ISC 2019 第七届互联网安全大会

网络战时代的挑战与应对

周鸿祎

360集团董事长兼CEO

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

周鸿祎
Zhou Hongyi

ISC大会主席 360集团董事长兼CEO
Chairman of ISC
Chairman and CEO of the 360 Group


网络战时代的挑战与应对
周鸿祎
ISC大会主席 360集团董事长兼CEO


ISC 2019
第七届互联网安全大会
360万联网安全中心
2019事件回顾
APT34组织网络武器库被曝光
12家中国机构 位列被攻击名单,覆盖金融、电信、能源、交通、制造领域
链接地址
域名
地区
行业
https://122.146.71.136/owa/auth/error3.aspx
mail.talfo.com.tw
中国台湾
电信
https://59.124.43.229/owa/auth/error0.aspx
tgpf.org.tw
中国台湾
NPO
https://1.202.179.13/owa/auth/error1.aspx
mail.cecep.cn
中国大陆
能源
https://1.202.179.14/owa/auth/error1.aspx
mail.cecep.cn
中国大陆
能源
https://114.255.190.1/owa/auth/error1.aspx
mail.generali-china.cn
中国大陆
金融
https://180.166.27.217/owa/auth/error3.aspx
exchange.bestv.com.cn
中国大陆
媒体
https://180.169.13.230/owa/auth/error1.aspx
bdo.com.cn
中国大陆
能源
https://210.22.172.26/owa/auth/error1.aspx
lswebext.sdec.com.cn
中国大陆
能源
https://221.5.148.230/owa/auth/outlook.aspx
mail.swsc.com.cn
中国大陆
金融
https://222.178.70.8/owa/auth/outlook.aspx
mail.swsc.com
中国大陆
金融
https://222.66.8.76/owa/auth/error1.aspx
lswebext.sdec.
中国大陆
能源
https://58.210.216.113/owa/auth/error1.aspx
mail.neway.c
中国大陆
制造
https://60.247.31.237/owa/auth/error3.aspx
c
中国大陆
交通
https://60.247.31.237/owa/auth/logoff.aspx
cr
中国大陆
交通
https://202.175.114.11/owa/auth/error1.aspx
webmail.n
中国澳门
电信
https://202.175.31.141/owa/auth/error3.aspx
exchange
中国澳门
教育


2019事件回顾
俄罗斯
6.17
纽约时报称俄罗斯电网被植入后门
3.17
委内瑞拉大规模停电
委内瑞拉
巴西
智利
乌拉圭
阿根廷
6.17
针对关键基础设施的潜伏与攻击频繁


2019事件回顾
资料
伊朗击落美无人机 紧张局势再度升级-美媒
美军已发起对伊朗的网络攻击
6月20日，美网军对伊朗发动准军事行动，通过网络攻击破坏了伊朗的导弹控制系统
美伊网络安全攻击“你来我往”
7月13日，纽约突发大面积停电，美军方声称遭到了来自伊朗革命卫队信息
的打击，后又辟谣。
NEW YORK POWER BLACKOUT; DID IRAN DID PERFORMED A COUNTER CYBERATTACK?
Share this...
Last Saturday night, a blackout in New York left the entire Manhattan area without electric power; interestingly, the incident occurred on the anniversary of the massive blackout that happened in 1977 that left the entire city without power, crippling traffic and all work, academic and domestic activities, network security specialists report.

