信息安全综合实践

第一讲 信息安全概述

网络空间安全学院 孟魁

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

主要内容

1 信息安全概念

2 网络空间安全

3 网络安全管理

4 网络安全评估

主要内容

安全的含义

- 安全
  - 平安，无危险；保护，保全。 ----《汉语大词典》
  - 没有危险；不受威胁；不出事故。 ----《现代汉语词典》

- 国家安全
  - 全国人大常委会通过的《国家安全法》规定，国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。

信息安全的含义

- Bruce Schneier
  - “如果把一封信锁在保险柜中，把保险柜藏起来，然后告诉你去看这封信，这并不是安全，而是隐藏”
  - “如果把一封信锁在保险柜中，然后把保险柜及其设计规范和许多同样的保险柜给你，以便你和世界上最好的开保险柜的专家能够研究锁的装置，而你还是无法打开保险柜去读这封信，这才是安全…”

信息安全的定义

- 国际标准化委员会ISO/IEC 27000:2018
  - Information Security：preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
  - Information security involves the application and management of appropriate controls that involves consideration of a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimizing consequences of information security incidents.

信息安全的属性

机密性、真实性
可控性、可用性

机密性、完整性、可用性、真实性、不可抵赖性

主要内容

1 信息安全概念

2 网络空间安全

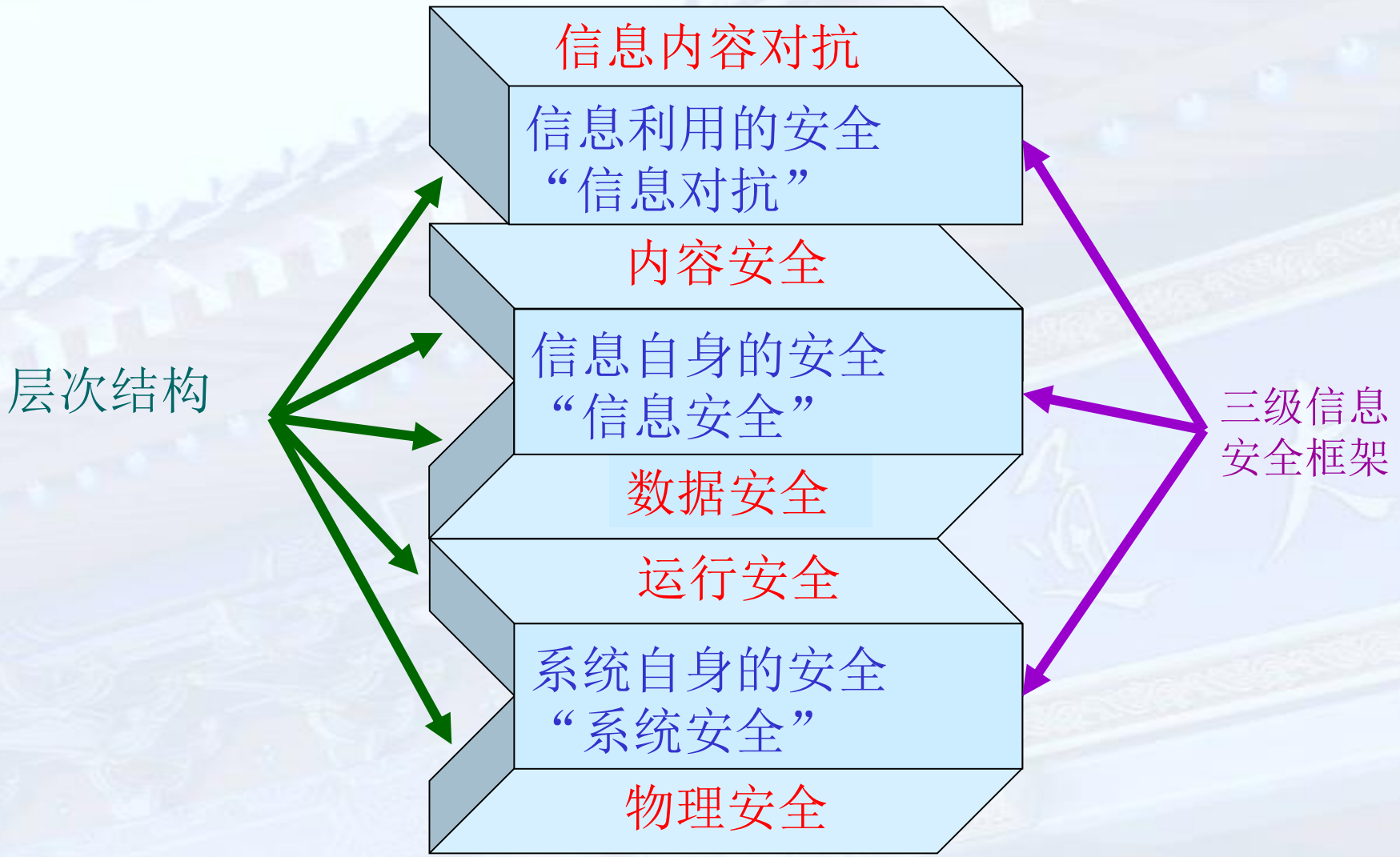
3 网络安全管理

4 网络安全评估

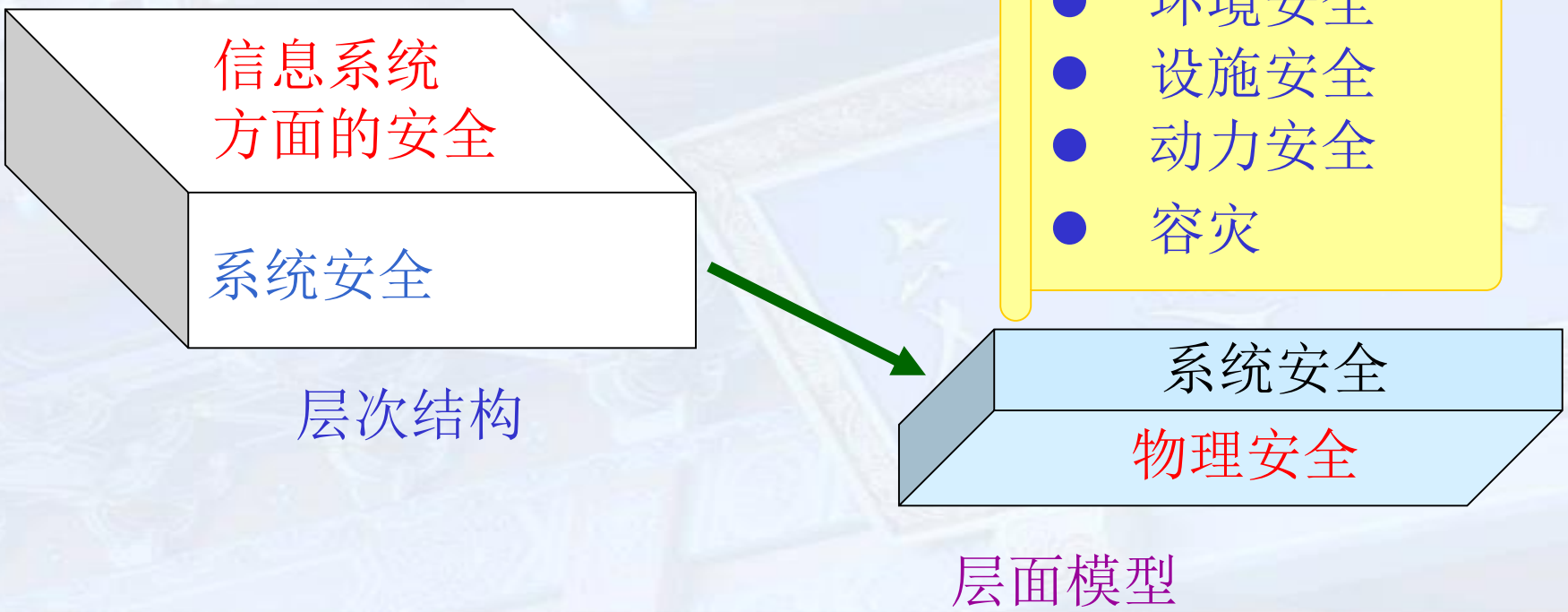
何谓信息


合理地应用知识并进行正确判断决策的能力
在对信息集合进行综合、提炼的基础上，
获得经验、判断与理解
经加工后有逻辑、有意义的数据
原始素材
Wisdom 智慧
Knowledge 知识
Information 信息
Data 数据
DIKW模型

信息安全的分层结构

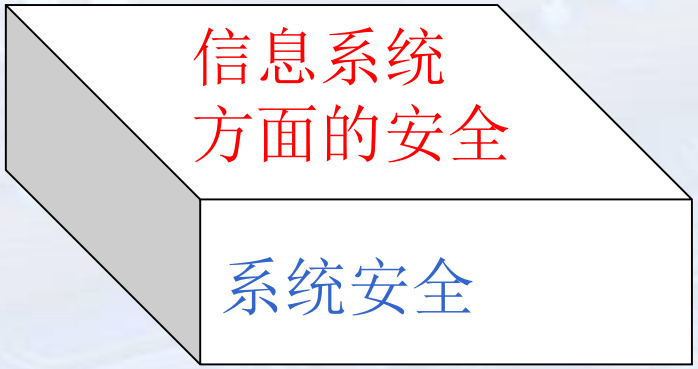

信息内容对抗
信息利用的安全
“信息对抗”
内容安全
信息自身的安全
“信息安全”
数据安全
运行安全
系统自身的安全
“系统安全”
物理安全
层次结构
三级信息
安全框架

