国防网络安全与数据治理研究

齐鹏云
中国人民公安大学法学院，北京 100038

摘要
健全和完善我国国防网络安全和数据治理架构，既是国家网络安全与数据治理的重要一环，也是在《数据安全法》框架下细分领域内的重要实践。运用比较分析和文献分析法，提炼美国2013—2022年《国防授权法》中国防网络安全与数据治理的逻辑特征，吸收美国国防网络安全与数据治理的成功经验，完善我国国防网络安全与数据治理的总体架构。总体国家安全观下的国防网络安全与数据治理需要兼顾传统安全与非传统安全建设的核心要素，完善国防网络与数据安全的专项立法、构建政民预警交互意识和政企合作交互布局的“双重交互”体系，完善我国国防网络安全与数据治理格局。

关键词
国防授权法；国防网络安全；国防数据战略；重要数据治理

中图分类号：D93/97 文献标志码：A doi: 10.11959/j.issn.2096-0271.2023038

Research on the national defense cyber security and data governance

QI Pengyun
School of Law, People's Public Security University of China, Beijing 100038, China

Abstract
Improving and perfecting China's national defense cyber and data security governance structure is not only an important part of domestic national network and data security governance, but also a key practice in subdivided data fields under the framework of the “Data Security Law”. Through comparative analysis and literature analysis, we can extract the logical characteristics from the 2013-2022 U.S. National Defense Authorization Act, the successful experience of which can be valuable for improving domestic defense cyber and data security frame. Guiding by the holistic approach to national security with the core elements of traditional and non-traditional security construction, we can improve special legislation on national defense network and data security, and a “double interaction” system of government-civilian early warning interaction awareness and government-enterprise cooperation interaction layout to improve the strategic pattern of China's defense network security and data governance.

Key words
national defense authorization act, national defense cyber security, national data strategy, governance of critical data

0 引言

自2020年以来，国家安全机关接连发现有境外机构开设网站，以非营利组织名义为掩饰，招募国内志愿者使用其提供非免费设备收集我国各类飞行器航空数据并非法向境外传输，其中不乏对我国部分军事数据的收集和探测，直接威胁我国的国防安全。数据时代的快速发展虽然加速了社会数字化的进程，却也给国家安全、社会安全等提出了巨大挑战。面对这些数字风险，既要在传统安全范畴内继续加强国防安全的建设，同时也要保持对非传统安全领域中的信息安全技术与治理方案进行迭代。与此同时，应在《数据安全法》确定的数据制度框架下加快确立国防网络安全与数据治理的本土化方案。对此，可以对应美国《国防授权法》（以下简写为NDAA）中对国防网络安全与数据治理的框架脉络。美国NDAA是美国国会主要通过的两项年度法案之一，始于1961年，该法案经由参议院和众议院审议通过之后，由美国总统签署后生效。美国国防网络安全建设和国防数据治理最早在2013 NDAA中得以体现，随着数字经济时代的发展以及网络空间治理的慢慢成熟，国防网络空间及其数据治理规则愈发重要，开始在《国防授权法》中成为独立的重要篇幅。

本文主要围绕美国自2013年至2022年在其《国防授权法》中进行国防网络安全与数据战略布局的整体概览、发展脉络和前进路径进行系统分析，梳理其逻辑特征，对其发展趋势进行深度剖析，最后依托现阶段我国网络安全与数据治理方面的立法与实践现状，解析我国国防网络安全与数据治理建设路径的启示与对策。

1 美国国防网络安全与数据治理的战略框架

1.1 美国国防网络安全与数据治理框架简述

以美国近十年《国防授权法》为文本，分析美国在国防网络安全与数据治理方面的战略框架，大体可以分为六大板块。第一板块以网络数据的安全管理为核心，涉及网络数据产品与服务的采购、使用、处理等数据生命周期的全流程，加强了对敏感信息的安全管理，并对自2010年发布的《受控非密信息》实施安全报告程序。第二板块是信息网络架构中“零信任”架构建设，“零信任”是2010年由Forrester公司推出的通过对访问发起方进行认证授权、监测评估等访问控制从而建立信任关系的一种安全理念。在美国国防信息安全架构演进上，通过“用户–设备–授权”三重验证实现具体的访问安全控制。第三板块是网络关键基础设施建设，主要包括安全识别威胁能力建设、网络安全弱点竞争与报告和网络哨兵建设，从技术控制、程序控制和网络布局控制3个维度进行。第四板块是网络威胁应对机制，主要通过网络安全成熟度模型认证实现，该模型可以对国防信息安全领域表现进行测算，分析其信息安全的成熟度，优化升级信息安全系统从而达到迅速适应外部信息环境变化的目的。第五板块是网络事件响应机制，确立具体的事件响应程序，在网络演习中模拟复杂环境下网络攻防场景，验证国防网络安全机制，提升网络空间中的作战能力。第六板块是公私合作，包含网络安全检测、技术发展和人才储备3个方面，将国防网络安全方面的社

