网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

乱雲飛渡

资源代价与安全算力

国外国防供应链安全现状及应对举措

安天 | 研究院

CONTENTS

目 录

01 供应链安全与国家安全

美方对破坏朝鲜战略武器计划的筹划

- 布什政府认识到美国可以渗入朝鲜核计划，接着布什总统对朝鲜导弹供应链开展了深入调查。
- 奥巴马政府认为：在核威慑失败时可将对朝导弹供应链的攻击作为渗入朝导计划的一种选项。

美方对破坏朝鲜战略武器计划的筹划（续）

朝鲜导弹残片

美方通过朝鲜光明星-3的导弹残片，分析，发现其绝大多数元器件均来自美国、英国和韩国。还发现光明星-3上使用其他来源的电子元器件（如照相机电磁干扰过滤器和压力传送器），这些情况说明，朝鲜导弹计划可通过对供应链进行攻击而渗入。

02 国防供应链的安全风险

软硬件供应链安全相关的攻击案例

网络安全影响传统安全的典型案例 — SolarWinds 事件

- 2020年12月13日，《华盛顿邮报》报道，美国知名IT公司SolarWinds旗下的Orion网络监控软件更新服务器遭黑客入侵并植入恶意代码，本次供应链攻击事件，波及范围极广，包括政府部门，关键基础设施以及多家全球500强企业。
- 供应链攻击，已经成为APT攻击中的常用攻击手段，该攻击方法攻击隐蔽，检测困难，且危害极大。

SolarWinds客户群（部分）

SUNBURST后门的指令功能

指令	功能
Idle	无动作
Exit	退出当前线程
SetTime	设置延迟时间
CollectSystemDescription	收集系统信息，包括主机名，用户名，操作系统版本，MAC地址，IP地址，DHCP配置和域等。
UploadSystemDescription	发送收集到的系统信息。
RunTask	运行程序、创建进程。
GetProcessByDescription	获取进程信息，无参数则仅返回PID和进程名。
KillTask	终止指定PID的进程。
GetFileSystemEntries	获取系统文件和目录。
WriteFile	将解码下发的Base64编码数据写入指定文件。
FileExists	测试指定文件是否已存在。
DeleteFile	删除指定文件。
GetFileHash	获取指定文件的MD5值。
ReadRegistryValue	读取指定注册表位置。
SetRegistryValue	写入指定注册表位置。
DeleteRegistryValue	删除指定注册表位置。
GetRegistrySubKeyAndValueNames	获取指定注册表路径下的子项和值。
Reboot	重启系统

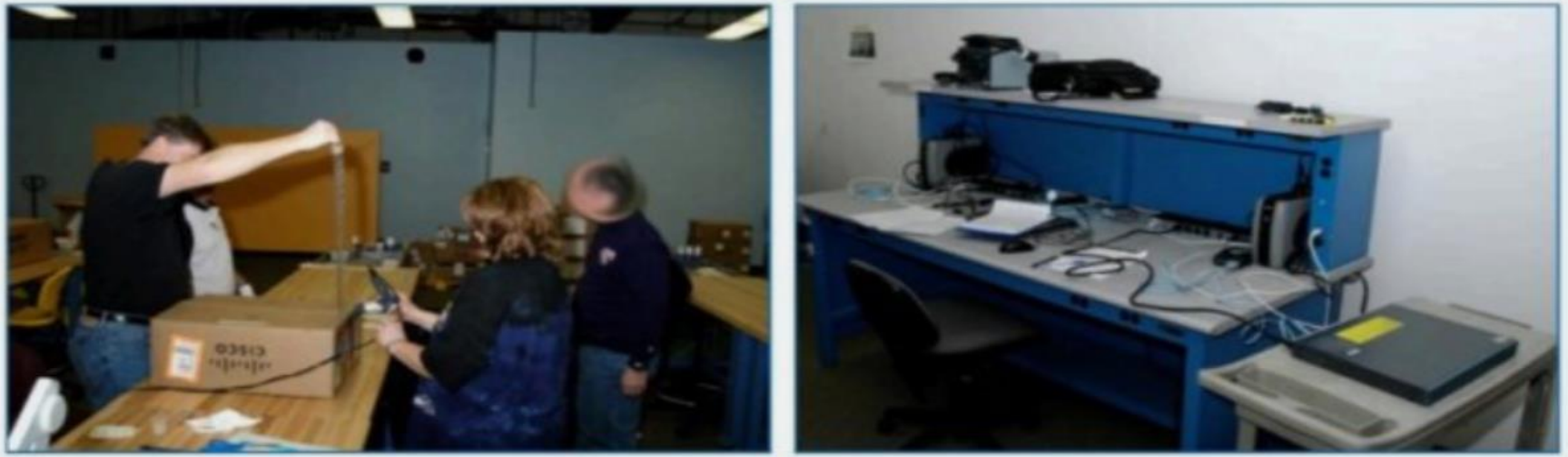
引自安天分析报告《SolarWinds旗下软件被用于供应链攻击事件分析》

CIA控制瑞士公司，长期窃听120国机密

2020年2月疫情严重期间，《华盛顿邮报》报道称，CIA自二战后长期控制瑞士密码机公司Crypto AG，在其产品中植入漏洞，借此窃听全球120多个国家的最高机密。