信息安全的分层结构

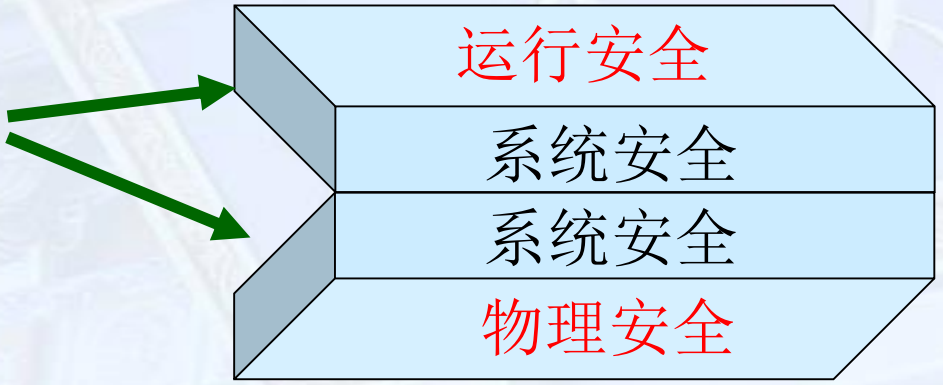


信息安全的分层结构

- 系统评估-测试评估能力
- 安全策略-信息对抗能力
- 访问控制-安全防护能力
- 入侵检测-安全预警能力
- 应急响应-应急响应能力

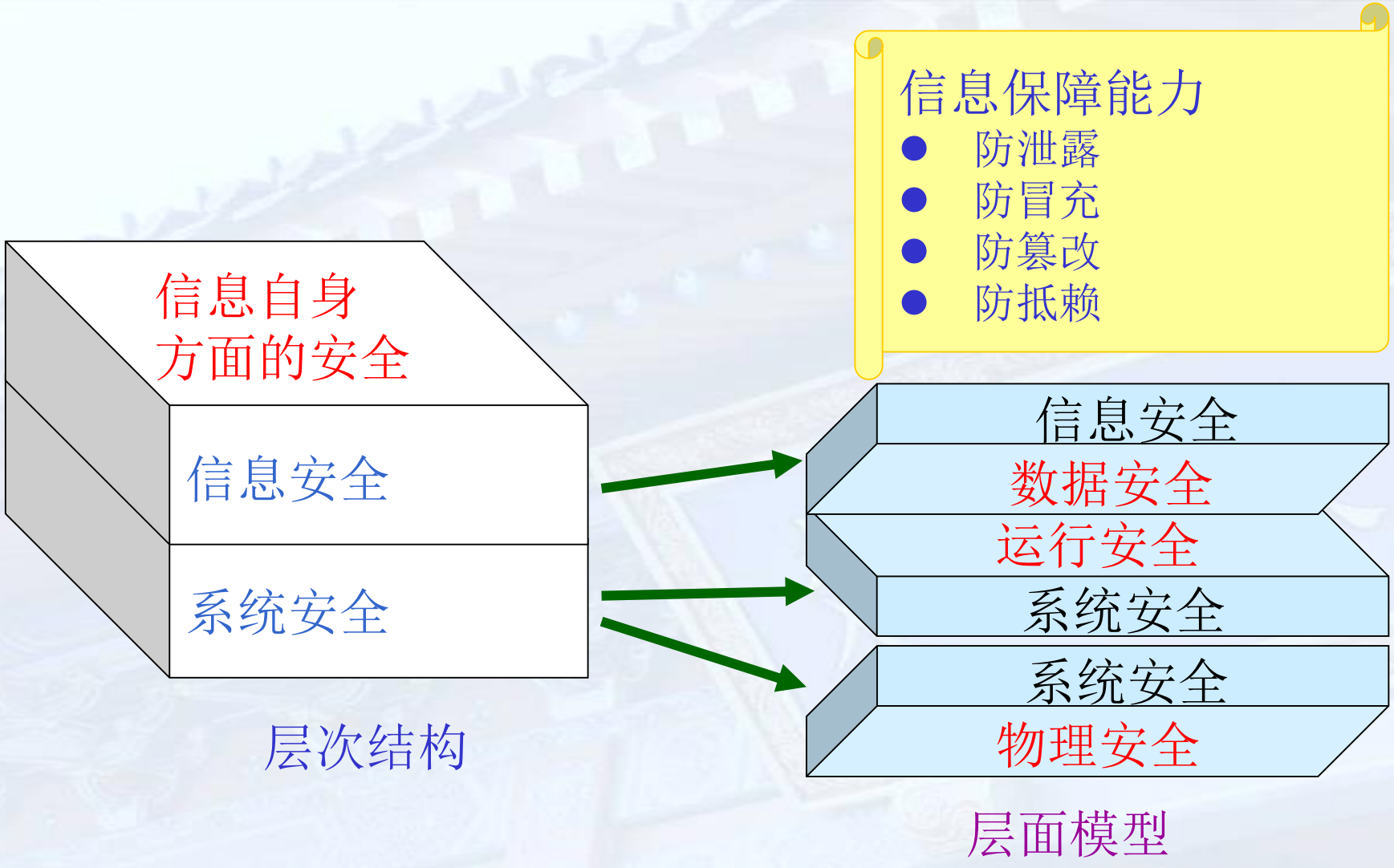


层次结构

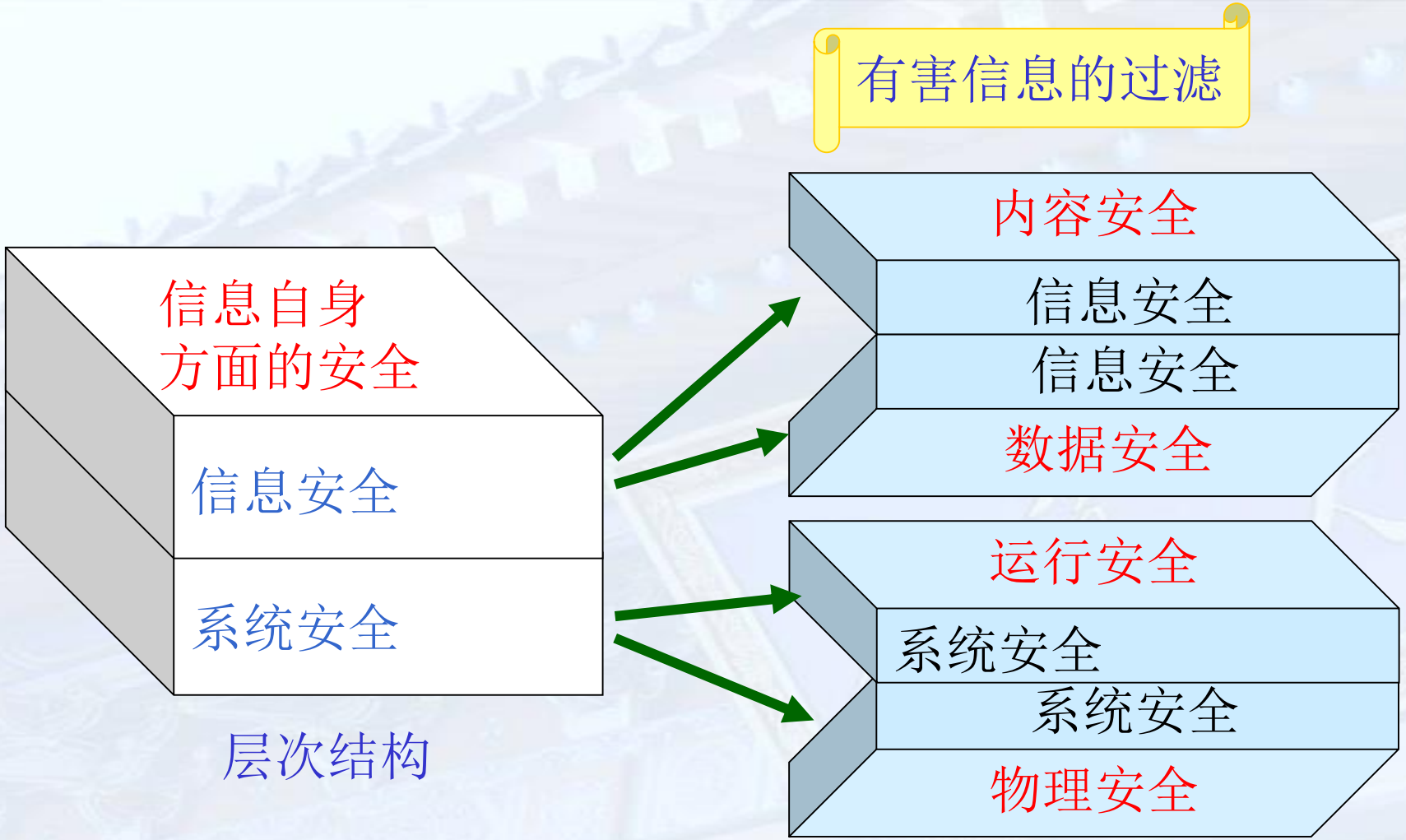


层面模型

信息安全的分层结构

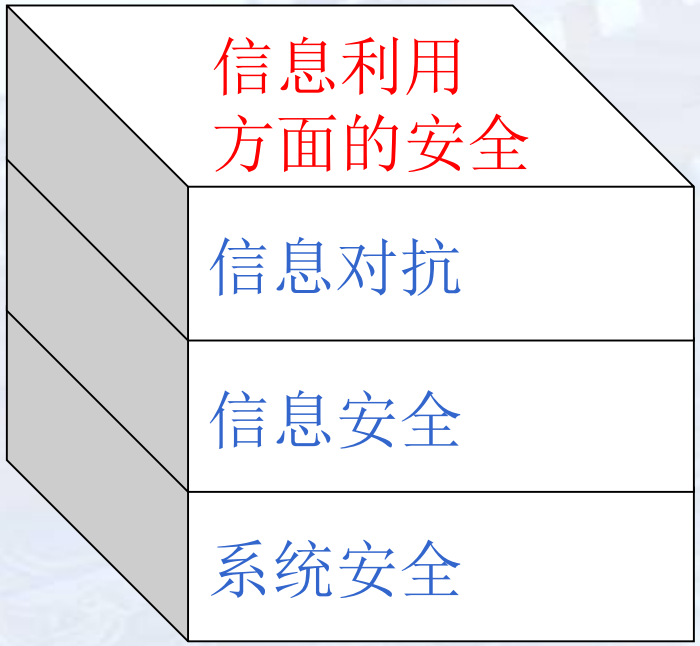

信息保障能力
防泄露
防冒充
防篡改
防抵赖
信息自身
方面的安全
信息安全
系统安全
层次结构
信息安全
数据安全
运行安全
系统安全
系统安全
物理安全
层面模型