会力量作为重要途径和储备保障。美国NDAA国防网络安全与数据治理框架如**图1**所示。

1.2 美国近十年NDAA中国防网络安全与数据治理框架的要素演变

美国早在奥巴马总统时代就在《2013国防授权法》中对国防网络安全与数据治理进行了规划，在其国防部门授权下“网络空间相关问题”板块中用11个条款明示有关网络空间与数据安全管理的建设架构。最初的网络空间建设包含战略布局、管理架构、技术保障和数据分析四大方面：战略布局方面主要围绕总体信息环境规划；管理架构方面主要涉及部门调整，由原来的网络司令部重新组成联合网络司令部，以在网络空间内形成联合指挥机构，构建攻防结合的管理机制；技术保障上部署开放的网络体系系统，并提供覆盖系统全周期的软件保障；数据分析方面，要对国防部网络流数据以及大规模数据库进行分析识别，及时提供预警检测和评估，同时要迅速将信息泄露和软件渗透情况及时上报，并进行取证分析工作[1]。

从2013 NDAA到2022 NDAA，美国国防网络和数据安全的建设总体呈现出由大到小、由粗到细的趋势。笔者在**表1**中对比了美国自2013年起近十年的NDAA相关内容，提炼分析了每年《国防授权法》中网络安全与数据治理的关键要素。

从美国近十年以来逐步演变形成的国防网络空间架构来看，其总体框架基本搭建完成。随着美国对网络空间治理的重视，其国防战略也随之变化，在数据作为资产要素的当下，国防数据更是国家安全的重中之重，从美国最新发展趋势也可看出其国防数据治理体系的愈发完善。美国2022财年NDAA在国防网络安全与数据治理方面展现了新的举措和发展趋势，针对国防网络安全管理与数据治理进行了比较详细的规定，使其在管理数据和使用数据上更加具备可操作性。网络安全与数据治理的重要举措与发展趋势见**表2**。

