信息安全工程原理

周宁

CISA　BS7799LA

zn_ning@sjtu.edu.cn

上海交通大学信息安全服务技术研究实验室

- 上海交通大学信息安全服务技术研究实验室（Lab of Information Security Service, LISS），隶属于信息安全工程学院，成立于2001年1月，是以安全攻击和防范技术、信息安全管理、安全产品测试、信息系统评估等信息安全服务技术研究为主的科研机构；也是专门从事信息技术产品、信息系统安全测评的专业第三方机构，是国内最早开展信息安全测评的机构之一。

上海交通大学信息安全服务技术研究实验室

- 2006年底，实验室业已通过了中国合格评定国家认可委员会（CNAS）的检测实验室认可、检查机构认可以及计量机构认可，是目前国内高校科研机构该类型认可的第一家。

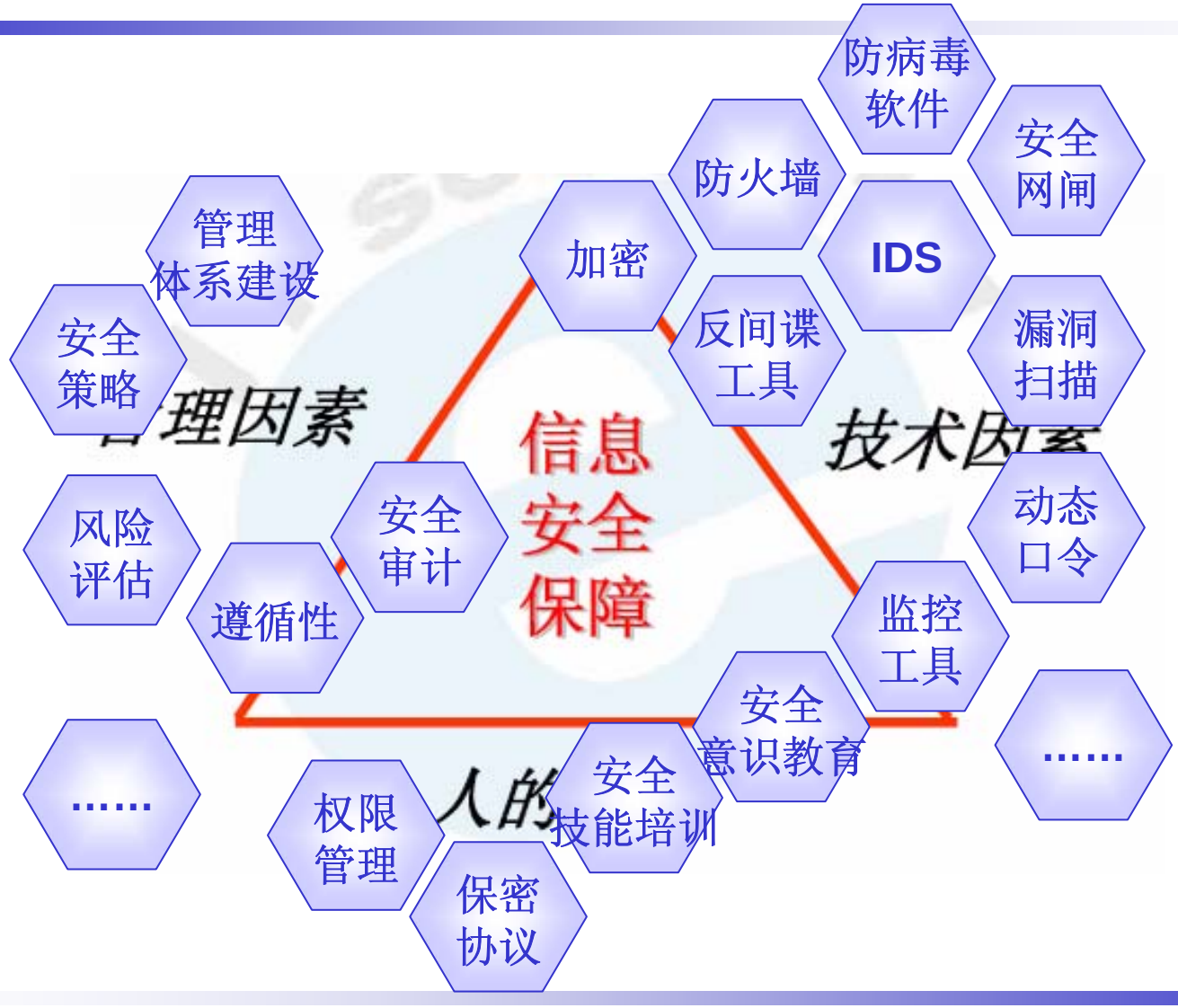
课程定位

- 从整体，实践、工程的角度思考信息安全

如何实现“安全”

