- 2014年2月27日，习总书记在中央网络安全和信息化领导小组第一次会议上指出：

没有信息化就没有现代化，没有网络（信息）安全就没有国家安全。

ZERO TRUST SECURITY

- 信息安全的基本要求：
  - 保密性
  - 完整性
  - 可用性
  - 可控性
  - 不可否认性

- 信息安全的两个层面：
  - 国家层面-保护国家的政治、军事、经济情报，取得信息优势；
  - 公众层面-保护商业机密、个人隐私，保障信息的可控利用。

面对来自两个层面的威胁。

- 信息安全的科学属性-学科建设
- 信息安全的工作属性-管理、法律法规
- 信息安全的产业属性-产品、服务

ZERO TRUST SECURITY

- 通信安全
- 网络安全
- 信息安全

ZERO TRUST SECURITY

- 信息安全核心技术-密码
  - 解决身份认证、信息保密、防抵赖等等。
- 密码技术、核技术、航天技术是国家安全的三大核心技术。

- 其他信息安全技术，如：入侵防范、安全审计（除数据备份、灾难恢复）等等，主要为保护密码系统。
- 信息安全的目标：所有对信息的处理均经过授权、严格按被授权者的要求，真实顺畅合理进行。信息的处理和使用可认证、可追溯。

四大领域

- 军政信息系统防护
- 国家基础设施的信息安全防护
- 公众信息服务的安全防护
- 信息管控

ZERO TRUST SECURITY

- 建立安全第一的观念
- 建立信息安全的强弱取决于系统最薄弱处的观念
- 建立信息系统安全防护从设计、研发、使用全过程的同等重要的观念
- 建立信息安全技术与管理同等重要的观念
- 建立安全产品与安全服务同等重要的观念

ZERO TRUST SECURITY

- 信息安全防护体系：
  - 保护
  - 检测
  - 响应
  - 恢复
  - 反制
- 技术+管理+教育

- 新挑战：
  - 未来网络、操作系统、核心器件与设备
  - 移动互联、物联网
  - 云计算、大数据、人工智能等新技术

- 短板1：缺乏顶层设计和长期战略
  - 基本是按照信息化的思路建设发展，过于强调跟踪世界最新技术发展、缩小数字鸿沟、提高带宽和网络普及率、积极推动互联网应用产业的发展，导致的结果就是大而不强、极易被卡脖子。网络安全的理念一直停留在外挂式、跟随式、应对式、集成式、产业式的发展模式，没有出现像赛门铁克、卡巴斯基这样的具有核心产品的网络安全企业。我们的网络安全基本是沿用信息化发展的思路，注重上市、产值、规模和经济效益，核心技术和算法基本都是引进和开源，导致的结果是在做产业、做市场，不真正解决安全问题。

ZERO TRUST SECURITY

- 对策1：树立安全和发展并重的理念，当前，可能要把安全放在更加优先的地位，既要大安全、又要小安全，特别是要引导、扶持、培养具有自主核心技术和产品的可长期发展的企业，要从源头和根子上树立自主设计、长期发展的战略指导。

ZERO TRUST SECURITY

- 短板2：网络空间核心技术受制于人
  - 管理、产品、标准、技术、资源主要由美主导控制，我们疲于跟随，这是美长期在网络空间的产品主导战略导致的结果。第一轮是八大金刚，新的一轮是大数据、云和AI，我们都认识到了，但应对不力，热衷炒概念，整个生态环境中真正做技术、做产品的比重极低。仅有的几家大型互联网企业，基本都是本土型、用户数量规模型、应用型、市场型。现在热火朝天的AI依然是应用技术型和产业型，不是军事主导型。

ZERO TRUST SECURITY

- 对策2：对内，实施自主可控、安全可信战略，鼓励、支持原创型、技术型、产品型的发展模式。对外，支持和扶持国际型和产品型企业的发展。加大、加速军事AI的牵引和发展。

ZERO TRUST SECURITY

- 短板3：网络空间美对我具有非对称优势，单向透明
  - 兰德公司报告形容，在网络空间我是“玻璃龙”，看我不仅一清二楚，而且一敲即碎。美具有强大的威慑能力，其威慑战略很清晰，而我的网络空间威慑能力严重不足，这是美政府威慑战略的结果。奥巴马宣称，“中美如果爆发网络战，美国必胜”。

ZERO TRUST SECURITY

- 对策3：网络空间与核、太空相似，攻难防更难，谁都不能确保完全防御，因此，必须实施**非对策制衡**战略，你打你的，我打我的，大力发展进攻能力，实施杀手锏工程，打造杀手锏武器。这方面，军队是主体、主力军，但是，需要政府、企业的全力配合。

ZERO TRUST SECURITY

- 短板4：网络空间优秀人才严重失衡
  - 美是面向全球，汇聚顶尖人才，机制也利于其发展，这是美DARPA等其他政策导致的结果。而我们人才基数不小，但基本立足国内，而且集中式、团队化发展很难。国际黑客大赛，美国人组织，自己不参加，获奖的都是中国团队。“攻击五角大楼”等系列活动，实际是“漏洞悬赏”，参加人员已经扩展到五眼国家。

- 对策4：建立网络空间国家安全战略实验室，迈开面向全球的步子，打造核心技术、人才、机制的高地。

- 短板5：网络空间数据主权顶层设计不足，使用数据的导向不清晰
  - 美西方再次抓住机遇，提前进入云计算、大数据时代，已经建立起数据资产保护、安全和发展的战略，而我们零散、分散。绝大部分大数据都被美国掌握，阿里、腾讯等都在境外上市，季度报表都含有核心数据信息的披露。目前，仅政府或关键行业相关的数据还在我们自己手里。

- 对策5：制定实用、管用的战略、政策，建立国家统一的大数据中心（不是一个），要能**管数据、用数据、出数据**。

- 短板6：政府、行业、企业的网络安全防护能力不强
  - 政府、行业、企业的网络安全防护水平不高、政策不当、技术不足，没有明确和清晰的策略，没有专业的队伍，各自分散防护，没有形成协同联动，这是我们致命的弱项。美防御职责十分清晰，网络空间司令部、国土安全部等分工明确，专业队伍、政策都很清楚。

- 对策6：抓紧建设“国家网络空间战略预警与积极防御工程”，建立“国家网络边防”系统。不能分散、独立防御，美国现在的策略都是动用全部国家或全部政府的力量和资源进行攻击和防御。我们防御要各负其责，但是，军队要指导，利用进攻的技术和对威胁的掌握进行指导，必须联合、联动、联防。

- 短板7：网络空间博弈的制胜理念不清晰
  - 网络空间的博弈始终表现为**能力的竞争**，是一种动态的、持续的对抗，依靠技术制胜、资源制胜、人才制胜，**综合性、变化性、融合性**很强。我们还没有深刻认识到这一点，还没有树立能力制胜的战略。在网络空间，有没有一招鲜；有没有核武器那样的杀手锏；如何取得制网权；不只是一个回合，而是反复斗志斗勇，如果赢了第一个回合，还要继续接招，继续打下去。

ZERO TRUST SECURITY

- 对策7：树立**能力制胜**的理念，努力、积极打造持续的网络能力，以**军事能力建设**为主带动国家网络能力建设，现在的牵引都是经济、产业、用户等为指标的带动，应该扭转，根本性的应该是以军事能力的提升为最重要的指标，历来如此。发挥制度优势，通过国家网络靶场的建设，全力打造军民融合网络军工集团，确保能力持续生成。

ZERO TRUST SECURITY


谢谢
ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原“中国互联网安全大会”）