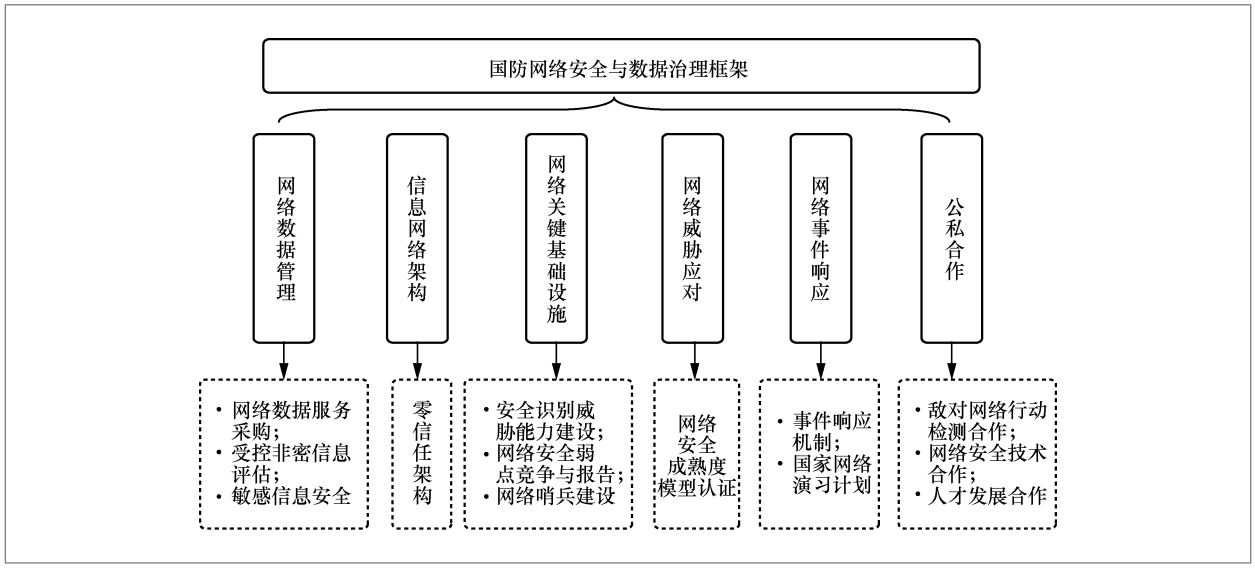

图1 美国 NDAA 国防网络安全与数据治理框架

表1 美国近十年NDAA中国防网络安全与数据治理关键要素

时间	条款数目/隶属板块	主要内容			
2013年度	11个条款（隶属于“国防组织与管理”板块）	网络安全战略布局	管理架构	网络技术保障	网络数据分析
2014年度	12个条款（隶属于“国防组织与管理”板块）	加强网络基础设施建设和人员培训	加强保密要求	建立跨部门行动程序	公私合作（与企业、教育中心）
2015年度	9个条款（隶属于“战略项目、空间与情报”板块）	网络事件报告和评估	网络测试和培训计划	跨域网络解决方案	
2016年度	9个条款（隶属于“战略项目、空间与情报”板块）	网络事件报告调整	应对网络攻击的准备行动、演习与评估	指定部门负责关键网络能力的获取	
2017年度	15个条款（隶属于“战略项目、空间与情报”板块）	网络基础设施漏洞评估	为易受到网络攻击的国防部人员提供网络保护支持	网络软件许可限制	向总统和国会提交网络空间威胁与应对报告
2018年度	20个条款（①隶属于“战略项目、空间与情报”板块；②区分一般网络安全事项和网络安全教育）	①制定网络空间安全的国家政策、安全计划和行动流程 ②对网络态势的全面审查和报告	限制特定网络产品和服务的使用	对网络新技术如区块链技术的应用报告	加强网络安全教育和网络安全人才的培养与资金支持计划
2019年度	27个条款（隶属于“战略项目、空间与情报”板块）	重述网络条款和网络安全相关政策应对恶意网络活动	授权国防部针对网络攻击可采取特别行动	个人身份信息和受控非机密信息（CUI）报告程序	①设立网络安全委员会 ②继续加强网络安全培训和人才培养
2020年度	27个条款（隶属于“战略项目、空间与情报”板块）	国防大数据平台方案的重新定位与布局	①针对特定国外实体[2]的网络攻击报告 ②改进网络安全态势审查	国防数据被盗取的控制与分析	继续加强网络安全培训与人才培养
2021年度	52个条款（单独成章：“网络空间相关事项”）	①重述网络安全战略与政策布局 ②构建国防数字服务方案	①整合网络安全中心计划 ②改进网络态势审查事项[3]	①加强网络安全领域公私合作 ②提出网络安全成熟度模型认证框架	①调整网络安全有关部门职能 ②继续加强网络安全培训与人才培养
2022年度	52个条款（①单独成章：“网络空间相关事项” ②分为3个子节：A-网络行动和网络力量、B-国防网络安全和信息技术、C-联邦网络安全）	①网络关键基础设施管理 ②信息网络架构 ③网络安全和信息系统的战略评估	①网络安全威胁评估与应对 ②网络安全事件响应 ③网络安全成熟度验证模型	①网络安全领域公私合作 ②网络安全数据管理 ③受控非加密信息评估 ④购买企业网络数据产品和服务	①公私合作 ②地区网络安全训练中心

表 2 美国国防网络安全与数据治理趋势

条款	内容	归类
Sec.1508	网络层面的公私合作	公私合作
Sec.1550	检测并干扰敌对网络行动的政企合作试点	
Sec.1510	应对勒索软件	网络威胁应对
Sec.1521	在企业范围内采购网络数据产品和服务	网络数据横向管理
Sec.1527	网络数据管理	
Sec.1526	受控非密信息评估	网络数据纵向管理
Sec.6423	敏感信息安全	
Sec.1528	“零信任”战略	信息网络架构
Sec.1533	网络安全成熟度模型认证	网络安全威胁应对
Sec.1541	网络安全和基础设施安全识别威胁能力	网络关键基础设施管理
Sec.1542	网络安全弱点	
Sec.1543	网络安全弱点报告	
Sec.1544	网络安全弱点竞争	
Sec.1548	网络哨兵计划	
Sec.1546	网络事件响应	网络事件响应
Sec.1547	国家网络演习计划	

