2021世界电信和信息社会日大会

电力系统信息物理综合安全

刘 烃

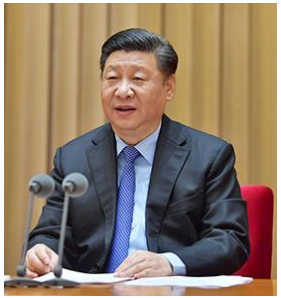
西安交通大学 网络空间安全学院

2021年5月18日

电力系统安全事件频发，威胁持续升级

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**。

习近平总书记，网络安全和信息化工作座谈会



蠕虫攻击导致核电站停运

震网攻击导致核设施故障

网络攻击导致基辅区域停电

网络攻击+物理破坏导致全国停电

攻击配电系统导致离心机损毁

攻击输油管道导致全美进入紧急状态

电力系统安全威胁1.0

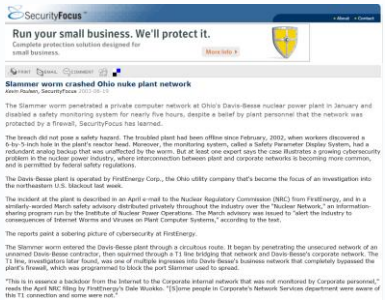
2003

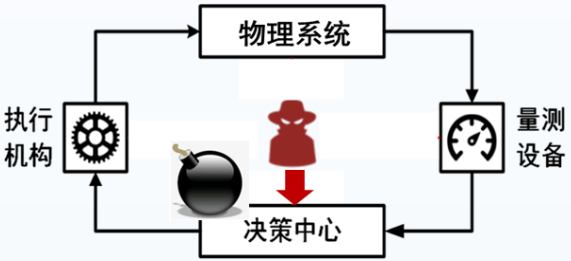
美国

电力系统安全威胁1.0

网络入侵、计算机病毒等网络空间攻击，导致电网的信息系统故障

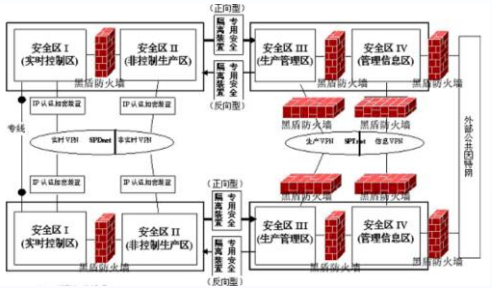
2003年，Slammer蠕虫入侵核电站，导致系统关闭

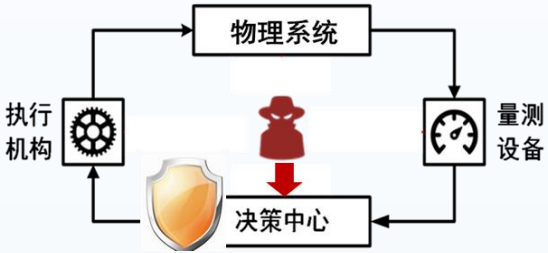




安全分区、网络专用、横向隔离、纵向认证

电监会5号令，2004年