2019事件回顾

北约举行全球最大网络安全演习“锁盾2019”应对网络战

多国参与，协同作战

多达25个国家、1200名专家参与

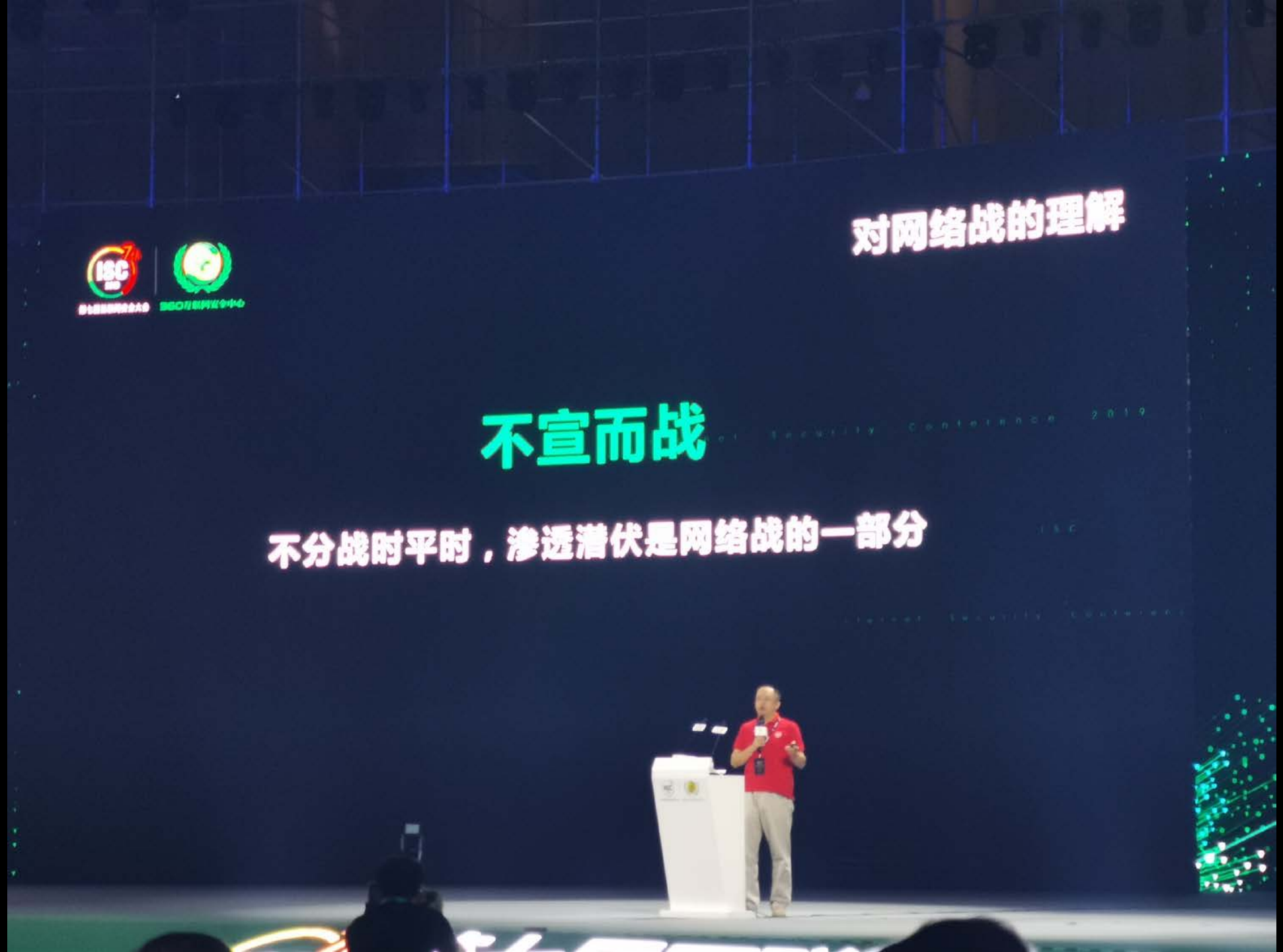
军事环境，实战演练

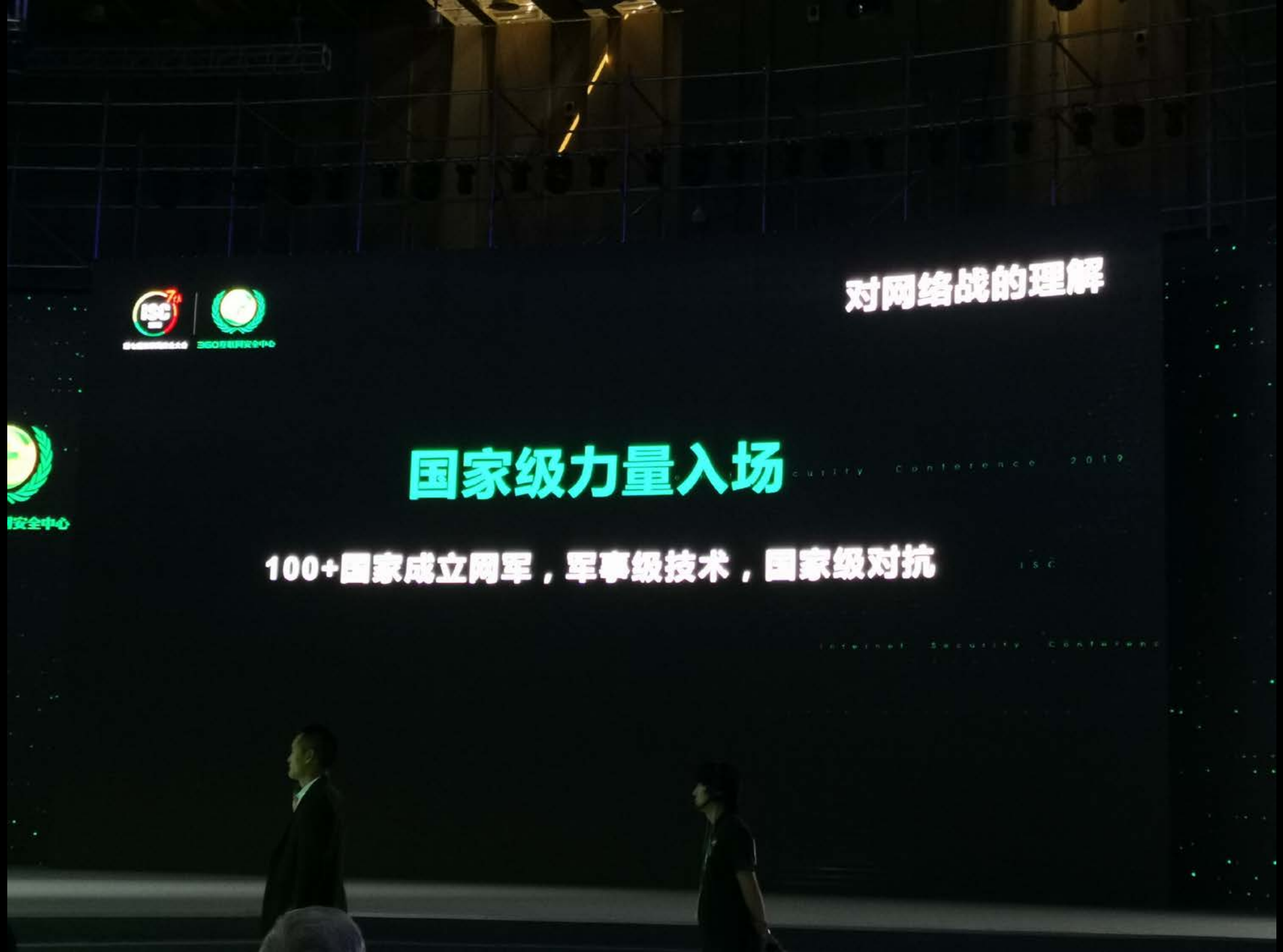
复杂的业务和军事系统

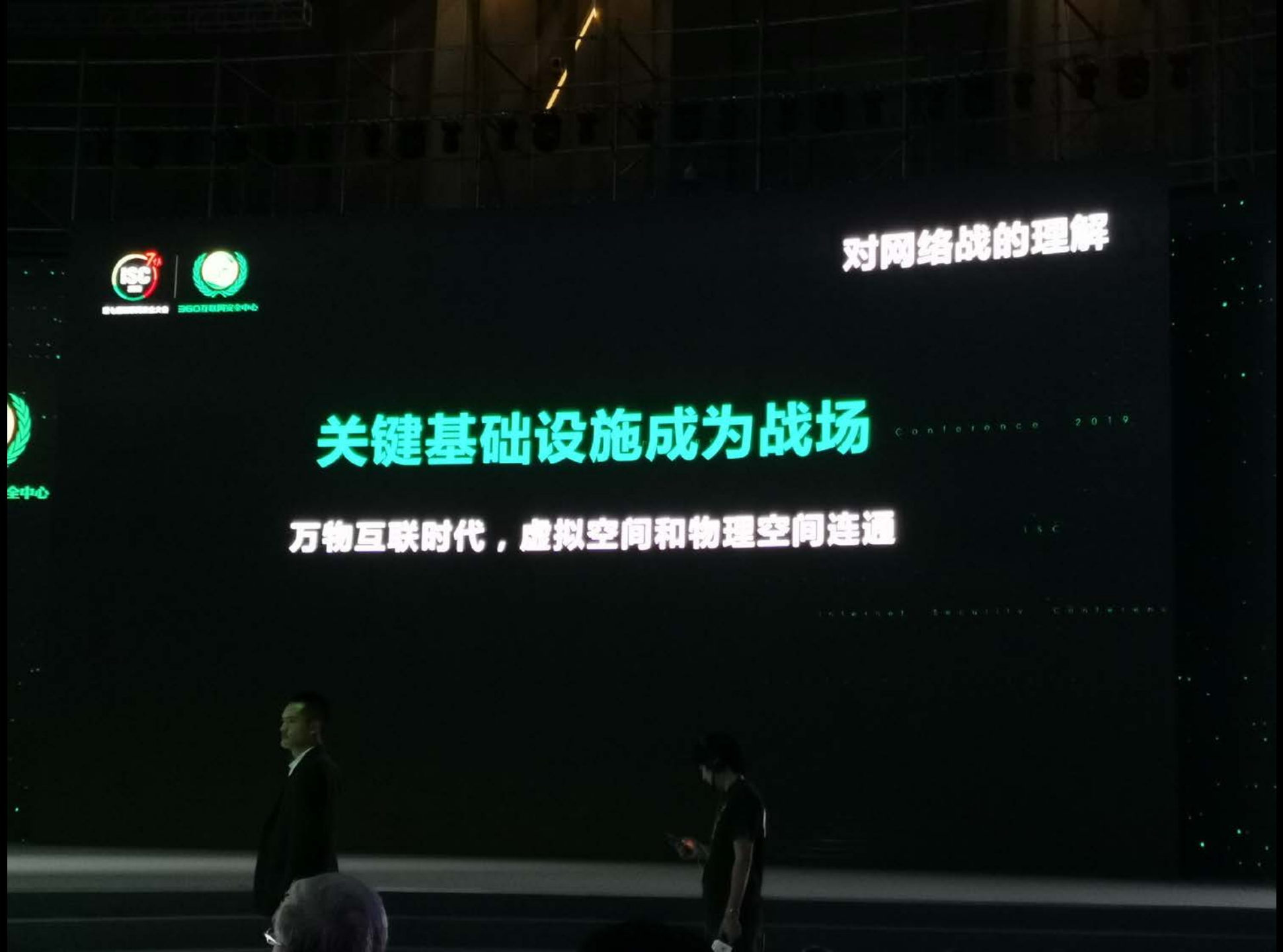