2 美国国防网络安全与数据治理的战略分析

2.1 国防网络安全职能体系的独立——合作并行战略

美国在国防网络安全建设方面是循序渐进逐步增加的，从2013年关注国防网络安全开始逐步增加相关的职能部门或者单设专家顾问职位，为美国的国防网络安全职能体系建造专业团队，形成了纵横交错的“网络委员会–部门与办公室–安全员”的独立与合作并行的职能架构体系，具体如**图2**、**图3**所示。

2.1.1 安全委员会级别：战略评估与建议

在安全委员会的层级中，主要包括网络空间日光浴委员会和网络安全咨询委员会。2019财年设立的网络空间日光浴委员会主要应对重大网络攻击事件，主要负责平衡各种国防网络战略的成本与收益；评估相关网络战略的最优执行方式；对相关战略审查并做出决定，制定制度、执行标准、审查可能发生的潜在影响；评估现行有关网络空间、网络安全和网络软件的网络政策在摧毁、打破或者阻止网络攻击方面的效果[4]。2021财年成立的网络安全咨询委员会主要职责是对与网络安全有关的政策、计划、规划和培训提出建议、磋商或者报告。网络安全咨询委员会委员对接触到的各类信息，要依据信息的分级分类适用各类机密信息保护程序，从源头上保证信息的安全性。委员会内部还可以组成小组委员会，主要就网络信息交流、关键基础设置、网络安全风险、网络服务公私合作关系等进行沟通建议。

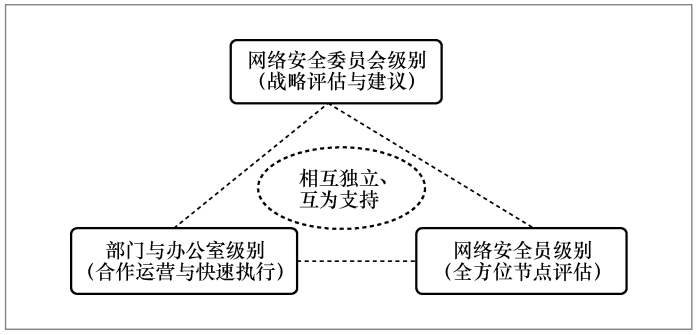

图 2 职能架构关系

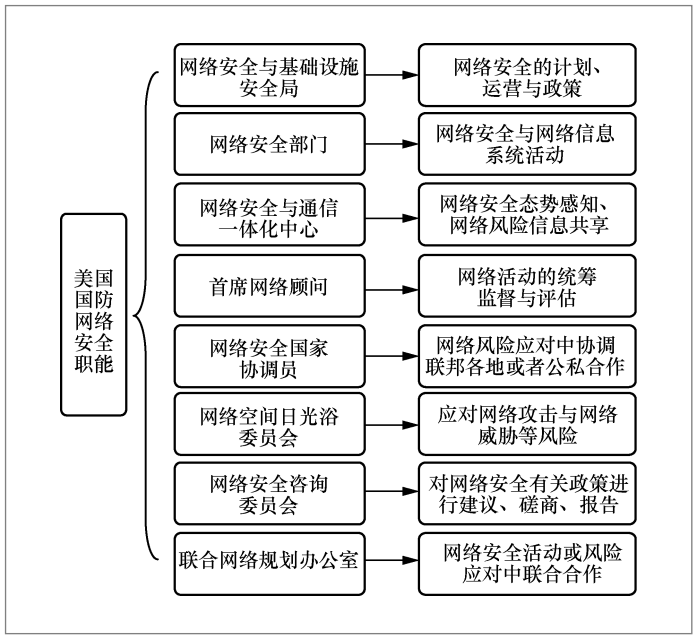

图 3 美国国防网络安全职能体系

2.1.2 部门与办公室级别：合作运营与快速执行

联合网络规划主要负责与其他联邦部门或者机构进行合作，建立一套必要的程序来发展和维持网络运营；为相关的联邦部门的网络能力和权力提供杠杆；加强与应对网络安全防线具有优势的私营部门的合作计划；为有关的联邦部门提供支持，尤其是在涉及发生网络安全风险事件时的情报支持以及快速执行方面[3]。

