

# 互联网进入大安全时代



360 互联网安全中心  
WWW.360.CN

谭晓生  
360公司 技术总裁、首席安全官

## 一、互联网进入“大安全”时代

## 二、应对网络安全威胁的思考和建议

## 三、利用新技术解决城市和社会安全问题

- 近年来重大安全事件频发
- 网络空间成为大国博弈斗争焦点
- 美国升级网络司令部

## 震网病毒

NSA网络武器拍卖

## 乌克兰电厂攻击

雅虎15亿用户账号泄露

## WannaCry勒索病毒

一半美国个人信用数据泄露  
美国断网事件

## 希拉里邮件门

孟加拉央行8100  
万美元被窃

徐玉玉案

海莲花

# 没有网络安全， 就没有国家安全！

## ■ 网络犯罪已成为第一大犯罪类型，未来绝大多数犯罪都可能借助

**网络实施** —— 孟建柱书记在全国社会治安综合治理表彰大会讲话

➤ 国内网络诈骗从业者160万人

➤ 黑产年产值上千亿

➤ 新型诈骗方式不断涌现

- 虚假网贷诈骗

- 付款二维码盗刷

- 假冒共享单车客服电话

## ■ WannaCry勒索病毒肆虐全球，严重影响社会安全



- 150多个国家被攻击
- 国内3万多个机构
- 30多万台电脑被感染

