制网络需要尽可能少的故障点，而部署了大量信息安全产品后，故障点不减反增。在追求稳定性、可用性、实时性的工业控制网络中，信息安全产品反而带来一系列问题。

第三阶段是工业控制系统内部生长的持续性防御体系。在经历了一系列事件后，国外工业控制系统网络安全策略已从“事后免责”转变为“主动防御”。根据工业控制网络自身特点，持续性的防御体系需要关注三点。第一，故障点尽可能要少。这是工控系统与生俱来的需求，因此，安全设备也要符合工控设备的特点。除了尽量避免多层部署外，安全设备在保护工控系统正常生产运行的同时还要保证即使断电、设备更新也能对系统不产生任何影响。第二，防御体系要有可持续性。适应工业控制网络特点的持续性防御体系可以通过基础硬件的创新来实现，使安全防护满足低延时、高可靠、可定制化、可持续更新、操作与实施简易化等特性。第三，主要解决存量系统问题。存量在装系统的问题，才是真正的与人民生产生活息息相关的、直面安全威胁的主体。

第四阶段是以攻为守的国家战略。2013 年初，奥巴马发布了总统令，责成 NIC、DHS 等机构对美国所有的基础设施进行普查，要求有问题的企业在年底前进行整改，至今效果并不显著。美国转而将大量经费投往攻击手段的研究上，以攻为守促进整个工控安全技术的进步。不仅是美国，其他各国以攻为守的策略也大同小异，以色列是以技术公司的形式出现，俄罗斯是通过民间组织在实施。我国近两年在有关部门的领导下，建立了多个工业控制系统安全研究实验室，以高仿真工控系统攻防平台为基础，通过对典型工控网络威胁的复现、工控系统脆弱性的研究、工控系统风险的评估，在高对抗的复杂环境中正一步步赶上国际工控系统攻防技术的前沿水平。

当下，工控网络安全防护体系构成层次正逐级提高。整个工业自动化界急需一个能落地的工控系统网络安全防护标准，按照国外相关经验，此类标准应由跨政府部门的多个机构来推动组织。国内的存量在装工控系统以国外工控设备与复制国外陈旧技术的国产设备为主，相关标准照搬国外会使我国处于被动境地。在国家层面驱动、行业用户推广下，以史为鉴、以实为据，凭我国现有基础设施规模和先进性完全有能力引领工控网络安全的技术创新和标准制定。我国工控网络安全防护理念的进步也将不只停留在技术人员的研究中，而是切切实实为业界所接受。最终用户与安全供应商将共同突破传统安全理念，真正助力我国工控网络安全技术进步与发展。

5.2 匡恩网络“4+1”工控网络安全防护理念

对于工业物联网安全的产业化发展，一个系统化安全保障体系将是其实践运营的核心支柱。企业要清晰地打造自己的工业物联网安全体系，必须系统化、立体化对其进行考量。匡恩网络在对国内外各个行业工业物联网系统进行大量深入调研，全面了解工业物联网安全特性的基础上，总结出了涵盖“结构安全、本体安全、行为安全、基因安全四个安全性以及安全的时间持续性”的“4+1 安全保障体系”。

图 31 匡恩网络“4+1”工控网络安全防护理念

▸ 结构安全性

从工控业务系统的网络结构入手，分析工控网络攻击路径，在网络攻击的入侵通路上设立关卡，保护工控系统安全。包括网络结构的现状梳理、优化设计和实施改造，网络边界隔离和认证等防护技术的应用和实施。

▸ 本体安全性

从组成工控业务系统的软硬件实体入手，分析软硬件自身的漏洞与缺陷，通过加强工控实体自身的安全能力，提升工控系统整体防护水平。包括工控系统主机、工控设备和移动介质自身的漏洞情况和补偿措施。