- 明确信息安全工程是什么？信息安全工程怎么做？如何评价信息安全工程？

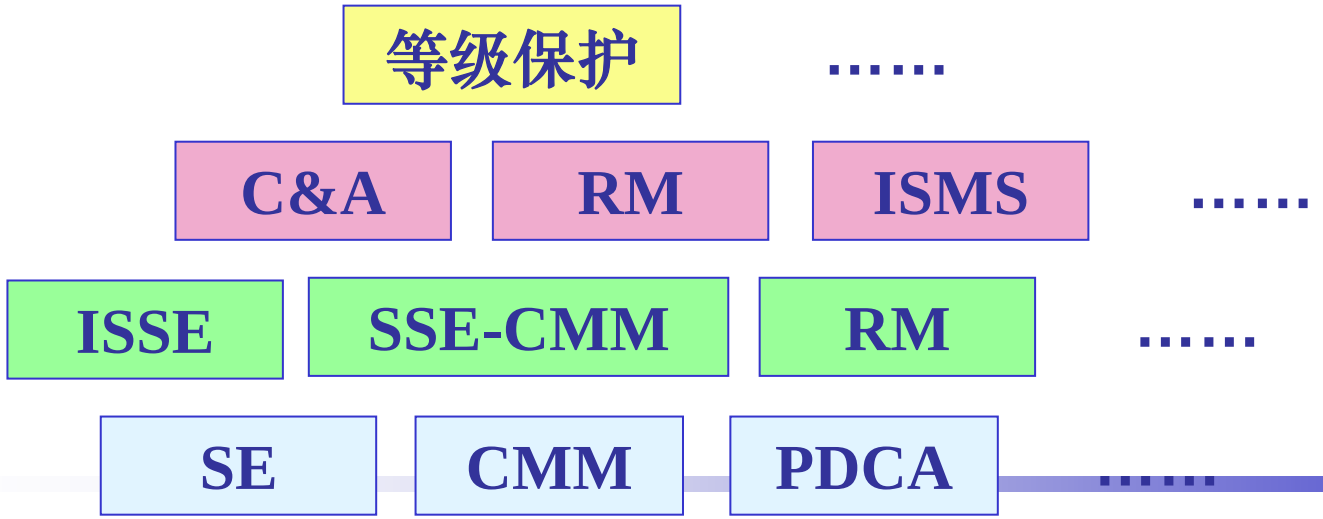
信息安全问题的复杂性


防病毒软件
安全网闸
防火墙
加密
IDS
管理体系建设
安全策略
反间谍工具
漏洞扫描
管理因素
技术因素
信息安全保障
风险评估
安全审计
动态口令
遵循性
监控工具
安全意识教育
……
……
人的
安全技能培训
权限管理
保密协议

课程基本内容

目的

- 理解信息安全工程基本模型
- 掌握系统安全工程-能力成熟度模型的基本内涵和方法
- 掌握一些实践的方法和过程



参考资料

- 教材《信息安全工程导论》，沈昌祥
  - 以SSE-CMM为核心
- 参考资料
  - 系统工程导论 ，陈宏民 高等教育出版社，安德鲁.P.塞奇 詹姆斯.E.阿姆斯特朗 西安交通大学
  - 信息系统安全等级保护基本要求，等
  - SSE-CMM V2.0，SSAM 2.0
  - NIST SP 800系列，800-30、800-37、800-53，……
  - ISO27001，ISO17799
  - CC2.1 ISO/IEC15408 1999.12 GB/T 18336-2001
  - IATF 3.1
  - 《信息安全管理概论》,机械工业出版社，2002 ，2002。
  - 《信息安全管理》，Christopher Alberts,Audrey Dorofee，吴晞译，清华大学出版社，2003
  - ……

课程考核

- **考核方式：考试**
- **最终成绩：平时30% 考试70%**
  - 平时成绩：作业和课堂提问（15%），出勤（15% 5次）
- **资料下载**
  - ftp://public.sjtu.edu.cn 用户名：zn_ning 密码：ssecmm

