网络空间威胁对抗与防御技术研讨会
暨 第七届安天网络安全冬训营

美军武器系统风险管理的认知与启示

安天研究院

威胁框架：认知与实践

寒夜远征

寒夜远征

CONTENTS

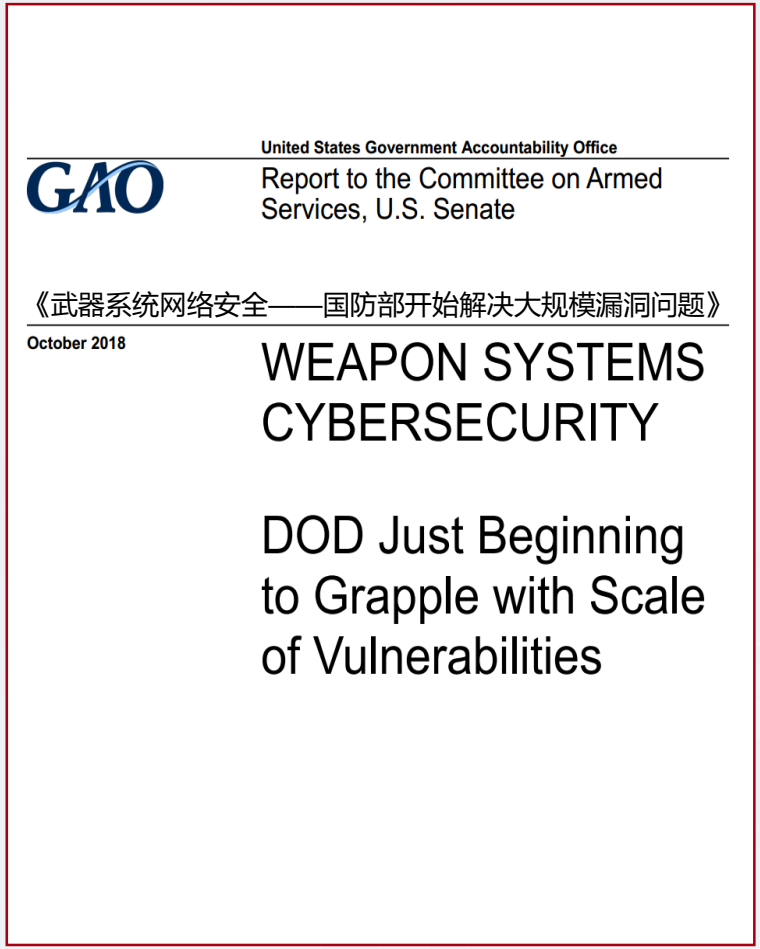
目 录

寒夜速纪

威胁框架：认知与实践

01 风险管理框架

美方如何认识自己的武器系统网络安全


United States Government Accountability Office

GAO

Report to the Committee on Armed Services, U.S. Senate

《武器系统网络安全——国防部开始解决大规模漏洞问题》

October 2018

WEAPON SYSTEMS CYBERSECURITY

DOD Just Beginning to Grapple with Scale of Vulnerabilities

- 报告称美国防部在保护武器系统免受网络威胁方面面临巨大挑战。这是由武器系统计算机化的本质、武器系统网络安全起步晚、以及对武器系统安全性理解不够等综合决定的。随着国防部武器系统的软件化和网络化趋势不断加强，这一问题亟待解决。
- 一直以来，国防部将网络安全工作的重点放在保护网络和传统IT系统，直到最近才开始研究如何更好地解决武器系统网络安全问题。计划投入约1.66万亿美元来开发目前的武器系统组合，这些武器对维持美国的军事优势和威慑力至关重要。

美方如何认识自己的武器系统网空安全（续）

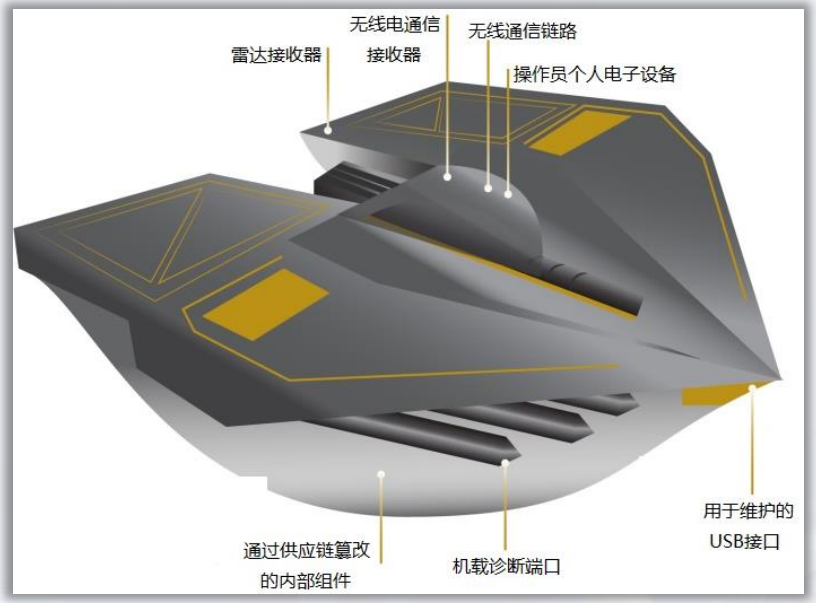
美国国防部武器系统比以往更加依赖于软件和IT，并且更加网络化。自动化和连通性成为美国现代军事能力的基本推动力，但它们使武器系统更容易受到网空攻击。截至目前，美国国防部仍在探索如何更好地解决武器系统的网络安全问题。

嵌入式软件和信息技术系统在武器系统中普遍存在

导致美方武器系统网络安全现状的因素

武器系统是大型的、复杂的，具有各种形状和大小，功能各异的系统中的系统。多种因素促成了国防部武器系统网络安全的现状，具体包括：

- 美国国防部武器系统的日益计算机化；
- 美国国防部武器系统比以往更加依赖商业软件和IT实现预期的性能；
- 越来越多的连接到并依赖外部其他网络系统；
- 自动化和连通性成为现代军事能力的基本推动力，使武器系统更容易受到网空攻击；
- 武器系统网络安全起步较晚，美国国防部过去没有优先考虑武器系统的网络安全；
- 美国国防部对如何更好地开发网络安全武器系统存在误解，对面临的问题、存在的漏洞、解决办法仍不清楚。