红蓝对抗，攻守兼备

4000个虚拟系统，承受2500次攻击


网络战正在发生
貌似和平很久，但战争从未远离，只是形式不同
必须用作战的视角看待网络安全


对网络战的理解
不宣而战
不分战时平时，渗透潜伏是网络战的一部分

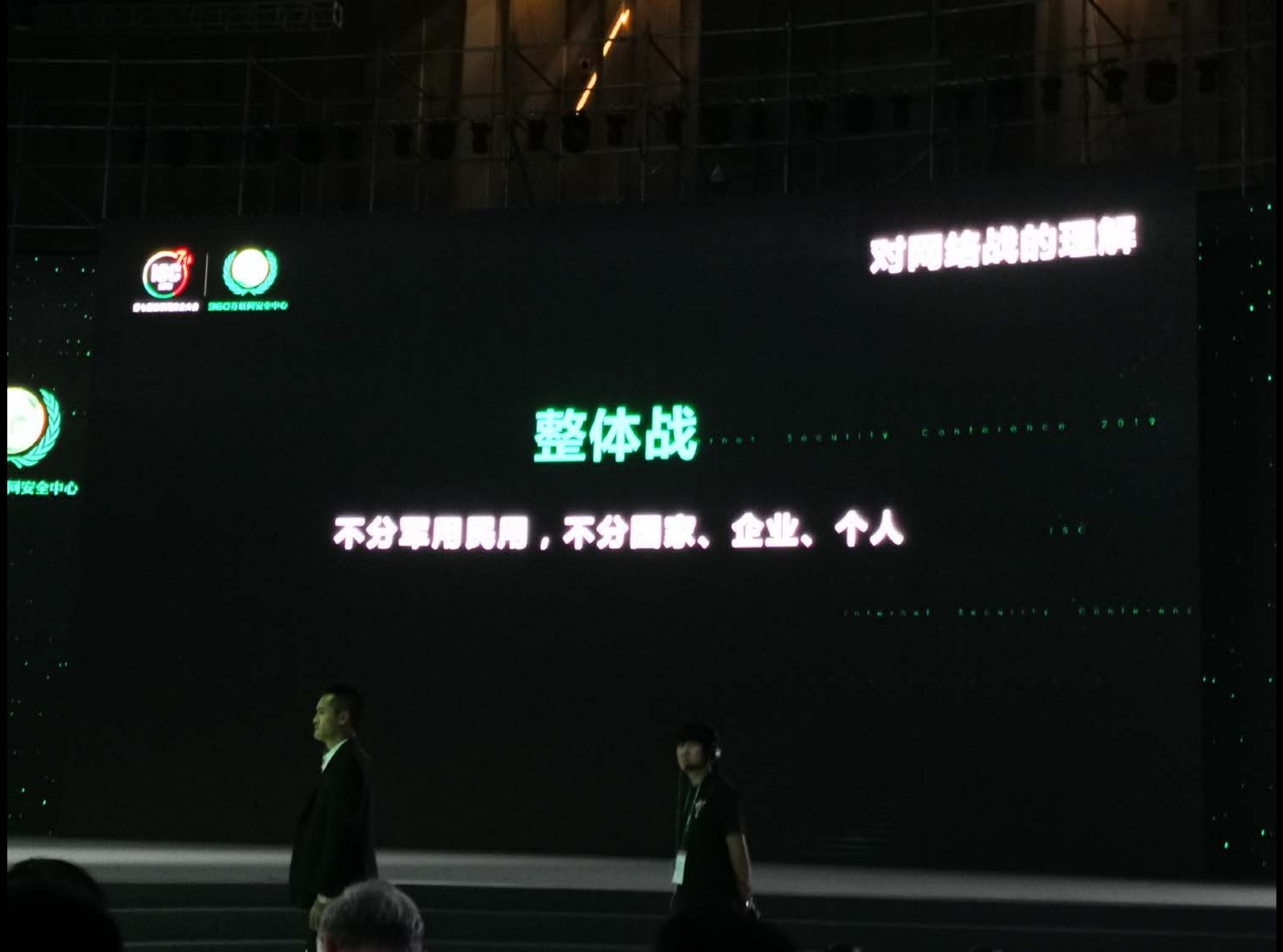

对网络战的理解
国家级力量入场
100+国家成立网军，军事级技术，国家级对抗


对网络战的理解
关键基础设施成为战场