勒索病毒攻击威胁社会安全和民生服务

- “震网病毒”、乌克兰电厂攻击事件，表明网络攻击已可穿透网络虚拟空间，对国家、城市的关键基础设施进行控制、破坏



2015年12月的乌克兰电厂攻击

## ■ 针对金融系统的网络攻击

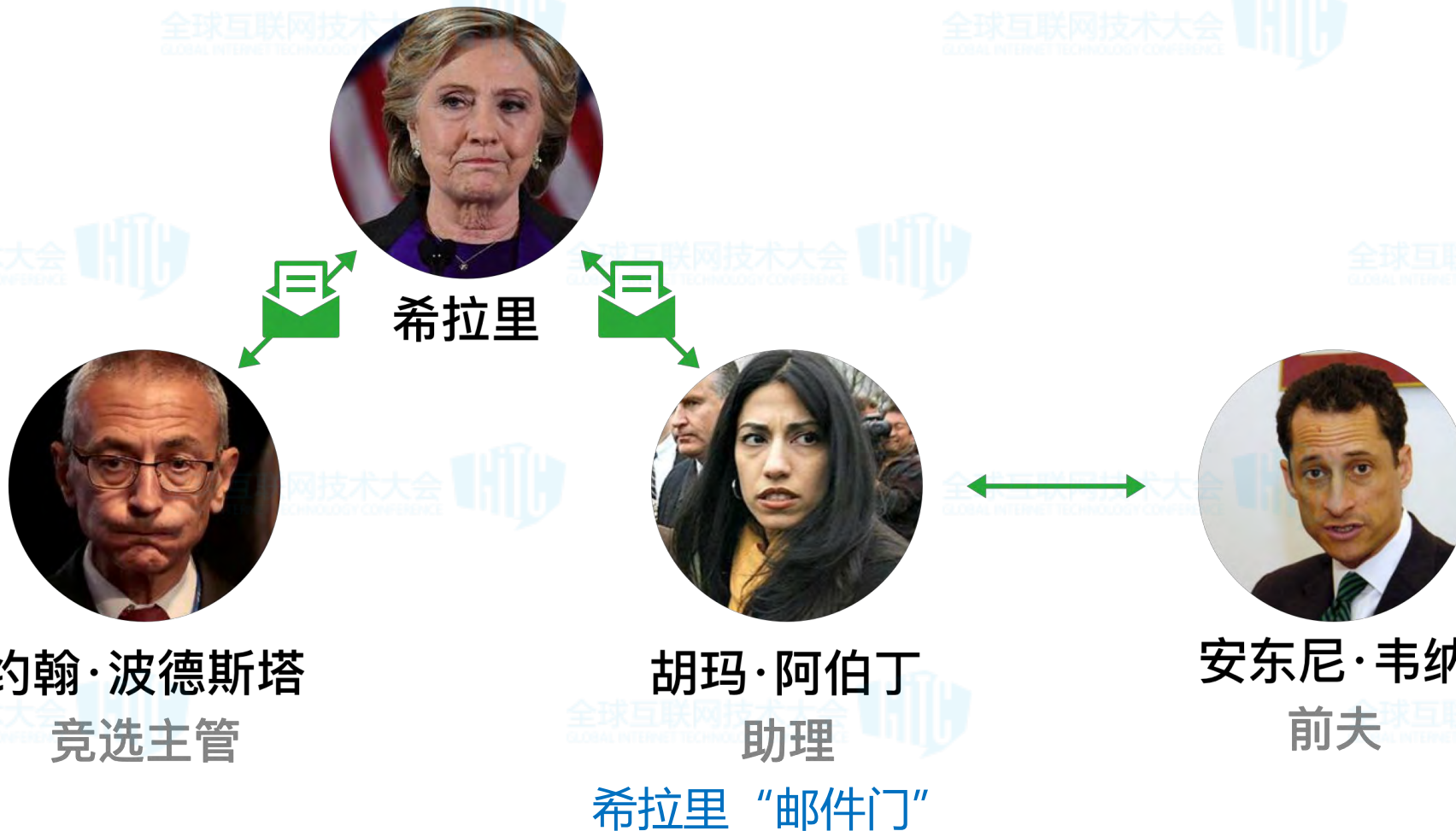


2016年2月孟加拉央行8100万美元被窃取



2016年7月台湾ATM机200万美元失窃

## ■ 网络攻击甚至可以改变一个国家的政权格局





# 世界已进入“大安全”时代

全球互联网技术大会

全球互联网技术大会

全球互联网技术大会



360互联网安全中心

人身安全

社会安全

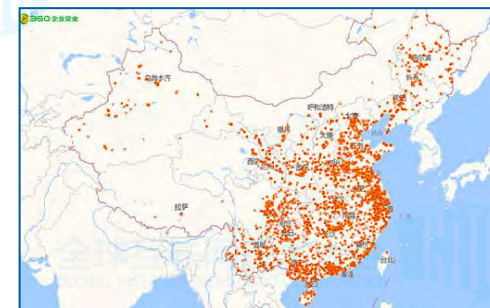
基础设施安全

城市安全

国防安全

国家安全

信息安全



# “WannaCry” 勒索病毒事件就是网络战的一次预演



360互联网安全中心

## ■ “WannaCry” 事件是网络战的分水岭

- 使用了NSA的网络武器
- 手段低劣，但影响巨大
- 美国网络战能力遥遥领先
- 将引发网络武器军备竞赛
- 打开了网络恐怖主义的“潘多拉盒子”



