网络信息安全

从国家到企业的若干思考

演讲人：吴亚飞

职务：国家信息中心信息与网络安全部主任

日期：2014年9月24日

提纲

- 背景和形势
- 信息安全面面观
- 发展战略性新兴产业：云计算与大数据
- 若干思考

今年2月27日揭开了中国信息化新篇章

- 2014年2月27日注定要成为一个值得纪念的日子，这一天中央网络安全和信息化领导小组宣告成立。
- 这是十八届三中全会以来继中央全面深化改革领导小组、中央国家安全委员会之后，中央在现有架构外新设立的第三个“超级机构”。由中国最高领导人出任领导小组组长，国务院总理及主管意识形态工作的政治局常委担任副组长，规格之高、力度之大、立意之远，前所未有，这将更有力、更权威地统筹指导中国迈向网络强国的发展战略
- 今年是中国互联网发展20年，作为世界第二大经济体和第一网民大国，中国在面对信息技术革命时做出的任何一项重大决策变化都会引起国内外格外关注。

中央网络安全和信息化领导小组宣告成立体现了中国最高层加强顶层设计、保障网络安全、推动信息化发展的决心

- 中央网络安全和信息化领导小组宣告成立和中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，再次体现了中国最高层全面深化改革、加强顶层设计的意志，显示出在保障网络安全、维护国家利益、推动信息化发展决心
- 这是中共落实十八届三中全会精神的又一重大举措，是中国网络安全和信息化国家战略迈出的重要一步，标志着这个拥有6亿网民的网络大国加速向网络强国挺进。

网络安全和信息化是当今世界之大势

习近平指出:

- 当今世界，信息技术革命日新月异，对国际政治、经济、文化、社会、军事等领域发展产生了深刻影响。信息化和经济全球化相互促进，互联网已经融入社会生活方方面面，深刻改变了人们的生产和生活方式。
- 我国正处在这个大潮之中，受到的影响越来越深。我国互联网和信息化工作取得了显著发展成就，网络走入千家万户，网民数量世界第一，我国已成为网络大国。
- 同时也要看到，我们在自主创新方面还相对落后，区域和城乡差异比较明显，特别是人均带宽与国际先进水平差距较大，国内互联网发展瓶颈仍然较为突出。

网络安全和信息化是一体之两翼、驱动之双轮

习近平强调指出:

- 网络安全和信息化对一个国家很多领域都是牵一发而动全身的，要认清我们面临的形势和任务，充分认识做好工作的重要性和紧迫性，因势而谋，应势而动，顺势而为。
- 网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。
- 做好网络安全和信息化工作，要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业 。

新时期网络安全赋予了更加深刻与广泛的内涵

- 在不同时期，对网络安全有过不同的称谓和解释，其内涵在不断深化，外延在不断扩展。
- 当前，我们关注的网络安全包括意识形态安全、数据安全、技术安全、应用安全、资本安全、渠道安全等方面，其中既涉及网络安全防护的目标对象，也反映维护网络安全的手段途径。

政治安全是头等大事 基础网络和重要系统安全是重中之重

- 网络安全中涉及政治安全是根本。
- 网络安全的另一个重要方面是网络与信息系统的安全。几年前的“震网”病毒使伊朗核设施受到大面积破坏，显示出关键基础设施已经成为网络武器的真实攻击目标，有可能引发灾难性后果。试想，在危机时刻，如果一个国家涉及国计民生的关键基础设施被人攻击后瘫痪，甚至军队的指挥控制系统被人接管，那真是“国将不国”的局面。

严峻的形势 紧迫的需求

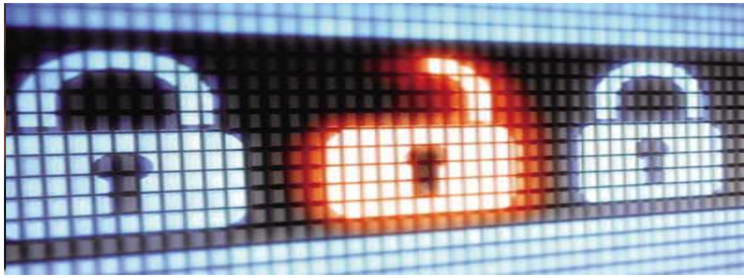
- 回顾近两年，信息安全领域就像是上演了一部跌宕起伏的大片，吸引了整个世界的眼球，也彻底颠覆了人们对信息安全的认识，世界各国纷纷调整在网络空间的战略部署，网络空间格局面临重大变革。
- 一方面我国在信息安全方面经历了广泛的质疑，我国信息技术企业遭遇了广泛的“安全壁垒”，认识到了信息安全的差距，“棱镜门”事件给我国敲响了警钟，促使我国将注意力转向本质安全。
- 展望2014年，网络空间竞争将更加激烈，我国面临的信息安全风险将进一步加剧，为应对这一严峻形势，我国信息安全将转向自主发展之路。