第一部分：绪论

—— 信息安全与信息安全工程

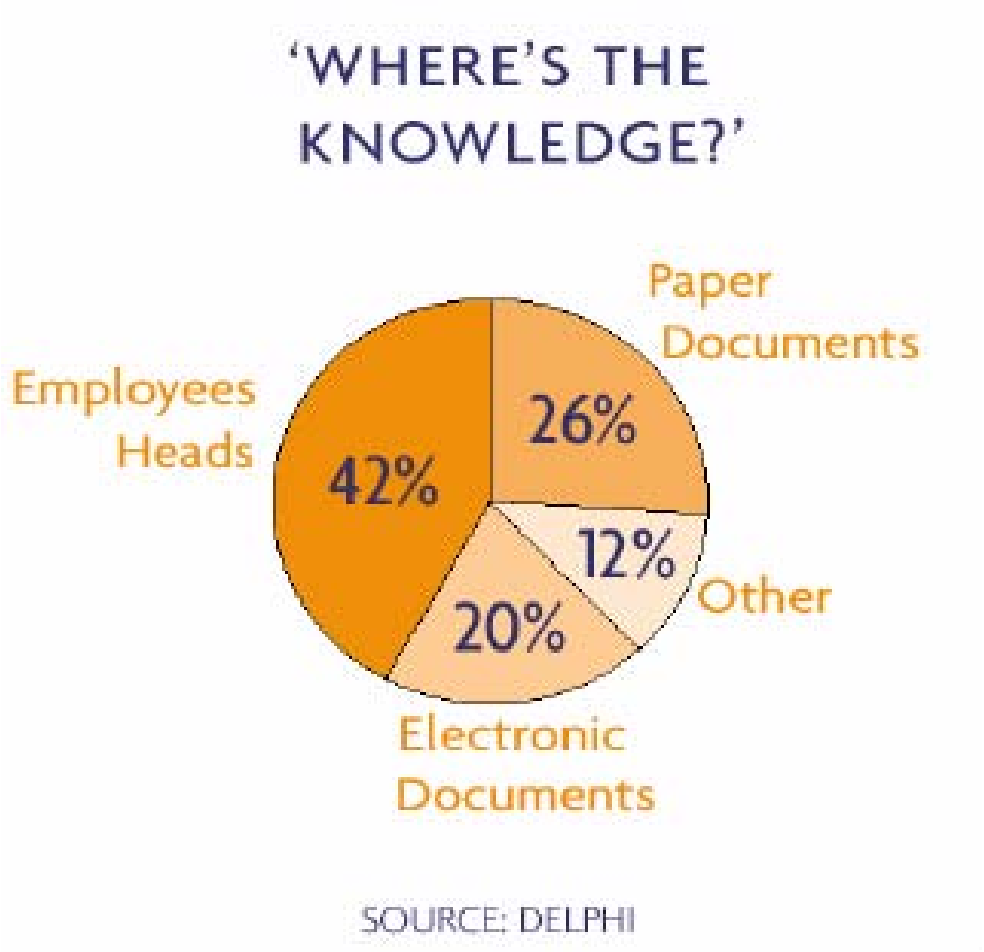
主要内容

- 信息安全基本概念
- 信息安全的现状
- 什么是信息安全工程

主要内容

- 信息安全基本概念
- 信息安全的现状
- 什么是信息安全工程

问题一：信息在哪里?


'WHERE'S THE KNOWLEDGE?'
Paper Documents
26%
Employees Heads
42%
12%
Other
20%
Electronic Documents
SOURCE: DELPHI

信息 --- 永不耗竭的资源

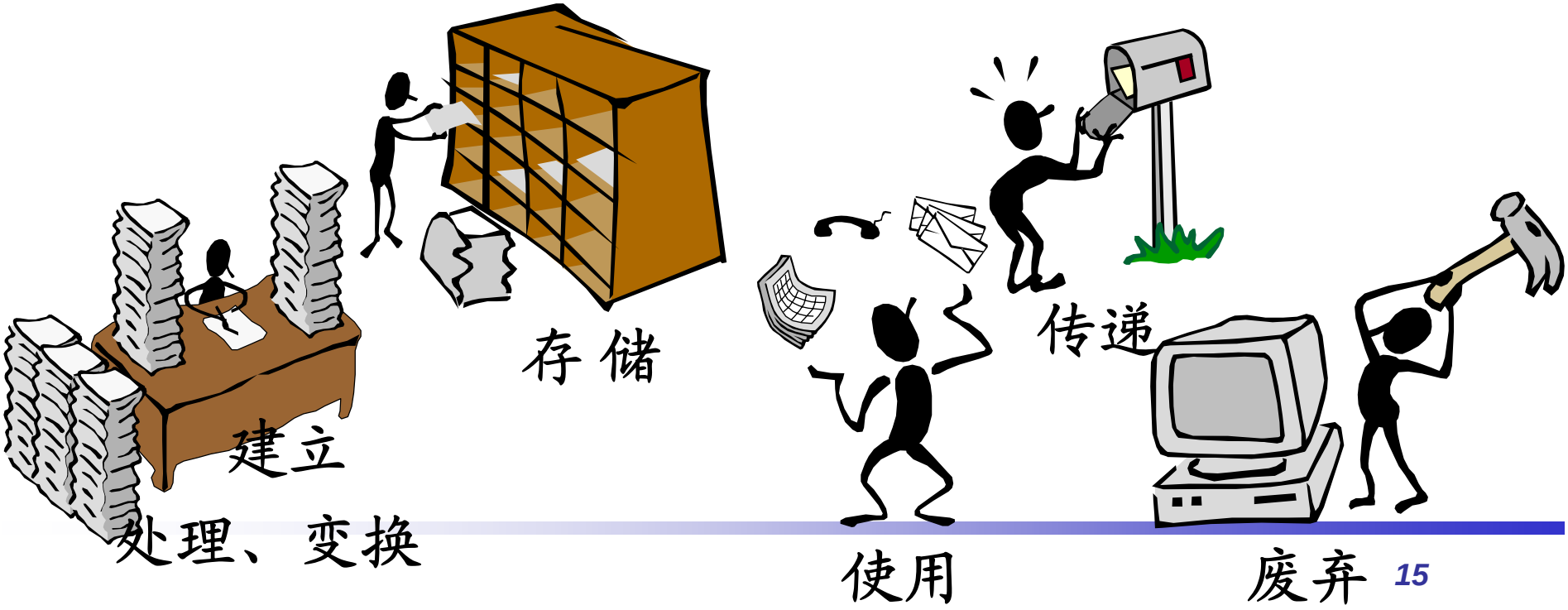
- 信息（Information）：是通过在数据上施加某些约定而赋予这些数据的特殊含义。（ISO/IEC 的IT 安全管理指南GMITS，即ISO/IEC TR 13335）
- 信息是一种资源，永不枯竭
- 对现代企业来说，信息是一种资产，包括计算机和网络中的数据，还包括专利、标准、商业机密、文件、图纸、管理规章、关键人员等，就象其它重要的商业资产那样，信息资产具有重要的价值，因而需要进行妥善保护。

