



教育系统网络安全培训



谨慎能捕千秋蝉
小心驶得万年船



——新郑市教育系统网络安全培训

**

2018.4.9



● 网络安全背景分析

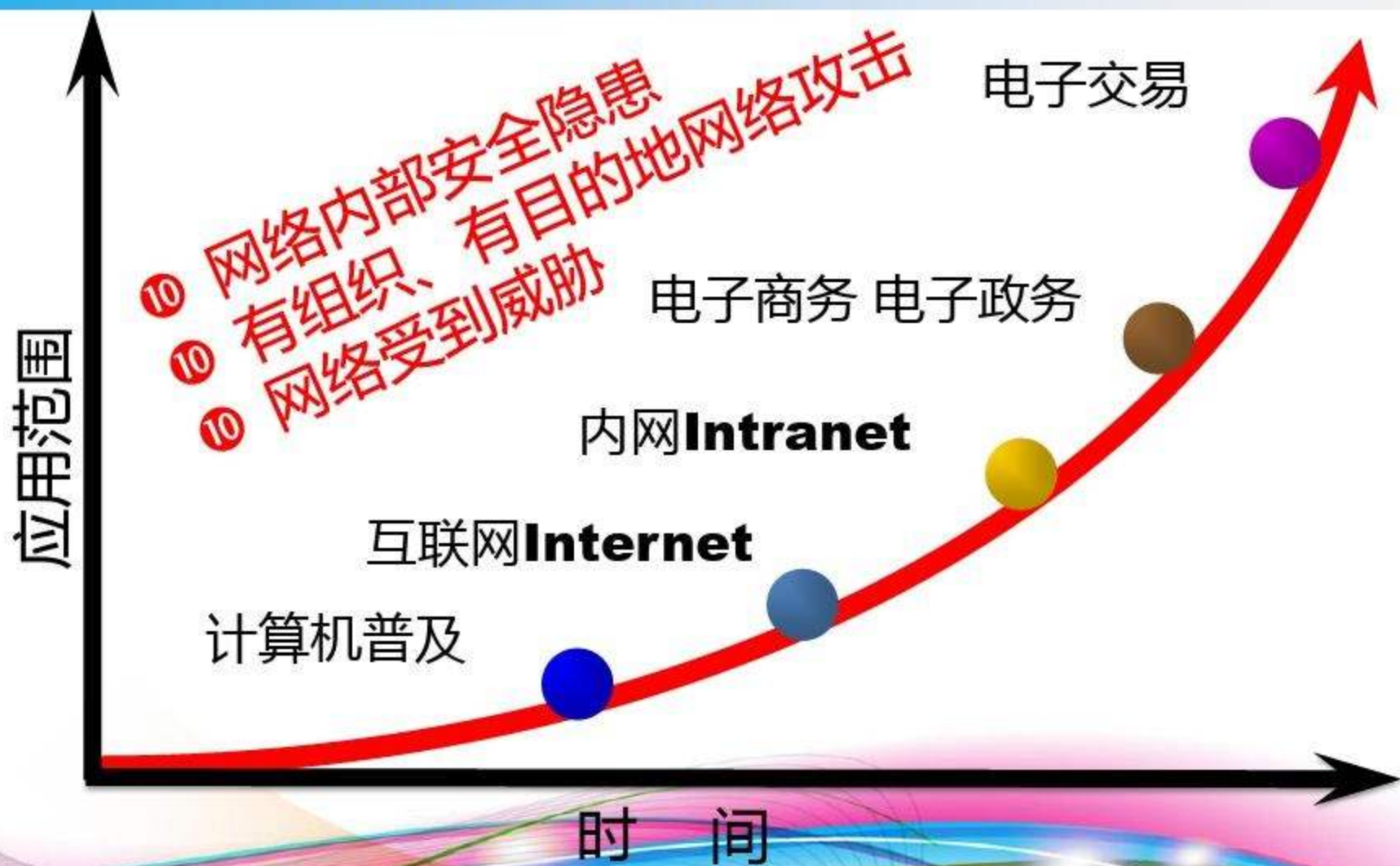
● 网络安全的目的

● 学校网络安全问题

● 网络安全防护策略

● 简单故障排查