## ■ 网络战成为战争首选

- 网络战具有颠覆性的时空优势
- 陆战以天和周为单位，空战以小时为单位，而网络战是秒和分钟级
- 成本低，效果好

1981年，以色列空袭伊拉克核设施

**空战+电子战+战术欺骗**

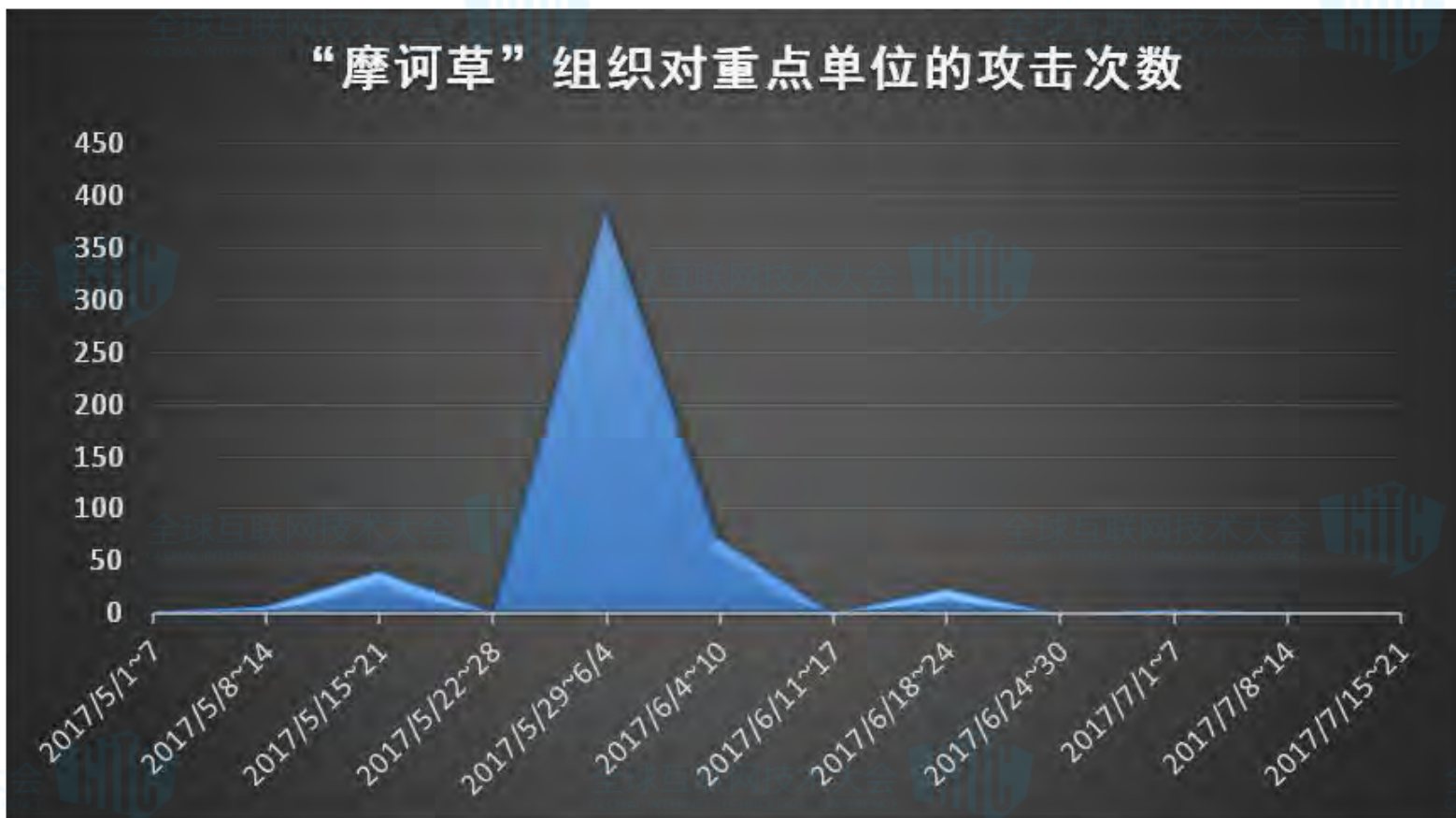
2007年，以色列空袭叙利亚核设施

**空战+电子战+网络战**

2010年，以色列/美国攻击伊朗核设施（震网事件）

**纯网络战**

## ■ 网络战案例：来自南亚某国的网络战攻击“摩诃草”



“摩诃草”攻击监测

## ■ 我国是近年来遭受APT攻击的最主要受害国

➤ 截止2016年底，360监测到针对中国的境内外APT组织36个

排行	APT攻击领域	攻击组织数量
1	政府（公、检、法、司等）、外交	21
2	金融	15
3	大型企业、商业组织、技术组织	14
4	军事、部队、国防	13
5	能源、交通、电力、医疗等基础设施	12
6	特殊个人	3
7	教育、科研	2

