ISC 2019 第七届互联网安全大会

新挑战、新架构、新应对

杨斌

天融信科技集团高级副总裁

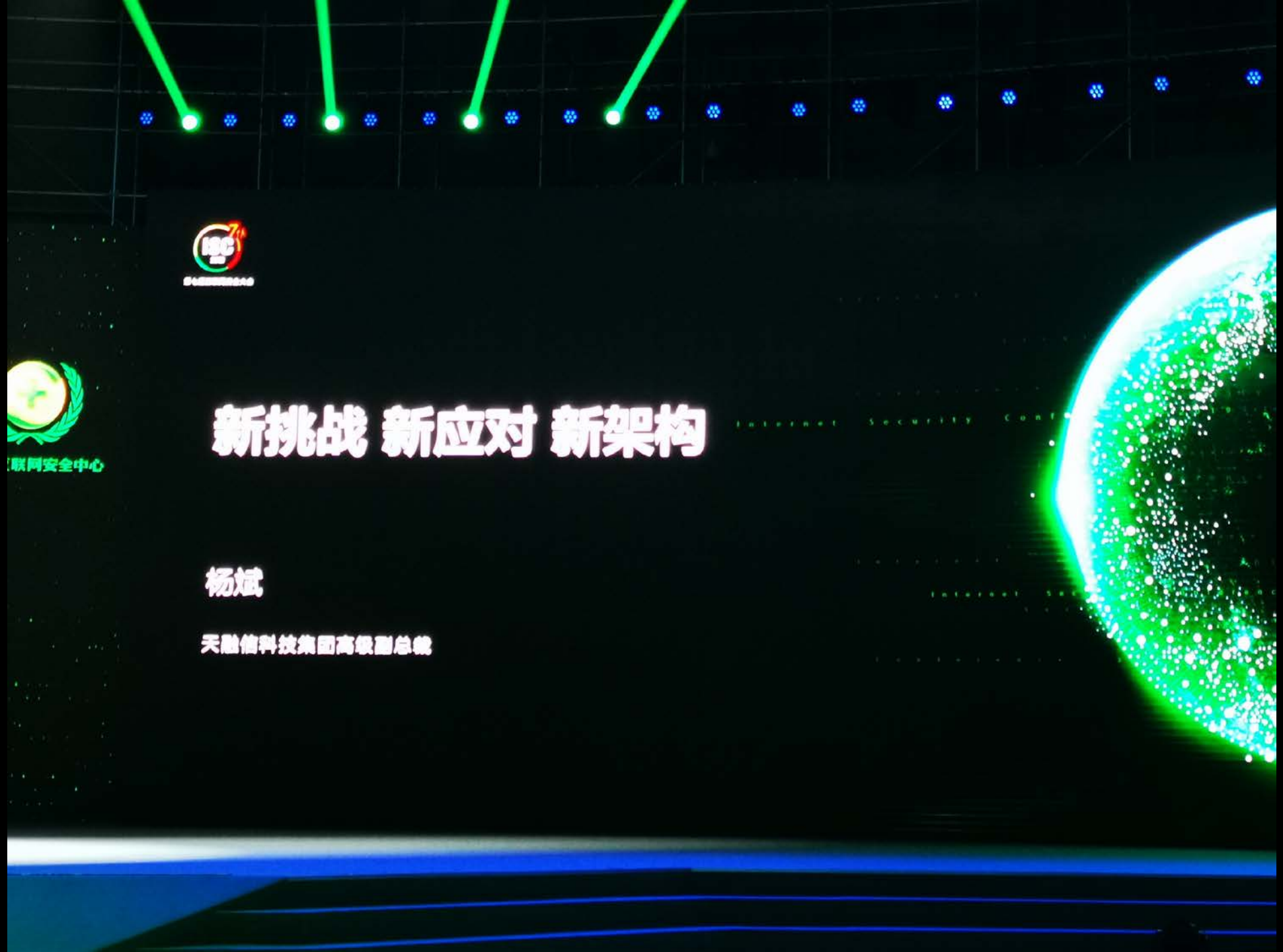
小鹅助理

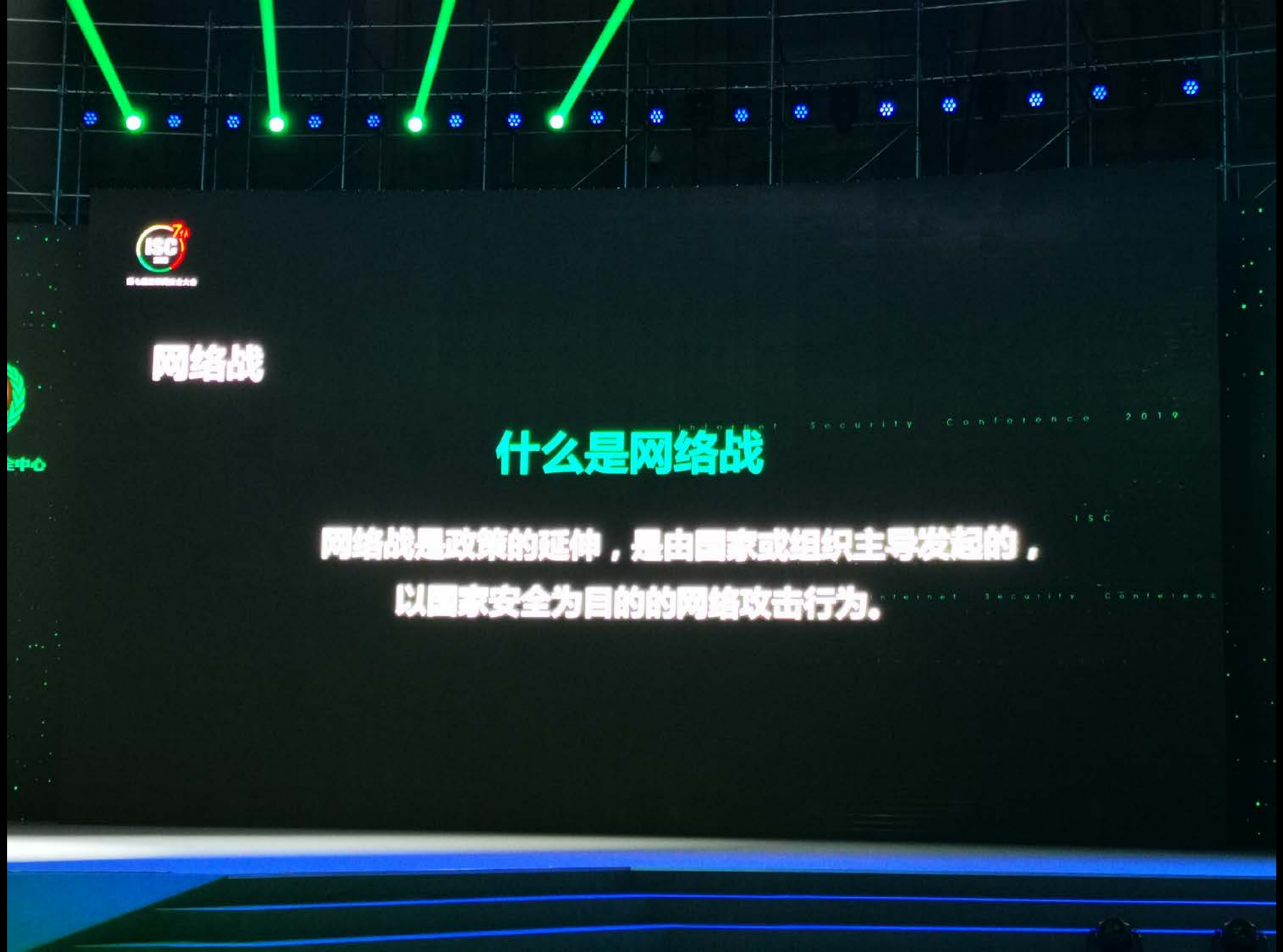
扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费

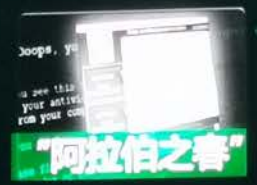
门票


杨斌
Yang Bin
天融信科技集团 高级副总裁
Senior Vice President, Topsec Technologies Group Inc.


