中国移动
China Mobile

网络与信息安全

www.10086.cn

目录

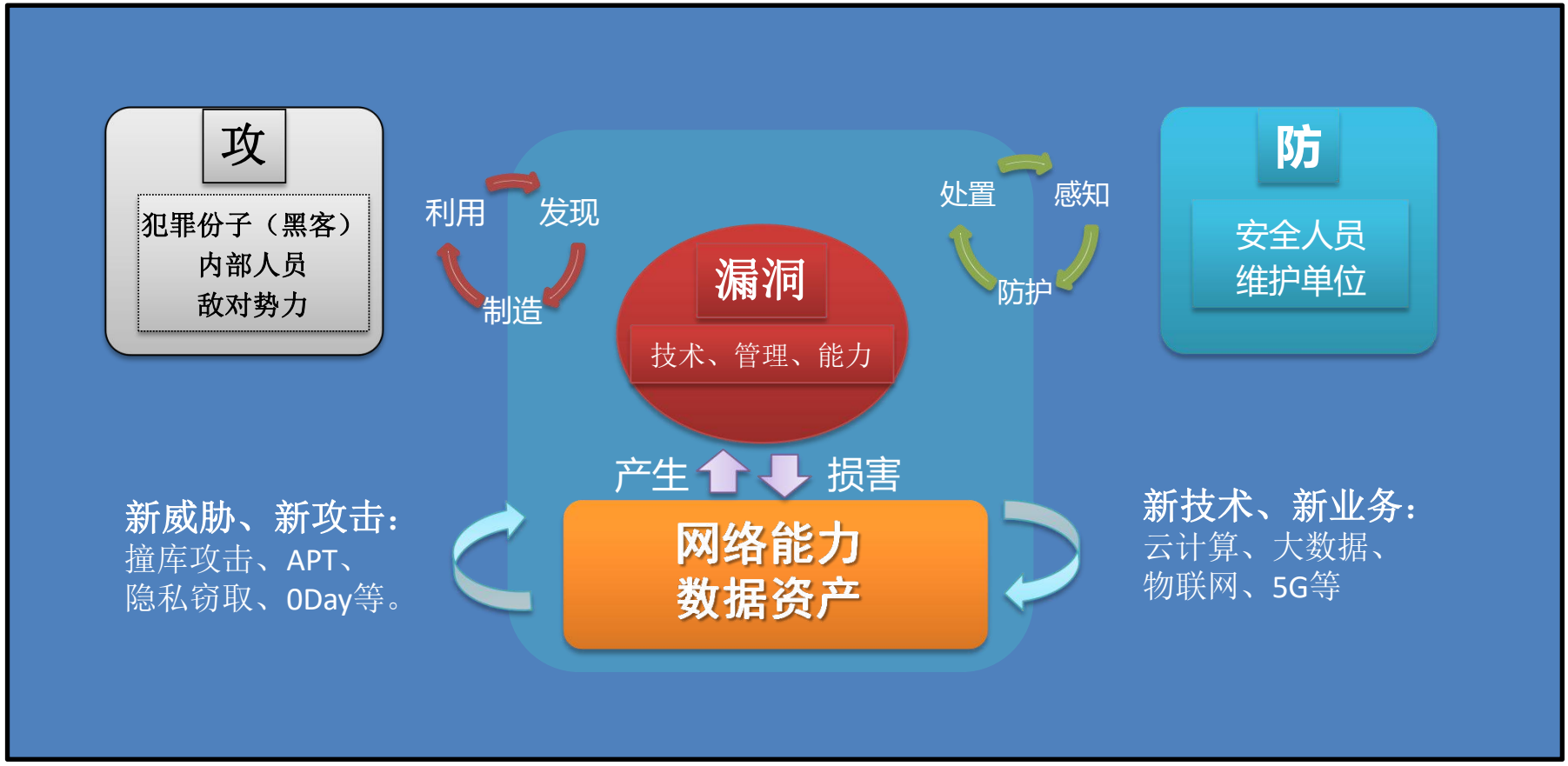
安全的定义和属性

网络与信息安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。 网络与信息安全包含网络设备安全、网络信息安全、网络软件安全。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

保密性	使信息不泄露给未授权的个人、实体或过程或不使信息为其所利用的特性。Confidentiality
完整性	保护信息及处理方法的准确性和完备性。 Integrity
可用性	被授权实体一旦需要就可访问和使用的特性。Availability
真实性	确保主体或资源的身份正是所声称身份的特性。真实性适用于用户、过程、系统和信息之类的实体。
可核查性	确保可将一个实体的行动唯一地追踪到此实体的特性。
抗抵赖性	证明某一动作或事件已经发生的能力，以使事后不能抵赖这一动作或事件。
可靠性	预期行为和结果相一致的特性。

从攻防动态对抗的视角看网络安全

网络安全是企图发现漏洞的攻击者与尽力弥补这些漏洞的防护者之间的动态对抗过程。



全球网络安全态势

中国移动 China Mobile

全球范围内针对政府、电信、金融及公共基础设施等行业的网络攻击层出不穷，呈现出愈演愈烈的态势。

- 网络安全国际形势更为复杂，网络攻击和网络犯罪已经并将继续困扰全球各国
- 带有政治色彩及政治目标的黑客主义行动日益频繁

- 针对金融机构及公共基础设施的网络攻击呈上升趋势
- 高级持续性攻击事件数量明显增加

全球攻击事件概览

中国移动 China Mobile

攻击政府事件

- 俄通信部长社交网站账号遭土黑客攻击
- 美总统候选人官方网站遭黑客攻击
- 多个沙特政府网站遭黑客攻击致瘫痪四小时
- 泰国警方官网遭黑客攻击

攻击金融机构事件

- 乌克兰银行遭黑客攻击致1千万美元被窃
- 俄英国乐购网上银行2000多账户遭窃取
- 南非银行数据泄漏导致被盗刷14.4亿日元
- 俄罗斯中央银行遭黑客攻击致1亿卢布被窃

攻击电信运营商事件

- 美国威瑞森电信公司超四百万IP被恶意控制
- 法国IDC服务商遭大规模DDoS攻击
- 美国域名解析服务器商遭大规模DDoS攻击
- 德国电信遭网络攻击致大量用户网络中断

攻击公共基础设施事件

- 美国旧金山轨道交通系统遭黑客攻击
- 乌克兰电网遭恶意软件攻击破坏致使断电
- 芬兰两栋大楼因网络攻击停止供暖
- 国际民航系统每月遭网络攻击千余次

从世界范围看，网络安全威胁和风险日益突出，并日益向政治、经济、文化、社会、生态、国防等领域传导渗透。特别是国家关键信息基础设施面临较大风险隐患，网络安全防控能力薄弱，难以有效应对国家级、有组织的高强度网络攻击。这对世界各国都是一个难题，我们当然也不例外。

网络安全战争

- 2015 年12 月23 日，乌克兰电力部门遭受到恶意代码攻击，乌克兰新闻媒体TSN 在24 日报道称：“至少有三个电力区域被攻击，并于当地时间15 时左右导致了数小时的停电事故”；“攻击者入侵了监控管理系统，超过一半的地区和部分伊万诺-弗兰科夫斯克地区断电几个小时。”Kyivoblenergo 电力公司发布公告称：“公司因遭到入侵，导致7 个110KV 的变电站和23 个35KV 的变电站出现故障，导致80000 用户断电。”