# 关键基础设施成为主要攻击目标，威力不亚于传统战争



360互联网安全中心

- 网络攻击可以造成物理伤害
- 电网、水利、机场、工厂等皆可被攻击
- 美国非常重视基础设施保护
- 基础设施网络恐怖袭击将越来越多



# 没有攻不破的网络，人是最薄弱环节



360互联网安全中心

## ■ 漏洞无处不在

- 任何程序都是人编的，只要是人就会犯错
- 平均每千行代码有**6个**安全缺陷
- 360 “补天” 平台每年发现漏洞超过**8万个**

## ■ 人是最薄弱环节

- 邮件门事件中希拉里身边的人
- 假冒的免费WiFi
- 印有“XXX照片”的U盘
- 通过手机私搭WiFi热点上网





# 没有攻不破的网络，人是最薄弱环节

全球互联网技术大会

全球互联网技术大会

全球互联网技术大会



360互联网安全中心

- 没有攻不破的网络，没有绝对的安全



**网络战时代没有“马奇诺防线”**

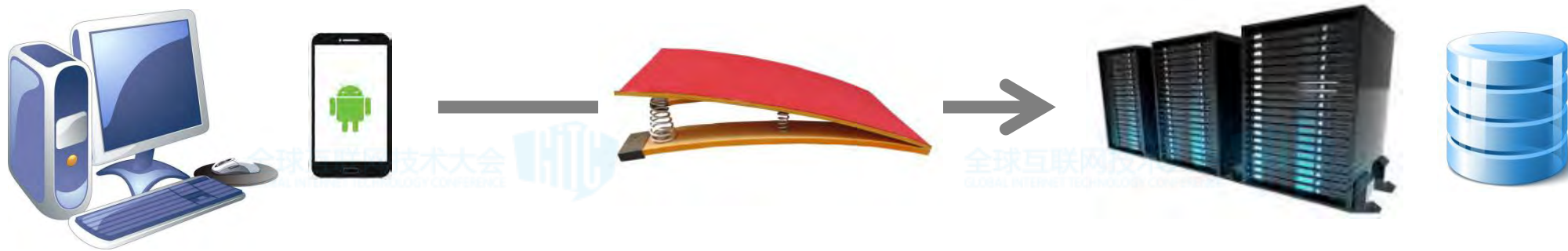
**隔离内网更要重视安全**

# 网络战是整体战，终端安全非常关键



360互联网安全中心

- 网络战攻击不分军民
- 网络是相互连接的整体，任何设备被攻破都可能导致整个网络沦陷



网络战往往首先攻击终端设备

## 转变网络安全技术思想

1、拦截阻断 → 检测响应

2、边界防护 → 终端安全

3、检测引擎 → 安全大数据

## 4、做好网络隔离和网段划分



航母隔离舱

## 5、采用应用程序白名单



CARBON  
**BLACK**  
ARM YOUR ENDPOINTS

终端安全白名单技术

## 6、重要系统要进行多重身份认证



多重身份认证

## 7、做好数据备份对抗数据破坏攻击



## 8、建立钓鱼邮件过滤系统



## 9、加强物联网设备安全检测、监控和运营管理



- 网络安全要做顶层规划设计
  - 从中央到地方统一规划和建设
- 网络安全要有集中统一管理
  - 要建立安全运营中心
- 信息化和网络安全同步推进
  - 业务系统开发的时候就要考虑安全问题

