法律有国界，网络安全无国界

新形势下的白帽子成长与漏洞发现报告机制探讨

白健

补天漏洞响应平台

一、我国目前网络安全相关法律

法律很明确

犯罪 - 刑事处罚：《刑 法》第285、286条

违法 - 治安处罚：《治安管理处罚法》第29条

处分 - 从业禁止：《网 络 安 全 法》第27条

后果如何

对于国内：刑事处罚//治安处罚//从业禁止，后果很严重

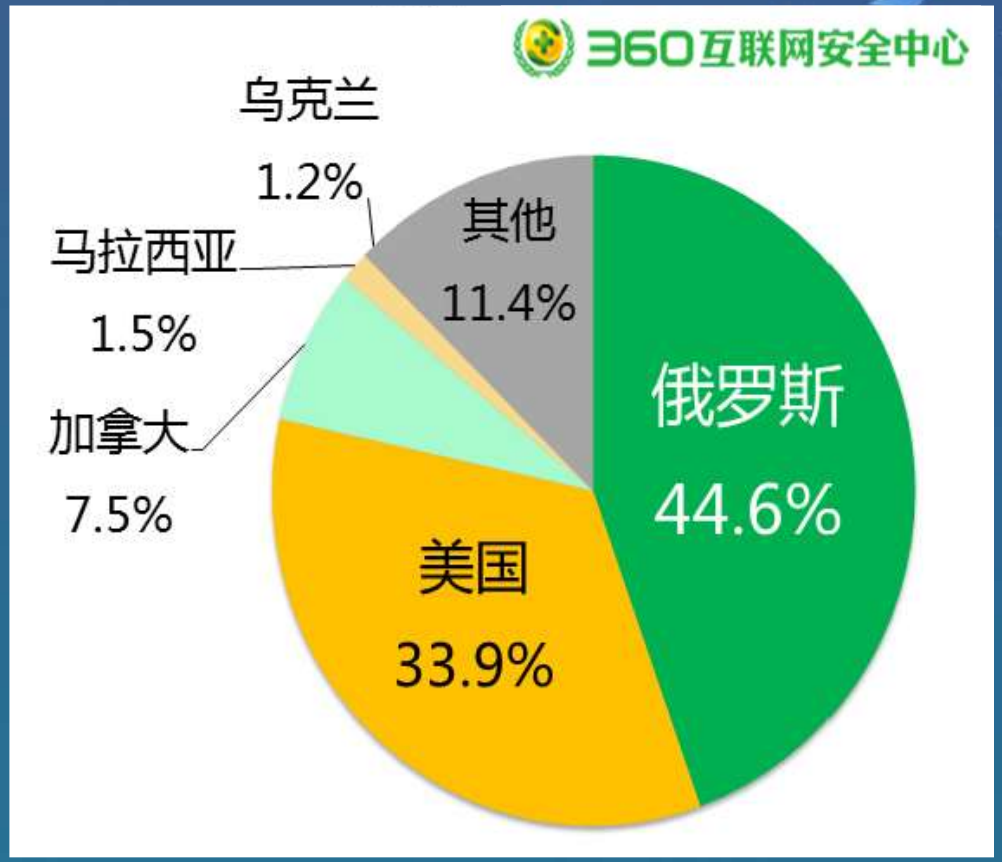
对于国外：无法溯源，无法惩罚

二、中国面临的境外网络安全威胁分析

中国网站受到境外IP攻击情况

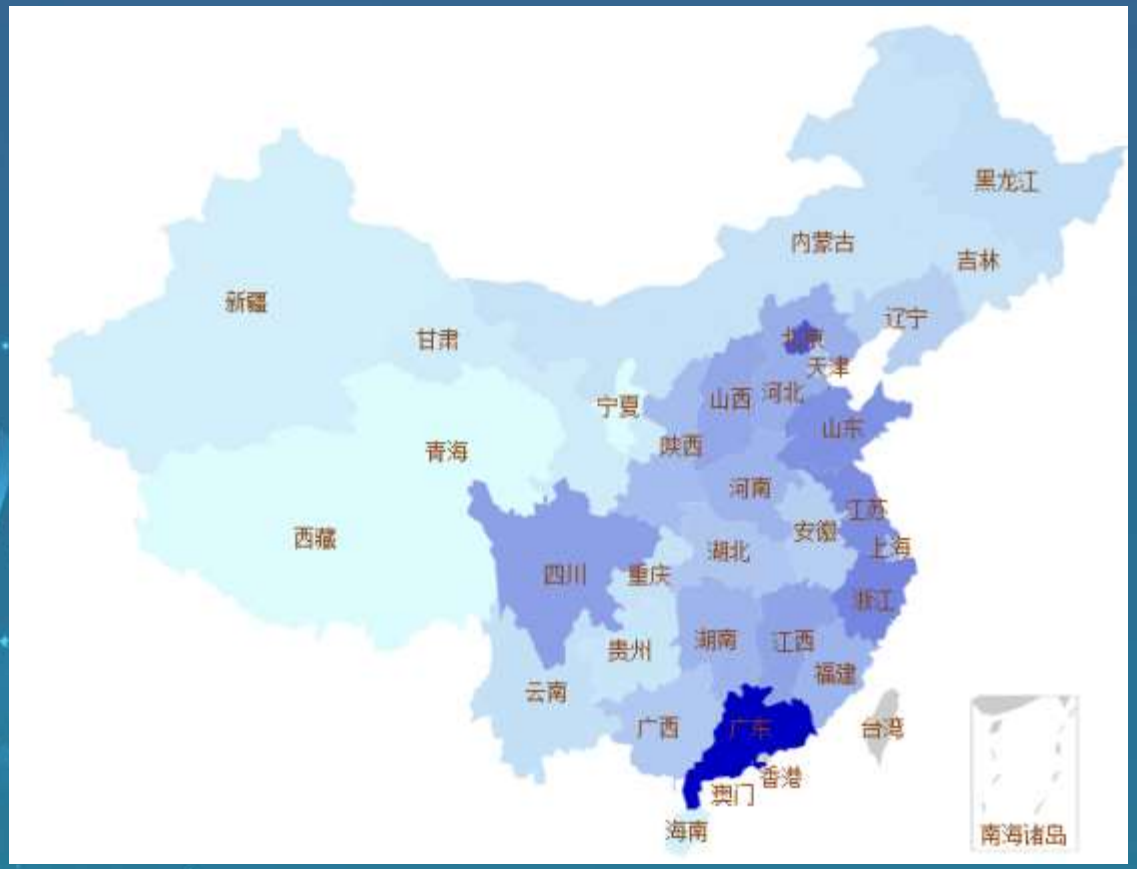
根据360互联网安全中心的报告，

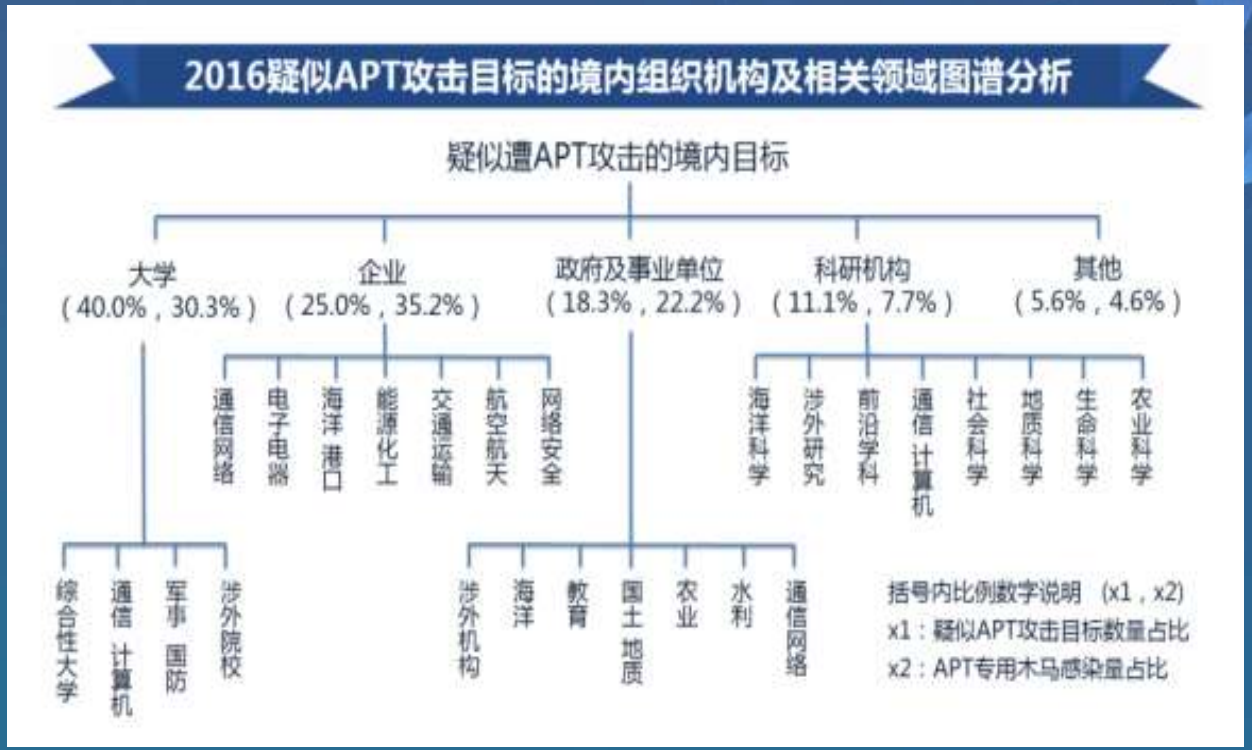
2016年境外IP地址对我国网站的攻击次数高达3.86亿次!



中国APT攻击受害情况

