2018年
中国城市规划信息化年会

新时代、新智慧、新安全

360企业安全集团/大区总经理/夏伟

2018年8月

2018年
中国城市规划信息化年会

PART / 01

新时代-从数字中国到智慧社会

新时代

人民日益增长的美好生活需要和不平衡不充分的发展之间的矛盾

新课题

- 变化：由“人与社会实体的集合”向“真实空间与虚拟空间的集合”转变
- 目标： 数字中国　智慧社会　国家安全
- 战略：　大数据　人工智能　网络安全

- IT技术将改变三大格局：经济格局、利益格局、安全格局
- 社会治理模式3个转变：
  - ✓ 从单向管理转向双向互动
  - ✓ 从线下转向线上线下融合
  - ✓ 从单纯的政府监管向更加注重社会协同治理转变

- 建设智慧城市，推动三融合和五跨
  - ✓ 技术融合、业务融合、数据融合
  - ✓ 跨层级、跨地域、跨系统、跨部门、跨业务、的协同管理和服务

- 三期叠加：战略机遇期、起步探索期、创新发展期

新导向

智慧城市不仅要使实体空间信息化，而且还要在信息网空间中重塑一个更好的更智能化管理和服务的城市。因此智慧城市的水平不仅取决于虚拟世界信息化的水平，还有人的平均素质、物质世界的合理规划管理水平。

过去9年过度的用信息化的概念对传统城市进行所谓的信息化提升，并没有决绝智慧城市核心的内涵所在。2016年底，国家发改委会同网信办、国家标委，开展新型智慧城市评价工作。

【新型智慧城市评价标准】

新型智慧城市评价分为成效类指标、引导性指标、市民体验指标三大类：

成效类指标：惠民服务【37%】

精准治理【9%】

生态宜居【8%】

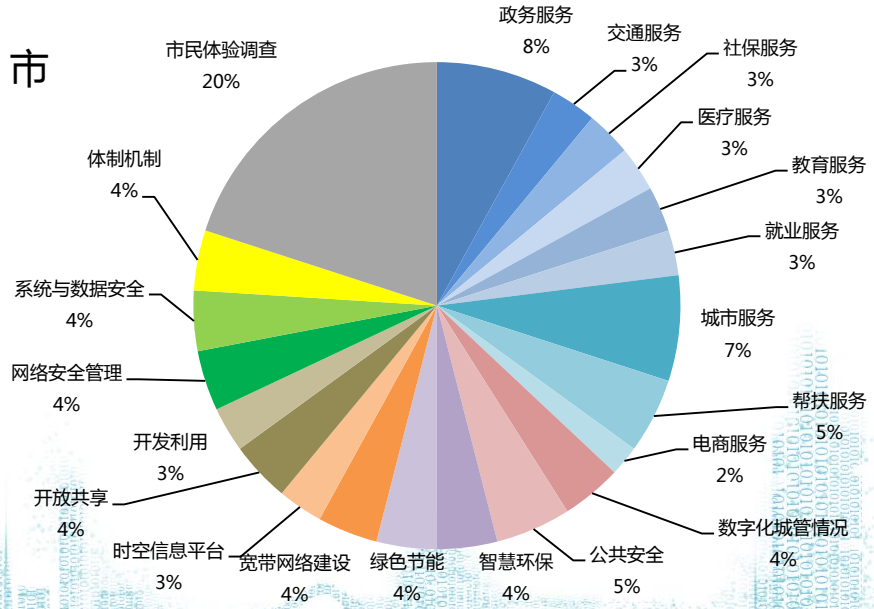
引导性指标：智能设施【7%】

信息资源【7%】

网络安全【8%】

改革创新【4%】

市民体验类指标：市民体验【20%】



2018年
中国城市规划信息化年会

PART / 02

新智慧-理想智慧城市架构蓝图

智慧城市理想图

政务服务
交通服务
社保服务
医疗服务
教育服务
就业服务
城市服务
帮扶服务
电商服务
城市管理
公共安全
环保节能
……

国内智慧城市建设的主流技术模型

智慧应用层安全威胁

- 网站内容被篡改
- 0day漏洞
- 钓鱼网站
- 僵尸网络攻击
- 木马攻击
- 蠕虫攻击
- 病毒攻击
- ……

网络通信层安全威胁

- 物理攻击
- 网关节点捕获
- 普通节点捕获
- 传输截获
- 传输窃听
- 传输篡改
- 传输伪造
- DDoS攻击
- 重放攻击
- 完整性攻击
- Sinkhole黑洞攻击
- Wormholes虫洞攻击
- HelloFlood攻击
- ……