▸ 行为安全性

从工控系统内部的流量行为、应用行为和操作行为入手，构建行为模型，分析行为特征，事前预警攻击行为，事中阻止破坏行为，事后追溯操作行为。包括工控系统流量检测、应用分析和日志安全审计等措施。

▸ 基因安全性

从工控业务系统的软硬件开发入手，实现工控安全设备基础软硬件的自主可控、安全可信，并进一步将可信平台植入到工控业务系统。包括软硬件备案、国产化、可信计算等措施。

▸ 时间持续性

时间持续性就是安全的持续人财物的投入、管理与运维，在持续对抗中保障安全。

“4+1 安全保障体系”从影响工控安全的五个要素着手，将安全需求和部署与业务、应用和整体系统构架连接起来，有步骤地逐步实现从网络安全到功能安全到基础设施安全的综合防护能力，做到安全与互联随行。

“4+1 安全保障体系”的建立，基于国资委、工信部、能源局等国家部委对于工控安全的监管要求、推荐标准和工控系统安全要素的分析，充分吸收现有工控安全体系的精髓，在结构安全方面吸纳专网专用、隔离认证等技术，在本体安全方面吸收设备加固与白名单控制等技术，在行为安全方面引入工业大数据技术，基因安全方面引入可信可控，时间持续性方面引入管理持续化等技术与管理体系，实现对现有工控安全体系的融合与发展。

“4+1 安全保障体系”将工业物联网与工业基础设施安全相结合，为工业企业提供基于工业物联网的平台化专业安全服务，解决工业基础设施互联互通带来的安全问题；解决当前工控企业缺乏安全管理和专业化安全服务的问题；解决工业企业信息安全与生产安全脱节的问题。帮助工业企业建立、提升立体化主动防御能力，实现工业基础设施安全与生产安全相结合的一体化大安全。

5.3 匡恩网络工控网络安全整体防护体系

匡恩网络在工控网络安全防护实践中积累了丰富的经验，基于上述的“4+1”工控网络安全防护理念，匡恩网络为工业企业建立了一套从集团公司总部到其二级公司、三级单位的三层工控网络安全防护体系。

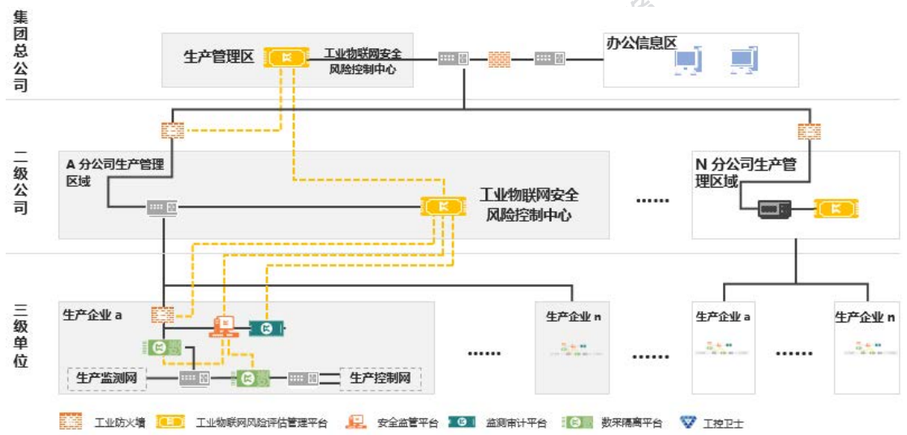


图 32 匡恩网络集团化公司整体工控网络安全蓝图

在集团公司的总部与其二级子公司中建立了工业物联网安全风险控制中心，统一管理其三级及以下子公司的生产控制网络。其中每一个二级子公司建立的工业物联网安全风险控制中心，统筹管理集团公司下属所有生产企业中的生产控制网络。