信息的存在

- 通常情况下，我们可以把信息可以理解为消息、信号、数据、情报和知识。信息本身是无形的，借助于信息媒体以多种形式存在或传播，它可以存储在计算机、磁带、纸张等介质中，也可以记忆在人的大脑里，还可以通过网络、打印机、传真机等方式进行传播。

信息的生命周期

- 信息是有生命周期的，从其创建或诞生，到被使用或操作，到存储，再到被传递，直至其生命期结束而被销毁或丢弃，各个环节各个阶段都应该被考虑到，安全保护应该兼顾信息存在的各种状态，不能够有所遗漏。



问题二：什么是安全？

安全(safety)，顾名思义．“无危则安，尤缺则全”

1. 安全是指客观事物的危险程度能够为人们普遍接受的状态

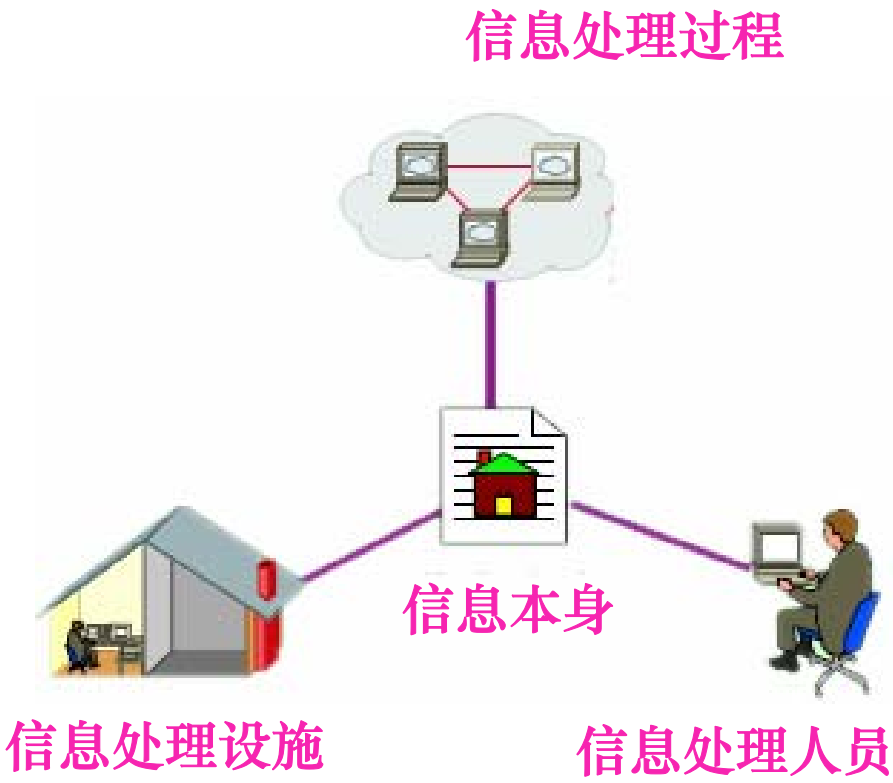
2. 安全是指没有引起死亡、伤害、职业病或财产、设备的损坏或损失或环境危害的条件。（美国军用标准MIL—STD— 382C ）

3. 安全是指不因人、机、媒介的相互作用而导致系统损失、人员伤害、任务受影响或造成时间的损失。

安全是一种状态　安全是相对的　安全是信心的度量

问题三：什么是信息安全?

信息安全保护什么?



信息安全属性

■ 信息安全属性

- 保密性 Confidentiality
- 完整性 Integrality
- 可用性 Availability
- 可控性 Controllability
- 不可否认性 Non-repudiation
- 其它：真实性(Authenticity)、可追究性(Accountability)、可靠性(Reliability)