2.1.3 安全员级别：全方位节点评估

这一级别主要包括首席网络顾问与网络安全国家协调员，前者主要负责为对网络空间运营的所有活动进行统筹监督与评估，包括相关的政策、资源、人员、技术发展、传输和购买服务等事项，评估和监督网络战略的实施以及网络态势审查的执行。在作为国防网络首席顾问评估监督网络战略时，需要与首席信息运营顾问、首席信息官等进行协调以确保网络信息和情报等活动运营的整合。在与其他部门的合作方面，首席网络顾问华应当与来自国防部的其他网络专家或者组织、军队部门等组成联合团队，建立并维持一个全时的多功能的网络团队①。网络安全国家协调员作为网络安全风险顾问，必须在每一个州都有独立配备，负责支持与网络安全风险事件相关的准备与响应工作，对网络威胁信息进行共享，提高对网络安全风险的理解和对网络安全事件的态势感知能力，支持网络安全的培训工作，为非联邦实体自愿与联邦政府合作应对网络安全事件的联络点，在自愿基础上协助州和地区政府制定州网络安全计划等[5]。

2.2 国防网络安全公私合作建设战略

美国在国防网络安全与数字领域进行的公私合作最典型和有效的尝试是美国国防数字服务处（Defense Digital Service，DDS），DDS是美国在2015年由美国数字服务处（United States Digital Service，USDS）②在美国国防部设立的机构。由DDS作为数字联络点，将私营实体与联邦政府的合作建立起来，成功解决了在国防部内部搭建高端数字人才体系的困境。这是因为美国国防部当时亟须技术信息等数字化人才，但是有限的预算不足以在国防

① 对联合网络团队的组建是在《2017 财年国防授权法案》中首次提出的。

② 美国数字服务处是美国在 2014 年成立的，原因在于美国 2013 年经历了其医保网站的技术障碍，最后通过私营实体的帮助得以解决。

部内部直接搭建，更关键的是受限于军方烦琐的规章制度等约束，国防部直接寻求私营实体的合作也较为困难。因此，美国国防部在2015年成立DDS之后，加速了调动军方资源的灵活性，并在2017年将DDS作为常设机构，用于搭建与私营实体部门的技术合作，寻求技术服务与数字现代化的最佳实践方案。

从2018 NDAA开始，针对发生的网络攻击，规定美国众议院领导有权力向外寻求资助，特别是在必要时向私营的网络安全公司寻求合作[6]。2021 NDAA则直接确认DDS的核心功能与人才体系应向USDS看齐，保障国防数据战略的顺利进行[3]。2022 NDAA则进一步提出网络安全部联合国防部等有关部门应进行一个为期5年的联合试点项目，对网络安全的公私合作关系的可行性和有效性进行评估，促进合作的私营实体在发现和摧毁恶意网络行动方面有关的平台建设、系统服务和技术设施上进行提升。

2.3 国防网络安全评估与支持战略

2.3.1 国防网络安全评估战略

自2018年起，网络态势评估成为美国未来5~10年的网络威慑战略重要内容，这是美国首次在NDAA中将网络安全提到与核安全、太空安全等同样重要的地位，对于网络安全建设具有里程碑的意义[7]。一般来说，网络安全评估需包含以下要素：①评估现有的网络安全威胁警示政策和技术项目，尤其要依据网络安全成熟度模型验证要求的级别要素进行逐一检验；②检验正在施行的网络安全技术项目在收集分析网络活动元数据、快速审查与修复补漏方面的成效；③恶意网络攻击的情报共享机制。除了网络态势评估之外，还要对国防部的网络治理架构进行评估报告。例如，2022财年NDAA要求评估国防部实施的网络战略，包括网络行动、网络技术、信息支持和公私合作等方面，同时可以对网络治理的职能架构、网络安全政策、信息政策等提出建议[8]。

2022年美国在网络评估方面增加了新举措，设立“国家网络训练计划项目”，专门用来评估国家网络安全的相应机制的有效性。这一项目加固了网络安全的风险保障，还可以对网络事件造成的网络能力丧失进行模拟演练，为事件响应和信息共享提供系统性的支持，快速提供事件后报告和恢复计划等[9]。

2.3.2 国防网络安全人才支持战略

人才支持体系由两部分组成，第一部分是网络安全奖学金计划。该计划主要针对高等教育学生，符合条件的个人可以参加情报机构与网络安全部门的实习，接受政府资助并于毕业后在情报或者网络安全部门任职。第二部分是网络教育和培训项目。该项目针对小学和中学的网络安全教育，不仅在中小学阶段教授学生有关网络安全的技能，同时会引导学生探索网络安全方面的职业道路，为美国的网络安全人才体系建设打下基础，可以说从起跑线开始建设网络安全人才体系。在网络安全人才支持体系中，既包括正式的学位教育人才，也包括技术型人才和拥有相关知识专长的非学术执业培训发展项目。

