泛在电力物联网安全防护体系架构及关键技术

国网辽宁省电力有限公司

2019.11

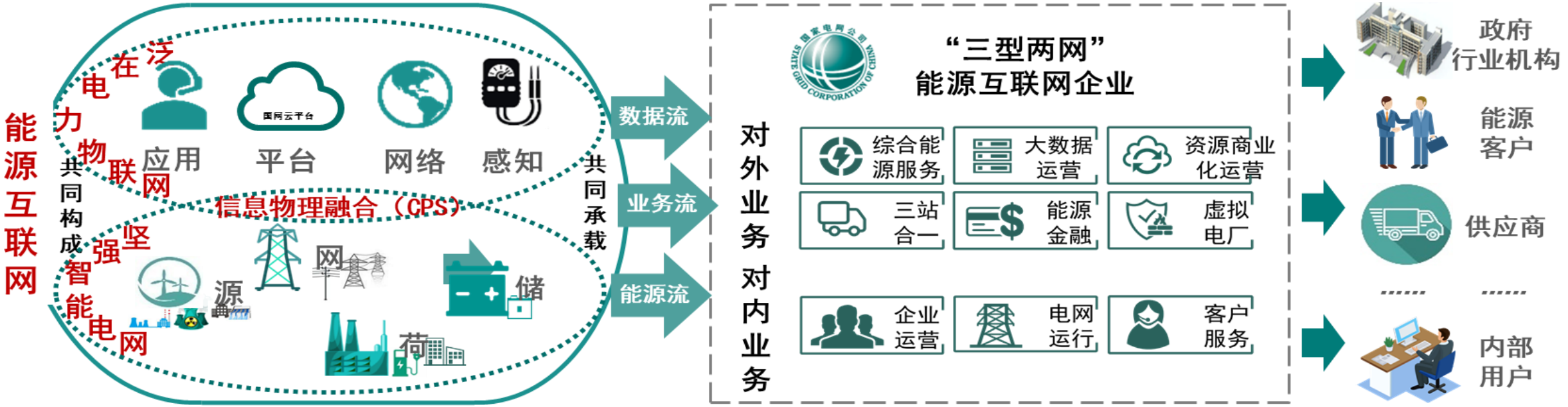
目 录

报告提纲

contents

泛在电力物联网建设引导行业变革

- 2019年国网公司做出全面推进“三型两网”建设，加快打造具有全球竞争力的世界一流能源互联网企业的战略部署，是网络强国战略在公司的具体实践，是落实中央部署、发挥央企带头作用的重要举措，是适应内外部形势和挑战的必然要求。
- 泛在电力物联网具有连接泛在化、终端智能化、数据共享化、服务平台化等主要特征，通过互联网新技术的运用，实现全面感知、精准预测和智能决策，带来质量变革；实现体制创新、快速响应，带来效率变革；实现技术创新和模式创新，带来动力变革。



世界网络安全形势不容乐观

- **部分国家网络安全“先发制人”，组建国家式、集团式网络安全组织，通过相关技术垄断和软件后门，并应用各类网络武器，持续对世界主要国家进行针对性、长期的隐蔽攻击，攻击范围和影响呈快速扩大态势，给各国安全造成巨大威胁，全世界深刻认识到网络安全的重要性和艰巨性。。**