信息安全属性如何实现？采用什么样的方法、技术或措施？

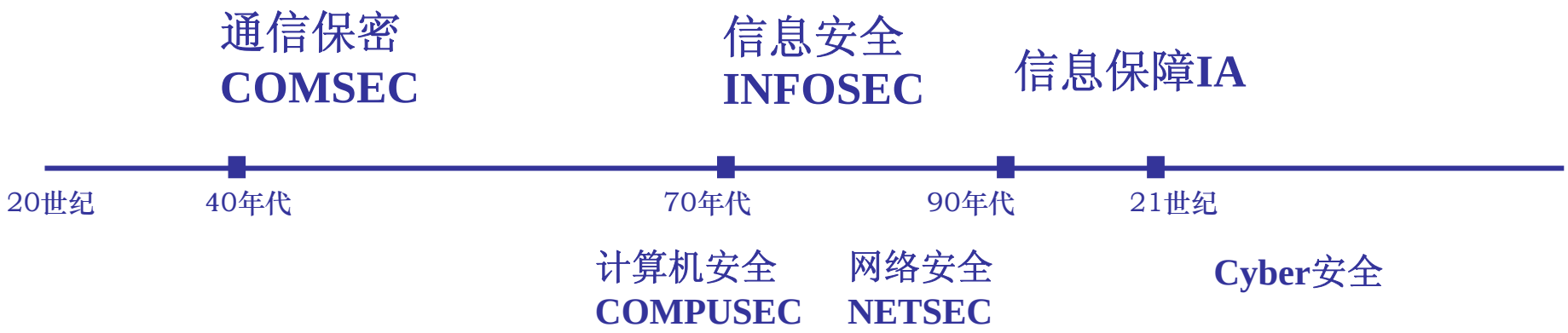
信息安全的一种描述

- **ISO17799中的描述**

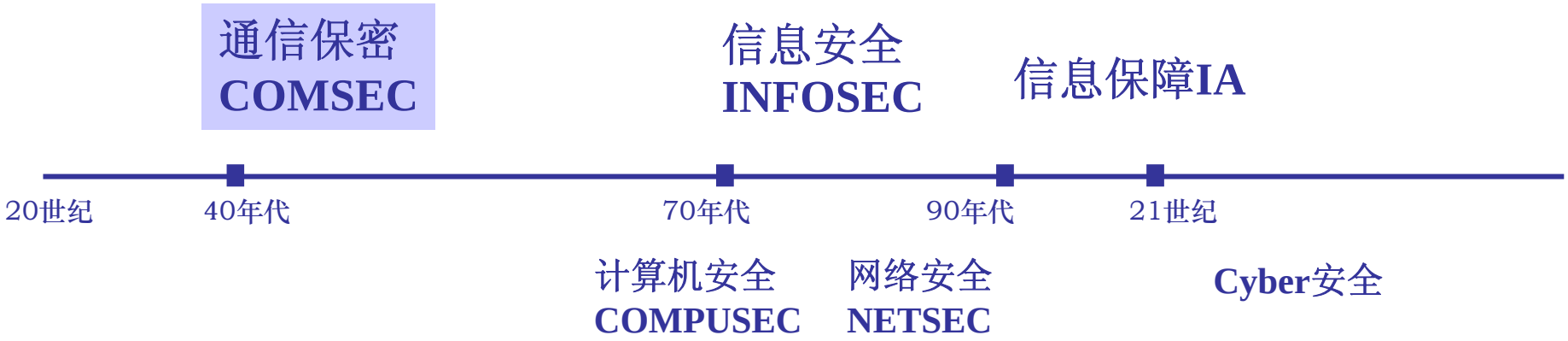
  “Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.”

- 信息安全：
  - 保护信息免受各方威胁
  - 确保组织业务连续性
  - 将信息不安全带来的损失降低到最小
  - 获得最大的投资回报和商业机会

信息安全发展过程


通信保密
COMSEC
信息安全
INFOSEC
信息保障IA
20世纪
40年代
70年代
90年代
21世纪
计算机安全
COMPUSEC
网络安全
NETSEC
Cyber安全

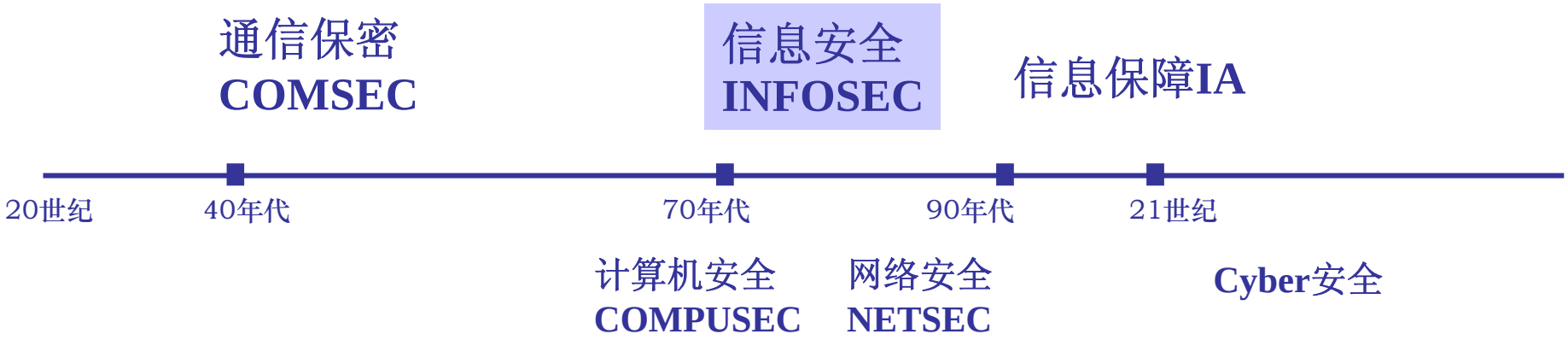
信息安全发展过程



– 通信保密 --- 保密

- 背景：电报、电话、无线通信的大量应用，特别是二次大战的需求
- 主要威胁：搭线窃听，密码学分析
- 主要防护措施：数据加密
- 标志：1949年Shannon发表的《保密系统的信息理论》，密码学诞生
- 涉及安全性：保密性、可靠性（通信的真实性）