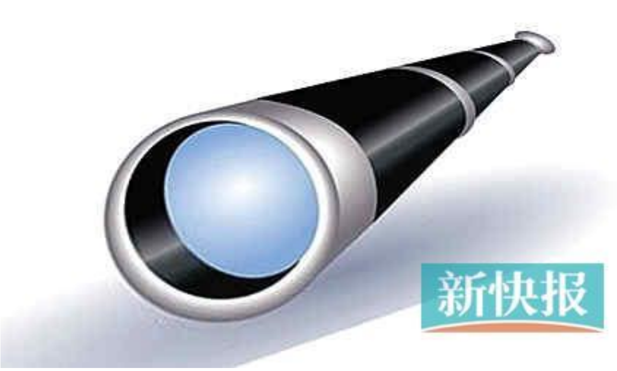
信息安全形势的基本判断

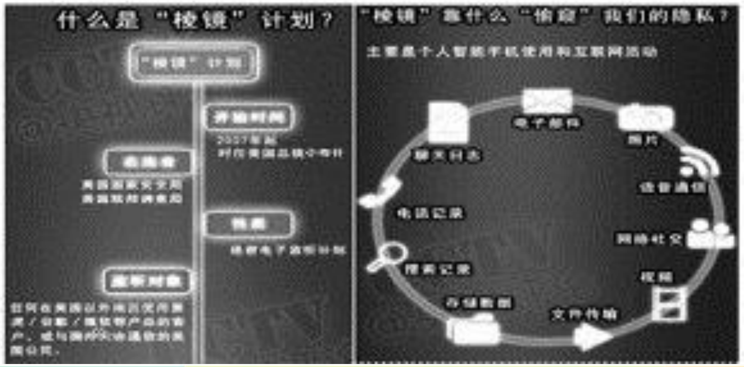
- 世界各国纷纷加强网络战备，网络空间剑拔弩张
- 当前，网络空间已经上升为与海、陆、空、太空并列的第五空间，世界各国都高度重视加强网络战的攻防实力，发展各自的“网络威慑”能力。
- 西方启动贸易保护安全壁垒，相关企业将受重大冲击


SNOWDEN
IS A
HERO!
WORLD CAN'T Wait.org for Truth


PASSWORD




新快报


什么是"棱镜"计划？
"棱镜"靠什么"偷窥"我们的隐私？


So SAFE I'm SCARED
Don't LISTEN to
Albert Einstein
Thomas Edison
Ben Franklin
They were High School DROP OUTS TOO!

棱镜门验证了网络信息安全风险比以往时候更加严重

“棱镜门”折射我国信息系统安全风险依然存在

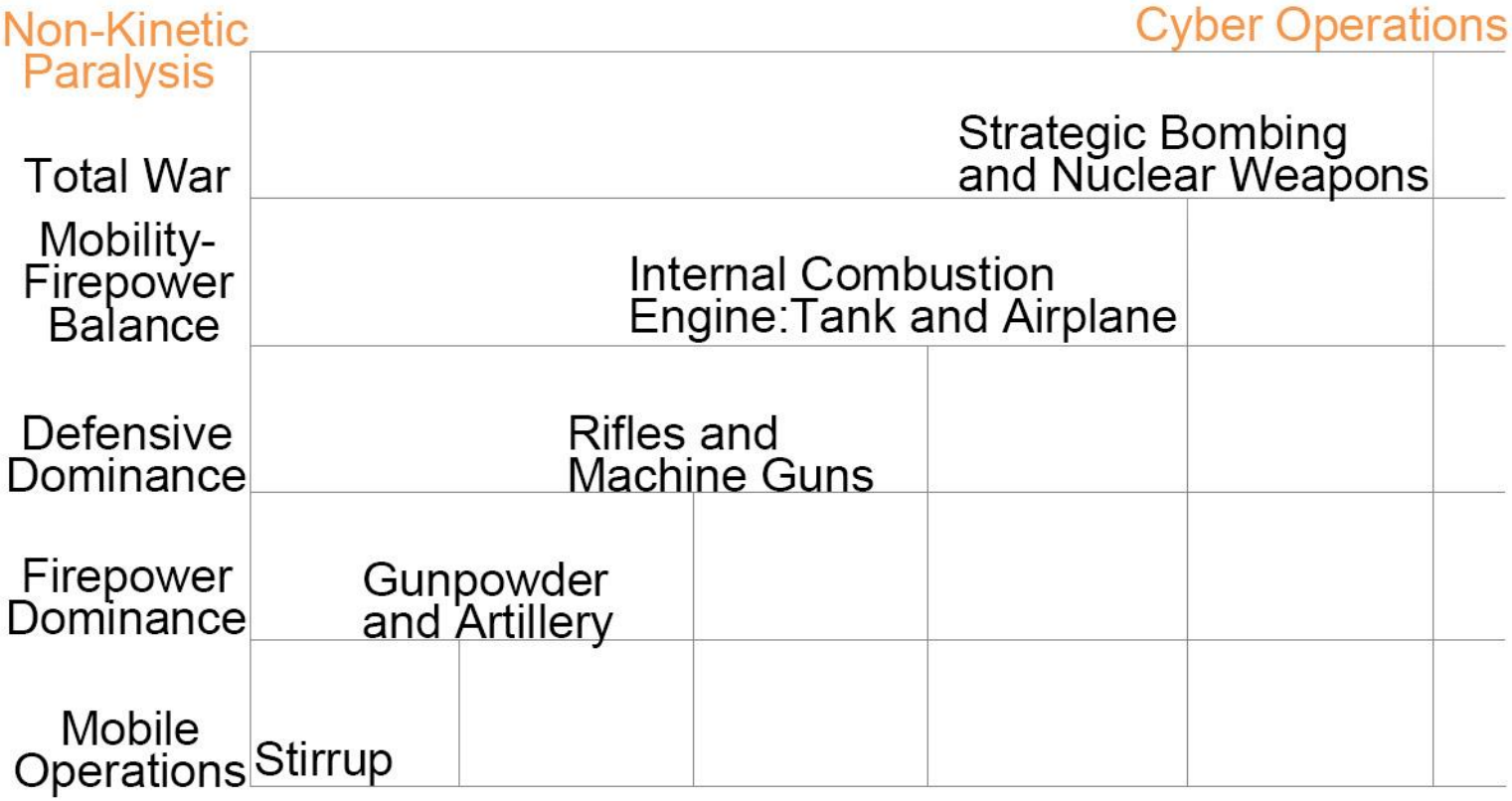
- “棱镜门”事件的曝光，使我们既感到震惊，更使我们认识到加强我国网络信息安全仍然是一项长期而艰巨的任务，其中之一就是必须痛下决心，加强我国信息产业的自主创新，从根本上加强我国基础网络和重要信息系统的安全保障与安全防护能力。
- “棱镜门”事件再次验证了由于基础信息网络和重要信息系统的核心设备、技术和高端服务主要依赖国外进口，在操作系统、专用芯片和大型应用软件等方面不能自主可控，给我国的信息安全带来了深层的技术隐患。
- 随着信息化推进和“大数据”时代的到来，无疑给“信息安全”带来了更加严峻的考验。