联网安全中心
新挑战 新应对 新架构
杨斌
天融信科技集团高级副总裁


网络战
什么是网络战
网络战是政策的延伸，是由国家或组织主导发起的，
以国家安全为目的的网络攻击行为。

网络战



网络空间已经逐步发展成为继陆、海、空、天之后的 **第五大战略空间**

互联网安全中心

网络战的特点

破坏力、影响力巨大

关乎民生、危及国家安全，会对国际政治产生重大影响

攻击手段多样化

定制化的攻击方案，综合运用社会工程学、供应链缺陷、木马等

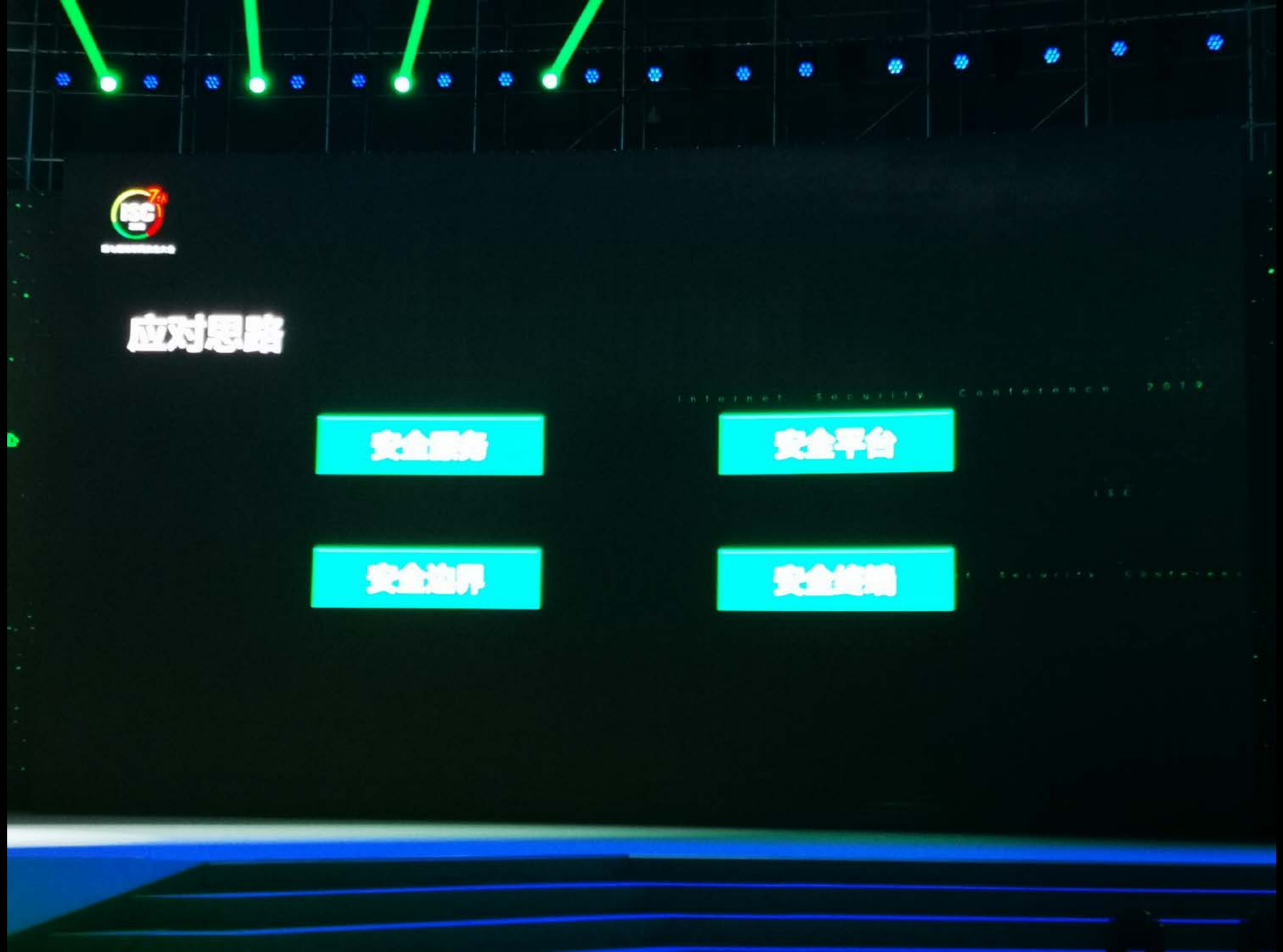
隐蔽性高

一般采用0日攻击，未知恶意代码攻击、高级逃逸伪装，很难在前期发现

潜伏时间长

从入侵成功，到产生破坏，可进行长时间潜伏


网络战为何难以应对
技术上无法彻底解决
设计缺陷无法避免
产业链缺陷无法避免
现有漏洞无法彻查
人为因素难以防范
社工手段隐患
内部人员隐患
管理人员隐患
防护成本高
人才培养周期长
技术创新投入大
收益不明显
防护力量不集中
各自为阵
重复投入
缺乏体系


应对思路
安全服务
安全平台
安全运营
安全检测


新应对——终端安全传统篇
终端往往是攻击程序运行的最终载体，终端安全是网络安全防御的重要一环。
分类
传统终端、虚拟终端、
移动终端、工业终端、
物联网终端...
威胁
非法接入、恶意程序、
系统漏洞、数据泄漏...
防御
终端杀毒、
主机监控、外设管控、
EMM移动终端管理...