2010年，美国和以色列联合制造的“震网”病毒攻击伊朗核设施，导致伊1000台离心机报废，致使伊朗核计划几乎“停滞”。

——摘自德国2013年07月《明镜周刊》

2016年，美国前国防部长卡特首次承认，美国使用网络手段攻击了叙利亚ISIS组织等，这是美国首次公开将网络攻击作为一种作战手段。

——摘自德国2013年07月《明镜周刊》

2018年，特朗普签署命令，推翻前总统奥巴马2012年签署的“第20号总统政策指令”，让军方更自由地部署先进网络武器，不用受国务院和情报界阻挠。

——摘自2019年06月《人民日报》

2019年，据《纽约时报》报道，美国正在加大对俄罗斯的网络攻击，从2012年开始美国已将侦查探测器置入俄罗斯电网的控制系统。

——摘自美国2019年06月《纽约时报》

2019年6月，目前业界公认的两个顶级的高级持续性威胁（APT）组织“方程式”和“索伦之眼”，其后台都是美国国家安全局（NSA）。

——摘自2019年06月《人民日报》

《2018年我国互联网网络安全态势综述》指出，美国对我国网络攻击较2017年增长约90%。

国家不断提升网络安全要求

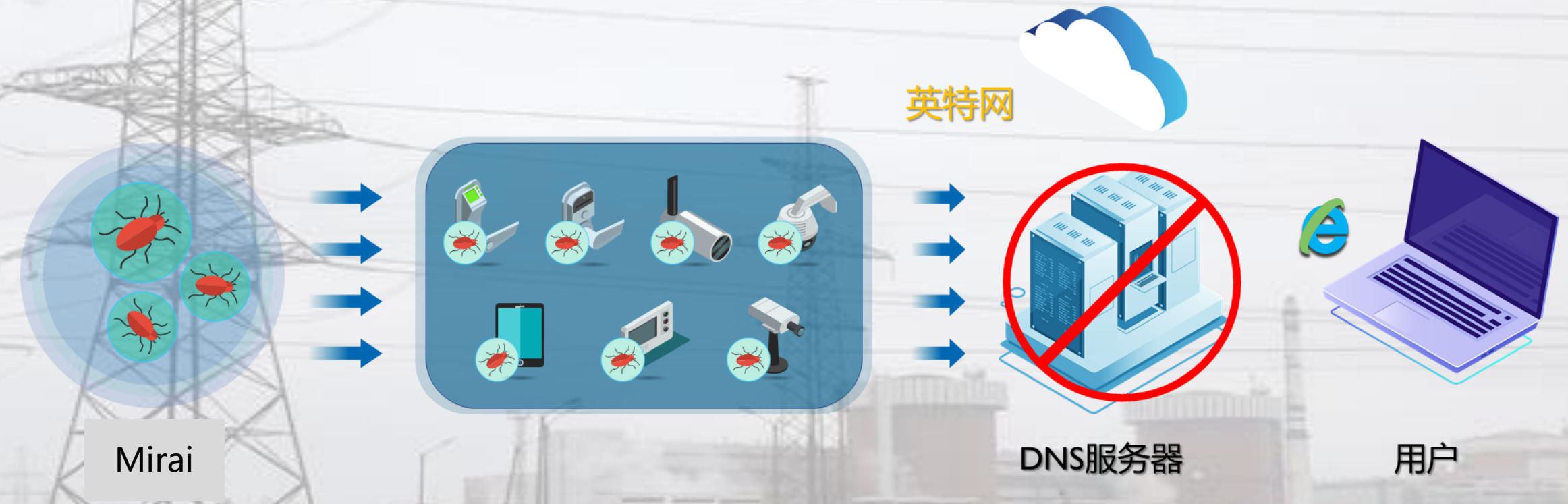
- **党中央、国务院高度重视网络安全。**习近平总书记多次就网络安全发表重要讲话，强调“没有网络安全就没有国家安全”，做出了一系列重大部署。
- 国家发布了《网络安全法》《密码法》等系列法律法规，将网络安全上升至法律高度。2018年，国家能源局印发电力行业网络安全工作的指导意见，指导电力行业网络安全工作。

国家发布多项法律法规等重要文件

- 2017年6月1日，《中华人民共和国网络安全法》正式施行
- 2017年，《个人信息保护法（草案）》发布
- 2017年7月，《关键信息基础设施安全保护条例（征求意见稿）》公开征求意见
- 2018年6月，《网络安全等级保护条例（征求意见稿）》公开征求意见
- 2018年9月，国家能源局印发《关于加强电力行业网络安全工作的指导意见》
- 2019年10月，《中华人民共和国密码法》经全国人大常委会表决通过。

