



构建工业互联网安全 人才培养生态

王冰

北京益安在线科技股份有限公司联合创始人&运营总监



目录

01

工业互联网安全现状及发展形势

02

工业互联网安全人才现状

03

工业互联网安全人才培养体系

04

构建工业互联网安全人才培养生态

国际形势一：全球网络空间攻防对抗强度不断升级，网络攻防呈现新特性



国际形势二：各国纷纷加快推进战略部署实施，网络空间博弈更趋激烈

国际形势三：全球网络攻击与网络犯罪事件频发已成为全球性安全挑战



国际形势四：数据安全和个人信息保护形势严峻全球数据安全保护规则升级

国际形势五：全球安全产业规模稳步增长发展态势总体良好



国际形势七：加快布局**工业互联网安全**融合安全关注度持续提升

国际形势六：欧美等国网络安全人才培养起步早体系化培养机制趋于成熟



国际形势八：新技术新业务领域活力涌现带来全新安全挑战

全球安全 **八** 大形势

我国安全六大形势

国内形势一：国家高度重视网络安全加速推进纵深领域立法工作



国内形势四：逐步完善工业互联网安全顶层设计构建安全生态体系

国内形势二：NB-IoT和5G发展迅猛，面临新的安全挑战和需求



国内形势五：我国网络安全产业体系日趋完备步入崭新发展阶段

国内形势三：产学研协同联动积极推动车联网安全防护工作



国内形势六：多措并举，积极推进网络安全人才队伍建设与培养



工业互联网 安全发展趋 势

- 新技术持续创新融合推动网络安全攻防角色转变
- 5G安全新需求驱动需解决不同层次的安全问题
- 数据安全与国家安全密切相关保护数据安全逐渐成为各国共识
- **政产学研形成合力，助力构建工业互联网安全保障体系**
- 人才成为各国发展的关键要素完善网络安全人才培养体系成为下一步工作重点

政产学研形成合力，助力构建工业互联网安全保障体系



□ 工业互联网安全防护智能化将不断发展

- 将转变工业互联网安全防护的传统思维模式，由传统的事件响应式向**持续智能响应式**转变

□ 工业互联网安全态势感知将成为重要技术手段

- 在安全威胁对工业互联网正常运行造成实质性影响之前及时发现并妥善处置，态势感知的实现离不开政、产、学、研的协同合作

□ 信息共享和联动处置机制成为重要一环

- 政、产、学、研需统一认识、密切配合，建立健全运转灵活、反应灵敏的**信息共享与联动处置机制**

□ 工业互联网安全人才将成为工作重点

- 高等院校、专业机构和安全企业建立**联合培养机制**，加快培养既掌握工业控制知识又熟悉安全防护技术的复合型人才成为必然趋势
- 开展**攻防演练、安全竞赛**等成为选拔不同层次的工业互联网安全从业人员的重要手段



目录

01

工业互联网发展现状及安全形势

02

工业互联网安全人才现状

03

工业互联网安全人才培养体系

04

构建工业互联网安全人才培养生态

网络安全人才现状分析

01



网络安全人才严重不足

02



人才需求爆发式增长

03



规模有限队伍构成不完整

04



高层次实战型人才不足

我国安全专业人才缺口达**70万** 高校培养每年递增1.5万人

140万

预计到**2020**年，我国重要行业信息系统和信息基础设施需要各类安全人才将达140万人

1.5万

近几年，我国高校学历教育培养的信息安全专业人才数量远远不能满足企业用人需求，2000余所高校，每年约培养1.5万人

(数据来源：智联招聘)