万物互联时代，虚拟空间和物理空间连通

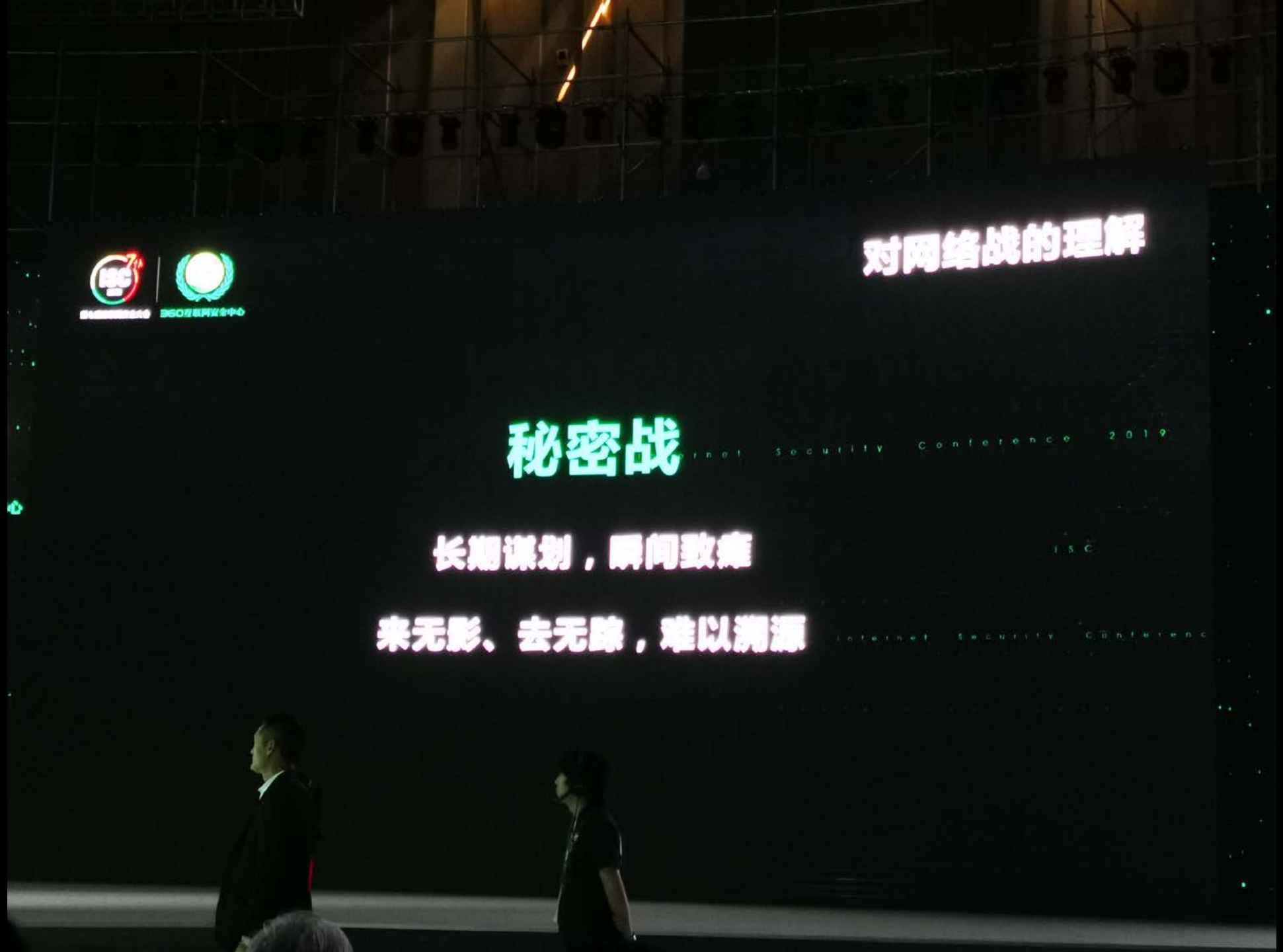

对网络战的理解
没有攻不破的网络
漏洞不可避免，漏洞无处不在


对网络战的理解
敌已在我
Security Conference 2019
ISC
Internet Security Conferenc

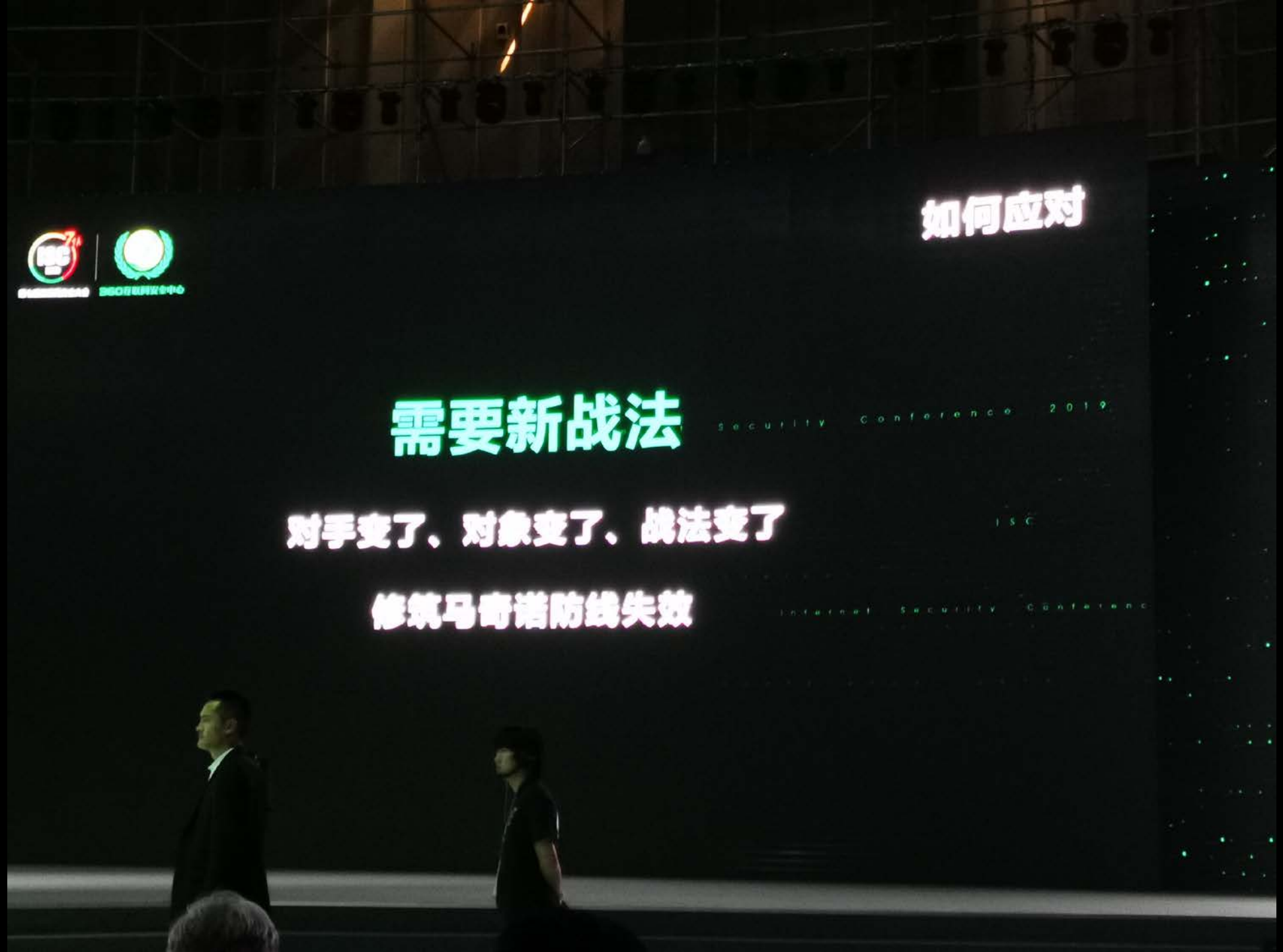

对网络战的理解
易攻难防