棱镜门事件表明我国重要信息系统安全防护面临新的复杂形势

网络与信息安全面临日益复杂严峻的形势

- 进入新世纪以来，经济社会发展对信息网络和信息化的依赖程度越来越高，信息化已成为推动社会和经济发展的重要力量和各国竞相争夺的制高点，国际信息化大势不可逆转。
- 随着中国迅速崛起引起国际社会的广泛关注。信息化不仅成为经济发展的强大推动力，而且成为中国联接世界的重要纽带。在全球网络空间国际竞争日趋激烈的背景下，我国的信息安全问题更加错综复杂，对灾备西建设的需求日益紧迫。

棱镜门事件验证了实体空间的大规模毁灭战争正在向网络空间的大规模瘫痪战争转移



安全新问题层出不穷

Tenda®

D-Link®
Building Networks for People

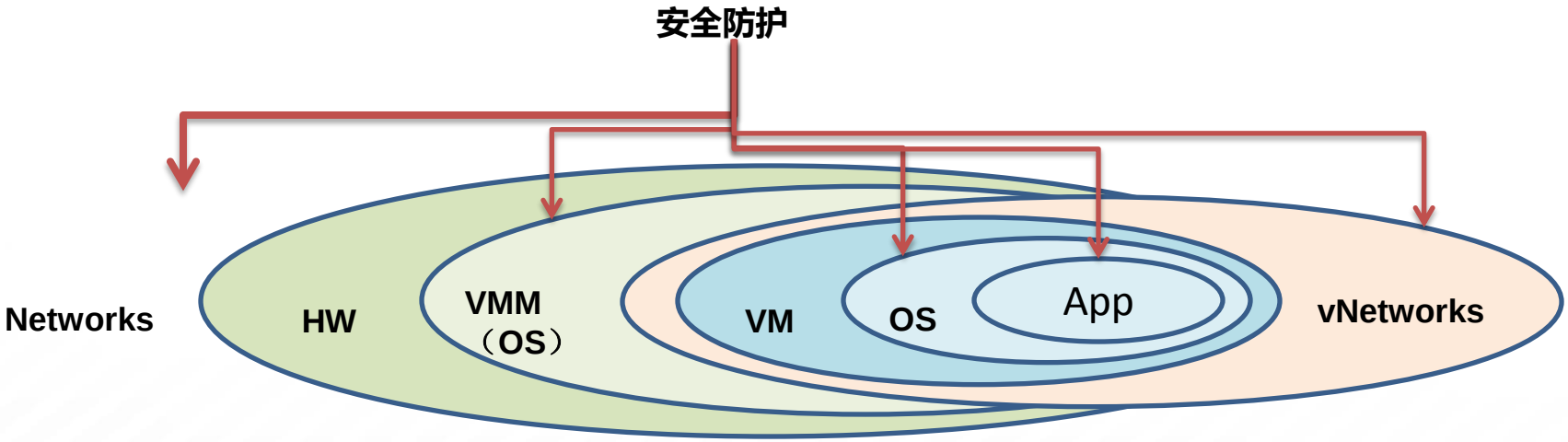
Struts™

微软公司停止为Windows XP提供服务

- 微软將於今年4月8日起停止為Windows XP推送安全補丁及系統修復。這一決定給中國的信息安全帶來重大影響？我们也将要為此付出巨大成本？中國工程院院士倪光南表示，對中國而言，微軟對XP停止服務如不予以重視，可能會是一個“重大的信息安全事件” 。
- 《2012年度中國軟件盜版率調查報告》的數據，在中國的PC中，XP的市場份額佔73.5%，即XP在用量約為2億台，其中84.2%用戶沒有升級到“視窗8”的計劃。由于视窗8安全机制对我没是一个黑盒子，其架構會使用戶電腦被微軟高度掌控，因此国家明确政府现阶段禁止采购。

云计算面临新的网络安全威胁

传统威胁	引入威胁
主机安全威胁：主机操作系统漏洞利用	虚拟化自身的安全威胁： Hypervisor脆性
网络安全威胁：拒绝服务攻击	虚拟化引入的安全威胁：虚拟机及虚拟网络管理
应用安全威胁：Web安全威胁	多租户引入的安全威胁：多租户接入及数据存储



移动终端安全问题突出

◆ **iOS 7.0.3破解**

- KeenTeam
- 在东京举办的全球顶级安全竞赛Pwn2Own上，国内团队碁震云计算安全研究团队在不到30秒的时间内攻破了苹果最新手机操作系统iOS 7.0.3

APT攻击持续不断

◆ **APT（Advanced Persistent Threat）**

- 高级持续性威胁顾名思义，这种攻击行为首先具有极强的隐蔽能力，通常是利用企业或机构网络中受信的应用程序漏洞来形成；
- 其次APT攻击具有很强的针对性，攻击触发之前通常需要收集大量关于用户业务流程和目标系统使用情况的精确信息，情报收集极强；

Google

2009：极光攻击

2010：震网攻击伊朗核电站

RSA SECURITY

2011：窃取RSA令牌种子

Flame COOKING WITH FIRE

2012：大量攻击中东多年