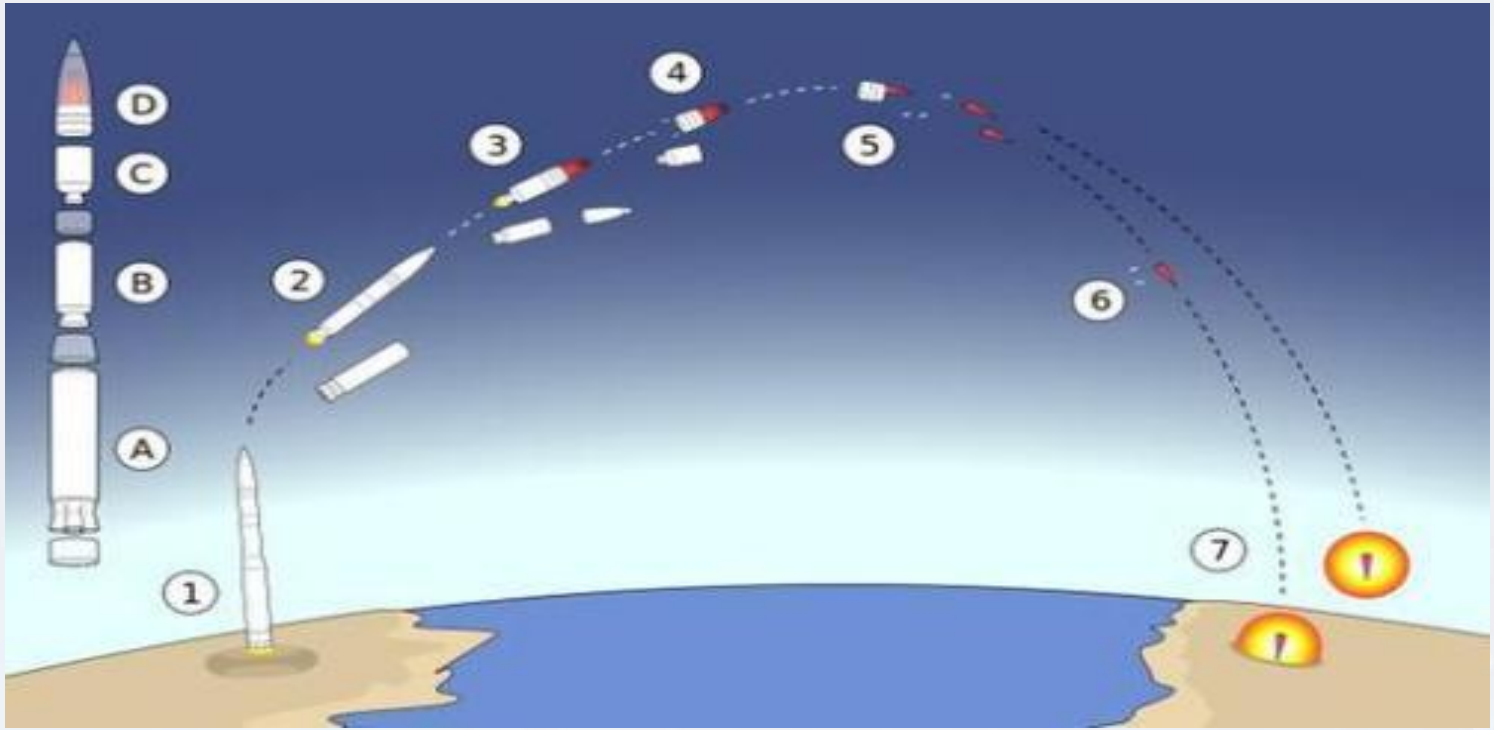
武器包括众多接口，扩大了武器系统被攻击面

（基于保密原因，通过虚构的武器系统表示）

示例：战略导弹系统——发射井

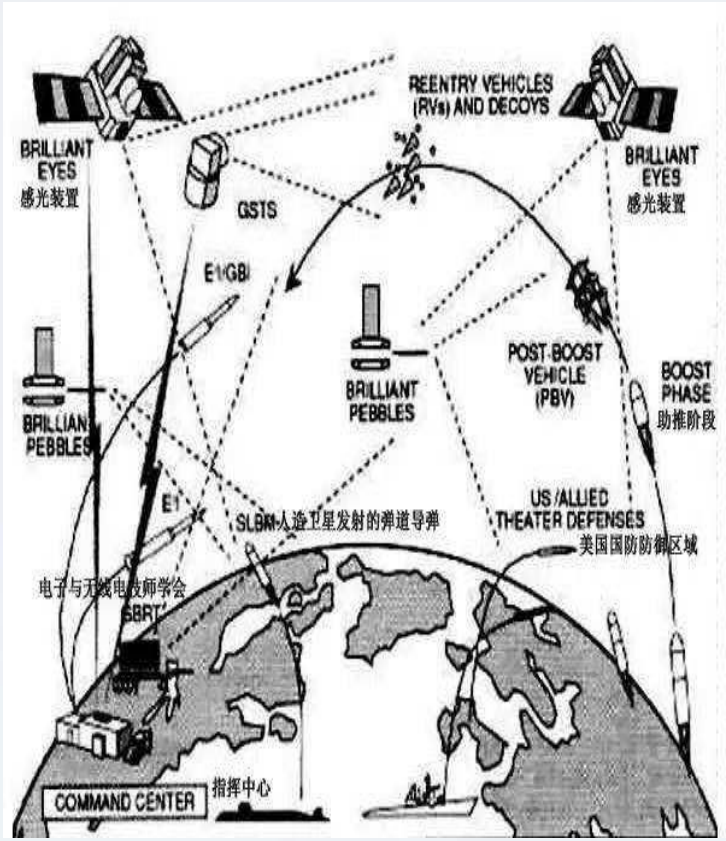
美方在检测中发现发现存放民兵核武器的发射井存在巨大安全隐患，因为也与互联网相连，它很可能会使导弹飞行制导系统失灵。

战略导弹-系统设计阶段



在设计战略导弹之初时，因当时计算机能力有限，没有考虑潜在的网络漏洞。攻击者可通过对源代码、固件和内部门户进行入侵。

战略导弹系统-通讯中可被攻击部分

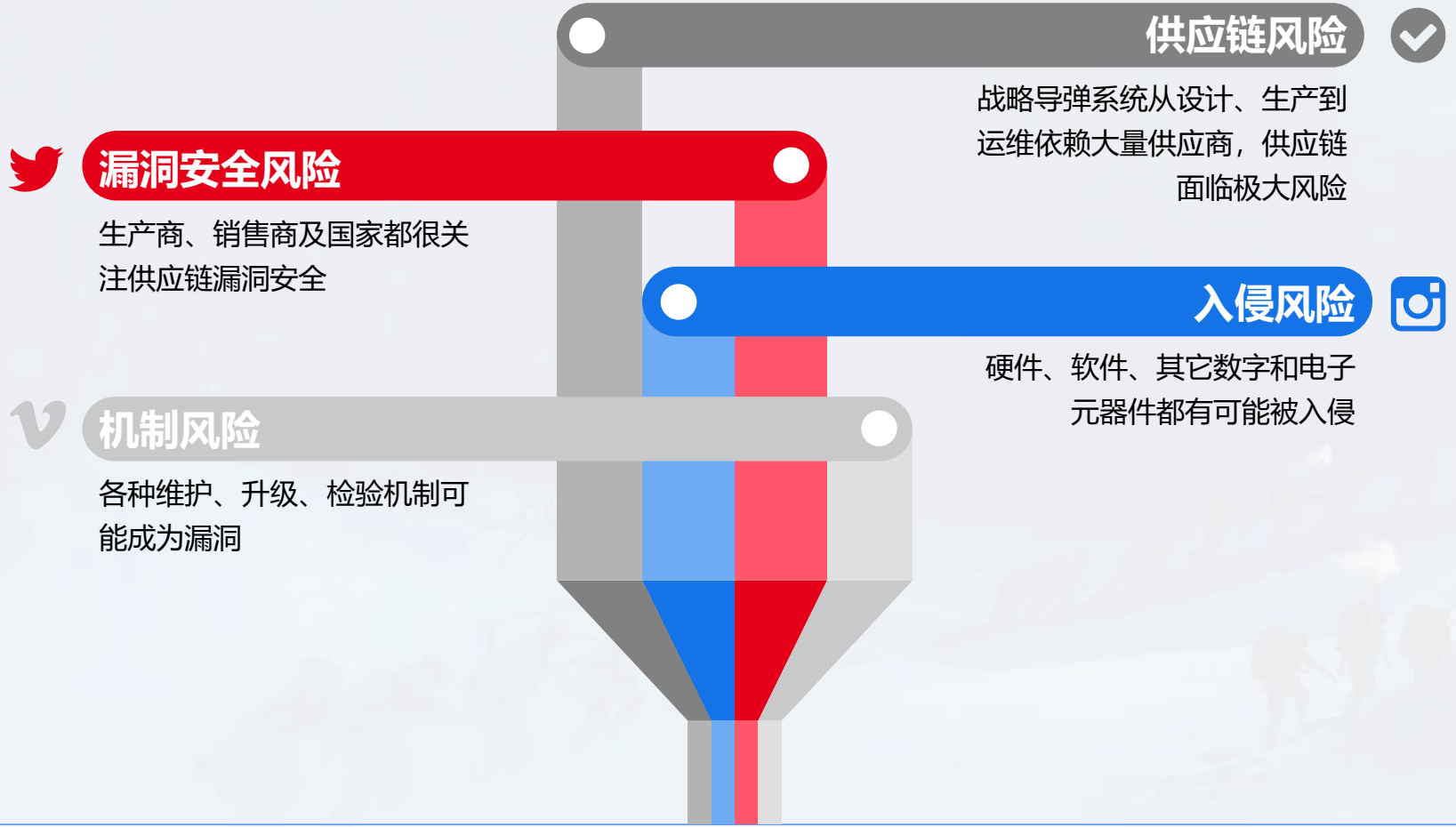


- 命令与控制中心之间的通讯；
- 从命令指挥中心到导弹平台和导弹的通讯；
- 从导弹到地基和天基命令和控制部分的遥测数据；
- 收集和解译长期和实时情报的分析中心
- 运输中的网络技术；
- 实验室和装备设施中的网络技术；
- 上载的预发射目标信息；
- 来自天基系统的实时目标信息，包括来自全球导航系统的位置、导航和时间数据；
- 来自天基、空基和地基传感器的实时天气信息；
- 发射平台（如核潜艇）的位置数据；
- 地面站的实时目标信息；
- 协作命令中心联盟之间通讯；
- 战略基础设施内的机器人自主系统

战略导弹-系统维护阶段

- 在测试时，通过端口植入恶意软件入侵系统；
- 通过新组件的更换，在新组件中植入恶意代码入侵系统。

战略导弹的风险梳理


供应链风险
战略导弹系统从设计、生产到运维依赖大量供应商，供应链面临极大风险
漏洞安全风险
生产商、销售商及国家都很关注供应链漏洞安全
入侵风险
硬件、软件、其它数字和电子元器件都有可能被入侵
机制风险
各种维护、升级、检验机制可能成为漏洞

美方提高武器系统网络安全采取的措施

国防部加强网络系统安全相关策略时间线

美方提高武器系统网络安全采取的措施

- 美国国防部在整个武器系统全生命周期从需求开发开始，直到系统退役制定网络安全相应规范，这一过程由采办系统（DAS）完成。 DAS由JCIDS(联合能力集成与开发系统，负责需求开发)、采办流程（负责系统开发、部署、运维支持）、PPBE（规划计划预算与执行，资金）流程3部分组成，各阶段对应的指南如图所示。

（1）系统概念设计阶段： 网络可生存性确认指南（CyberSurvivability Endorsement,CSE）

（2）系统开发阶段：网络可生存性测试与评估指南（CyberSurvivability Test&Evaluation, CS T&E）

（3）系统部署阶段：风险管理框架指南（Risk Management Framework ,RMF）

美方提高武器系统网络安全采取的措施

2014, 国防部副部长要求联合参谋部开发“网络安全”关键性能参数（KPP）
- 目标：通过精细的设计，以及在实际应用环境中测试和相关的DOTmLPF-P流程，在部署之前消除或有效缓解已知漏洞
- 问题：需求文档中的系统可生存性需求并不足以阐述网络攻击的预防、缓解、恢复

2015-, 对新武器系统，从需求上改善“网络可生存性”
- 2015.12：《JCIDS手册》中增加了将网络可生存性作为系统可生存性关键性能参数（SS-KPP）之一予以确认的要求
- 2017.01：JROCM《网络可生存性确认实施指南》
- 2018.08：《JCIDS手册》增加了初始功能设计和对CSRC及的细节要求

2016-, 对原有武器系统提升网络可生存性->2019.12+
- 对国防部重大武器系统进行网络漏洞评估
- 优先对导弹、作战司令部等136个关键武器系统进行评估