信息安全的分层结构

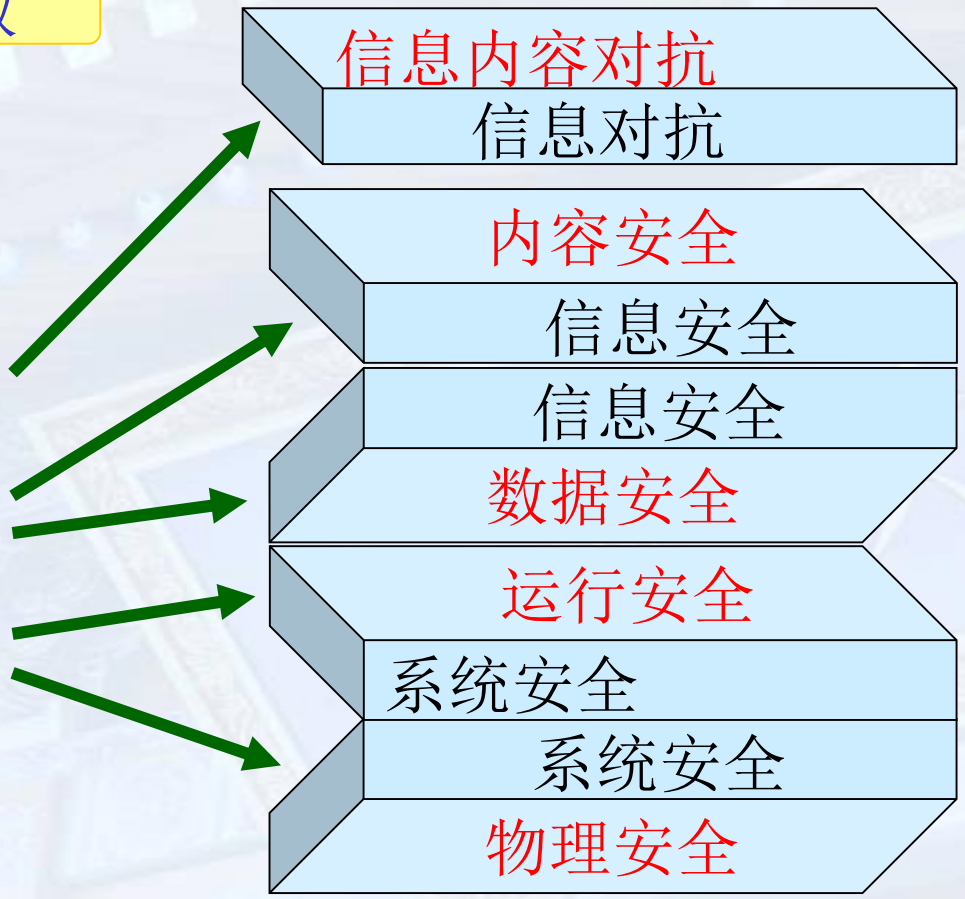

有害信息的过滤
信息自身
方面的安全
信息安全
系统安全
层次结构
内容安全
信息安全
信息安全
数据安全
运行安全
系统安全
系统安全
物理安全

信息安全的分层结构

- 信息的隐藏与发现
- 信息的干扰与提取



层次结构



层面模型

信息安全的分层结构

信息安全分层结构
面向应用的信息安全框架

网络安全 Vs. 信息安全

- 网络安全=网络运行安全+网络信息安全

网络安全

- 网络运行安全：保证构成网络系统的软件、硬件、数据资源具有可用性
- 网络信息安全：保护网络系统存储、使用的信息具有机密性、完整性、真实性和可控性

网络安全分类

- 根据计算环境

- 根据计算对象

网络空间

- 网络空间（Cyberspace）
  - 继陆、海、空、天之后的第五大空间
  - **The interdependent network of information technology infrastructures, and includes the *Internet*, *telecommunications networks*, *computer systems*, and *embedded processors and controllers in critical industries*. Common usage of the term also refers to the virtual environment of information and interactions between people.**

--National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23)，2008

网络空间发展

网络融合性：互联网，通信网络，广电网络，物联网IoT，工控网络…
终端多样性：PC，手机，平板，电视，手环，手表，智能终端…
内容多样化：云计算，社交网络，对等网络服务…
领域广泛性：涉及政治，经济，文化，军事等社会各个层面

20世纪90年代中期以前

技术发展阶段

INTERNET

NSFNET

ARPANET

20世纪90年代中期-2010年

商业化阶段

yahoo! amazon ebay

icq 網易 搜狐 SOHU.com

Google Tencent 腾讯 sina

Alibaba Group 阿里巴巴集团 Baidu 百度

2010年以来

社会化阶段

WhatsApp facebook in

网络空间安全威胁


应用层的安全威胁
接口多样化
恶意应用
应用层
API
系统面临的威胁
虚拟拓扑的动态性
系统安全防护策略多样性
巨大规模网络
网络虚拟与抽象
面向用户的网络抽象描述
缺乏统一协议架构
上千种网络协议
网络控制软件
控制层的安全威胁
IP地址欺骗
DDoS攻击
控制与数据平面分离
后门、隐蔽通道
控制-转发接口
基础设施层
网络设备
传感节点
移动终端
工控设备

网络空间安全展望

- 网络空间安全威胁泛在化和复杂化，网络攻击更有持续性和隐蔽性
- 网络空间安全最大的威胁是什么？
  - 是不确定威胁：未知漏洞、未知后门、未知攻击

主要内容

网络安全管理

习近平在中央网络安全和信息化领导小组第一次会议上讲话
（2014年2月27日）

CERT

- 计算机应急响应小组Computer Emergency Response Team
  - 源自于1988年的“莫里斯蠕虫事件”
  - CERT/CC，1988年美国成立，作为Carnegie Mellon大学的软件工程协会SEI的下属组织，是一个非政府的研究机构
  - JPCERT/CC，日本，成立于1996年10月
  - US-CERT，美国，成立于2003年6月，美国国土安全部与Carnegie Mellon大学合作
  - APCERT，亚太，2003年成立应急组织，包括亚太地区的20个国家和地区的33个CERT组织

FIRST

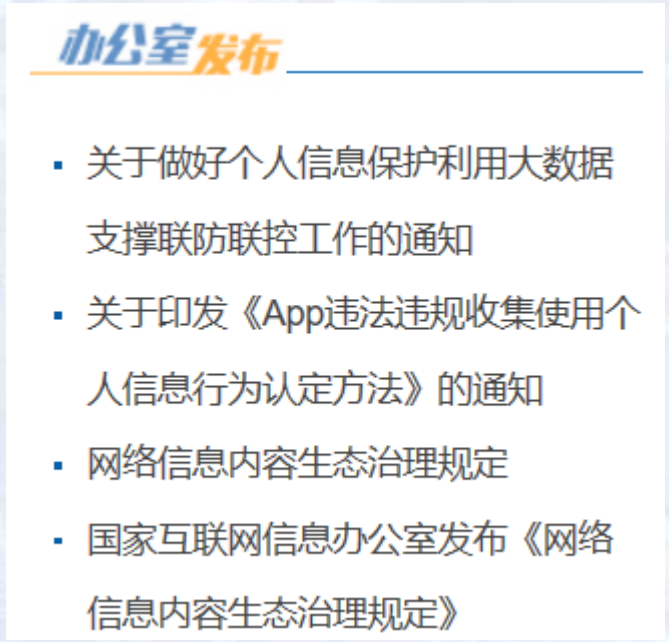
- 事件响应与安全组论坛(Forum of Incident Response and Security Teams，FIRST)
  - 1990年由11个应急响应安全组织成立，促进各应急响应组织之间的有效交流与合作。
  - 截止到目前(2022年2月)，包括全球608个应急响应安全组织
    - 我国大陆CNCERT/CC、阿里(ASRC)、中国移动(China Mobile)、腾讯云计算(Tencent Cloud)、奇安信(Qi An Xin CERT)、数字观星(Data Star Observatory)、恒安嘉新(Eversec)、OPPO(OSRC) 、中兴(ZTE PSIRT)、大华(Dahua PSIRT)、华为(Huawei PSIRT)、海康威视(HSRC)
  - 2021年2月，562个成员

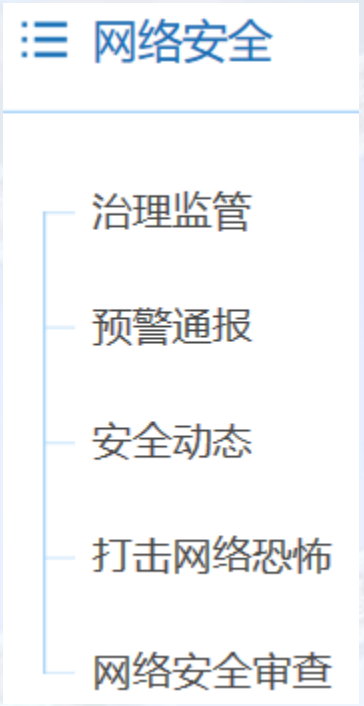
我国网络安全管理

- 国家互联网信息办公室/中共中央网络安全和信息化委员会办公室
  - 中央网信办，原中央网络安全和信息化领导小组
- 国家计算机网络应急技术处理协调中心
  - 国家互联网应急中心（CNCERT/CC）
- 全国信息安全标准化技术委员会（TC260）