数据及服务支撑层安全威胁

- 大数据成为网络攻击的显著目标
- 大数据加大隐私泄露风险
- 大数据技术被应用到攻击手段中
- 高级持续攻击APT
- ……

计算与存储层安全威胁

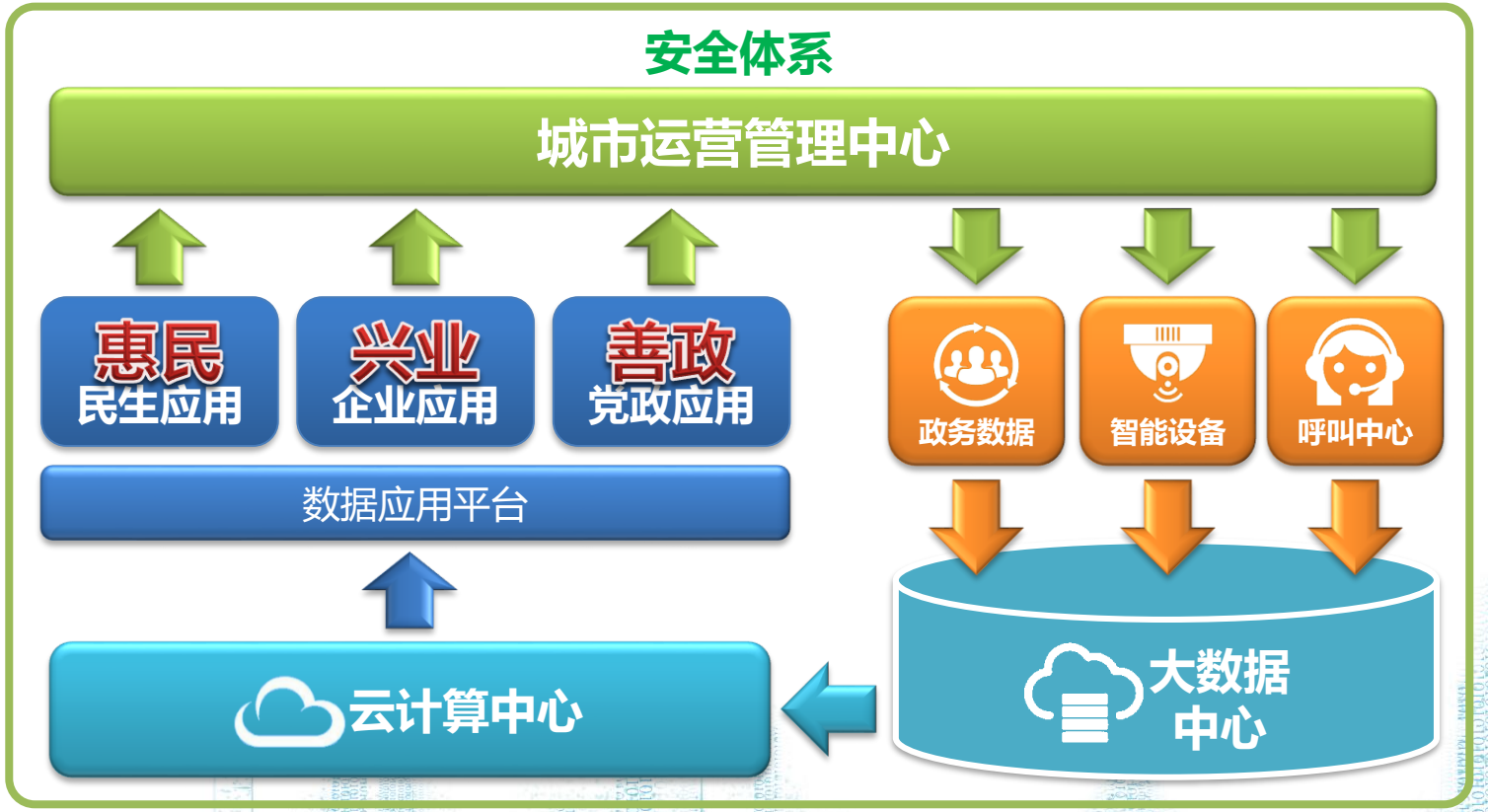
- 物理破坏攻击
- 物理灾难风险
- 存储和安防架构风险
- 敏感数据泄露
- 恶意数据注入
- ……