电力系统安全威胁 2.0

2003 2010 2015

美国

伊朗

乌克兰

电力系统安全威胁1.0

网络入侵、计算机病毒等网络空间攻击，导致电网的信息系统故障

电力系统安全威胁2.0

定向攻击电力系统感知、决策和执行环节，造成物理系统的运行故障、设备损毁

电网安全威胁2.0 - 2010年Stuxnet攻击伊朗核设施

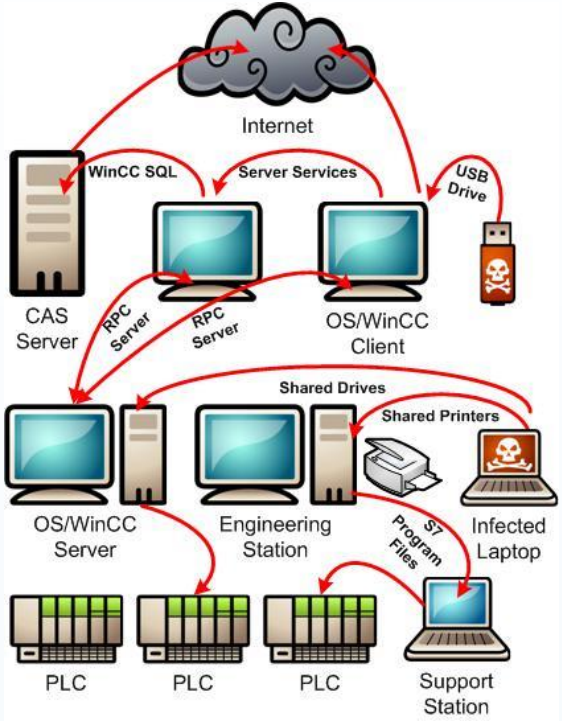
Stuxnet

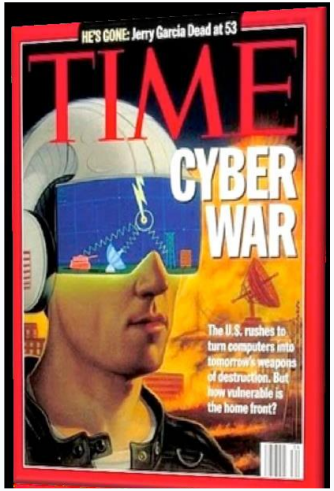
系统接入　U盘摆渡

漏洞利用　MS08-067等安全漏洞

数据篡改　控制指令与量测数据

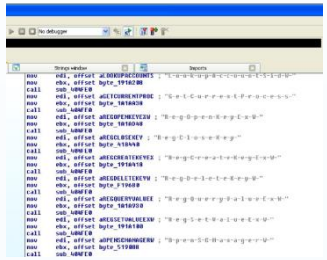
应用/业务威胁　损坏离心机





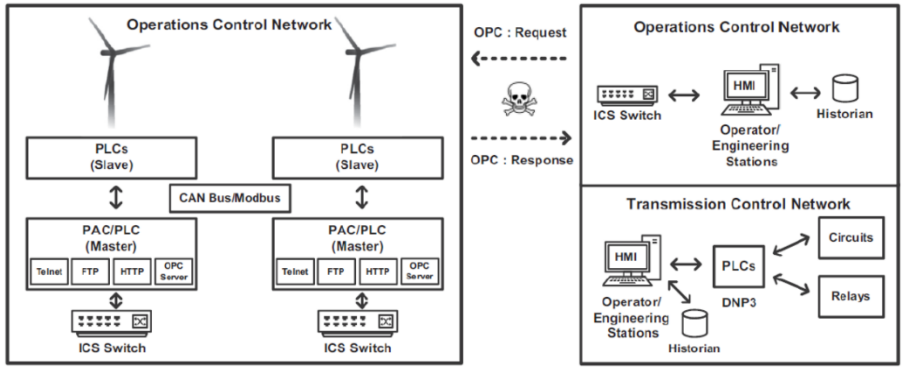
电网安全威胁2.0 - 2015年BlackEnergy3攻击乌克兰电网

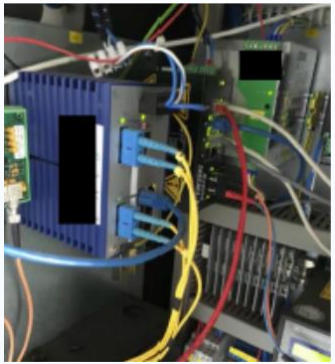
	Stuxnet	BlackEnergy3
系统接入	U盘摆渡	钓鱼邮件 VPN
漏洞利用	MS08-067等 安全漏洞	PLC漏洞
数据篡改	控制指令与 量测数据	控制指令
应用/业务 威胁	损坏离心机	关闭电闸， 大规模停电 电话DDoS



