构建工业互联网主动防御体系：实践与思考

姚羽

二〇一九年十一月

议题

1、工业互联网的安全防护需求

2、工业互联网主动防御体系的建设思路

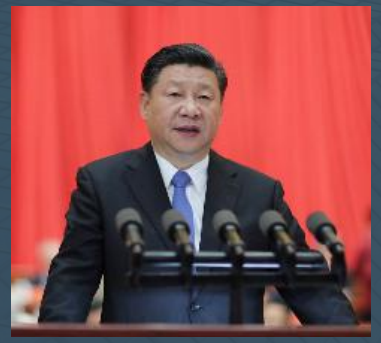
3、“谛听”团队的实践与思考

工业互联网安全事件

2010	2011	2013	2014	2015	2016	2017	2018	2019
第一款针对工业设施的病毒		网络安全成为国家战略		第一次对主权国家工业网络攻击	网络战争形态工业设施遭受大规模攻击	针对关键基础设施勒索攻击	针对工业安全设备攻击	有政治目的的工业网络攻击
震网病毒	Duqu工业病毒	蜻蜓工业病毒 斯诺登事件	Havex工业病毒	乌克兰机场和电网遭受Black Energy攻击	美军对ISIS发动网络战 美国网络基础设施瘫痪	Wannacry蠕虫爆发	TRITON 蠕虫攻击	委内瑞拉 电厂遭到攻击
2000s		2010s		2010s				

工业互联网安全直接关乎国家安全

国家顶层设计



- 习近平总书记在党的十九大报告中全面系统深刻地论述了坚持总体国家安全观的重要思想。

- 2018年4月20-21日召开的全国网络安全和信息化工作会议上进一步强调指出，要“树立正确的网络安全观，加强信息基础设施网络安全防护”。

- 国务院《深化“互联网+先进制造业”发展工业互联网的指导意见》：引导企业提高网络安全防护能力。围绕汽车、电子、能源、航空航天等重点制造领域建设网络和平台安全保障与技术体系。

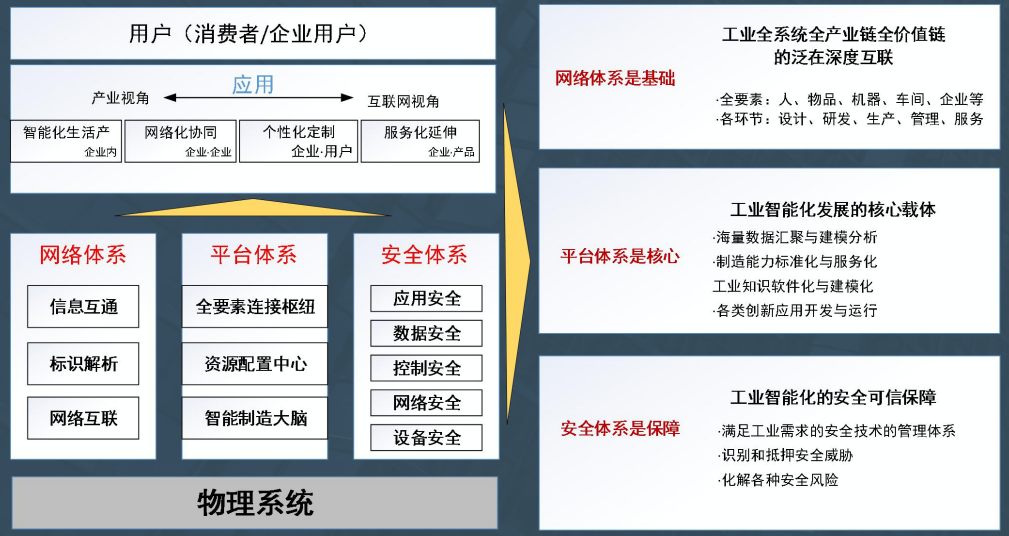
工信部工业互联网安全布局

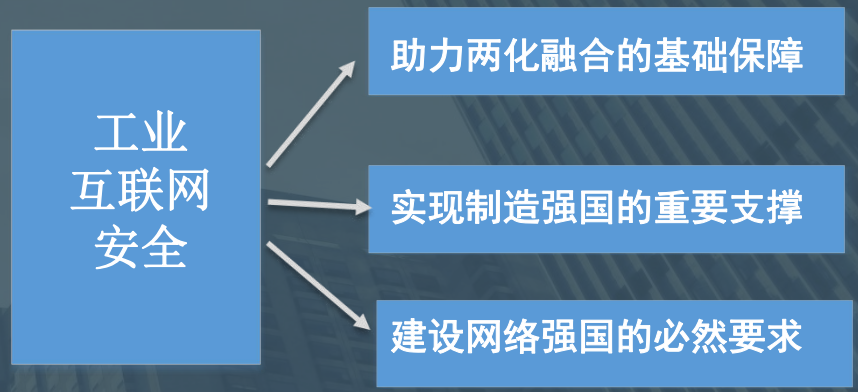
《工业控制系统信息安全行动计划（2018-2020年）》

√重点提升工控安全态势感知、安全防护和应急处置能力，促进产业创新发展，建立多级联防联动工作机制，为制造强国和网络强国战略建设奠定坚实基础。确保信息安全与信息化建设同步规划、同步建设、同步运行。

