网络空间安全**基本含义**:

信息安全要保证信息的保密性，真实（认证）性，完整性，不可否认性
网络空间安全涉及四个层面：设备系统数据应用
网络安全的目的是保护信息免受威胁，减少损失

主要威胁有:

非授权访问，窃取，篡改，假冒，抵赖，拒绝服务攻击

网络空间安全的主要目标:

实现信息机密性，完整性，　　认证性，　　不可否认性，　　可用性，可控性
实现方法：加密　完整性机制　　身份认真机制　审计，不可抵赖机制　备份恢复及可用机制

网络空间安全**基本属性：**

机密，完整，认证：（分为实体认证和消息认证）？不可否认（是针对通信各方信息真实同一性的安全要求）可用性（可提供服务）可控性，可审查性（事后追究）？？（问）
可将网络空间安全的发展划分为传统安全阶段和现代安全阶段

通信安全阶段主要指信息的保密性，研究仅限于密码学，在计算机出现之前都属于这个时期
信息保障 IA 的模型 **PDRR:**protect,detect,react,restore 信息安全保障体系

CIA 三元组（金三角）是信息安全的三个最基本的目标：confidentiality 机密性，integrity，availability
密码学是 CIA 的技术基础
DAD 是最普遍的三类风险：disclosure，alteration，destruction
OSI?
APPDRR 动态安全模型 比 PDRR 多了 assessment policy(安全策略)（安全策略在整个网络安全工作中处于原则性的指导地位）系统防护，实时监测，实时响应，灾难恢复