网络安全现状、法律、及市场

李雨航 (院士级教授) Prof. Yale Li, XJTU Fellow

国际云安全联盟CSA全球总顾问/亚太区代主席

华为全球网络安全首席专家/终端安全首席架构师

全球网络犯罪激增

根据PWC连续几年发布的网络安全调查报告，2014年全球所有行业检测到的网络攻击达到4,280万次，同比增长了48%。

2015年，中国内地及香港企业检测到的信息安全事件暴增了5倍！2016年，这个数据又攀升了两倍。

客户信息、企业内部数据和知识产权成为黑客主要窃取的对象。

每年网络犯罪活动为世界经济带来的损失超过4450亿美元。在中国，这个地下黑产业链的规模估计超过千亿元人民币。

2019年，网络犯罪造成经济损失将达2.1亿美元。

网络勒索

受到勒索软件攻击的国家分布

Symantec Inc

勒索软件攻击的成本低、产出高。而且攻击已从面向个人的攻击快速转向了医院、政府机构、企事业单位等各行业的IT基础设施。 。

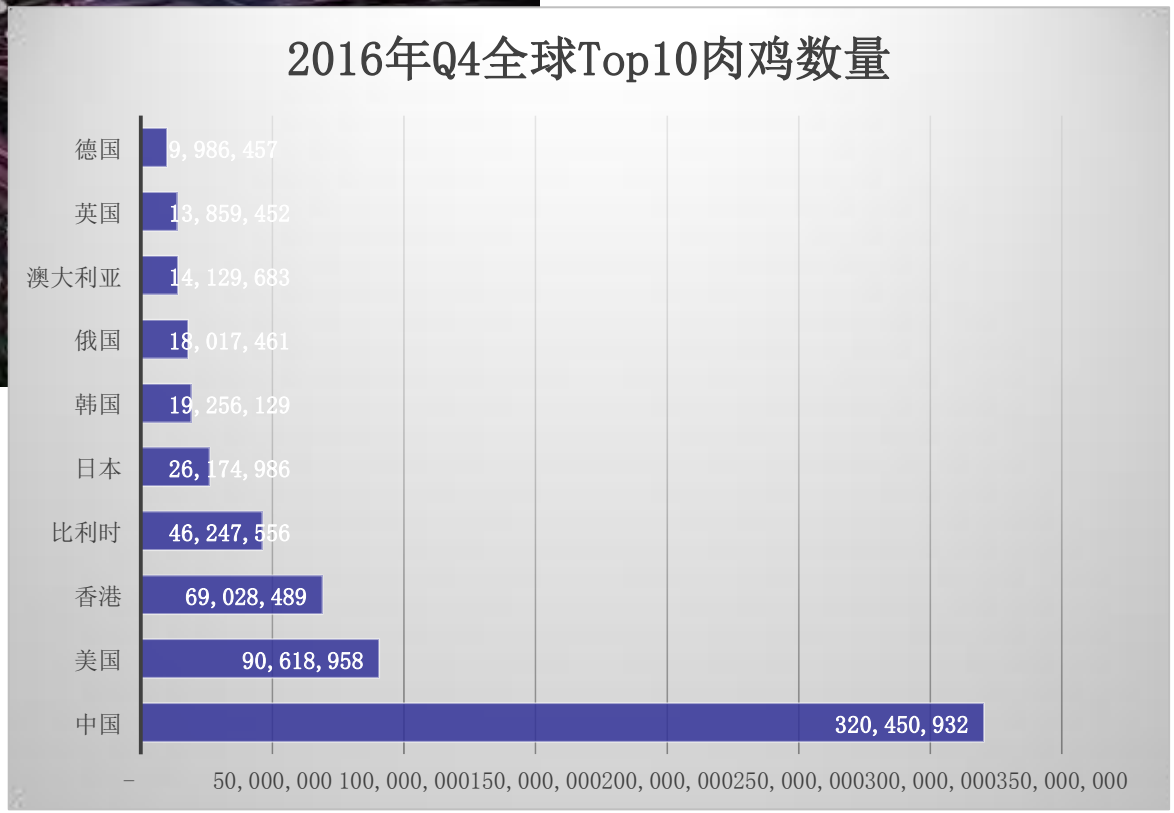
勒索软件已成为2016年增长最快的网络安全威胁， 上半年勒索软件数量即暴增了172% 。

