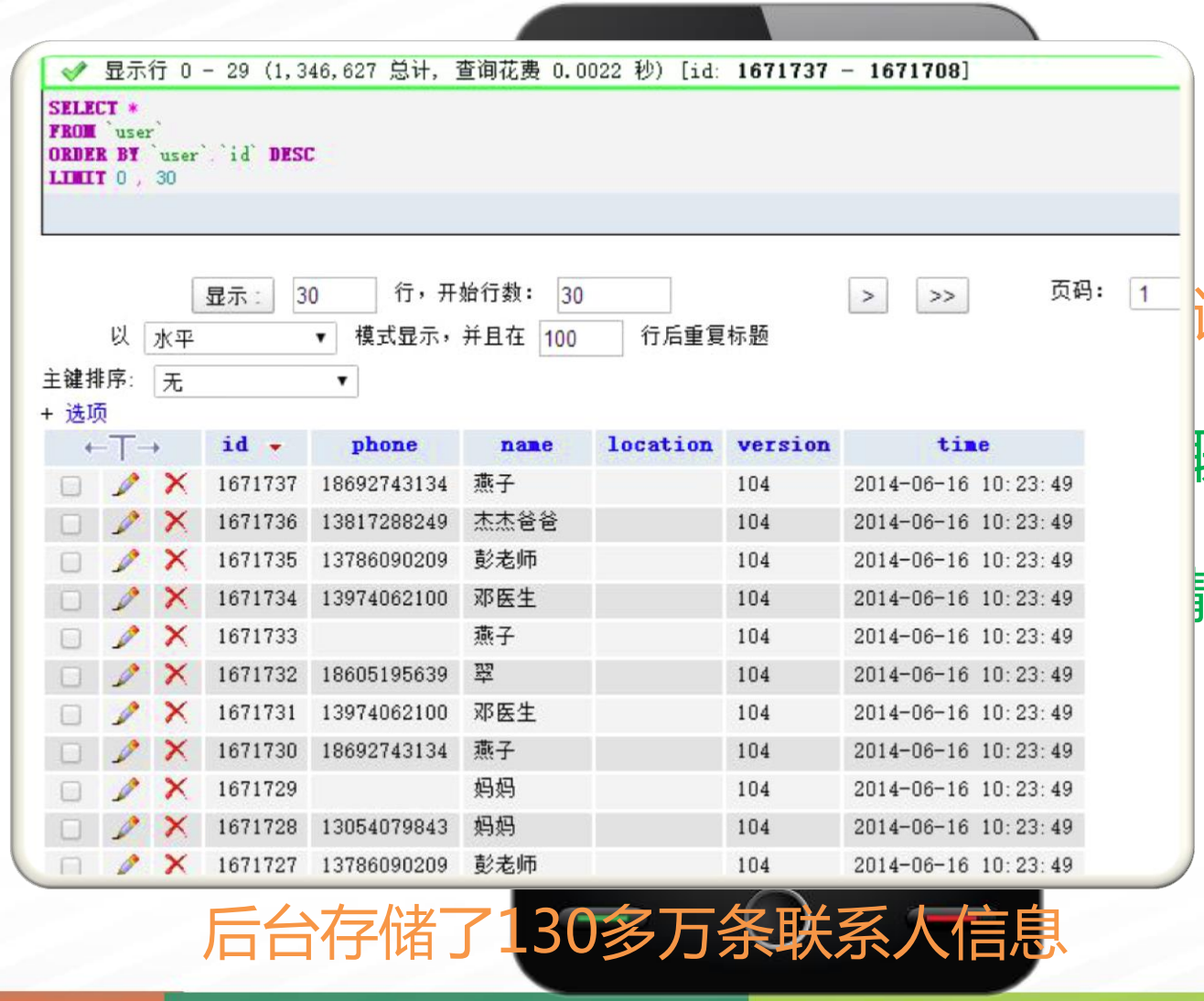
携手共建国家网络安全保障体系

云晓春

2014年9月

题纲

从细节折射我国网络安全保障困局



后台存储了130多万条联系人信息

由于法律依据不足，无法对制作者彻底打击

静默回传

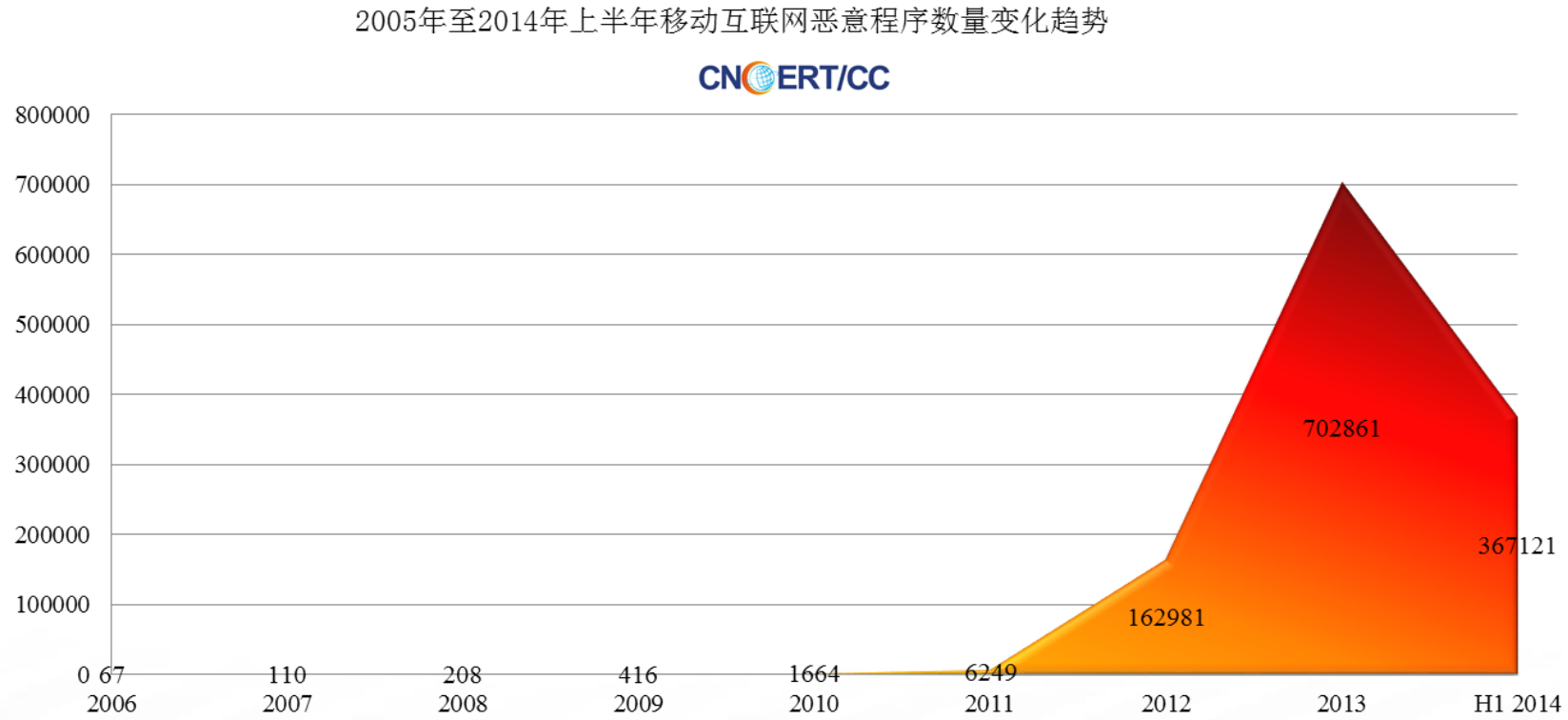
从国家级对抗反射我国网络安全保障困局

分而有余 合而不足

我国互联网网络安全形势严峻

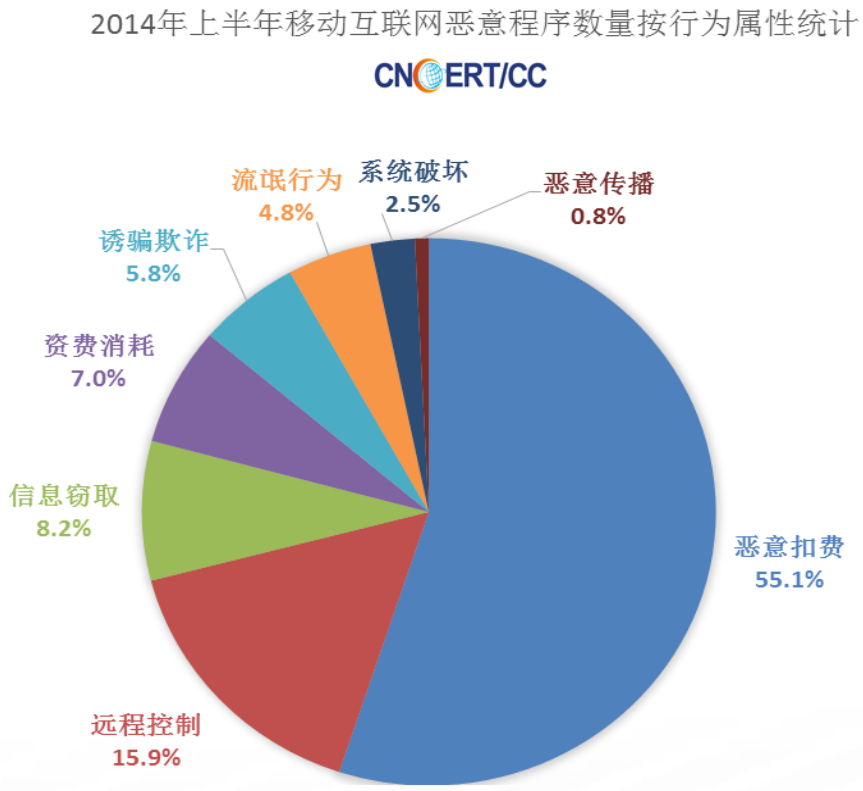