2.4 数据治理的内外并重发展战略

2.4.1 国防数字产品和服务采购的单独授权

为了加强国防网络技术和数字服务的支持度，2022年美国国防部新设一个具有独立授权的数字产品采购代理，负责执行

适用于国防网络的商业化数字产品的购买政策。具体的数字产品和服务可能包括但不限于商业数据集、网络威胁数据集、数据分析软件、数字产品和数据服务的集成等形式。采购代理负责实施独立的市场调研，结合国防部门的需求单独或者共同决定产品的购买、做出商业沟通、签订数字服务和产品合同。采购代理的设立不仅便于及时对接国防网络需求，更能够迅速在市场上获取匹配的数字产品和服务，得益于独立的职能授权和预算，采购代理能够对市场化的数字产品进行动态沟通，同时具有通过公私合作定制适配国防网络安全发展的特定数字产品或服务的能力。

2.4.2 国防数据安全治理的分级分类

在数据安全治理中，美国国防数据也配备了最新治理方案。首先，所有涉及国防数据的部门都负有相关数据的安全管理义务，包括美国网络安全司、军方相关部门都要联合网络安全首席顾问、首席信息官、国防部首席数据官、联合网络规划办公室等。主要任务是对与国防有关数据的评估、购买和使用，对情报数据、网络流量数据、地理数据、网络威胁信息、国防部信息制定数据治理政策和处理程序；其次还要对数据管理的平台进行评估和报告。

在国防数据网络安全管理中，一直属于重点保护与治理地位的有两项，分别是特定个人信息保护和受控非机密信息（CUI）的保护，对这两类重要信息的保护增加了明确的信息泄露触发程序。①加强国防网络相关个人信息的泄露报告程序。虽然美国对多个领域内的个人信息数据的保护出台了诸多的法律方案，但都散见于各个单行法案③中，属于基于实践需求逐个击破的立法方式。在保护内容方面，国防网络安全个人信息保护对象为国家安全部门或者军队的特定人员的个人信息，对其姓名、职员编号、生物特征、家庭或者个人联系方式以及其他人口特征、就业、医疗与金融信息等所有可能识别或者追踪到特定人员的信息都纳入国防网络信息保护系统。在相关人员的信息泄露时，必须及时向国防委员会做出报告，报告可依据具体情况决定是否采取加密形式。配套的报告程序必须在国家安全政策下进行，并且以最有利于个人信息保护的方式进行[10]。②加强对受控非机密信息泄露的报告程序。虽然美国对受控非机密信息在法律层面的治理始于2010年奥巴马政府对《受控未分类信息》法案的签署，但直到2022年美国才将CUI信息的泄露报告程序在国防网络战略中进行明确。CUI信息共分为8类④，时至今日，美国有关CUI的信息管理部门相关职能、信息使用监督、滥用信息制裁等都已形成了相对成熟的模式。为了保护国家安全，CUI管理部门在其年度报告中不止一次强调要对CUI计划进行全面实施，其中就包括国防数据的网络管理计划[11]。2022国防战略对CUI信息的定义进行了进一步说明，便于实践中更好地进行数据识别⑤，并特别强调当受控非机密信息发生泄露时，必须遵循特定程序及时向国防委员会报告。

2.5 美国国防网络安全与数据治理的战略分析

2.5.1 国防网络安全成为国防战略的转型核心

当前美国国防将反恐作为头等大事，虽然自2013财年开始注重对国防网络空间的建设，但是总体处于比较平稳的投入状态。从特朗普政府的《国家安全战略》和《国防战

③ 例如隐私权领域的《加州消费者隐私权法》、金融领域的《公平信用报告法》和卫生服务领域的《卫生信息可移植性和责任法》等。

④ CUI信息分为8类：仅供官方使用的信息、执法敏感信息、国防部受控非密核信息、限制分发信息、国务院敏感非密信息、缉毒署敏感信息、外国政府信息和技术文件分发声明。

⑤ 例如2022 NDAA指示了国防部正确标记或者以其他方式识别CUI的程度，在何种情况下可以将商业信息视为CUI，要求使用唯一的CUI图例进行标记的优缺点以及视为或者不被视为CUI的信息示例。