针对资产（设备）的预制作业

左图为 4 名NSA工作人员打开拟交付的思科产品包装
右图为预制后门器件操作台



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

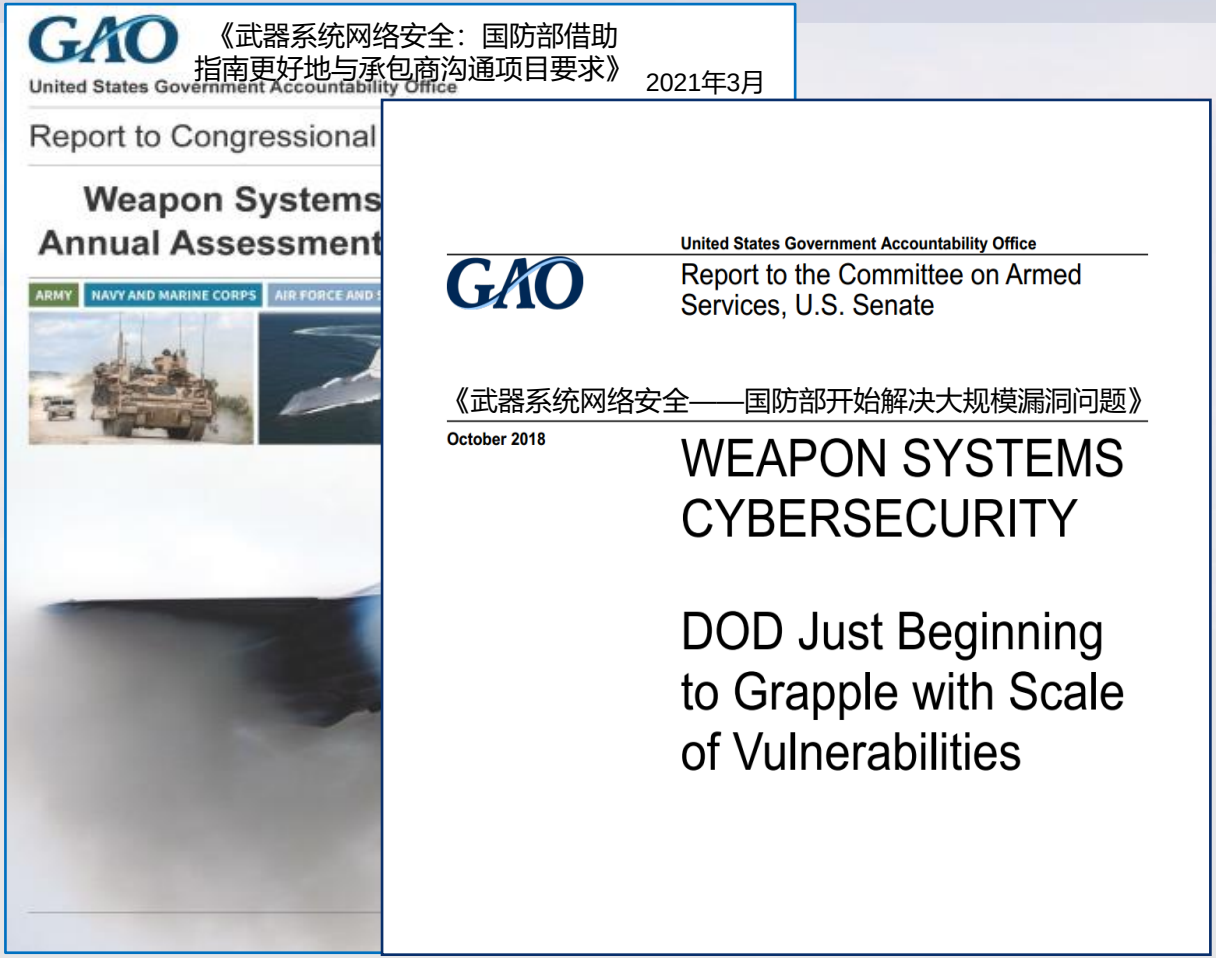
03 美方武器系统供应链安全认知

美方武器系统网空安全风险分析及其改善安全现状的重要举措

美方在网络安全中曾出现的问题

- 26美元的软件被用来破坏伊拉克战场上的关键武器（怀疑伊朗支持）
  - Skygrabber软件，截获未加密通信链路上的实时视频
- 计算机病毒攻击美军无人机系统
  - “捕食者”和“死神”无人机系统感染病毒，秘密任务系统被安装键盘记录器，对加密和未加密系统进行攻击，利用GPS欺骗漏洞
- 黑客攻击了联邦航空管理局（FAA）空中交通网络
  - 空中交通控制系统被入侵，口令被盗，安装恶意软件，给飞行员发虚假消息，发出求救信号等。

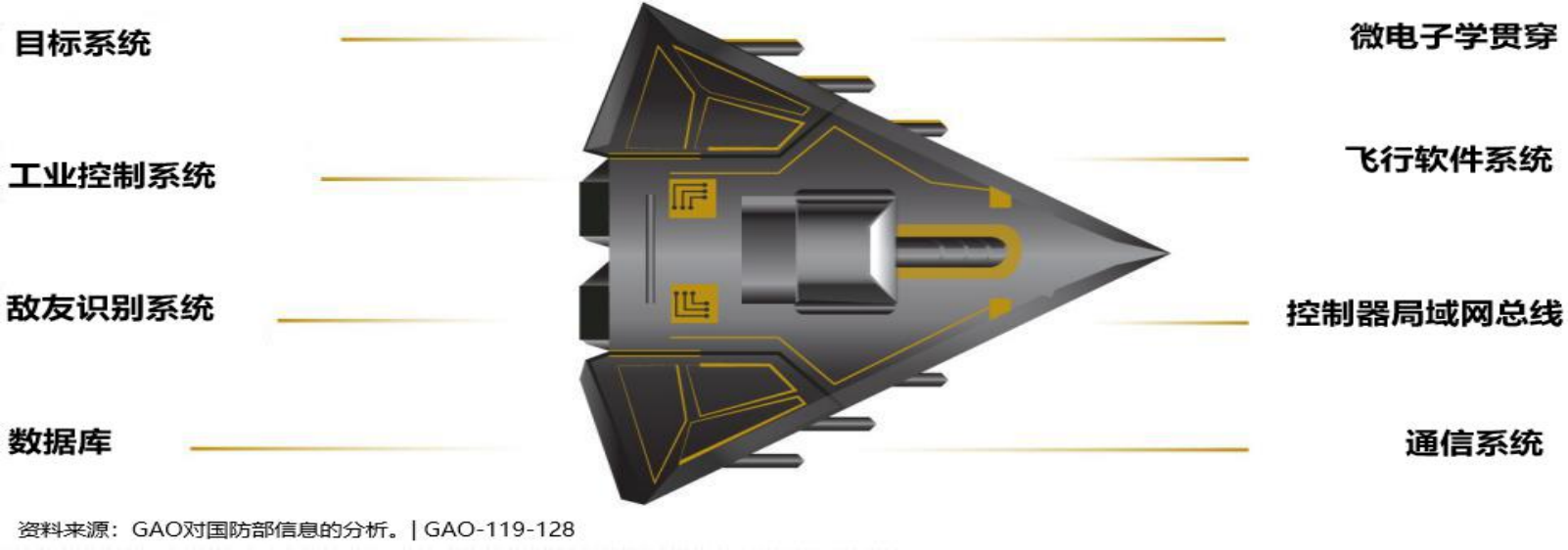
美方如何认识自己的武器系统网络安全



- **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。**
- 相比于2018年10月GAO发布的研究报告而言，2021年的报告提出的措施建议更加聚焦，其核心观点是：**要降低武器装备网络安全风险，必须在开发需求和合同阶段明确网络安全要求。**

