XDef 2012
对话·交流·合作

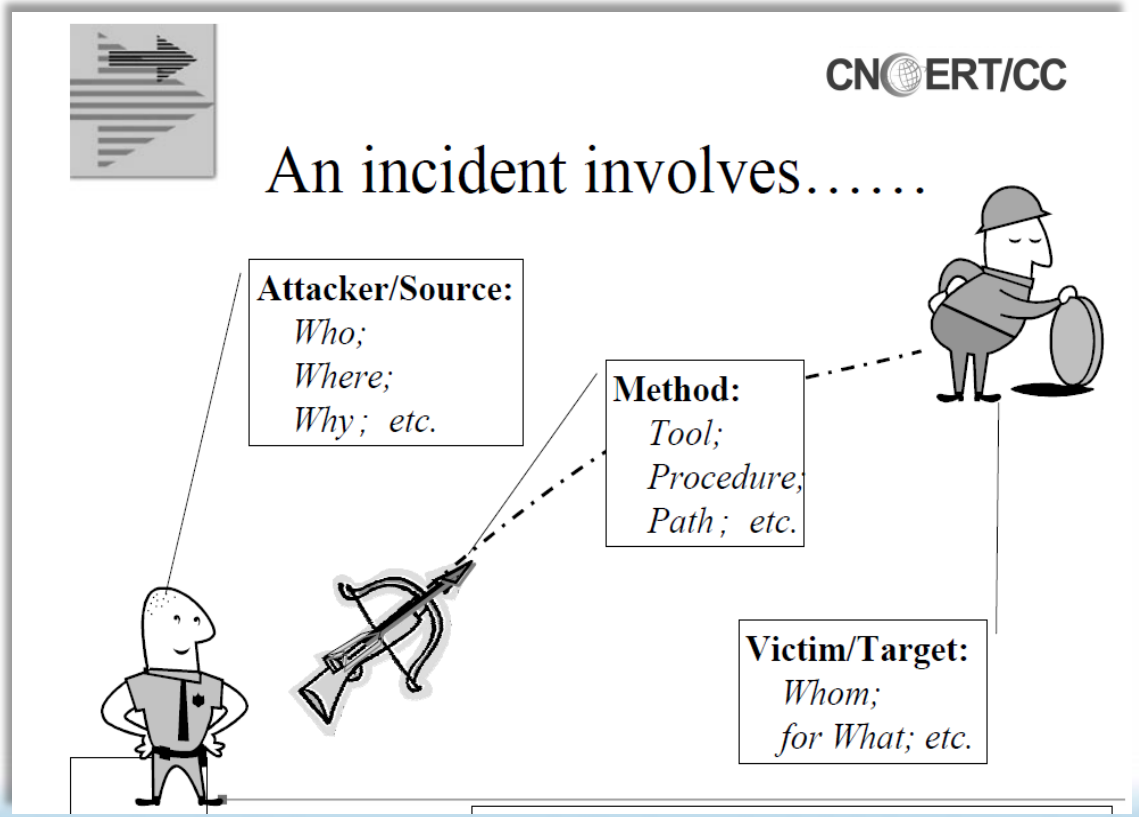
国际对抗环境下的网络安全防护能力建设

杜跃进
国家网络信息安全技术研究所　　所长
国家互联网应急中心　　副总工

关键词：网络安全防护

对话·交流·合作

- 什么是网络安全防护
  - 事前能力：预防**事件**，降低风险
- 什么是事件？
  - 事件的组成
  - 了解新自己吗？
  - 了解新威胁吗？
  - 了解新对手吗？



关键词2：国际对抗环境

对话·交流·合作

- Stuxnet,Duqu,Flame
- 纽约时报
- 国际战略
- 各国动作
- 网络战
- APT

Cyberattacks on Iran –

Updated: Aug. 9, 2012

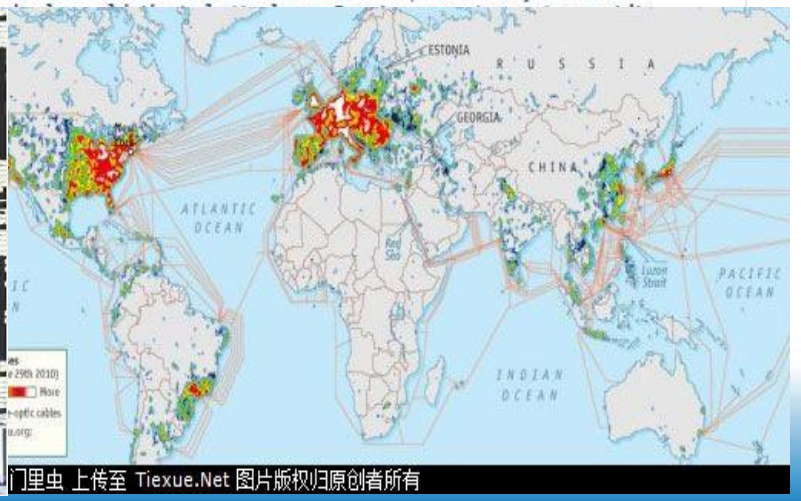
The New York Times

Friday, October 19, 2012

malicious computer program.