移动恶意程序数量继续呈增长趋势

- 上半年新增恶意程序36.7万，较2013年同期增长13.0%

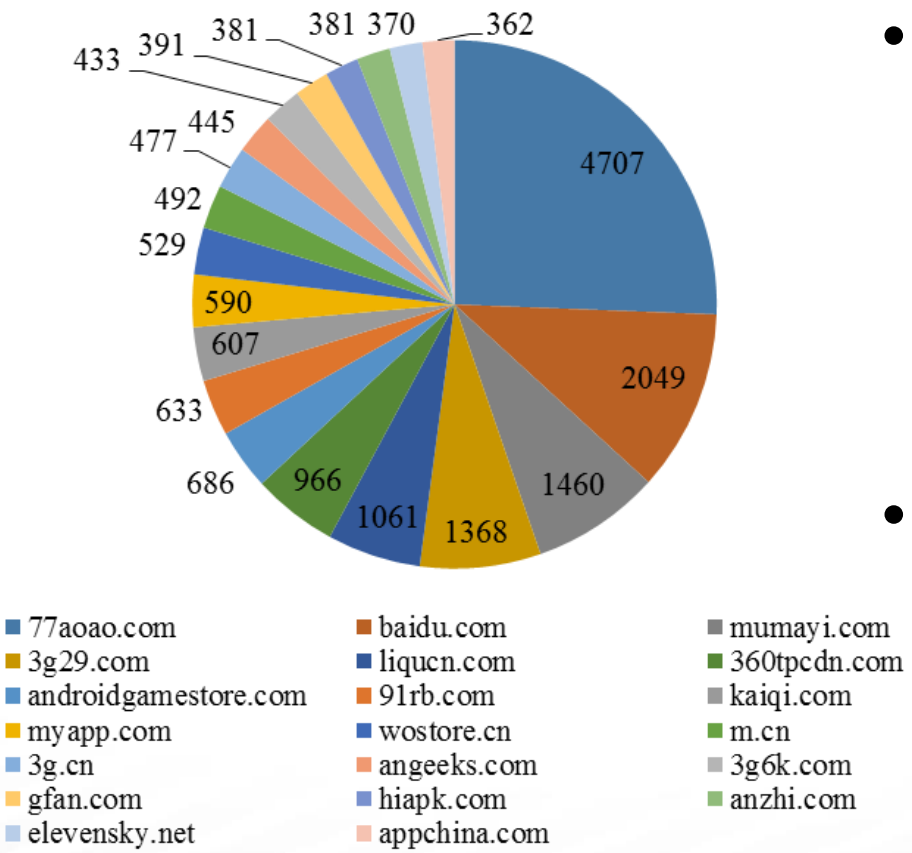


移动恶意程序趋利性明显

- 恶意扣费类和资费消耗类占62%以上



移动恶意程序传播渠道众多



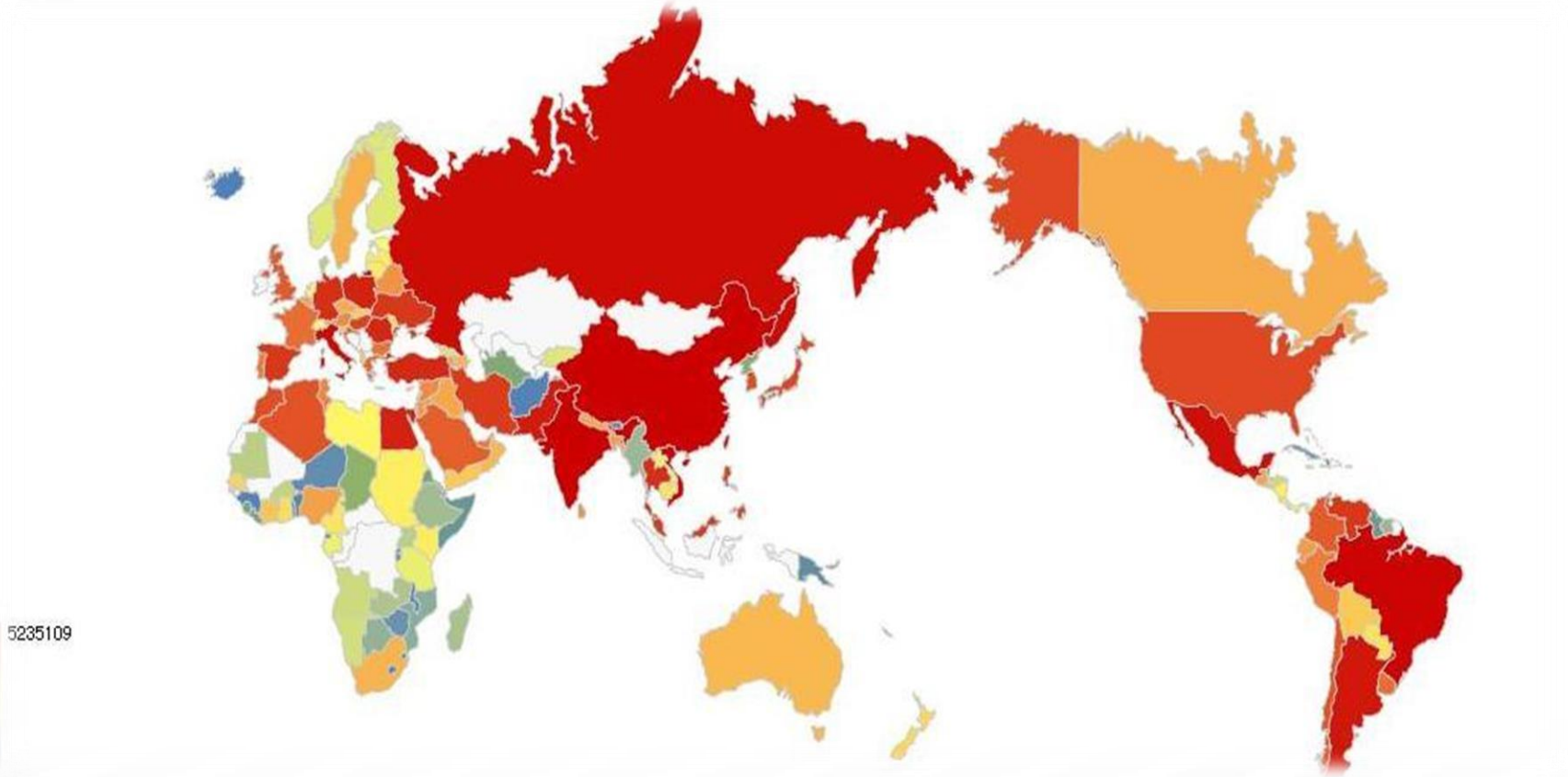
- 应用商店、论坛、下载站点是主要传播渠道
  - 传播移动恶意程序的域名811个
  - 存在移动恶意程序的应用商店超过300家
- 单个域名包含的移动恶意程序最多达4707个