攻防不平衡，资源向攻击方倾斜

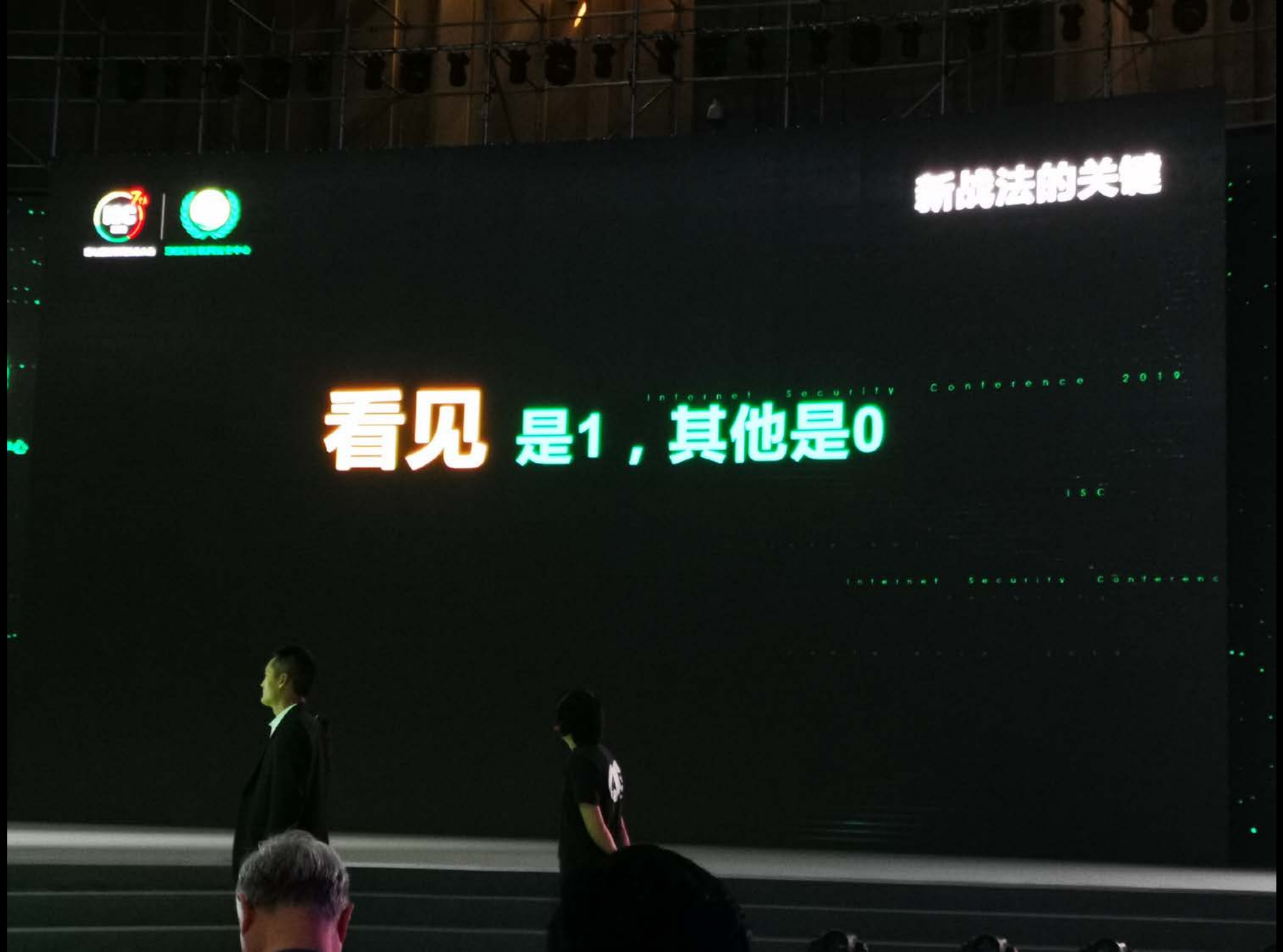

对网络战的理解
整体战
不分军用民用，不分国家、企业、个人

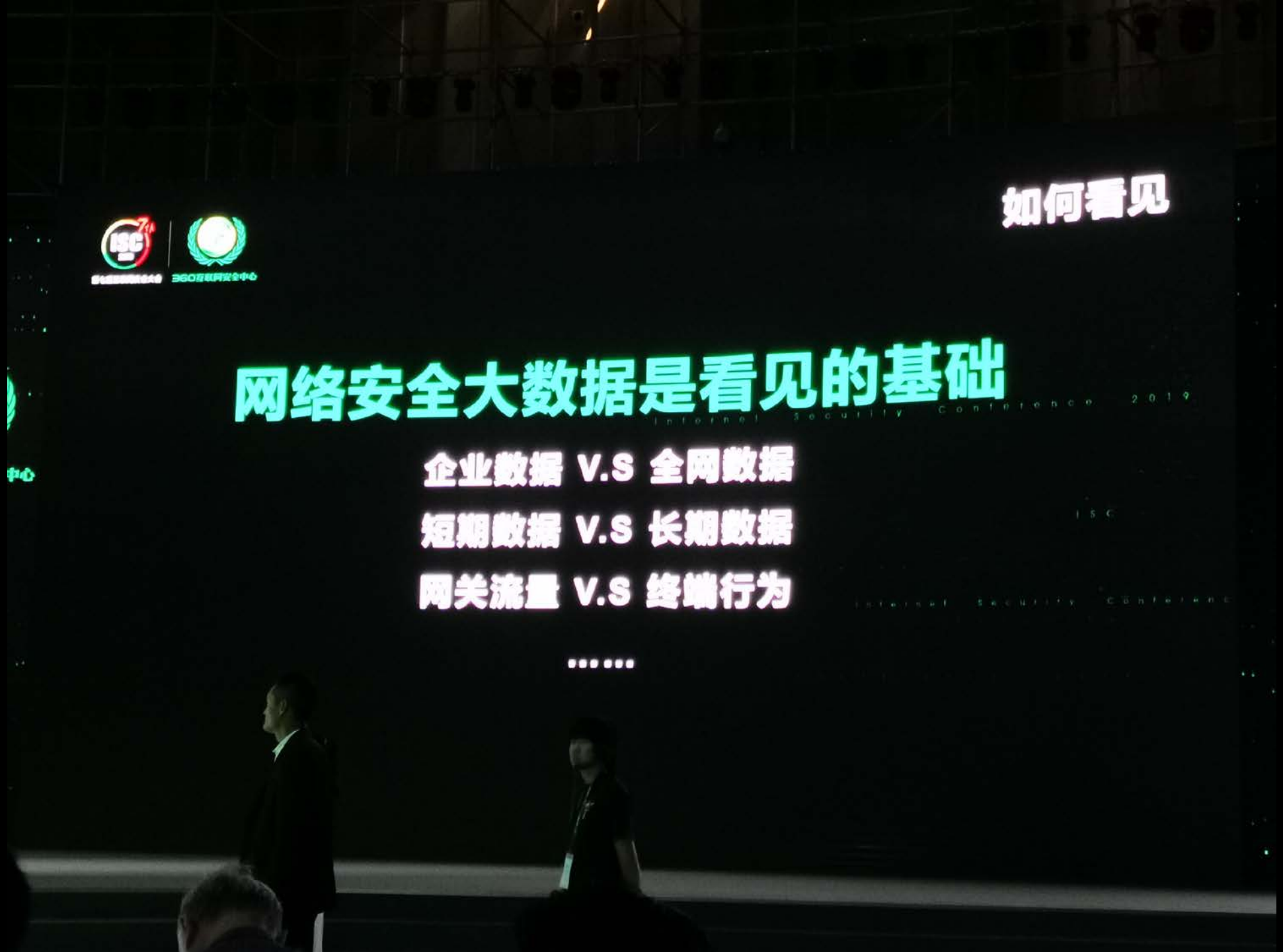

对网络战的理解
超限战
Internet Security Conference 2019
手段多元，无所不用其极
ISC
Internet Security Conference