- 2010年,伊朗境内的诸多工业企业遭遇了一种极为特殊的超级病毒“震网”袭击，其中包括伊朗布舍尔核电站，安全专家称，该病毒能取得工业用电脑系统的控制权，这可能是全球第一种投入实战的网络武器。

网络战争威胁国家安全

超级病毒攻击伊朗基础核设施

- 2009年6月23 日，美国国防部长盖茨下令宣布组建网络战司令部，围绕网络战的新一轮军备竞赛已经开始。世界各国纷纷“招兵买马”扩充网军，组建网络战部队，英国、日本、俄罗斯、法国、德国、印度等国家都已建立成编制的网络战部队，极力加强信息安全对抗能力。

目录

网络安全：国之大事

没有网络安全就没有国家安全

2016年11月7日审议通过《网络安全法》

- **第五空间：** 人类活动从**实体社会**向**网络空间**转变的**新挑战**
- **网络主权：** 国家实力对抗的**新领域**、战略争夺的**新制高点**
- **国家安全：** 影响国家稳定、社会安定、人民生活的**新要素**
- **网络强国：** 从网络大国成为网络强国的**新要点**

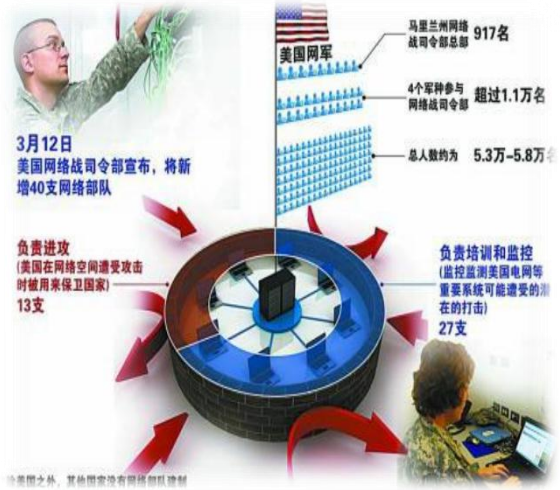
网民6.88亿　网站400万

国内域名3102万

网购用户3亿

信息消费2.2万亿

电子商务交易突破10万亿



境外控制国内主机近2000万

恶意代码 苹果XcodeGhost

用户信息泄露 12306网站600万

威胁形势严峻APT攻击、方程式组织

DDOS攻击 DYN 峰值流量1.5T

9

总书记系列重要讲话精神

中国移动 China Mobile

2014年2月27日，习近平总书记在中央网络安全和信息化领导小组第一次会议上系统提出了新时期建设网络强国的战略目标，全面阐述了加快信息化发展和维护网络安全的辩证关系，明确给出了建设网络强国的基本路径。

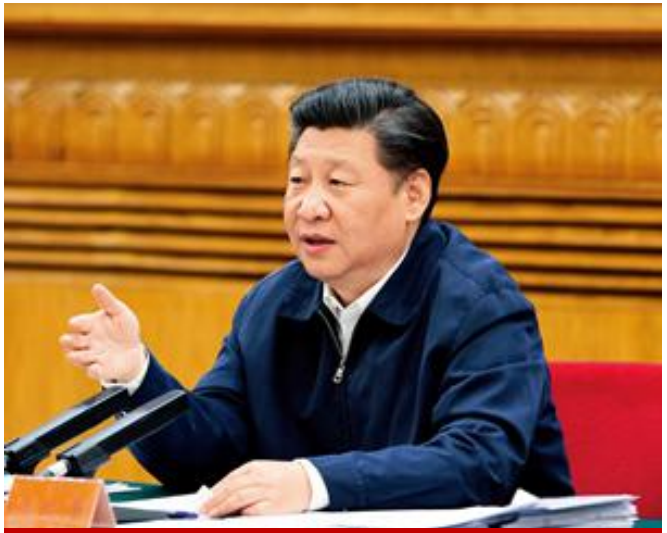
没有**网络安全**
就没有**国家安全**

中国移动 China Mobile

2016年4月19日，习近平总书记在网络安全和信息化工作座谈会上首次提出了**树立正确的网络安全观**的重要论断。

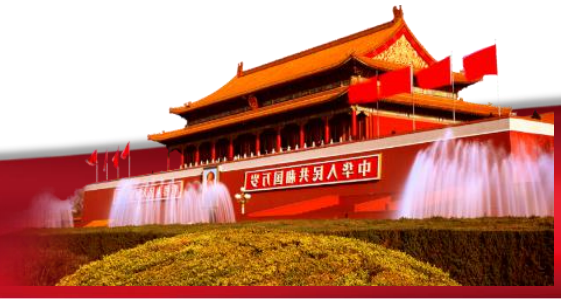
网络安全

- 是整体的而不是割裂的
- 是动态的而不是静止的
- 是开放的而不是封闭的
- 是相对的而不是绝对的
- 是共同的而不是孤立的。



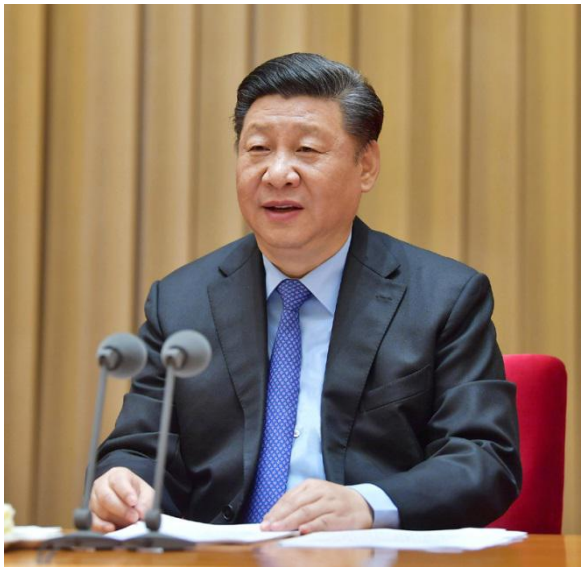
习近平总书记强调

✓ 网信工作要以人民为中心，要坚持**网络安全为人民，网络安全靠人民**。



中国移动 China Mobile

要加强党中央对网信工作的集中统一领导，确保网信事业始终沿着正确方向前进。



2018年4月20日，习近平总书记出席全国网络安全和信息化工作会议，并发表重要讲话。

- ✓ 要提高网络综合治理能力，加强信息基础设施网络安全防护，提升网络基础设施防护能力；
- ✓ 加强网络安全技术手段和平台建设，提升网络安全事件应急指挥和处置能力；
- ✓ 积极发展网络安全产业，提升核心技术和产业支撑能力；
- ✓ 依法严厉打击网络黑客、电信网络诈骗、侵犯公民个人隐私等违法犯罪行为，提升维护人民群众合法权益能力。

国内网络安全的顶层设计

中国移动 China Mobile

党和国家高度重视网络安全工作，成立了中央网络安全与信息化委员会，习总书记多次对网络安全工作作出指示，《网络安全法》已经发布实施，全社会高度关注网络安全工作。

顶层设计

- 习总书记指出“没有网络安全就没有国家安全，没有信息化就没有现代化”。
- 网络安全工作事关党的长期执政，事关国家长治久安，事关广大人民群众利益。
- 中共中央办公厅印发了《关于贯彻落实党委（党组）网络安全工作责任制实施办法》。

法律法规

- 《网络安全法》由全国人大常委会于2016年11月7日通过并发布，自2017年6月1日起施行。
- 《网络安全法》是我国第一部全面规范网络空间安全管理的基础性法律。
- 《网络安全法》的基本原则是网络空间主权原则、网络安全与信息化发展并重原则、共同治理原