感知安全风险是终端安全的重点


新应对——终端安全挑战篇
工业终端防护
环境脆弱
业务连续性
物联网终端防护
部署分散
缺乏认证
主机白名单
虚拟补丁
身份唯一标识
终端安全新技术
EDR
检测
响应
行为检测
威胁情报
威胁捕获
终端具备完整安全数据
协同终端和安全平台

新应对——边界安全篇

不同安全级别的网络环境相连接，就产生了网络边界，防止来自网络外界的入侵就要在网络边界上建立可靠的安全防御措施。

入侵检测、木马检测、
APT检测、网络审计...

访问控制、拓扑隐藏、
入侵防御、Web防护...

边界安全防护是在不同网络环境之间部署多种的综合安全防御措施


ISC
2018
第七届互联网安全大会
新应对——边界安全挑战篇
安全检测
新应对
新挑战
新应对
安全防护
恶意代码检测
隐蔽通道检测
加密流量检测
被动检测
+
主动探测
网络攻击手段武器化
未知漏洞后门风险
网络流量加密传输
静态防护
+
动态防护
拟态防御
行为基线
动态防护
协同——边界 安全平台：实时上报安全数据，动态执行安全策略

新应对——安全平台篇

- 数据收集：网络资产安全探测
- 数据收集：终端检测防护系统
- 数据收集：网络行为检测系统
- 数据处理：数据预处理及存储
- 数据分析：资产画像关联情报
- 数据分析：攻击检测综合判定
- 数据展示：可视化建模展示
- 通报预警：安全事件信息通报
- **快速处置：动态下发安全策略**