物联感知层安全威胁

- 感知设备被攻击
- 执行设备被攻击
- 伪基站攻击
- ……

来源：国家智慧城市标准化总体组《中国智慧城市标准化研究报告》

智慧城市的基本架构


安全体系
城市运营管理中心
惠民
民生应用
兴业
企业应用
善政
党政应用
政务数据
智能设备
呼叫中心
数据应用平台
云计算中心
大数据
中心

2018年
中国城市规划信息化年会

PART / 03

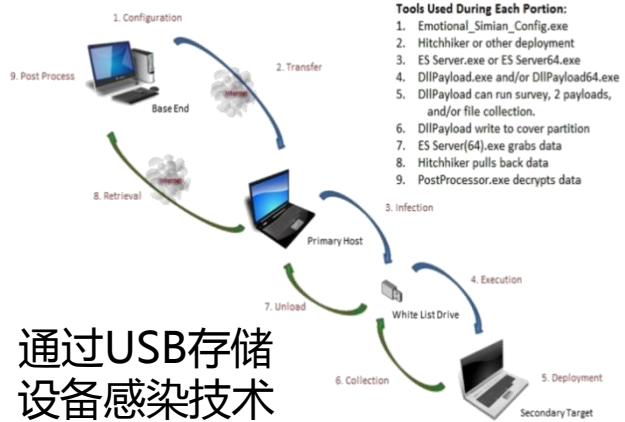
新安全-大、智、移、云时代智慧城市的安全之道

便捷还是安全，这是一个值得考虑的问题

政府现有大数据真有想象的那么重要吗

- 人际探真雷达：社交分析与渗透系统

脑洞大开的各类攻击



通过USB存储设备感染技术攻击安全隔离网络

接口设备+射频照射回收数据攻击

Apple, Cisco, Dell, Juniper, Maxtor, Seagate, Western Digital, HUAWEI

未说明这些公司是否协助了这些工具的开发

如果我们的城市真的智慧了？

- 水
- 电
- 燃气
- 交通
- 医疗
- ……

“护网2016/2017”行动

- 「行动主体」：公安部主办/360公司承办
- 「行动目标」：国内民航系统和国家电网
- 「行动描述」：实网攻击演习
- 「持续时间」：两周

突破了某航空单位和某机场的内网安全防护，直接控制了离港调度系统，可扰乱某机场离港航班次序，并可获取所有民航购票数据。

渗透进入某省电力公司物理隔离的内网系统，控制了该省电网的域名解析系统，可以劫持所有网络通信，获取包括密码等各类信息。

1. 某租车几乎全部沦陷-邮件服务器、GPS定位系统
2. 中国某保险几乎全部沦陷,运维服务器/内网路由权限
3. 中国国家某局若干业务的Web网站权限
4. 中国某科研单位文献中心若干业务的Web网站权限
5. 某教育考试院 任意文件下载漏洞等
6. 某自来水集团节水平台若干注入等