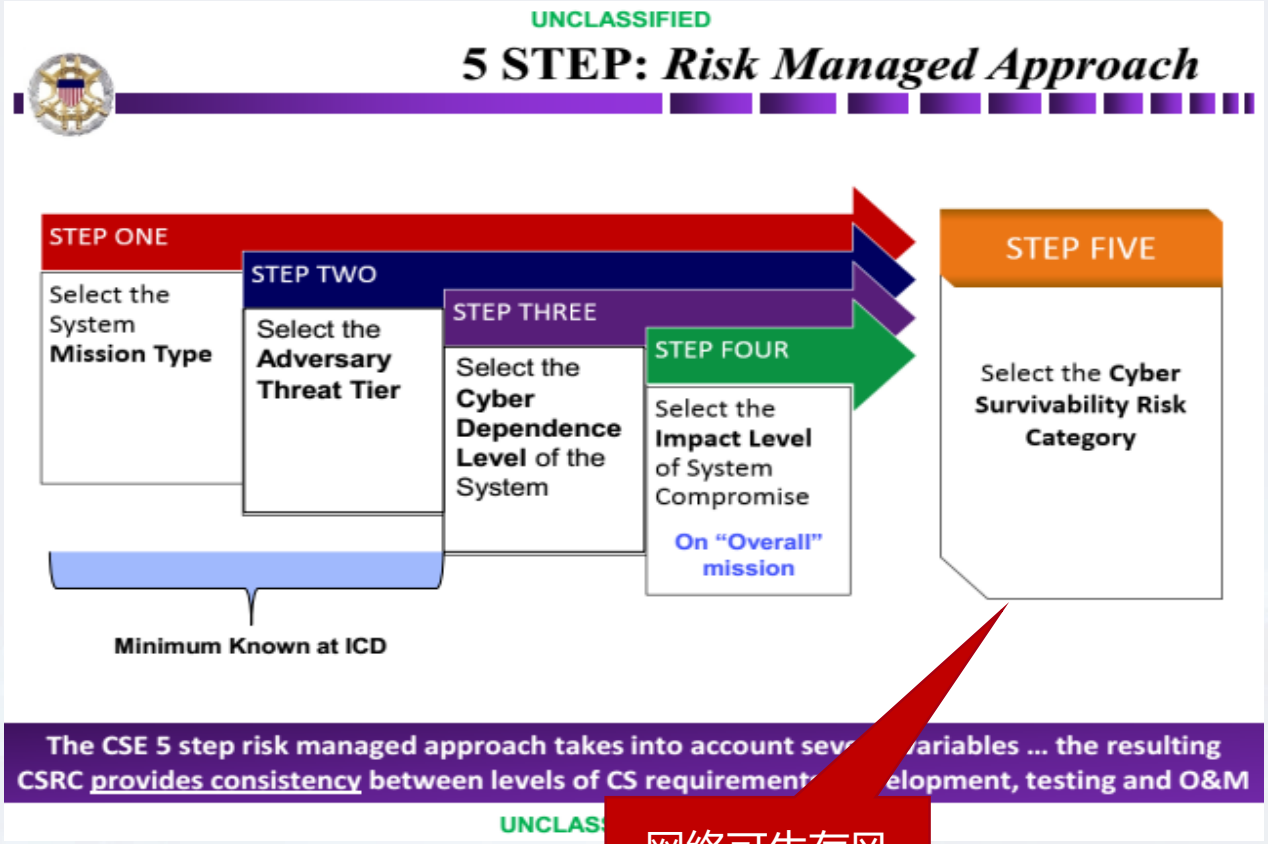
2017-， 提升国防部驻军关键基础设计的网络可生存性->2020.12
- 对国防部驻外关键基础设施进行网络漏洞评估
- 优先对474个驻外基地进行评估

3个不同方向

所有国防部武器系统及支撑基础设施都具备与风险管理相称的网络可生存性

CSE 5要素

- CSE 5步风险管理流程
  - 确定系统任务类型
  - 确定对抗威胁水平等级
  - 确定系统的网络依赖等级
  - 确定系统受损的影响等级
  - 确定网络可生存性风险类型

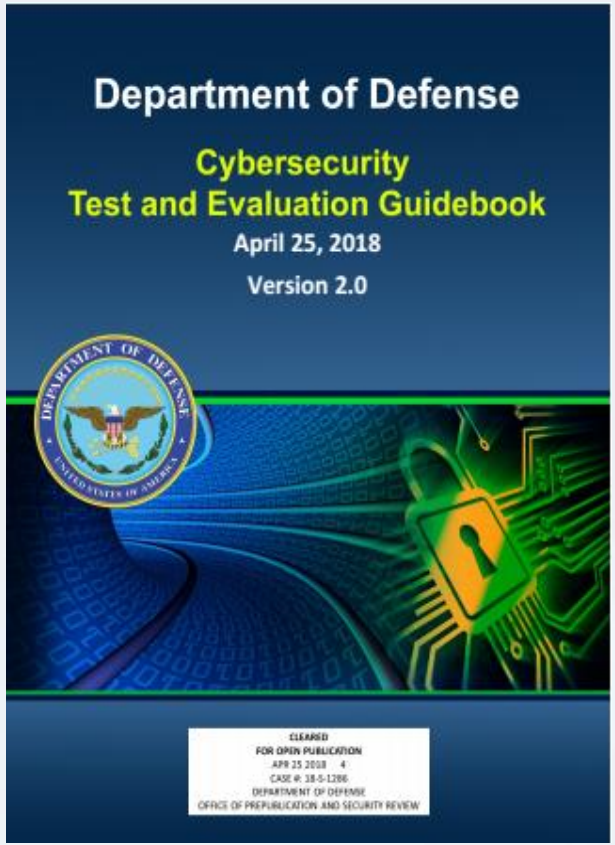


CSE 5要素

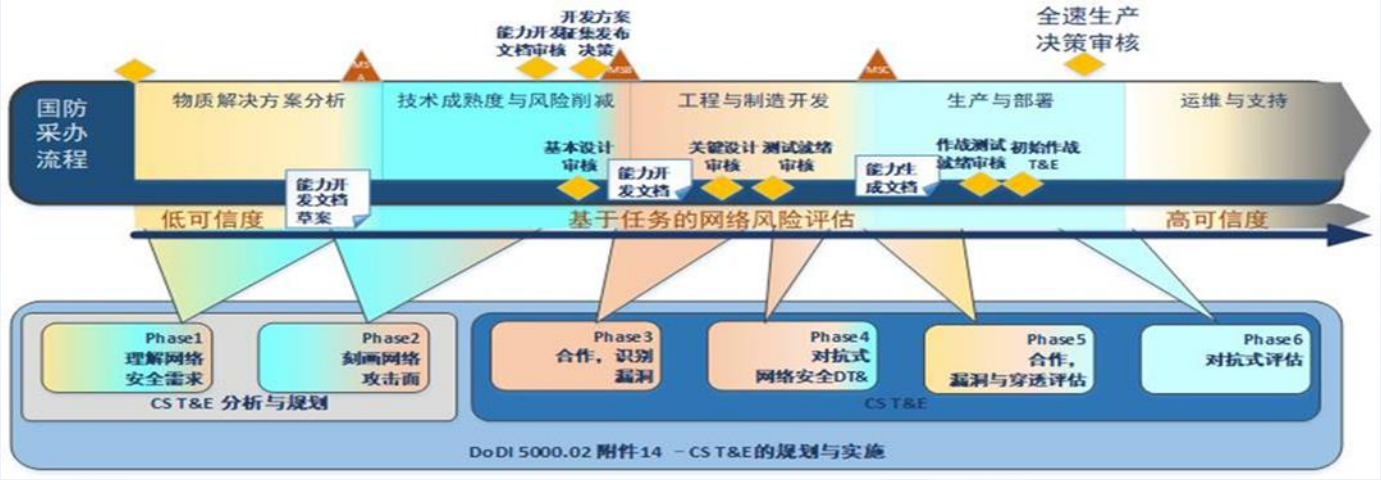
步骤		核心目标	子任务
知彼知己	理解网络安全需求	充分理解系统工程流程开发的系统安全和弹性需求，并以之为基础开发初始CS T&E方法和方案。	编制网络安全和弹性需求清单
			准备网络安全 T&E活动
			设计 CS T&E方案
	刻画网络攻击面	识别任务关键组件、数据、已知漏洞，以及对手可能如何利用这些漏洞。	识别网络攻击面
			网络攻击面分析
			生成网络攻击面分析报告
			形成DT&E策略及事件安排
DT&E 检验系统在任务条件下是否达到其宣称的能力。是一个测试-分析-调整-再调整的过程	合作识别漏洞（CVI）	“合作”指的是本过程与前一过程中“攻击面评估”的迭代关系。从战术角度（杀伤链）对攻击面进行再评估	开发承包商/政府工具测试方案，聚焦于组件、接口、架构在任务条件下的功能漏洞
			进行迭代测试活动，记录测试结果，并生成测试报告
			完成ACD基础设施设计方案
	对抗式网络安全开发T&E(ACD)	验证网络安全及弹性需求是否满足，以及发现未知关键漏洞并判断其任务影响，在安全的作战测试环境中对系统进行充分漏洞利用测试	更新网络威胁评估和攻击面分析（审核第2步完成的攻击面分析，并利用网络杀伤链来识别当前威胁战术和目标，并更新）
			ACD方案设计—开发详细测试方案
			实施ACD测试，并生成测试报告
OT&E 评估系统在预期作战环境下对关键任务的赋能作用）2017年（DoDI 5000.02附件14）和2018年 DOT&E备忘录要求	合作漏洞与穿透评估（CVPA）	了解系统在完全作战条件下的网络安全和弹性状态，支持下一步对抗评估。	设计测评方案
			协调测评活动
			实施测评并生成报告
	对抗评估（AA）	通过红-蓝对抗对系统(漏洞)对关键任务效用进行评估，同时也评估现有支持人员及装备在预期作战环境下的能力，以及系统防御能力的效能。	设计对抗评估方案
			与作战测评组协调
			实施作战测评，并生成报告

- 阶段 1—理解CS需求。目的：以检查系统的网络安全及弹性需求，为开发初始CST&E方法和规划做准备。
- 阶段2 - 描述攻击面。目的：识别漏洞和对手可能使用的攻击途径，并开发任务影响评估计划。
- 阶段3 – 合作漏洞识别。目的：校验网络安全和弹性，识别漏洞及所需的缓解，相关信息（网络可生存性和弹性改善需求）将提供给系统的设计、开发、工程人员。
- 阶段4 – 对抗性网络安全开发测试评估（DT&E），由一个对手组（红队）测试系统的网络安全和弹性。测试使用任务上下文，在真实的对抗作战环境中，使用真实的威胁利用技术来识别残余风险。
- 阶段5 – 合作漏洞与穿透评估。目的：充分刻画系统在完全作战环境中的网络安全和弹性状态，提供系统侦察支持对手评估（AA）
- 阶段6 – 对手评估，描述典型威胁的网络活动对关键任务构成的实际效果，以及防御能力的有效性。