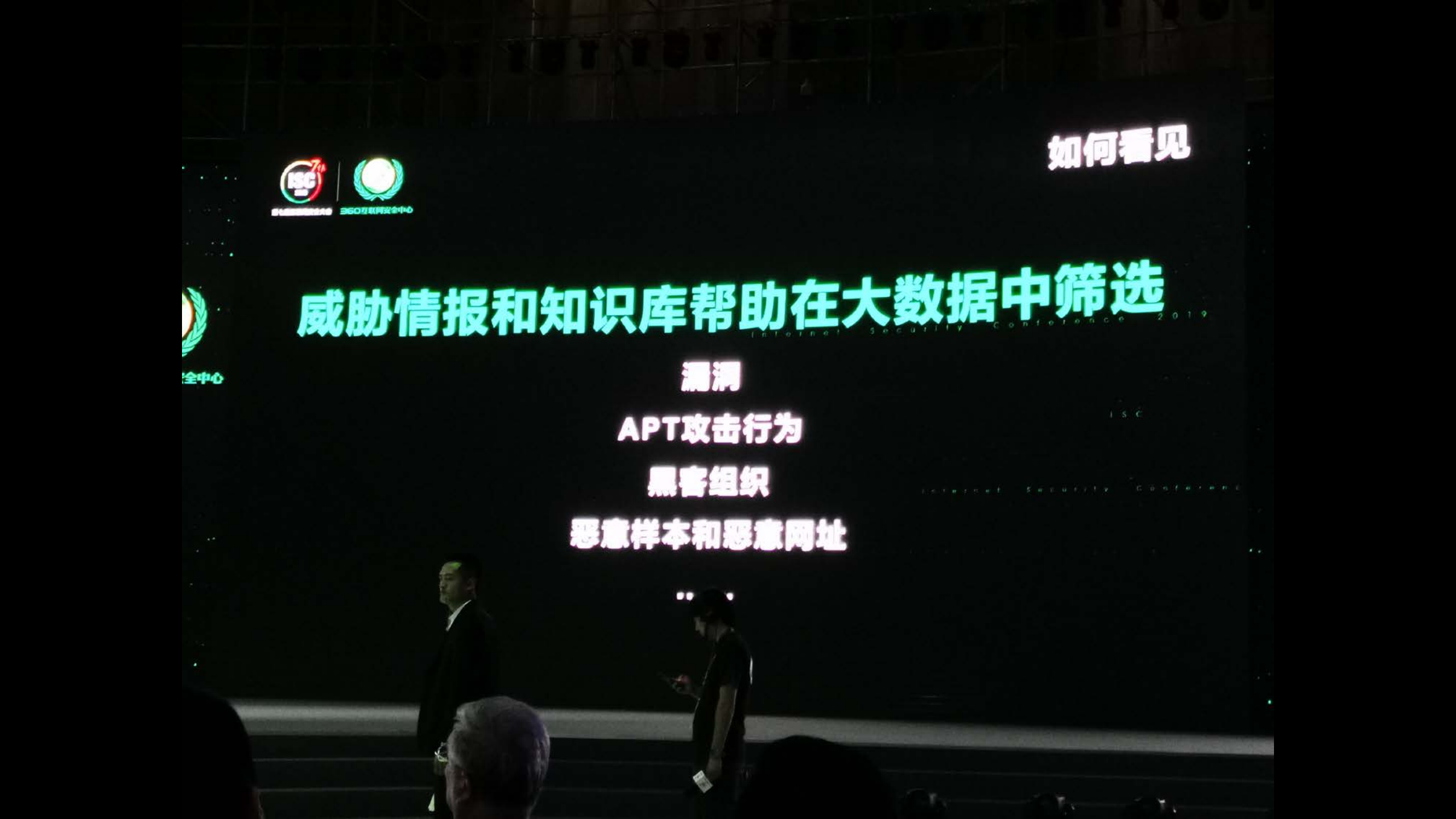

对网络战的理解
秘密战
长期谋划，瞬间致瘫
来无影、去无踪，难以溯源


对网络战的理解
网络战成为战争首选
成本低，效果好，烈度可控

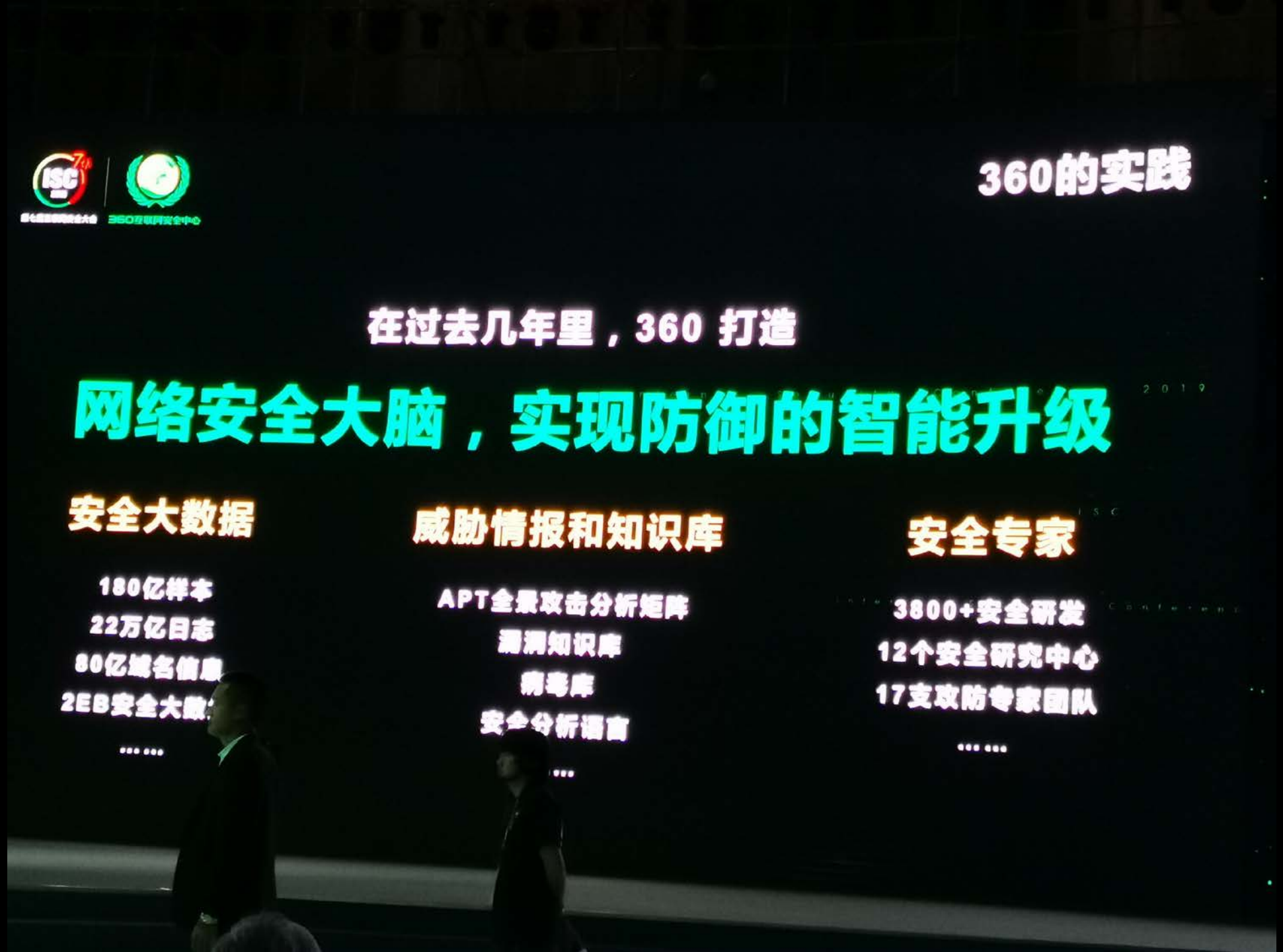

如何应对
需要新战法
Security Conference 2019
对手变了、对象变了、战法变了
修筑马奇诺防线失效
ISC
Internet Security Conferenc

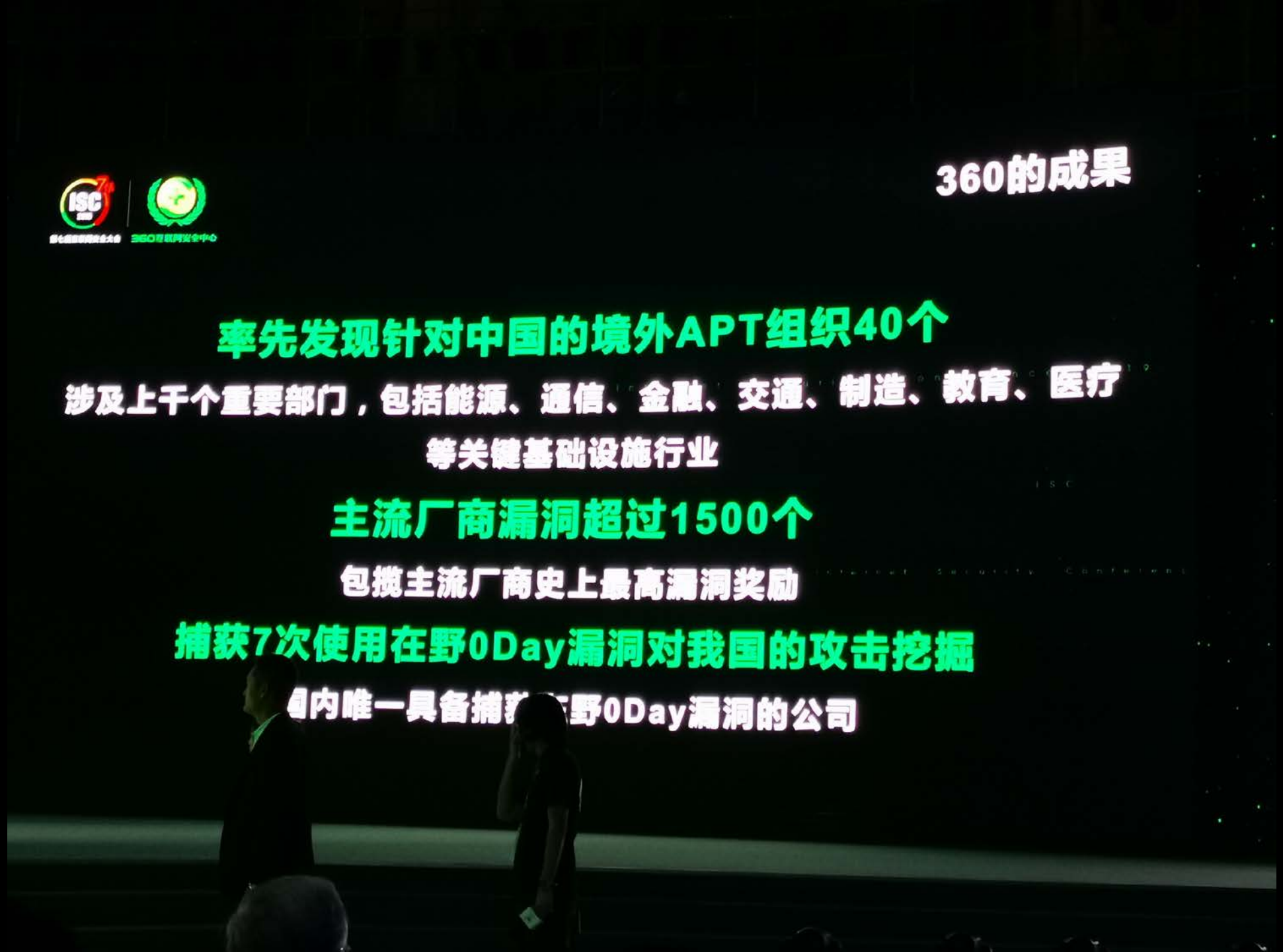

新战法的关键
Internet Security Conference 2019
看见 是1，其他是0
ISC
Internet Security Conferenc