国家互联网信息办公室

- 国家互联网信息办公室/中共中央网络安全和信息化委员会办公室
  - 中央网信办，原中央网络安全和信息化领导小组



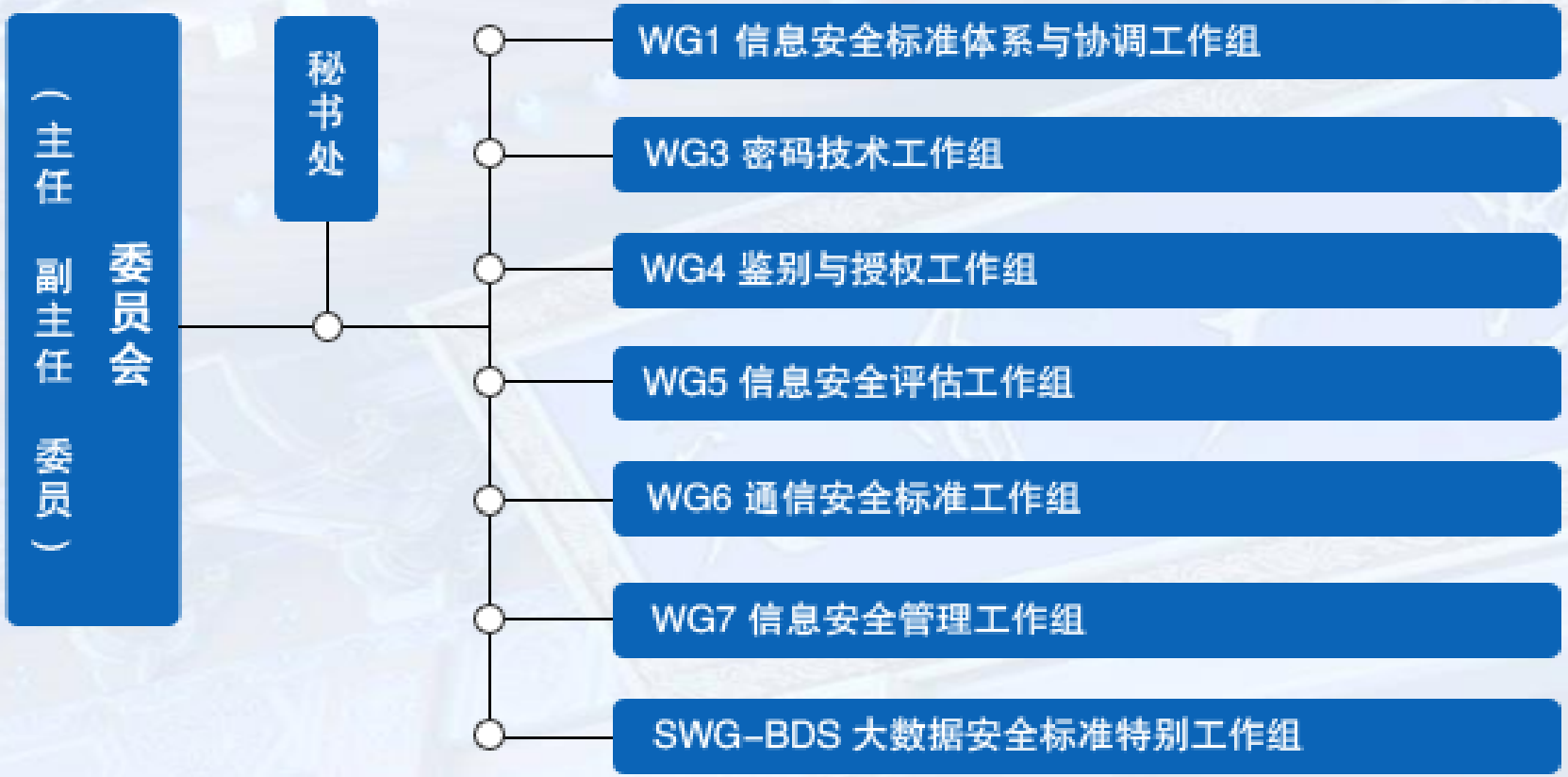


国家互联网应急中心

- 国家计算机网络应急技术处理协调中心
  - **http://www.cert.org.cn/**
  - **成立于2001年8月，为非政府非盈利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位，属于国家级应急中心**
  - **在中国大陆31个省、自治区、直辖市设有分支机构**
  - **发起成立了国家信息安全漏洞共享平台（CNVD）、中国反网络病毒联盟（ANVA）和中国互联网网络安全威胁治理联盟（CCTGA）**

全国信息安全标准化技术委员会（TC260）

- 委员会是在信息安全技术专业领域内，从事信息安全标准化工作的技术工作组织。



相关法律、法规、管理办法

- 2016年11月，《中华人民共和国网络安全法》（全国人大）
- 2019年07月，《加强工业互联网安全工作的指导意见》（工信部等十部门）
- 2019年07月，《云计算服务安全评估办法》（国家网信办、发改委等四部门）
- 2019年10月，《中华人民共和国密码法》（全国人大）
- 2019年11月，《网络安全威胁信息发布管理办法（征求意见稿）》（国家网信办）
- 2019年12月，《App违法违规收集使用个人信息行为认定方法》（国家网信办）
- 2020年10月，《个人信息保护法（草案）》正式向社会公布并征求意见
- 2021年6月，《中华人民共和国数据安全法》（全国人大）
- 2021年8月，《中华人民共和国个人信息保护法》（全国人大）
- 2021年8月，《关键信息基础设施安全保护条例》（国务院第745号）
- 2021年11月，《网络安全审查办法》（国家网信办）

相关法律、法规、管理办法

- 2021年2月20日，国家市场监督管理总局(国家标准化管理委员会)正式发布网络安全领域强制性国家标准：GB 40050-2021《网络关键设备安全通用要求》，于2021年8月1日正式实施。

美国网络空间管理

- **National Security Agency（NSA）**
  - 美国政府机构中最大的情报部门
  - 专门负责收集和分析外国及本国通讯资料，隶属于美国国防部，又称国家保密局。

【环球网综合报道】据香港《文汇报》1月16日报道，美国《纽约时报》引述前中情局雇员斯诺登泄露的文件及美国政府官员和计算机专家的评论指出，美国国安局早于2008年起，向全球近10万台计算机植入软件，务求时刻监控或攻击目标计算机，即使计算机没有连接上网，美国当局仍可通过无线电波入侵，其中，中俄军方最常受监控。

美国网络空间管理

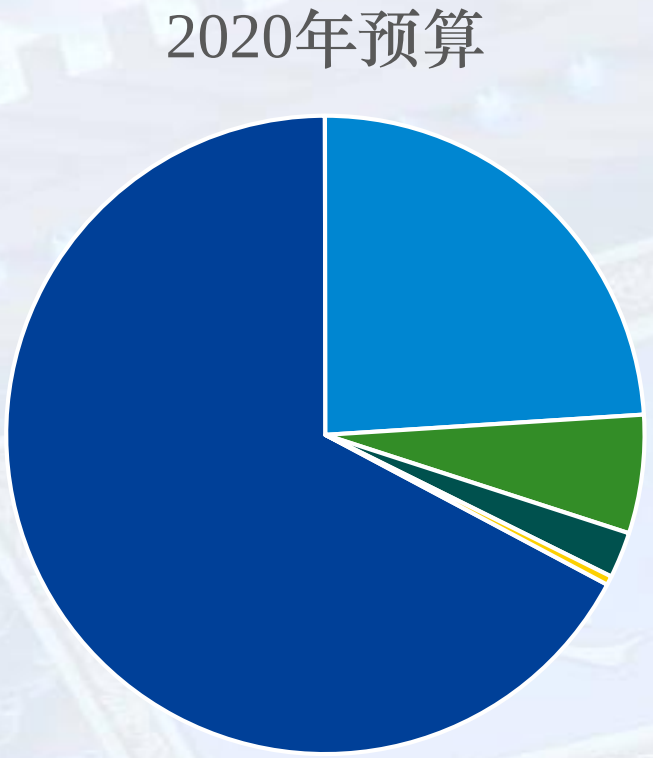
- **Cybersecurity and Infrastructure Security Agency (CISA)**
  - 2018年，美国国会签署《网络安全和基础设施安全局法案》，将**原有的国家保护和计划司**（National Protection and Programs Directorate，NPPD）重组为新的机构CISA（**网络安全和基础设施安全局**）
  - **美国国土安全部副部长、前NPPD副主管Christopher Krebs为首任局长**
  - 2020财年CISA预算为10亿多美元，约占DHS预算过半

CISA
CYBER+INFRASTRUCTURE

Defend Today, Secure Tomorrow

美国网络空间管理

- CISA职责



国家网络安全和通信中心（NCCIC）运营、规划与演习

网络安全教育与意识、加强网络安全服务、网络安全顾问，以及新设的“网络安全技术战略计划”项目

全国网络安全保护系统（NCPS）、持续诊断与缓解（CDM）、联邦网络安全弹性（FNR）

美国网络空间管理

- **United States Cyber Command (USCYBERCOM)**
  - 2009年5月，美军宣布征召4000名士兵组建一支网络战“特种部队”。
  - 2009年6月，成立美国网络司令部，统管全美军的网络安全和网络作战指挥。2010年5月21日正式运行，首任司令由美国国家安全局局长Keith Alexander兼任。
  - 2016年10月，网络司令部宣布下属133支网络任务部队已全部具备初始作战能力。
  - 2016年12月24日，奥巴马任期末签署的《国防授权法案》中，将网络司令部提升为完备的作战司令部。
- 陆、海、空都在建网络战部队

美国网络空间管理

- **Cyberspace Solarium Commission (CSC)**
  - **2019年，由美国政府资助成立**
  - **成员包括来自行政部门、国会、情报部门、执法部门和私营部门的代表**
  - **Reform the U.S. Government's Structure and Organization for Cyberspace**
  - **Strengthen Norms and Non-Military Tools**
  - **Promote National Resilience**
  - **Reshape the Cyber Ecosystem**
  - **Operationalize Cybersecurity Collaboration with the Private Sector**
  - **Preserve and Employ the Military Instrument of National Power**