恶意程序感染主机规模庞大

- 境内感染木马僵尸网络的主机达626万台

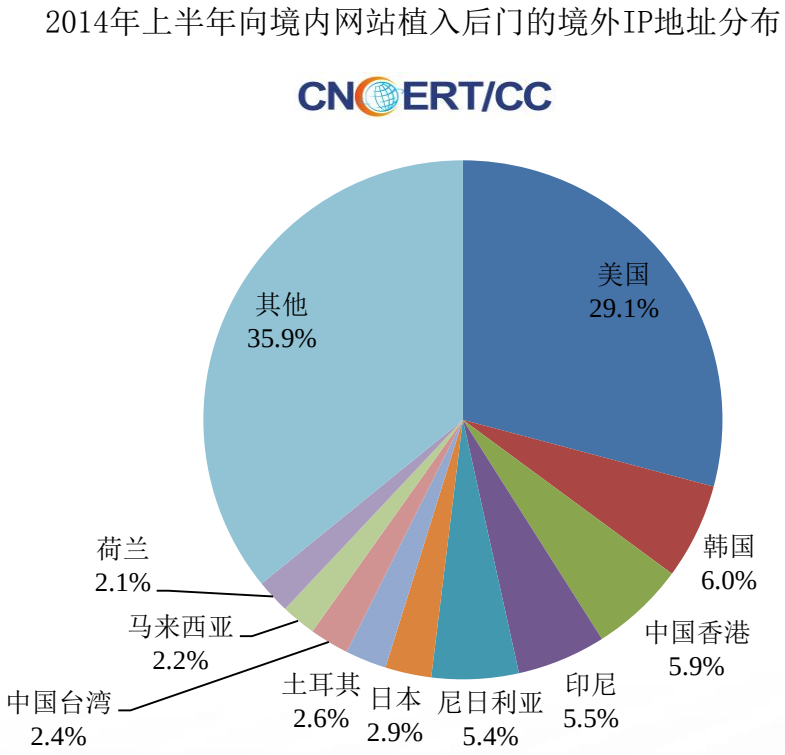
恶意程序感染主机规模庞大

- 境内飞客蠕虫感染主机数量占全球11.3%



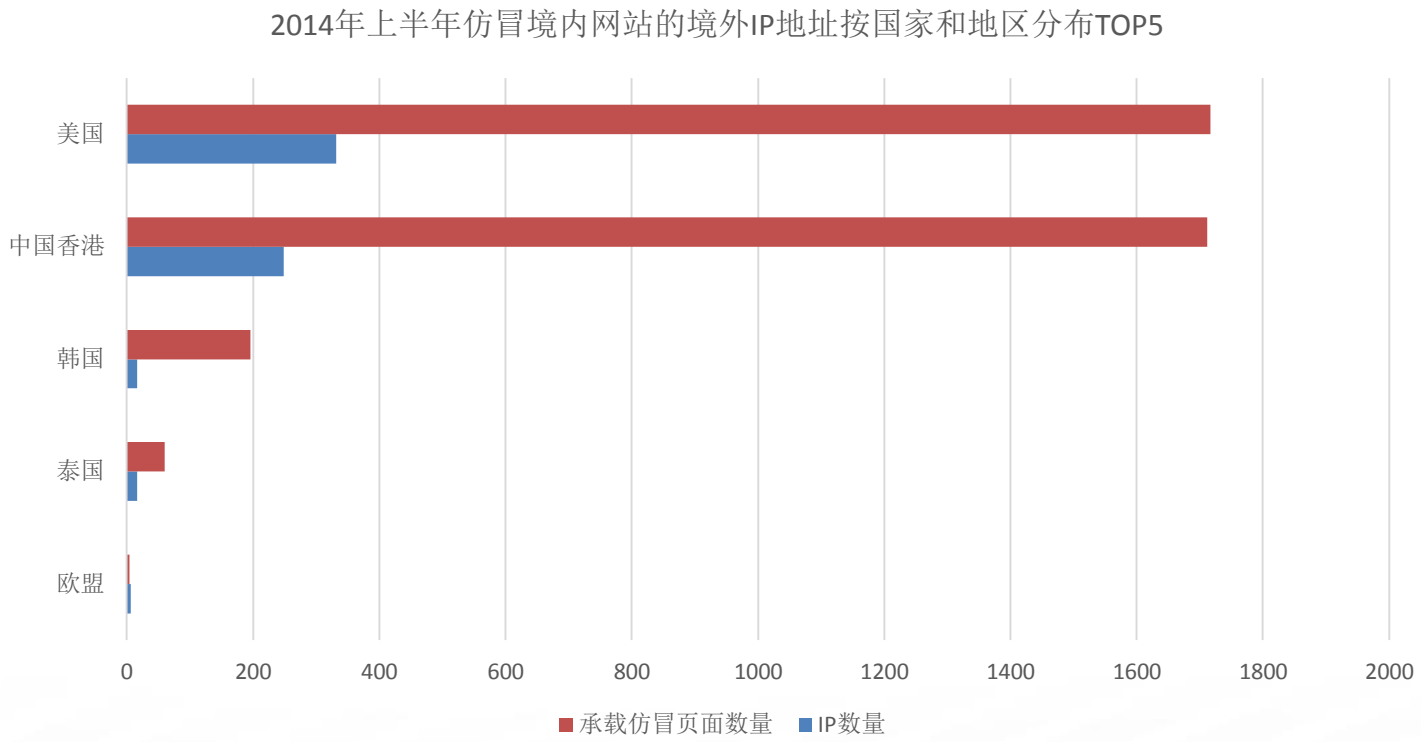
大量境外攻击难以处置追溯

- 上半年被植入后门的网站中84.8%被境外控制



大量境外攻击难以处置追溯

- 上半年针对境内网站的钓鱼站点90.4%位于境外

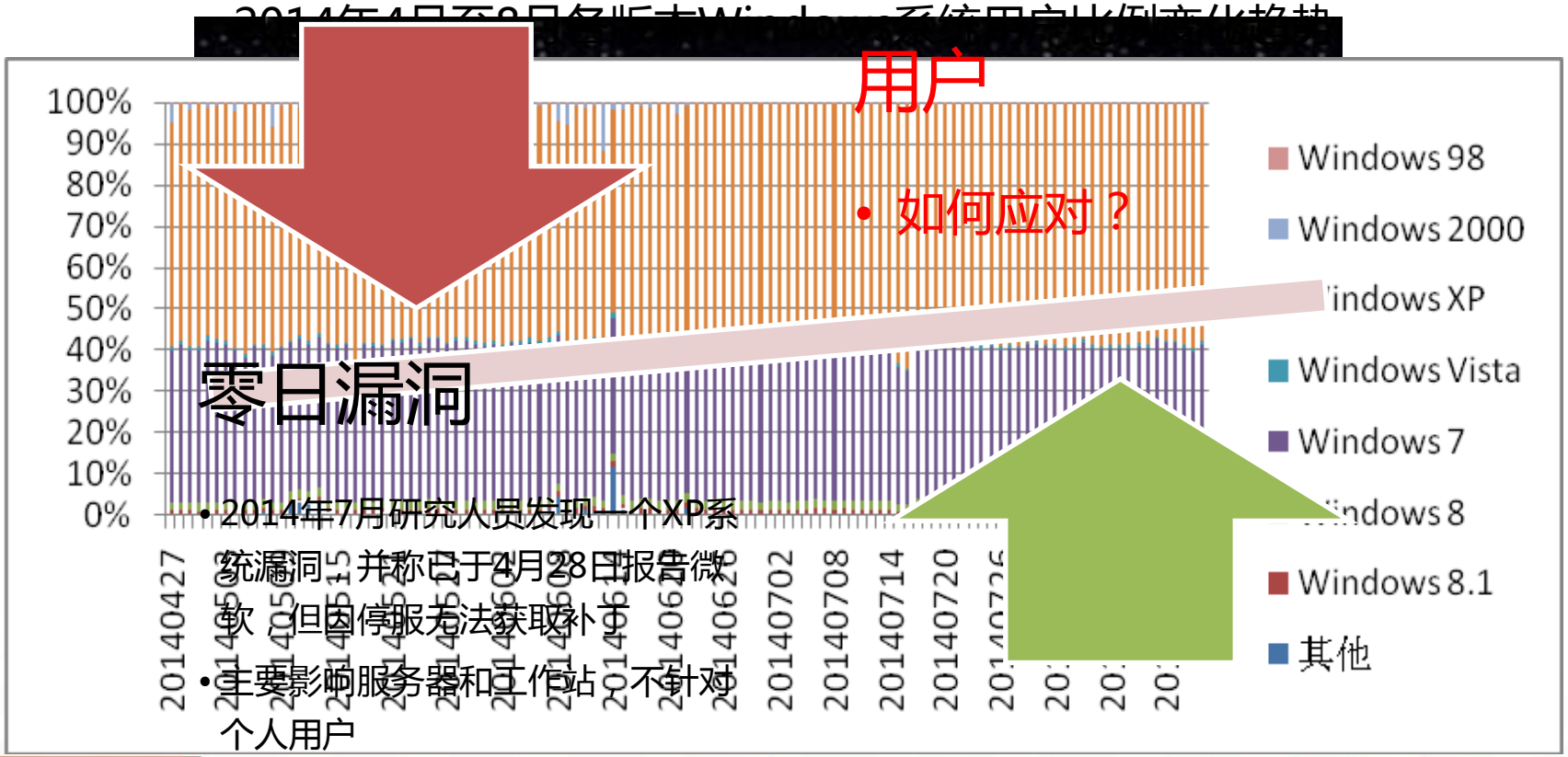


“一大波”黑客组织来袭

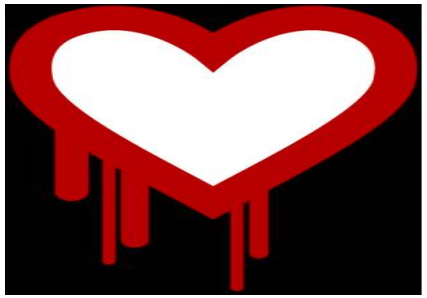

CHINA
YOU HAVE BEEN HACKED BY
#ANONCALAPAN
Official #ANONGHOST PH
Like Us on Facebook
https://www.facebook.com/Calapan.Legion.Anonymous.Calapan
TO CHINA - USE YOUR COMMON SENSE
COMMON SENSE
Spratly Island is "OURS"
Special Greetz :
#AnonCalapan Members
#Official AnonGhostPH Members
#AnonGhost Around the world