狼真的来了—滴血心脏

- 在WindowsXP停服的同一天，网络安全协议OpenSSL曝出安全漏洞，危及全球包括银行、电商在内关键部门和普通用户财产和信息安全。这一漏洞一旦被恶意利用，意味着用户登录电商、网银的账户、密码等关键信息可能会泄露，造成财产损失。
- ZoomEye最新完成的扫描数据显示，中国160万个443端口中，已有3.3万个受本次OpenSSL漏洞影响。在国外，受到波及的网站也数不胜数，连NASA（美国航空航天局）也已宣布，用户数据库遭泄露。
- “这个漏洞是地震级别的。打个形象的比喻，就像家里的门很坚固也锁好了，但是发现窗户虚掩着。”这个漏洞损失多大无法确认，很多受到该漏洞威胁的公司并未认识到问题的严重性
- “这一次，狼真的来了”。

我国面临的信息安全问题的性质

- 我国面临的信息安全问题已不再是一个局部性和技术性的问题，而是一个跨领域、跨行业、跨部门的综合性安全问题。
- 它不仅是一个“不对称”的高技术对抗问题，而且是一个直接影响国计民生、关乎国家安全与政权稳定的现实问题。
- 确保信息网络安全也正在成为新世纪国家安全的重要基石和基本内涵。
- 必须高度重视这一问题

社会管理新形势使网络安全面临新挑战

发展不平衡

发展中不平衡、不协调、不可持续，地区之间、城乡之间的发展差距以及部分社会成员之间的收入分配差距依然较大，统筹兼顾各方面利益难度加大。

社会结构变化

随着改革开放的深入和社会主义市场经济的发展，长期以来在封闭半封闭环境和计划经济条件下形成的社会结构发生了全方位、根本性变化。

公民意识多元化

人们的思想意识、价值取向、道德观念多元多样多变，公平意识、民主意识、权利意识、法治意识、监督意识不断增强，共享改革发展成果的愿望日益强烈。

风险管理滞后和非常态化

◆风险评估：对风险的理解主要限定在技术层面，而不是相关方的核心利益；

- 主要基于静态，可是风险的变化日益频繁；
- 主要基于脆弱性，可是对动态发生的安全事件可能带来的风险缺乏能力

◆风险控制：技术因素 和 非技术因素

- 局部VS全局

个人信息保护严重滞后

- 用户和企业的意识淡薄
- 法律欠缺
- 对服务上的约束欠缺
- 相应的技术手段不足
- 第三方监督审计的体制和技术空缺

完善我国信息安全保障体系，也是一个持续、渐进过程

- 同其他领域一样，我国各部门各领域在涉及网络信息安全的理念、管理、操作手段上，存在着不同程度的条块分割、部门交差、效率低下等问题，导致重复投入、资源浪费、效果甚微等脱离实际、脱离民心，甚至出现形式主义现象。
- 信息安全保障体系建设要在国家信息安全战略的指导下，进一步整合资源，推进改革，革除弊端，逐步实现战略与实施的统一，建设与管理的协调，需求与投入的平衡，保障信息化建设与安全保障能力提升的统一，这必然要经过长期、渐进、甚至有反复的过程。