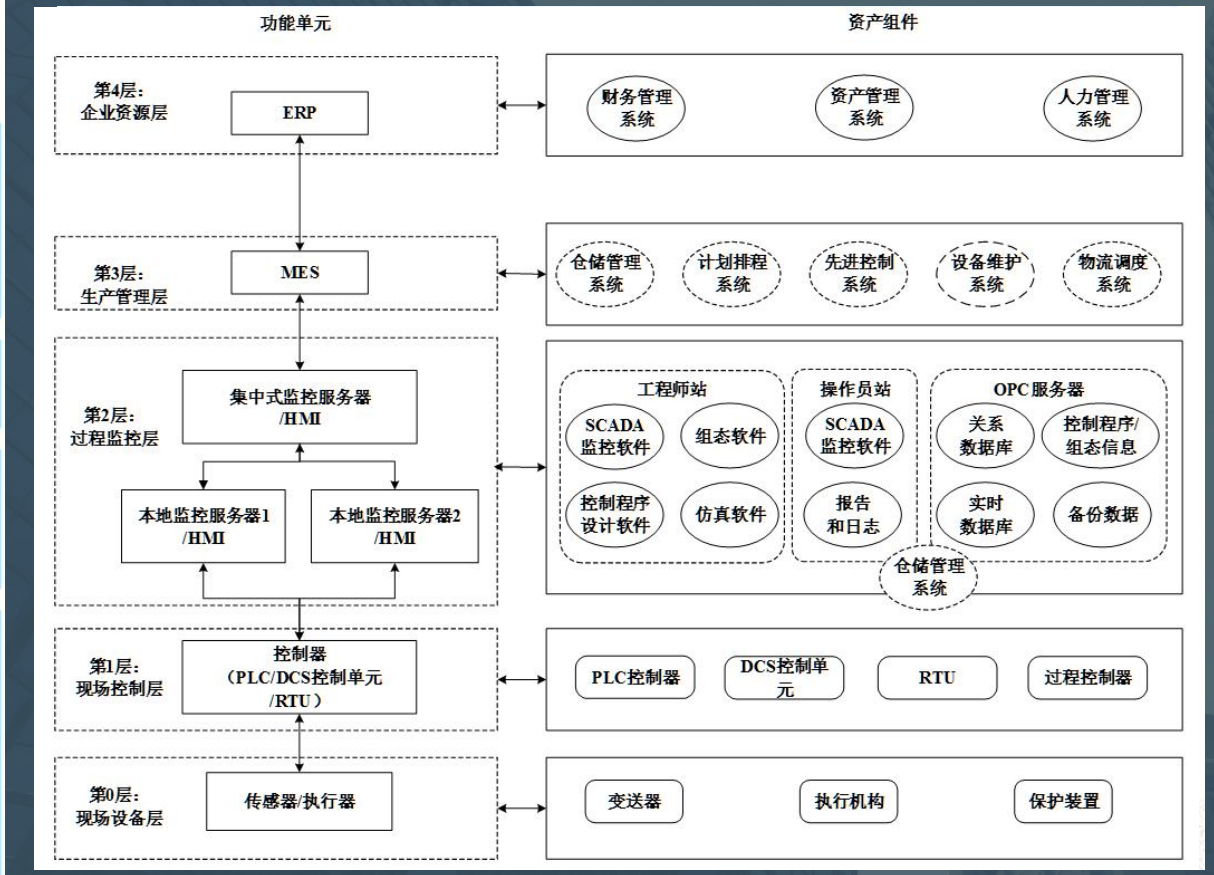
《工信部关于加强工业互联网安全工作的指导意见》

√构建责任清晰、制度健全、技术先进的工业互联网安全保障体系，覆盖工业互联网规划、建设、运行等全生命周期，形成事前防范、事中监测、事后应急能力，全面提升工业互联网创新发展安全保障能力和服务水平。





工业企业功能单元和资产组件



- 供应链：美国四家输气管道公司被迫关闭（2018.4.5）
- 第4层，企业资源层：信息收集，挖矿攻击
- 网络边界：思科路由器漏洞（2018.3.28）
- 第3层，生产管理层：“Wanncry”勒索攻击
- 第2层，过程监控层：“Industroyer”攻击乌克兰电网
- 第1层，现场控制层：“震网”攻击伊朗核设施
- 第0层，现场设备层：TRITON攻击沙特石油天然气厂