To all Filipino Hackers Around the world
./Calapan Legion
http://ghost-mirror.org
./The Greatest
CHINA, BACK-OFF FROM PANATA SHOAL!

XP停服引发“零日”风险

- 使用Windows XP的用户比例未明显减少



“心脏出血”漏洞震动互联网



- 4月8日，OpenSSL内存泄露漏洞（Heartbleed）震动整个互联网界。
- 据不完全统计，我国境内超过3万IP受影响。

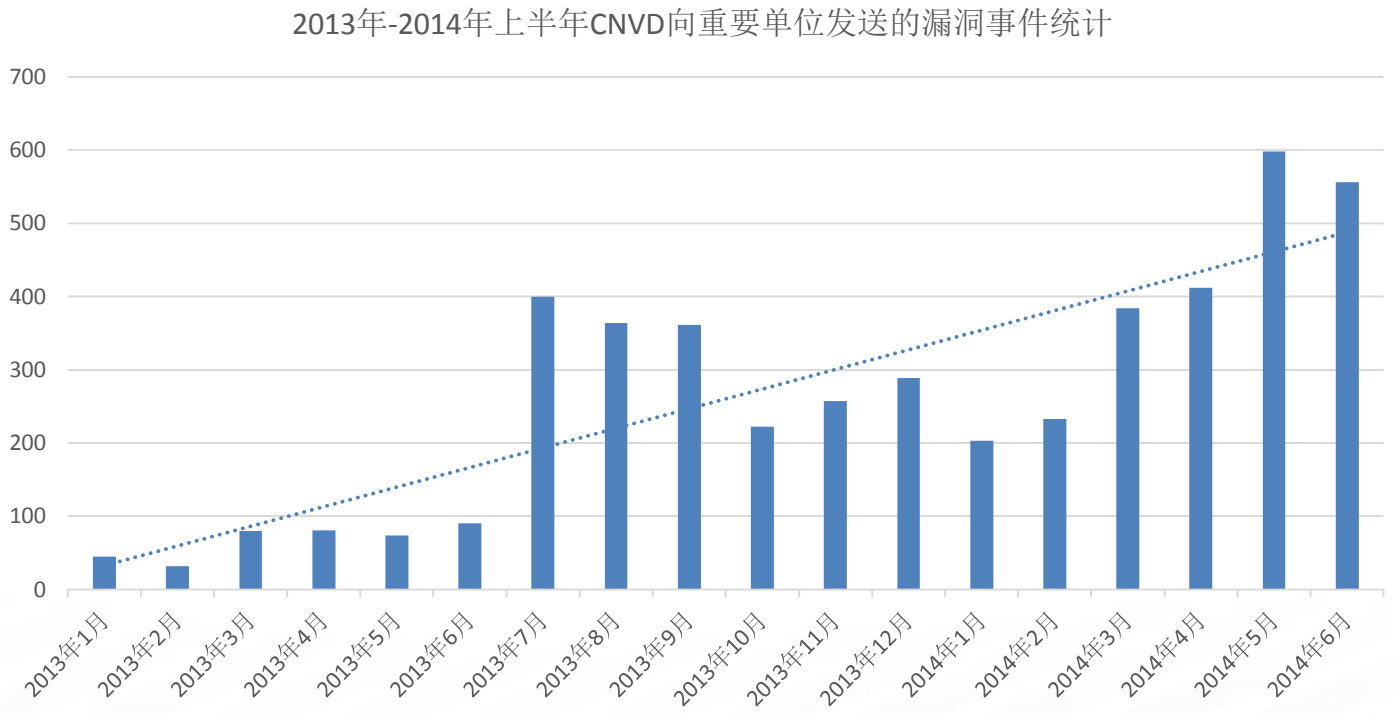
X.509证书	用户名和密码	即时通讯消息	电子邮件	重要商业文档	重要通信内容

网银	在线支付	电子邮件	即时通讯	VPN

政府	高校	银行	电商	邮件服务商	互联网站

涉及重要单位的漏洞事件增多

- 上半年通报漏洞事件数量已超2013年全年
  - 涉及政府机构、基础网络、重要信息系统等重要单位

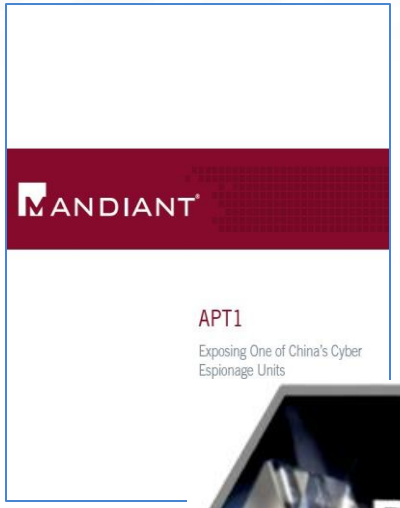


漏洞半衰期与威胁

漏洞举例	影响系统	未修复的漏洞比例	
BIND拒绝服务	DNS系统	1月后：93%	2月后：91%
Vxworks远程身份认证	网络设备	1周后：67%	1月后：65%
Ngnix文件解析	Web应用	半年后：70%	1年后：55%
OpenSSL信息泄露	应用软件	2天后：40%	至今：16%