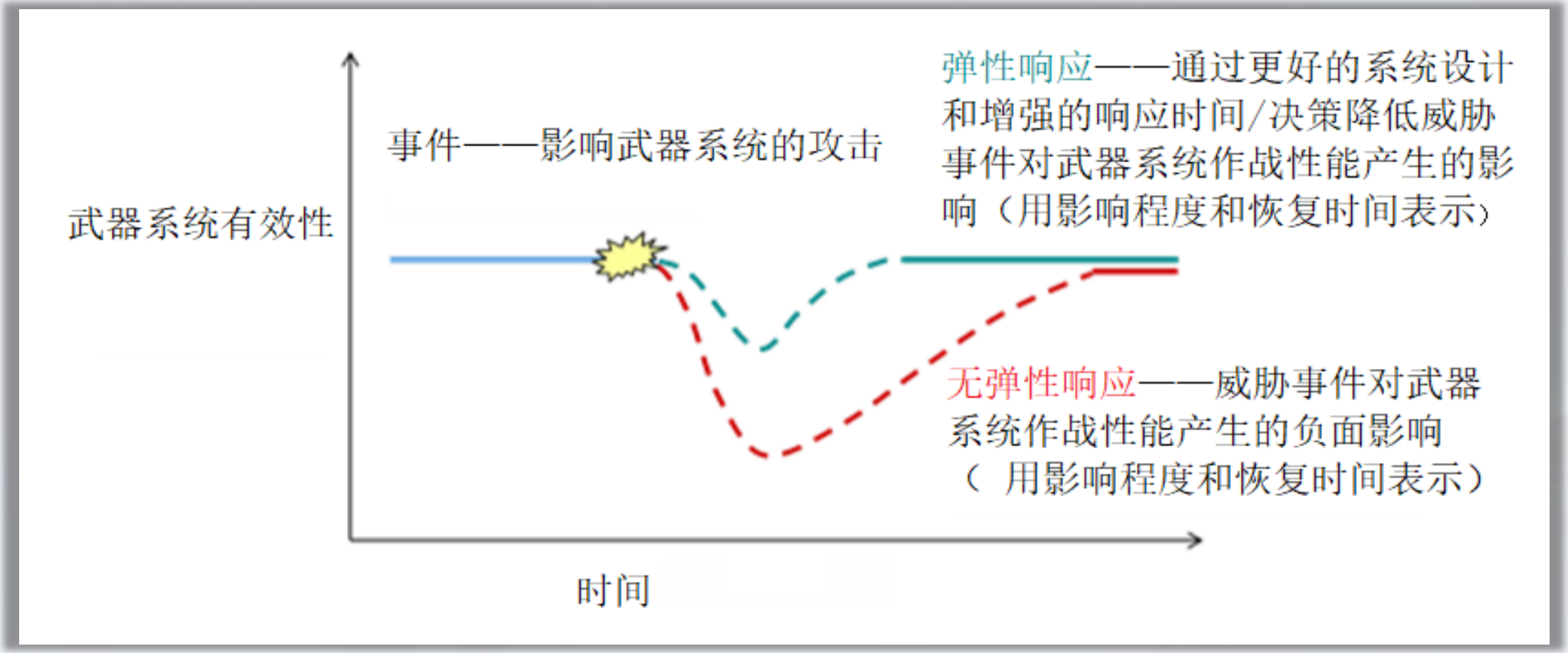
系统开发过程：CS T&E



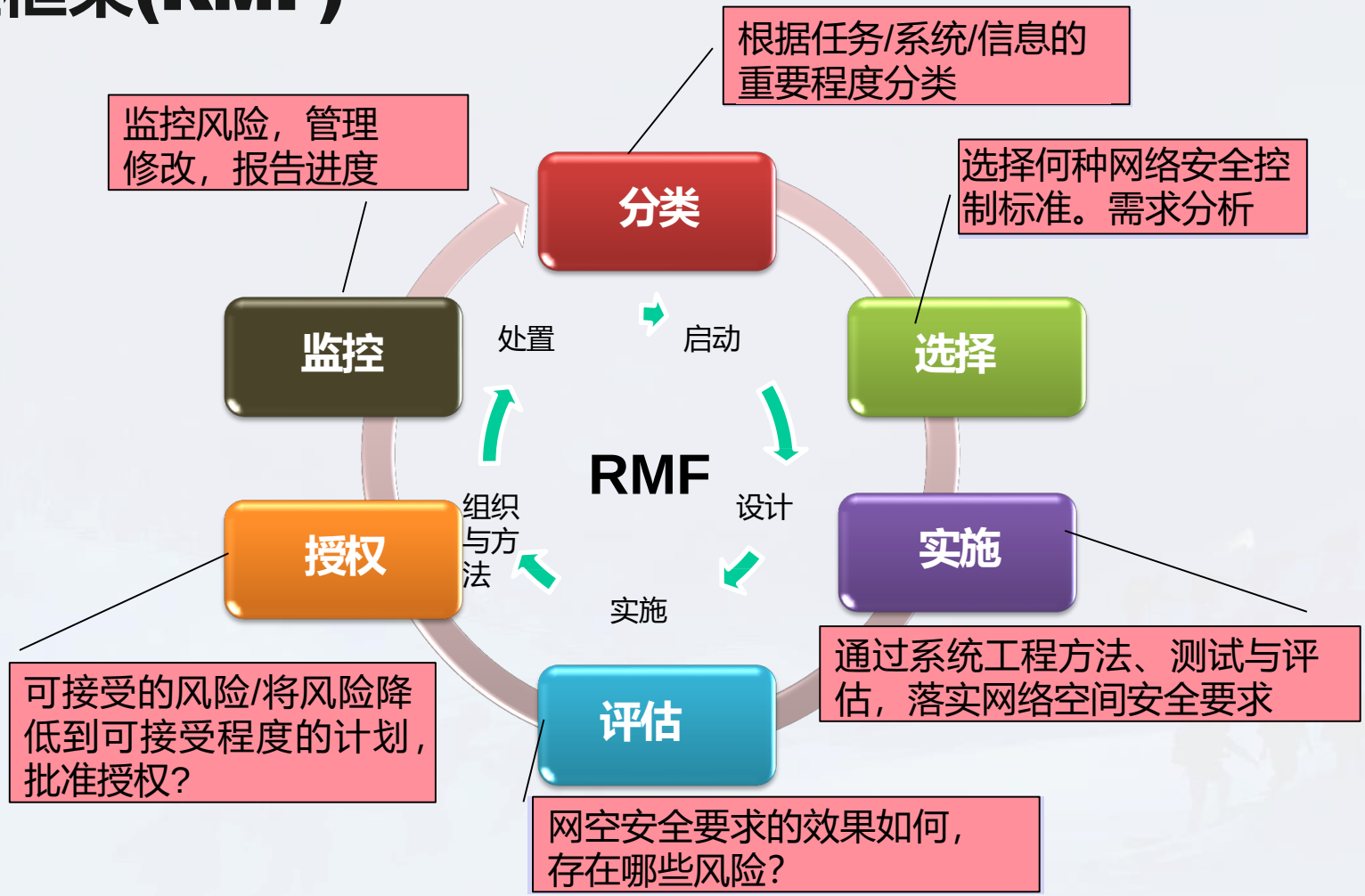
- 目标：在系统开发生产阶段，通过开发和作战测试评，实现RMF要求（baked-in）
- 回答两个问题：
  - ✓ 系统在作战条件下的网络可生存能力



武器系统作战单元的网络可恢复弹性（韧性）能力



风险管理框架(RMF)


根据任务/系统/信息的
重要程度分类
选择何种网络安全控
制标准。需求分析
通过系统工程方法、测试与评
估，落实网络空间安全要求
网空安全要求的效果如何，
存在哪些风险?
可接受的风险/将风险降
低到可接受程度的计划，
批准授权?
监控风险，管理
修改，报告进度
分类
选择
实施
评估
授权
监控
RMF
启动
设计
实施
组织
与方
法
处置

RMF基本内容

- 步骤1：分类
  - 根据可能的最坏情况，对组织、任务/业务、系统的负面影响，判断信息和系统的重要性。
  - 支撑标准-FIPS 199 （安全目标->影响分级）
- 步骤2：选择
  - 根据步骤1的分类结果，结合风险评估，选择安全控制基线
  - 支撑标准 – SP 800-53、FIPS 200
- 步骤3：实施
  - 在企业架构和系统内实施安全控制，使用成熟的系统安全工程方法，实现安全配置设施。
  - 支撑标准- SP 800 160等

RMF基本内容（续）

- 步骤4：评估
  - 确定安全评估的有效性—是否正确实施、按预期运营、以及满足安全需求?
  - 支撑标准- SP 800-53A
- 步骤5：授权
  - 检查安全控制评估结果，确认风险是否可接受
  - 支撑标准 – SP 800-37
- 步骤6：监测
  - 对实施的各项控制进行持续监测，并将监测整合为整个机构的统一监测项目。
  - 支撑标准- SP 800-39(风险监测)、SP 800-128（配置管理监测）、SP 800-137（控制有效性监测）