工业互联网安全防护的需求

- 全方位的威胁需要全方位的网络安全保障
  - IT + OT，安全的全方位保障

- 集团、公司级场景下需重点保障IT安全
  - 集团、公司级网络安全态势感知

- 工厂、现场级场景下需重点保障OT安全
  - 工厂、现场级网络安全态势感知

议题

1、工业互联网的安全防护需求

2、工业互联网主动防御体系的建设思路

3、“谛听”团队的实践与思考

IT网络安全体系的变迁

P2DR动态安全模型

本质：安全就是响应+防护的安全运维体系

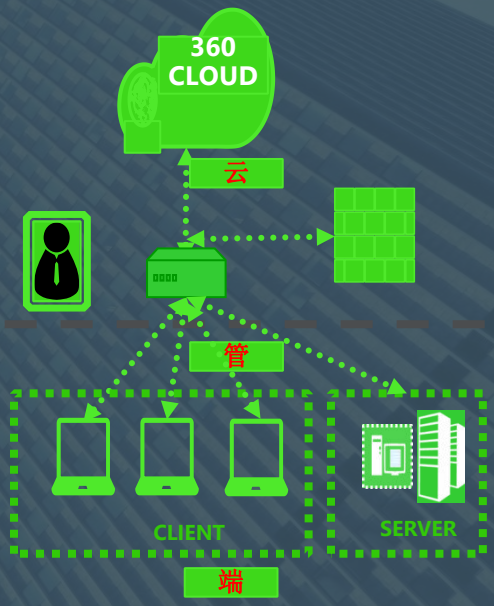
安全木桶理论

本质：安全就是用安全产品堆砌出来的线式防御体系

立体防御体系

本质：安全就是分层的、分级的多层次防护体系

云管端联动体系



本质：安全云端、管道、终端三者统一升级，协同联动

工业控制网络（OT网络）防护需求的特殊性和复杂性

	传统IT信息网络	工业控制网络	对网络防护产品的要求
性能要求	不要求实时性；可以忍受高时延和延迟抖动；高吞吐量；	实时通信；延迟和抖动都限定在一定的水平；适度的吞吐量；	优先考虑旁路式部署
生命周期	3年至5年	15年至20年	无法改动，优先考虑旁路式部署
可用性	可用性缺陷可容忍；中断重启可随时进行	可用性要求高；系统中断重启必须要提前制定严格的计划；	优先考虑旁路式部署
操作复杂性	简单；可自动升级	复杂；修改或升级时需要不同程度的专业知识	优先考虑旁路式部署，需要定制化的防护手段
通用性	无行业差别，场景通用；	行业、场景间差别大。行业碎片化，场景碎片化	产品难以通用化，需要定制化的防护手段
网络协议	TCP/IP,常见互联网协议；	协议碎片化；Modbus，S7，EthernetIP，DNP3,BACnet，.....；	产品难以通用化，需要定制化的防护手段

- **优先考虑旁路式部署的防护产品**
- **产品的通用化与实施的定制化存在矛盾**

网络安全安全体系模型的演进趋势

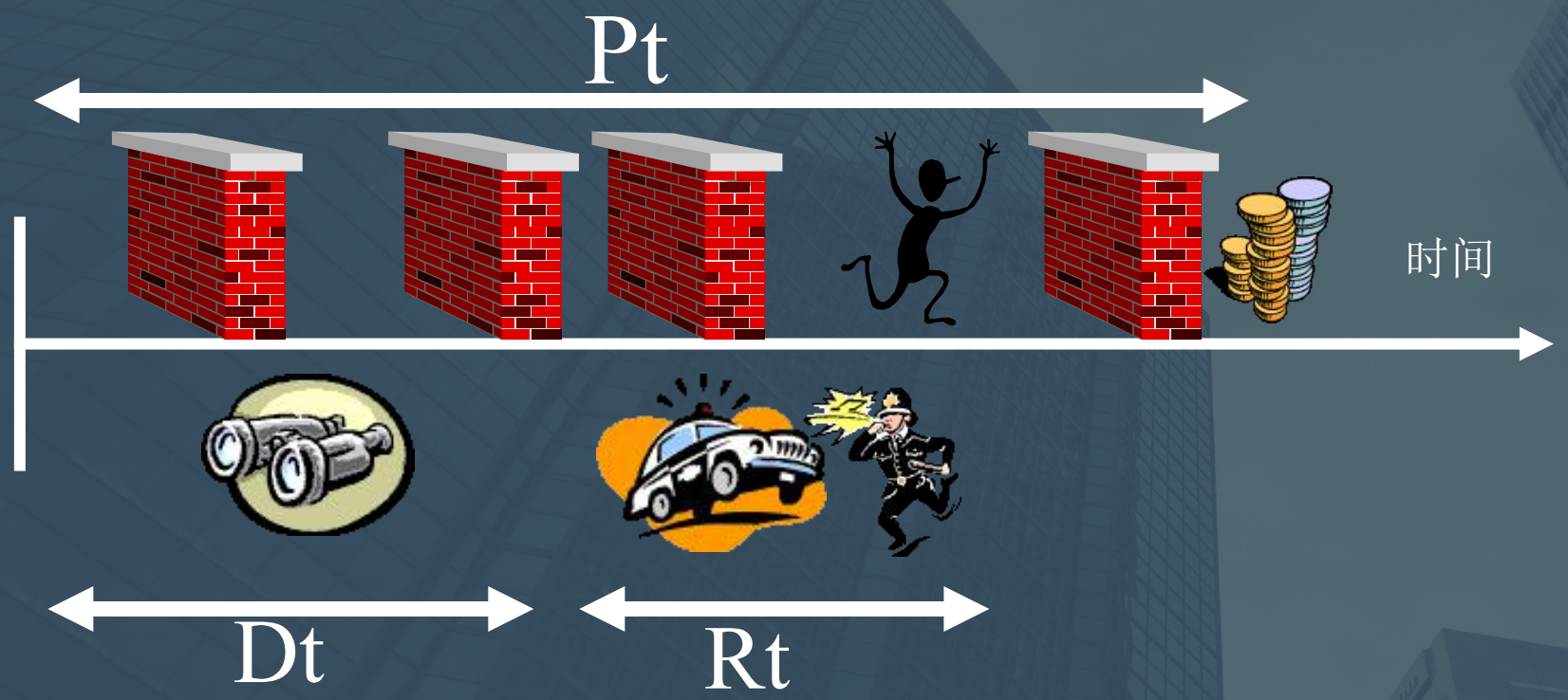
网络安全滑动标尺模型（The Sliding Scale of Cyber Security）