- 360持续追踪的有36个APT组织，基本覆盖国内全部省份。





- 科研、政府、军事、基础设施相关都是APT攻击的受害重灾区。

永恒之蓝

2017年5月12日晚2017年4月泄露的NSA黑客数字不法分子利用武器库中“永恒之蓝”工具发起蠕虫病毒攻击进行勒索，也成WannaCry病毒

截止到5月16日勒索软件攻击了100+国家。据360威胁情报中心监测，至少有29000+个机构被感染。

受害主机中招后，病毒就会在受害主机中植入勒索程序，硬盘中存储的文件将会被加密无法读取。攻击者要求支付300美元进行解密。

网络战越来越激烈，

网络恐怖主义的潘多拉盒子也已经打开。

我们该怎么办？

攻防对抗的核心就是：

安全人才培养和漏洞的收集利用！

三、国际漏洞报告领域发展现状

美国漏洞平台代表

Hackerone——面向全球的漏洞发现与报告平台

Synack——创始人NSA背景，封闭众测

美国HACK大事件

2016.4 .18-5.12　Hack the Pentagon

参与人数　1400名
有效漏洞　138个
发放奖金　7.12万美元

2016.11.30-12.21　Hack the Army

参与人数　500+名
有效漏洞　118个
发放奖金　10万+美元

2017.5.30-6.23　Hack the Air Force

参与人数　272名（33名外籍）
有效漏洞　207个
发放奖金　13.34万美元

美国法律环境

美国《网络安全法案》

（一）授权：701条 “获得第三方授权”

（二）合法限制：702条

★披露的目的仅限于保护目标信息系统及其数据的安全；

★在披露相关安全威胁时确保不泄露相关数据中的个人隐私；

★不将待披露的威胁用于获取不正当的竞争优势

VEP：《商业与政府信息技术和工业控制产品或系统的漏洞裁决政策和程序》（Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process）