美方如何认识自己的武器系统网络安全

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。

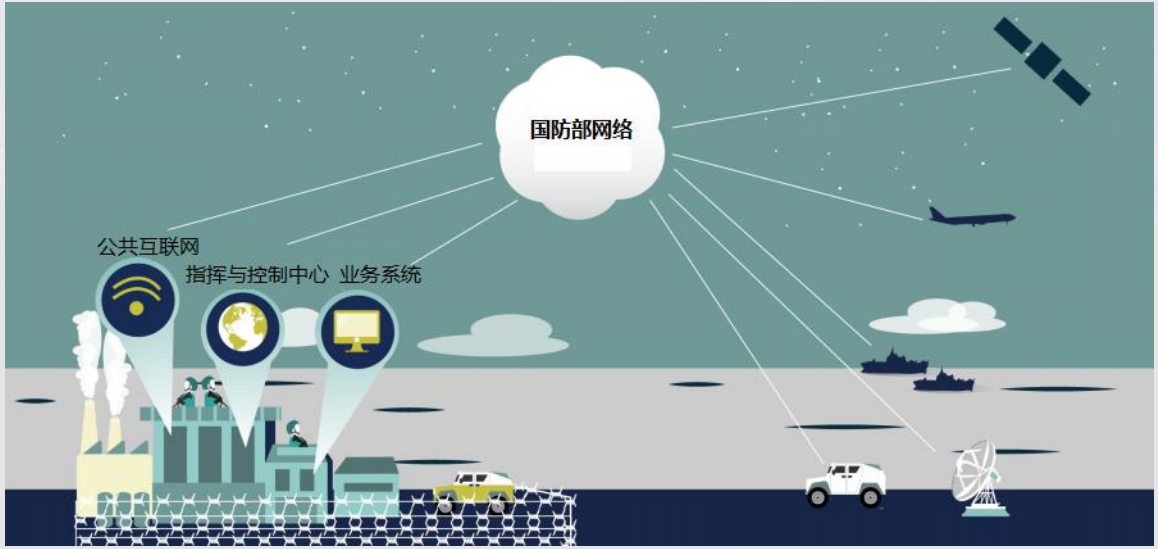


嵌入式软件和信息技术系统在武器系统中普遍存在

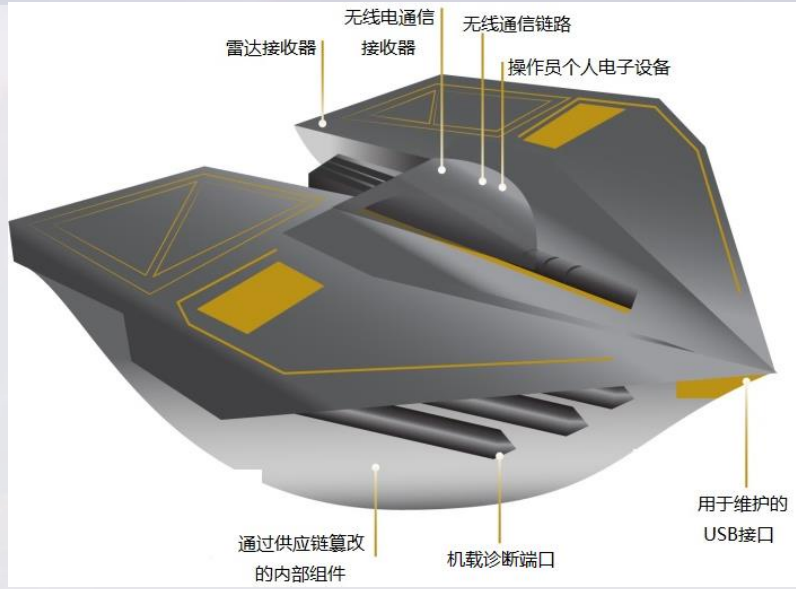
美方所关注的武器系统网络安全的挑战因素

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**；比以往更加**依赖商业软件和IT**实现预期的性能；**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。



武器系统连接到到许多其他系统的网络，间接连接到公共互联网



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）

美DOD武器系统连接到国防部信息网络，同时也会连接到外部网络，**例如国防承包商的网络。**此外，一些武器系统可能不直接连接到网络，而是连接到其他系统（如电气系统），**从而被间接地连接到公共互联网。**

美方认为提高武器系统网络安全面临的挑战

面临的挑战

目前，国防部仍在学习如何更好地解决武器系统网络安全问题，为了改善武器系统网络安全状况，面临以下挑战：

- 由于武器系统可能是**非常庞大、非常复杂的系统**，具有相互**依赖性**，因此**更新系统的一个组件可能会影响其他组件。**
- 国防部面临信息共享的障碍，主要体现在信息共享的障碍和网络安全人才挑战两方面。这严重阻碍了国防部在程序内和程序之间共享漏洞和威胁信息的能力。

共享有关网空漏洞和威胁信息的挑战

挑战	示例
对连接系统的有限洞察力	来自具有高度关联武器系统的计划的官员表示，他们的系统只有最薄弱的环节才能安全，但他们没有关于由于分类而连接到的系统的漏洞的信息。
获取攻击细节的问题	如果武器系统遭受网空攻击，由于该信息的分类类型，国防部计划官员将不会从情报界提供该攻击的具体细节。
无法利用跨程序的信息	负责评估武器系统网络漏洞并制定降低风险战略的国防部长官员办公室不允许与其他计划分享他们对特定漏洞的了解。
不知情的运营商	包括维护者在内的一些系统操作员没有访问威胁或漏洞信息的许可。
部署时无法获取机密信息	一些海军舰艇没有接收或存储高度机密信息的设施。