**网络安全是  
三分技术，七分管理**

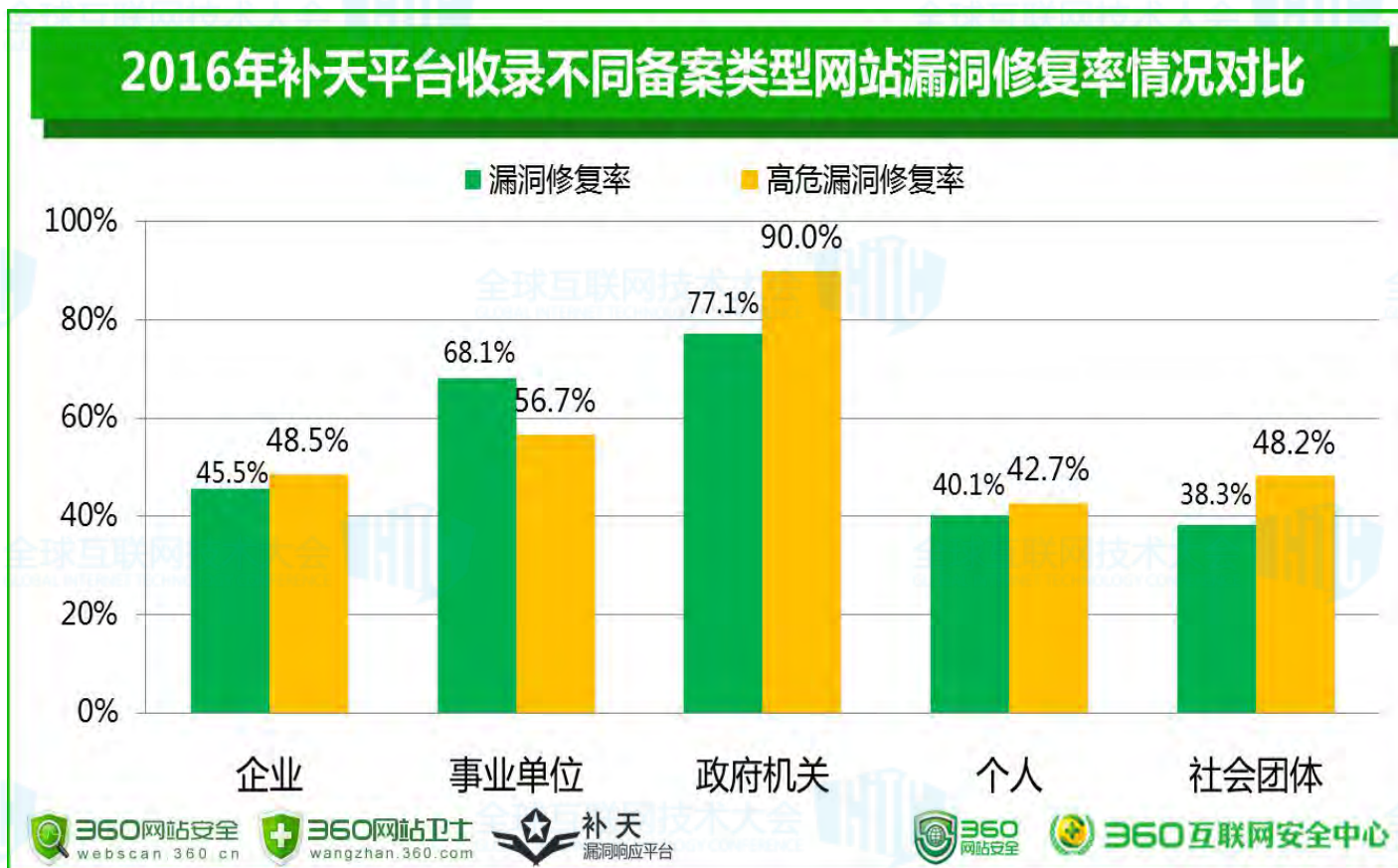
- 建立网络安全应急体系
  - 成立领导小组
  - 建立专家技术团队
  - 制定应急预案
  - 加强应急演练
- 管理要有技术手段来保障
  - 人难免违反规定