PATCH：《2017反黑客保护能力法案》（Protecting Our Ability to Counter Hacking Act of 2017）

现状

1、我们使用的绝大多数软件都源于美欧；

2、美国人在面向全球收集各种漏洞；

3、美国政府和军方与漏洞平台都有深度合作；

4、美国政府非常重视漏洞平台的发展。

四、国内漏洞平台的战略价值

安全漏洞（内在脆弱性）+外部威胁=信息安全风险

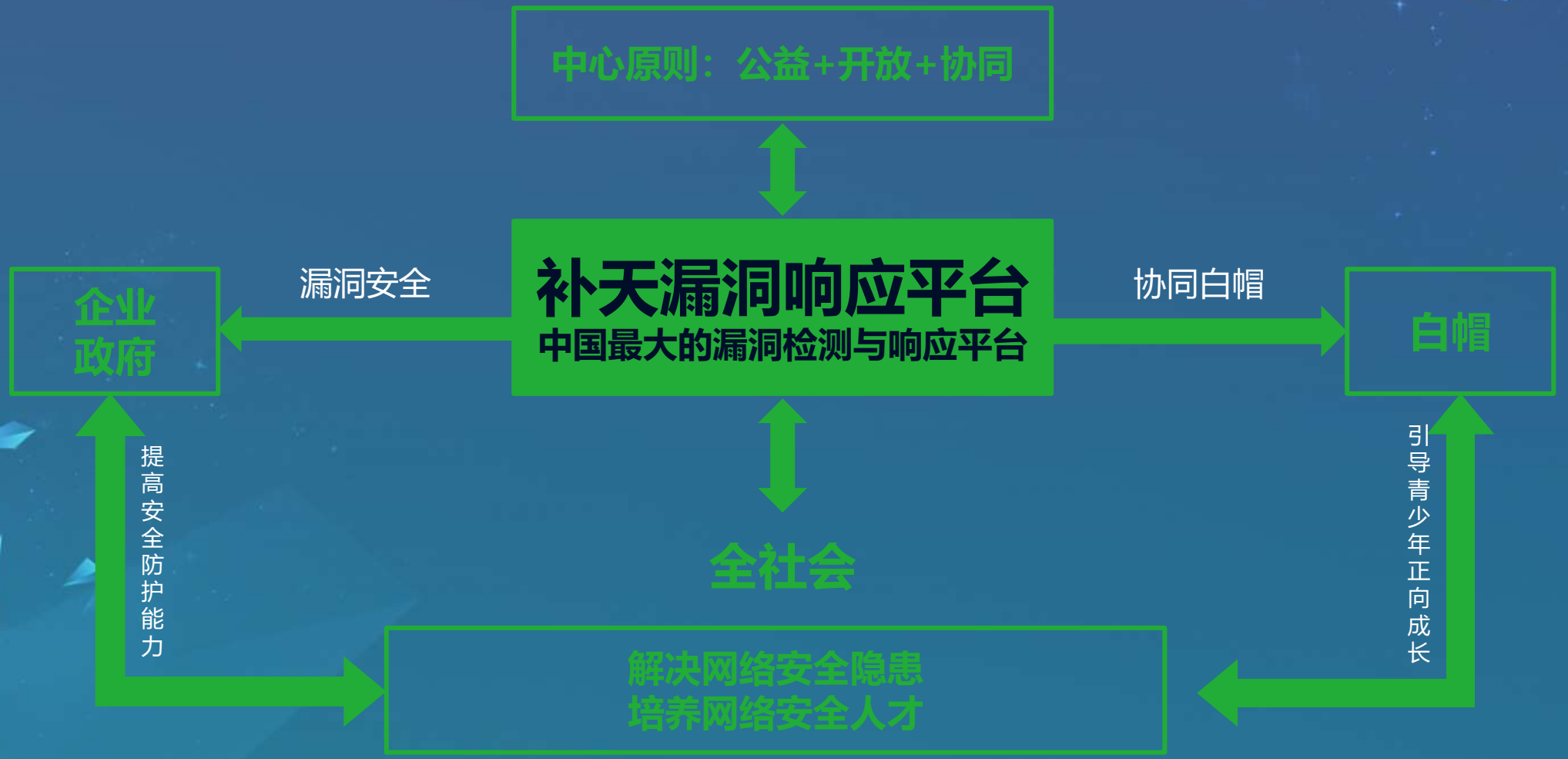
- 可利用性
- 难以避免性
- 普遍性
- 长期存在性

双重法律属性

安全漏洞具备的**非传统缺陷和资源双重法律属性**导致对其发现所产生的行为后果具有多重法律意义，无论是传统缺陷理论，还是法律单一惩治，都不能体现和承载双重属性所展现的复杂性和多样性；

安全漏洞发现的立法建议：一方面需最大限度减少利用安全漏洞产生的危害，提高应对网络攻击的防御能力，惩治危害网络安全的行为；另一方面也要通过政策引导和立法的持续性保持安全漏洞的合法发现、跟踪、创新与突破。

补天平台整体逻辑


中心原则：公益+开放+协同
补天漏洞响应平台
中国最大的漏洞检测与响应平台
企业
政府
漏洞安全
协同白帽
白帽
提高安全防护能力
引导青少年正向成长
全社会
解决网络安全隐患
培养网络安全人才

补天
漏洞响应平台

使命
网聚安全力量
协同保护全社会网络安全

愿景
让全中国网络实现漏洞的
及时发现与快速响应

公益

开放

协同

SRC
免费构建企业专属的应急响应平台

- 企业自主悬赏，平台白帽子竞争式发现与报告
- 企业自助调整测试范围及服务白帽资源
- 专业的SRC安全运营支撑团队，解决后顾之忧

众测
基于众包模式的攻防驱动互联网安全测试