美方对正在开发的武器系统的脆弱性判断

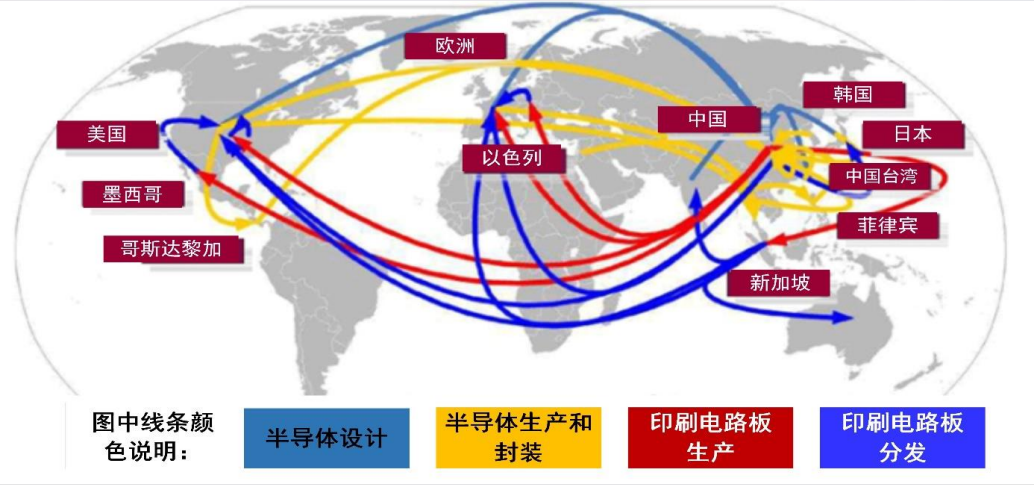
测试显示：正在开发的大多数武器系统存在严重漏洞，且漏洞全部范围还处在未知状态。

- 从2012年到2017年，国防部测试人员在几乎所有正在开发的武器系统中发现关键任务的网络漏洞。测试人员使用相对简单的工具和技术，就能够控制这些系统并且规避被检出。
- 由于测试时间短、信息保密、测试的范围和复杂程度有限等多种原因，网络安全评估并未反映出武器系统在运行中可能面临的各种威胁。

由于网络安全测试的限制，国防部发现的漏洞数量可能远远少于实际漏洞数量

美方武器系统供应链安全现状—暴露的攻击面

- 2017年2月，美国国防科技委员会（DSB）发布报告《网络空间供应链安全》；
- 美国防部供应链的供应商包括多个工业领域的企业，各个企业间也彼此互销产品，根本无法保证各个流程中薄弱环节不被利用。



F-35某部件安装之前经15级中间供应商

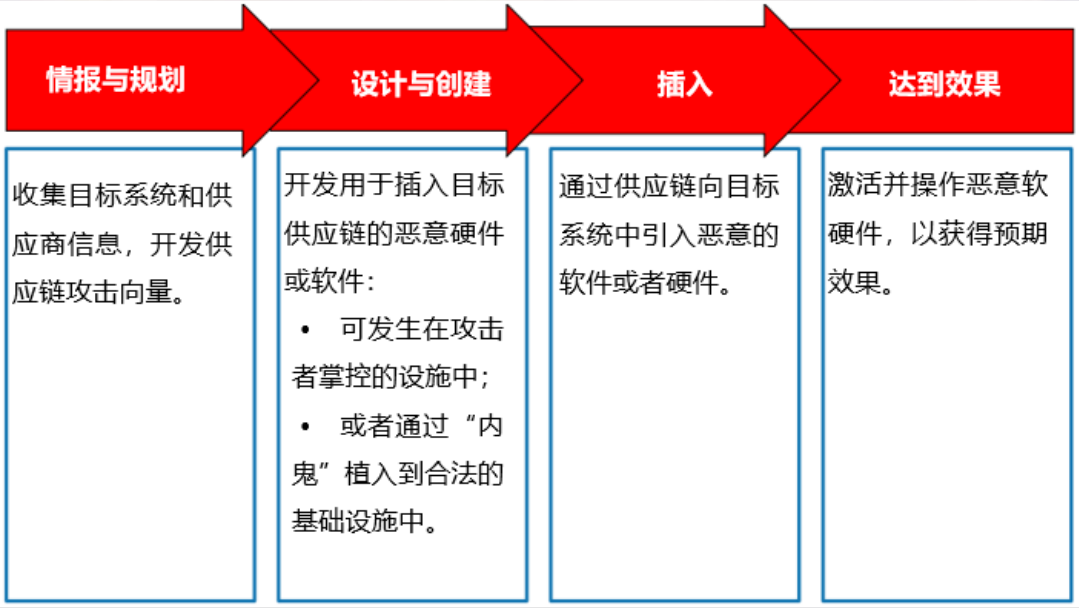
三大供应链攻击难易度和精准度对比

供应链类别	全球商业供应链	国防采办供应链	国防维持供应链
含 义	以商用现货采购为主，是大多数元器件采购来源，也是采购供应链和维护供应链的基础。	由主承包商主导，用于支持武器系统的开发和生产。	由国防部武器装备维护部门或装备集成商设计和主导，主要采购装备维修用电子元器件。
供应链介入难度	容易	供应商数量众多，介入难度中等。	对供应商有一定的审查要求，介入相对困难。
攻击精准度	因国防部需求只占全球总市场极小份额，攻击精准度最低。	一旦介入，可知晓元器件在整个系统中的作用，提供攻击精确度。	可明确知道精准位置，攻击精准度最高。

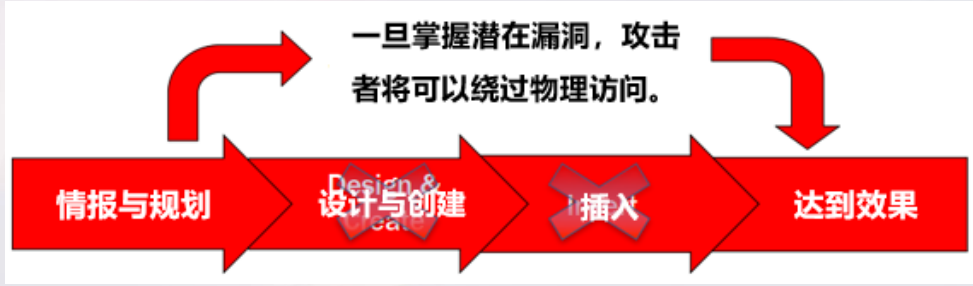
- 三个不同的供应链呈现广泛的攻击面
  - 全球商业供应链：最容易被恶意入侵；
  - 国防采办供应链：恶意入侵表较容易介入；
  - 国防维持供应链：对复杂高级对手最具吸引力。

美方武器系统供应链安全现状—攻击类型

- 供应链攻击主要基于两种类型：
  - 通过多步骤执行恶意插入
  - 利用现存潜在漏洞



恶意插入过程



攻击者利用潜在漏洞绕过恶意插入过程

《网络空间供应链安全》研究报告指出

- 武器系统整个生命周期中都可能存在漏洞；
- 目前已部署的武器系统中，元器件很可能存在漏洞，将成为攻击目标；
- 到2025年，部署的这类有缺陷系统所具备的功能将占全部军事能力的80%。