According to an article in The New

President Obama's first few months



再次审视我们自己

对话·交流·合作

- 新技术新应用的**快速**发展
- 新一代信息技术的基本特点
  - 智能
  - 融合
  - 泛在
  - 宽带
  - 移动
  - 隐匿
  - 不对称

BYOD?

- 为什么不能放弃新技术？
  - 信息化这么脆弱，为什么美国非要依赖它？
  - 我们不怕伤亡，就能赢得对抗吗？
- **结论：依靠限制新技术的应用来保障安全，绝对不是长久之计**

再次审视新威胁

- Stuxnet/Duqu/Flame带来的问题：
  - 技术上的领先程度
  - 网络战的目标？防护的职责分工？
  - 美国的网络武器库中，还有什么样的作品？
  - 有没有其他已经部署、早已潜伏在关键部位等待最后一击的网络武器？
  - 有没有针对我国的？现在？将来？
  - 他们是怎么做到的？
  - 效仿者？
  - **我们防得住这类威胁吗？什么地方需要调整？**

面对新环境，出现哪些新问题

新环境带来的关键影响

- 世界各国对网络空间安全空前重视本是好事。但是没有走向联手打击网络犯罪、规范网络秩序的道路，而是开始建立同盟、展开威慑与对抗，这对原来的网络安全工作带来根本性的影响：
- 信任遭到破坏
  - 技术能力面临巨大挑战
  - 流程机制需做重大调整

安全产品

- 人工智能VS 人的智能：不要迷信“自动”
- 明处 VS 暗处：总可以找到绕过的方法
- 结论：
  - 大众化的产品可以应对传统的安全威胁，提升攻击者的成本和难度，降低风险。但是无法应对高级的、专业化的、非常有目标的安全攻击
  - 对于重要保护对象来说，依靠大众化的安全产品构建的安全防护体系，是不靠谱的
- 推论：未来需要更多的“定制”安全，尤其是服务。人的因素更加重要

风险评估

- 提升普遍的安全水平，但是重点目标呢？
- 基于已知漏洞？
- 仅仅是技术漏洞吗？
- 结论：原来的漏洞信息共享机制，不适应国家间网络安全对抗所带来的威胁风险分析；现在的风险评估工作，不足以了解国家间网络安全对抗所带来的风险
- 推论：漏洞发现和分析能力需要大力加强；风险评估方法和手段建设需要改进加强

渗透测试

- 测试者的水平和方法，和潜在的攻击者相比如何？
- 结论：原来的做法还不规范、不成体系，不能为重点保护目标提供更多的参考
- 推论：
  - 需要大力开展新威胁研究
  - 建立研制更加完备的和成体系的渗透测试方法和工具
  - 需要打破固有模式，建立联合协作机制

安全测试

- 被忽视的安全性测试
- 测试的重要性
- 现状：测试能力的缺失（并非想象中那么简单）
  - 测试设备
  - 测试方法
  - 测试环境
  - 测试人员
- “自主可控”实现之前：测试设备完全依赖进口，怎么能发现对方的国家攻击行为？
- 需要重视安全测试工作，以及相关的研发

软件安全

对话·交流·合作

- 软件安全的问题被极大地放大
- 安全的根本，但却非常薄弱
- 安全测试是一方面，安全编程呢？大型软件的安全编程呢？
- 软件安全测试本身也面临很多挑战
- 需要提升用户意识、推动政策制定、建立硬性需求；需要大力加强有关研发、鼓励相关产业发展、提升软件安全开发和测试水平

事件发现

- 社会工程学攻击的发现能力
- APT事件的发现能力
- 恶意代码分析能力

- 发现能力面临的挑战
- 0-day漏洞：
  - 隐藏多年的（战略级储备）
  - 多如牛毛的（自主开发）
  - 复杂关联的（代码共用）
- 社会工程学
  - 广泛的社交网络应用
  - 人的脆弱性
  - 网站信息泄露（新的短板）
- 未知特征的攻击程序
- 复杂环境：BYOD

分析能力

- 如何才算“发现”：技术层面的、单一的“事件”，并非“发现”的目的
- 然而真正的“发现”谈何容易
- 如今则变得更加困难
  - 更强的代码隐藏能力、代码反分析能力
  - 更复杂的攻击路径
  - 被分裂的国际社会，导致追踪、溯源、调查难度更大
- 所谓态势感知

人才培养

- 你们从哪里了解真实的网络安全现状和需求？
- 你们从哪里了解最新的攻防对抗技术和技巧？
- 你们从哪里了解各种相互关联的现实系统所使用的实际技术、配置策略，以及面临的实际风险？
- 你们从哪里获得反应真实情况的研究实验环境和数据资源？
- 结论：高校人才培养，缺乏与实际的结合；社会人才培养，缺乏生存环境

未来之路

对话·交流·合作

- 应对国家间的对抗，需要形成举国之力
- 需要强化国家级核心能力的研究与建设，并用之带动人才培养、研究实验、产业发展、服务水平
- 需要从过去的分散能力转变为整体能力
- 人的作用更甚以往，需要打造核心专业人才队伍
- 安全服务更加重要
- 针对重点防护目标，需要“定制”安全服务

谢谢！

AND ONE MORE THING