电网安全威胁2.0 - 2017年WindShark攻击美国风电场

	Stuxnet	Black Energy3	WindShark
系统接入	U盘摆渡	钓鱼邮件 VPN	物理连接 控制系统
漏洞利用	MS08-067等 安全漏洞	PLC漏洞	SCADA 身份认证漏洞
数据篡改	控制指令与 量测数据	控制指令	控制指令
应用/业务 威胁	损坏离心机	关闭电闸， 大规模停电 电话DDoS	控制风力 发电机





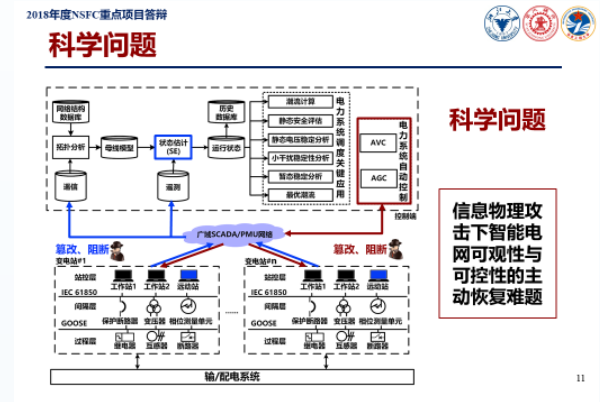
电网安全威胁2.0 – 网络安全视角

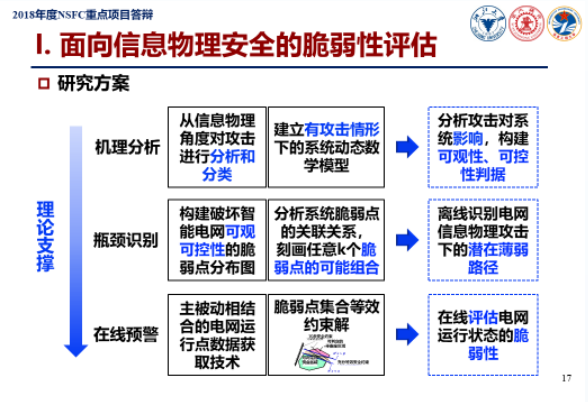
针对典型的电网攻击流程，探索智能电网的威胁模型和信息安全纵深防御架构，提出设备接入监测与阻断、脆弱性分析与加固、控制指令与量测数据异常检测等信息安全防护理论与技术，为智能电网的安全运营提供支撑。

国家电网-NSFC重点项目. 智能电网信息安全纵深防护关键技术 (U1766215)

电网安全威胁2.0 - 控制安全视角

挖掘智能电网信息空间和物理空间深度融合的特征，从识别、检测和保护三个方面设计安全回路，构建具有自演化能力的识别-检测-防护一体化主动防御模型，突破信息物理融合的威胁识别、基于电网物理特征的异常检测、信息物理安全控制理论与技术





NSFC重点项目. 面向智能电网的信息物理安全理论和主动防御技术(61833015)