社会关注

- 网络安全与百姓民生密切相关，全社会期待健康、安全的信息化应用。
- 电信诈骗、骚扰电话、垃圾短信、个人隐私信息泄露等问题成为舆论关注热点。

网络安全与党建的关系

2019年6月开始，在全党范围内开展“不忘初心、牢记使命”主题教育，主题教育要贯彻“守初心、担使命、找差距、抓落实”的总体要求，网络安全工作要结合主题教育，守住**网络安全为人民**的初心，担起**网络安全保发展**的使命，找出**网络安全存风险**的差距，抓**网络安全看行动**的落实。

责任观

- 党委责任制，党委对网络安全负主体责任，党委书记是第一责任人；
- 领导干部“一岗双责”。
- 自觉践行央企政治责任、经济责任与社会责任

发展观

- 理顺安全和发展的辩证关系，安全是发展的前提，发展是安全的保障，安全和发展要同步推进。
- “安全是刹车，发展是油门”，缺一不可。

行动观

- 网络安全工作重在落实，要加大人力、财力、物力支持。
- 网络安全工作“七分管理、三分技术”，要将安全工作嵌入到日常生产、运营流程中。

红线意识

- 网络安全工作要有红线意识，有敬畏心，不能心存侥幸心理。

案例思考

- 2010年11月16，某单位发现某公司一台计算机被境外间谍情报机关网络攻击控制并窃取资料。资料包括：网络拓扑、IP地址、账号口令。 在事发计算机上发现了两个木马，一个是蠕虫病毒多个变种，主要对内网用户通过建立IPC空链接等方式进行尝试随机感染，被感染的主机会将本机的大量信息往外发送。另一个是注入svchost的木马，会不断尝试与台湾中华电信的IP地址发起连接，并且该木马功能十分强大，能获取终端的帐号、磁盘文件、对文件操作、获取屏幕、关机重启感染计算机、关闭终端杀毒软件等。

安全治理面临持续压力

移动互联网恶意程序保持高速增长，电信网络诈骗呈蔓延态势，电信行业网络信息安全治理面临前所未有的压力，加强网络信息安全已经成为电信行业重要工作内容。

移动互联网恶意程序保持高速增长趋势

- 2016年，CNCERT监测移动互联网恶意程序数量 **205万** 余个，较2015年增长 **39.0%**。
- CNERT发现的移动互联网恶意程序下载链接近 **67万** 条，较2015年增长近 **1.2** 倍，恶意程序传播次数达 **1.24亿** 次。

- 以诱骗欺诈、恶意扣费、锁屏勒索等攫取经济利益为目的的应用程序骤增，占总数的 **59.6%**，较2015年增长近 **3** 倍。
- 从恶意程序攻击模式发现，通过**短信方式传播窃取短信验证码**的恶意程序占比较大，全年获得相关样本 **10845** 个，移动互联网黑色产业链已经成熟。

— 数据来源：CNERT

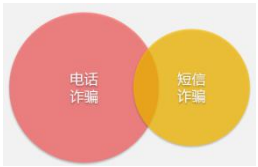
电信网络诈骗呈上升趋势

案件总量

- 2015年至2016年，全国电信网络诈骗案件量呈上升趋势。2016年较2015年同比上升 **51.47%**。

案件特征

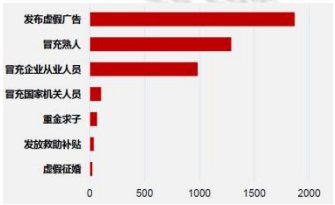
- 在电信网络诈骗案件中，**48.59%** 的案件为电信诈骗，59.47%的案件为网络诈骗，其中，8.06%的案件涉及电信诈骗和网络诈骗



电信诈骗手段

在电信网络诈骗案件中：

- 通过打电话进行诈骗的占比为 **69.08%**
- 通过群发短信进行诈骗的案件占比为 **38.64%**
- 在短信诈中通过**伪基站群发欺诈**信息的占比为 **68.59%**



— 数据来源：最高人民法院信息中心

安全威胁新趋势

随着物联网技术的迅速普及，以及“互联网+”时代的到来，安全攻击的新方式和新目标也陆续出现。

物联网智能设备网络攻击事件将持续增多，物联网智能设备被用于发起大流量DDoS攻击

攻击事件

- 2016年底，美国东海岸大规模断网事件和**德国电信大量用户访问网络异常**事件，使得Mirai恶意程序受到关注。（Mirai是利用物联网智能设备漏洞进行入侵渗透以实现对设备控制的恶意代码）
- 2016年10月，**新加坡电信运营商**遭受DDoS网络攻击，造成部分家庭宽带用户断网。该攻击利用了被感染的网络摄像头、联网的家用电器等500种以上的设备。

数据统计

- 截止2016年底，共发现2526台控制服务器控制了***125.4万***余台的物联网智能设备；

2016年第四季度

- 发现817台控制服务器控制了***42.5万***台物联网智能设备
- 累计发起超过***1.8万***次的DDoS攻击，其中峰值流量在5Gbps以上的攻击次数高达***72***次。

漏洞数量

- 2016年底，CNVD收录物联网智能设备漏洞***1117***个，主要涉及网络摄像头、智能路由器、智能网关等设备。

漏洞类型

- 2016年智能设备的漏洞类型主要为权限绕过、信息泄露、命令执行等。
- **弱口令（或内置默认口令）漏洞**为被攻击利用的重要风险点

落实《中华人民共和国网络安全法》

保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展

网络运行安全

一般规定

网络安全等级保护制度

- 制定安全管理制度和操作规程，落实安全责任
- 网络攻击和入侵防范
- 网络运行状态监控与记录
- 数据分类、备份与加密

网络产品/服务

- 网络产品/服务提供者提供**持续安全维护**
- 收集用户信息的，**须向用户明示并征得同意**
- 网络关键设备和网络安全专用产品须经**安全认证和检测**

用户实名制

- 网络接入、域名注册、电话入网、信息发布、即时通讯等服务
- 网络运营者在用户签订协议或者确认提供服务时，**应当要求用户提供真实身份信息**

➢**业务开通实名：**
用户真实身份信息核验和登记
➢**服务提供过程实名**
过程鉴权，避免伪造身份进行通信

网络安全事件应急预案

- 网络运营者应当制定**网络安全事件应急预案**
- 发生安全事件时，立即启动预案，并报告有关主管部门

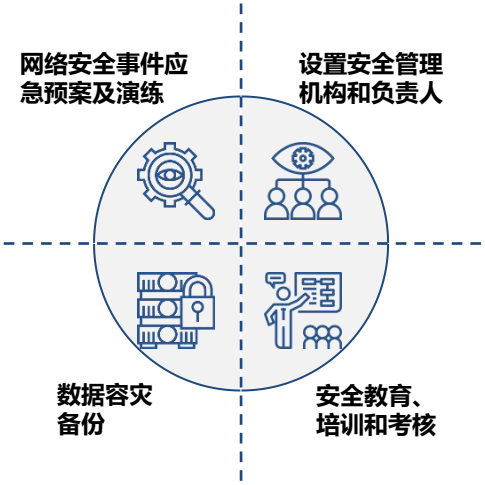
关键信息基础设施的运行安全

关键信息基础设施安全规划

关键信息基础设施安全技术措施“三同步”