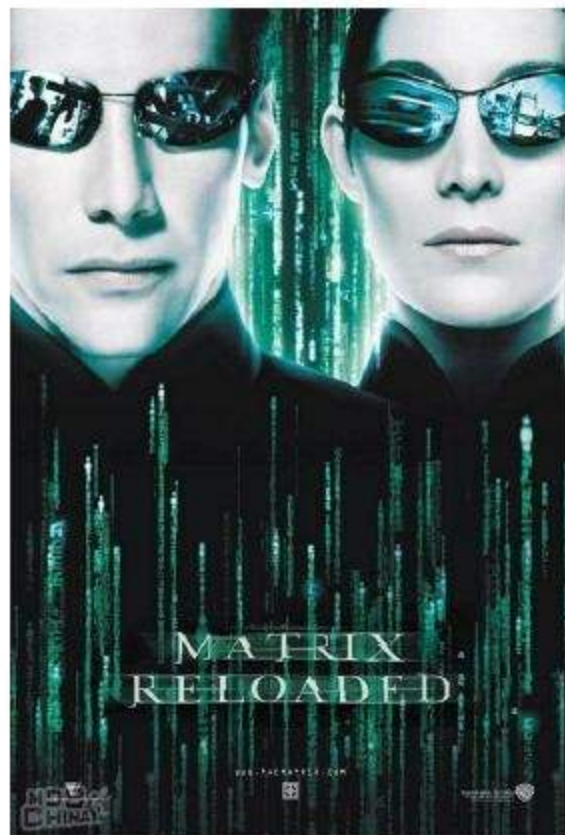
1. Internet 技术的迅猛发展和普及



2. 黑客 (Hacker) 产生

黑客方：尼奥 (病毒、木马)

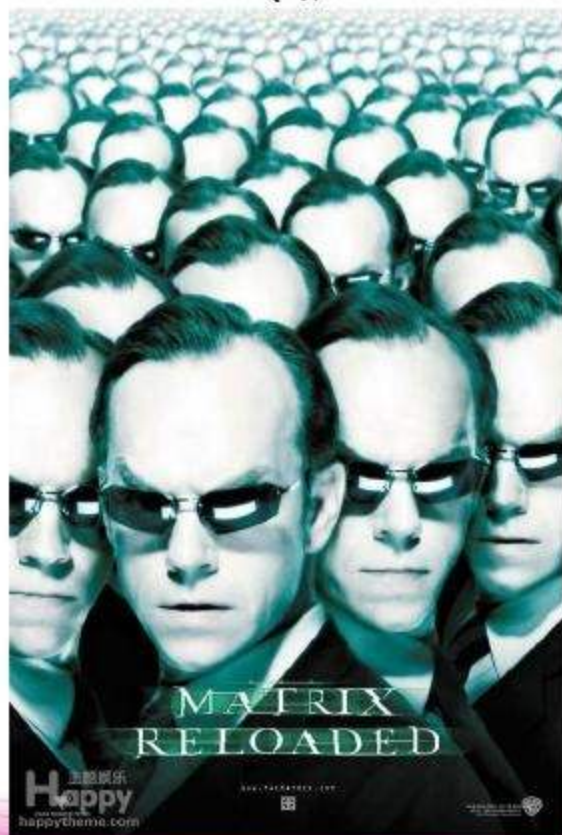
反黑客方：史密斯 (防火墙、杀毒软件)