电力系统安全威胁2.0 - 防御

2003 2010 2015

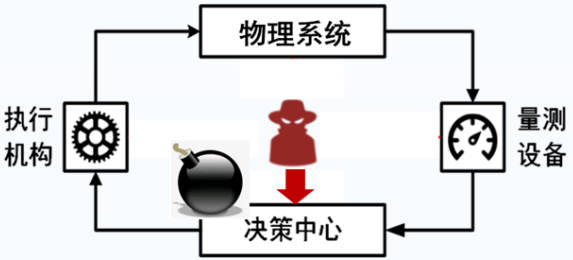
美国

伊朗

乌克兰

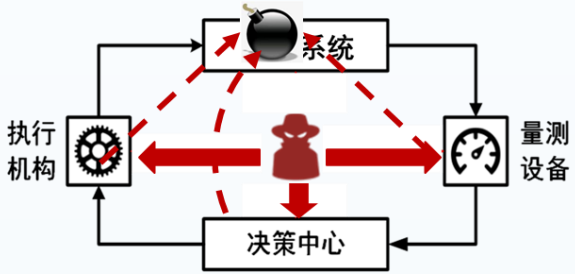
基础设施安全威胁1.0

网络入侵、计算机病毒等网络空间攻击，导致信息系统故障

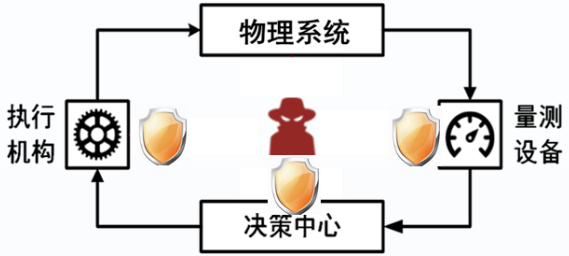


基础设施安全威胁2.0

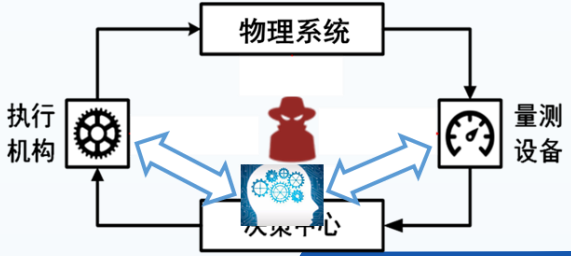
定向网络攻击基础设施信息系统，干扰物理系统运行，造成设备损坏和系统瘫痪



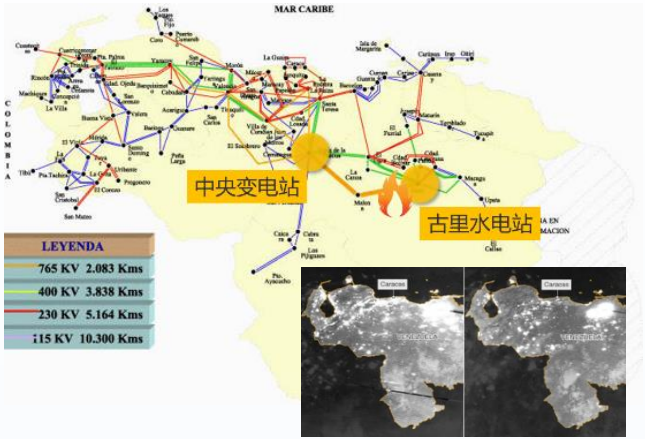
网络安全：建立纵深安全防护体系



控制安全：构建更智能和安全的控制能力



电网安全威胁3.0 – 2019.3.7委内瑞拉大停电



现任总统：马杜罗

电力系统遭受网络攻击、电磁攻击、燃烧爆炸。

反对党领导人：胡安·瓜伊多

现政府不作为，新政府可解决停电问题。

委内瑞拉政府难以应对电网的潜在崩溃，将导致公众骚乱……

反对政府可借此获得民众支持

应用非暴力行动与策略中心(CANVAS)