安全事件频发增加物联网建设担忧

- 2016年10月，针对IP摄像头等物联网设备的Mirai恶意程序，控制全球近 40 万物联网设备，对美国域名服务商Dyn发起网络攻击，致使**美国东海岸的大部分互联网瘫痪**。



以物联网设备为感染目标形成僵尸网络

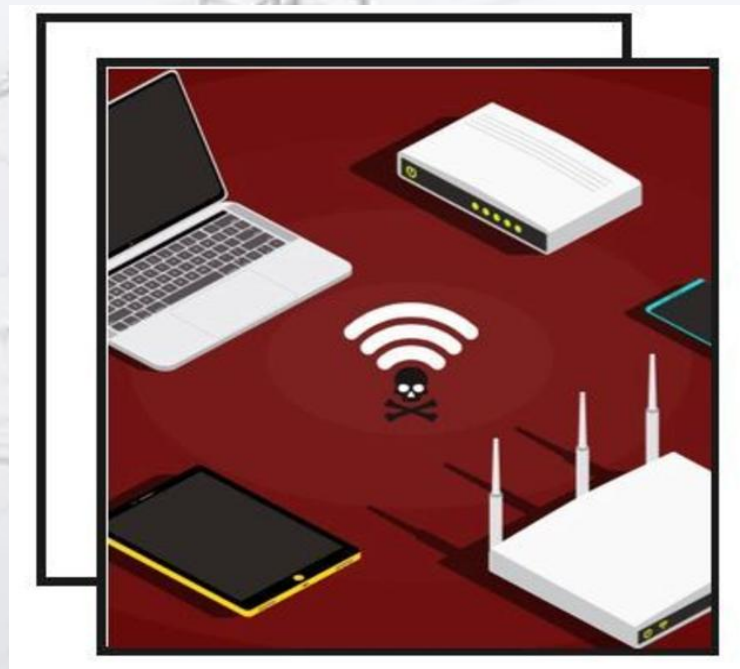
安全事件频发增加物联网建设担忧

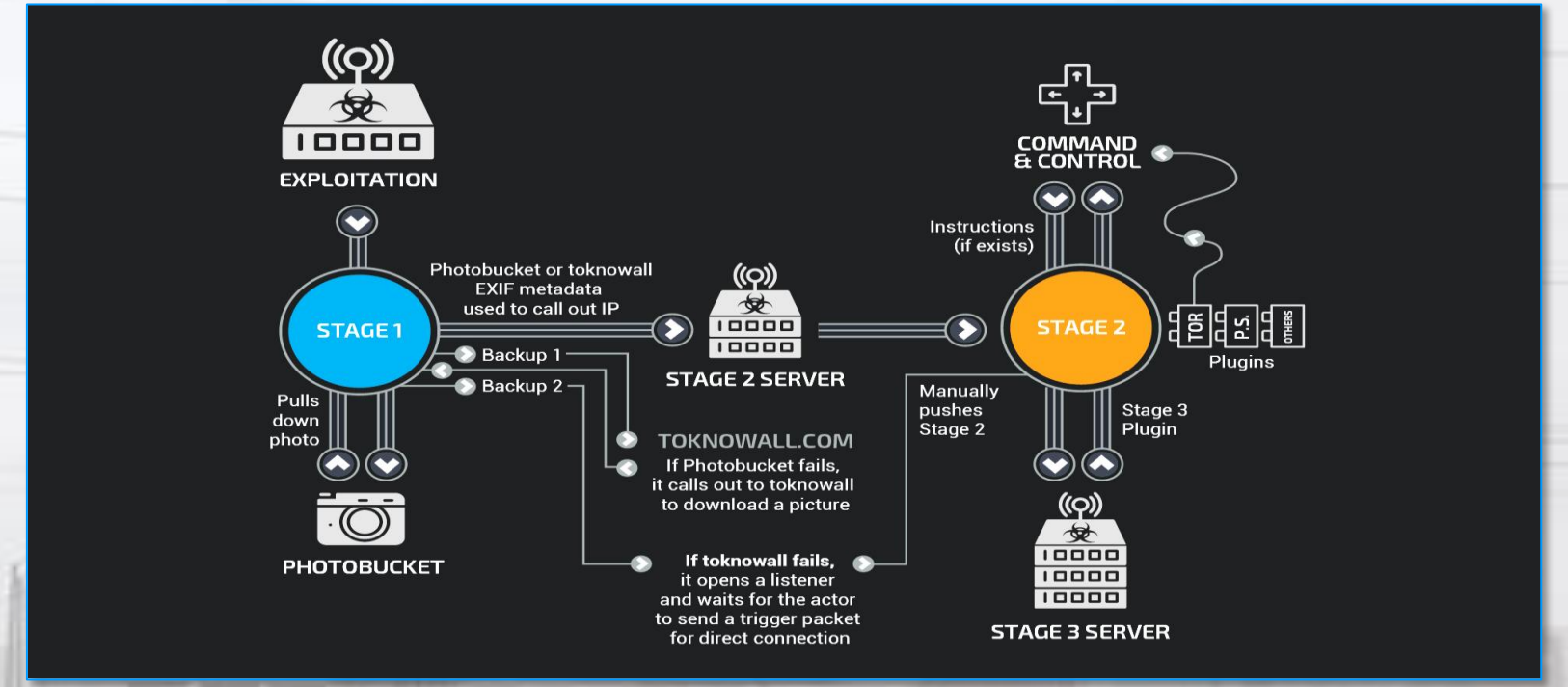
- 2018年1月，HNS （“捉迷藏”）僵尸网络开始感染物联网设备，**是首个能在设备重启后存活下来的恶意软件，开启了物联网僵尸网络的“新时代”**，5个月内感染超过9万台设备，可发起超过800Gbps的DDOS攻击。