题纲

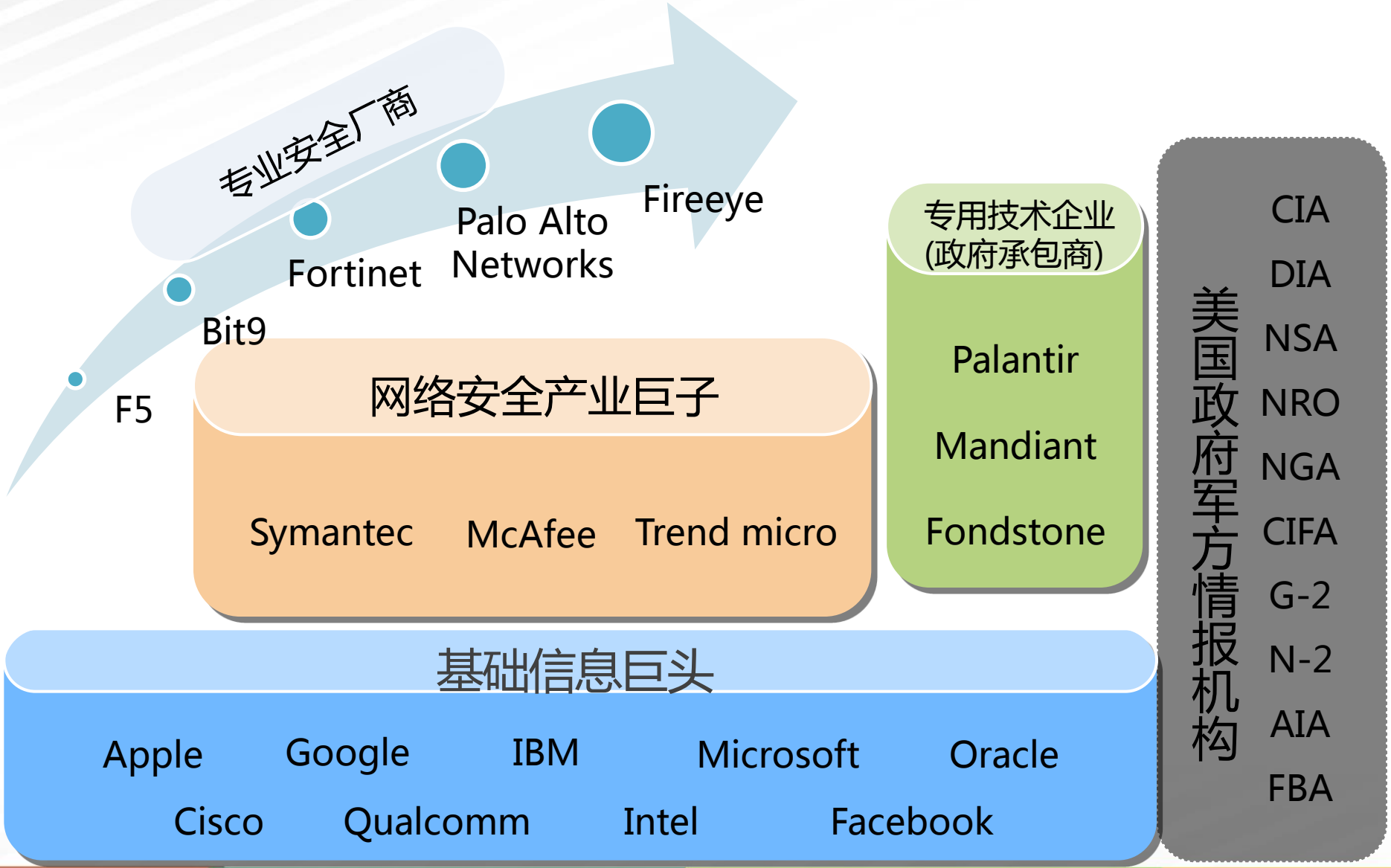
APT1和棱镜背后的两国能力差距



U.S.A	CHINA
拥有发现、威胁评估、追踪溯源、取证能力	追溯能力较弱、缺少精确案例和证据分析
拥有全面监管、精确制导能力	网络安全基础设施仍然薄弱、防渗透能力不足
有效协调安全厂商、技术机构、媒体，形成常态化优势	在技术标准、监管机制、产业联合引导不足，产业分工同质分散

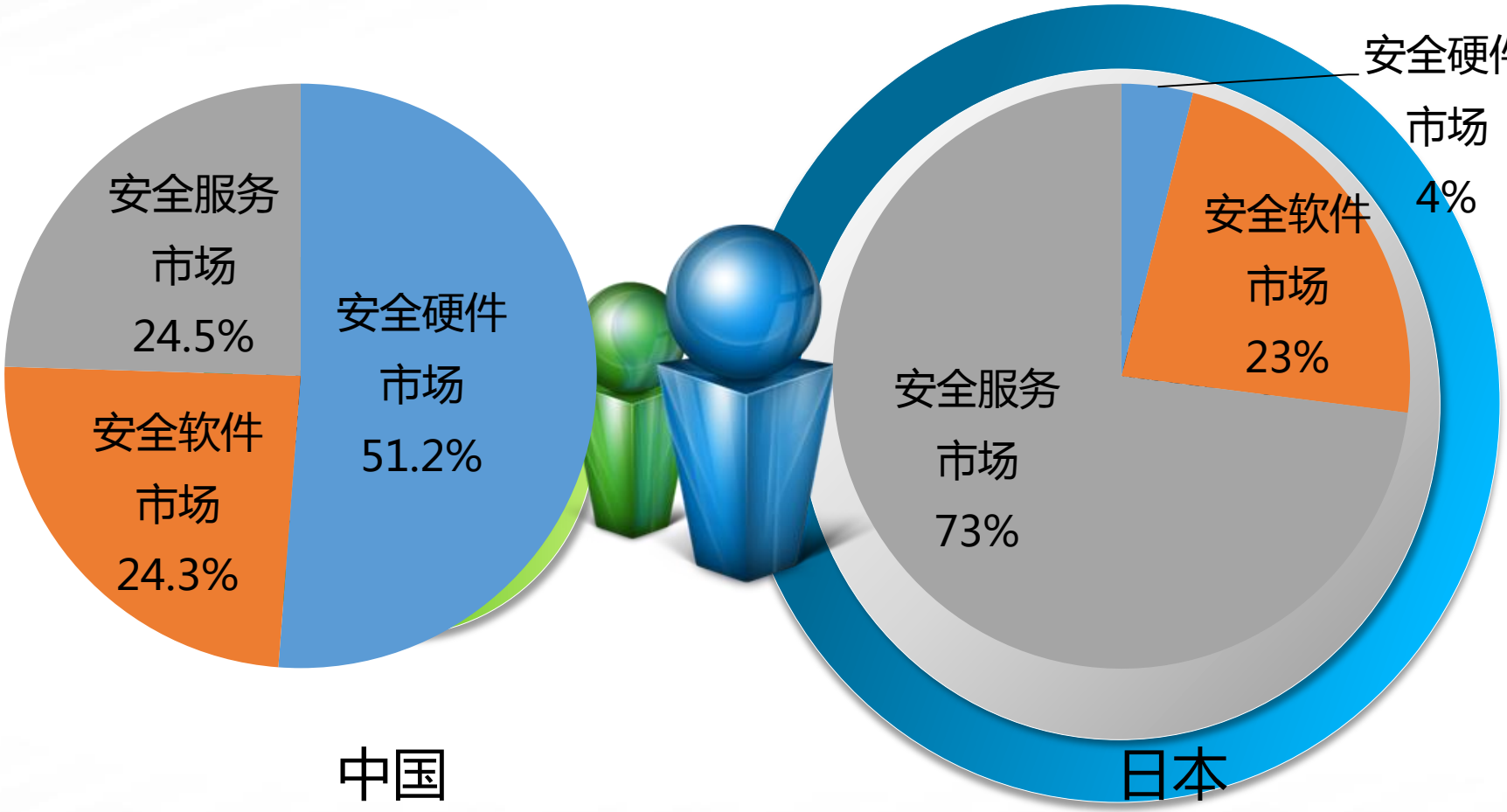
美国新兴网络
安全厂商的崛起

美国网络安全产业总体格局



美国反APT的“产业联盟”

国内外网络安全产业投入和结构对比



根据2012年IDC统计数据

人才储备存隐忧

FireEye

Symantec.