➢**关键信息基础设施安全三同步**
➢**网络日志留存时限要求**
➢**制定网络安全事件应急预案，并定期演练**

关键基础设施运营者 安全保护义务



关键基础设施运营者 管理要求

- 采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的**国家安全审查**
- 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**
- 应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次**检测评估**

落实《中华人民共和国网络安全法》

中国移动 China Mobile

网络信息安全

用户信息保护

网络运营者

- 应当建立健全**用户信息保护制度**
- 明示收集、使用个人信息的目的、方式和范围，并**经被收集者同意**
- **不得泄露、篡改、毁损**其收集的个人信息
- 加强对其用户**发布的信息的管理**
- 电子信息发送服务提供者和应用软件下载服务提供者，应当履行**安全管理义务**
- 及时受理并处理有关网络信息安全的投诉和举报

➢**对可识别到具体个人的业务，须获得用户授权**
➢**防止个人信息泄露，做好用户信息保护**

打击网络诈骗犯罪

不得利用网络发布涉及实施诈骗等**违法犯罪活动的信息**

➢**落实实名制，加强用户违规违法行为监控**
➢**建立网络信息安全投诉、举报制度**

监测预警与应急处置

建立健全网络安全**监测预警和信息通报制度**

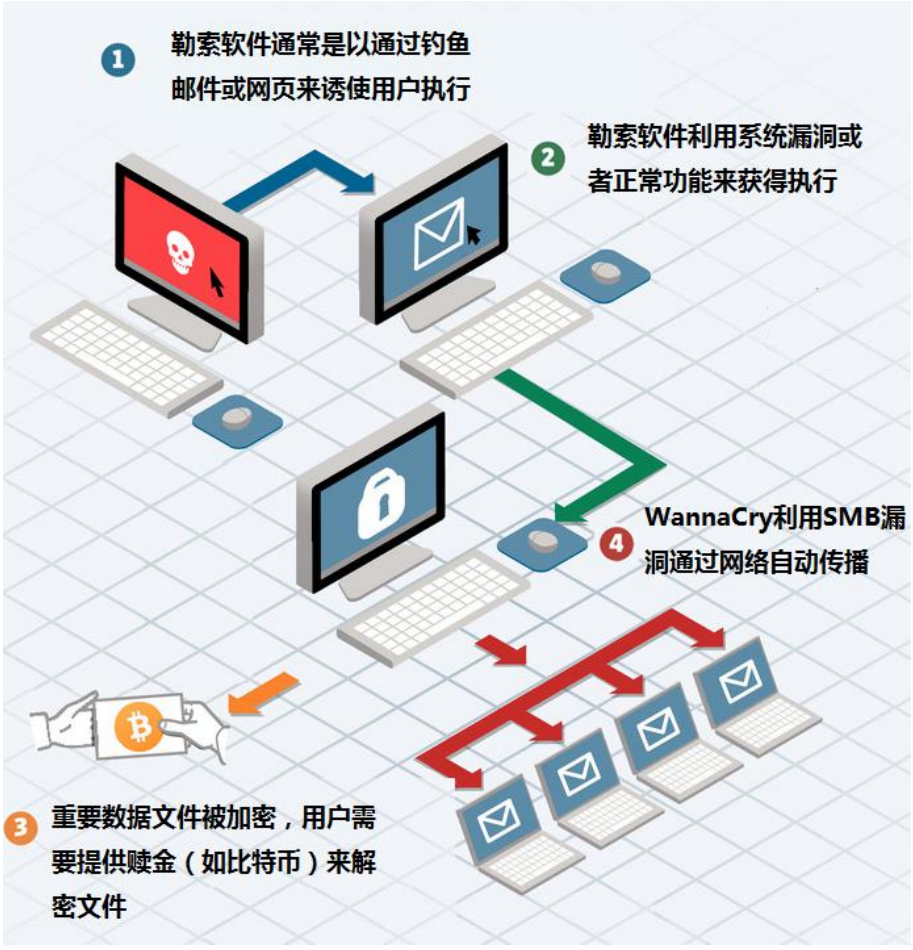
制定**网络安全事件应急预案**，并定期组织**演练**

发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行**调查和评估**，并采取技术措施和其他必要措施

➢**制定适用于省公司、地市公司的网络信息安全事件应急预案，定期组织演练及教育培训**

目录

新病毒：WannaCry第一例蠕虫型勒索软件



- 一种“蠕虫式”的勒索病毒软件，大小3.3MB
- 2017年3月份更新漏洞
- 2017年4月份出现利用代码
- 该恶意软件会扫描电脑上的TCP 445端口(SMB)
- 攻击主机并加密主机上存储的文件，
- 要求以比特币的形式支付赎金，300至600美元。

- 2017年5月12日起，全球范围内爆发基于Windows网络共享协议进行攻击传播的蠕虫恶意代码，这是不法分子通过改造之前泄露的NSA黑客武器库中“永恒之蓝”攻击程序发起的网络攻击事件。五个小时内，包括英国、俄罗斯、整个欧洲以及中国国内多个高校校内网、大型企业内网和政府机构专网受影响。

数据安全成为新形势下网络工作的新挑战和难点

- “网络运营者应当按照网络安全等级保护制度的要求，……，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“——《网络安全法》
- 数据安全管理是一项长期性极具挑战性的工作。

数据安全本身的挑战

- 数据安全是涉及国家安全。
- 用户隐私收到前所未有的威胁。
- 数据价值日益受到不法分子觊觎。
- 数据安全挑战传统的防护边界。
- 数据安全对管理精细化要求高。
- 大数据技术的应用而相应的数据保护技术还不完善。

内部问题和难点

- 制度不完善，未成体系。
- 相适应的组织结构尚未建立。
- 做好数据安全管理对帐号权限、日志审计、安全漏洞等基础性安全管理工作提出了更高要求。
- 数据安全防护手段缺失。

江苏移动安全服务产品

江苏移动网络与信息安全服务产品发展目标

- 在电信运营商网络信息安全服务市场快速发展的趋势下，江苏移动顺势而为
- 依托品牌优势及自身技术积累，通过与国家专业队伍及安全厂商等合作
- 提供专业可靠的安全解决方案、产品和服务
  （涉及安全评测、DDoS攻击防护、安全专业人才培养和资质认证等内容）
- 逐步成长为 ***区域的***、***可信的***、***优质的*** 网络信息安全服务提供商

业务优势

品牌硬

- 中国移动实践品牌经营，具备强大的企业竞争优势和综合实力

能力强

- 江苏移动业务基础雄厚
- 网络安全实验室为江苏移动网络安全创新发展奠定坚实基础

服务对象

政企客户（包括IDC客户）

- 面向集团客户提供DDoS攻击防护、安全评测等安全服务

行业客户

- 面向行业从业人员提供网络信息安全专业教育培训和资质认证服务

目录

网络钓鱼-社会工程学攻击成为未来的重点

- 9月2-3日，江苏移动组织了全省范围的人员安全意识的测试，是本次70周年保障应急演练的一部分
- 通过仿造OA邮箱做了一个重置密码的网页。使用139邮箱，修改邮箱别名，假冒管理员向省市公司目标人群发送钓鱼邮件，被钓鱼人员收到邮件后，就会误认为自己邮箱登录异常。如果安全意识薄弱，不加以仔细识别。就会直接在邮件里面点击链接，访问假的重置密码页面，一旦点击提交，这个账号就会被记录。
- 本次测试发送钓鱼邮件给重点岗位人员764人，共18人被钓鱼，其中有人重复输入2-3次。