信息安全发展过程

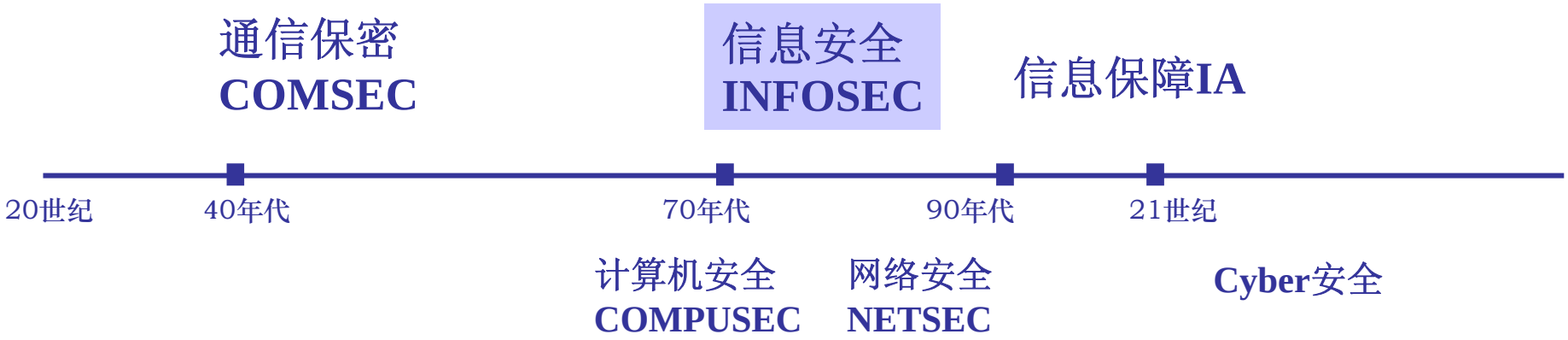


– 信息安全 --- 保护

- 背景：计算机软硬件技术开始快速发展，并且开始出现了对内开放、对外封闭的计算网络
- 主要威胁：计算机在处理、存储、传输和使用时易被滥用、干扰和丢失，而信息也就易被泄漏、窃取、篡改、破坏。
- 过程：从仍注重保密性 ⇨ CIA ⇨ 五性（可控性和不可否认性）

  从保护计算机为重点 ⇨ 以保护信息为出发点

信息安全发展过程



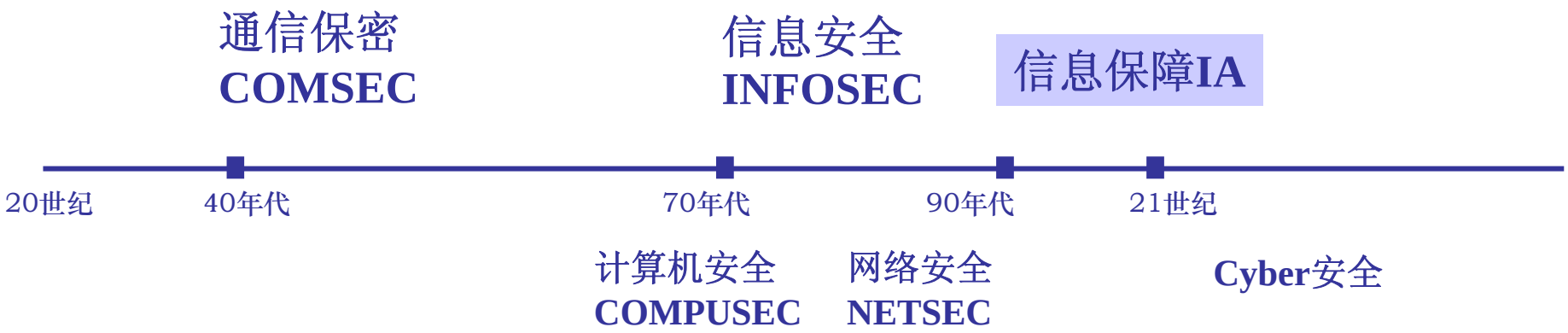
– 信息安全 --- 保护

- 标志：1977年 NBS 公布的《国家数据加密标准》

  1985年 DOD 《可信计算机系统评估准则》（TCSEC）

  法、英、荷、德欧洲四国90年代初联合发布欧洲四国制定的《信息技术安全评估标准》ITSEC
- TCSEC 以信息安全的机密性为主，ITSEC则强调保障信息的机密性、完整性、可用性，其后由于社会管理以及电子商务，电子政务等的网上应用的开展，人们又逐步认识到还要关注可控性和不可否认性。