管理者与全民的安全意识还远远不够

- 新型智慧城市要着力补齐五大短板
  - 改革创新的短板
  - 发展实效的短板
  - 区域差异的短板
  - 长效运营的短板
  - 网络安全的短板

- 企业：重业务，轻安全
- 政府：安全看不见，难以出政绩
- 民众：复杂的技术与便捷的功能将安全隐患封装

智慧城市的网络安全体系是否完善？

智慧城市网络空间安全保障体系的完善直接关系到安全的投入是否能够达到预期的效果，安保体系的覆盖同样适用于“木桶理论”，最短的一块板子决定着安全的水平。

安全 = （技术 + 管理）× 执行效率

智慧城市的网络安全体系是否完善？

多角度感知智慧城市网络空间安全

安全视角1 - 已知威胁

1

安全体系是否对目前已知的可能发生的安全威胁风险做好了充分的准备，以达到系统的基础安全目标。

已知威胁

安全视角2 - 高级威胁

2

安全体系是否可自动感知可能带来安全风险的内外部异常事件（如APT）并告警处理。

高级威胁

安全视角3 - 善意假定

3

假定系统的使用人员均为善意“好人”，安全体系提供的管控方案是否完善并严格执行。

安全视角4 - 恶意假定

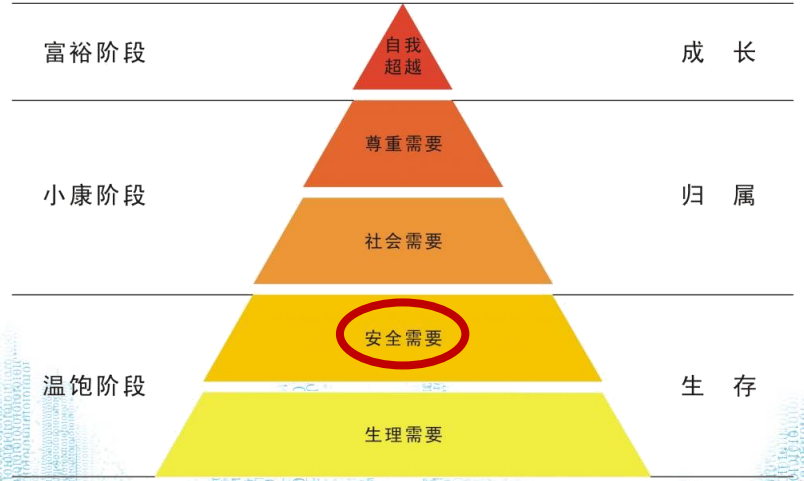
4

假定系统的使用人员均为恶意“坏人”，安全体系提供的管控方案是否存在漏洞，应急是否完备。

新型智慧城市网络空间安全愿景

新型智慧城市的建设核心是利用信息技术更好的满足市民在城市生活中的各方面需求，根据马斯洛人类需求层次理论，任何高阶需求的基础都是安全需求，因此新型智慧城市网络空间安全愿景应该是：

构建新型智慧城市网络空间安全感



安全是政治

2016.4.19讲话：树立正确的网络安全观：网络安全是整体的而不是割裂的，是动态的而不是静态的，是开放的而不是封闭的，是相对的而不是绝对的，是共同的而不是孤立的。那种依靠装几个安全设备和安全软件就想永保安全的想法已不合时宜，需要树立动态、综合的防护理念。

2018.4.20讲话：**没有网络安全就没有国家安全**，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。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，加强网络安全信息统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设**，积极发展网络安全产业，**做到关口前移，防患于未然**。要落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任，主管部门履行好监管责任