略》开始，美国国防战略开始发生转变，最终在《2019财年国防授权法》确定了从反恐到大国竞争的战略转变[12]。这也是美国自金融危机后开启新一轮军事建设周期的起点，在特朗普政府新的美国国家安全观的指导下，加强了对国防战略的全面转型，国防网络空间的建设与发展是其重要内容[13]。

随着国防网络空间的重要性日益增加，美国国防网络发展战略也随之转型。从**表1**的分析可知，美国国防网络安全战略的第一个转折点发生在2015财年，国防网络空间建设从国防组织板块一章中脱离出来，重新规整到战略项目、网络与情报一章中，有了相对独立的地位。而后在2018财年中进行了较为重大的调整，不仅区分一般网络安全事项，更加强调网络安全教育事项，更重要的是对网络安全的国家政策进行了重述，对国防发展中的新技术给予了高度重视，在资金支持与人才培养上开始双管齐下，共同发力。2019财年NDAA决定拨款成立美国国家人工智能安全委员会，面对来自国际竞争对手的网络舆论战和宣传战成立了专门的国家指挥机构，并建立国家网络空间安全委员会开展隐蔽的网络行动以应对潜在的网络攻击。第二个转折点发生在2021财年，2021 NDAA中网络空间安全板块单独成章，条款激增，是截至目前美国历史上通过的最全面的国家网络安全立法，在网络安全战略上也更加注重联邦和地区、政府和私营实体之间的公私合作[14]。

2.5.2 持续增加对国防网络安全技术发展的预算投入

想要了解一个政府在做什么，只需要去看它的预算[15]。自2013财年NDAA开始，美国不断加大对网络空间安全有关事项的预算投入，并用于当年的重点项目。例如，2019财年的国防预算共7 160亿美元，同比涨幅为2.3%，为2011年以来国防预算涨幅最大的一次[16]。更引人注目的是，2019财年加大对网络建设、人工智能等先进科学技术的预算投入，总投入比2018年增长了4个百分点，远超国防总预算的涨幅，主要用于对先进网络技术的发展、基础研究和应用研究。2022财年对网络空间的预算总额比2021年增加6%左右，而2022年的全年国防预算总额增幅不到1.7%，足以见得美国对网络空间战略发展的重视与投入。

2.5.3 保障国防网络安全职能体系内的独立与合作渠道

在国防网络安全系统中，安全委员会-部门与办公室-安全员的架构体系，同时赋予了美国网络安全职能体系的独立性与合作性，各级别职能相互独立，又能够合作进行，充分保障了网络安全工作需要的保密、独立与合作需要。例如部门级别会向委员会提供情报、基金、人员、设备以及其他支持，部门与办公室在执行计划时必须与其他部门建立联系或者与私营实体进行合作等。

2.5.4 加大对国防网络安全与数据治理中的公私合作空间

在国防数据产品和服务采购方面，通过与第三方合作方式，能够以较低的成本尽可能多地进行数字化产品实验，从而寻找最符合国防需求的产品与服务。此外，将国防网络安全与数据治理需求以单独的功能模块为基础进行分散，可以在扩大公私合作空间的同时保障国防信息的安全，降低某一单独合作方信息泄露的风险。

人才支持方面，一方面对合作院校中特

定人才培养进行早期介入，在人才培养方案、实践发展项目和人才输送渠道上提供支持并形成一定的话语权，既能够提高相关学校的合作积极性，还能够有效聚焦特定人才培养的方向，快速提高特定领域的顶尖人才数量和质量。另一方面公私合作中的高端人才流动渠道可以拓展和补充网络与数据技术领域的合作范围，保持开放的技术视野。

在对特定类型国防数据安全治理方面，美国对个人信息和受控非机密信息的保护一直是在相关领域内进行单独的治理，对相关信息的收集、使用和传输等都已有可行的操作方案。在正式法案中要求国防部制定有关的个人信息和受控非机密信息的泄露报告程序，说明对其信息和数据的治理方式更加细化和深入，可操作性程序的出台也让数据保护的深入治理不再浮于表面，与国防网络安全发展建立了实质链接。