RMF主要特点

- RMF采用系统工程思想来管理复杂系统的风险，特点包括：

可复制性

- 可复制性意味普适性，提供可重复的流程，用以推动不同信息及信息系统的风险防护。

可定制性

- 可定制意味着灵活性，框架可扩展和可迭加，CS T&E是RMF的扩展。

可度量性

- 可度量意味着可对流程的效果进行量化分析。

寒夜速纪

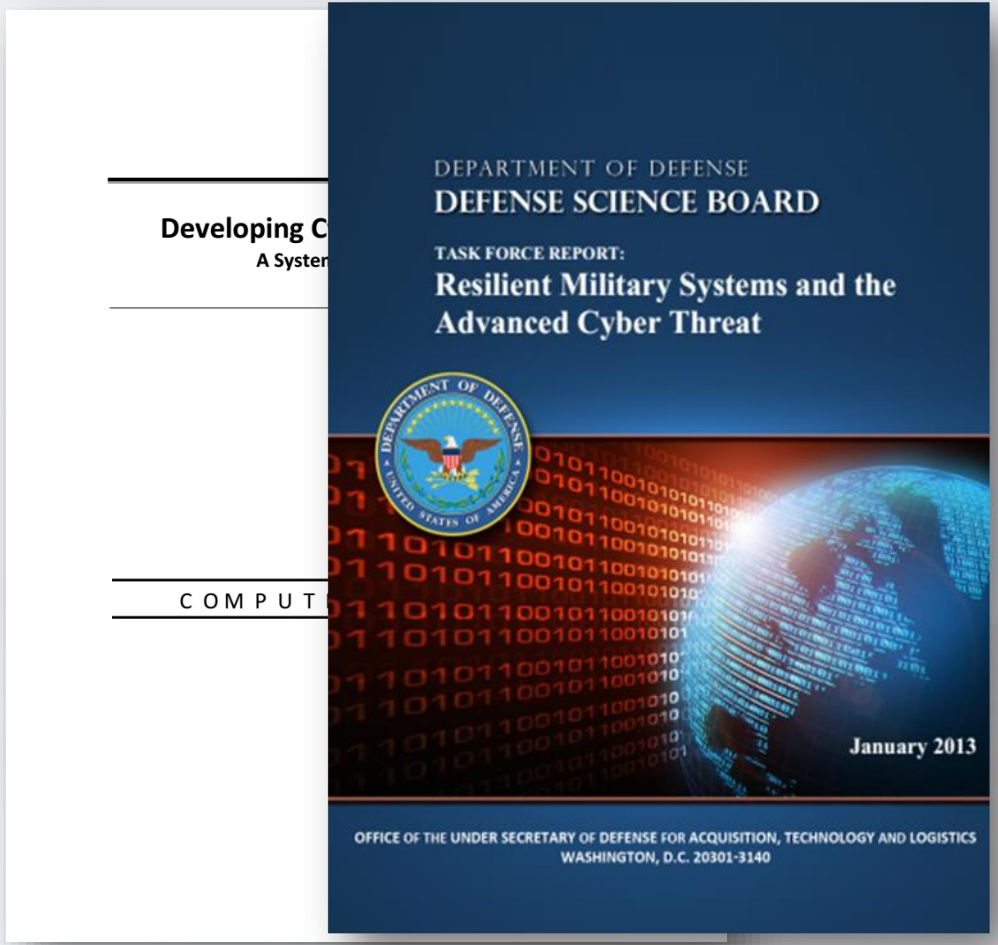
威胁框架：认知与实践

02 网络可恢复弹性（韧性）

1. 什么是网络可恢复弹性（韧性）

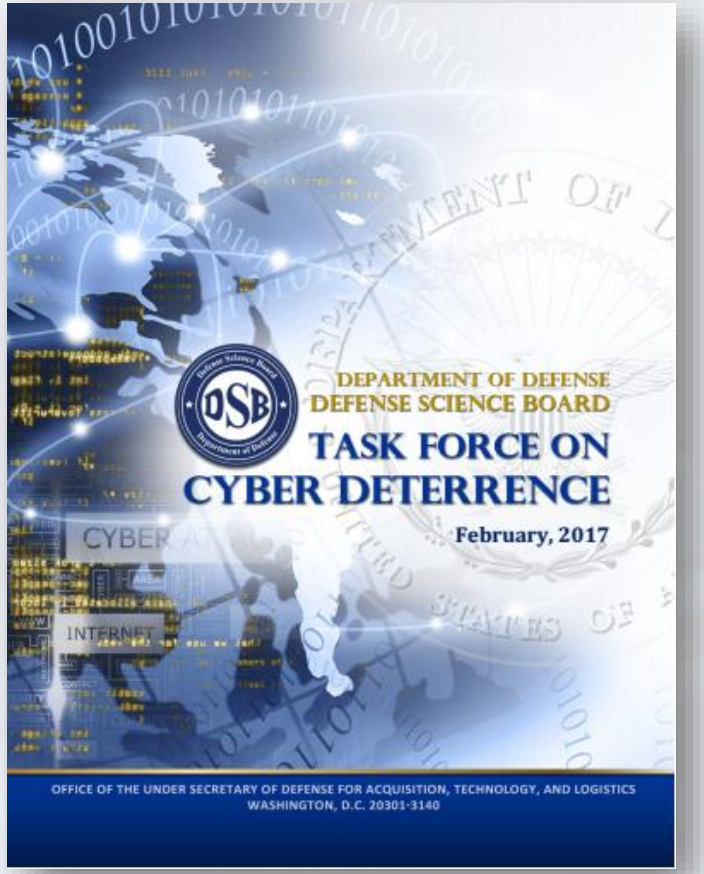
- 定义：网络弹性是系统(包括网络资源)预判和承受不利条件、压力、攻击、损害，并从中恢复和适应的能力。

- 系统
- 组件（部件）
- 服务，通用基础设施
- 机构
- 关键基础设施区域或部分
- 体系
- 国家



1. 什么是网络可恢复弹性（韧性）

- 目的（为什么要提出网络可恢复弹性要求）：解决日益复杂的供应链和日益尖锐的网络对抗带来的不确定性。
  - 在国家战略层面，是通过确保“第二次打击能力”，实现网络威慑。
  - 在战术应用层面，是通过武器平台的网络可恢复弹性，保障网络环境下的作战可靠性。



2. 网络可恢复弹性（韧性）的工程实施

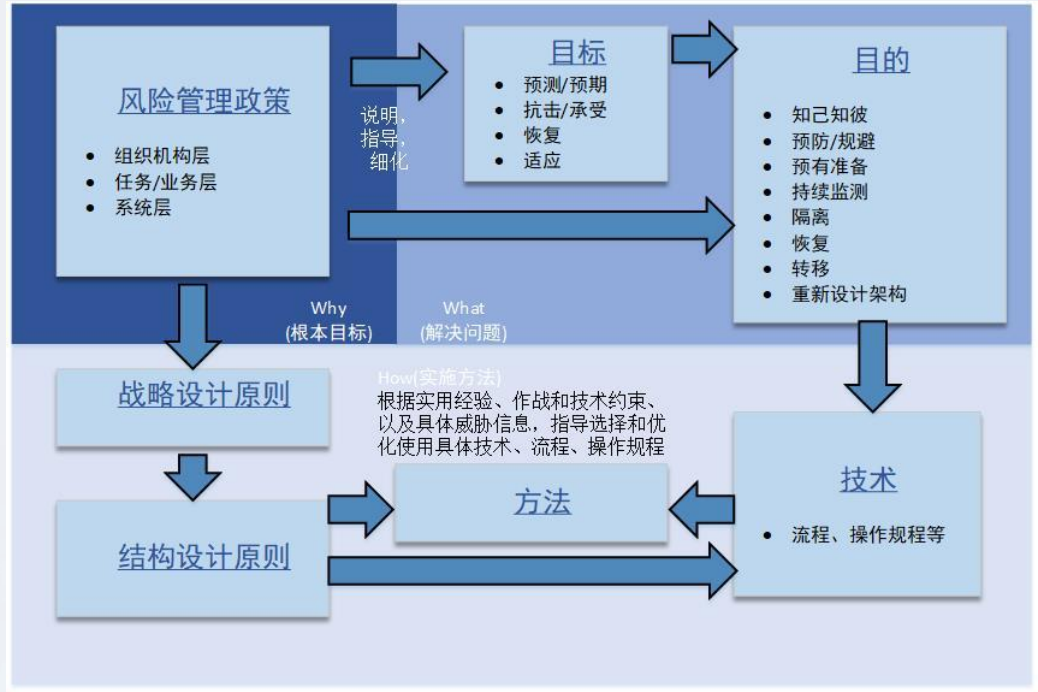
- NIST SP 800-160 提出网络可恢复弹性（韧性）的层次化工程实施框架

层次结构	定义、功能与应用说明		
目标（Goal）	定义：从多个角度（即预测、抗击、恢复、适应）描述弹性需求 功能：把网络弹性作为系统整体需求 应用：用于描述高层要求		
目的（Objective）	定义：从客户和开发人员两方面定义系统在全寿命周期以及作战环境中的任务可靠性和弹性安全需求，比目标层更具体、更面向威胁； 功能：使客户与开发人员对网络弹性达成共识，提出共同认可的度量标准 应用：用于量化评分或综合定性分析		
	子目的	定义：从不同角度对实施目的进行细化描述 功能：通过对实施目的逐层细化，分解为可定义性能指标的活动和能力 应用：用于量化评分或定性分析，可反映在系统功能需求中得	
		活动或能力需求	定义：描述可支持达成子目的的能力或活动 功能：帮助定义具体性能或效能指标，作为选择、定制或优先考虑的出发点 应用：用于量化评分或定性分析，反映系统功能需求
战略设计原则	定义：从多个角度（即预测、抗击、恢复、适应）描述弹性需求 功能：把网络弹性作为系统整体需求 应用：用于分析的非功能性需求描述		
结构设计原则	定义：对系统架构及设计的描述和定义 功能：指导在系统全寿命周期中使用合适的技术和方法进行设计和实施 应用：用于指导系统工程实施的非功能性需求描述		
技术	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程		
实施方法	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程		
解决方案	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程		