RSA

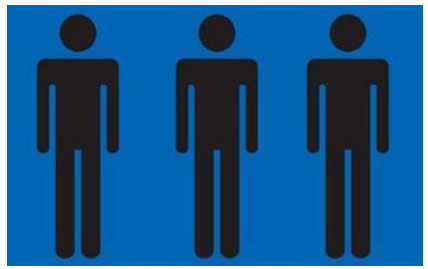
境外

行业

游戏应用

移动互联网

黑客地下产业



学历认定为主

实践衔接少

高校

职业

资格认定为主

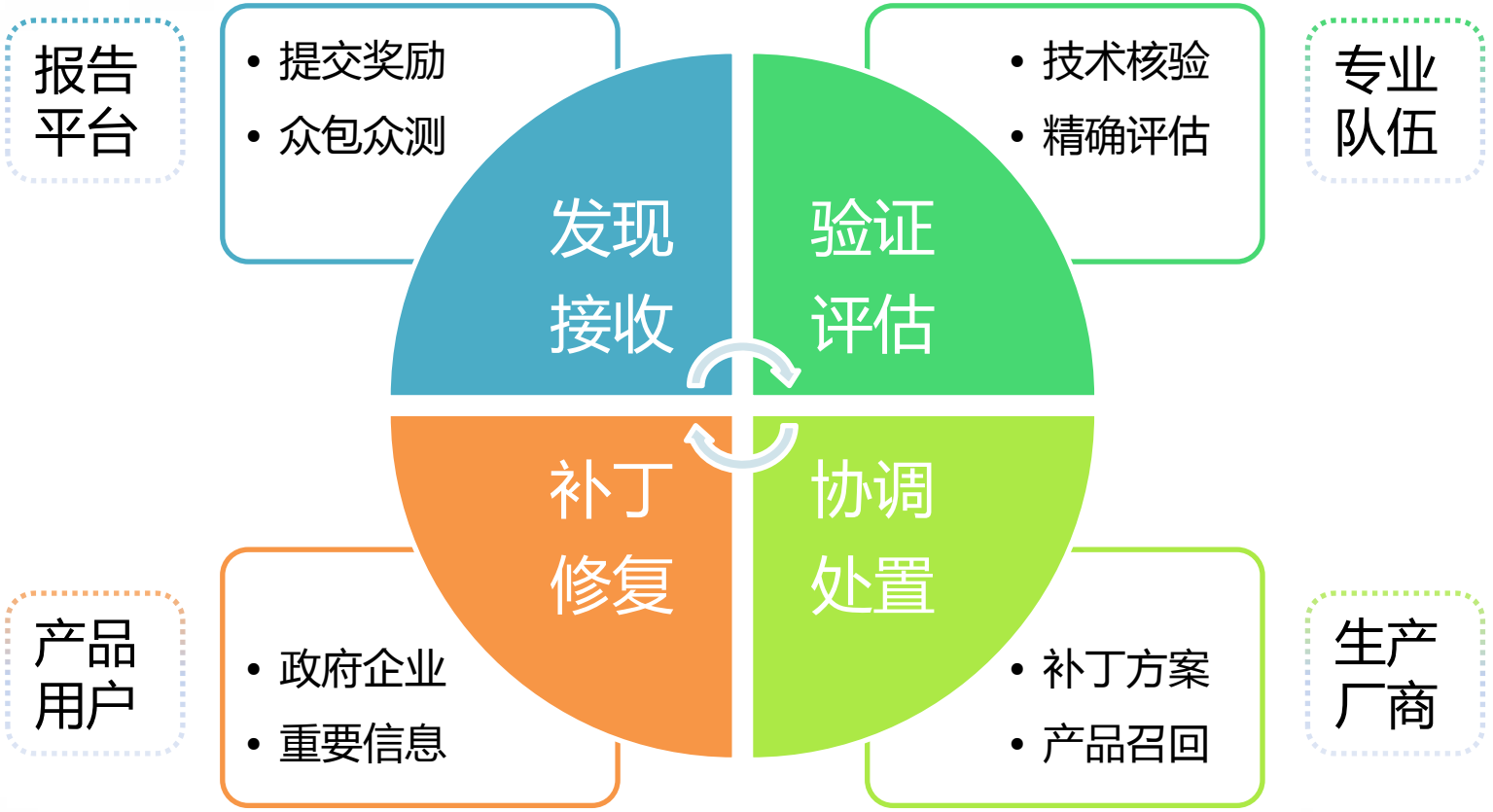
技术更新慢

题纲

广泛建立合作体系

与境内711家单位建立合作机制

打造漏洞整体防御体系

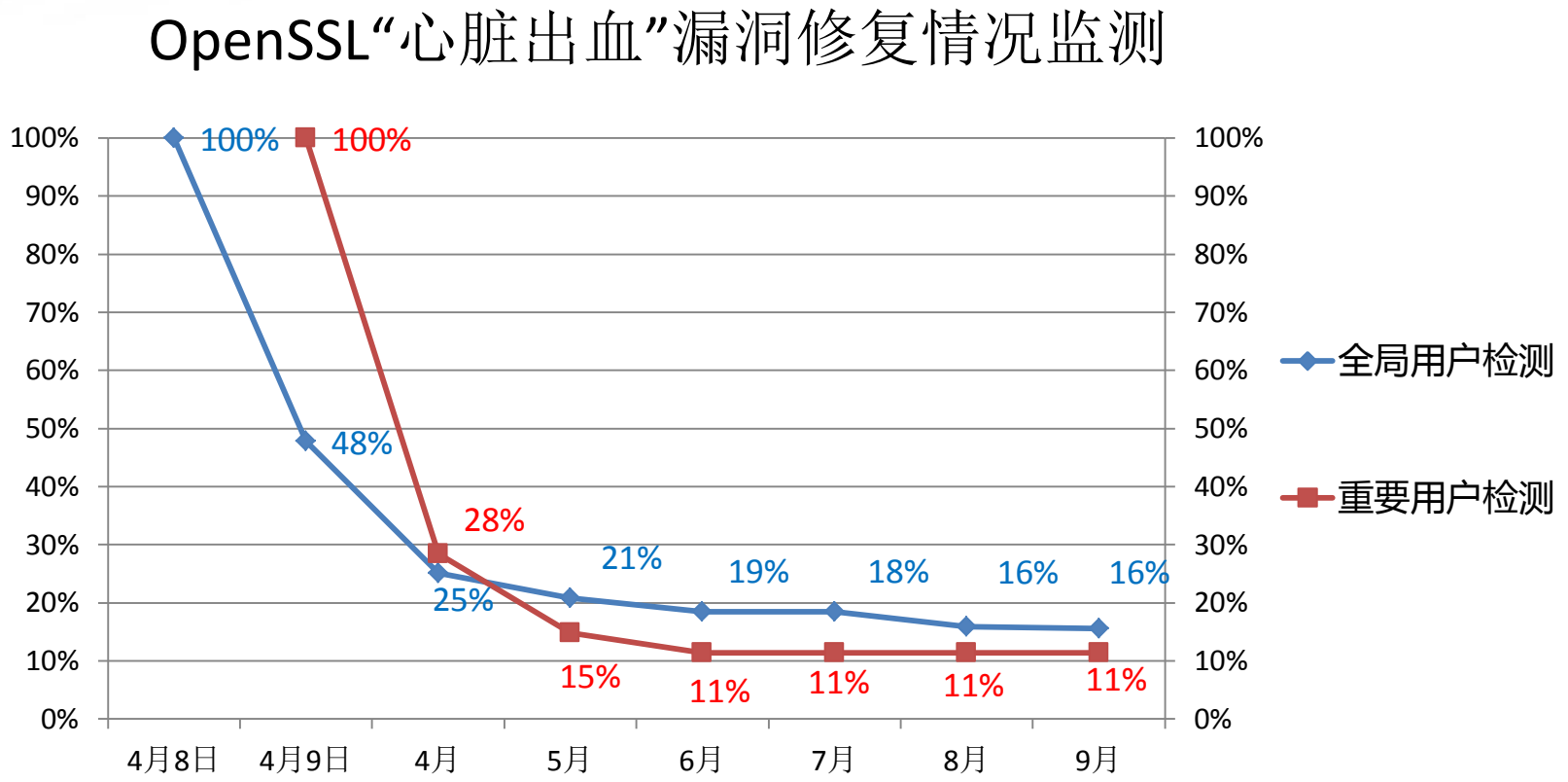


有力监管　业界联盟　环节对抗

CNVD工作实践

漏洞发现和报送	支撑政府和重要部门	监督和协调厂商
激励机制、报送接口、2000+白帽子群体	日均处置50-100起漏洞事件	建立与700+厂商协作渠道，开展持续有效监督