工业互联网安全从业人员**供需严重失衡**，存在结构性问题



我国网络安全学科教育年度培养规模**约 1 万人左右**



自我期望和要求较高，培养需求难以得到充分满足



整体发展不充分，地域、行业、岗位间差异较明显



从业人员**普遍**在知识储备、技能等方面存在**短板**



职业发展路径不明确，缺乏人员分类和评价的标准



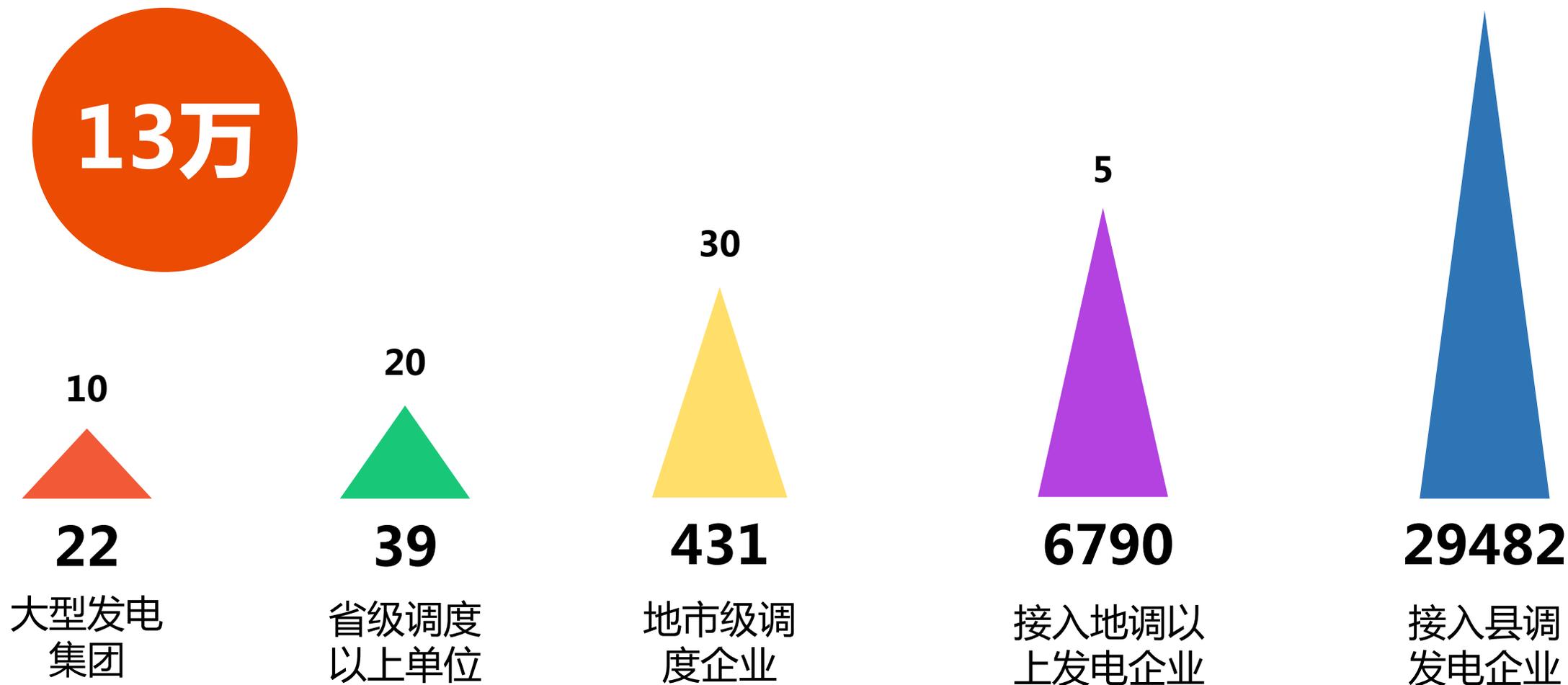
压力感受普遍比较大，但整体职业满意度依然向好



资质认定能有效促进职业发展，但持有情况不乐观

我国目前工业互联网安全人才形势严峻，需加紧完善网络安全人才培养体系

◆ 电力行业工业控制网络安全人才现状





供不应求





目录

01

工业互联网发展现状及安全形势

02

工业互联网安全人才现状

03

工业互联网安全人才培养体系

04

构建工业互联网安全人才培养生态

开展工业互联网安全人才培养的国家政策导向

2017年

- 国务院印发《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，明确了建设网络、平台、安全三大体系，这是国家工业互联网发展的纲领性文件。