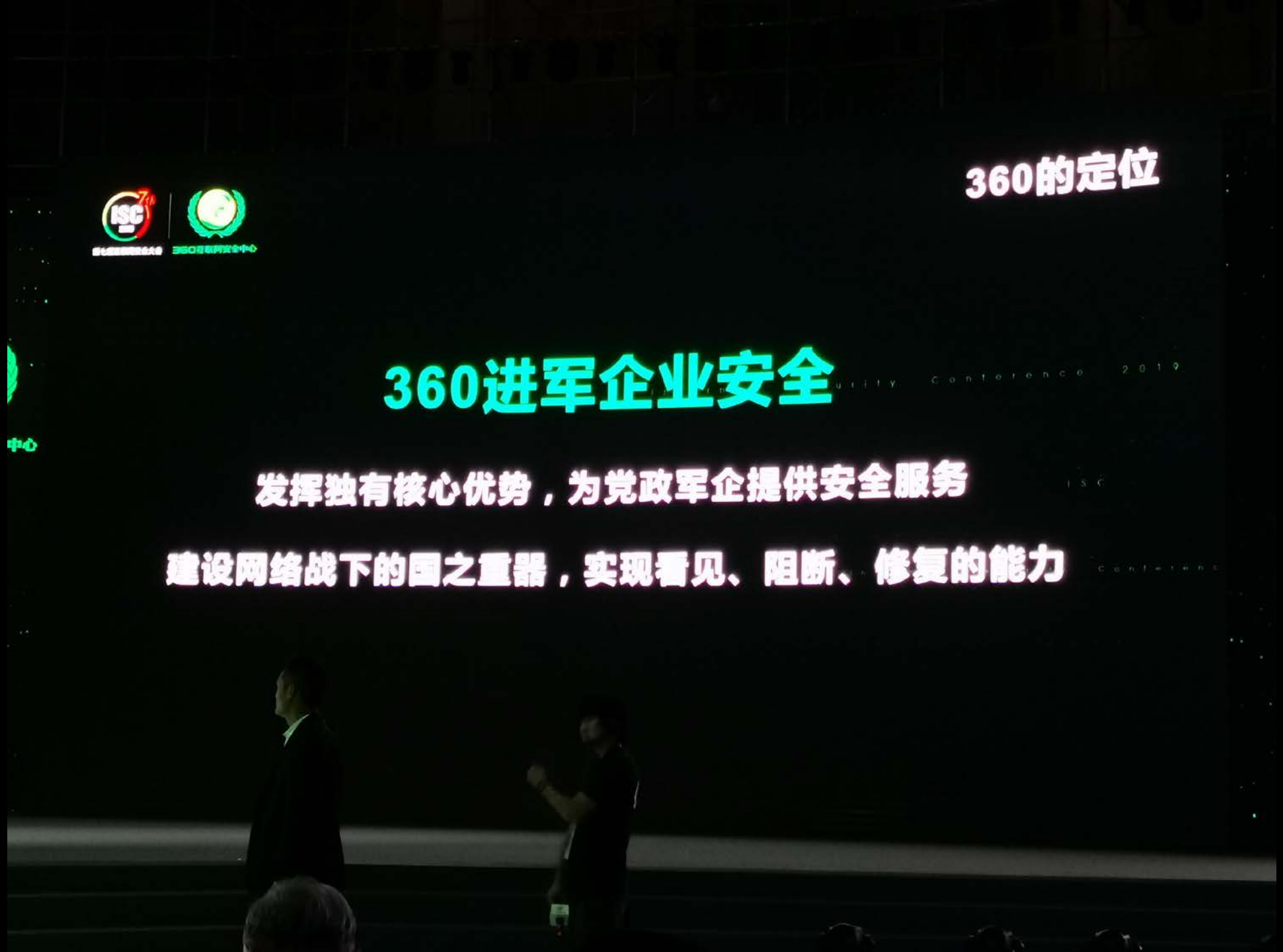

如何看见
网络安全大数据是看见的基础
企业数据 V.S 全网数据
短期数据 V.S 长期数据
网关流量 V.S 终端行为
……

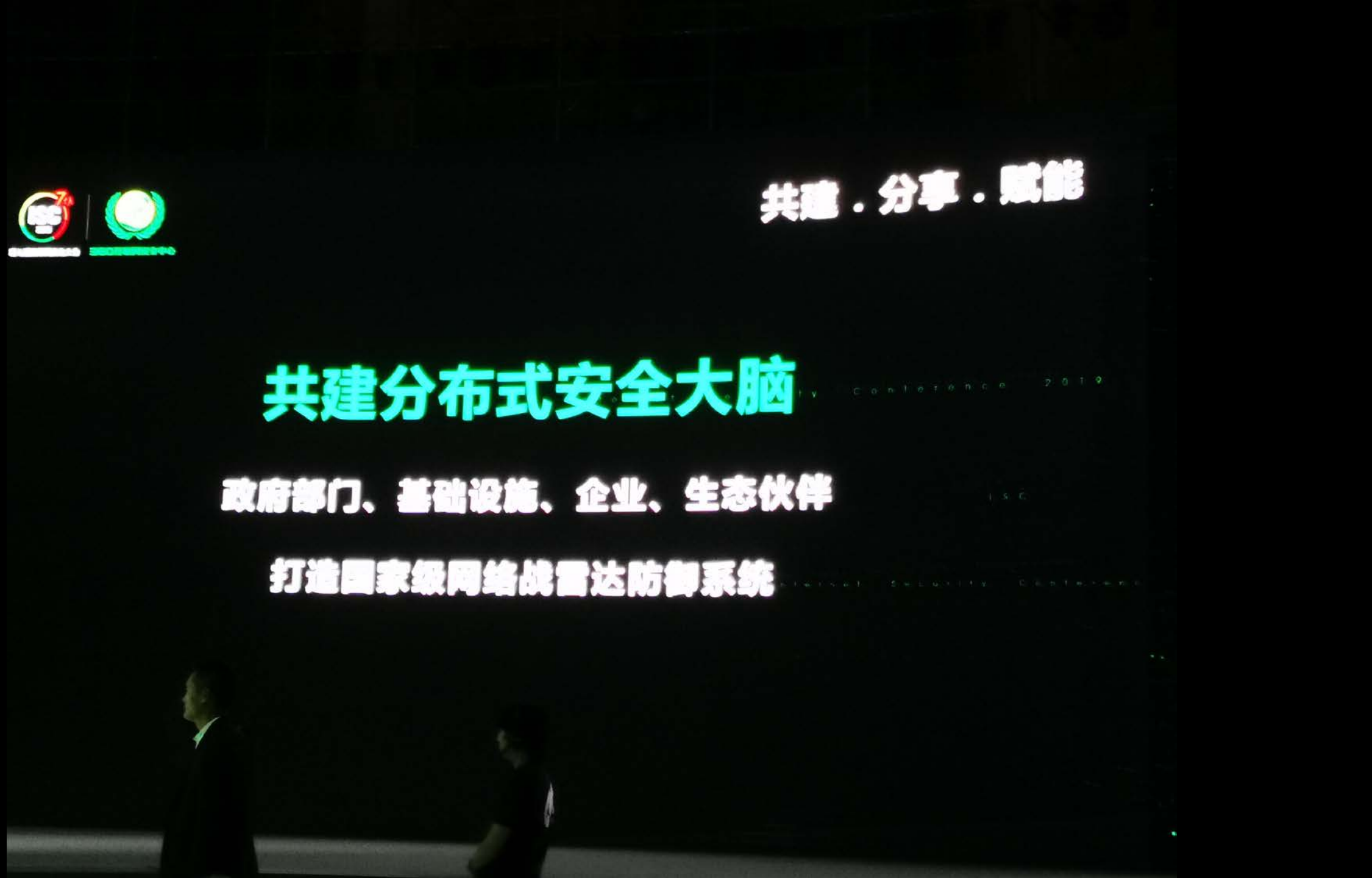

如何看见
威胁情报和知识库帮助在大数据中筛选
漏洞
APT攻击行为
黑客组织
恶意样本和恶意网址
...