偶然的破坏者

坚定的破坏者

间谍



3. 网络攻击事件



2015年初，希拉里



加拉央行8100万
月，俄罗斯央行 20
万美元) 不翼而飞

2017年2-4月份洲际酒店(IHG)信用卡数据泄露

4.网络攻击后果

- 政治影响恶劣
- 经济财产损失
- 知识产权损失
- 时间消耗
- 生产力消耗
- 责任感下降
- 激化社会矛盾

5. 《网络安全法》颁布

- 《中华人民共和国网络安全法》（以下简称《网络安全法》）于2017年6月1日正式实施。
 - 《网络安全法》作为我国网络空间安全管理的基本法律，框架性地构建了许多法律制度和要求，重点包括网络信息内容管理制度、网络安全等级保护制度、关键信息基础设施安全保护制度、网络安全审查、个人信息和重要数据保护制度、数据出境安全评估、网络关键设备和网络安全专用产品安全管理制度、网络安全事件应对制度等。
-
- ⑩ 一方面，以国家互联网信息办公室（以下简称“网信办”）为主的监管部门制定了多项配套法规
 - ⑩ 另一方面，全国信息安全标准化技术委员会（以下简称“信安标委”）同时制定并公开了一系列以信息安全技术为主的重要标准的征求意见稿

6. 《网络安全法》明确了六点内容

(1) 网络安全法明确了网络空间主权的原则；

第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任。

明确了网络是国家主权范围，需要进行管辖。明确网络空间主权至少已经从最基础的层面提出国家对网络空间行使权力的问题。

(2) 明确了网络产品和服务提供者的安全义务；

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

其中“相关国家标准的强制性要求”在《网络产品和服务安全审查办法》中规定，网络产品和服务由国家依法认定网络安全审查第三方机构进行安全审查。

6. 《网络安全法》明确了六点内容

(3) 明确了网络运营者的安全义务；

第二十一条 **国家实行网络安全等级保护制度**。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

其中网络安全等级保护制度尚未出台。

(4) 进一步完善了个人信息保护规则；

第四十四条 **任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息**。

在此之前，《电信和互联网用户个人信息保护规定》、《刑法》及《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》均规定了个人信息保护。而**网络安全法在强调了个人信息保护重要性的基础上，规定了如何落实相关信息保护制度**。

6. 《网络安全法》明确了六点内容

(5) 建立了关键信息基础设施安全保护制度；

第三十一条规定“关键信息基础设施的具体范围和安全保护办法由国务院制定。”

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

国家互联网信息办公室起草了《关键信息基础设施安全保护条例（征求意见稿）》。

(6) 确立了关键信息基础设施重要数据跨境传输的规则。

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

7. 《网络安全法》涉及民生

与网络空间国内形势、行业发展和民生紧密的主要有以下三大重点：

- ⑩ 一是确立了网络空间主权原则，将网络安全顶层设计法制化。网络空间主权是一国开展网络空间治理、维护网络安全的核心基石；离开了网络空间主权，维护公民、组织等在网络空间的合法利益将沦为一纸空谈。
- ⑩ 二是对关键信息基础设施实行重点保护，将关键信息基础设施安全保护制度确立为国家网络空间基本制度。
- ⑩ 三是加强个人信息保护要求，加大对网络诈骗等不法行为的打击力度。近年来，公民个人信息数据泄露日趋严重，“徐玉玉案”等一系列的电信网络诈骗案引发社会焦点关注。《网络安全法》从立法伊始就将个人信息保护列为了需重点解决的问题之一。

8. 《网络安全法》对一些网络词汇进行定义

- ⑩ **网络**，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。
- ⑩ **网络安全**，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。
- ⑩ **网络运营者**，是指网络的所有者、管理者和网络服务提供者。
- ⑩ **网络数据**，是指通过网络收集、存储、传输、处理和产生的各种电子数据。
- ⑩ **个人信息**，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