OpenSSL漏洞修复情况对比



打造反网络病毒联盟

中国反网络病毒联盟
Anti Network-Virus Alliance of china

举报报送 → 黑白名单 → 联合打击

举报报送

CN ERT/CC 国家互联网应急中心 移动互联网恶意程序报送平台 https://msample.anva.org.cn

1、打造恶意程序举报平台，面向企业与个人，在线实时权威鉴定；

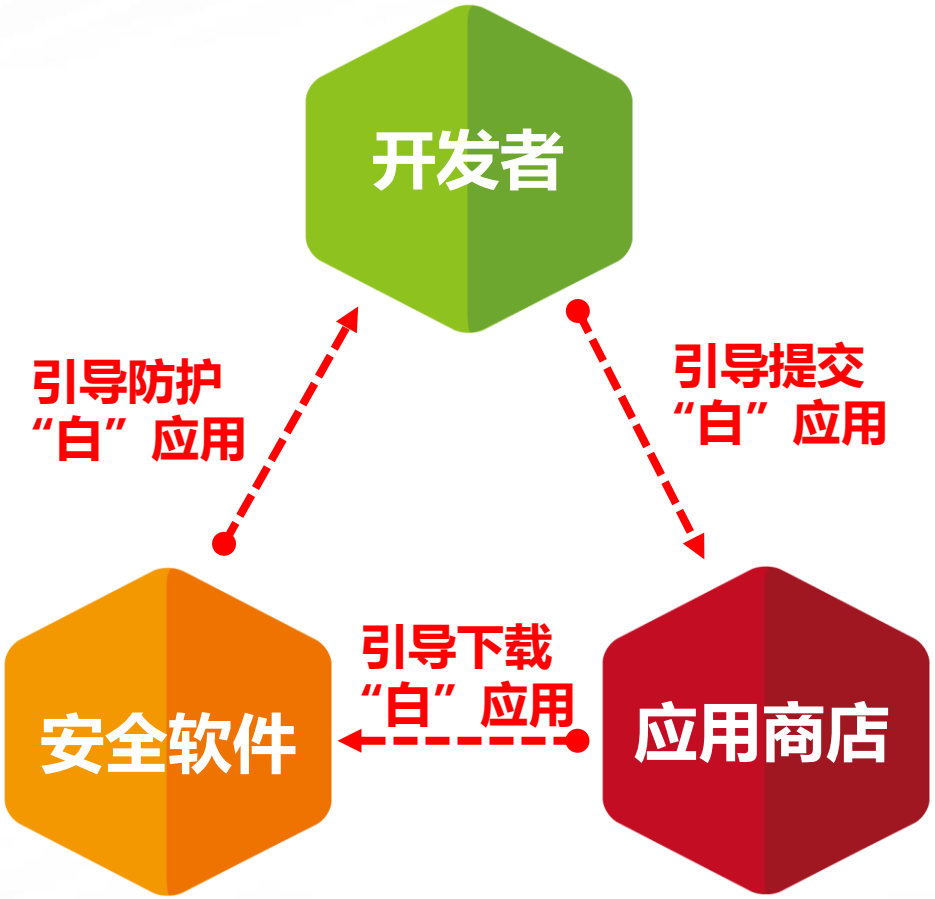
2、同时提供在线文件检测和URL文件链接检测；

发布黑名单

1、发布PC恶意程序、移动恶意程序、恶意URL地址等黑名单；

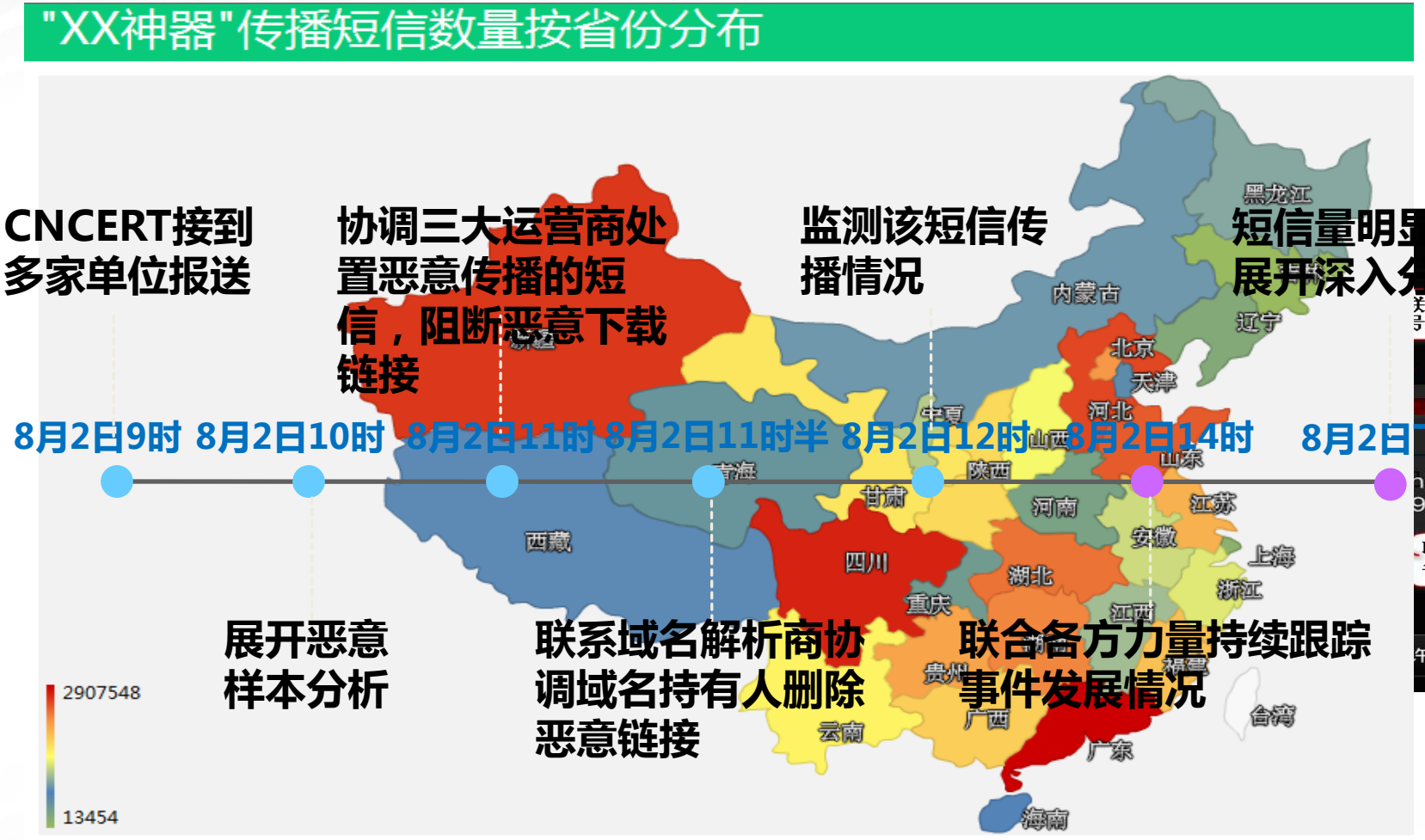
2、提供公共接口，实现同步、查询、统计等功能。

发布移动互联网白名单



将网民引向“白色”的安全生态环境！

联合处置——案例：“XX”神器



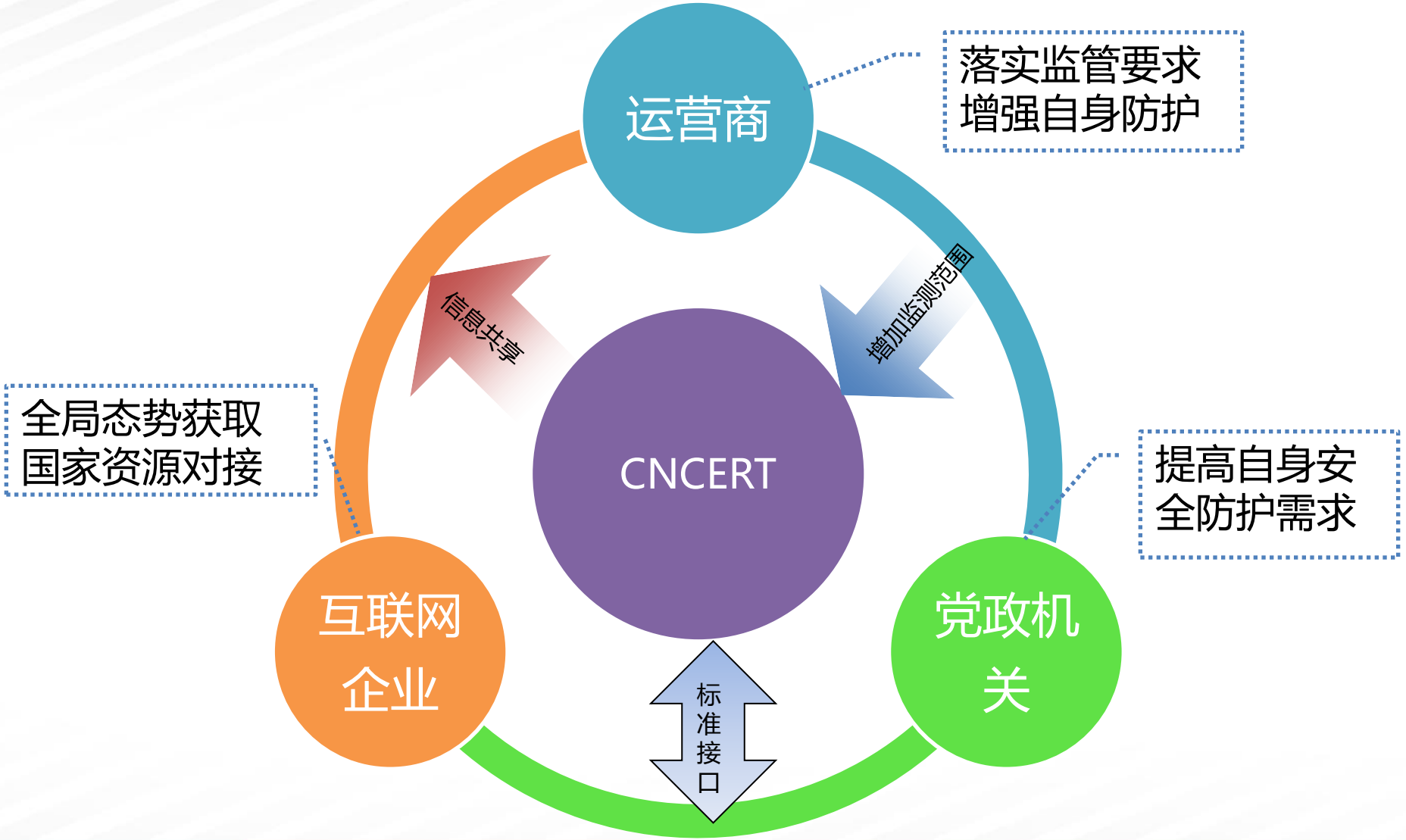