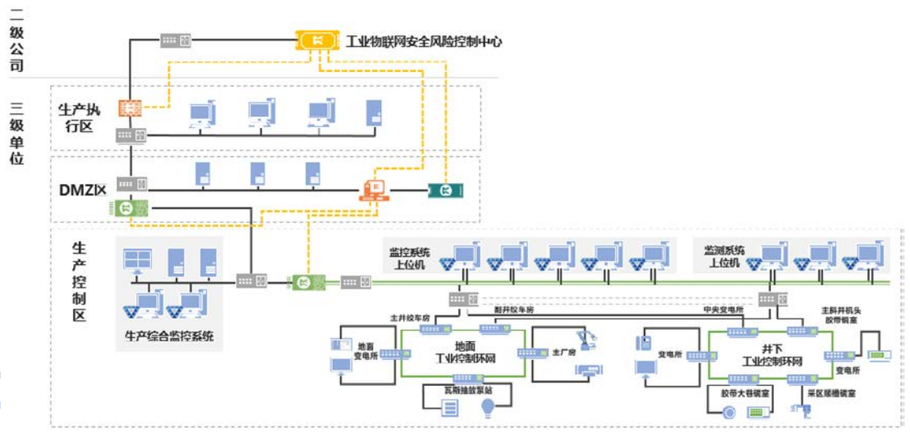


图 33 匡恩网络生产企业控制系统安全防护示意图

对于集团公司三级及其以下生产企业的安全防护，匡恩网络的工业防火墙、数采隔离平台、安全监管平台等产品分别部署在工业企业生产执行区、DMZ 区及生产控制区相应的网络系统中，建立了从上至下全方位保障该集团公司的工控网络安全防护体系。

- 匡恩网络工控网络防护产品设计理念

匡恩网络拥有前沿科技创新和深厚的技术积累，通过基础硬件创新，为工业智能化、“中国制造 2025”植入安全基因，实现从“工控的安全”到“安全的工控”跨越。

图 34 匡恩网络由工业控制系统内部生长的持续性防御体系

匡恩网络工控安全持续性防御体系承接之前所阐述的“4+1”工控安全防护理念，首先，为了达到结构安全和行为安全，一般情况下都需要在原有的工业控制网络环境中新加安全设备，比如工业防火墙、工业入侵防御系统、工业 VPN 或工业监测审计产品等。由于工业环境通常对系统的稳定性、可靠性、完整性以及网络延时存在较高的要求，而这些“外来”的安全设备一般采取“外挂”的方式进行部署，这势必会给原有的网络结构、系统完整性、数据延时带来影响，每引入一个安全设备也即多引入了一个故障点，这使得网络安全问题解决的同时引入了新的问题。而本体安全是指工控系统自身的安全，这涉及到控制设备自身抵御外部攻击的能力，也即安全工控的概念。安全应该作为工控系统的核心要素之一，在工控系统设计之初就需要考虑其安全需求。

针对上述工控网络安全中存在的问题，匡恩网络致力于形成先进的并且适应于市场需求的工控网络防护产品规划设计理念，积极打造基于行业的系统检测平台、智能保护平台、检测审计平台及安全大数据平台，在各平台之上开发出各行业针对性的工控安全防护产品、安全服务及解决方案等。

匡恩网络一方面在研发外挂式的安全设备，同时也在从基因安全角度去保护各行业工控

系统，匡恩网络投入大量资源进行安全芯片研发，把安全芯片作为相对独立的模块，内嵌入工控系统当中，成为工控系统的一部分，为工控设备提供身份认证、通信加密、行为审计等安全功能，从源头上为国内工控系统提供底层安全防护。目前匡恩网络在积极向国内工控设备厂商寻求合作。

- 匡恩网络致力于打造可信计算绿色生态环境

与传统防火墙、病毒查杀和入侵检测相比，可信计算体系结构问题，在计算模式上是主动免疫的新计算模式，可信计算使计算结果总是与预期一样，计算全程可测可控，不被干扰，因此是一种新的免疫的计算模式，能及时准确地识别“自己”和“非己”。