美国网络空间管理

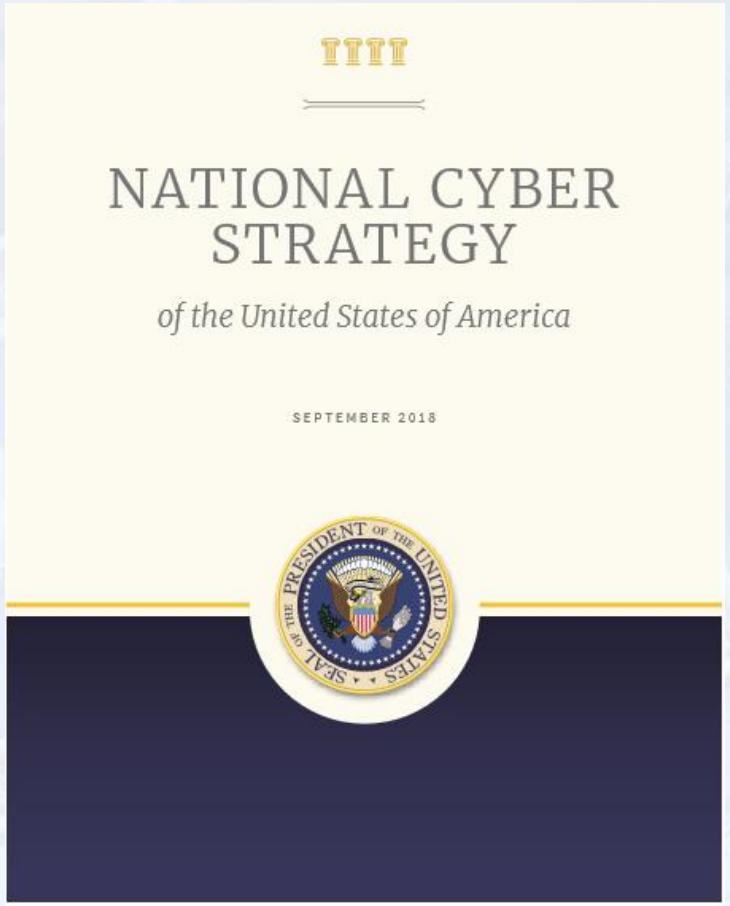
- **Cyberspace Solarium Commission (CSC)**
  - **Strategy & recommendations**
    - **March 11, 2020, "Executive Summary."**
    - **June 2, 2020, "Cybersecurity Lessons from the Pandemic"**
    - **September 4, 2020, "Growing a Stronger Federal Cyber Workforce"**
    - **October 19, 2020, "Building a Trusted ICT Supply Chain"**
    - **January 19, 2021, "Transition Book for the Incoming Biden Administration"**
  - **Propose over 80 recommendations, 25 recommendations have been codified into law.**

美国网络空间管理

- 2003年2月《网络空间安全国家战略》，将网络空间发展战略从“发展优先”调整为“安全优先”。
- 2009年5月《网络空间政策评估报告》。
- 2011年5月《网络空间国际战略》，宣称要建立一个“开放、互通、安全和可靠”的网络空间，并为实现这一构想勾勒出了政策路线图。
- 2016年2月《网络安全国家行动计划》。
- 2017年12月《国家安全战略报告》。数十次提及网络安全，称美国将遏制、防范，并在必要的时候打击使用网络空间能力攻击美国的黑客。

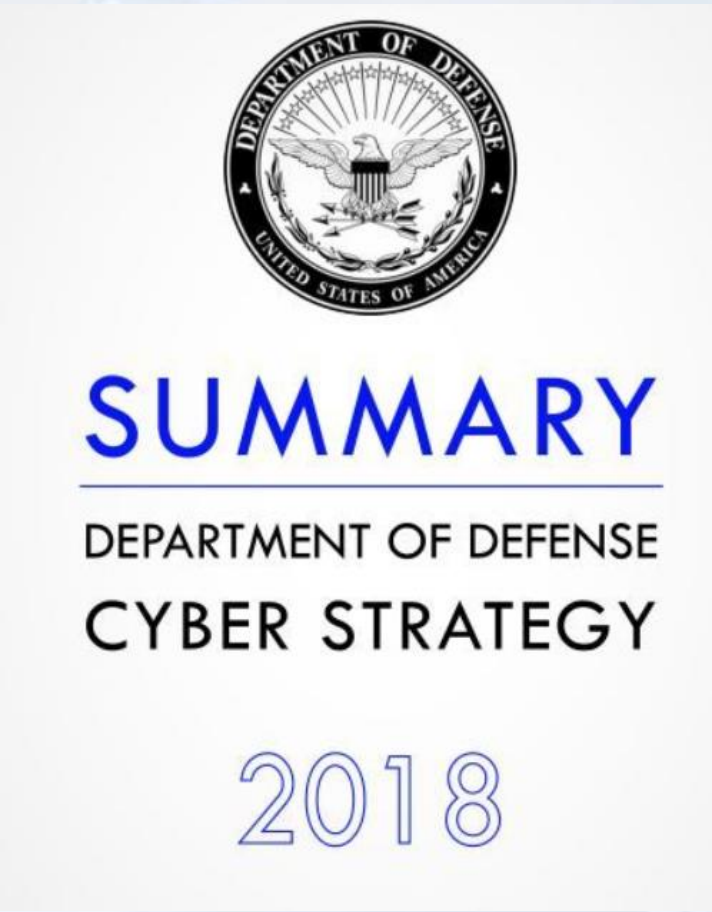
美国网络空间管理

- 2018年9月20日，白宫发布国家网络战略，旨在赋予政府机构和司法机关更强的网络犯罪及民族国家网络攻击响应能力，美国迄今为止最为激进的网络战略计划。



美国网络空间管理

- 2018年9月，发布2018年国防部网络战略，认为美国在网络空间也面临来自中国、俄罗斯等国的战略竞争，需通过提高网络空间作战能力、前摄性制止有关恶意网络活动、加强跨部门及跨国合作等加以应对。提出了美国的网络空间目标，并明确了实现这些目标的战略途径。

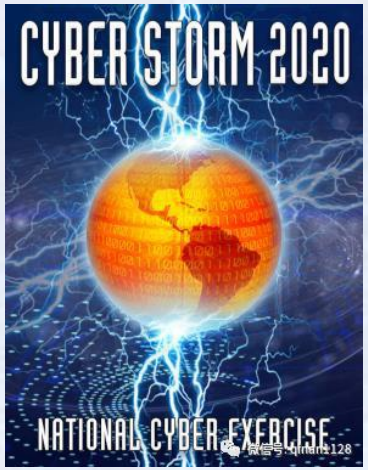


网络安全演练

- 美国
  - 网络风暴（Cyber Storm），由美国国土安全部主办
  - 从2006年开始，每两年举行一次，每次5天，以先前发生的真实事件为基础
  - 参与单位：
    1. 联邦部门、州政府
    2. 行业机构
    3. 国际政府伙伴
    4. 私营企业

网络安全演练

- 美国



2006, 两年一度

2011, 一年一度

2012, 一年一度

2012, 一年一度

网络安全演练

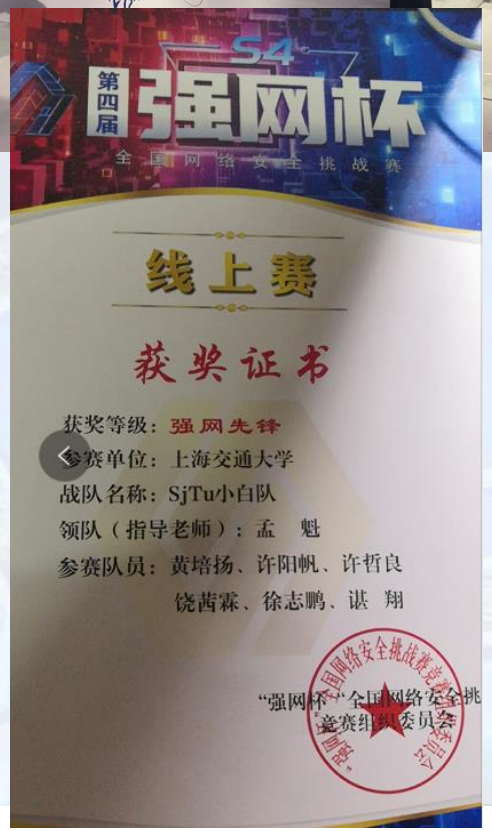
- 欧盟
  - “网络欧洲”(Cyber Europe)演习，由欧盟网络与信息安全局主办
  - 每两年举办一次，迄今为止已经举办了六次。

网络安全演练

网络安全威胁堪比核武器
应搞"网上朱日和"

网络安全竞赛

- 国内CTF
  - 网鼎杯
  - 强网杯
  - 护网杯
  - 各类企业、高校的CTF赛事




字节跳动
安全中心
2021 College
Security Competition
安全范化
高校挑战赛


TCTF
Tencent CTF


ATEC2021
科 · 技 · 精 · 英 · 赛
www.ATECup.cn (10月8日开放)
燃烧
一场AI与欺诈的较量
burning
参赛对象
全国计算机专业在校学生
人工智能及安全行业从业者、研究者
本次大赛不收取报名费，大赛报名以团队为单位，不接受个人形式报名。
阶段1：线上赛
10.15 / 11.15
设2个赛道，分别考察包括协作学习、多模态识别、半监督学习等各类能力。
阶段2：线下赛 （限时60小时）
11.25 / 11.28
限时60小时，将综合考察参赛团队在反欺诈识别中解决实际问题的能力。