CONSTRUCT	DEFINITION, PURPOSE, AND APPLICATION AT THE SYSTEM LEVEL		
Goal	**Definition**: A high-level statement supporting (or focusing on) each aspect (i.e., anticipate, withstand, recover, adapt) in the definition of cyber resiliency. **Purpose**: Align the definition of cyber resiliency with definitions of other types of resilience. **Application**: Can be used to express high-level stakeholder concerns, goals, or priorities.		
Objective	**Definition**: A high-level statement (designed to be restated in system-specific and stakeholder-specific terms) of what a system must achieve in its operational environment and throughout its life cycle to meet stakeholder needs for mission assurance and resilient security; the objectives are more specific than goals and more relatable to threats. **Purpose**: Enable stakeholders and systems engineers to reach a common understanding of cyber resiliency concerns and priorities; facilitate definition of metrics or measures of effectiveness (MOEs). **Application**: Used in scoring methods or summaries of analyses (e.g., cyber resiliency posture assessments).		
	Sub-Objective	**Definition**: A statement, subsidiary to a cyber resiliency objective, which emphasizes different aspects of that objective or identifies methods to achieve that objective. **Purpose**: Serve as a step in the hierarchical refinement of an objective into activities or capabilities for which performance measures can be defined. **Application**: Used in scoring methods or analyses; may be reflected in system functional requirements.	
		Activity or Capability	**Definition**: A statement of a capability or action which supports the achievement of a sub-objective and hence, of an objective. **Purpose**: Facilitate the definition of metrics or MOEs. While a representative set of activities or capabilities have been identified in [Bodeau18b], these are intended solely as a starting point for selection, tailoring, and prioritization. **Application**: Used in scoring methods or analyses; reflected in system functional requirements.
Strategic Design Principle	**Definition**: A high-level statement which reflects an aspect of the risk management strategy that informs systems security engineering practices for an organization, mission, or system. **Purpose**: Guide and inform engineering analyses and risk analyses throughout the system life cycle. Highlight different structural design principles, cyber resiliency techniques and implementation approaches. **Application**: Included, cited, or restated in system non-functional requirements (e.g., Statement of Work [SOW] requirements for analyses or documentation).		
Structural Design Principle	**Definition**: A statement which captures experience in defining system architectures and designs. **Purpose**: Guide and inform design and implementation decisions throughout the system life cycle. Highlight different cyber resiliency techniques and implementation approaches. **Application**: Included, cited, or restated in system non-functional requirements (e.g., Statement of Work [SOW] requirements for analyses or documentation); used in systems engineering to guide the use of techniques, implementation approaches, technologies, and practices.		
Technique	**Definition**: A set or class of technologies, processes, or practices providing capabilities to achieve one or more cyber resiliency objectives. **Purpose**: Characterize technologies, practices, products, controls, or requirements, so that their contribution to cyber resiliency can be understood. **Application**: Used in engineering analysis to screen technologies, practices, products, controls, solutions, or requirements; used in the system by implementing or integrating technologies, practices, products, or solutions.		
Implementation Approach	**Definition**: A subset of the technologies and processes of a cyber resiliency technique, defined by how the capabilities are implemented. **Purpose**: Characterize technologies, practices, products, controls, or requirements so that their contribution to cyber resiliency and their potential effects on threat events can be understood. **Application**: Used in engineering analysis to screen technologies, practices, products, controls, solutions, or requirements; used in the system by implementing or integrating technologies, practices, products, or solutions.		
Solution	**Definition**: A combination of technologies, architectural decisions, systems engineering processes, and operational processes, procedures, or practices which solves a problem in the cyber resiliency domain. **Purpose**: Provide a sufficient level of cyber resiliency to meet stakeholder needs and to reduce risks to mission or business capabilities in the presence of advanced persistent threats. **Application**: Integrated into the system or its operational environment.		

2. 网络可恢复弹性（韧性）的工程实施

层次结构	定义、功能与应用说明
目标（Goal）	定义：从多个角度（即预测、抗击、恢复、适应）描述弹性需求 功能：把网络弹性作为系统整体需求 应用：用于描述高层要求
目的（Objective）	定义：从客户和开发人员两方面定义系统在全寿命周期以及作战环境中的任务可靠性和弹性安全需求，比目标层更具体、更面向威胁； 功能：使客户与开发人员对网络弹性达成共识，提出共同认可的度量标准 应用：用于量化评分或综合定性分析
子目的	定义：从不同角度对实施目的进行细化描述 功能：通过对实施目的逐层细化，分解为可定义性能指标的活动和能力 应用：用于量化评分或定性分析，可反映在系统功能需求中得
活动或能力需求	定义：描述可支持达成子目的的能力或活动 功能：帮助定义具体性能或效能指标，作为选择、定制或优先考虑的出发点 应用：用于量化评分或定性分析，反映系统功能需求
战略设计原则	定义：从多个角度（即预测、抗击、恢复、适应）描述弹性需求 功能：把网络弹性作为系统整体需求 应用：用于分析的非功能性需求描述
结构设计原则	定义：对系统架构及设计的描述和定义 功能：指导在系统全寿命周期中使用合适的技术和方法进行设计和实施 应用：用于指导系统工程实施的非功能性需求描述
技术	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程
实施方法	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程
解决方案	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程



2. 网络可恢复弹性（韧性）的工程实施

层次结构	定义、功能与应用说明		
目标（Goal）	定义：从多个角度（即预测、抗击、恢复、适应）描述弹性需求 功能：把网络弹性作为系统整体需求 应用：用于描述高层要求		
目的（Objective）	定义：从客户和开发人员两方面定义系统在全寿命周期以及作战环境中的任务可靠性和弹性安全需求，比目标层更具体、更面向威胁； 功能：使客户与开发人员对网络弹性达成共识，提出共同认可的度量标准 应用：用于量化评分或综合定性分析		
	子目的	定义：从不同角度对实施目的进行细化描述 功能：通过对实施目的逐层细化，分解为可定义性能指标的活动和能力 应用：用于量化评分或定性分析，可反映在系统功能需求中得	
		活动或能力需求	定义：描述可支持达成子目的的能力或活动 功能：帮助定义具体性能或效能指标，作为选择、定制或优先考虑的出发点 应用：用于量化评分或定性分析，反映系统功能需求
战略设计原则	定义：从多个角度（即预测、抗击、恢复、适应）描述弹性需求 功能：把网络弹性作为系统整体需求 应用：用于分析的非功能性需求描述		
结构设计原则	定义：对系统架构及设计的描述和定义 功能：指导在系统全寿命周期中使用合适的技术和方法进行设计和实施 应用：用于指导系统工程实施的非功能性需求描述		
技术	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程		
实施方法	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程		
解决方案	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程		

2. 网络可恢复弹性（韧性）的工程实施

层次结构	定义、功能与应用说明
目标（Goal）	定义：从多个角度（即预测、抗击、恢复、适应）描述弹性需求 功能：把网络弹性作为系统整体需求 应用：用于描述高层要求
目的（Objective）	定义：从客户和开发人员两方面定义系统在全寿命周期以及作战环境中的任务可靠性和弹性安全需求，比目标层更具体、更面向威胁； 功能：使客户与开发人员对网络弹性达成共识，提出共同认可的度量标准 应用：用于量化评分或综合定性分析
子目的	定义：从不同角度对实施目的进行细化描述 功能：通过对实施目的逐层细化，分解为可定义性能指标的活动和能力 应用：用于量化评分或定性分析，可反映在系统功能需求中得
活动或能力需求	定义：描述可支持达成子目的的能力或活动 功能：帮助定义具体性能或效能指标，作为选择、定制或优先考虑的出发点 应用：用于量化评分或定性分析，反映系统功能需求
战略设计原则	定义：从多个角度（即预测、抗击、恢复、适应）描述弹性需求 功能：把网络弹性作为系统整体需求 应用：用于分析的非功能性需求描述
结构设计原则	定义：对系统架构及设计的描述和定义 功能：指导在系统全寿命周期中使用合适的技术和方法进行设计和实施 应用：用于指导系统工程实施的非功能性需求描述
技术	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程
实施方法	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程
解决方案	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程

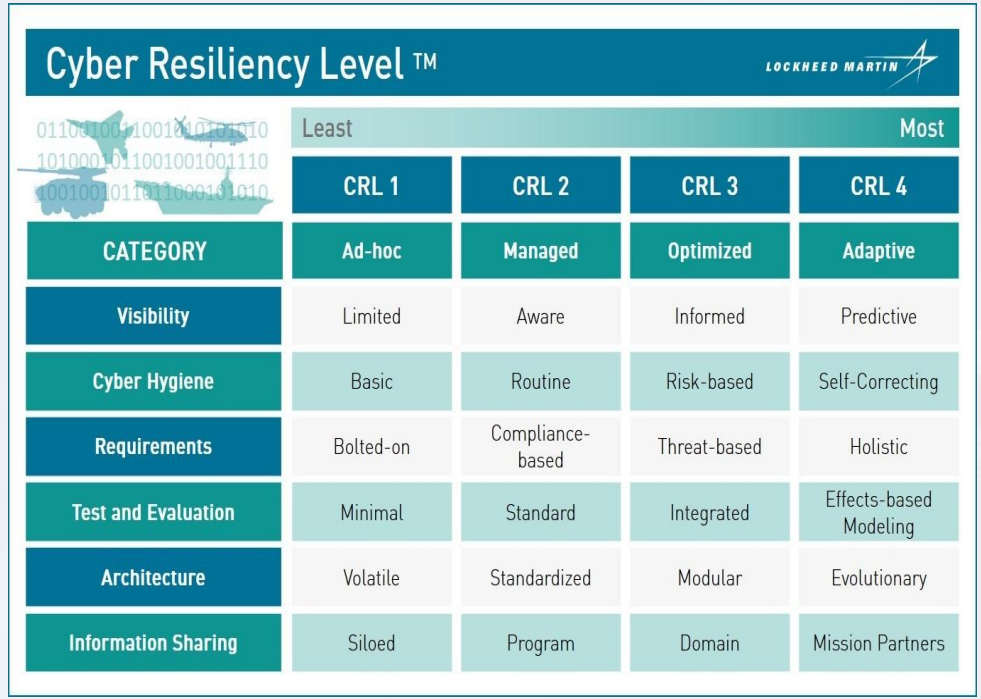
目的	说明
预防或规避	预期将会受到攻击，或攻击条件将会具备
预备	针对预测或预期的攻击，设计并保持可行的应用方案
持续	在攻击解除之前尽可能保持任务或业务功能持续
隔离	限制攻击影响范围
恢复	尽可能恢复任务或业务功能
认识	对于可能受到攻击影响的资源，尽可能保持其业务/业务依赖关系的了解
改变	修改任务或业务功能及支撑流程，对攻击进行处置，有效地解决任务/业务环境变化带来的问题
架构调整	对架构进行调整，以适应攻击造成的环境改变