2017年5月， 150个国家遭WannaCry勒索病毒攻击。

DDoS攻击

对于世界上的每一个机构组织，DDoS攻击已成为最危险的网络威胁之一。

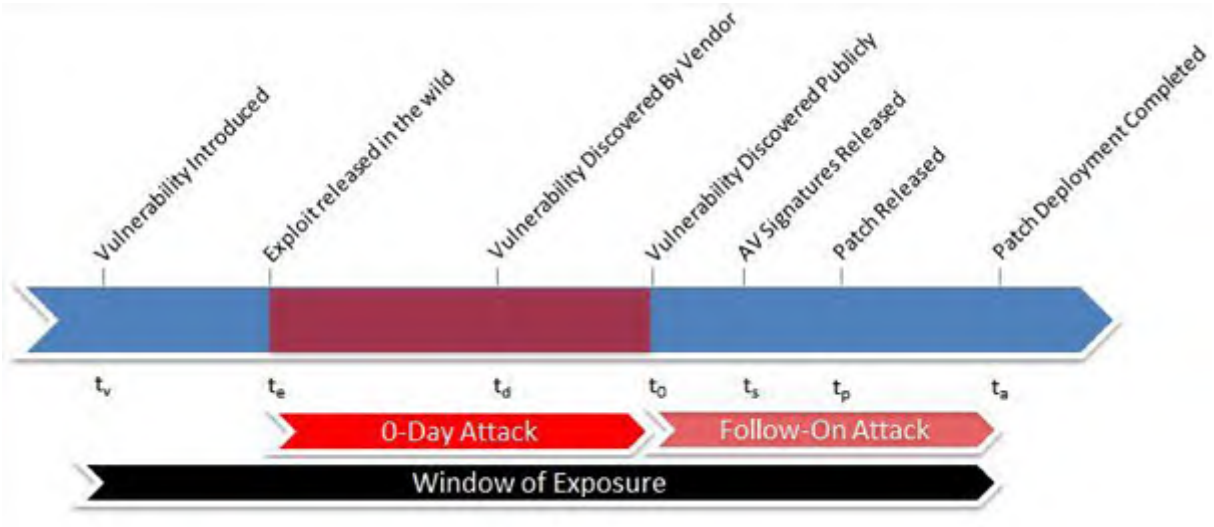
去年Q4，200Gbp以上的攻击事件大幅增加，攻击频率也增长了152%。



2016年10月21日上午，美国东海岸包括纽约时报在内的几大网站的DNS服务器，遭遇了来自物联网终端肉鸡的DDoS攻击，导致网站无法访问。

NEXUSGUARD

Zero-Day攻击



“每年增长1110亿行新的软件代码，使得应用攻击面不断扩大”。基于签名的恶意代码防护和漏洞检测不能有效防范Zero-Day攻击。

根据IBM黑鸭子估计，在一般的商业应用中，百分之30的代码为开源代码。

在2016前11个月， Adobe产品发现135个漏洞，微软产品发现76个漏洞。与此同时，苹果产品零日缺陷的数量比上一年翻了一番，从25个上升到了50个。

2015年黑客利用漏洞入侵了波兰航空公司的IT系统，导致该航空公司取消了20趟航班，1400名乘客受到影响。

概览 - 全球网络安全法律

- **美国：**自1978年以来，美国先后出台130多项涉及互联网管理的法律法规，互联网监管体系主要包括立法、司法和行政三大领域和联邦与州两个层次，既有针对互联网的宏观整体规范，也有微观的具体规定，著名法律例子：

  - 1996年《电信法》，明确将互联网世界定性为“与真实世界一样需要进行管控”的领域，它主要涉及保护国家安全、未成年人、知识产权及计算机安全四个方面。2001年《爱国者法案》，美国安全部门能以反恐为由窃听民众的电话通话内容和互联网通信内容。 2002年《联邦信息安全管理法》，全面保护美国政府机构信息系统的信息安全。

  - 2010年《网络空间作为国有资产保护法案》授权国土安全部对国家机构的IT系统进行维护监管，规定总统可宣布进入紧急网络状态， 2010年《网络安全法案》，对网络安全的人才发展、计划和职权、网络安全知识培养、公私合作进行规定。2010年《国家网络基础设施保护法案》规定，国会应在网络基础设施保护领域设置“安全线”，以保障美国的网络基础设施安全，并在政府和私营部门之间建立起网络防御联盟的伙伴关系，促进私营部门和政府之间关于网络威胁和最新技术信息的信息共享。

  - 2015年《网络安全法》作为《2016年综合拨款法案》中的一部分，已于2015年12月18日获得正式通过，成为美国当前规制网络安全信息共享的一部较为完备的法律，其中首次明确了网络安全信息共享的范围包括：“网络威胁指标”（Cyber Threat Indicator, CTI）和“防御性措施”（Defensive Measure）两大类，重点关注网络安全信息共享的参与主体、共享方式、实施和审查监督程序、组织机构、责任豁免及隐私保护规定等，并通过修订2002年《国土安全法》的相关内容，规范国家网络安全增强、联邦网络安全人事评估及其他网络事项。

- **欧盟：** 2016年出台首个网络与信息安全指导性法律 《欧盟网络与信息系统安全指令》，以加强欧盟各成员国之间在网络与信息安全方面的合作，提高欧盟应对处理网络信息技术故障的能力，提升欧盟打击黑客恶意攻击特别是跨国网络犯罪的力度。欧盟颁布的《一般数据保护条例》GDPR将于2018年5月25日生效，GDPR替换了1995年的欧盟数据保护指令，在当今快速的技术变化中，加强对欧盟所有人的隐私权保护，物联网的隐私权保护，并且简化数据保护的管理。

- **其它国家：** 英国，澳大利亚，日本，新加坡，印度等均有网络安全相关法规，50+国家制定了网络安全国家战略。

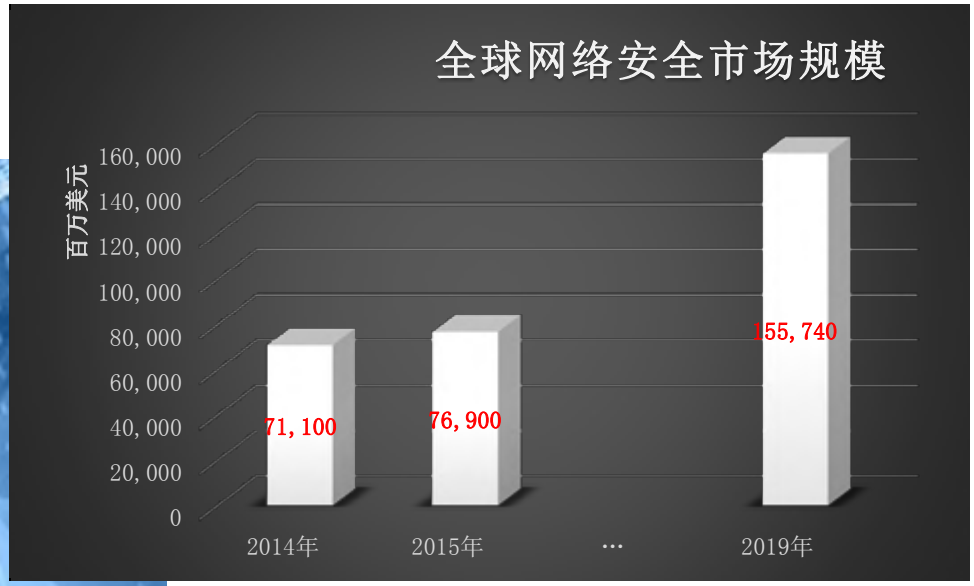
解读 - 中国网络安全法

2016年11月7日，我国通过《中华人民共和国网络安全法》，这是中国第一部有关网络安全方面的法律，2017年6月1日执行。

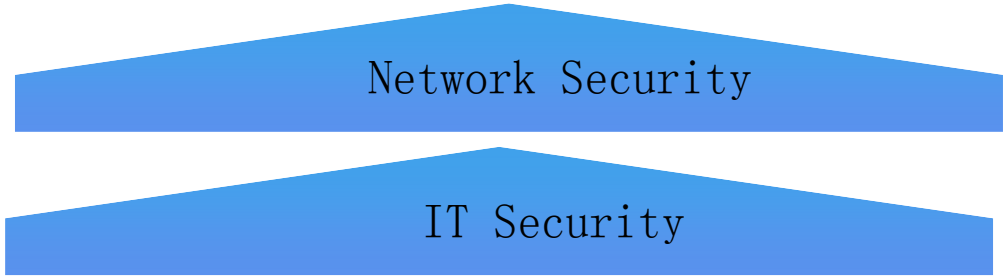
1. 提出了个人信息保护的基本原则和要求，相当于一部小型的“个人信息保护法”，使后续的相关细则、标准有了上位法；
2. 对网络产品和服务提供者提出了要求，针对的是当前一些企业任性停止服务或依靠垄断优势要挟用户、随意收集用户信息等问题；
3. 在反恐法确立的电信用户实名制基础上，规定了信息发布、即时通讯等服务的实名制要求，但这个实名是指“前台匿名、后台实名”，不影响用户隐私；
4. 规范了重要网络安全信息的发布服务，现在很多企业或机构都在发布漏洞、安全事件等信息，有一些不实信息造成了很大范围的不良影响，国家将制定这方面的规定；
5. 明确了网络运营者的执法协助义务，这是国际惯例，但我们以前多依靠“红头文件”，这一局面将改变；
6. 从法的层面规定了对网上非法信息的清理，使国家的互联网管理系统有了明确的法律依据；
7. 确立了国家关键信息基础设施保护制度，特别是规定了运营者的强制性义务，并为主管部门开展监管作了授权；
8. 建立了网络安全监测预警、信息通报和应急处置工作体系，有利于解决目前存在的多个部门各自发布预警通报、应急预案体系不完整不协调等问题；
9. 建立了通信管制制度，以支持重大突发事件的处置，但同时也将通信管制的权限严格限制在了国务院；
10. 进一步理顺了网络安全工作体制，规定国家网信部门负责统筹协调网络安全工作和相关监督管理工作。

外国技术公司必须提供运行其产品的软件源代码，设计细节，以便中国有关部门可以检查是否有黑客可以打入的安全漏洞或后门，中国的网络安全必须达到“安全和可控”的标准。 但是，居然有许多外国企业表示对这部法律感到不满，此前甚至还有40多家国际企业和技术团体致函中国政府，对网络安全法深表“关注”，微软、英特尔、IBM等对中国的新规定提出反对意见。

全球网络安全市场规模



– *CYBERSECURITY MARKET REPORT 2015*



预计到2019年，全球网络安全市场规模将超过1500亿美元。从2014年至2019年，5年全球网络安全市场复合年增长率(CAGR)将达到10.3%。

业务驱动安全 - 网络空间维度的扩展

数据互联

云

空间互联

移动办公

人人互联

社交网络

物物互联

物联网

新的安全挑战成倍增长 - 业务需要保障

技术驱动安全 – 业界的机会

人工智能和机器学习助力网络安全

软件定义安全以及网络安全功能虚拟化

大数据安全分析和威胁感知

云计算催化新的安全防护模式

三大领域、三个趋势

- 移动安全
- 业务定制化安全
- 云安全
- 智能感知化安全
- 物联网安全
- 整合平台化安全

案例 - 华为云安全实践（2017Q2）

华为企业云服务安全体系

基础设施安全

物理环境安全

网络安全

云平台安全

设备安全

了解详情>>

租户层安全

网络隔离

数据安全

权限管理机制

外部防御攻击

了解详情>>

运维安全

风险管理

安全信息与事件

特权账号

智能分析

了解详情>>

CSA的C-STAR认证

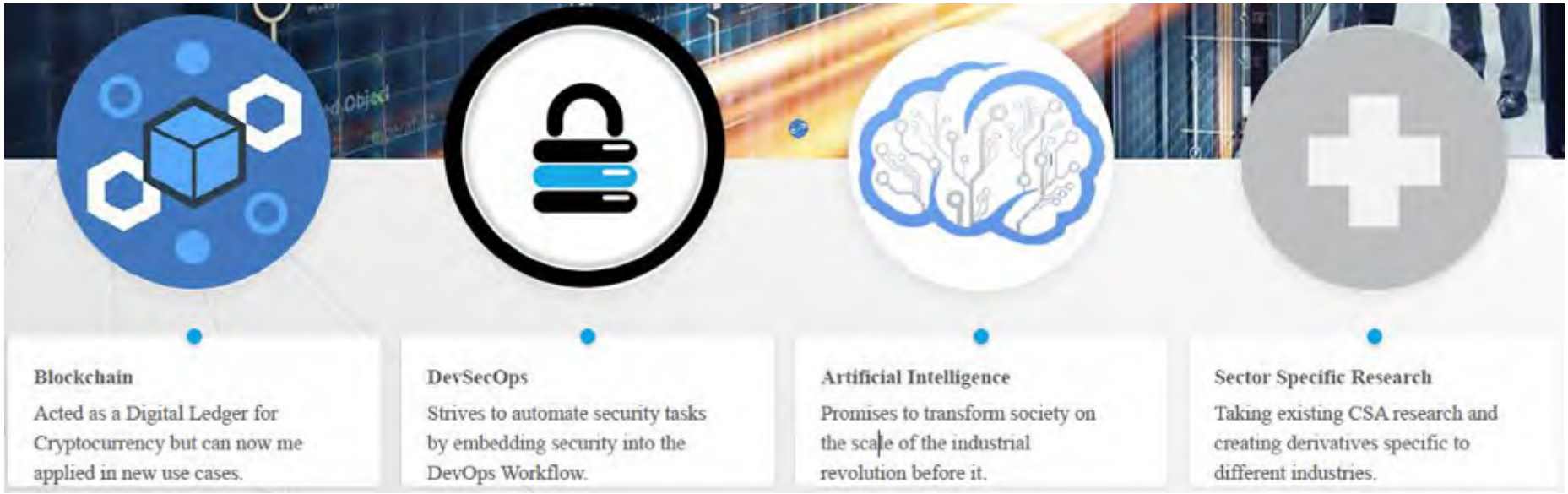
公安部信息安全等级保护三级

ISO27001-2013

网信办网络安全审查试点

可信云认证

案例 – CSA安全研究项目（2017Q2）



Blockchain
Acted as a Digital Ledger for Cryptocurrency but can now me applied in new use cases.

DevSecOps
Strives to automate security tasks by embedding security into the DevOps Workflow.

Artificial Intelligence
Promises to transform society on the scale of the industrial revolution before it.

Sector Specific Research
Taking existing CSA research and creating derivatives specific to different industries.

CLOUD CONTROLS MATRIX WORKING GROUP
Shared Assesments Mapping
PCI DSS V. 3.2 Mapping

QUANTUM SAFE SECURITY WORKING GROUP
QR QKD Paper
Glossary of Quantum Terms Whitepaper

IOT WORKING GROUP
IoT Municipal Drone Program Whitepaper
Connected Vehicles Whitepaper

SDP WORKING GROUP
SDP for IaaS

CLOUD DATA GOVERNANCE WORKING GROUP
Data Classification Scheme

CSA 在中国： 云计算、大数据、物联网安全技术标准

全球网络安全产品和服务预测

•到2021年，由于用户的广泛接受、认证终端基础设施的普遍存在（如手机）、低廉的实施成本，50%的在线交易将使用基于生物识别技术（如人脸识别、声音、指纹等）的身份验证。
•到2019年，超过75%的物联网设备制造商将通过提高其安全能力和隐私能力，使他们成为技术买家更值得信赖的合作伙伴。
•到2019年，70%根植于美国和欧洲的主要跨国公司，将面临旨在扰乱以商品经销为目的的重大网络安全攻击。其核心原因可能是黑色产业链为了谋取利润，也可能是由于地缘政治分歧的原因，阻碍跨国公司在本国的经销。
•在未来两年，发达国家中80%的消费者将面临交易缺陷，这是由于个人的识别信息可能存在因安全漏洞而导致被泄漏的风险所致。
•到2018年，70%的企业在其网络安全环境中将使用认知和人工智能（AI）技术来帮助人类处理与日俱增、纷繁复杂的网络威胁。
•2017年，50%的企业级客户将利用分析即服务（Analytics as a Service），对安全相关的数据和安全事件进行精细梳理，从而帮助企业解决其面临的安全挑战。
•到2020年，为了吸引IT领导者们将其产品迁移到云上，云安全网关的功能将开始被集成并作为Web服务产品的一部分。
•到2020年，30%的美国宽带家庭将至少拥有一个基于IP的家庭自动化或安全监控传感器或设备。
•到2020年，超过80%的全球企业将投资于应急响应框架建设。
•到2020年，超过25%的企业将通过云、托管、SaaS安全服务保障其IT架构的安全。

来源：IDC 2017年预测

谢谢！

更多的信息及关于云安全联盟，请联系:

- 邮箱
  info@china-csa.org
- 微信ID
  csagcr
- 微信公众号
  云安全联盟CSA （csa_china）