- 习总书记指出：**网络安全的本质在对抗，对抗的本质在攻防两端能力较量。**人是网络安全中最重要的因素
- 网络安全已成为智力密集型服务业，因此需要
  - 建立自己的网络安全技术队伍
  - 强化安全队伍的培训
  - 加大对专业网络安全服务的采购



## ■ 制定漏洞修复管理细则，建立监督检查及责任追究机制



漏洞修复不及时的问题在我国政企单位普遍存在

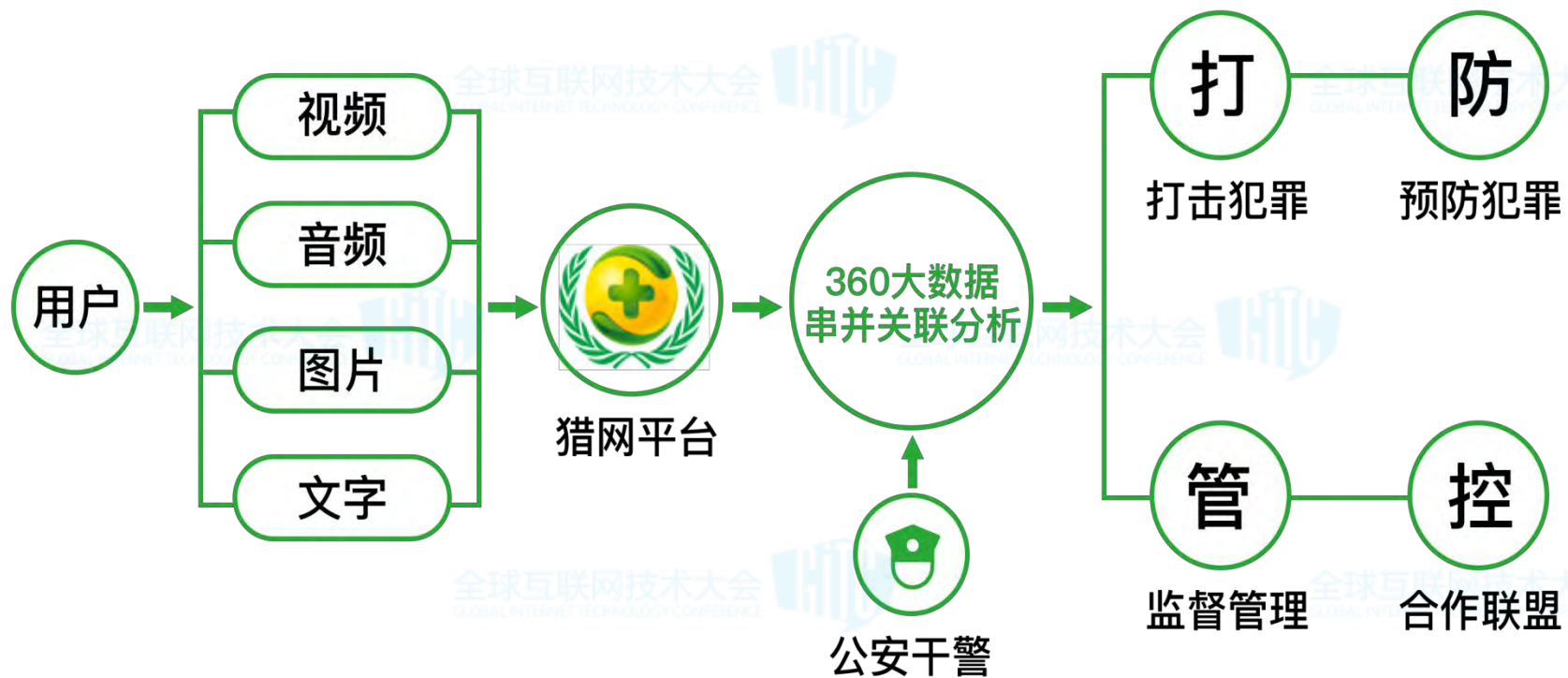
## ■ 鼓励政企单位及时披露遭到的网络攻击

- 及时披露有助于发现漏洞、修补漏洞、分析溯源
- 因害怕承担责任，很多单位往往掩盖和隐瞒攻击
- 安全事故追责要区分具体情况

# 利用大数据方法打击网络犯罪



360互联网安全中心



与全国**300多个**地方公安机关建立了合作