新形势对系统安全建设提出紧迫的要求

- 国际网络信息安全形势的日趋严峻，要求我们必须进一步提高对我国重要信息系统的信息安全保障体系的重视程度 ；
- 频发的重大灾害和巨大的安全风险要求我们建设重要信息系统灾备系统必须加快进度；
- 信息化积累和我国社会经济发展对重要信息系统的高度依赖型，也要求我们必须加快重要信息系统安全保障体系建设的统筹规划和实施推进。

深刻理解未来信息化发展迅速与安全风险增大趋势长期并存的局面

ISC 2014

◆**互联程度会进一步加强**

- 互联网；三网融合；智能电网、智能交通、物联网……

◆应用类型和范围会更快地扩展（有价值目标进一步增多）

- 智能终端

◆安全保障风险增大，难度加大

坚持“以安全保发展、以发展促安全”坚持创新，努力破除“懒政”思维

- 长期以来，对网络安全与信息化发展的关系，存在一些争论。我们确实看到，一些应用上去了，安全问题随之而来；一些新技术出来了，传统的网络安全技术防线和管理规定就会失效。没有网络安全，信息化发展越快，造成的危害就可能越大。而没有信息化发展，经济社会发展将会滞后，网络安全也没有保障，已有的安全甚至会丧失。“以安全保发展、以发展促安全”的要求，充分体现了马克思主义的辩证法，体现了科学的发展观。
- 网络安全是信息化推进中出现的新问题，只能在发展的过程中用发展的方式加以解决。不能简单地通过不上网、不共享、不互联互通来保安全，或者片面强调建专网。这样做的结果只能是造成不必要的重复建设，大量网络资源得不到充分利用，增加信息化的成本，降低信息化效益，失去发展机遇。这种“懒政”思维必须破除。要努力实现技术创新和体制机制创新，不断形成维护网络安全的新思路、新方法、新举措、新本领。

完善我国信息安全保障体系是一个持续、渐进过程

- 同其他领域一样，我国各部门各领域在涉及网络信息安全的理念、管理、操作手段上，存在着不同程度的条块分割、部门交差、效率低下等问题，导致重复投入、资源浪费、效果甚微等脱离实际、脱离民心，甚至出现形式主义现象
- 信息安全保障体系建设要在国家信息安全战略的指导下，进一步整合资源，推进改革，革除弊端，逐步实现战略与实施的统一，建设与管理的协调，需求与投入的平衡，保障信息化建设与安全保障能力提升的统一，这必然要经过长期、渐进、甚至有反复的过程

谋大事　讲战略　重运筹

- 信息安全保障工作常态化，不因一时一事更改大战略
- 网络信息安全不应影响信息化大局
- 网络信息安全不应影响中国和平崛起
- 大连通、大交互、大数据时代的到来
- 新时代呼唤大改革，大改革呼唤大开放
- 网络信息安全必须服务和保障两个大局
- 国内大局：实现中华民族复兴的中国梦
- 国际大局：为我国改革开放稳定发展争取良好外部条件

互联网最大的挑战是什么？

- 2014中国互联网大会刚刚召开，互联网影响日益深化，最大的挑战是什么？网络安全成为监管部门和互联网厂商最关心的话题
- 以手机操作系统为例，随着不同厂商对安卓系统的修改，对本已脆弱的安全体系可谓雪上加霜。上半年进行测试，发现这些手机100%存在安全漏洞。缺乏自主可控、安全可信的互联网核心技术也让网络安全形势更为严峻。
- 工业和信息化部部长苗圩坦言，“要把增强网络信息安全保障能力摆在更加突出的位置。以健全完善行业网络与信息安全保障体系为目标，坚持与时俱进、统筹考虑、综合施策、大力加强网络与信息安全保障能力建设，积极推动完善网络与信息安全的法律法规、技术标准，加强基础设施和技术手段体系化建设。

认真贯彻落实中央网络安全和信息化领导小组会议精神

- 当务之急是要认真贯彻落实中央网络安全和信息化领导小组会议精神，把各项工作做细、做实、做到位。
- 要加强顶层设计和战略统筹，加快制定网络安全和信息化发展战略、宏观规划和重大政策；
- 创新改进网上宣传，弘扬主旋律，激发正能量，综合治理网络生态；
- 加快制定急需的网络安全和信息化法律法规与技术标准，加强自主创新，建设网络安全保障体系；
- 大力提升经济社会各领域信息化水平，促进信息产业发展；
- 加快人才队伍建设。

全面提升我国信息安全保障能力，实现国家在信息领域关键和重大利益上不受侵害的“七个确保”