主要内容

1 信息安全概念

2 网络空间安全

3 网络安全管理

4 网络安全评估

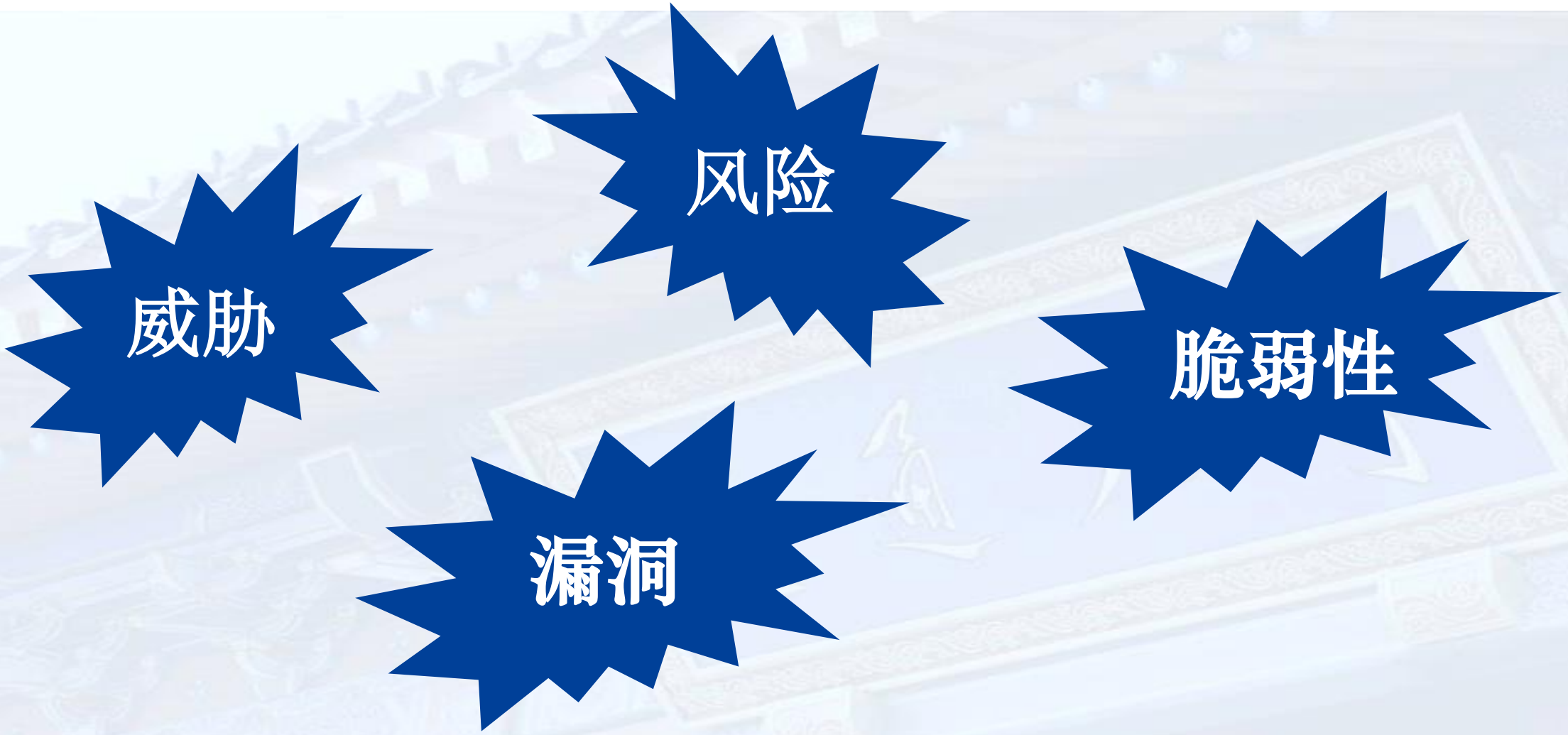
安全评估

- 1983 年，美国国防部颁布了历史上第一个计算机安全评价标准TCSEC（Trusted Computer System Evaluation Criteria)橙皮书。
  - 最初是军用标准，后成为民用标准
  - 主要是针对操作系统的评估
  - 分为4个等级，7个级别，共27条评估准则
    - A、B、C、D
    - A1、B3、B2、B1、C2、C1、D

安全级别越来越低

  - 美国国防部采购的系统，要求其安全级别至少达B级，商业用途的系统也至少达到C级

系统安全



系统安全

- **威胁 Threat：**
  - 对资产或组织可能导致负面结果的一个事件的潜在源
  - 威胁是客观存在的
  - 威胁的来源包括自然威胁、人为威胁和环境威胁
  - 威胁的来源可能不只一个
  - 动机和能力是威胁的重要属性

系统安全

- 脆弱性 Vulnerability：
  - 也可称为弱点或漏洞，是资产或资产组中存在的可能被威胁利用造成损害的薄弱环节。
  - 与资产紧密相连，是其固有的属性，是客观存在
  - 脆弱性可能存在于物理环境、组织、过程、人员、管理、配置、硬件、软件和信息等各个方面。
  - 一般包括技术层面和管理层面两方面
    - 前者主要与资产本身的属性有关，典型的是操作系统和应用软件的漏洞
    - 后者包括安全管理体系不完备和管理制度体系没有有效执行

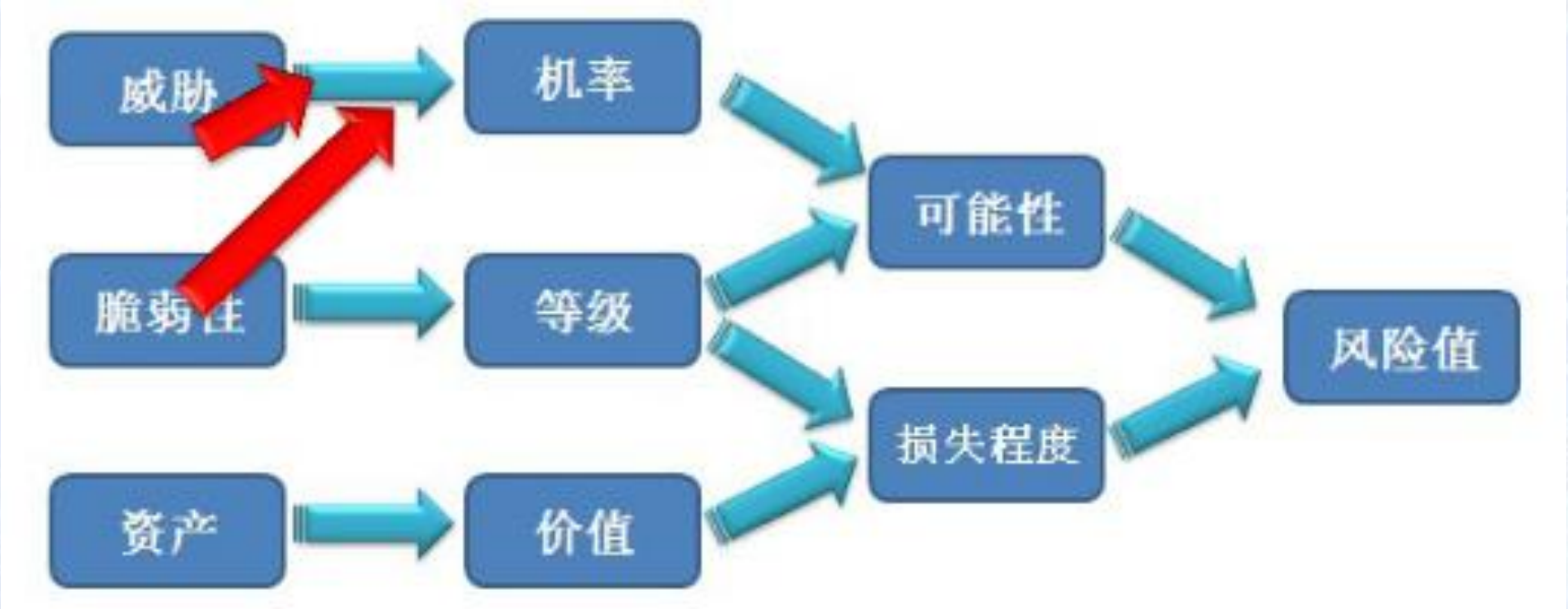
系统安全

- 风险 **Risk**：不确定性对目标的影响
  - 风险强调的是损害的潜在可能性，而不是事实上的损害
  - **Risk is the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability**
  - 信息安全是围绕风险展开，一般对风险进行定性描述
  - 风险评估围绕着资产、威胁、脆弱性和安全措施这些基本要素展开

系统安全

- 每一威胁可能利用一个或数个脆弱性
- 脆弱性本身不会引起风险
- 如果没有脆弱性，威胁也无法造成风险
- 一般先识别威胁后识别脆弱性

- 风险评估



安全评估方法

- 信息系统安全评估框架 ISSAF
- Web应用安全联合威胁分类 WASC-TC
- NIST SP 800-115 信息安全测试和评估技术指南
- 网络安全等级保护

安全评估方法

- 信息系统安全评估框架 ISSAF
  - Information Systems Security Assessment Framework, supported by the Open Information Systems Security Group (OISSG)
  - 一种开放源代码的安全性测试和安全分析框架，分为若干个领域(network security, host security, application security, database security, social engineering)，可以根据实际情况对每个领域进行相应调整。
  - 兼顾了安全测试的技术方面和管理方面。技术上有完备的评估程序，管理上明确了测试过程中应当遵循的管理原则和最佳实践。
  - 技术评估基准十分全面，可用于测试各种技术和不同流程
  - no longer maintained

安全评估方法

- Web应用安全联合威胁分类 WASC-TC
  - Web Application Security Consortium Threat Classification
  - 从攻击手段和安全弱点两方面讨论安全问题
  - 帮助开发人员和安全审计人员以不同的视图了解Web应用程序面临的安全威胁
    - 枚举视图、开发视图和交叉引用视图
  - 和OWASP、CWE/SANS兼容