2. 网络可恢复弹性（韧性）的工程实施

层次结构	定义、功能与应用说明
目标（Goal）	定义：从多个角度（即预测、抗击、恢复、适应）描述弹性需求 功能：把网络弹性作为系统整体需求 应用：用于描述高层要求
目的（Objective）	定义：从客户和开发人员两方面定义系统在全寿命周期以及作战环境中的任务可靠性和弹性安全需求，比目标层更具体、更面向威胁； 功能：使客户与开发人员对网络弹性达成共识，提出共同认可的度量标准 应用：用于量化评分或综合定性分析
子目的	定义：从不同角度对实施目的进行细化描述 功能：通过对实施目的逐层细化，分解为可定义性能指标的活动和能力 应用：用于量化评分或定性分析，可反映在系统功能需求中得
活动或能力需求	定义：描述可支持达成子目的的能力或活动 功能：帮助定义具体性能或效能指标，作为选择、定制或优先考虑的出发点 应用：用于量化评分或定性分析，反映系统功能需求
战略设计原则	定义：从多个角度（即预测、抗击、恢复、适应）描述弹性需求 功能：把网络弹性作为系统整体需求 应用：用于分析的非功能性需求描述
结构设计原则	定义：对系统架构及设计的描述和定义 功能：指导在系统全寿命周期中使用合适的技术和方法进行设计和实施 应用：用于指导系统工程实施的非功能性需求描述
技术	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程
实施方法	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程
解决方案	定义：实现一个或多个网络弹性目标的技术、流程或操作规程 功能：描述具体技术、流程、操作规程对实现弹性的作用 应用：用于工程分析，选择应使用的技术、流程或操作规程

3. 网络可恢复弹性（韧性）度量

- 洛克希德-马丁公司提出的网络弹性水平度量框架，2019年9月公开，可能成为工业标准。



寒夜速记

威胁框架：认知与实践

03 网络安全成熟度认证模型

什么是网络安全成熟度模型认证

- 网络安全成熟度模型认证（CMMC）是美国国防部（DoD）为正确保护其国防工业基地（DIB）而创建的一个网络安全评估模型和认证计划。该标准将成为国防部对外部项目承包商约束的统一安全标准。

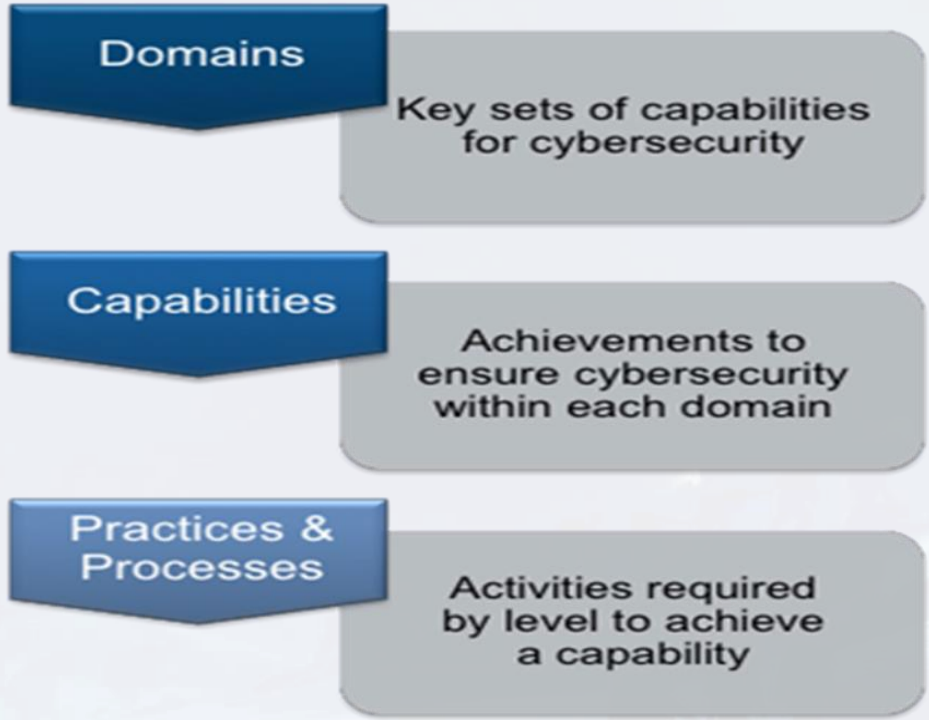
什么是网络安全成熟度认证

- 背景：美国防部通过评估认为：绝大多数承包商尚未在其信息系统中实施NIST 800-171，均未达到DFARS 7012的要求，还有更多政府承包商不具备满足法规要求的知识或措施
- 现有采购标准：成本、进度、性能、安全性

CMMC框架（一）

- CMMC框架由“域”，“能力”和“规程和流程”组成，目前共有17个域。

- CMMC的核心内容条款来源于NIST 800-171，并参考了ISO 27001，NIST 800-53，RMF,FIPS 140-2，CMMI,SANS,FedRAMP等



CMMC 框架（二）

Access Control	Indentification and Authentication	Recovery	Awareness and Training
Asset Management	Incident Response	Risk Assessment	Personnel Security
Audit and Accountability	Maintenance	Security Assessment	System and Communications Protection
Configuration Management	Media Protection	Situational Awareness	System and Information Integrity
Physical Protection			

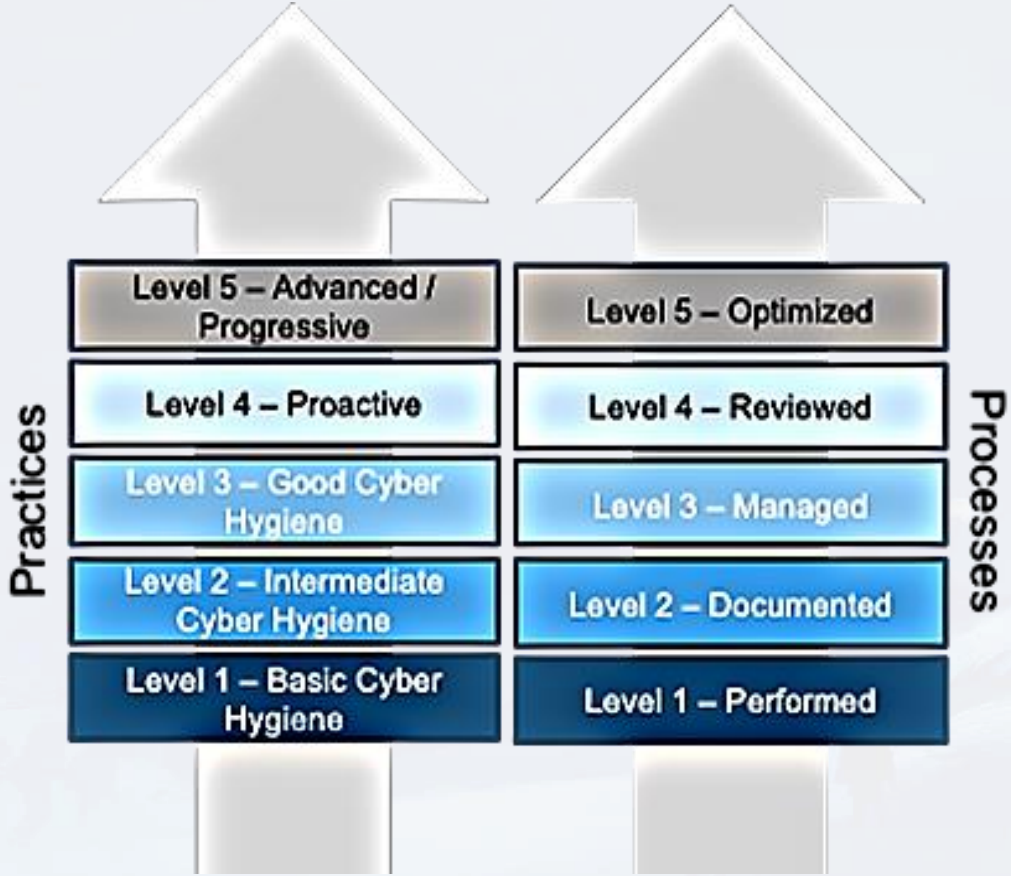
域

Table 2. List of Capabilities for Each Domain

Domain	Capability
Access Control	Establish system access requirements
	Control internal system access
	Control remote system access
	Limit data access to authorized users and processes
Asset Management	Identify and document assets
	Manage asset inventory
Audit and Accountability	Define audit requirements
	Perform auditing
	Identify and protect audit information

规程与流程（一）

- CMMC 定义五个级别，每个级别规定了相对应的规程与流程
- 获取某个级别资质，必须满足该级别及其以下级别规程和流程的所有要求



规程与流程（二）

Table 1. Summary of CMMC Levels

	Level 1	Level 2	Level 3	Level 4	Level 5
Technical Practices	Demonstrate basic cyber hygiene, as defined by the Federal Acquisition Regulation (FAR)	Demonstrate intermediate cyber hygiene	Demonstrate good cyber hygiene and effective NIST SP 800-171 Rev 1 security requirements	Demonstrate a substantial and proactive cybersecurity program	Demonstra a proven ability to optimize capabilities an effort to repel advanced persistent threats
Process Maturity	N/A	Standard operating procedures, policies, and plans are established for all practices	Activities are reviewed for adherence to policy and procedures and adequately resourced	Activities are reviewed for effectiveness and management is informed of any issues	Activities a standardiz across all applicable organizatio units and identified improveme are shared

规程与流程（三）

Table 3. Processes for each CMMC Maturity Level (ML)

Process Maturity Level	Processes
ML 1: Performed	*There are no maturity processes assessed at ML 1. A Level 1 organizat performs Level 1 practices but does not exhibit process institutionalizat*
ML 2: Documented	1. Establish a policy that includes [DOMAIN NAME]. 2. Establish practices to implement the [DOMAIN NAME] policy. 3. Establish a plan that includes [DOMAIN NAME].
ML 3: Managed	1. Review [DOMAIN NAME] activities for adherence to policy and practices. 2. Provide adequate resources to meet the plan for [DOMAIN NAME] activities.
ML 4: Reviewed	1. Review and measure [DOMAIN NAME] activities for effectivene 2. Review the status and results of [DOMAIN NAME] activities with hi level management and resolve issues.
ML 5: Optimized	1. Standardize a documented approach for [DOMAIN NAME] across a applicable organizational units. 2. Share identified improvements to [DOMAIN NAME] activities acros the organization.