- 确保国家信息主权的独立和完整；
- 确保国家网络基础设施的稳固和正常运行；
- 确保信息内容健康、网络空间秩序可控；
- 确保建立在信息化基础上的国民经济可持续发展与社会稳定；
- 确保国家信息安全体系的自主性和具有较强的防卫能力和国际竞争力；
- 确保避免和化解局部或全局性信息安全危机应变能力的不断提高；
- 确保应对信息网络攻击的有效反制能力。

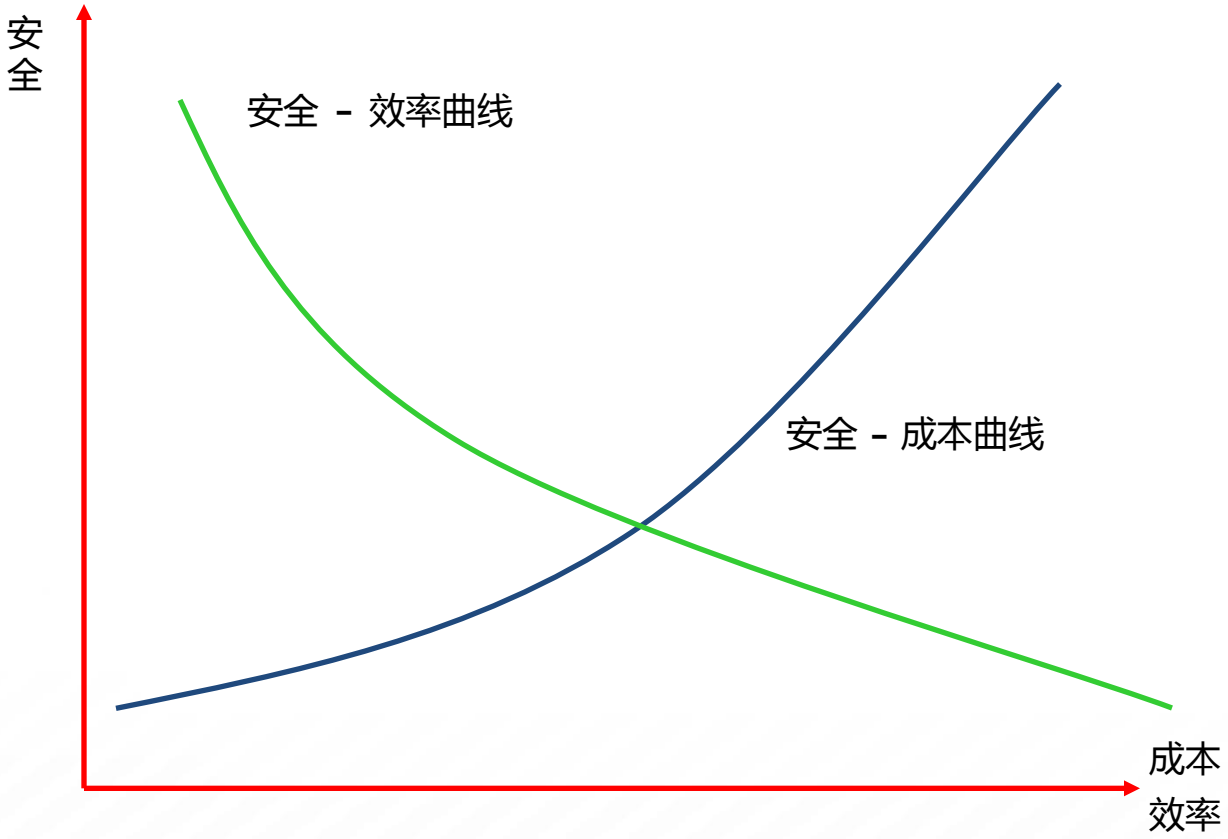
当前我国信息安全保障工作的九大任务

- 实行信息安全等级保护
- 加强以密码技术为基础的信息保护和网络信任体系建设
- 建设和完善信息安全监控体系
- 重视信息安全应急处理工作
- 加强信息安全技术研究开发，推进信息安全产业发展
- 加强信息安全法制建设标准化建设
- 加快信息安全人才培养，增强全民信息安全意识
- 保证信息安全资金
- 加强对信息安全保障工作的领导，建立健全信息安全管理责任制

继续实施“积极防御”战略的五大举措

- 建立和完善四大基础支撑体系
- 强化全社会的信息安全意识
- 稳步推进信息保障体系建设
- 积极寻求技术优势和威慑防范能力
- 加强国际合作实现和平崛起

更加关注信息安全保障体系建设的实际效能



要研究建设信息安全的综合成本与信息安全风险之间的平衡，而不是要片面追求不切实际的安全不同的信息化应用系统，对于安全的要求不同，不是,杜绝形式主义和脱离实际需求。

加快立法，加强国际合作

- 信息安全领域亟待立法。
- 信息安全领域仍需加强国际合作，
  - 开放性信息系统及其安全体系建设的合作，完善信息立法
- 重视信息系统安全风险评估工作
- 研发核心技术
- 发展信息安全产业
- 争取后发优势，确保我国的信息安全和国家安全。