——SANS（美国系统网络安全协会）

架构安全	被动防御	威胁情报	态势感知	主动防御
安全评估 等保测评 渗透测试 自主可控	自动化、层次化安全体系建设： ·网络安全防护 ·主机安全防护 ·IoT安全防护 ·统一安全防护	威胁数据源采集 威胁情报生产 威胁情报验证 威胁情报分发体系	安全大数据平台 态势感知 云端威胁情报自动化应用体系 事件分析 安全协同	行为捕获 溯源分析 攻击者定位 法律手段
确保基础架构的合规性	提供基础的防御能力，抵御常规的IT威胁	收集数据，建模分析，产生共享威胁情报	监控网络内部异常行为，通过学习建立分析模型，对其进行响应和可视化	针对攻击者的分析刻画及取证，以便采取法律对策和自卫行动

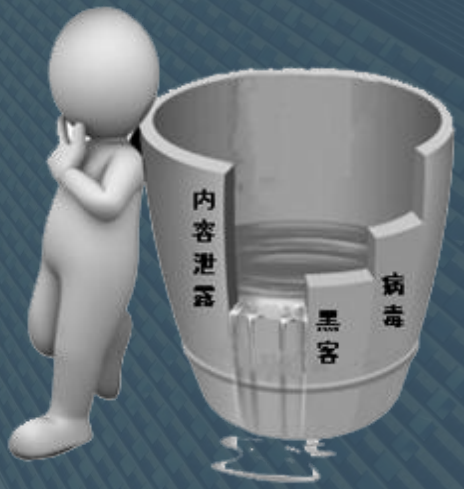
应充分重视蜜罐的作用

- 及时的检测和处理



Pt > Dt + Rt

安全木桶理论



- 蜜罐：故意暴露的短板
- 基于木桶理论：吸引攻击者的资源投入
- 基于P2DR模型：迟滞攻击时间
- 高效鉴别恶意流量，与探针形成互补

态势感知的三要素

- 态势认知
  - 了解当前系统运行状态，包括状态识别与确认（攻击发现），以及对态势认知所需信息来源和素材的质量评价
- 态势理解
  - 分析了解攻击的影响、攻击者的行为和当前态势产生的原因及方式。
- 态势预测
  - 对态势发展情况的预测评估。主要包括态势演化（态势跟踪）和影响评估（情境推演）