认证过程

- 在CMMC框架下，独立的第三方评估组织将审核承包商的网络安全合规性，并证明承包商的成熟度。

认证时间表

- 2019年11月，发布0.7版本
- 2020年1月，发布 CMMC 1.0版本
- 2020年6月，纳入 REQUEST FOR INFORMATION (RFI) 信息邀请书（咨询的要求，无约束）
- 2020年秋天，纳入 REQUEST FOR PROPOSAL (RFP) 建议邀请书（有约束）

寒夜速纪

威胁框架：认知与实践

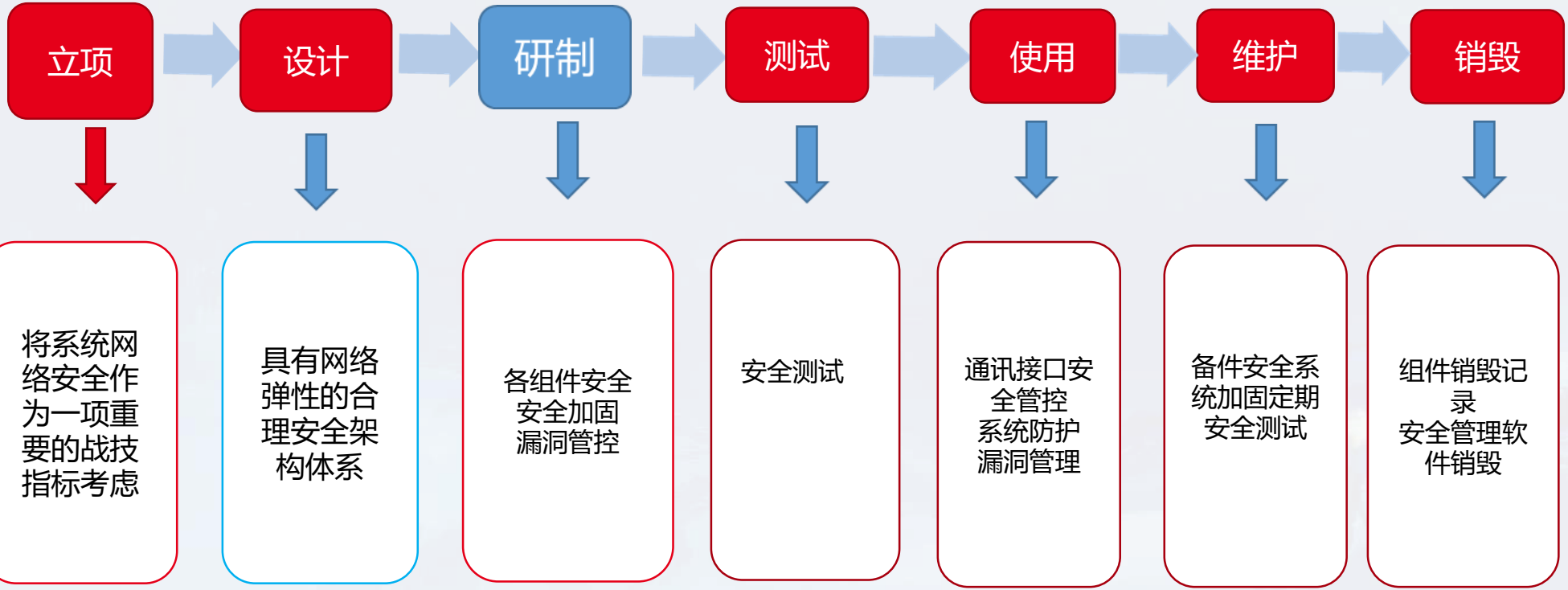
04 启示与思考

启示一：尽快制定具有我军特色的网络安全统一标准体系，确保武器系统和国防供应链安全

- 借鉴美方的经验，建立覆盖武器系统全生命周期的网络安全风险管标准
  - （1）现役装备的网络风险管理标准
  - （2）在研装备的网络弹性测试流程标准
  - （3）概念开发过程装备的网络可生存性设计与评估标准

- 近年来，安天组织强有力的工作团队，对美军网络可恢复弹性设计、RMF和CMMC 等框架模型进行了深入研究，形成了10余万字研究成果，同时结合安天多年来在国防供应链安全防护上积累的经验，研制了一批实用的安全防护产品，愿将所积累的成果与经验应用到我军网络安全统一标准体系制定中。

启示二：将网络安全和可恢复弹性（韧性）作为重要性能指标纳入各类武器系统研制



启示三：加大网络安全经费投入，实现武器系统风险管理转变

- 从合规管理到风险管理，管理方法从静态对照列表打勾转变为动态调整的控制和控制实施情况的持续监测。
- 从风险管理框架到弹性工程框架，工程方法从控制“可接受的被攻击风险”转变为控制“在被攻击情况下任务/业务功能受损的可接受风险”。

美国政府的集中的能力建设投入阶段

财政年	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
联邦政府FISMA花费	5.5	5.9	6.2	6.8	12.0	13.3	14.6	10.3	12.7	13.1	3.96	**5.1**
联邦政府IT 花费	66.2	68.2	72.8	76.1	80.7	76.0	75.0	73.2	75.6	80.4	90.3	**94.1**
FISMA 占 IT 总 花费比例(%)	**8.3**	**8.7**	**8.5**	**8.9**	**14.9**	**17.5**	**19.5**	**13.8**	**16.7**	**16.2**	**4.4**	**5.95**

200 200

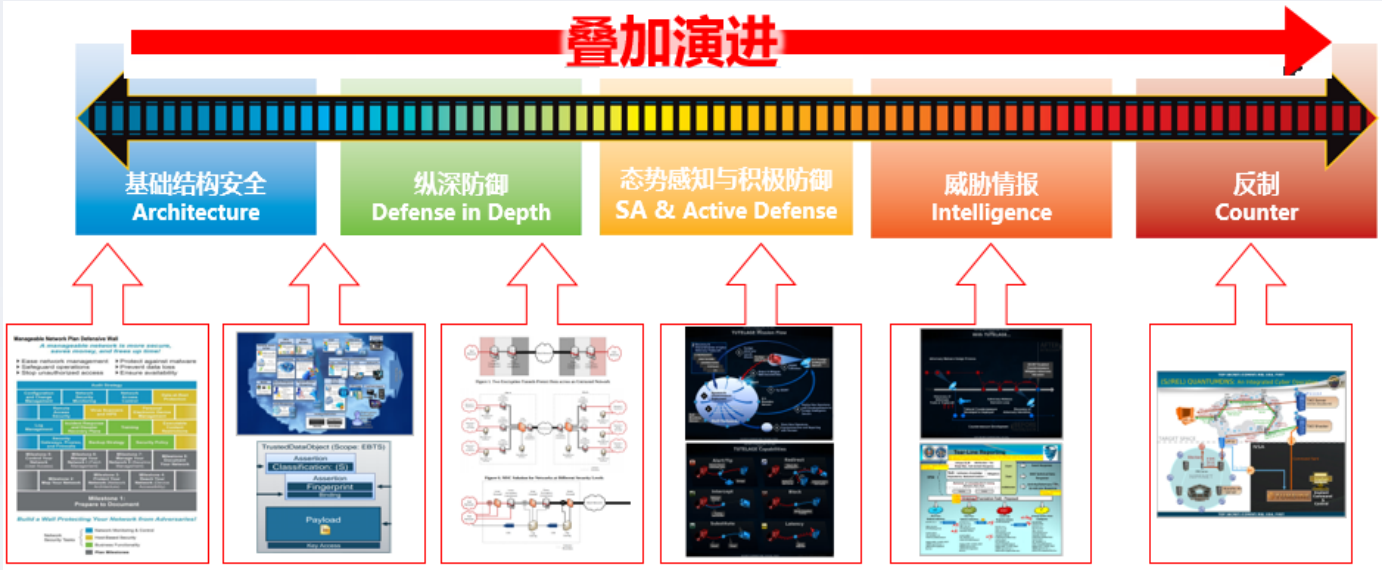
2002年，美国推出了《联邦信息安全管理法案》即FISMA，充分认识网络安全对于美国经济和国家安全利益重要性的基础上，要求各联邦机构指定并实施适用于本机构的信息安全计划，保障联邦信息和信息系统安全

小布什执政阶段（2001-2009）

奥巴马执政阶段（2009-2017）

启示四：发挥能力型网安厂商优势，赋能客户建立有效防御体系

- 充分发挥能力型网安厂商的技术优势，深度研究当前高级网空威胁行为体，协助相关机构建立“敌情想定”，在充分消化美方相关成果的基础上，基于叠加演进模型构建动态综合网络安全防御体系，推动安全产品落地，实现对武器系统安全的有效防御。



叠加演进是安天从能力型安全厂商的公共安全模型滑动标尺演绎发展的一套模型，滑动标尺模型由SANS提出，由安天翻译引入国内。

Rule #1: They are going to get in.
敌方终将进入我方内网

Rule #2: Network defenders cannot change rule #1.
网络防御者不能改变规则#1

Rule #3: They are already in.
敌方已经进入我方内网

Rule #4: Attacks will continue.
攻击将会持续进行

Rule #5: It's going to get worse.
情况会越来越糟

美IAD的“敌情想定”

谢谢大家