2010年（维基解密2013年透漏）

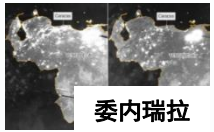
电力系统安全威胁 3.0

2003 2010 2015 2019 2021

美国

伊朗

乌克兰


委内瑞拉


伊朗


美国

电力系统安全威胁1.0

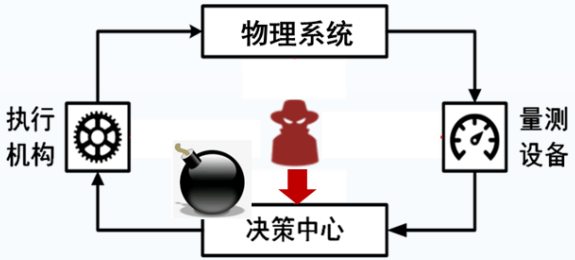
网络入侵、计算机病毒等网络空间攻击，导致电网的信息系统故障

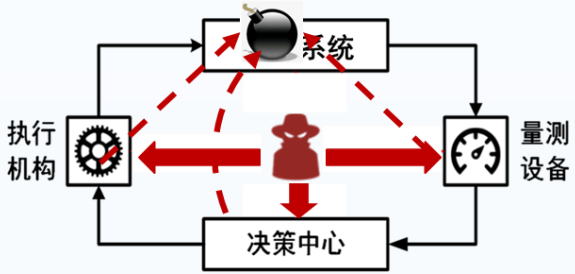
电力系统安全威胁2.0

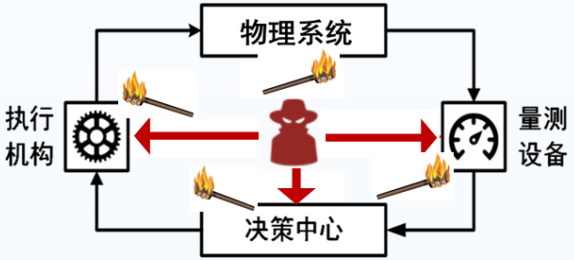
定向攻击电力系统感知、决策和执行环节，造成物理系统的运行故障、设备损毁

电力系统安全威胁3.0

信息攻击与物理破坏相结合的混合攻击，造成电力系统的系统性瘫痪







电力系统信息物理综合安全

“系统安全性问题正在从工程故障为主的物理安全问题，变成同时考虑物理系统安全和网络信息安全的综合安全性”

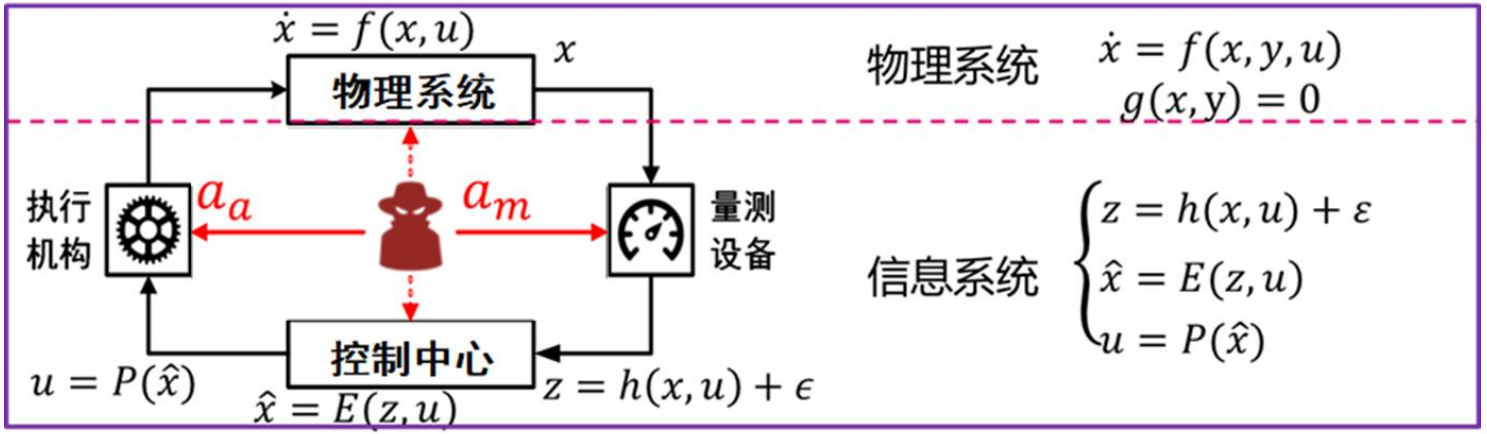
“电网的安全控制正从面向物理系统的安全防护走向涉及自然和社会因素的综合灾变防御”。