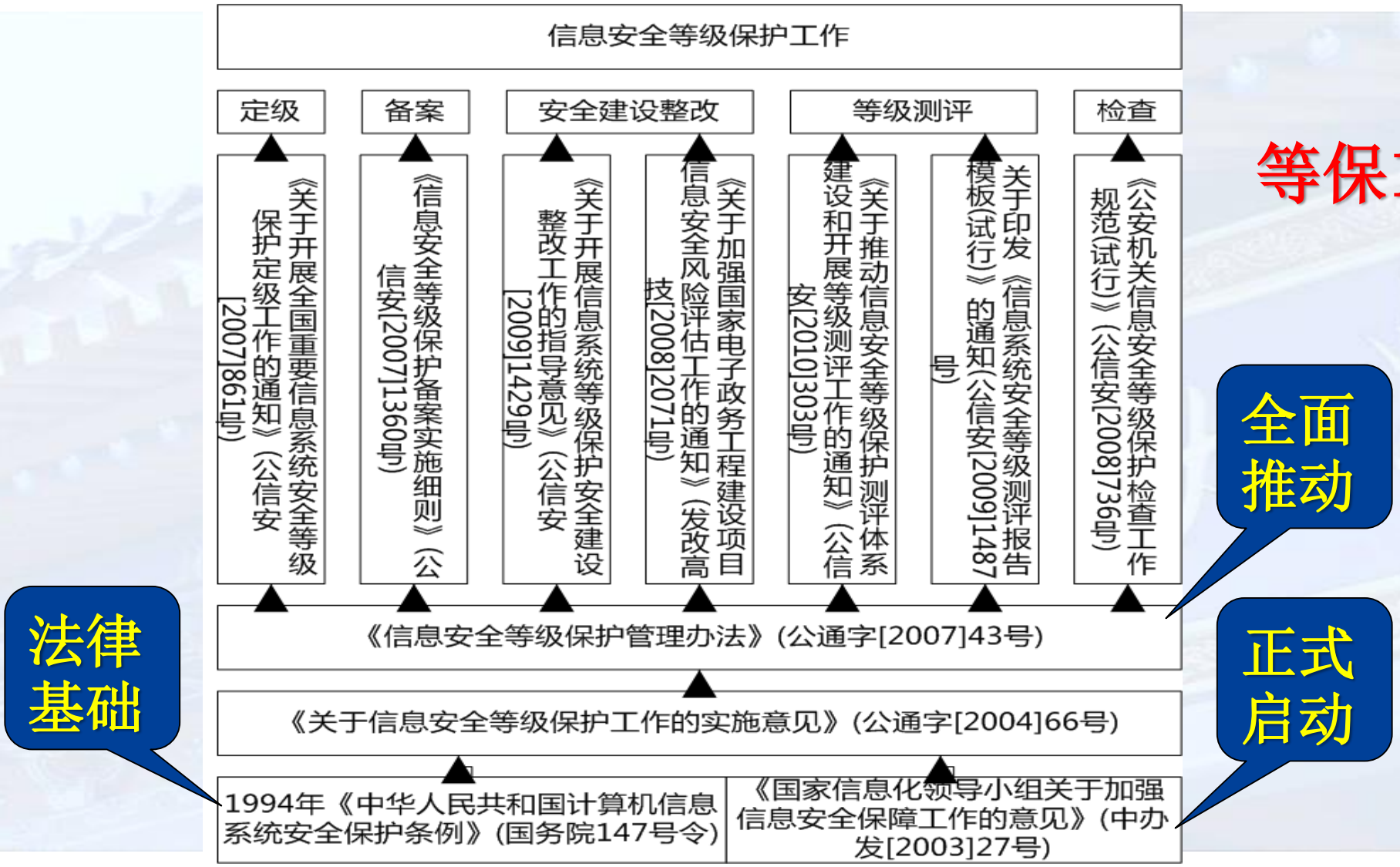
安全评估方法

- NIST SP 800-115 信息安全测试和评估技术指南
  - Technical Guide to Information Security Testing and Assessment, 2008
  - SP800是美国NIST（National Institute of Standards and Technology）发布的一系列关于信息安全的指南（SP, Special Publications）
    - 不是正式出版物，但得到美国和国际安全界广泛认可
    - 是指导美国信息安全管理建设的主要标准和参考资料

网络安全等级保护

- 《中华人民共和国计算机信息系统安全保护条例》（1994）
  - 第九条 计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。
- 《信息安全等级保护管理办法》2007
- 《信息安全等级保护标准体系》2008

网络安全等级保护



等保1.0

全面推动

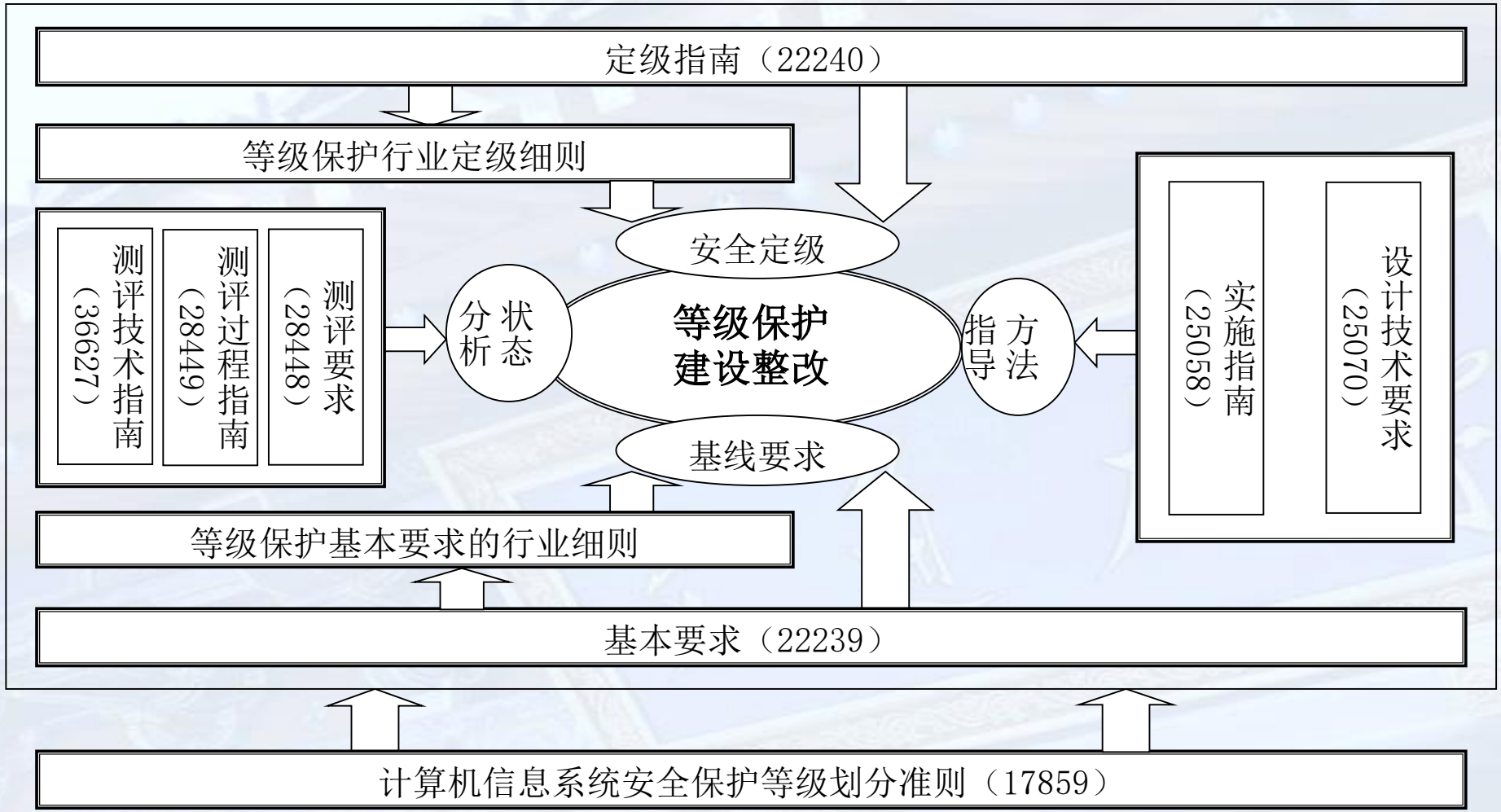
正式启动

法律基础

网络安全等级保护

- 等保2.0
  - 《网络安全法》(2017)
    - 第二十一条　国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，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
  - 《网络安全等级保护条例》（2019）
  - 《网络安全等级保护标准体系》（2019）
    - 2019年5月13日下午，国家市场监督管理总局召开新闻发布会，正式发布了网络安全等级保护2.0（简称等保2.0）核心标准，网络安全等级保护正式进入2.0时代。