美方改善武器系统安全现状努力方向

- **理解供应链风险**：扩展漏洞评估，各军种主管与军队采购执行官每年至少举行一次“网络觉醒”演习，及时训练采购、作战和支持人员的相关能力。
- **减轻潜在脆弱性**：改进检测和报告能力，USD（AT＆L）指导DASD（研究部）和国防高级研究计划局（DARPA）建立技术方法来识别软件和固件中的差异，以及针对恶意代码或其他硬件污点进行筛选。
- **改变采购方式**：加强项目保护计划、提高供应商审查及时性、改善系统工程、有效利用联合联邦保证中心（JFAC）和联合采购保护与开发部（JAPEC）两个机构的职能、考虑COTS产品和组件对网络安全的影响。
- **支持生命周期操作**：为指定部署系统开发维护程序的持续性保障计划、收集零部件漏洞并采取相应措施；制定并发布指南类文件，确保项目采购符合相关需求；针对关键部件供应链的可见性进行研究，并将相关信息纳入到国防部应用程序数据库。
- **寻求技术解决方案**：与先进制造商建立合作关系；国防高级研究计划局（DARPA）和情报高级研究计划局（IARPA）持续投资研发分离式制造解决方案；制定并发布指南类文件，确保设计工具链的完整性和安全性；要求特定部门向国防部提供可信赖的元器件。

美方提高武器系统网络安全采取的措施—政策/战略

DoD Policy and Strategy （美国国防部策略与战略）

Oct '10: Establishment and standup of U.S. Cyber Command

Feb '13: PPD-21, security and resilience of critical infrastructure against cyber threats

August 14: Directed Cybersecurity in OT&E

J. Michael Gilmore, Director, OT&E

2015: Multiple proposed bills to address information sharing between gov't and private sector

提倡军民融合，信息共享，加强武器系统网络安全。

2017: DoD 5000.02 Encl 14, Cyber security in the Defense Acq Sys

强调确保武器系统采购生命周期安全

2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017

Jul '11: Memo outlining Program Protection Plan (PPP) for Cyber hardening of DoD Systems

Frank Kendall
Deputy Under Secretary for AT&L

Gen. Alexander, Commander USCYBERCOM

Mar '13: Public acknowledgement of Cyber warfare "teams" ready by 2015

Apr '15: DoD strategy expands network defense beyond their own systems and addresses synchronization of Cyber operations with kinetic effects

扩大网络防御范围，除保护网络系统外，同步加强武器系统的网络安全。

2016: NDAA 16 Section 1647 Evaluation of Cyber Vulnerabilities

强调严格执行武器系统网络漏洞评估程序。

"*加强武器系统网络安全*：国防部将根据作战需要评估并启动当前和未来武器系统的网络安全。对于将获得或采购的所有未来武器系统，国防部将要求满足特定的武器系统网络安全标准。"

《美国国防部网络战略》2015年4月

策略在发展，采购需求需要包含策略需求。

国防部加强网络系统安全相关策略时间线

美国加强国防供应链安全政策

美近年发布/更新的关于国防供应链安全的相关政策

名称	发布/更新时间	相关内容
DoDI 5200.44 保护任务关键功能达成可信系统与网络	2018年 (更新)	国防部可信系统与网络战略的实施，在关键系统的全寿命周期对任务关键功能和部件进行风险管理。主要方法包括供应链风险管理、软件可靠性、安全设计模式等。
NDAA FY2020第645条	2019	要求国防部长为国防工业基础制定流畅的数字化国防供应链风险管理办法。
DFARS(252.204-7012) 保护相关国防信息和网络事件报告	2019	对国防承包商处理国防受控非密信息（CUI）提出具体要求。
NIST SP 800-171 保护非联邦信息系统中的受控非密信息	2019年 (更新)	对受控非密信息处理、存储或传输，以及为这些功能的实现提供安全保护的非联邦系统和机构（国防供应商包含在内）提出安全要求，保护受控非密信息的机密性。
NIST SP 800-171A 受控非密信息的安全要求评估		与SP 800-171配套，提供对受控非密信息保护方法和流程的评估程序和方法。
NIST SP 800-161 联邦信息系统和组织的供应链风险管理实践		为联邦机构提供各级组织（包括国防部），对信息通信系统的供应链风险进行识别、评估和缓解的实践指南。
供应链安全战略	2019	提出以“供应链安全”代替“供应链风险管理”的要求，以及具体实施框架、规则、手段和方法。
网络安全成熟度模型认证(CMMC V 1.0)	2020	按网络安全流程和实践两个维度，评估DIB企业网络安全成熟度等级的标准框架。
DFARS(252.204-7021) 网络安全成熟度模型认证(CMMC)要求	2020	自2020年11月30日起，对DIB企业进行CMMC分级评估分级，并把CMMC等级作为授予国防订单条件。
DoDI 5000.02 自适应采办框架实施	2020 (更新)	要求对国防采办项目运用系统安全工程方法，制定项目保护计划，对关键项目信息、任务关键功能及信息的安全风险进行管理。
DoDI 5000.83 技术和项目保护	2020	国防部采办项目系统安全和网络安全技术风险管理政策、职能和流程。
DoDI 5000.89 测试与评估	2020	各采办途径下的测试与评估政策、职能和流程。
DoDI 5000.90 采办决策机构与项目经理的网络安全	2020	确立国防部采办流程中决策机构和项目经理对网络安全风险进行管理的管理政策、职能和流程。
EO 14017 美国供应链	2021	要求对关键产品和行业的供应链风险进行 “全球供应链调查” ；要求对现有国防（和其他）工业基础进行重新评估，并建立每四年一次的供应链审查机制。
《国家安全战略临时指南》	2021	再次明确提出重建关键物资供应链，包括与盟友及伙伴一起建设和保护可信关键供应链和技术基础设施。