工控网络安全所涉及的行业众多，产品覆盖面广，技术种类多样，可信计算经过十几年的发展，已经演变成为一项综合芯片设计技术、密码算法、操作系统、软件应用等多项技术的综合性安全防御方法，未来不可能由一家企业就可以提供完整的解决方案。国内已有不少单位和部门按照可信计算相关标准研制了芯片、整机、软件和网络连接等可信部件和设备，并且部分产品全面支持国产化的硬件和软件。尽管国产化产品存在一些缺陷和漏洞，在可信计算技术保障下，缺陷和漏洞无法被攻击利用，从而确保国产化产品比国外产品更安全。

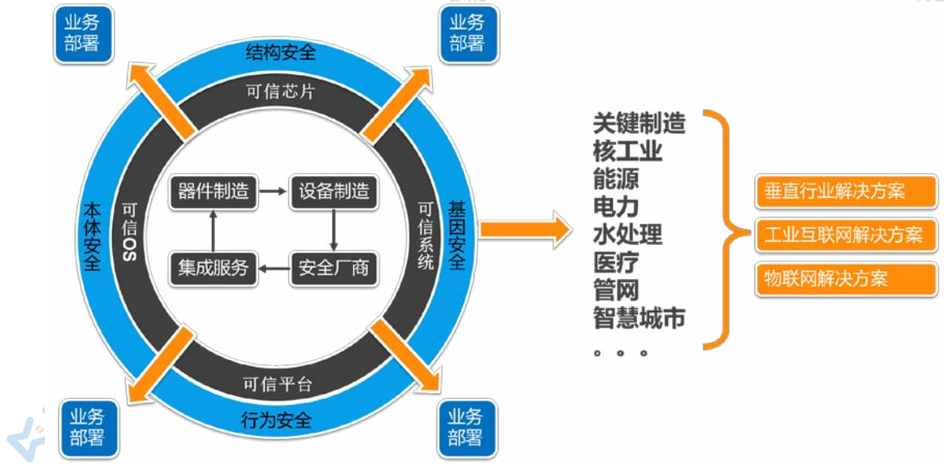


图 35 匡恩网络打造可信计算绿色生态环境

匡恩网络志在联合器件制造商，设备提供商，集成服务商以及广大的安全厂商，共同打造包括可信芯片，可信操作系统，可信开发平台以及可信工业系统在内的绿色产业生态环境，并广泛覆盖关键制造、核工业、能源等垂直行业，提供包括行业、工业互联网以及物联网的安全解决方案，构筑结构安全、本体安全、行为安全以及基因安全的“4+1”安全战略。

在过去两年中，匡恩网络的创新技术与解决方案在行业深耕细作和广泛实施，辐射了基础设施、智能制造、民生、以及军民融合四大领域。未来，匡恩网络将向工控网络安全的更底层技术下沉，将“4+1”安全防护体系根植于更多行业，更专业化、更精细化的有效融合，为更多行业的工控网络安全防护创造更多的可能性。

5.4 匡恩网络 PDCA 安全环整体服务方案

匡恩网络工控安全环整体服务方案包括计划准备、方案实施、结果评估和优化提升，四个步骤环环相扣形成 PDCA 安全环，它是爬楼上升式循环，每转动一周，工控安全水平上升一个台阶。