安全是法律：《中华人民共和国网络安全法》

2017.6.1实施《中华人民共和国网络安全法》，全面依法治国的决心，共7章79条

指导思想 - 安全滑动窗口模型

指导思想 - Gartner自适应安全体系框架

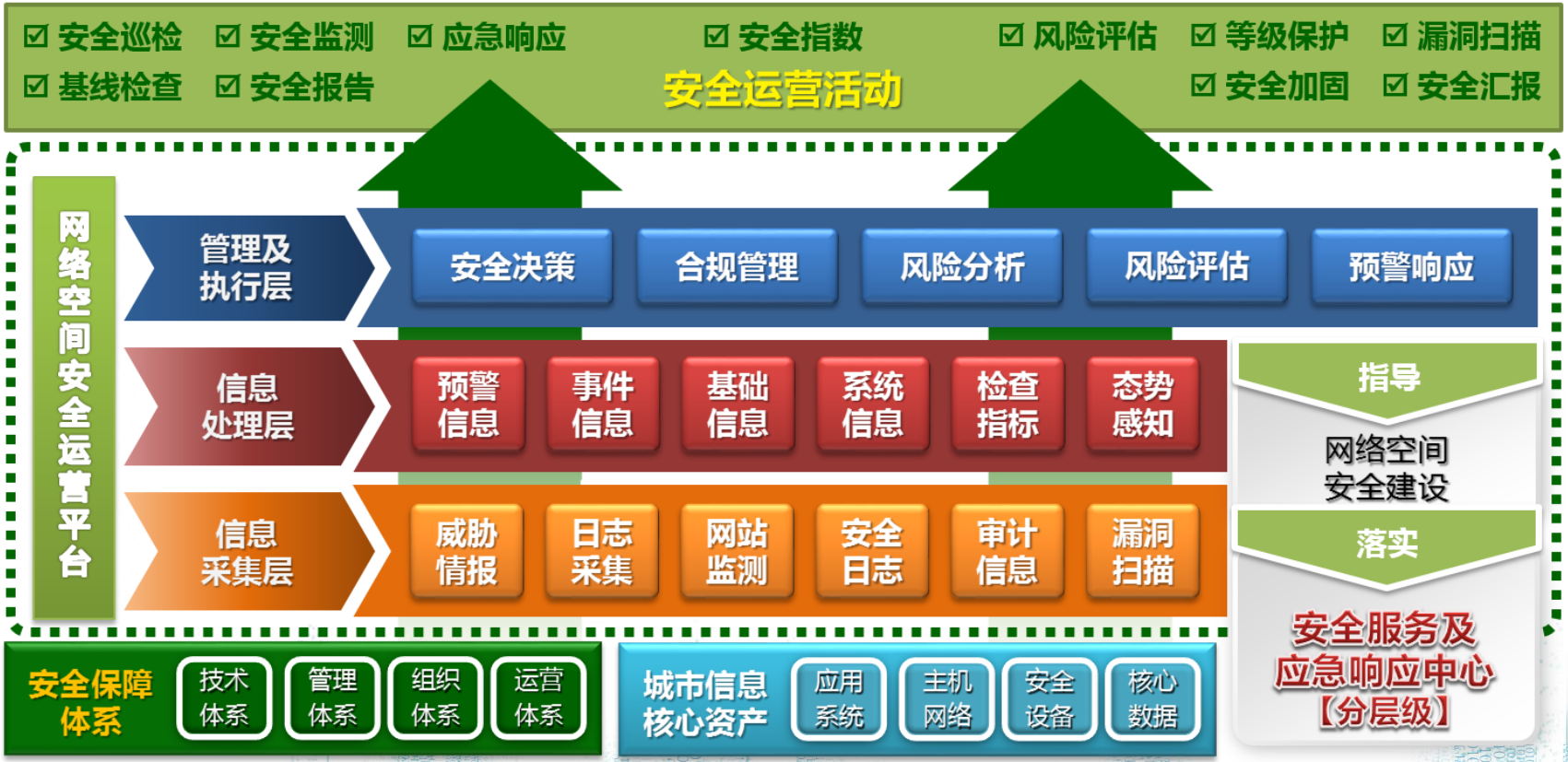
新时代 新战略 新探索

分层级重点保护

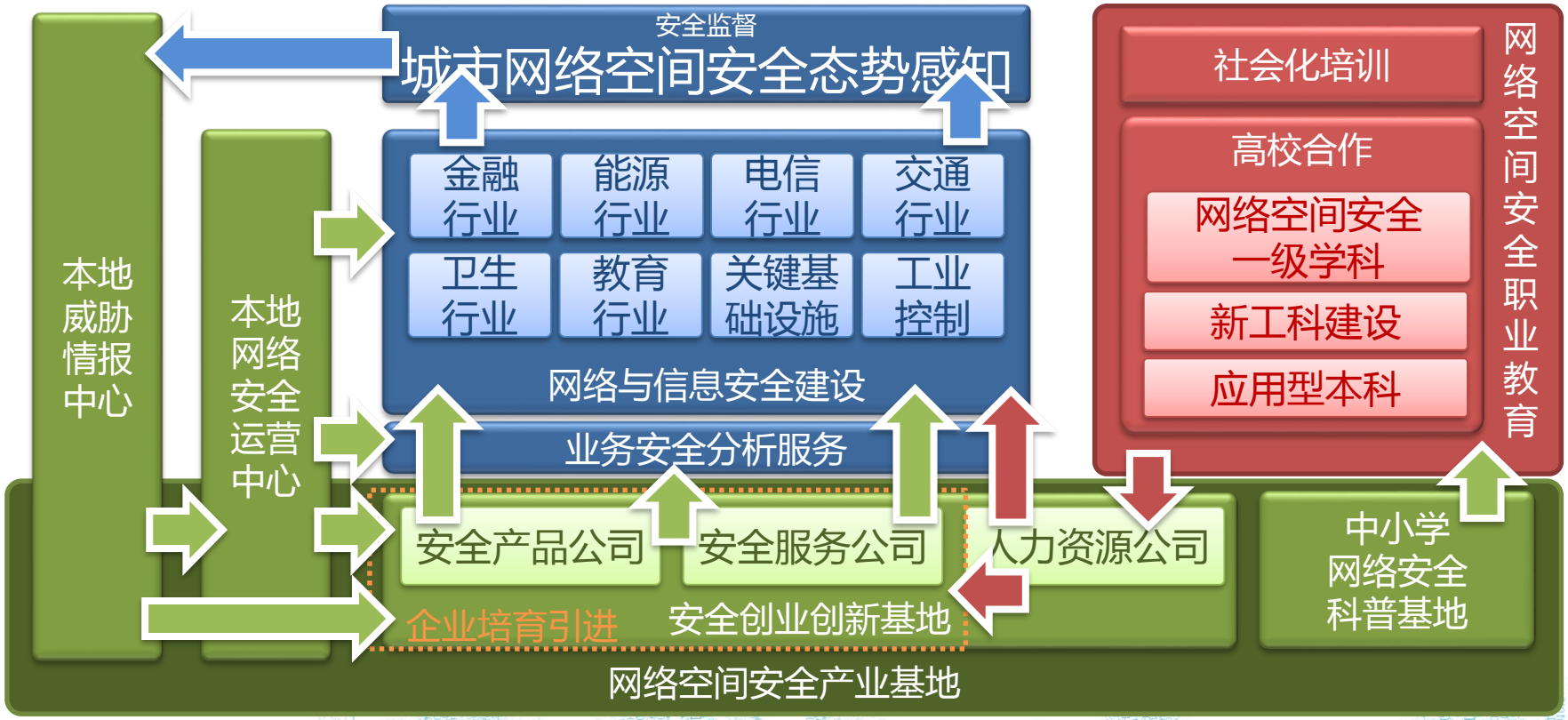

形成免疫平衡体系
安全体系
城市运营管理中心
惠民
民生应用
兴业
企业应用
善政
党政应用
政务数据
智能设备
呼叫中心
常保健
勤体检
数据应用平台
防脑瘫
防心梗
云计算中心
大数据中心

智慧城市安全运营中心

新时代 新战略 新探索



智慧安全运营中心产业闭环

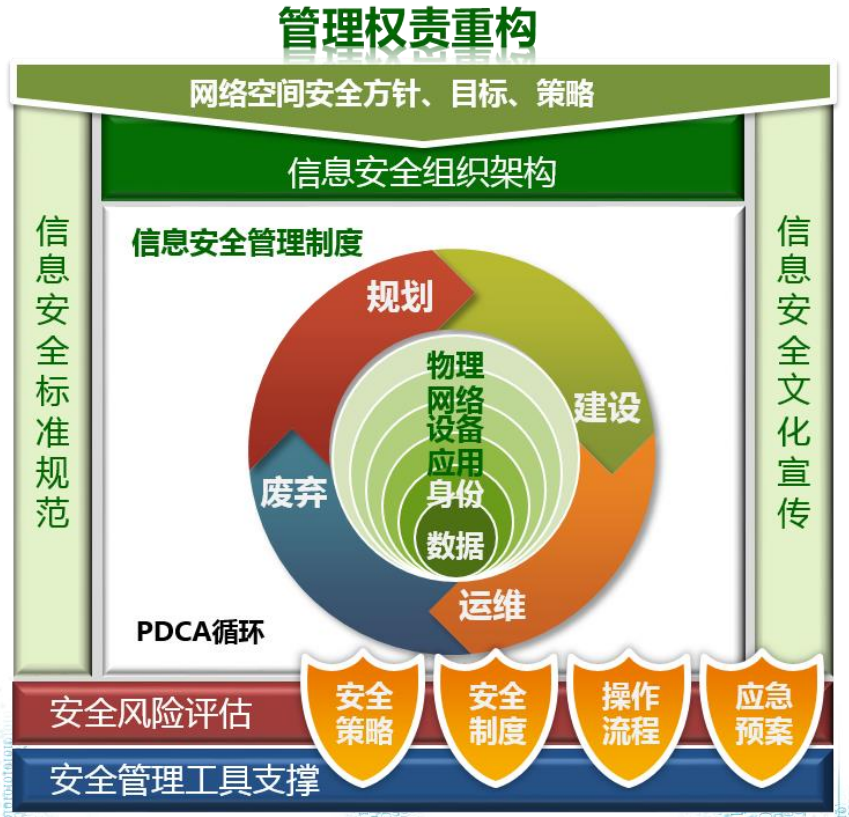


内容安全与技术安全分离

请专业的人做专业的事

重构政务管理模型


组织结构重构
决策层
管理层
执行层
监督层


管理权责重构
网络空间安全方针、目标、策略
信息安全组织架构
信息安全管理制度
信息安全标准规范
信息安全文化宣传
规划
建设
运维
废弃
物理
网络
设备
应用
身份
数据
PDCA循环
安全风险评估
安全管理工具支撑
安全策略
安全制度
操作流程
应急预案

构建智慧城市的“免疫平衡体系”

- **广泛宣传，**【尽快提升体系内外网络空间安全意识】
- **安全第一，**【信息化建设过程中全面考虑安全风险】
- **防患未然，**【通过数据分析构建风险态势感知能力】
- **亡羊补牢，**【事件发生后及时补强避免进一步损失】
- **釜底抽薪，**【借助专业公司安全服务实时应急响应】
- **厚积薄发，**【大力培养网络空间安全人才支撑产业】

南平市城市安全运营中心

新时代 新战略 新探索

南平市延平区城市安全运营中心基于威胁情报的“网络空间安全综合运营管理中心”与本地已建成信息系统联动，通过中心的第一阶段建设完成**“网络空间安全态势可见+部分可管”**目标，并根据具体业务需求深入建设运营管理中心，以期达到**“网络空间安全可管、可控”**目标，随着安全经验与数据的积累，逐步实现安全态势**可预测**的最高目标。