2018年

- 2018年6月7日，工业互联网专项工作组第一次会议审议通过《工业互联网发展行动计划》（2018-2020年）

2020年底

- 2020年底，初步建成工业互联网基础设施和产业体系

一大联盟

工业互联网产业联盟 (AII)：成为推动我国产业发展的重要载体（756家会员，涵盖国内外主要工业和ICT企业，20个工作组/任务组+11个垂直行业领域，29份报告，45个测试床，44个应用案例）



两大阵营

应用性企业：
主要包括各类离散和流程型制造企业

基础性企业：
包括基础电信、互联网、自动化、软件、集成商和部分先发性制造企业等

三大路径

路径1：
面向企业内部的生产率提升—智能工厂

路径2：
面向企业外部的价值链延伸—智能产品/服务/协同

路径3：
面向开放生态的平台运营—工业互联网平台

四大模式

基于现场连接的
智能化生产

基于企业互联的
网络化协同

基于产品联网的
服务化延伸

基于供需精准对接的
个性化定制

◆ 工业互联网安全人才的要求和能力



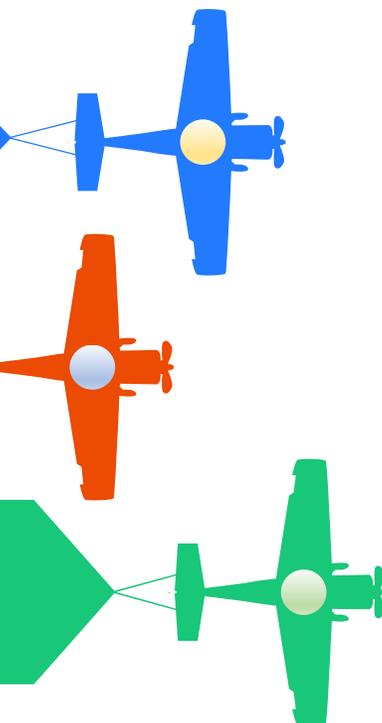
防护技术要求更高



防护标准更复杂



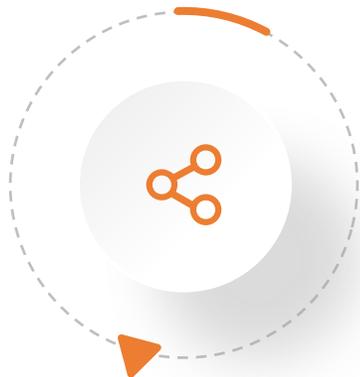
漏洞和攻击途径更多



企业所需的技术人员应具有工业互联网安全知识、应急处置能力、安全运维技能才能更好的解决工业互联网安全问题。

- 网络安全普及类课程
- 网络安全法标准类课程

基础课程培训



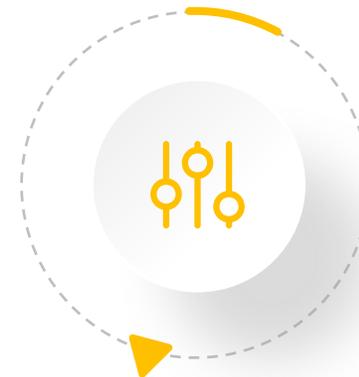
提升课程培训

- 网络安全技术类课程
- 网络安全专项课程



- 工业互联网安全系列认证

权威资质认证，益安在线培训



实战训练+应用实践

- 安全攻防演练
- “护网杯”大赛



多种形式的人才培养生态链

目录

01

工业互联网发展现状及安全形势

02

工业互联网安全人才现状

03

工业互联网安全人才培养体系

04

构建工业互联网安全人才培养生态



培养模式

网络安全人才队伍
培养模式“推陈出新”

倡导总体布局，构建人才体系

加强网络安全人才顶层设计，建立网络安全人才岗位框架体系，制定多样化网络安全人才培养总体规划，协同政府、高校、企业等力量共同推进网络安全人才的培养工作。

构建“精英模式”，创新人才选训

打造网络安全专业技能标准化体系。与国家有关部门联合，充分调用网络安全企业顶尖网络安全技术专家团队、知名高校、行业专家资源和能力，以网络安全人才能力培训体系为基础，按照“防控、预警、处置、等级保护、审计”为细化方向，开展线上线下结合的网络安全专业技能标准化课程和训练体系。