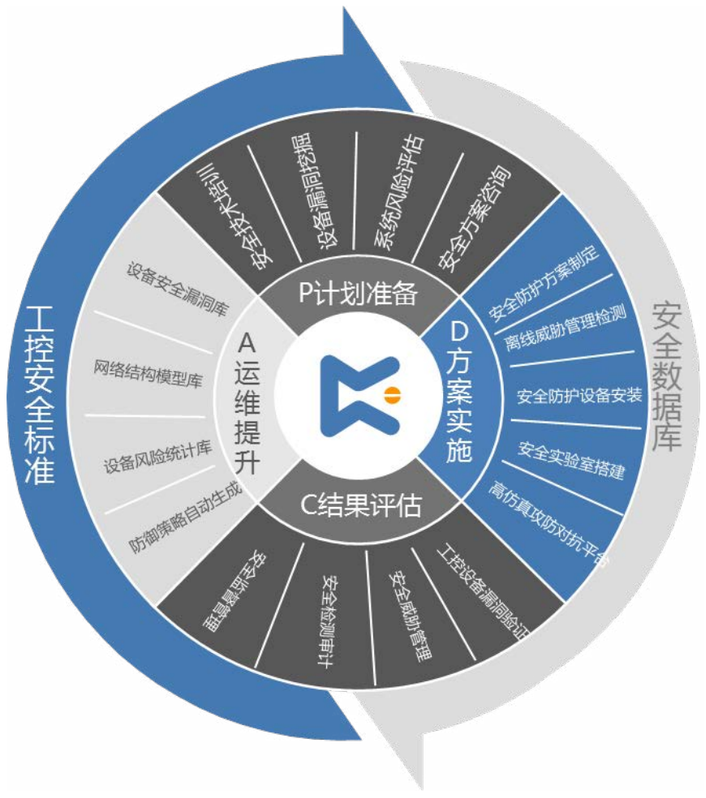


图 36 匡恩网络 PDCA 安全环

如上图所示，PDCA 安全环四个步骤具体内容描述如下：

- P（PLAN）：计划准备，包括：
  - 安全技术培训
  - 初步现场调研
  - 设备漏洞挖掘
  - 系统风险评估
  - 安全方案咨询
- D（DO）：安全防护方案实施，包括：
  - 安全防护方案制定
  - 离线威胁管理检测
  - 安全防护设备安装调试
  - 安全实验室搭建
  - 高仿真攻防对抗平台搭建
- C（CHECK）：结果评估，包括：
  - 工控设备漏洞验证
  - 安全威胁管理
  - 安全检测审计
  - 安全监督管理
- A（Action & Acceleration）：优化提升，包括
  - 设备安全漏洞库维护
  - 网络结构模型库维护
  - 设备风险统计库维护
  - 防御策略自动生成

基于以上匡恩网络 PDCA 安全环的全生命周期工控网络安全防护核心内容总结如下：

（1）设备检测：设备检测在工控系统的规划、设计阶段就能够开展，在系统的上线之前就能及时发现隐患与漏洞，对上线后的存量系统仍可以开展设备、系统的安全检测以对其进行深层次的安全风险评估。设备检测必须覆盖主要的工控协议，包括通用的 Modbus、OPC 等协议以及主流厂商私有的通讯协议，同时需要支持多种总线、对未知协议的检测与漏洞挖掘，最大程度上为工控系统、工控设备提供丰富的检测手段。

（2）安全服务：工控网络安全服务对实施人员的技术要求极高，安全服务内容有对工控系统的风险评估、漏洞挖掘、渗透攻击以及针对性的安全技术培训。工控网络安全服务伴随着整个工控系统生命周期，是各类工控网络安全防护实现方式，也是工控网络安全技术的集中体现。

（3）威胁管理：工控系统威胁管理作为一个高瞻远瞩的安全防护手段，能满足上至政府机关、监管机构下至业主自身对于实时安全自查、自我评估与安全态势感知的需求。离线情况下的工控系统威胁管理可以采用多种威胁评估工具、集成工控设备漏洞验证功能并因地制宜提出对工控网络的安全防护建议，是存量工控系统可靠的安全防护手段。

（4）监控审计：在工控网络安全工作推进过程中，在工控系统中部署旁路监控审计类产品，细至安全行为的审计是现阶段业主较为认可也是更易于接受的安全防护手段。对工控网络的安全监控审计产品需要有满足现场环境要求的工业等级硬件设计，功能上针对工控网络协议的特点进行网络行为的自学习，采用工控网络行为“白名单”与工控漏洞“黑名单”相结合的策略进行全网流量的安全监控审计。