近期目标	短期目标	中期目标	长期目标
信息安全态势 可见	信息安全态势 可管	信息风险工作 可控	信息安全态势 可预

主管部门

南平市延平区委、区政府

建设运营模式

南平市延平区城市安全运营中心由延平区国有资产运营公司出资建设，由360企业安全集团负责总体建设和运营。

运营服务内容

城市公共网络安全态势感知、公共特殊业务监测、大数据安全追踪溯源、城市网络安全漏洞预警、通信指挥、政务终端安全、安全移动政务办公、政务邮件安全、安全代码审计、大数据治理平台运营。

城市网络安全运营中心

一带一路峰会网络安全重保

“一带一路”国际合作高峰论坛于2017年5月14日至15日在北京举行，公安部和北京市外办进行了峰会网络安全重保

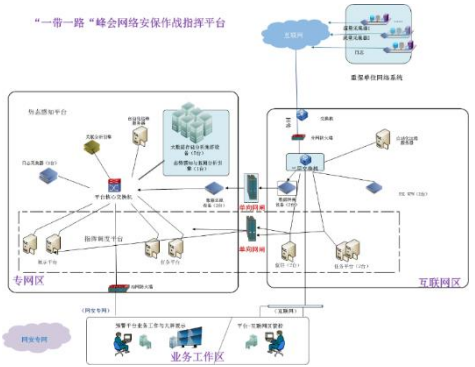
威胁预测：基于大数据的安全预警

实时防御：纵深防御体系

分析检测：持续监测与数据分析

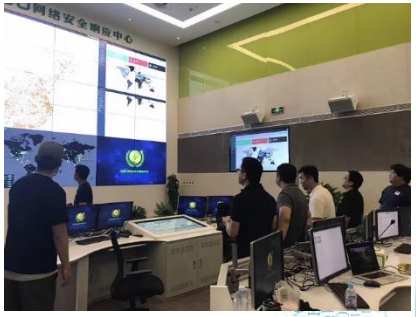
应急响应：专家应急响应及处置

APT攻击检测与安全大数据威胁情报相结合进行预警



纵深防御体系化保障，降低受攻击面，实现“攻击减速”

可视化监测、大屏实时展示



专家型应急响应及处置

360网络空间安全保障能力

新时代 新战略 新探索

获得威胁情报借助人民战争的力量

新时代 新战略 新探索

全球文件样本库
- -每天新增900万样本
- -总样本数145亿+
- -20亿+黑名单
- -1亿+白名单

最全的样本行为库
- -总日志数18.9万亿条
- -每天新增380亿条

最大的存活网址库
- 每天查询300亿条
- 每天处理100亿条
- 每天拦截访问钓鱼数超过1.4亿URL

全球域名信息库
- -90亿DNS解析记录
- -每天约新增100万条
- -13年+Whois信息存储
- -占中国30%DNS解析与查询记录

- 数据来源：全球**6.3亿PC**安全客户端，**8.2亿移动**端安全客户端；360浏览器、搜索终端应等
- 数据来源：互联网基础设施DNS，猎网、补天等各类举报与响应平台，以及 **100+第三方**数据源
- 大数据服务器规模超过**60000台**，总存储数据量接近**1.3EB**，每天新增超过**1.5PB**
- 每天各种数据计算任务**10万个**，每天处理数据量**10PB**