美方提高武器系统网络安全采取的措施—组织

军事部门建立了**以网络安全为中心的武器系统办公室**，以改善武器系统的网络安全状况。

军事服务计划专注于武器系统网络安全

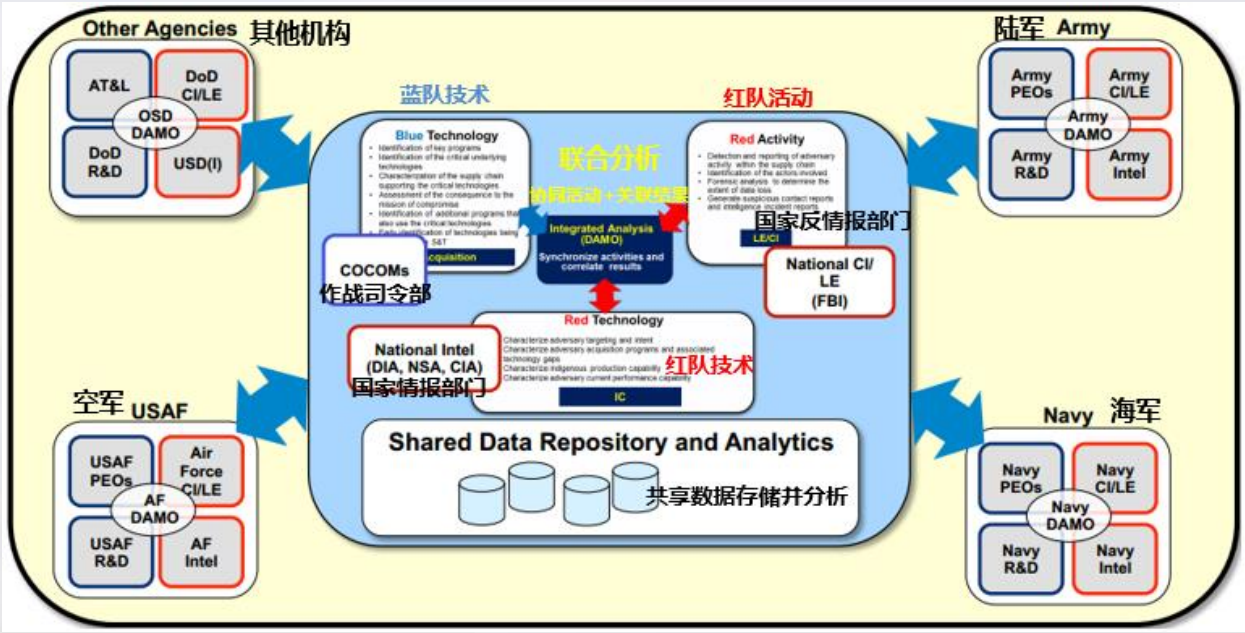
军种	组织机构及成立年份	任务
海军	CYBERSAFE软件（2015年）	帮助确保关键作战信息技术和系统组件及的生存能力和弹性恢复能力。为系统和组件提供增强的保证要求。
空军	武器系统网络弹性恢复能力办公室（2017年）	将网空弹性限制在空军文化中，以便在不利条件下保持任务有效能力。重点关注任务级网络风险分析，将网络整合到系统工程中，培养精通网络安全的员工队伍，并加强网络情报整合。
陆军	网络加强专责（2017年）	在全军范围内进行深入调查，以评估服务的网空需求、优势、劣势和资产。有了这些信息，他们计划制定一个整体方法来解决武器系统和工业控制系统的网空安全问题。

美提高武器系统网络安全采取的措施—新设机构

联合联邦保证中心（JFAC）

- 目标：2015年2月成立，运行并制度化安全保障能力；
- 国防部各部门组成的一个联合机构，通过来自军事部门、国防机构和其他国防部组织的内部协调组织和设施联合，开发、维护并提供软硬件漏洞检测、分析和补救能力。

JFAC成员分布



JAPEC协作成员部门

联合采购保护与开发部门（JAPEC）

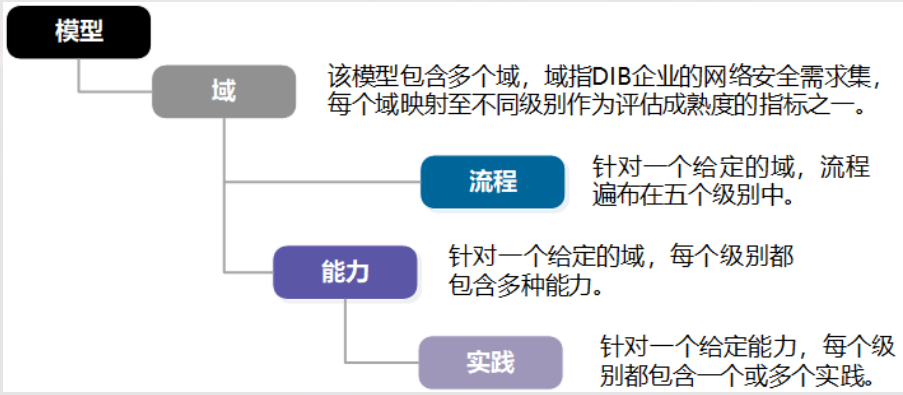
- 2016年成立，旨在形成一种联合分析力量，用于评估技术信息损失并确定所造成的影响，进而指导采购需求及战略方针制定；
- 使命：减少国防部企业的受控技术信息（CTI）风险，开发相关方案以阻止、拒绝和破坏可能威胁美国军事优势的对手。

美提高武器系统网络安全采取的措施—项目/计划

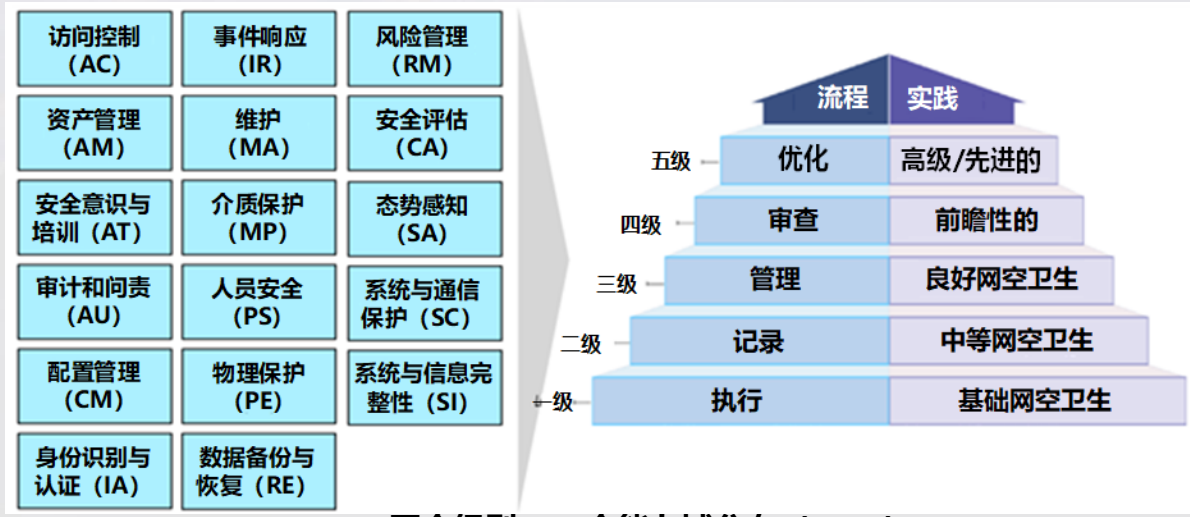
网络安全成熟度模型认证（CMMC V 1.0）

- 评估公司网络安全成熟度的模型，旨在让经认可的第三方评估所有与美国国防部有业务往来的公司，并依据模型成熟度级别，确定企业网空安全成熟度水平。
- CMMC框架由域、能力、规程和流程组成，目前共有17个域。
- CMMC模型共分为五个级别：包含17个领域和43种功能，跨5个级别的5个流程来衡量流程成熟度；以及171个跨级别的规程来衡量技术能力。