协助侦破网络诈骗案件**200多起**

破获大型诈骗团伙**10余个**

“360猎网平台” 利用大数据协助公安部门打击网络犯罪

# 利用人工智能+智能硬件提升社会综合安全防控水平



360互联网安全中心

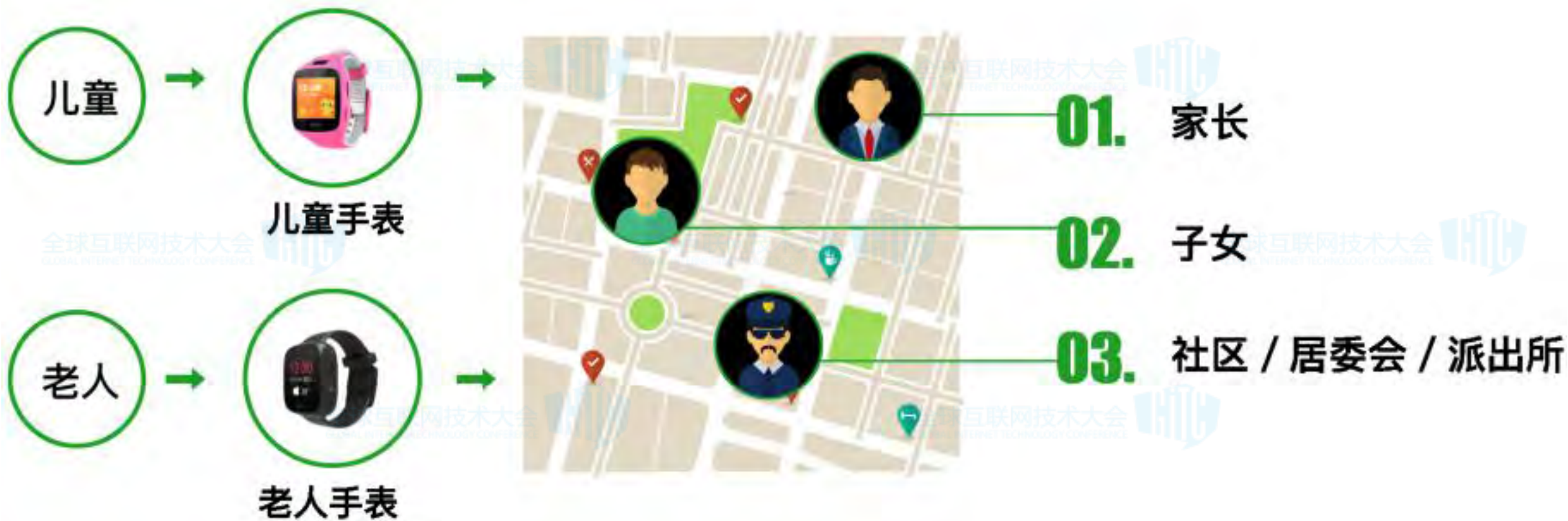


利用人工智能和智能硬件实现城市微型末梢安全监控

# 利用人工智能+智能硬件提升社会综合安全防控水平



360互联网安全中心



利用人工智能和智能硬件保护老人和儿童安全

# 互联网+方式创新社会信用体系建设



360互联网安全中心



360手机卫士标记老赖电话



360信用卫士查询失信信息



360互联网安全中心

安全是人类的基本需求

互联网已进入大安全时代

协同联动，共同防御