互联网痕迹大数据

攻击武器大数据

享誉全球的十五大安全研究团队

新时代 新战略 新探索

360
Vulcan Team
伏尔甘团队

360
QVM Team
QVM团队

360
Helios Team
追日团队

360
Vulpecker Team
威派克团队

360
Nirvan Team
涅磐团队

360
Alpha Team
阿尔法团队

360
Sky-Go Team
天行者团队

360
Marvel Team
Marvel团队

360
Unicorn Team
独角兽团队

360
Corpsec Team
安全服务团队

360
CORE Team
CORE团队

360
Okee Team
Okee团队

360
QEX Team
QEX团队

360
Gear Team
Gear团队

360
Codesafe Team
代码卫士团队

独步全球的安全技术研究能力

519

漏洞致谢519次

2017年，360安全创新中心共荣获微软、谷歌、苹果、Adobe、Vmware、华为等全球顶级组织漏洞报告致谢519次，排名全球第一。

总冠军

破解大师总冠军

世界黑客大赛Pwn2Own 2017：360获世界破解大师总冠军奖杯。

20

20 次夺冠

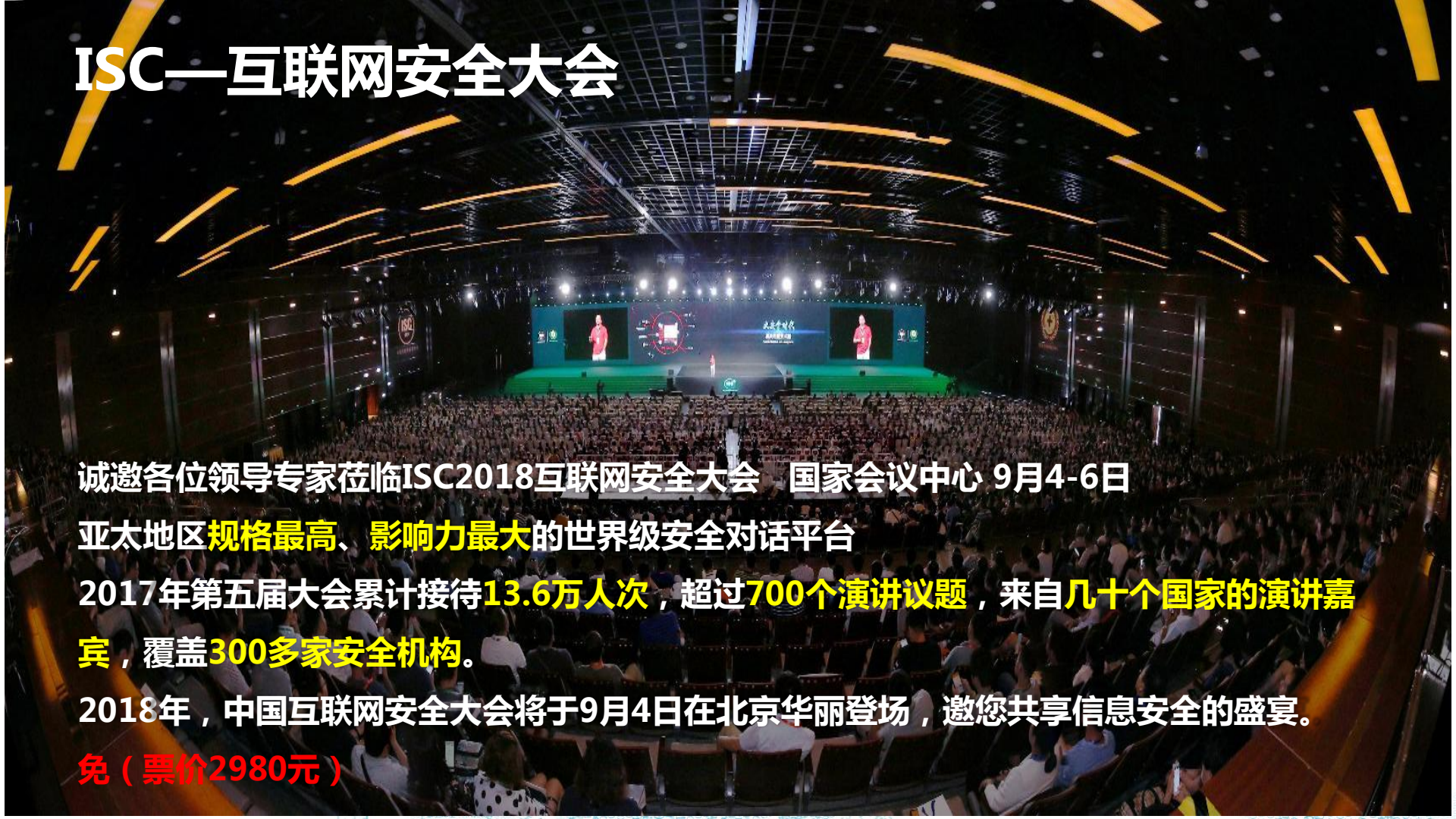
2015-2017，360安全创新中心在世界黑客大赛中20次夺冠并创造多项历史。

10

10人上榜

微软TOP100安全贡献榜中，360有**十人上榜**，其中七人排名前50，成为入选人数最多、综合排名最高的安全厂商。

ISC—互联网安全大会



诚邀各位领导专家莅临ISC2018互联网安全大会　国家会议中心 9月4-6日

亚太地区**规格最高、影响力最大**的世界级安全对话平台

2017年第五届大会累计接待**13.6万人次**，超过**700个演讲议题**，来自**几十个国家的演讲嘉宾**，覆盖**300多家安全机构**。

2018年，中国互联网安全大会将于9月4日在北京华丽登场，邀您共享信息安全的盛宴。

免（票价2980元）

2018年
中国城市规划信息化年会

THANKS