级别	描述	流程
1 级	执行	成熟度 1 级中不设置成熟度评估流程。组织执行一级实践，但不强制流程制度化。
2 级	记录	创建包含域名（DOMAIN NAME）的策略 记录 CMMC 实践以实施域名（DOMAIN NAME）策略
3 级	管理	制定、维护域名（DOMAIN NAME）计划，并给与资源支撑。
4 级	审查	审查并衡量域名（DOMAIN NAME）活动的有效性
5 级	优化	标准化适用于组织中所有单元且记录下来的方法，并加以优化。

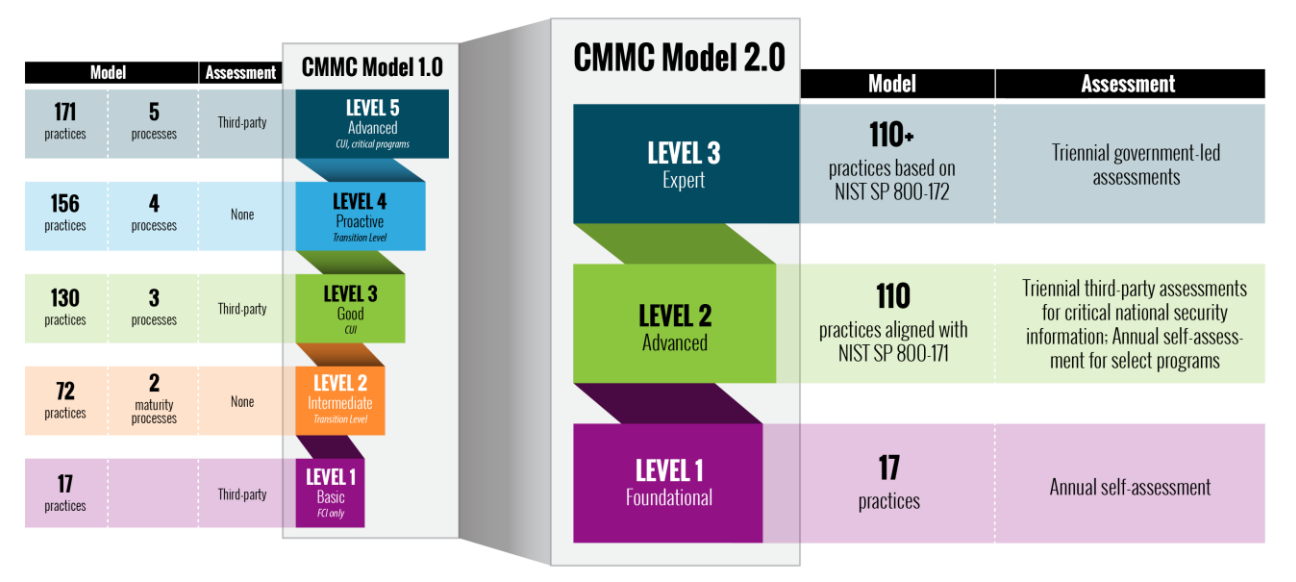


CMMC的域、能力、规程和流程（V 1.0）



五个级别、17个能力域分布（V 1.0）

美提高武器系统网络安全采取的措施—项目/计划（续）



CMMC 2.0 的主要特点

- 保护敏感信息以启用和保护作战人员
- 动态增强国防工业基础网络安全以应对不断变化的威胁
- 确保问责制，同时最大限度地减少遵守国防部要求的障碍
- 为灌输网络安全和网络弹性的协作文化做贡献
- 通过高专业和道德标准保持公众信任

网络安全成熟度模型认证（CMMC V 2.0）

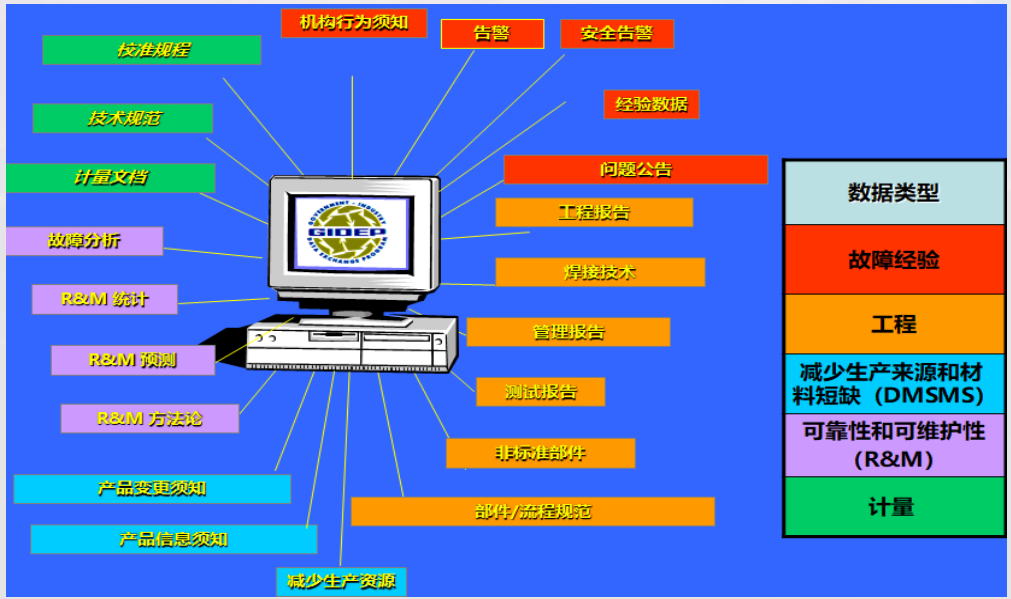
2021年11月，美国防部发布 CMMC 2.0版，更新相关计划和要求。将原来的五个级别简化为**基础（Foundational）、高级（Advanced）和专家级（Expert）**三个级别，以实现内部审查主要的目标：