-- 《信息物理融合能源系统》 科学出版社. 2016

综合安全攻击定义：攻击者利用信息网络与物理系统之间的紧密耦合关系，利用网络攻击或者物理攻击技术，造成CPS系统故障或诱导故障在系统传播，破坏CPS完整性、可用性或保密性的行为。

--信息物理融合系统综合安全威胁与防御研究综述, 自动化学报,2019

信息物理融合系统威胁建模



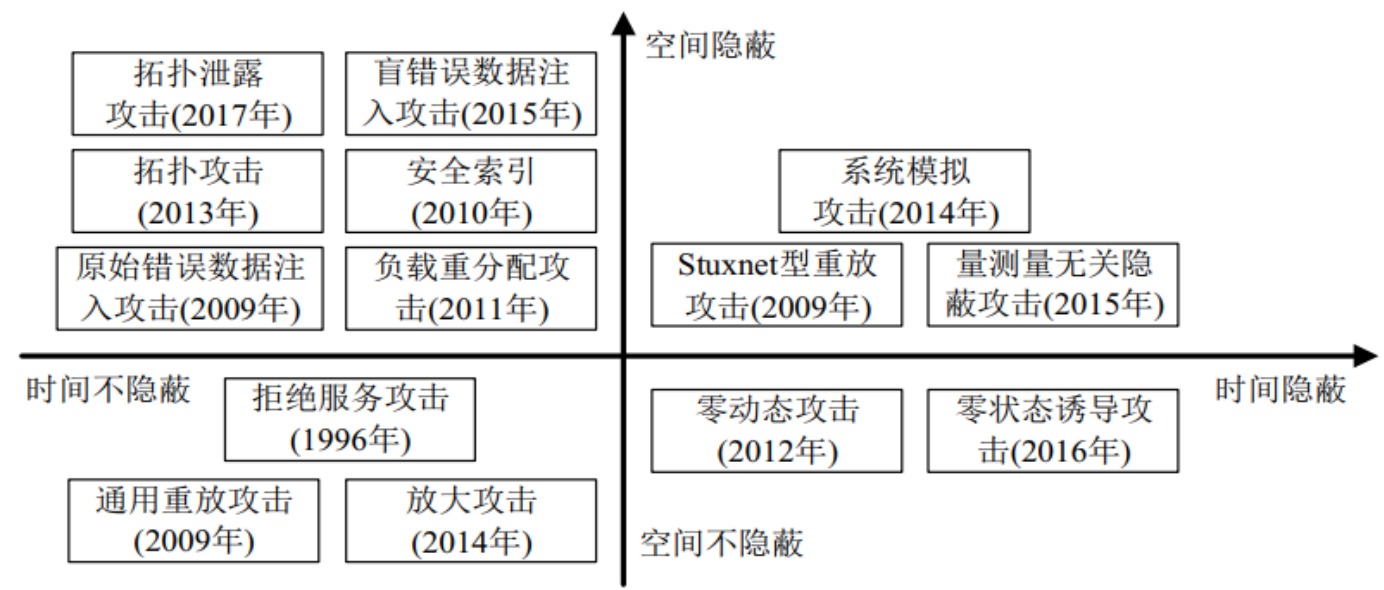
- 量测数据篡改：伪造量测数据隐藏攻击行为或诱导系统做出错误决策
- 控制指令篡改：伪造控制指令直接干扰系统正常运行

物理系统
$$\dot{x_a} = f(x_a, u_a)$$
$$g(x_a, y) = 0$$

信息系统
$$\begin{cases} z_a = h(x_a, u_a) + \varepsilon + a_m \\ \hat{x} = E(z_a, u) \\ u_a = P(\hat{x}) + a_a \end{cases}$$