- ⑩ 保护信息的安全
- ⑩ 保护信息交互、传输的安全
- ⑩ 保护信息系统的正常运行



进不来

看不懂

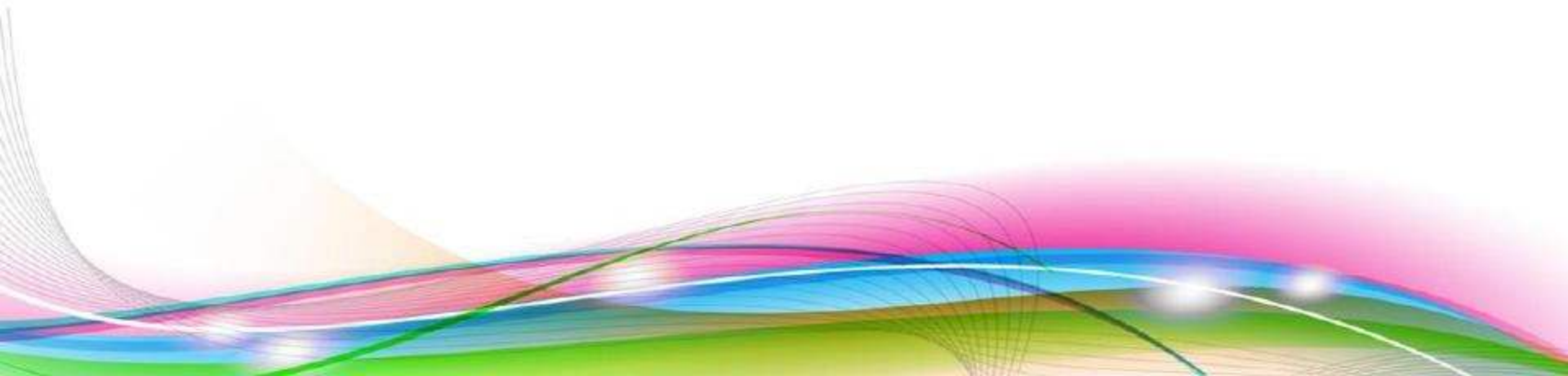
拿不走

改不了

跑不了

可审查

- ⑩ 网络安全意识淡薄
- ⑩ 网络安全方面的投入严重不足，没有系统的网络安全设施配备
- ⑩ 学校的上网场所管理较混乱
- ⑩ 无任何安全管理和监控的手段
- ⑩ 网络安全管理制度缺失

- ◆ 人——网络安全防护的决定因素
 - ◆ 制度——网络安全防护的基础和核心
 - ◆ 技术——网络安全防护的基本保证
- 

人——网络安全防护的决定因素

⑩ 人是网络安全防护中的最薄弱环节

对安全防护工作重视的**领导**是安防工作顺利推进的**主要动力**

有强烈安全防护意识的**教职员**是安防体系得以切实落实的**基础**

杜绝单位内部员工攻击网络系统是加强安全防护的一项**重要工作**

⑩ 加强安全教育、提高网络**安全意识**尤为重要

人——网络安全防护的决定因素

- ⑩ **安全意识**是指人们发现可能存在的威胁、判断其危害性并及时预防或化解威胁的一种能力
- ⑩ 加强自身对威胁相关知识的掌握以及正确的使用习惯可以提升这种能力。
即**提高安全意识**

人——网络安全防护的决定因素

为什么要培养用户的网络安全意识？

- ∞ 网络的基础元素是用户
- ∞ 网络应用的多样化、用户个体习惯的多样化
- ∞ 对于学校来说网络安全主要是管理和制度的问题，对于个人来说网络安全主要是意识和使用习惯的问题，技术仅仅是辅助手段

人——网络安全防护的决定因素

首先要让用户清楚哪些东西是需要保护的？

- ☞ 终端设备（PC、平板、手机等）
- ☞ 软件系统及网络
- ☞ 真实的钱财（网络银行账号、股票基金帐户）
- ☞ 虚拟财产(微信帐号、qq帐号、游戏帐号等)
- ☞ 帐号信息及密码（开机、Email、各类应用及App等）
- ☞ 研究成果、各类文档等
- ☞ 私密的信息（头像、指纹、身份证号、电话号码、车牌号码、家庭地址）

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/177033103121010004>