安全节点定位管理

安全态势全网感知

威胁情报关联分析

安全事件综合判定

安全策略动态下发

协同——安全平台 边界 终端：实时分析安全数据，动态下发安全策略

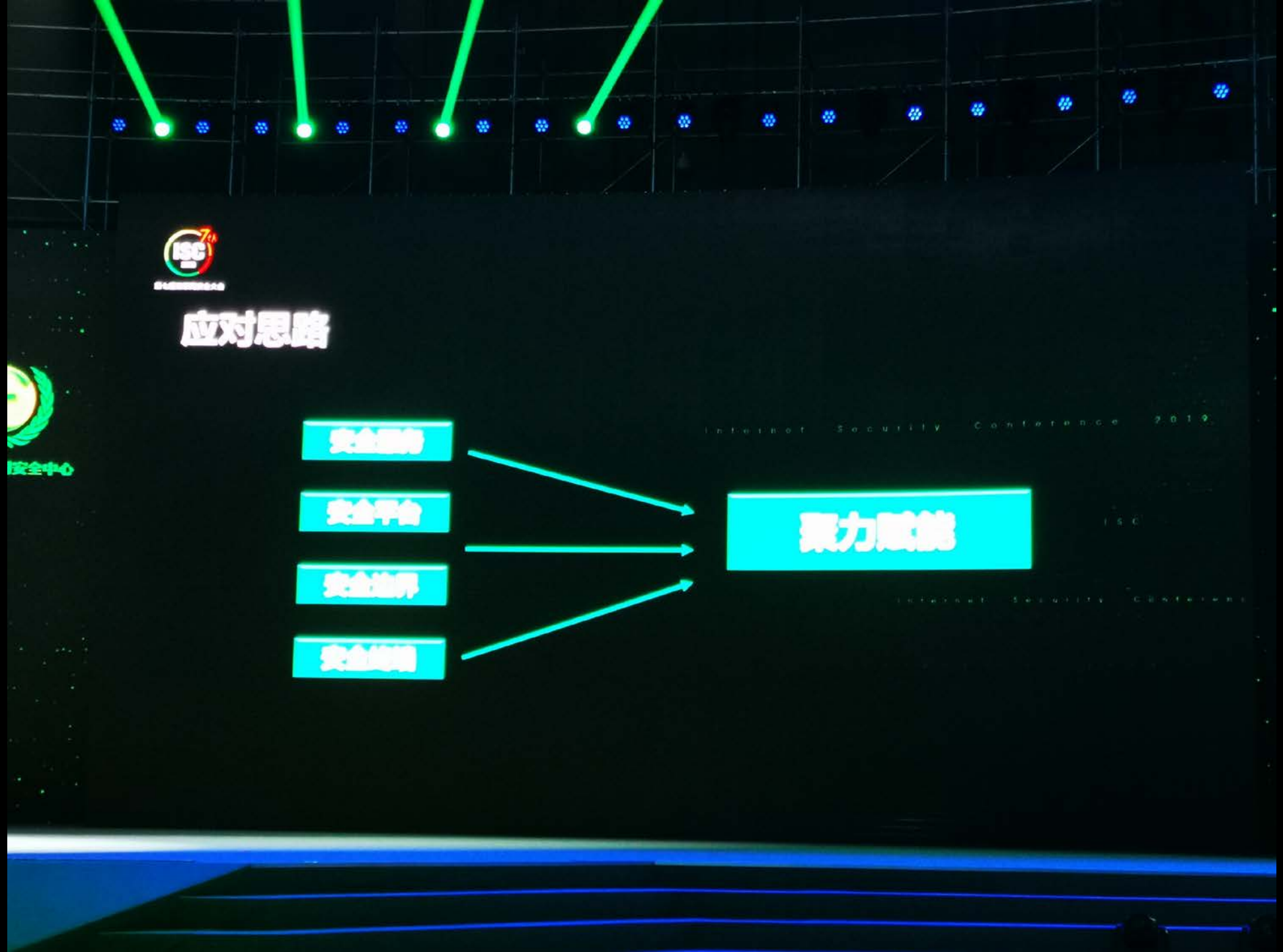
新应对——安全服务篇

- 安全平台需要人工干预
- 设备不能解决所有问题
- 人才是网络安全的核心
- 国外安服投入高于国内
- 安全培训赋能势在必行

7×24小时实时监测

攻击前（事前预防）	攻击中（事中监测）	攻击后（事后优化）
识别目标 掌握弱点 情报监测 加强意识 提升能力 服务团队	实时监测 攻击预警 应急处置 安全运维 服务团队	溯源取证 威胁处置 安全培训 服务团队
资产梳理（风险探知）	应急响应服务（安全运维）	安全培训服务
威胁情报（推送数据）	网站监测分析（网站监测）	日志分析服务
其他产品和服务	其他产品和服务	其他产品和服务

全生命周期应急响应与处置


应对思路
Internet Security Conference 2019
安全中心
安全平台
ISC

新架构——天融信NGTNA

NGTNA——下一代可信网络安全架构

- 全面感知为基础
- 动态防护为理念
- 智能协同为核心
- 聚力赋能为目标

小鹅助理

谢谢！

扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费门票