现阶段，在工业互联网安全态势感知与主动防御体系中

- **旁路式数据采集是态势认知的主要手段**
- **数据分析是态势理解与主动防御的关键**

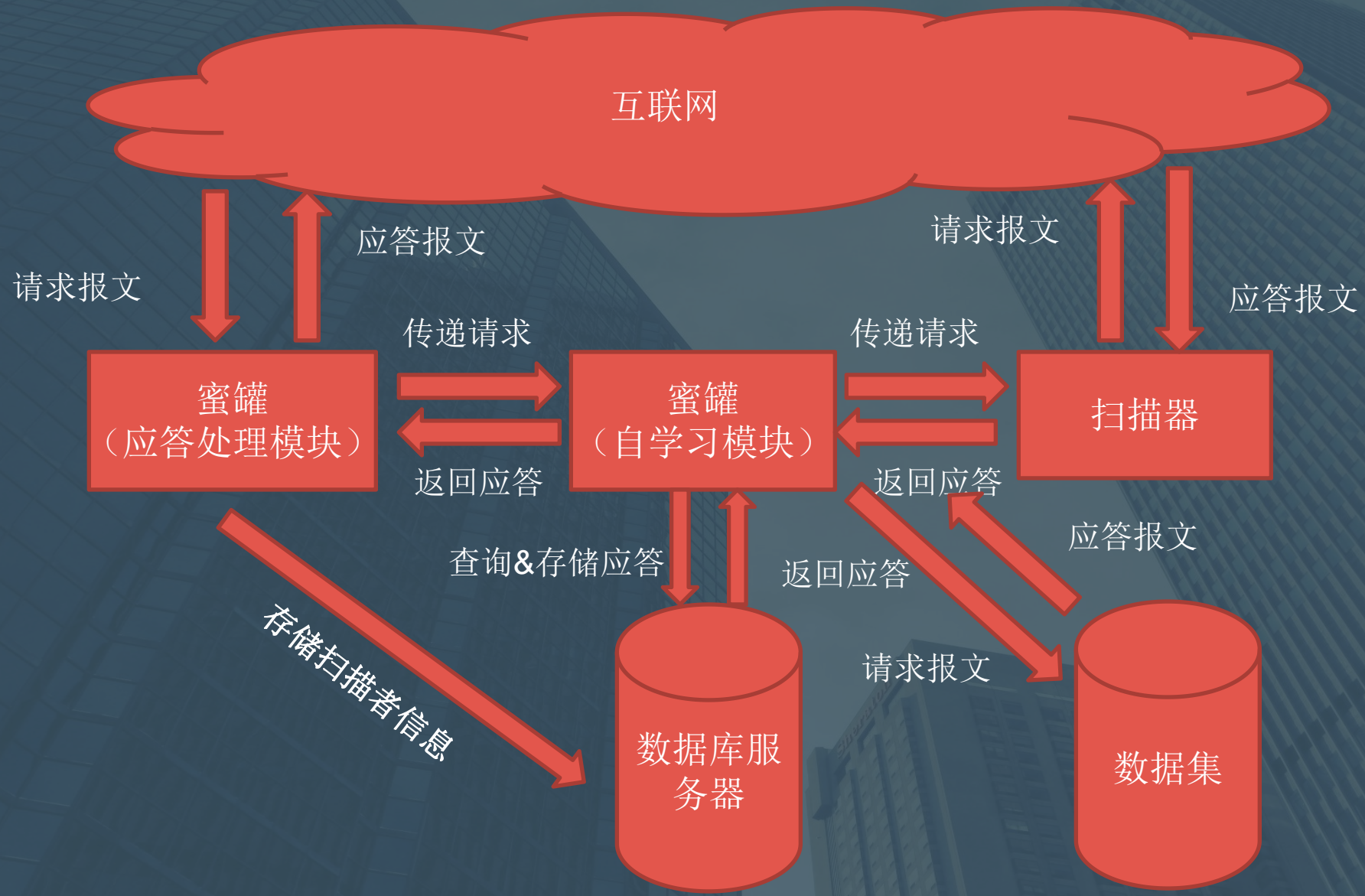
议题

1、工业互联网的安全防护需求

2、工业互联网主动防御体系的建设思路

3、“谛听”团队的实践与思考

“谛听”左耳：数据驱动蜜罐的伪装

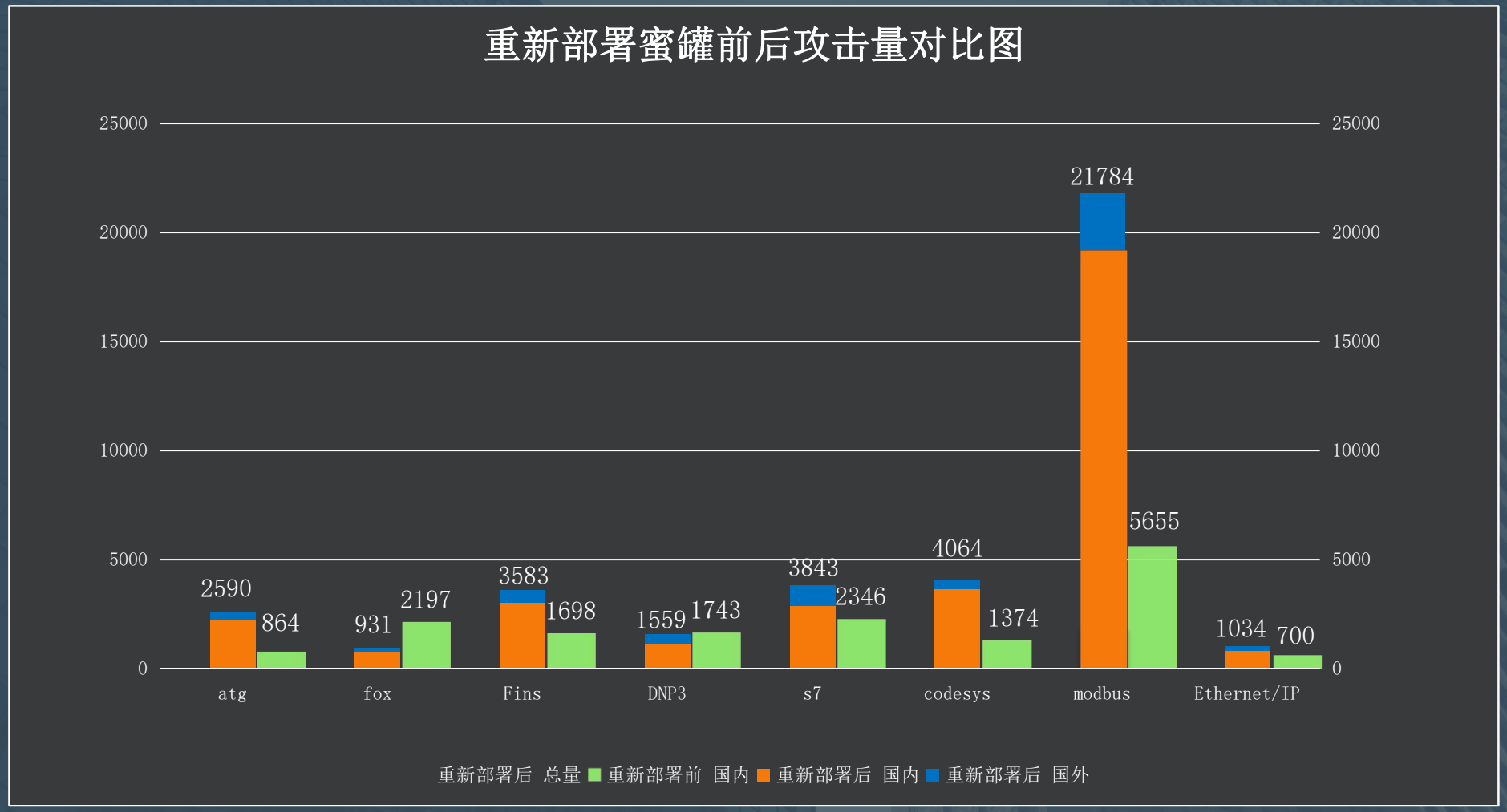


蜜罐全球部署情况

国内：华北、华东、华南、西部(8个)
国际：北美、西欧、东欧、东亚、东南亚（8个）

重新部署前后捕获数据对比

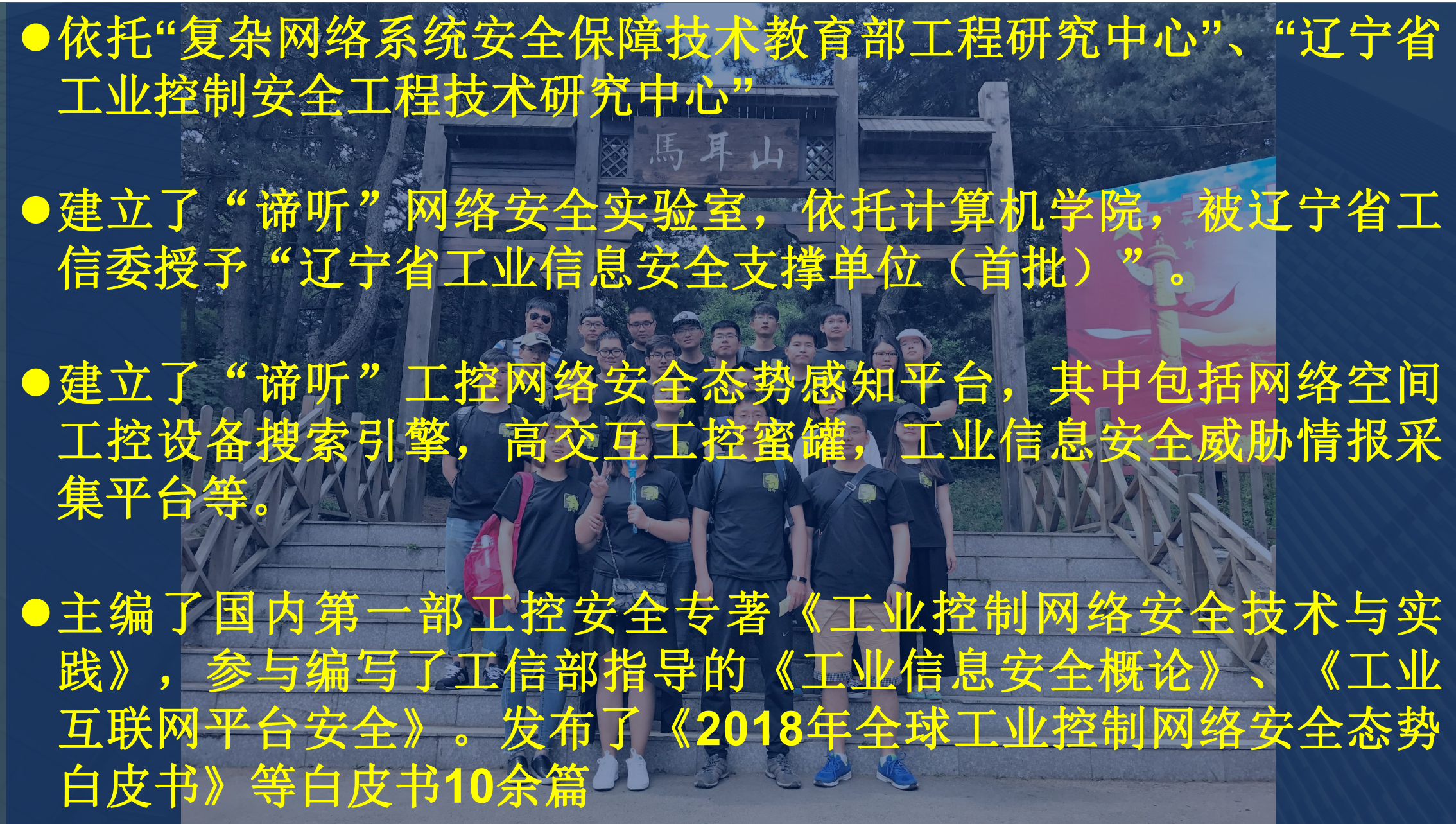
- 部署前后排名柱形图



一点思考

- 工业互联网中的OT防护需要旁路式部署的网络安全设备
- 应关注工控蜜罐+探针在OT防护中的重要作用
- 基于威胁情报的数据分析是态势感知与主动防御的重要手段
- 攻击的溯源分析与关联分析需通过人工智能方法结合人机交互实现

我的团队



- 依托“复杂网络系统安全保障技术教育部工程研究中心”、“辽宁省工业控制安全工程技术研究中心”
- 建立了“谛听”网络安全实验室，依托计算机学院，被辽宁省工信委授予“辽宁省工业信息安全支撑单位（首批）”。
- 建立了“谛听”工控网络安全态势感知平台，其中包括网络空间工控设备搜索引擎，高交互工控蜜罐，工业信息安全威胁情报采集平台等。