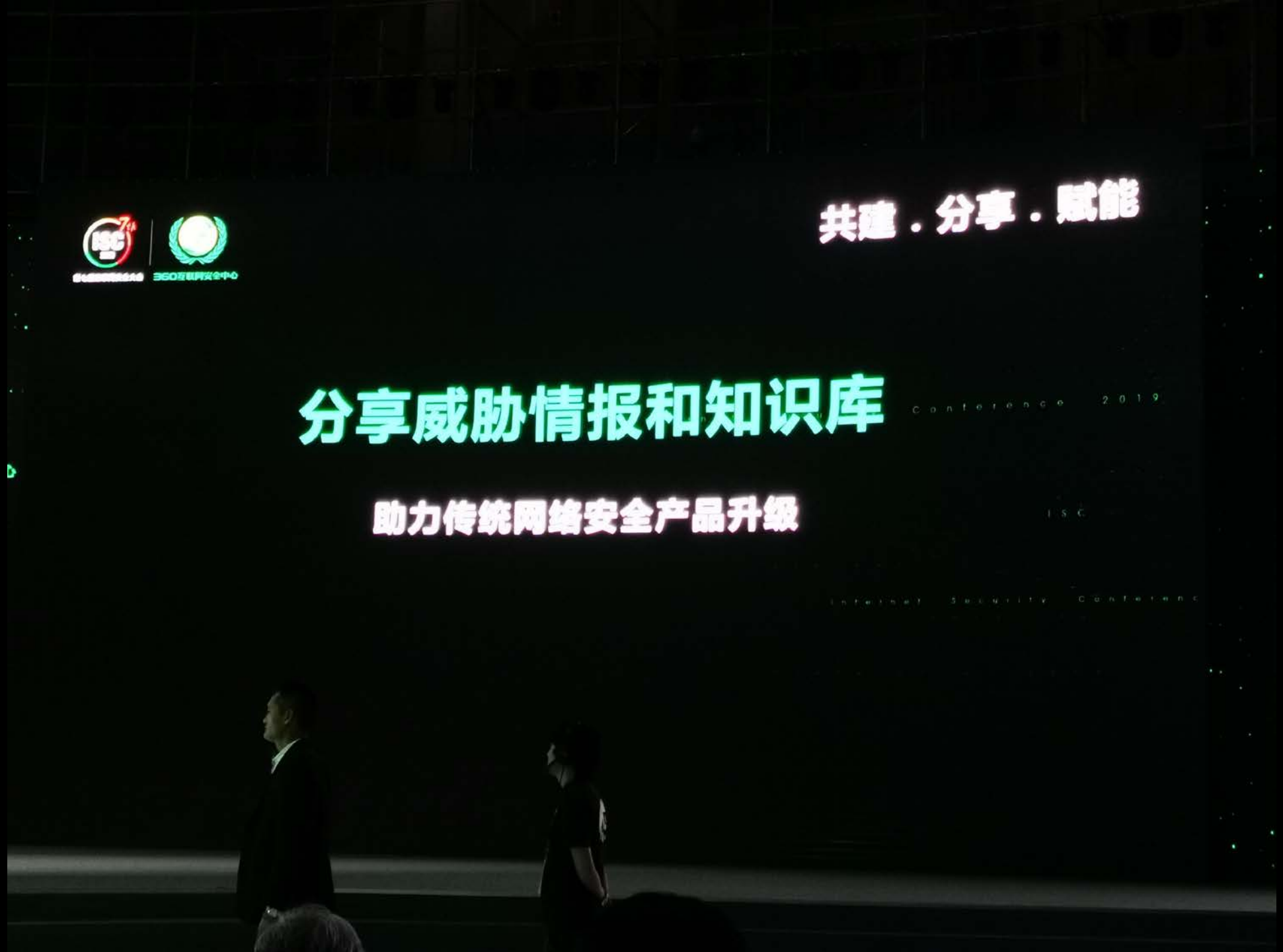

如何看见
高级别攻防专家起决定作用
网络战的本质是人与人的对抗

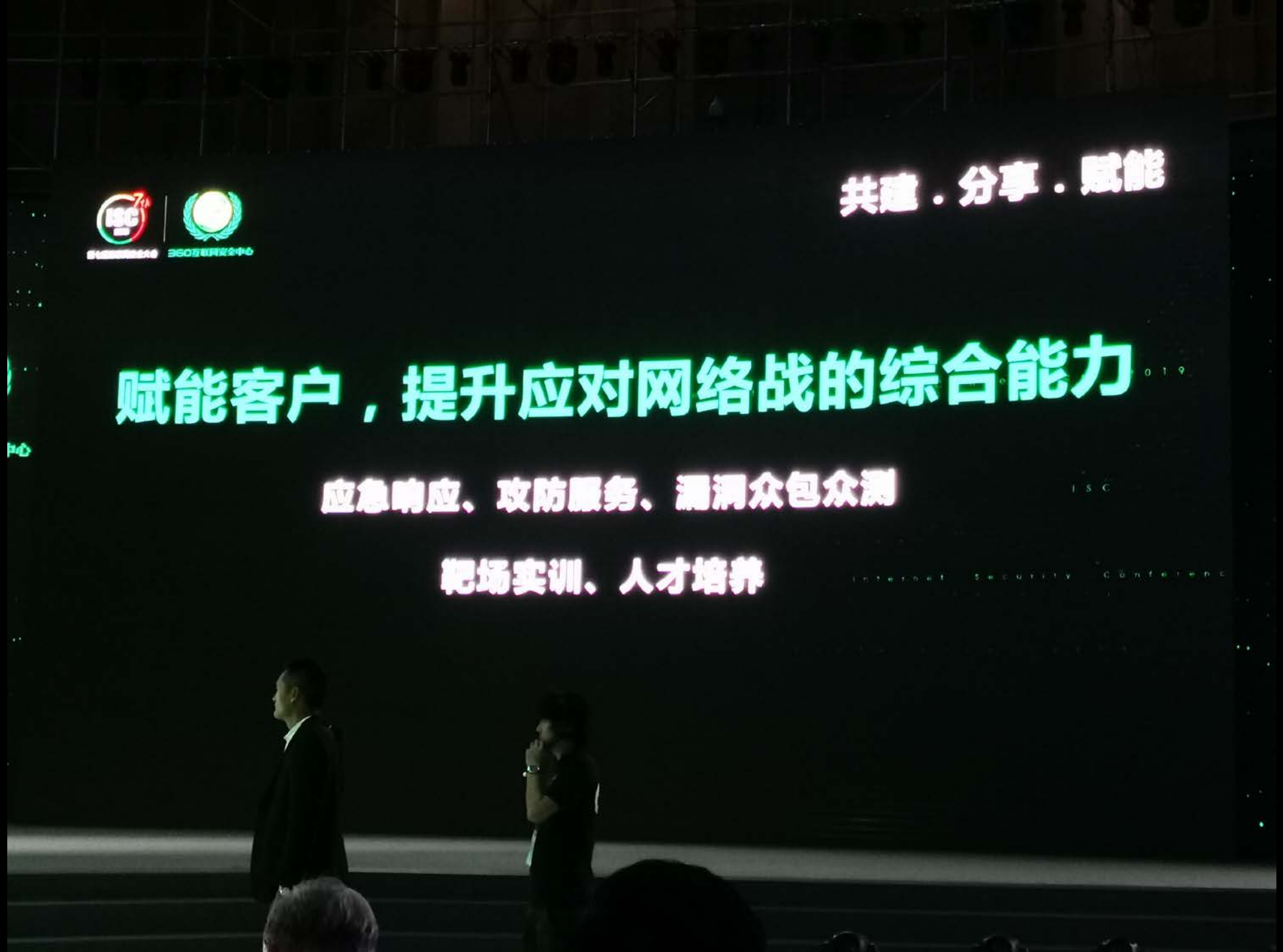

360的实践
在过去几年里，360 打造
网络安全大脑，实现防御的智能升级
安全大数据
180亿样本
22万亿日志
80亿域名信息
2EB安全大数
……
威胁情报和知识库
APT全景攻击分析矩阵
漏洞知识库
病毒库
安全分析语言
…
安全专家
3800+安全研发
12个安全研究中心
17支攻防专家团队
……


360的成果
率先发现针对中国的境外APT组织40个
涉及上千个重要部门，包括能源、通信、金融、交通、制造、教育、医疗
等关键基础设施行业
主流厂商漏洞超过1500个
包揽主流厂商史上最高漏洞奖励
捕获7次使用在野0Day漏洞对我国的攻击挖掘
内唯一具备捕
野0Day漏洞的公司


360的定位
360进军企业安全
发挥独有核心优势，为党政军企提供安全服务
建设网络战下的国之重器，实现看见、阻断、修复的能力


共建．分享．赋能
共建分布式安全大脑
政府部门、基础设施、企业、生态伙伴
打造国家级网络战雷达防御系统


共建．分享．赋能
分享威胁情报和知识库
助力传统网络安全产品升级


共建．分享．赋能
赋能客户，提升应对网络战的综合能力
应急响应、攻防服务、漏洞众包众测
靶场实训、人才培养


ISC寄语
ISC新目标，国际一流
行业平台、创新生态

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