（5）智能保护：最直接、最有效的工控系统安全防护手段，是进行工控网络流量的在线实时过滤与异常数据拦截。如前所述，传统信息安全产品并不能满足这一要求。针对工控网络的智能防护除了同样要求满足现场环境的工业级硬件设计外，自主学习网络行为、自动生成防御策略，能适应自动化控制人员操作特点进行一键式安全部署均是其必备的功能特性。

（6）安全数据库：要使工控网络安全防护成为一个可持续发展过程，必须要有可供依赖的安全数据库。工控网络安全数据库需要覆盖主流厂商设备、各行各业系统，并至少包括有设备安全漏洞库、网络结构模型库、设备风险统计库等数据库，以大数据的理念全面、高效地支持工控网络安全的实时智能防护与威胁态势感知。

第六章

工业控制网络安全保护对策与建议

工业控制网络安全不仅关系到工业企业的生产安全和经济安全，而且关系到社会稳定，甚至国家安全。工业控制网络的安全防护工作是一项系统工程，需要政府部门、行业协会、工业企业及安全厂商等单位紧密协作、各司其职，才能打赢这场攻坚战和持久战。

6.1 充分发挥政府引导和监管作用，提高工控安全防控水平

- 加快工控网络安全相关国家政策、标准和指导意见落实工作

以《网络安全法》为指导原则，加快推进《工业控制系统系统信息安全防护指南》推进落实，加快《工业控制系统信息安全等级保护》等系列标准制定和发布实施工作。明确不同重点领域工控系统所应具备的安全保护水平和要求，构建我国重点行业领域工控系统抗威胁能力分类分级安全管理体系和工控系统网络安全保护技术体系。同时各行业由本行业监管机构牵头加快编制和落实顶层设计、法律法规以及标准体系。

- 从准入、检查、追责等全方位建立立体监管防控体系

监管机构统筹协调有关部门对国家安全和人民生命财产安全产生重大影响的工控系统的信息安全保护采取强制性措施，如：抽查检测、风险评估、应急演练、设备本身进行可信化改造等。

建立完善的产品安全准入标准体系，鼓励优先采用性能可靠、具有自主知识产权的国产化工控和安全防护装备。引导国外厂商在修复自身产品漏洞方面积极提供技术服务支持并对其行为进行规范，建立健全工控系统信息安全事件应急响应、应急处置、事件分析和责任追究体制，要求各工控设备系统生产企业参照国际上认可的开放式漏洞评价体系国际标准，建立适合国内各工控设备系统升级的产企业行业漏洞评价体系，对漏洞进行评分，帮助业主单位判断修复不同漏洞的优先等级。并且把工控系统信息安全纳入国家安全生产管理体系并以此作为各级政府领导干部和基层单位主要领导工作任务考核指标之一。

加大经费投入，建设全国工控系统安全状况大数据分析平台，动态感知工控网络面临的安全威胁；积极出台激励政策，大力培育安全咨询、安全评估、委托测试、远程运维、

业务审计以及威胁管理等服务产业；建设全国工控系统安全智库，完善安全监测、评估、认证体系；支持工控系统安全培训体系建设，开展单位工控系统安全从业人员资格认证。

- 加大科技创新推动力度

各级政府应不断加大财政资金支持力度，组织关键技术与产品产业化攻关，加快推进工控网络安全关键技术突破和 PLC 等核心工控设备国产化进程，推动工程示范应用。希望各地政府积极践行企业为技术创新主体的认识，加大对新兴的网络安全高技术企业的扶持力度，鼓励企业联合科研院所、高校建立产、学、研协作机制。同时对网络安全企业的重大科技成果予以评价和奖励，扶持推进工控信息安全关键技术突破和产品国产化进程。