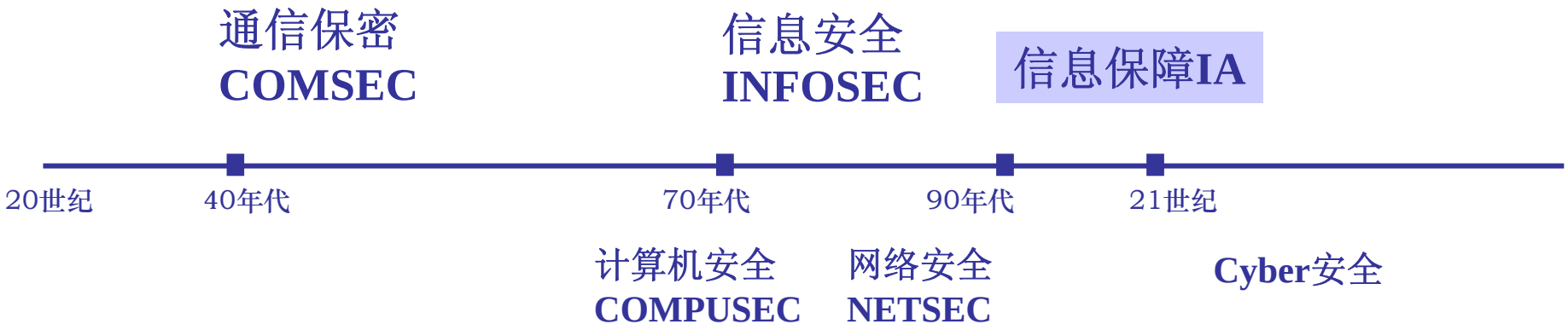
信息安全发展过程



– 信息保障 --- 保障

- 安全不再局限于信息的保护，人们需要对信息和信息系统的保护和防御，强调信息系统整个生命周期的防御和恢复，同时安全问题的出现和解决方案也超越了纯技术范畴。由此形成了包括了预警、保护、检测、反应和恢复五个环节的信息保障概念，即信息保障的WPDRR模型
- 以美国国家安全局制定的《信息保障技术框架》（IATF）为标志。它核心思想是深层防御战略（Defense in Depth）

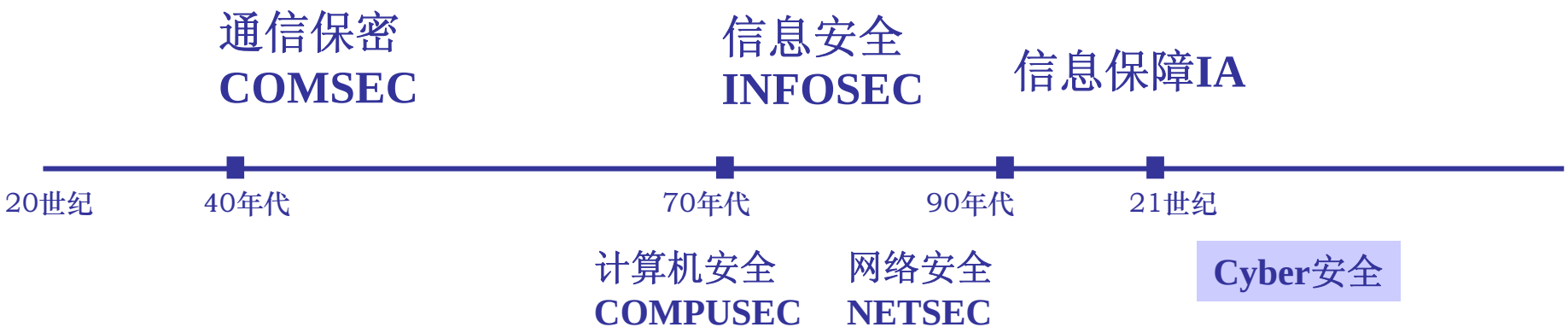
信息安全发展过程



– 信息保障 --- 保障

- 安全与应用的结合更加紧密，其相对性、动态性引起注意，追求适度风险的信息安全成为共识，安全不再单纯以功能或机制的强度作为评判指标，而是结合了应用环境和应用需求，强调安全是一种信心的度量，使信息系统的使用者确信其预期的安全目标已获满足