- 服务内容量身定制，白帽专家全方位诊断
- 专业修复方案，及时回检确保漏洞修复，彻底消灭漏洞
- 技术与管理控制并行，风险控制机制完善

漏洞情报
更接地气的精准行业情报，为企业争取更多响应时间

- 做好网络空间的“朝阳群众”，提前预知风险，提前防范于未然
- 人是安全的尺度，将企业的安全运营能力扩展到云端，协同处置未知风险
- 先人一步，化被动防御为积极防御，降低运维成本

补天平台战略价值

积极响应国家战略

保护企业网络安全

正面引导安全人才

五、真爱必然克制

坚守正义

“向后转肯定是个不归路”

“直面问题，迎接挑战”

“如何做的更好”

一个原则

遵从法律框架，规范技术手段

守住底线

恶意黑客 X

逃避打击 X

以安全测试为目的所实施的漏洞挖掘有一定的合法行为空间 √

积极争取法律空间

中国互联网协会《漏洞发现与报告守则》（草稿）

按照对信息系统**机密性、可用性、完整性**等三方面要素的影响评估，漏洞风险发现与技术验证应遵循无害化原则：

（一）信息系统机密性无害化验证指导场景：

★可实现非授权访问或用户权限越权，在完成非授权逻辑、越权逻辑验证时，不应再获取和留存用户信息和信息系统文件信息；

★可执行数据库查询条件，在获得数据库实例、库表名称等信息证明时，不应再查询涉及个人信息、业务信息的详细数据；

★可获得系统主机、设备高权限，在获得当前用户系统环境信息证明时，不应再获取其他用户数据和业务数据信息。

（二） 信息系统可用性无害化验证指导场景：

（三） 信息系统完整性无害化验证指导场景：

一些建议

法律法规要加强学习

技术操作要规范

交友要谨慎

不忘初心，守护网络安全！

THANKS

Thanks for watching