- 加大人才培养推动力度

推动高校工控网络安全学科建设和教学，开放关键基础设施实验平台，加强专业人才培养，鼓励单位引进毕业生，不断壮大企业的专业技术队伍；基层单位应加大工控安全从业人员技能培训力度，派员参加相关高校和专业机构举办的专业知识学习，定期组织专业知识培训，不断提高从业人员的专业技术水平。

6.2 工控系统运营单位要完善防护技术体系，提高网络防护能力

工业控制网络安全与企业生产安全和经济安全密切相关，各工业企业（运营单位）要提高工业控制网络安全意识，重视安全规划和防护方案落地，切实提高工业控制网络防护能力。

- 建立安全补偿机制。工业企业对于新装系统，应实现结构安全同步建设；对于再装系统，应进行结构安全改造；对于因条件限制无法进行改造的，应建立安全性补偿机制。对条件具备的工业物联网部署经过基因安全性改造的工控系统与设备；对条件暂不具备的工业控制系统采取安全加固措施，建立安全补偿机制。

- 优化改造工控系统现有网络结构，配备功能完善的边界防护产品，建立工控系统安

全监测预警机制，对远程访问和远程维护行为必须采用专门的接入方式和安全访问控制策略，形成完善的边界防护技术体系；

- 采用标准化检测工具，对设备离线、入网及在线安全以及系统全生命周期过程进行持续检测，通过安全配置、系统补丁等安全性补偿措施提升工控设备漏洞、后门等威胁抵御水平，形成有效的本体安全防护技术体系；

- 建立设备、行为以及软件白名单等控制机制，实现对已知、未知威胁以及全局、局部安全态势的感知，具备多种安全防护技术联动和主动防御的能力，形成事前预警、事中阻止和事后追溯的行为安全防护体系；

- 部署经过基因安全性改造的自主工控系统设备以及经过基因安全性加固的进口系统设备，实现 CPU、存储、操作系统内核、基本安全算法与协议等基础软硬件的自主可控和安全可信，未来实现将可信平台植入到工业业务系统，形成良好的基因安全技术防护体系；

- 建立健全专门管理机构，明确岗位职责，构建安全运维、应急响应与事件处理、经费保障等运行机制，形成完善的安全管理体系。

总之，对于工业企业而言，工控网络安全是一个从人财物的投入、管理与运维投入到持续的对抗中保障信息安全的全过程，需要持续不断地关注与投入。

6.3 充分利用社会组织力量，积极推动技术创新实践

目前我国网络安全面临诸多新形势，要充分认识关键基础设施保护工作的重要性，树立起正确网络安全观，创新保护方法，构建多方参与、协同保护的工作体系。鼓励行业联盟、协会、组织在工控网络安全领域大力发展；鼓励行业组织积极拓展与国内外企业及行业间技术交流，促进国内企业的国际化视野，力争赶上国际先进国家的防护水平；积极开展行业人才培养，建立专家人才库，建立分层级、专业化的人才培训体系等。集合各方力量，整合资源，促进跨行业的技术联合与创新，提高我国关键基础设施网络安全的防护水平。

综上所述，面对我国工控系统信息安全存在的问题及风险，国家协调和监管机构加强

配合、形成合力，加快制定完善工控信息安全法律法规和标准规范，充分发挥产业联盟、安全服务商等社会力量在此过程中的推动作用，积极推动工控系统信息安全关键技术与装备的自主研发和国产化进程，大力培养各类专业技术人才，尽快提升我国工控系统信息安全水平。

匡恩网络作为工控安全及工业物联网安全领域的领军企业，将针对工控网络攻击的手段不断更新和变化，积极提高和改进工控安全和工业物联网安全的防御技术，并且将从全局考虑工业企业的安全防护方案，为全面提升我国工控安全及工业物联网安全的整体防护水平做出积极的贡献。同时希望通过这份态势报告的细致阐述与分析，能为工控安全及工业物联网安全的从业者提供参考。