面向物联网设备的病毒不断演进

安全事件频发增加物联网建设担忧

- 2018年5月，VPNFilter恶意软件在互联网中蔓延，通过感染小型或家用路由器，拦截、篡改、伪造经过路由器的Modbus、SCADA协议指令对工控网络和网络基础设施进行攻击破坏，感染了全球 54 个国家的超过 50 万台路由器与 NAS 设备。

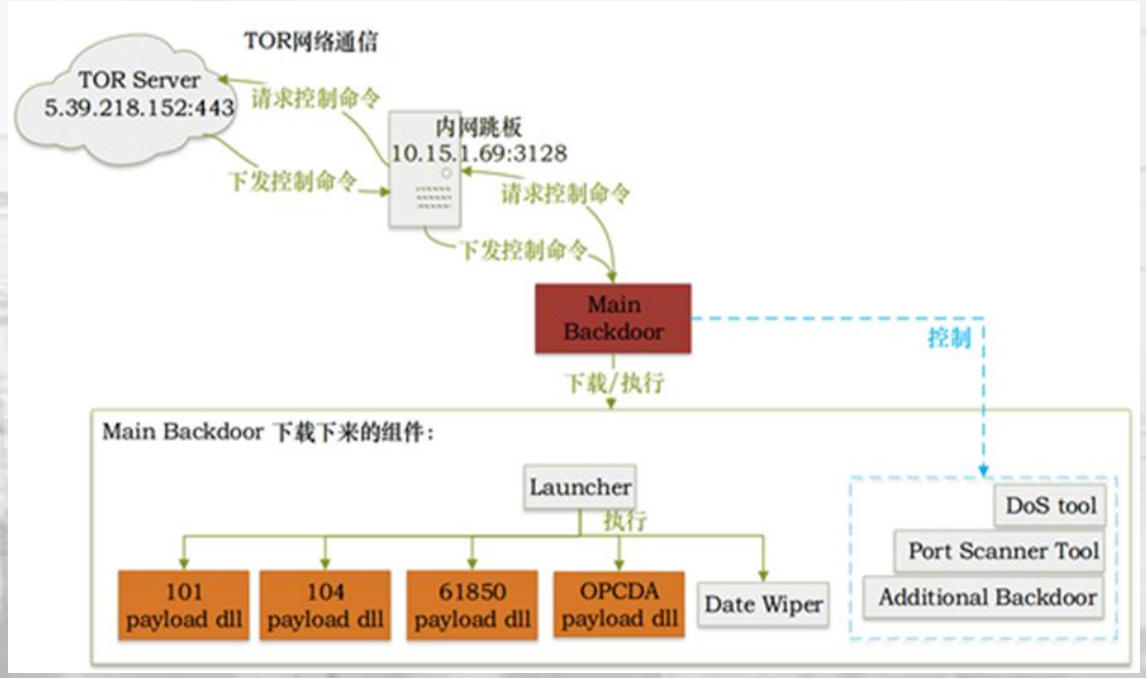




首个通过控制物联网路由器威胁工控安全的恶意软件

安全事件频发增加物联网建设担忧

- **电力物联网方面，2017年6月，国外发现针对电网智能终端的“Industroyer”恶意软件，该恶意软件利用通用工业通信协议在安全认证机制上的缺失，随意篡改控制指令，可以无限循环打开关闭断路器，从而对全球近百个变电站智能终端进行控制。**



电力工控协议在设计之初安全性考虑不足

安全事件频发增加物联网建设担忧

- 2016年，国内个别型号配电终端被发现存在配置界面弱口令和权限绕过漏洞，安全专家模拟的攻击者可利用漏洞登录配电终端，**进入配电自动化系统网络**。
- 2017年，国内部分充电桩使用的SIM卡被发现无线专网访问控制失效，且内置系统存在硬编码漏洞，**攻击者可利用上述问题，远程访问充电桩内系统存储的文件和数据**。