钓鱼邮件群发

发件人: 中国移动OA邮箱系统<oa-system@139.com>
收件人: 中国移动OA邮箱系统<oa-system@139.com>
时间: 2019年8月31日 (周六) 10:51
大小: 40 KB

您好！
系统检测近期您的邮箱账户存在多地点登录的情况，疑似账户信息已泄露，请尽快核实处理！

中国移动OA邮箱系统提示：
1、切勿轻信陌生地址/号码发送的邮件、短信、即时通讯信息；
2、不要随意访问来源不明的网站，谨防网页上的钓鱼链接；
3、不要轻易在网上留下身份证号、手机号等重要个人身份信息；
4、不定期的更新账户密码，增强密码强度，避免使用123456、password这样的弱口令。

近7日登陆历史：

登录地点	IP地址	登录时间（以北京时间为准）
浙江杭州	112.57.85.*	2019/9/2 11:36
美国加利福利亚	121.257.85.*	2019/9/2 8:34
浙江杭州	212.57.85.*	2019/9/1 21:16
江苏苏州	132.151.56.*	2019/9/1 20:11
江苏无锡	132.151.62.*	2019/9/1 17:47
江苏南京	221.151.12.*	2019/9/1 15:17
江苏南京	211.32.19.*	2019/9/1 13:36
北京北京	221.32.159.*	2019/8/31 21:16
香港九龙坡	208.171.112.*	2019/8/31 18:34
北京北京	212.95.61.*	2019/8/31 15:39
江苏无锡	122.46.45.*	2019/8/30 21:16
北京北京	183.13.112.*	2019/8/30 23:16
上海上海	53.231.145.*	2019/8/29 22:17
上海上海	67.25.165.*	2019/8/29 21:09
福建南田	210.215.56.*	2019/8/29 19:06
福建南田	212.23.85.*	2019/8/29 17:33

构造仿冒网站，获取OA登录账号

钓鱼结果统计

地市	发送量	被钓鱼量
苏州	61	7
南京	63	2
无锡	60	2
常州	61	0
南通	68	0
扬州	30	1
镇江	30	1
泰州	63	1
徐州	30	0
淮安	64	0
连云港	65	0
宿迁	30	2
盐城	30	0
省攻速安全员	50	0
省公司室经理	50	2
共计	764	18

陌生异常的邮件不要轻易点击，所有输入个人账号口令的网站需要确认是否为源站。
访问的网站中可能存在恶意的木马程序，也有可能会利用浏览器漏洞获取个人终端的权限。

账号口令的破解日益频繁

近几年撞库大事件回顾

10亿账号
30万售价
——新浪财经

800万账号
40万售价
——搜狐新闻

195万账号
50万售价
——腾讯新闻

3000万账号
350售价
——快科技

暗网地下交易：你的密码只值1分钱

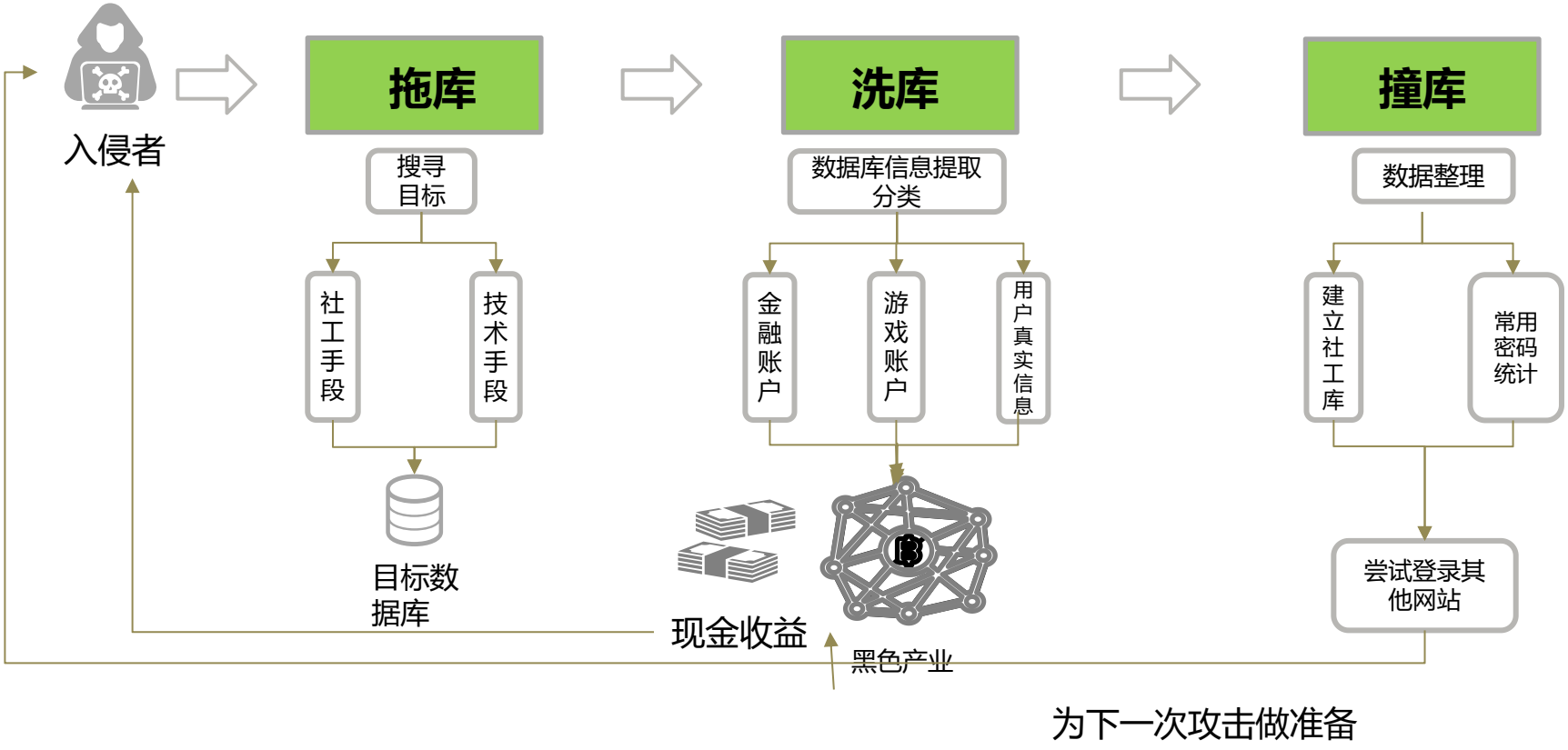
昵称：Peace_of_mind

LinkedIn
1.67亿账号

MySpace
3.6亿账号

Twitter
7100万账号

账号口令买卖已形成巨大产业链条



用户口令设置行为分析

对csdn社区、人人网、多玩网、微博等泄露的密码数据，300万+的口令样本进行分析，总结口令设置规律。

密码设置规律分布

简单型

- 密码过于简单
- 使用password密码
- 单字重复
- 使用邮箱名
- 密码=用户名

密码	排名	重复
0	3	27458次
111111	4	27328次
1	18	2781次
@163.com	51	1015次
password	70	755次
@qq.com	74	714次

手势型

- 使用电脑/手机键盘按照某种顺序排列组成密码

密码	排名	重复
qazxwsx	50	1017次
qwerty	67	777次
123qwe	78	680次
asdfgh	87	549次

规律型

- 记住一串数字的规律，演绎成复杂密码，而只需记住规则就好

常用数字规律:
- ✓ 叠词，如123123，112233，或叠加后对称 123321
- ✓ 平方根
- ✓ 开根号
- ✓ 取三角函数

密码	排名	重复
123123	6	14838次
112233	21	2536次
102030	100	484次

手机型

172418个同学中用手机号做密码的占比5%!