信息安全发展过程

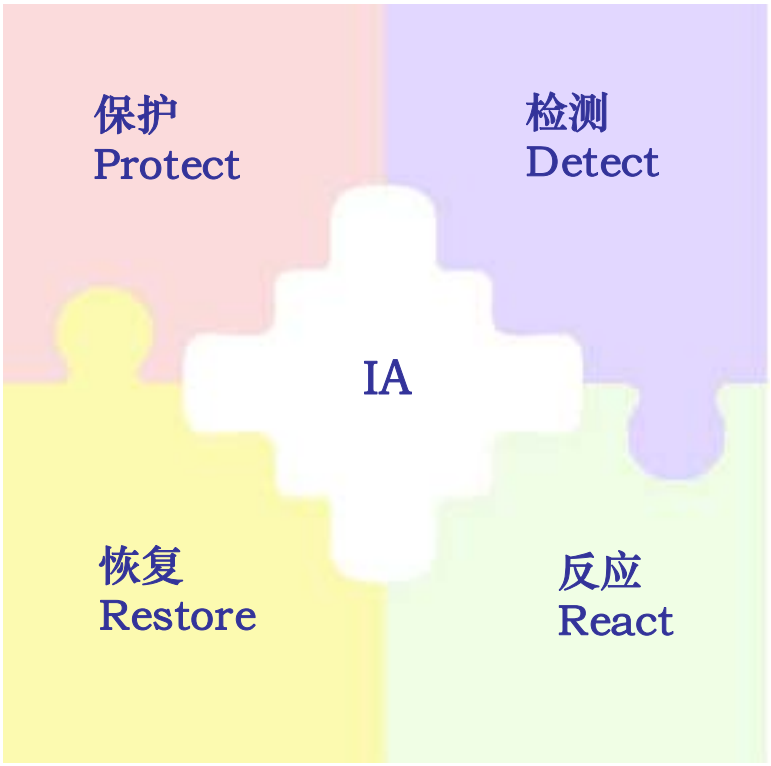


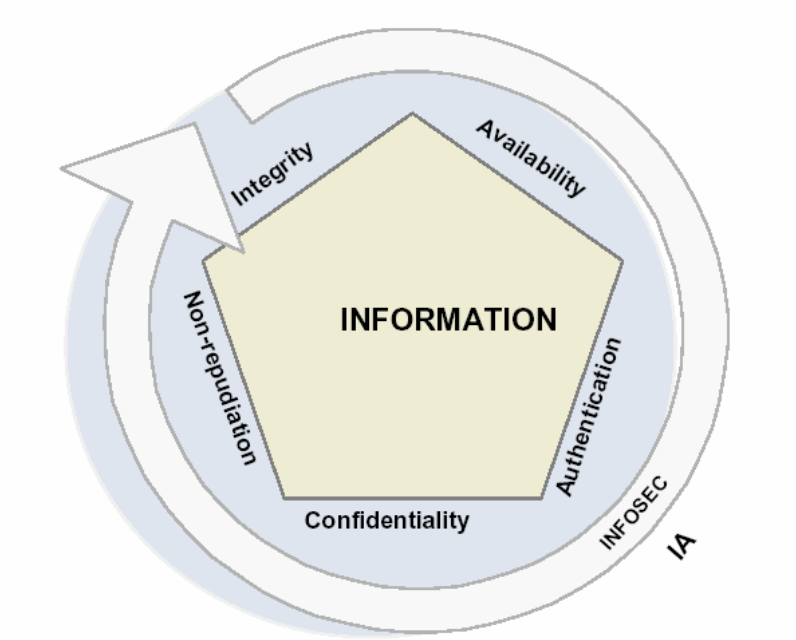
– Cyber security　多维度

- 信息安全被抽象成为一个由信息系统、信息内容、信息系统所有者和运营者、信息安全规则等多个因素构成的一个多维的问题空间
- 南湘浩教授：网络世界安全的最基本需求是赖于可信性建立的秩序。网络世界安全的基本构件可以用C3MSE来概括：即certification(认证)、control(控制)、confrontation(对抗)、management（管理）、supervision(监察)和emergency(应急)等六个方面。

信息保障框架

■ PDRR


保护
Protect
检测
Detect
IA
恢复
Restore
反应
React


Integrity
Availability
INFORMATION
Non-repudiation
Authentication
Confidentiality
INFOSEC
IA

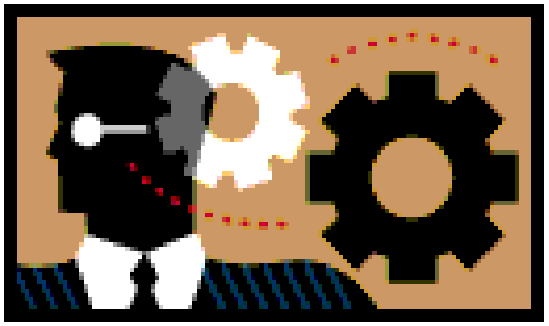
我国的信息安全保障的定义

■ WPDRRC

信息安全国家重点实验室给出如下定义：

我国的信息安全保障（续）

- 信息保障是对信息和信息系统的安全属性及功能、效率进行保障的动态行为过程。它运用源于人、管理、技术等因素所形成的预警能力、保护能力、检测能力、反应能力、恢复能力和反击能力，在信息和系统生命周期全过程的各个状态下，保证信息内容、计算环境、边界与连接、网络基础设施的真实性、可用性、完整性、保密性、可控性、不可否认性等安全属性，从而保障应用服务的效率和效益，促进信息化的可持续健康发展。



Q&A

信息安全属性 -- 保密性

■ 保密性 Confidentiality

- 定义：信息不被泄漏给非授权的用户、实体或进程，或被其利用的特性
- 信息内容的保密和信息状态的保密
- 常用的技术：防侦收、防辐射、信息加密、物理保密、信息隐形

信息安全属性 -- 完整性

■ 完整性 Integrality

- 定义：信息未经授权不能进行更改的特性，即信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。
- 主要因素：设备故障、误码、人为攻击、计算机病毒等
- 主要保护方法：协议、纠错编码方法、密码校验和方法、数字签名、公证等

信息安全属性 -- 可用性

■ 可用性 Availability

- 定义：信息可被授权实体访问并按需求使用的特性
- 目前没有理论模型，是综合性的度量
- 信息的可用性涉及面广
  - 硬件可用性
  - 软件可用性
  - 人员可用性
  - 环境可用性：主要是自然环境和电磁环境

信息安全属性 -- 可控性

■ 可控性 Controllability

– 指能够控制使用信息资源的人或实体的使用方式

- 信息的可控
- 安全产品的可控
- 安全市场的可控
- 安全厂商的可控
- 安全研发人员的可控

– 注:

- 可控性是对网络信息的传播及内容具有控制能力的特性。对于电子政务系统而言，所有需要公开发布的信息必须通过审核后才能发布。

信息安全属性 -- 不可否认性

- **不可否认性 Non-repudiation**
  - 也称抗抵赖性，是防止实体否认其已经发生的行为
  - 原发不可否认与接收不可否认
- **可追究性 Accountability**
  - 指确保某个实体的行动能唯一地追溯到该实体
  - 可分为鉴别和不可否认性
  - 部分体现可控性需求