电力物联网设备漏洞隐患时有发现

目 录

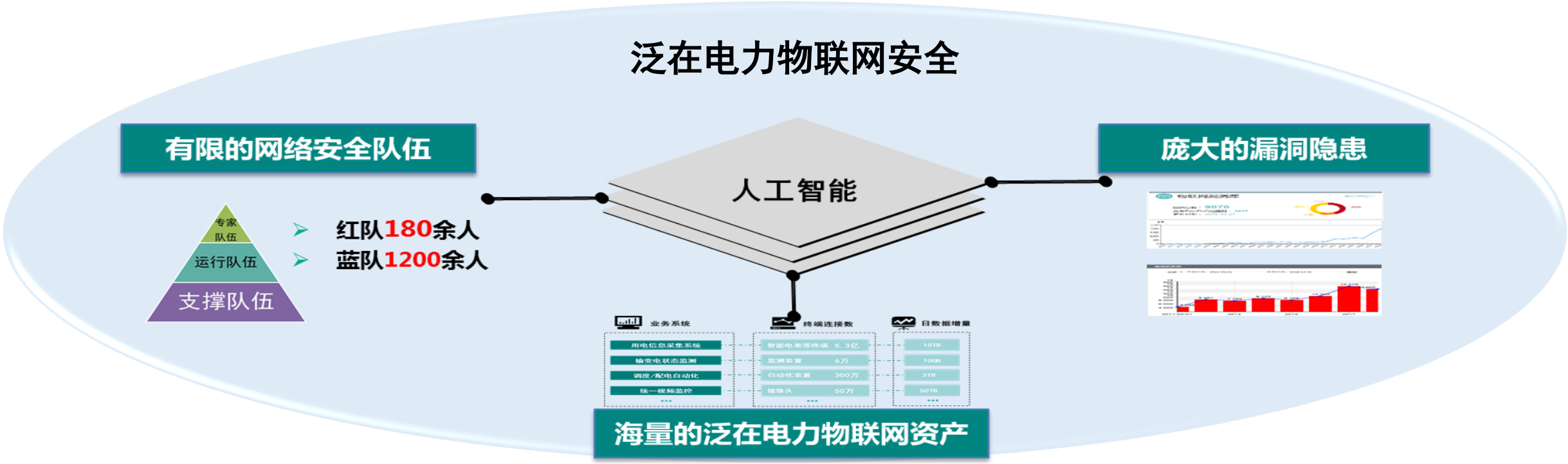
报告提纲

contents

泛在电力物联网安全防护关键技术

严监管—智能化的安全监管

- “聪者听于无声，明者见于未形”。感知网络安全态势是最基本最基础的工作。但面对**海量的**泛在电力物联网资产、**庞大的**漏洞隐患，凭人力已无法处置海量告警，**亟需引入人工智能技术**，以**提高攻防效率、降低安全成本、促进攻防经验固化**，从而有效保障泛在电力物联网安全。



泛在电力物联网安全防护关键技术

严监管——智能化的安全监管

- 打造网络安全事件的**统一监测、预警与通报体系**，建设**网络与信息安全风险监控预警平台**，实现对安全事件的集中预警、分析、处置。应用数据挖掘、深度学习等技术，建立多项安全分析场景，从全局视角提升网络安全威胁的识别、分析到处置的智能化水平。