- 移动：139 138 137 136 135 134 147 150 151 152 157 158 159 178 182 183 184 187 188
- 联通：130 131 132 155 156 185 186 145 176
- 电信：133 153 177 180 181 189
- 虚拟运营商：170

生日型

- 使用生日或纪念日作为密码

日期格式
YYMMDD
YYYYMMDD
MMDDYYYY
其他

情感型

- 使用有纪念性或有特殊含义的语句作为密码

密码	排名	重复
5201314	5	15015次
1314520	10	5473次
7758521	12	4833次
woaini	20	2659次
iloveyou	49	1054次

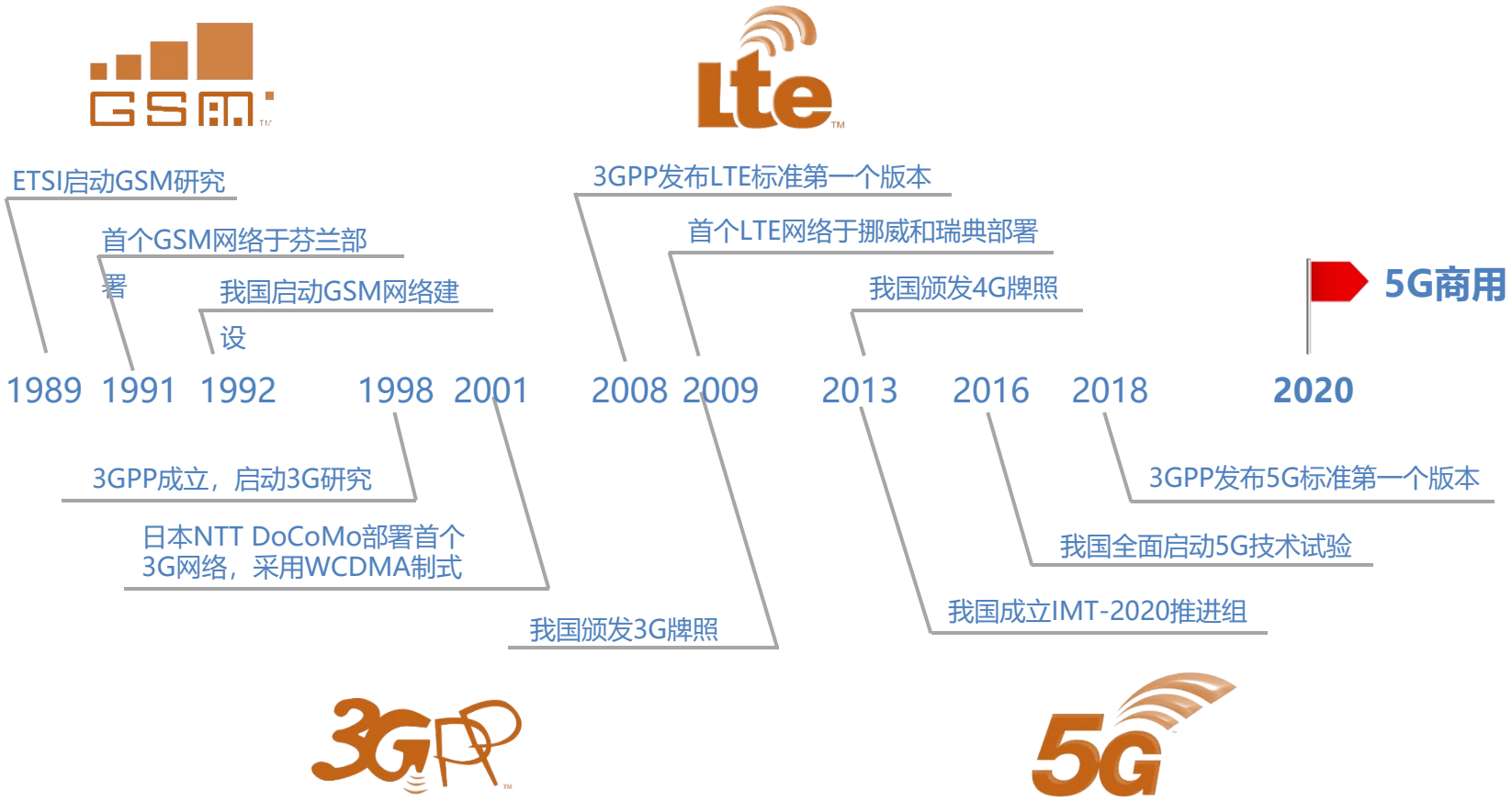
勒索软件+0day，发起主动攻击

- MongoDB勒索软件已波及上万数据库
- 你的大数据安全么？“Hadoop集群遭遇勒索软件攻击 ”（中国8300+ Hadoop集群暴露于互联网）
- ElasticSearch遭遇勒索攻击
- IBM:2016年勒索软件增长60倍 赎金规模10亿美元
- 去年攻击政府机构的勒索软件增长至三倍
- Satan依托RaaS平台提供勒索即服务
- 勒索软件成新“病毒之王”
- Wannacry勒索病毒利用微软445端口主动攻击
- 加拿大公司被迫支付赎金42.5万美金，备份数据也被加密

勒索软件发展趋势

- 勒索软件利用漏洞侵害主机
- 出现新漏洞利用，勒索软件也会更新自己的武器库
- 有些勒索软件达到10多个漏洞利用

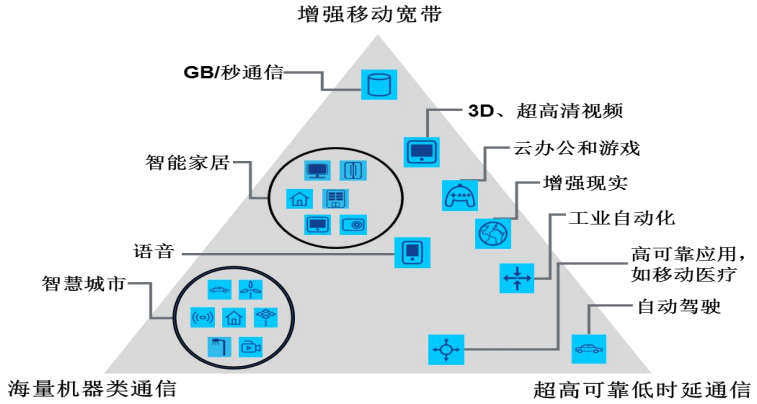
移动通信网络的演进脉络



5G：与4G有什么不同?