- 主编了国内第一部工控安全专著《工业控制网络安全技术与实践》，参与编写了工信部指导的《工业信息安全概论》、《工业互联网平台安全》。发布了《2018年全球工业控制网络安全态势白皮书》等白皮书10余篇

参考文献

本书既有对工业控制网络安全理论和技术的介绍，又有企业实战的经典案例，特别适合高校教学和技术培训使用。希望本书的出版能对我国工业控制网络安全领域的人才培养和技术发展起到积极作用，也希望更多的高校和企业加入到工控网络安全人才培养的队伍中来，产学合作，为我国网信事业发展培养更多人才。

—— **封化民** 教育部高等学校信息安全专业教学指导委员会秘书长

目前国内工业控制网络安全产业要解决的问题很多，其中一方面就是专业人才的培养。本书的出版恰逢其时，它填补了我国在工业控制网络安全领域教材的空白。本书既有理论价值，又汇集了实践经验，相信本书的出版能为工控网络安全的教学和研究提供有益的参考。

—— **孙一按** 北京匡恩网络科技有限责任公司 技术委员会主席

随着工业化与信息化的深度融合，工业控制系统中的信息化程度越来越高，随之而来的网络安全风险也越来越大，加之工业控制系统网络安全问题的独特性，掌握工业控制网络安全知识和工业控制网络漏洞分析与安全防御技术的专业人才极其缺乏，本书正是为满足这一需求而编写的。

主要特色