态势感知

知己知彼，百战不殆

监测主题

围绕场景，重点突破

主要功能

智能检测	广泛应用外部威胁情报，增强安全设备检测能力。
智能分析	安全日志自动化分析，网络安全态势预测。
智能处置	WAF、防火墙安全告警、处置的自动化联动响应。

安全资产看得见、安全风险看得准、安全威胁看得深

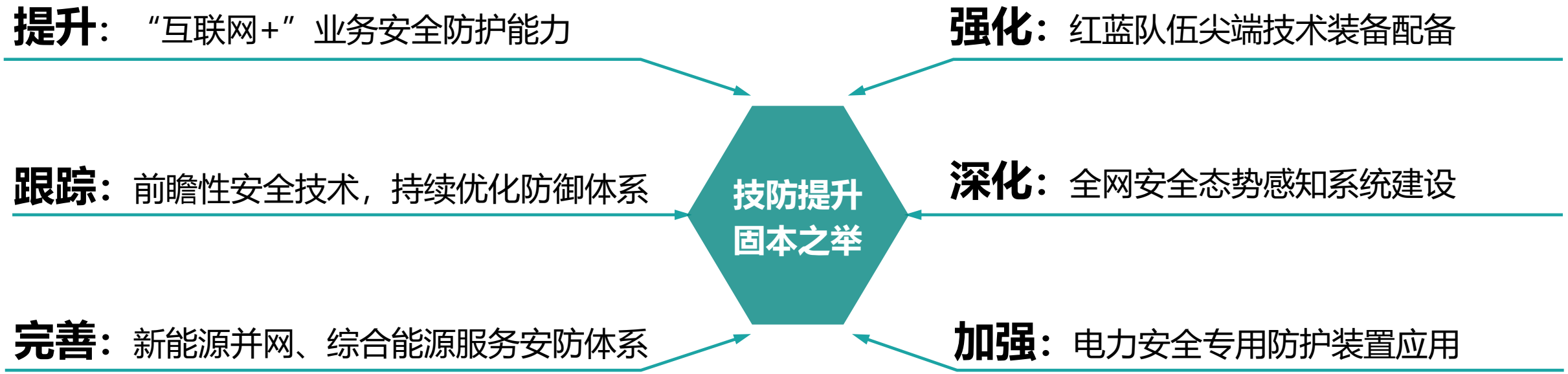
目 录

报告提纲

contents

不断提升安全技术防护能力和水平是确保网络安全长治久安的固本之举

随着能源互联网和泛在电力物联网建设深入开展，以及“大云物移智链”等新技术的应用，电力/能源用户将不断增加、网络边界不断扩大。不断**提升网络安全技防水平**，**加强技术管控**，是确保网络安全长治久安的**固本之举**。



谢　谢!