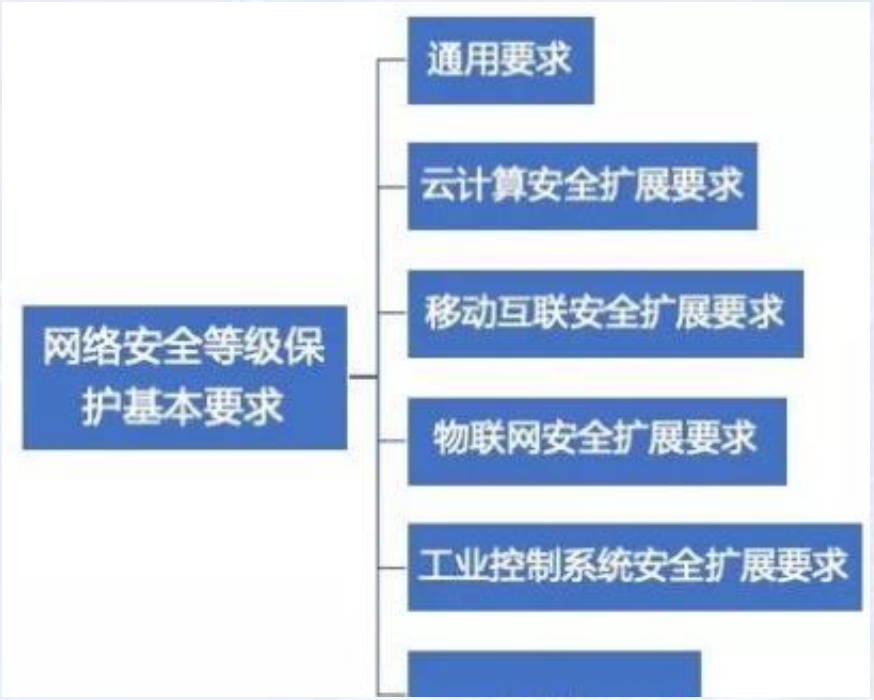
网络安全等级保护



等保 2.0

网络安全等级保护

- 等保2.0
  - 原来：《信息系统安全等级保护基本要求》
    - 改为：《信息安全等级保护基本要求》
      - 再改为：《网络安全等级保护基本要求》
  - 原来：安全要求
    - 改为：安全通用要求 + 安全扩展要求
  - 原来：被动防御
    - 改为：主动防御，分区、分层隔离，事前/事中/事后防御



网络安全等级保护


等保2.0
通用要求
+
扩展要求
云计算安全
移动互联安全
物联网安全
工控系统安全
技术要求
安全物理环境
安全通信网络
安全区域边界
安全计算环境
管理要求
安全管理中心
安全管理制度
安全管理机构
安全管理人员
安全建设管理
安全运维管理

网络安全等级保护

第一级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成损害，但不危害国家安全、社会秩序和公共利益；

第二级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成严重损害或特别严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全；

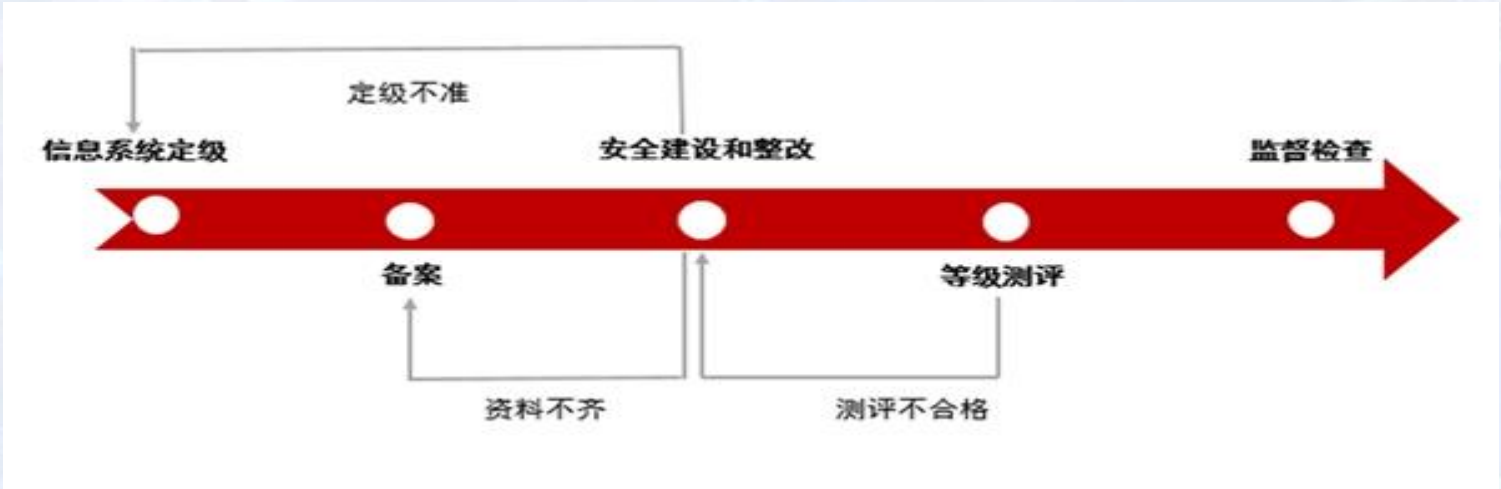
第三级，等级保护对象受到破坏后，会对社会秩序和公共利益造成严重危害，或者对国家安全造成危害；

第四级，等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重危害，或者对国家

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

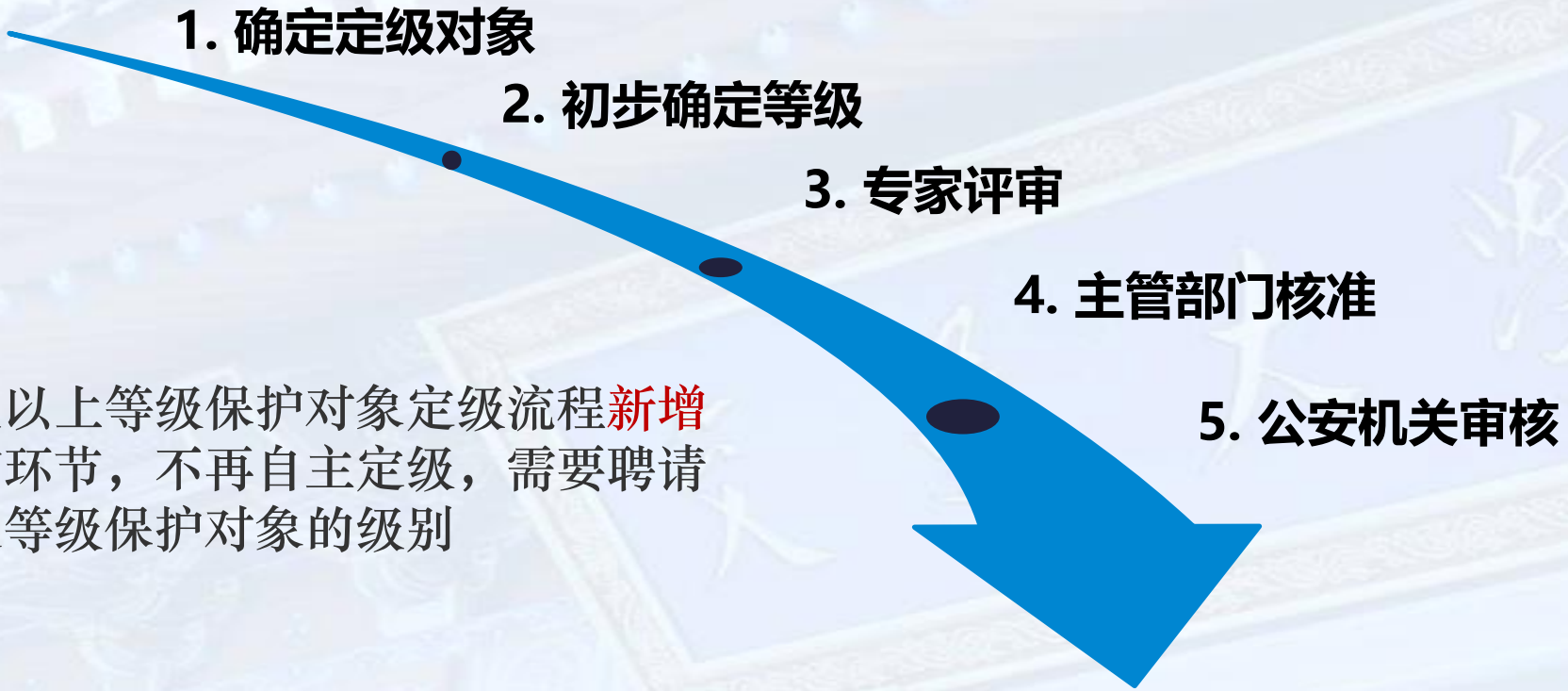
网络安全等级保护

- 包括：系统定级、系统备案、安全建设整改、等级测评和监督检查五个环节。



网络安全等级保护

- 定级流程



第二级及以上等级保护对象定级流程新增专家评审环节，不再自主定级，需要聘请专家认定等级保护对象的级别

网络安全等级保护

- 作为定级对象的信息系统应具有如下基本特征：
  - 具有确定的主要安全责任主体；
  - 承载相对独立的业务应用；
  - 包含相互关联的多个资源。

网络安全等级保护


等级保护对象
通信网络设施
信息系统
数据资源
传统信息系统
工业控制系统
云计算平台
物联网
采用移动互联技术的系统

表 5 报业网络安全等级保护定级参考

序号	分类	定级对象	单位类别			
			中央级报社	省级报社	行业报社	都市报社
1	新闻生产	融媒体/全媒体系统	第三级	第三级	第三级	第二级
2		新闻采编发系统	第三级	第三级	第二级	第二级
3		新媒体制作发布系统	第三级	第三级	第二级	第二级
4		网站新闻发布系统	第三级	第二级	第二级	第二级
5		报道指挥系统	第三级	第二级	第二级	第二级
6		新闻大屏系统	第二级	第二级	第二级	第二级
7	业务支撑和服务	云计算平台	第三级	第三级	第三级	第二级
8		大数据平台	第二级	第二级	第二级	第二级
9		媒资系统	第二级	第二级	第二级	第二级
10		舆情系统	第二级	第二级	第二级	第二级
11		邮件系统	第二级	第二级	第二级	第二级
12	管理	办公经营系统	第二级	第二级	第二级	第二级
13		运维管理系统	第二级	第二级	第二级	第二级

分级保护

- 分级保护针对涉密信息系统，由国家保密局发起，推广带有强制性
  - 等级保护是针对非涉密网，等级保护是公安部门发起的，执行力相对分保要弱一点。
- 分级保护按照所处理信息的最高密级，由低到高划分为秘密、机密和绝密三个等级。
  - 其保护水平总体上不低于等保第三级、第四级、第五级的水平。

Any Questions?