网络信息安全：政府和企业都不能“无为而治”

- 从斯诺登事件、到“棱镜门”，再到苹果公司“后门”事件等等，信息安全问题有愈演愈烈之势。在这个信息爆炸的时代，信息安全已不仅直接关系到国家经济安全、政治安全、国防安全、文化安全等重大问题，也与企业信息安全和个人权宜密切相关
- 今年5月22日，国家互联网信息办公室宣布，为维护国家网络安全、保障中国用户合法利益，中国即将推出网络安全审查制度。

现代企业必须确保自身信息安全

- 确保网络信息安全是所有现代企业的战略目标
  - 保密性（Confidentiality）—— 确保信息在存储、使用、传输过程中不会泄漏给非授权用户或实体。
  - 完整性（Integrity）—— 确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性。
  - 可用性（Availability）—— 确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源
  - 关键业务活动的持续性和有效性，这更是企业命脉所在，就信息安全来说，是其根本目标。当然，要让依赖于信息环境的业务活动能够持续，就必然要保证信息环境的安全，业务持续性对信息环境提出了CIA的要求，而信息环境CIA的实现支持着业务持续性目标的实现。

没有企业的充分参与就不可能拥有强大的和持久的网络信息安全

- 信息网络应用的特性决定了国家信息网络安全保障，若没有企业和全民的充分参与就不可能是强大的和持久的。目前中国企业网络安全整体防护能力和水平较低，网民的安全意识和责任也很薄弱，民间机构、团体尚未参与到保障能力建设的进程中来，还主要是靠政府、靠行政手段来推行、实施和监督。
- 网络信息安全是信息化社会的基石。企业网络信息安全问题是国家网络信息安全的基石。关键核心技术与设备研发的自主、创新、可控，是当务之急。保障关系国计民生的重要信息系统和基础设施的安全与稳定运行，是重中之重
- 大力扶持信息网络安全产业和应用服务，发展壮大民族企业特别是安全企业是网络安全保障不可缺少的重要环节。

信息安全的根基是“自主可控”

- 可控性是指对信息和信息系统实施安全监控管理，防止非法利用信息和信息系统，是实现信息安全的五个安全目标之一。而自主可控技术就是依靠自身研发设计，全面掌握产品核心技术，实现信息系统从硬件到软件的自主研发、生产、升级、维护的全程可控。简单地说就是核心技术、关键零部件、各类软件全都国产化，自己开发、自己制造，不受制于人。
- 自主可控是我们国家信息化建设的关键环节，是保护信息安全的重要目标之一，在信息安全方面意义重大。

国内民族企业的自主创新更具亮点

- 国内一批民族企业，也纷纷加大了关键技术自主可控技术研发，制定了企业攻关规划，不少企业技术也体现了自主可控的先进性特色和先进理念。
- 技术创新是产业创新的基础和引擎。必须加强对基础材料、元器件、高端通用芯片等技术的研究，必须坚持研发高端核心装备的攻关研究，形成保证基础网络和重要信息系统安全可靠的基础支撑，逐步走在新一代信息技术的前沿。
  - **国家信息化建设核心装备的自主可控对于我国信息化建设，加速自主可控进程具有重要的战略意义**

坚持自主可控，确保网络信息安全

- 在行业快速发展的背后，我国信息技术过于依赖国外使得网络安全处于受制于人的困境，"棱镜门"事件将国内在信息安全方面的短板显露无疑。因此，要保障国家基础网络和重要信息系统安全，必须鼓励民族核心技术及产品创新，运用具有自主知识产权的产品和技术。
- 另一方面，从中央政府采购网发布的最新信息来看，2014年中央国家机关政府采购协议供货商名单中，国产软件比例明显增加，不少还是首次入围。经过几十年的发展，当前我国一系列国产软件及硬件产品虽然与国外先进国家还存在一定的差距，但是总体上技术实力已能满足国内需求，因此，在国家的大力支持下，本土企业将迎来更广阔的发展空间

自主信息化装备在大范围示范应用中得到有效推广

- 国家发改委安全专项支持了多项信息系统示范工程项目，在证券、电力、电网、金融、公安、教育、审计、统计、就业等行业领域，重点支持采用自主信息化装备，国产信息化装备在我国重要信息系统应用示范效果已经显现。在示范工程项目推动下，各级政务部门对自主可控安全产品采购量逐年增加，自主可控安全产品在政务部门占有率大幅提升；
- 从2008年到2013年，政务部门对国产信息安全技术产品的采购率从82.9%上升到99%，而对国外设备的采购率从17.1%下降到1%。为提升我国重要信息系统的安全保障能力积累了经验。

我国信息安全产业发展现状

- 产业处在波动周期的成长初期
- 内需在产业发展中的拉动作用明显
- 产业发展环境有待改善
- 产业结构有待优化
- 产品配套能力有待提高
- 安全服务有待规范