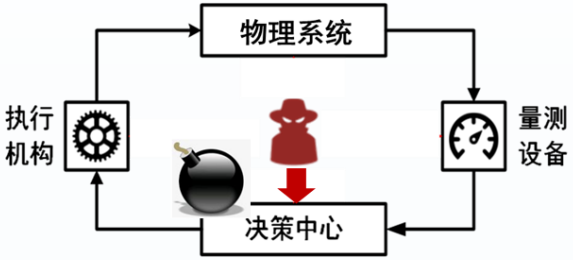
信息物理融合系统威胁建模

- 时间隐蔽型：通过持续攻击，使得伪造数据符合信息系统和物理系统的动态预期/规律
- 空间隐蔽型：通过同时攻击不同节点，使得多节点数据符合信息系统和物理系统的空间关联预期/规律



总结

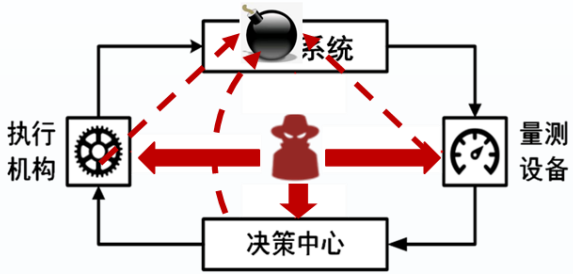
安全威胁1.0



防御方法：漏洞挖掘、网络管理（隔离、流量监控）等，发现和修复电力系统安全漏洞

攻击“进不来”

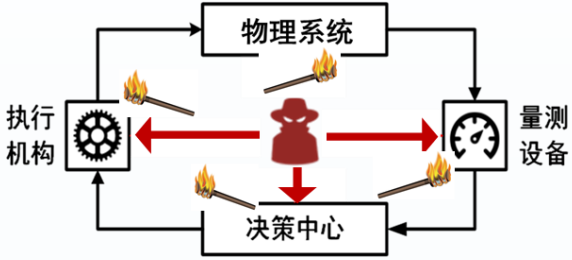
安全威胁2.0



防御方法：综合应用网络安全与物理安全技术，检测网络攻击行为、阻断攻击对物理设备的破坏

攻击“躲不过”

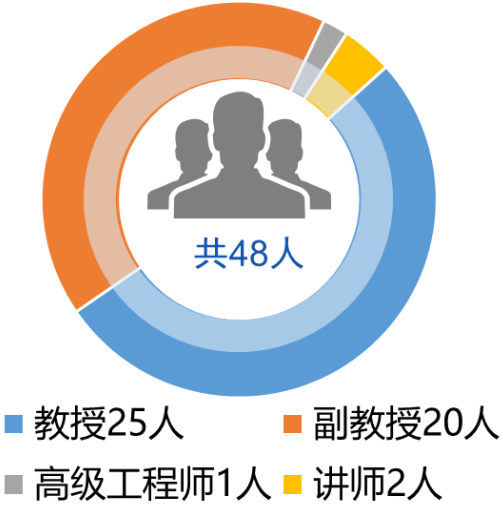
安全威胁3.0



防御技术：构建信息物理综合安全协同防御体系，感知信息-物理协同攻击、阻断威胁跨域影响、阻断故障传播

系统“打不垮”

西安交通大学网络空间安全学院
智能网络与网络安全教育部重点实验室



高层次人才
中国科学院院士 2人
教育部长江学者特聘教授2人，青年学者2人
国家自然科学基金委杰青2人，优青3人
千人计划1人，青年千人 4人

管晓宏 院士

徐宗本 院士

郑庆华 教授

欢迎领导专家莅临指导！

刘烃 tingliu@xjtu.edu.cn