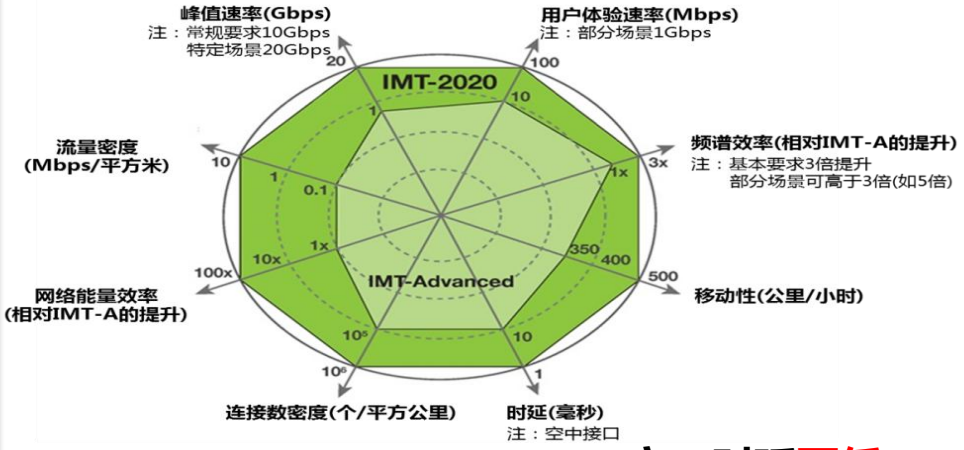
更多场景

5G不仅考虑人与人，也考虑人与物、物与物：增强移动宽带、海量物联网、低时延高可靠物联网



更强性能

相比4G主要追求速率，5G关注速率，时延和连接数密度三大关键性能指标



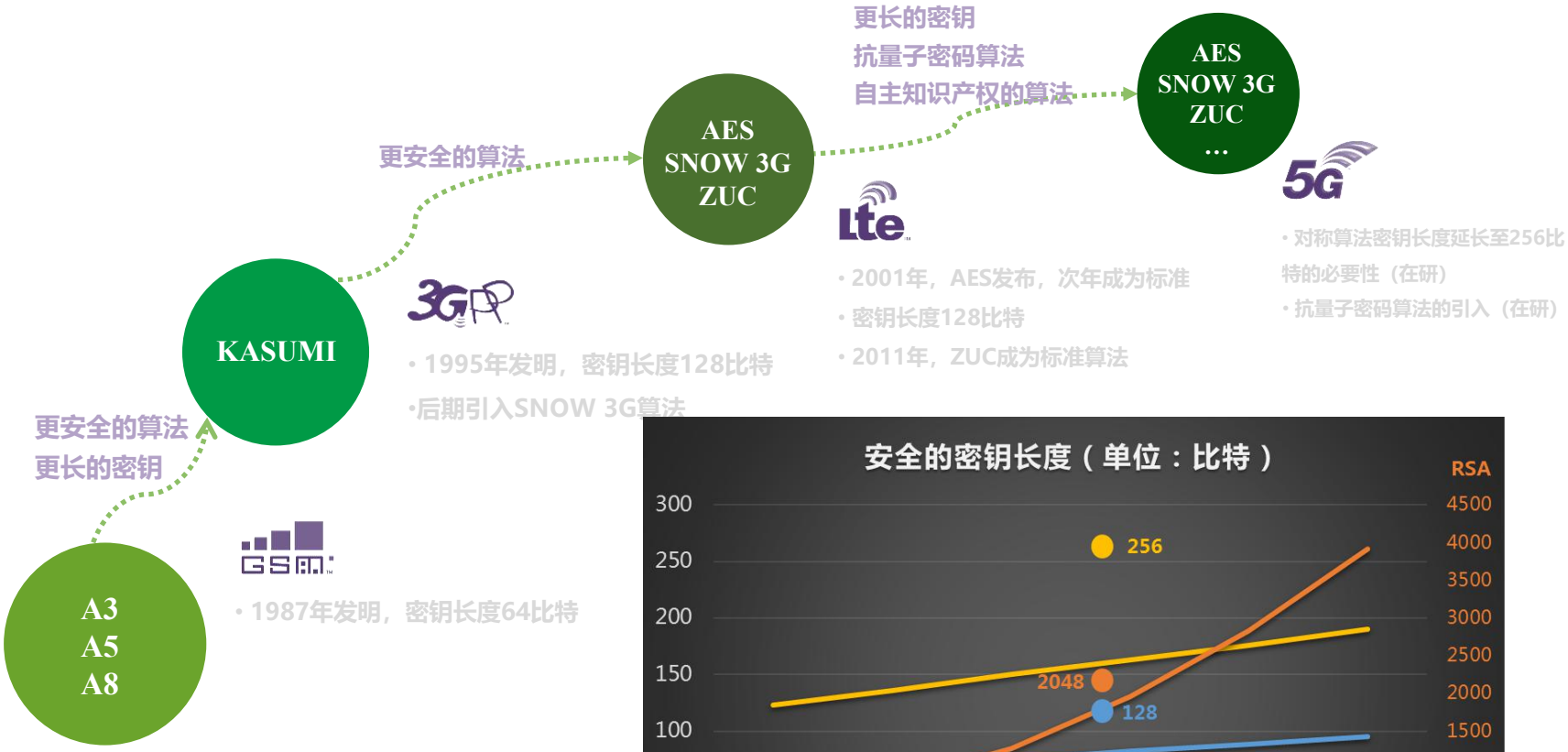
体验速率更快 4G x 100

连接数密度更高 4G x 10

空口时延更低 4G x 1/5

4G促成移动互联网的繁荣，5G将与各行各业深度融合，带来“万物互联”新机遇

移动通信网络密码算法持续演进



5G网络更安全

与2/3/4G相比，5G网络设计的安全机制更强。

更全面的

数据安全保护

- AES、SNOW 3G、ZUC
- 信令数据、用户数据完整性保护

相比的4G提升：

- 支持256位算法，**对抗量子计算机**
- 支持用户数据完整性保护，**可对抗aLTEr类攻击。**

更丰富的

认证机制支持

- 5G-AKA：抗内外部攻击
- EAP-AKA’：兼容垂直行业

相比的4G提升：

- 归属网络对拜访网络进行强制认证，**避免虚假话单。**

更严密的

用户隐私保护

- SUPI：不传递
- SUCI：由SUPI加密生成

相比的4G提升：

- IMSI（SUPI）不在空口明文传输，**保障用户隐私不被窃取。**

更灵活的

网间信息保护

- SEPP安全网关
- TLS加密传输

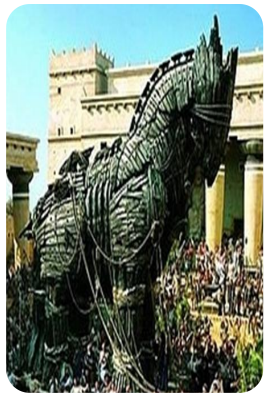
相比的4G提升：

- 标准安全网关、标准安全协议，**保障信令传输不被篡改。**

中国移动
China Mobile

谢谢！

常见信息安全事件



作弊

考试期间，利用手机、无线网络等高新科技进行作弊犯罪，QQ群里分享。

假证

黑客攻击某教育厅数据库，篡改数据记录，伪造学历证书，网上售卖。

挂马

高考期间，大量高校门户及招生网站被黑客攻击，网页挂马，造成考生电脑中毒，成肉机。

钓鱼

招生期间，不少假招生网站现身互联网，诱惑考生、家长访问，骗取用户的账户和密码。

泄密

某教授U盘被隐藏“轮渡”木马，致使办公电脑文件外泄，造成重大泄密事件。

APT攻击

斯诺登曝美国国家安全局NSA曾密集攻击清华大学 网络。

网络安全工作框架

网络安全三驾马车

中央网信办

- 制定网络安全和信息化发展战略、规划和重大政策；
- 统筹网络安全保障体系和可信体系建设；
- 负责互联网信息内容管理，维护互联网意识形态安全；

公安部

- 监督、监测、指导计算机信息系统安全保护工作；
- 查处计算机违法犯罪案件；
- 打击网上淫秽、反动等有害信息；

工信部

- 制定互联网安全的规划、政策和标准；
- 制定“双新”安全评估制度并组织实施；
- 指导企业落实网络安全管理责任，组织开展网络环境和信息治理，配合打击网络犯罪等；