短时间内全国短信传播量突破1000万，广东、四川、新疆成为重灾区

我们的思路

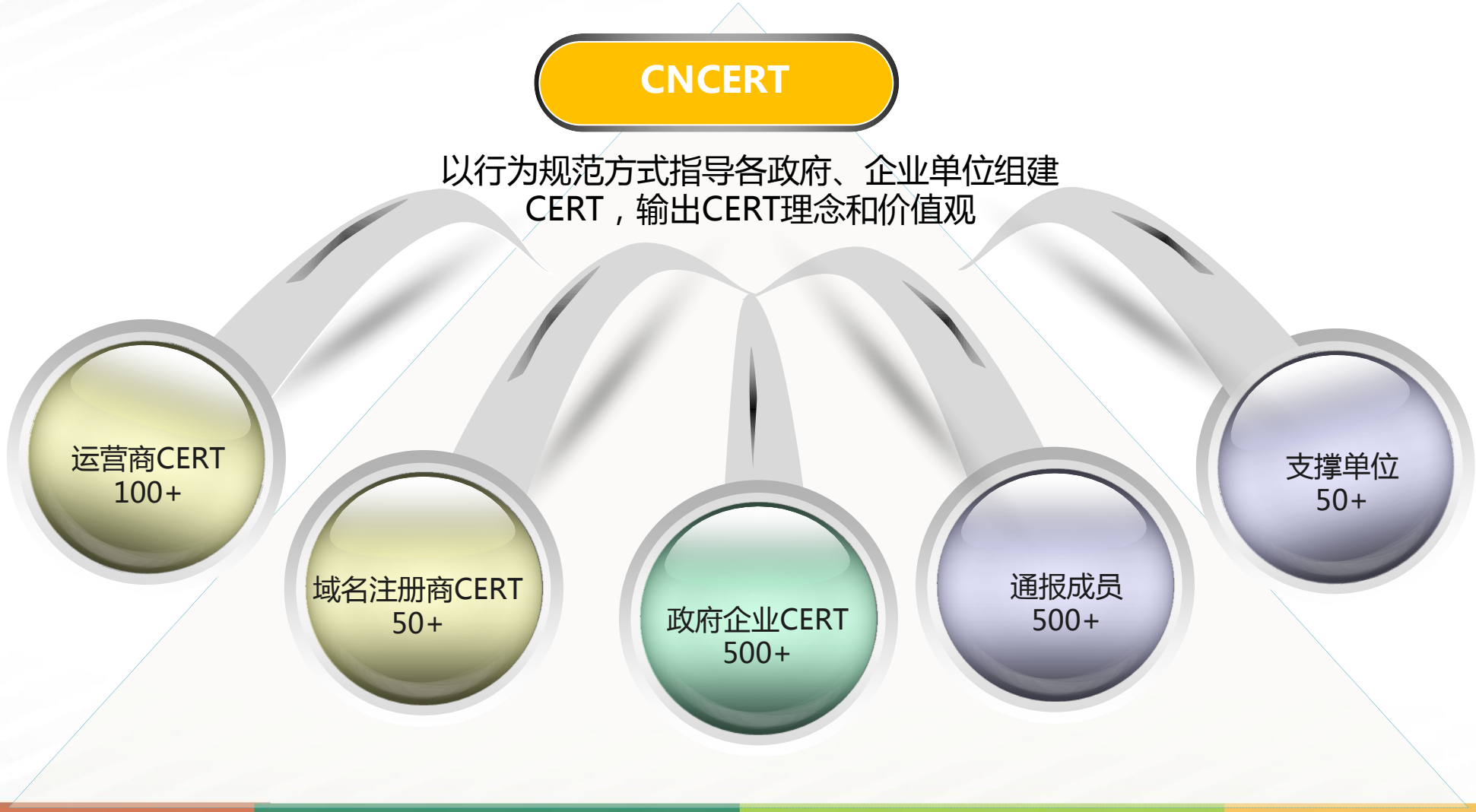
携手共建保障
我国网络安全
自增长体系

联网
维

打造自增长技术体系


运营商
落实监管要求
增强自身防护
信息共享
增加监测范围
全局态势获取
国家资源对接
CNCERT
提高自身安全防护需求
互联网企业
党政机关
标准接口

打造自增长合作体系


CNCERT
以行为规范方式指导各政府、企业单位组建CERT，输出CERT理念和价值观
运营商CERT
100+
域名注册商CERT
50+
政府企业CERT
500+
通报成员
500+
支撑单位
50+

打造人才自增长体系


产业扶持
重点引进
领域牵引
国家
战略
产权联合
产业
自育
精细分工
人才
自增长
学科复合学制
职业
教育
产业高校联合
职业体系对接
社会
组织
攻防竞赛
技能培训

打造自增长的网络安全热带雨林

资源共享　　标准化　　合作体系　　协同发展

谢谢！