- 聚焦工业控制系统网络安全。本书以工业控制系统网络安全为核心，系统介绍了工业控制系统、工业控制网络、工业控制系统整体安全性、SCADA系统的安全性、工业控制系统网络漏洞、协议、安全防御等，旨在帮助读者全面了解工业控制网络安全领域的知识。
- 理论与实践深度融合。由于工业控制网络安全是跨学科的交叉领域，本书采取了高校和企业联合编写的新型模式，将工业控制网络安全的基本原理、概念系统展现出来，并辅以企业由真实项目凝练而来的案例，能够满足读者从理论到实践的多层次学习需求。
- 丰富的教学辅助资源。为了帮助高校开展课程教学，本书还提供了PPT、习题答案、实验手册等教学辅助资源，需要的教师可登录华章网站（www.hzbook.com）下载。

投稿热线：(010) 88379604
客服热线：(010) 88379426 88361066
购书热线：(010) 68326294 88379649 68995259
华章网站：www.hzbook.com
网上购书：www.china-pub.com
数字阅读：www.hzmedia.com.cn

工业控制网络安全技术与实践

武传坤 祝烈煌 姚羽 编著

机械工业出版社 China Machine Press

信息安全技术丛书

- 国内首部面向初学者系统介绍工业控制网络安全的著作
- 工业控制网络安全领域的专家合作编写，从学术与工程视角全面涵盖工业控制网络的原理、技术与实践，帮助读者深度理解和掌握工业控制网络安全的精髓