部级机构	省级机构	地市级机构	主要接触点
CNCERT	CNCERT/JS		➢互联网漏洞监测
网络安全保卫局	网警总队	网警支队	➢等保检查 ➢网络案件调查配合
网络安全管理局	网络安全管理处	行管办	➢两部委考核现场检查 ➢远程监测

江苏移动网络安全服务体系

中国移动 China Mobile

安全评估类

- 主机安全漏洞扫描服务
- WEB安全漏洞扫描服务
- 安全基线配置核查服务
- 渗透测试服务

安全防护类

基础安全

- 网站安全防护服务（云WAF）
- IDC安全托管服务
- 安全专线服务

内容安全

- 电信欺诈治理服务
- 伪基站治理服务

移动安全

- APP安全检测服务
- 移动终端安全管理服务

网络安全

- DDoS安全防护服务
- 网络安全设备托管服务

专项保障

- 重大活动安全保障
- 安全威胁管理服务

安全专家类

- 安全专家培训服务
- 安全资质认证服务
- 单次现场安全服务（漏洞加固/应急响应）

重点推荐服务

云WAF服务

现有能力基础

云WAF

- 在苏州试点部署云WAF（Web应用安全云防护系统），实现云端协同联动和一键防护功能，提供网站集中化安全防护和防篡改能力

现有安全资源

- 目前苏州部署两个节点（主备系统），由厂商负责软硬件维护及配套的防护服务支撑

主要服务内容

WEB应用基础防护

- 防护网站面临的SQL注入攻击、XSS跨站攻击等常见的Web攻击，防护网站内容不被恶意篡改等

CC攻击防护

- 快速识别恶意流量，针对应用层CC攻击进行防护

抗D服务

- 可以防御对网站发起的如Syn Flood攻击、Tcp Flood攻击等大流量网络层DDOS攻击；

协同防御

- 当检测到多个网站被相同网站攻击后，根据大数据分析结果对恶意IP进行全网拦截

目标客户

集团客户（政企客户）

中小型网站

产品特点

“零部署”、“零维护”
弹性扩展、节省投资
可以按需按年按防护量弹性购买

服务组织

早期可以考虑安全厂商作为主要的服务支撑方，移动人员主要负责售前推广

DDoS安全服务

现有能力基础

省公司

- 省级流量清洗平台旁挂省网四核心，具备 **160G** 的清洗能力

地市公司

- 地市级流量清洗平台建设在地市城域网出口（已扁平化），一般 **40-80G** 清洗能力。
- 苏州具备 **400G** 的清洗能力。每个IDC出口单独配置清洗设备 **20-80G** 不等

可以采用厂家产品化的流量清洗平台，为客户提供抗DDoS服务

主要服务内容

流量监测

- 对客户的入流量进行实时采集和统计，对客户业务流量进行实时监测
- 针对异常流量进行跟踪及综合分析，及时提供告警（结合手机终端、邮件）

智能攻击防护

- 攻击源阻断
- 采用MPLS LSP，将攻击流量集中牵引至清洗云（用户零配置）；
- 将攻击流量进行遏制，清洗后正常流量回注给客户网络

可视化报表

- 提供实时的客户流量分析报表
- 提供客户的DDoS攻击特征分析报表（包括攻击时间、攻击流量分析、攻击来源等）

服务组织：正在组建省内7*24小时抗DDoS售后支撑团队，提供SLA服务

目标客户

集团客户

IDC客户

目前正在**无锡**和**苏州**等地对客户提供流量清洗试点服务

产品特点

1. **快速应急响应**
   结合数据采集主动探测快速发现
2. **快速告警自动清洗**
   结合手机终端实现秒级告警推送
3. **高感知客户自助**
   结合多维状态监测实现高度感知
4. **随时运营，高效自助**
   结合手机终端实现一键自助清洗

安全培训服务

现有能力基础

江苏安全实验室

- 目前已建设具备安全攻防实战与培训、网络流量监测、WEB安全实验、安全监控、产品验证测试等功能的网络安全攻防平台，具备培训实操中良好的实验室安全攻防环境；
- 实验室已经通过国家权威机构的权威认证，计划打造成安全认证基地

主要服务内容

技术实操培训

- **配置加固**：对操作系统、数据库、WEB应用等安全配置和加固手段进行实操
- **渗透测试**：对渗透测试原理及步骤进行讲解与演示
- **应急处置**：综合分析、定位并处理安全类事故、故障、事件的进行演练

实战攻防对抗

- 在虚拟化平台上模拟出由安全专家总结与抽象的的安全网络结构和配置进行演练
- 模拟生产网和支撑网，在复杂网络环境下进行红蓝两方攻防对抗演练

资质认证培训服务

- 与国家权威机构合作，结合资质培训课程，向通过从业人员提供权威的安全资质培训认证

目标客户

集团内部客户（总部、兄弟省公司、研究院等）

政企客户

产品特点

贴近行业与业务流
（含城域网流量监测和清洗贴近实际岗位能力要求）
可定制的培训方案
（支持客户定制所需培训项目）

服务组织

培训实施团队可考虑与CERT、测评中心等国家专控队伍合作；攻防平台由自有人员维护。

IDC安全托管服务

现有能力基础

IDC基础业务

- 机柜和带宽租赁，主机托管等

现有安全资源

- 抗DDoS手段
  - 防火墙
  - IDS/IPS
  - WAF
- 防病毒软件
- 网页防篡改防护
- 安全扫描产品
- 安全网关

主要服务内容

基础安全防护

- 采用硬件或者虚拟化的技术部署安全防护手段，提供补丁管理、防病毒等服务
- 在全网骨干节点部署DDOS防护设备，提供异常流量清洗服务

安全评估

- 通过扫描平台，为客户提供全面的安全扫描（主机漏洞扫描、WEB安全扫描、配置核查等），并定制化地提供月度的安全报告

WEB安全监控

- 部署Web防护设备，实现网页防篡改监测、挂马监测等，并防范常见的WEB安全攻击

目标客户

已入住IDC机房的重要客户、新增IDC入住客户

产品特点

高效性、广泛性、安全性、管理便捷

服务组织

可以考虑安全厂商作为主的服务支撑方，IDC业务现有安全运维人员为辅

安全专线服务

现有能力基础

现有业务

- 专线接入

现有安全资源

- 抗DDoS手段
  - 防火墙
  - IDS/IPS
  - WAF
- 防病毒软件
- 网页防篡改防护
- 安全扫描产品
- 安全网关

主要服务内容

安全评估

- 通过扫描平台，为客户提供全面的安全扫描（主机漏洞扫描、WEB安全扫描、配置核查等），并定制化地提供月度的安全报告

防DDoS

- 异常流量监测
- 异常流量清洗

WEB安全监控

- 挂马监测、内容监测、WEB攻击防护

网络安全基础服务

- 托管式方案在运营商侧专线汇聚机房集中部署安全网关，为客户提供FW、VPN、IPS、防病毒等安全服务；

目标客户

专线客户

产品特点

全面的、集成的安全防护平台自动化安全监测

服务组织

可以考虑安全厂商作为主的服务支撑方，网络安全运维人员为辅