CMMC 2.0 引入的关键变化

序号	变化	描述
1	流线型模型	• 专注于最关键的要求：将模型从 5 个合规级别简化为 3 个级别 • 符合广泛接受的标准：使用美国国家标准与技术研究院 (NIST) 网络安全标准
2	可靠的评估	• 降低评估成本：允许所有 1 级（基础）公司和部分 2 级（高级）公司通过自我评估证明合规性 • 更高的问责制：加强对第三方评估员专业和道德标准的监督
3	灵活的实施	• 合作精神：允许公司在某些有限的情况下制定行动计划和里程碑（POA&Ms）以获得认证 • 增加灵活性和速度：允许在某些有限情况下豁免 CMMC 要求

美提高武器系统网络安全采取的措施—项目/计划（续）

- **政企数据交换计划（GIDEP）**
  - 由美国和加拿大政府资助；
  - 国防部为促进政府机构和行业合作伙伴之间的技术信息共享而制定；
  - 提高系统的安全性、可靠性和就绪性，并降低系统开发、生产和所有权成本。



GIDEP计划数据库

- **项目保护计划（PPP）**：是一类单一来源的文档，用于指导协调和整合主要国防采购项目的所有保护工作。内容包括：确定项目的关键信息、任务关键功能和组件；项目面临的潜在威胁和脆弱性；应用对策以减轻相关风险的计划；并规划可出口性和外国参与项目的可能性。
- **国家工业安全计划（NISP）**：建立联邦政府和私营企业之间的一种合作伙伴关系，旨在保护机密信息。四大原则：实现安全规程的统一、在安全规程中执行互惠原则、消除重复或不必要的要求、降低安全成本。
- **网空供应链风险管理计划（C-SCRM）**：由NIST于2008年启动，旨在响应《国家网络安全综合计划》（CNCI）第11项提出的“制定多管齐下的方法，管理全球供应链风险”。
- **“网络觉醒”演习**：各军事部门该演习来测试供应链安全的脆弱性，评估系统的脆弱程度，并参考评估结果及时培训采购、作战和维护人员。

DARPA近年典型供应链安全相关技术项目

DARPA近年典型供应链安全相关技术项目（部分）

类别	名称	项目时间	项目概况
软件供应链	大型遗留软件的可验证安全与性能增强(V-SPELLS)	2021-2025	解决系统运维安全。利用形式化软件验证技术和增量式软件工程，打造软件验证与重构工具，为系统开发人员提供软件组件插拔式替换更新能力。
	自动化快速软件认证(ARCOS)	2020-2024	解决采购和部署过程安全，开发自动化、规模化的软件安全分析能力和工具。
	网络可靠系统工程（CASE）	2018-2022	解决系统开发阶段的安全。开发系统工程方法提高嵌入式系统的网络安全检查能力和工具
	商用计算系统检查 (VET)	2013-2017	解决采购和部署过程的安全。开发快速、规模化检测商业产品相关软件/固件中是否存在后门和恶意行为并修复的技术和工具。
硬件供应链	自动实现应用程序的结构化阵列硬件（SAHARA）	2021-2024	解决系统应用过程的安全,设计、开发和制造具有安全对策技术的专用集成电路（ASIC）处理器。
	安全芯片自动实现（AISS）	2019-2022	解决系统设计过程的安全,将可扩展防御机制整合到芯片设计中的过程。
	通过硬件和固件集成的系统安全(SSITH)	2017-2021	开发可嵌入到服务器、物联网设备和智能手机的专用集成电路。
	供应链硬件完整性电子防御（SHIELD	2015-2018	解决生产和应用和维护阶段的安全可信性。通过微型、低功耗传感器建立电子器件的可追溯可验证性。

其他国家加强国防供应链安全政策

其他国家近年来加强国防供应链安全政策

名称	组织/国家	发布/更新时间	相关内容
《综合物流施政推进计划 2017～2020年度》FY2017-FY2020 Comprehensive Physical Distribution Policy Outline	日本	2017	内容涉及：供应链协同，提高物流效率，如外包方与物流企业的合作、物流企业间协同运作；构建智能物流供应链、无缝连接与高附加值的供应链，通过采取标准技术、RFID、电子通关处理技术提升效率安全、可持续物流供应链。
《现代产业战略：构建适应未来的英国》Industrial Strategy: building a Britain fit for the future	英国	2017	2017年英国发布《现代产业战略：构建适应未来的英国》白皮书，布局英国脱欧的产业战略，拥抱技术变革和创新的机会，以保证英国在全球供应链中的优势。
《日本-欧盟经济伙伴关系协定》(EPA) EU-Japan Economic Partnership Agreement	欧盟、日本	2018	日本与欧盟签署了EPA，就全球供应链的发展达成共识：发展供应链风险管理技术，加强全球供应链的安全。
《德国国家区块链战略》Blockchain-Strategie der Bundesregierung	德国	2019	伴随区块链技术的不断成熟，2019年，《德国国家区块链战略》指出，德国将研究区块链技术如何促进供应链与价值链的透明度、效率、安全性。
《5G网络安全风险评估报告》EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks	欧盟	2019	国防部可信系统与网络战略的实施，在关键系统的全寿命周期对任务关键功能和部件进行风险管理。主要方法包括供应链风险管理、软件可靠性、安全设计模式等。
《5G网络安全工具箱》Cybersecurity of 5G Networks - EU Toolbox of Risk Mitigating Measures	欧盟	2020	不针对任何特定供应商或国家，而是力图加强针对网络运营商的安全要求，基于对供应商的风险评估而对所谓“高风险”供应商采取限制措施，呼吁推动欧盟层面的标准化进程，协调安全认证机制。
《战略指南针》Strategic Compass	欧盟	2021	提出投资于创新、减少战略依赖性和确保供应链安全的方法。新兴和颠覆性技术正在改变未来战场，对国防部门的影响越来越大，这些技术的开发是保持军事优势的关键。欧盟应充分利用现有的所有可用工具来推进这些能力并开发新项目。

04 总结

政策先行指导、专门机构推进、项目/计划实践

政策先行 — 立法保障 — 计划落地

针对当前存在的国防供应链安全风险，在新冠疫情的环境下，各国都纷纷调整供应链战略，并制定预案，呈现出以下特点：

- 高度重视国家供应链安全，制定并出台供应链战略，指导建立关系国家安全和国计民生关键产业供应链安全管理体系；
- 新增专门机构，负责相关工作推进，对供应链安全进行立法，从源头确保供应链安全；
- 高度重视国防军工、重点产业、高技术产业的供应链体系建设，积极推进提升供应链安全的项目和计划，确保安全、可持续的供应链体系，增强全球竞争优势。

谢谢大家

安天冬训营 wtc.antiy.cn