附录

参考文献

1、 匡恩网络《2015 工业控制网络安全态势报告》
2、 匡恩网络《国际工控安全动态》系列期刊
3、 匡恩网络《工业控制系统信息安全行业市场研究报告》
4、 匡恩网络微信推文《在乌镇读懂未来：工业物联网安全产业前景可期》
5、 匡恩网络《电网行业工控网络安全应用研究报告》
6、 匡恩网络《工业物联网行业安全研究报告》
7、 ICS-CERT 《ICS-CERT_Monitor_Sep2015-Feb2016》
8、 ICS-CERT 《ICS-CERT Monitor_Nov-Dec2016_S508C》
9、 申万宏源证券《工控安全：物联网与安全的邂逅》
10、 广发证券《美国大规模网路攻击 : 安全无穷期》
11、 银河证券《物联网进入规模化应用时代——物联网深度研究报告》
12、 国家互联网应急中心《2015 年我国互联网网络安全态势综述》
13、 国家信息安全漏洞共享平台：http://www.cnvd.org.cn/
14、 美国国土安全部《NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report》
15、 美国国土安全部《STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS （IoT）》
16、 赛迪智库《应大力构筑基于芯片的网络安全体系》
17、 赛迪网《2016 上半年网络安全事件盘点》
18、 德国国家科学与工程学院《“工业 4.0”战略计划实施建议》
19、 GE 《工业互联网：突破智能和机器的界限》
20、 美国国土安全部《网络空间安全国家战略计划》
21、 NIST SP800-82《Guide to industrial Control Systems Security》
22、 ISA/IEC 62443《Industrial network and system security》
23、 GB/T 30976.1—2014《工业控制系统安全第 1 部分：评估规范》
24、 GB/T 30976.2—2014《工业控制系统安全第 2 部分：验收规范》
25、 工信部协〔2011〕451 号文《关于加强工业控制系统安全管理的通知》
26、 国务院《2015 年政府工作报告》
27、 国务院《中国制造 2025》
28、 全国人大常委会《中华人民共和国网络安全法》
29、 国务院学位委员会《关于增设网络空间安全一级学科的通知》
30、 工信部信〔2013〕317 号文《工业和信息化部关于印发信息化和工业化深度融合专项行动计划（2013-2018 年）的通知》
31、 工信部电子科学技术情报研究所《2014 年工业控制系统安全蓝皮书》
32、 工业控制系统安全产业联盟《工业企业信息系统安全技术指引》
33、 中国轨道交通网，http://www.rail-transit.com
34、 中国燃气网，http://www.chinagas.org.cn/
35、 国家智能车发展论坛，http://www.caaiv.org/
36、 北极星电力网，http://www.caaiv.org/
37、 Digital Bond，http://www.digitalbond.com/
38、 Scadahacker，http://www.scadahacker.com/
39、 Shodan，http://www.shodanhq.com/
40、 《全国工控系统现场安全检查分析报告》
41、 安全牛 《工业网络控件安全态势分析报告》
42、 《我国工业控制系统信息安全现状及风险》陈东青
43、 《火眼 2016 工业控制系统漏洞趋势报告》
44、 工业互联网产业联盟《工业互联网体系架构》1.0
45、 艾伦咨询《工业网络安全威胁简报》
46、 《2016 上半年度中国物联网产业生态报告》
47、 《工业控制系统的安全研究与实践》
48、 物联网技术《工业物联网安全及防护技术研究》
49、 睿工业解读工业信息安全市场
50、 中商情报网《2016 年工业物联网发展现状及发展因素分析》
51、 中国信息安全博士网《2016 财年美国政府各部门网络安全财政预算》

www.kuangn.com

北京匡恩网络科技有限责任公司

北京市海淀区知春路 7 号致真大厦 D 座 13 层
电话：400-068-0583
传真：010-59512799
邮箱：info@acorn-net.com