统筹各方资源，重视社会力量

注重与网络安全企业、科研机构以及各类保障队伍的人才交流，政产学研用有机结合，建立人才培养完整生态。



- 我国从人才培养政策、一级学科建设、安全产业园区、开展竞赛、校企合作，以及每年网络安全宣传周活动等方面，积极推动网络安全人才队伍的建设与培养。

● 政策支持与学科建设

- 《关于加强网络安全学科建设和人才培养的意见》、《网络安全法》等：强化网络安全人才培养
- 学科建设：首批7所高校一流网络安全学院示范建设、29所高校设立一级学科博士点

● 产业园区建设与安全宣传

- 安全产业园区建设：2017年启动国家级网络安全产业园区建设
- 网络安全宣传教育：自2014年以来每年开展网络安全宣传周活动，大力宣传普及网络安全知识

● 竞赛与校企合作

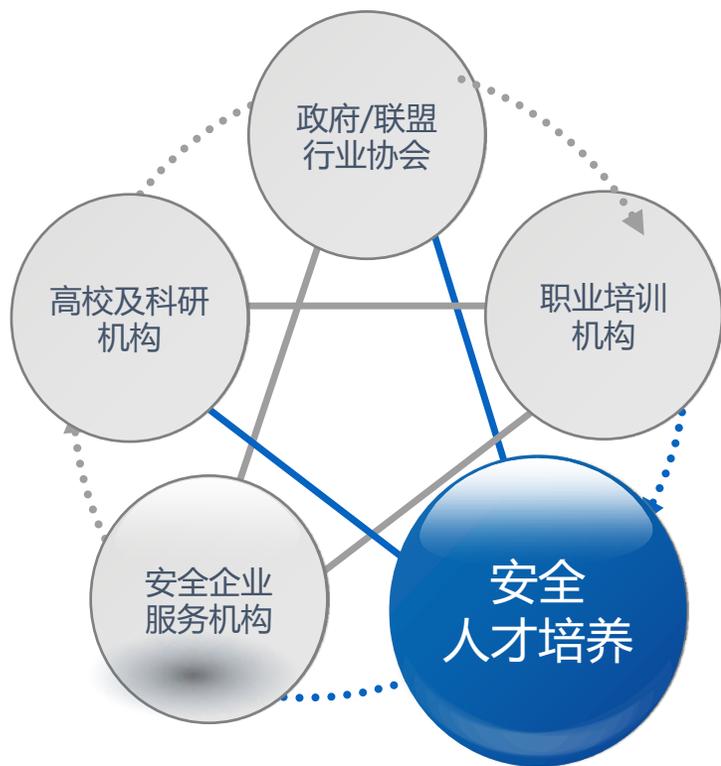
- “护网杯”：近3000支队伍报名参赛，44支队伍进入决赛，助推安全人才的发现选拔
- 校企合作：校企合作模式在高校和企业间得到有力推动

◆ “护网杯” 2018年网络安全防护赛暨首届工业互联网安全大赛



2018年10月26日，“护网杯”2018年网络安全防护赛暨首届工业互联网安全大赛闭幕式暨颁奖仪式在北京航空航天大学成功举办。

本次大赛强调实用性与融合性，紧密结合近年工信部安全防护执法检查发现企业存在的突出问题，比照企业真实系统和平台搭建安全防护场景，融合部署涵盖电信网、互联网、工业互联网和融合业务等新型领域的决赛场景。



构建健康合理的安全生态

- 网络安全教育以道德和法制教育为基础
- 网络安全需要形成合理的人才结构体系
- 安全产业需要人才的支撑，人才也需要在安全企业的得到滋养
- 网络安全教育不止于知识和技能教育，需要科学方法和探索求证的精神，培养网络安全人才的开拓创新精神。

THANKS
2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE