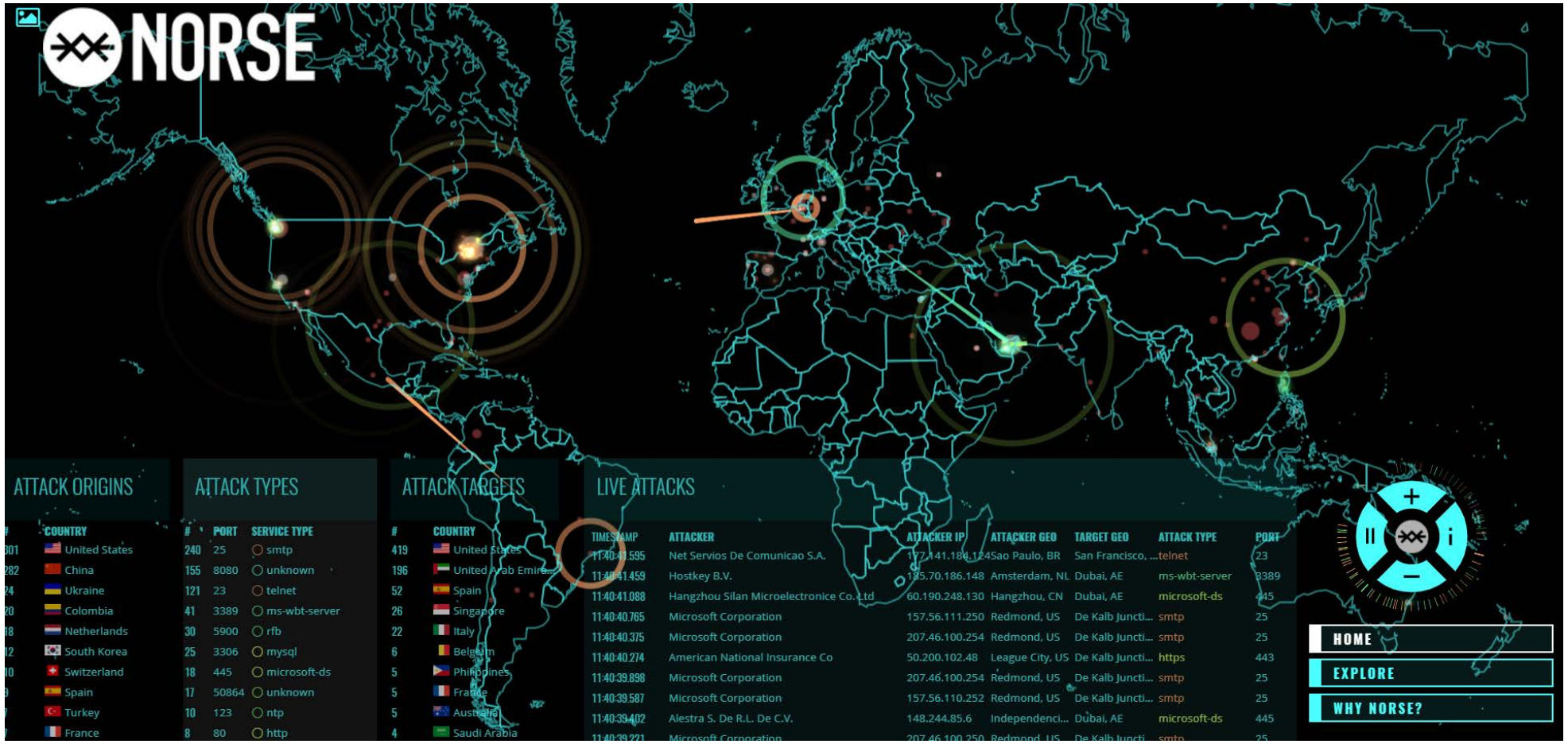
网络安全与隐私的政策和监管趋势

丹尼尔·卡斯特罗（ Daniel Castro ）
信息技术与创新基金会副主席（ ITIF ）

2017年9月12日

@castrotech

网络安全威胁具有全球性



2016年十大网络安全威胁

- 恶意软件
- 网页式攻击
- 网页应用攻击
- 服务拒绝攻击 (DDoS)
- 僵尸网络
- 网络钓鱼
- 垃圾邮件
- 勒索软件
- 内部威胁 (恶意/无意)
- 物理控制、损坏和盗窃

资料来源：欧洲网络与信息安全局（ ENISA ） 《 2016年威胁形势报告》

美国的网络安全政策

- 特朗普政府关于网络安全的行政命令
- 美国对于网络安全的监管措施
- 美国的网络安全立法

资料来源： Online Generator by hepwori

美国网络安全行政命令

2017年行政命令指示美国联邦政府推进三项工作：

1. 指导联邦机构，特别是民间机构，建立和分享更为稳健和安全的IT架构并增强其问责制

2. 指导联邦机构加强对关键基础设施的支持和安全能力建设，防范网络攻击

3. 指导联邦机构协调制订一项保护美国国民免受网络威胁的战略计划，并与其他国家合作确保全球互联网安全和韧性

美国网络安全监管机构

- 联邦贸易委员会(FTC)，针对“不公平或欺骗性”网络安全申诉的官方机构

- 不同特定行业的监管机构，如美国财政部的货币监理署，分别为各自对对应的行业起草指导方针

- 美国国家电信和信息管理局(NTIA）针对物联网（安全漏洞）组织了一个多利益相关方工作小组

美国网络安全法规

美国主要的网络安全法规包括:

- **2002年颁布的联邦信息安全管理法(FISMA)** ——要求联邦机构制定并实施网络安全的强制性政策、原则、标准和指导方针
- **2015年颁布的网络安全信息共享法(CISA)**——加强美国政府与科技、金融和制造业公司之间的网络威胁信息共享。
- **2014年颁布的网络安全增强法**——提供持续、自愿的公私合作伙伴关系，以改善网络安全，加强网络安全研究和开发
- 私营部门也有专门针对特定行业的安全法规，如针对健康数据的健康保险携带和问责法(HIPAA)、针对金融数据的金融服务现代化法案，以及针对保险交易所的联邦交易所数据泄露告知法案
- 美国各州也制定了形形色色的网络安全法规，包括保险和数据泄露告知等

欧盟的网络安全政策

- 网络和信息安全指令(NIS指令)
- 欧洲网络与信息安全局(ENISA)
- 一般数据保护条例 (GDPR)

网络和信息安全指令 （NIS）

NIS指令包括针对事故响应和基于风险的安全措施实施的若干要求。该指令旨在推动以下三项工作：

- 提高成员国的网络安全能力
- 加强成员国间网络威胁方面的合作和信息共享
- 为关键基础设施（如能源企业）和数字服务提供商(如搜索引擎)引入安全措施和事故告知义务

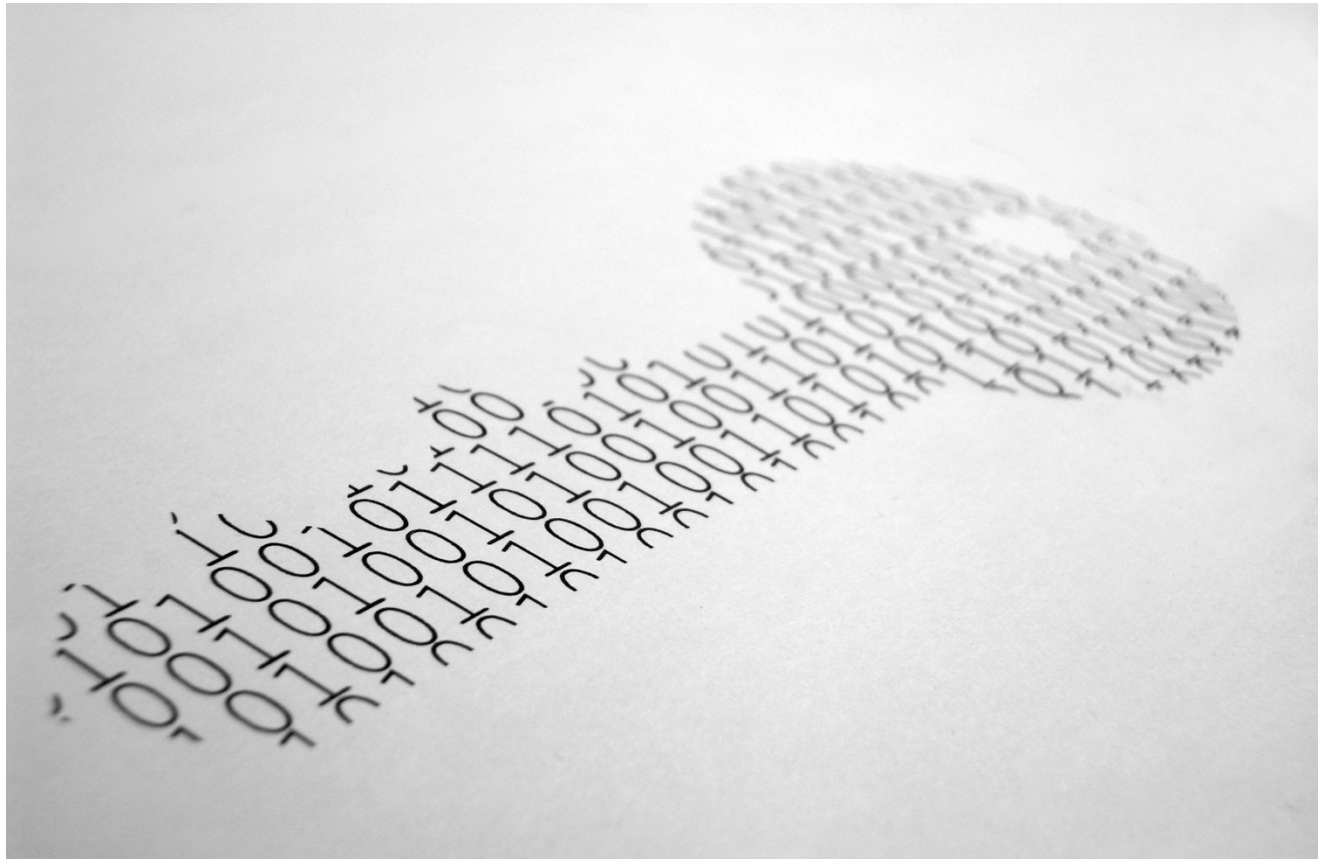
欧洲网络与信息安全局(ENISA)

- 欧洲网络与信息安全局是欧盟与其成员国及私营部门紧密合作并制定与实施NIS政策的机构。
- 欧洲网络与信息安全局经常发布关于管理NIS问题的安全指南和建议

欧洲网络与信息安全局

美国的隐私政策

- 没有专门的隐私法
- 不同监管部门制订了几个针对特定行业的隐私法案
- 美国消费者保护法
- 州立隐私安全法



来源： Morgue File

美国特定行业的隐私安全法案

在联邦层面，监管特定行业的隐私法通常是按行业分类的

- 健康保险携带和问责法(HIPAA)规定了医疗保健服务提供者如何保护医疗信息。
- 金融服务现代化法案(GLBA)规定了金融公司公开个人财务信息的方式
- 公平信用报告法(FCRA)规定了信用报告的个人信息隐私范围
- 视频隐私保护法(VPPA)监管内容里个人形象可识别的用于出租的视频和其他音频视觉材料信息

其他美国隐私安全法规

美国还有一些特殊的安全隐私法规，如针对儿童隐私的法规

- 儿童在线隐私保护法(COPPA) 要求在收集13岁以下儿童的信息时征得父母的同意
- 家庭教育权利和隐私法(FERPA)保护18岁以下儿童的学生教育记录隐私

来源: hackny.org

美国联邦贸易委员会执法情况

- 美国消费者保护法指定联邦贸易委员会（FTC）为实施其“不公平或欺骗性行为”条款的一般隐私保护的主要监管机构
- 当一家公司违背承诺，FTC可对其采取强制措施，包括罚款和合意判决
- 合意判决…
  - 最高可判20年；
  - 公司接受FTC的定期审计；
  - 违反将导致更高的罚款

州立隐私法

各州还制订了许多具体的隐私法规，这些只适用于州内的管辖范围。例如…

- 伊利诺斯州个人生物信息法
- 加州隐私政策法
- 40种不同的州范围内的无人机管理条例

资料来源: Andrew Turner

欧盟隐私保护

- 《欧盟基本权利宪章》中即包含有保护个人数据的权利
- 一般数据保护条例（GDPR）
- 网络隐私监管

资料来源: 欧盟

一般数据保护条例（GDPR）

GDPR旨在协调整个欧盟的数据保护法规。其涵盖了许多不同的隐私条款：

- 数据最小化
- 目的限制
- 消除权
- 被遗忘权
- 解释权
- 系统退出权
- 数据迁移权
- 国际数据传输限制

网络隐私监管

网络隐私监管的目的是为了促进欧盟通讯方面隐私法规的统一，如电话或网络浏览

网络隐私监管的组成部分包括:

– Cookie法规

– “机顶盒”服务提供商隐私法规

欧美“隐私之盾”

该框架使得企业在交换用于商业目的的私人数据时，可同时满足美国和欧盟的数据保护要求。

“隐私之盾”涵盖：

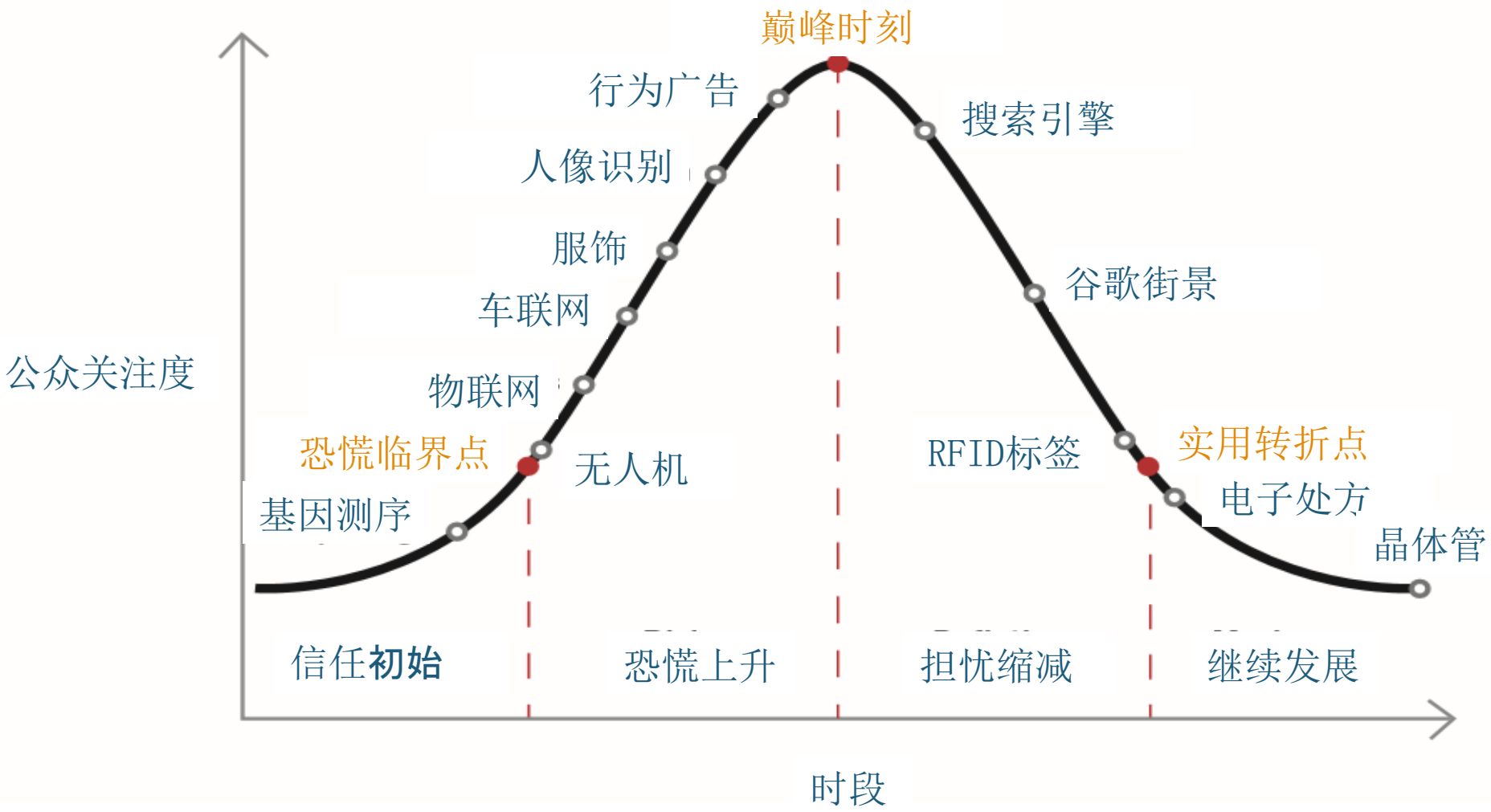
– 允许FTC与欧盟的数据保护机构合作，提供相互的执法协助

– 为个人申诉提供独立的追偿机制

– 确保签署了“隐私之盾” 协议的企业遵守承诺。

新兴技术会否带来新的挑战?

新兴技术带来的隐私发展趋势



谢谢大家！

丹尼尔·卡斯特罗 | dcastro@itif.org | @castrotech