工业控制网络安全技术与实践

姚羽 祝烈煌 武传坤 编著

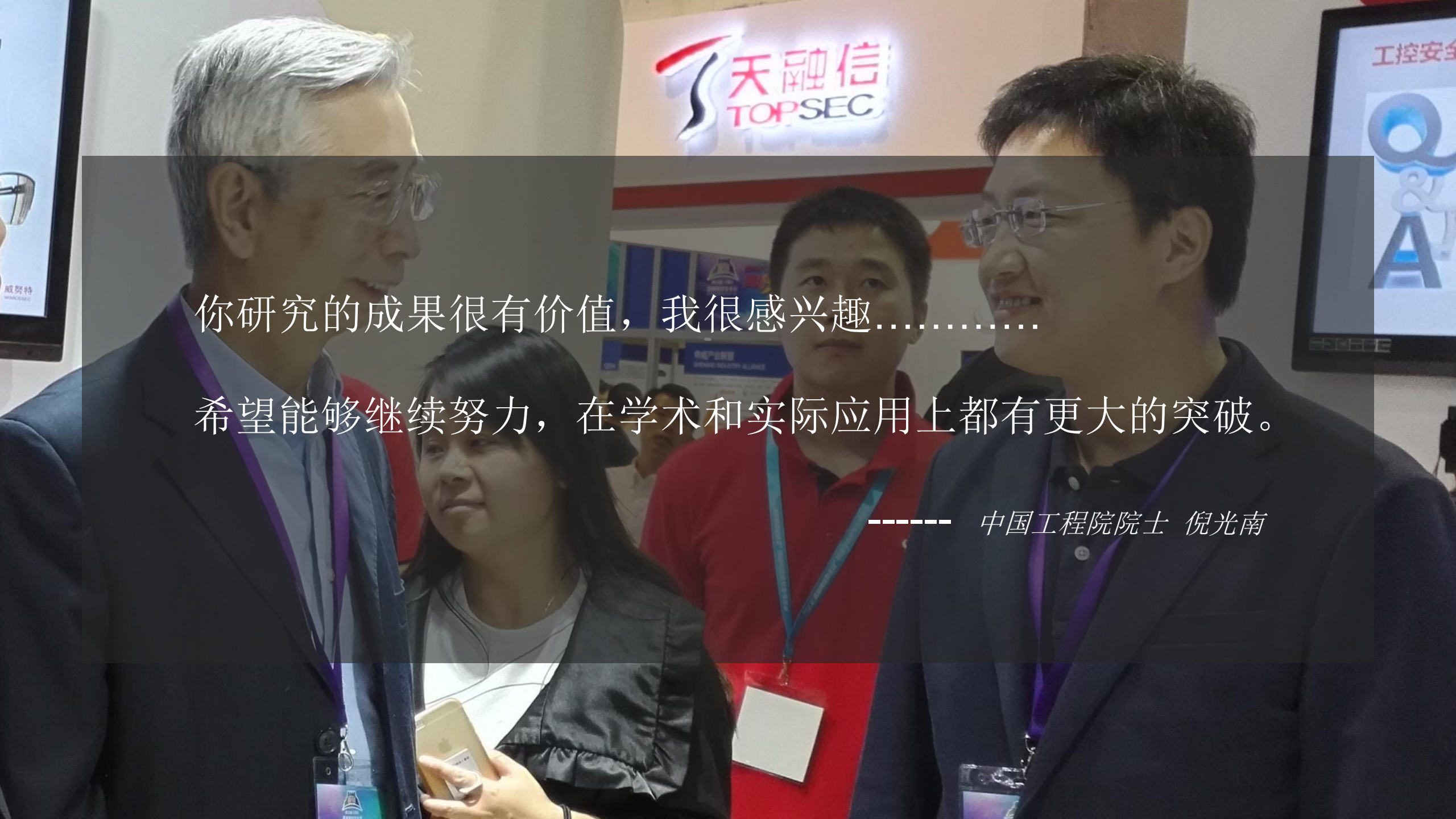
机械工业出版社 China Machine Press

作者简介

姚羽 东北大学教授、博士生导师，沈阳大数据局副局长（挂职），教育部新世纪人才。主要研究方向包括恶意软件攻防分析及建模、网络安全数据分析、网络安全数据可视化、工控网络安全分析、网络空间安全态势感知等。作为项目负责人主持国家自然科学基金项目、教育部“新世纪人才支持计划”等项目10余项，发表学术论文40余篇，获辽宁省科技进步二等奖、辽宁省自然科学学术成果一等奖。

祝烈煌 北京理工大学教授、博士生导师，教育部新世纪优秀人才。中国网络空间安全协会理事，中国人工智能学会常务理事，智能信息网络专业委员会主任委员。长期从事网络与信息安全方向的研究工作，承担国家重点研发计划课题、教育部新世纪优秀人才支持计划、国家自然科学基金、国防预研基金、北京市自然科学基金等国家级、省部级科研项目20余项。撰写英文专著1部，发表SCI/EI检索学术论文100余篇，获省部级科技奖励1项。

武传坤 博士，曾任西安电子科技大学教授，西悉尼大学研究员。1993年获国务院颁发的政府特殊津贴。2002年入选中国科学院“百人计划”，任中科院信息安全国家重点实验室研究员、博士生导师。2016年7月起受聘于北京匡恩网络科技有限责任公司，任智能安全工业研究院副院长。



你研究的成果很有价值，我很感兴趣.....

希望能够继续努力，在学术和实际应用上都有更大的突破。

------ *中国工程院院士 倪光南*

Thanks

谛听

感知工控网络空间安全态势

www.ditecting.com