信息安全成为“产业”的理由
——产业要素的特征凸显

- 作为独立产业标志的交易品、客户、提供商、第三方等四大产业要素在信息安全领域逐渐具有区别于其他产业的差异化特征，标志着信息安全产业作为IT产业的重要分支正在迅速成长。

我国信息安全产业初具规模

- 信息安全产业规模已从2004年的53.19亿上升到2013年的264.23亿，年平均增长率达30.1%。据不完全统计，年销售过亿元的信息安全企业数量也从2004年的几乎为零，增长到目前已经超过20家
- 接受专项支持的企业创新能力明显提高，原始创新技术比例由2004年51%上升到2013年75%，国外引进改造类技术比例由2004年40%下降到2013年3%。企业研发资金投入比例逐年增加，研发资金投入占总收入比重从2004年1.6%上升到2013年10.62%。企业获得相关发明专利的数量从2004年平均1.23个，上升到2013年的每个企业平均5.35个，增长近五倍。
- 信息安全服务业规模从2008年专项开始支持时的20.55亿，上升到2013年的42.2亿，年平均增长率达33.7%。

信息安全产业发展趋势

- 随着信息技术的快速发展和广泛应用，基础信息网络和重要信息系统安全、信息资源安全以及个人信息安全等问题与日俱增，应用安全日益受到关注，主动防御技术成为信息安全技术发展的重点，信息安全产品与服务演化为多技术、多产品、多功能的融合，多层次、全方位、全网络的立体监测和综合防御趋势不断加强。
  - 向系统化、主动防御方向发展.信息安全保障逐步由传统的被动防护转向"监测-响应式"的主动防御，信息安全技术正朝着构建完整、联动、可信、快速响应的综合防护防御系统方向发展。产品功能集成化、系统化趋势明显，功能越来越丰富，性能不断提高;产品问自适应联动防护、综合防御水平不断提高。
  - 向网络化、智能化方向发展.计算技术的重心从计算机转向互联网，互联网正在逐步成为软件开发、部署、运行和服务的平台，对高效防范和综合治理的要求日益提高，信息安全产品向网络化、智能化方向发展。网络身份认证、安全智能技术、新型密码算法等信息安全技术日益受到重视。
  - 向服务化方向发展。信息安全产业结构正从技术、产品主导向技术、产品、服务并重调整，安全服务逐步成为产业发展重点。信息技术网络化、服务化等都在积极推动信息安全服务化，信息安全服务在产业。

自主可控第一步：发展自主信息安全产业

ISC 2014

- 保障信息化建设安全的必需
- 信息产业新亮点和新增长点
- 推动信息产业跨越式发展

发展原则

- 安全可控。建立完整的信息安全技术、产品、服务和标准体系，保障新技术、新应用的安全可控，保障基础信息网络和重要信息系统的安全可控，为国家、企业和个人的信息安全保障提供产业支撑。
- 创新发展。聚集各方资源，加大信息安全技术创新投入力度，突破影响产业发展的核心技术和关键产品，创新服务模式，占领价值链高端，提升产业核心竞争力。
- 应用牵引。
- 环境营造。

发展目标

- 产业规模目标。我国信息安全产业保持年均30% 以上的增长速度，占信息产业的比重稳步提高。
- 产业结构目标。信息安全产品体系进一步丰富，服务在信息安全产业中的比重以及安全可控信息安全产品和服务在国内市场的占有率明显提高，集聚效应明显、协同效应突出、发展特色鲜明的产业格局逐步形成，信息安全产业链日趋完整
- 技术创新目标。进一步提升信息安全技术和服务创新能力，突破一批信息安全关键技术和产品，形成支撑云计算、物联网和移动互联网等应用的信息安全保障能力，逐步提高信息安全防护水平，部分信息安全技术和产品达到国际先进水平，信息安全竞争能力显著提高。
- 产业组织目标。形成以具有核心技术研发能力、新技术创新能力、国际竞争力的信息安全骨干企业为龙头，具有创新活力强、特色明显、产业链协同的中小企业为基础的产业发展格局，打造一批信息安全产品和服务知名品牌，发展一批特色突出、专业水平高、创新能力强的中小企业，培育出信息安全业务收入达50 亿元的骨干企业。

中国信息安全产品市场趋势预测

- 价值流动从单一产品向安全解决方案演变，安全集成将更加普及
- 主动性安全产品将更受欢迎
- 新应用推动安全产品与服务升级换代
- 安全应用领域更加广泛
- 并购整合、上市融资等将加速信息安全企业的分化

若干建议

- 亟待加快企业发展战略规划研究
- 整合资源,夯实基础
- 以紧密围绕市场需求推进技术和产品研发，完善核心业务能力建设
- 以打造智慧城市、信息消费试点城市、两化融合示范城市和信息惠民示范城市为抓手， 积极参与国家重点工程为抓手，逐步提升内蒙古自治区信息化和信息安全保障水平
- 进一步重视人才队伍建设

以上仅仅是个人思考，

可能不妥之处甚多，敬请批评指正。

谢谢大家 ！