3 美国国防网络安全与数据治理的中国启示

现阶段我国在网络安全与数据治理方面的立法与实践正处于探索与发展之中，在网络安全、数据安全和个人信息保护等方面均已出台相关法律。实践中，全国各地数据主管部门在大数据发展规划和政策措施上都在进行积极探索。以政务数据为例，2022年《全国一体化政务大数据体系建设指南》显示全国已建设26个省级政务数据平台、257个市级平台和355个县级平台，超过70%的地级市建设了数据云平台，在数据治理和数据公共服务方面取得了巨大成效。然而在国防网络安全与数据治理方面的立法与配套制度建设还不完善，国防网络安全与数据统筹管理机制还未建立起来，相关数据技术的开发还处在低水平重复状态亟须提高[17]、国防网络安全与数据保障能力等亟须强化[18]等。面对这些问题，以美国《国防授权法》为镜，提取美国国防网络安全与数据治理中的重要构成要素，为我国国防网络安全与数据治理制度建设提出完善建议。

3.1 完善国防网络安全与数据治理的专项立法

3.1.1 建议加快推进国防网络安全与数据治理专项立法

依托数字发展的国防网络安全战略离不开对数字法治的治理体系，网络安全战略与数字发展战略相辅相成，共同构成国家安全的重要部分，而国防网络安全战略则是保卫国家安全的重要手段。现代科技是网络安全战略的关键技术要素，其不仅包含“当地、当时、确定的威胁，还有全球化的、跨时代的、不确定的威胁”[19]。依据我国《国家安全法》，军事安全属于传统安全，信息安全属于非传统安全，由此可以分析国防网络安全战略属于在传统安全中构建局部的非传统信息安全体系，国防网络安全战略中的技术要素、数据或者数据集要素、网络与数据分析关键基础设施等均处于该体系的涵盖范围之内。因此国防网络安全战略应以遵循总体国家安全观为指导理念，从治理结构搭建到治理功能设置再到具体的网络安全要素运行，都应贯彻总体国家安全观思想，并融合传统安全与非传统安全的核心要素。

从我国《网络安全法》和《数据安全法》的出台来看，目前网络安全和数据治理框架均注重对总体国家安全观的贯彻。《网络安全法》站在国家总体网络架构的高点进行统筹规划，为国防网络安全建设提供法理依据[20]。《数据安全法》则在有关数据安全、保护与开放层面做出了制度

性的框架设置。但是从具体的方案内容切入，则能发现《数据安全法》并不应然直接适用于所有国防数据的治理，例如该法规定军事数据安全保护办法由中央军事委员会依照该法另行制定，但这并不意味国防数据的治理可以完全跳出《数据安全法》的方案，而是应当在《数据安全法》确定的总体框架与制度体系内进行细分领域的立法与实践探索。

针对国防网络安全，一方面应加强技术攻关，针对国防网络安全需求建设针对性的关键基础建设操作方案，配套信息国防网络安全制度，明确责任主体[21]。在军事数据安全保护方面的专项立法中，军事数据保护法作为下位法应当遵循《数据安全法》的原则性规定，避免与《数据安全法》相冲突。另一方面，在具体规则上应围绕国防网络安全职能体系、网络威胁应对机制、网络安全事件响应等潜在网络安全风险方面制定可操作性的执行规则；还有在国防数据安全上，应明确国防数据范围和判断标准，确定模糊边界的数据进行审查判断规则，在数据威胁感知、数据泄露响应方面建立公私合作机制，明确追责方案，形成具有可预知性、可期待性、可操作性的立法方案。

3.1.2 国防数据安全治理的专项机制

在数据作为生产要素并被冠以“21世纪最有价值的资源与新时代引擎的石油”[22]的重要背景下，我国的《网络安全法》和《数据安全法》对网络数据等要素出台了一个框架性的保护规则。总体而言，《数据安全法》明确了在实施数据分级分类保护之下，对属于国家核心数据的国家安全等数据实施更严格的管理制度。然而，关于应如何对数据进行分级分类、如何划定国防数据边界、实施何种程度的严格均未做出更加明确的规定，很难直接用于指导实践。目前我国《数据安全法》已确立的数据安全制度包括数据交易管理制度、数据分类分级保护制度、数据安全应急处置机制、数据安全审查制度、全流程数据安全管理制度。在上位法确定的基础制度下，除了针对细分领域的国防数据制定更具针对性的单行法案之外，应针对国防数据安全进行配套制度建设。

一是确立数据产权制度，明确国防数据治理边界和相关法律责任。在总体国家安全观的指导下，将国防数据安全边界贯穿数据供给、流通和使用的过程，划定国防数据监管底线。二是在数据分级分类管理原则下，依据2022年12月中共中央、国务院《关于构建数据基础制度更好发挥数据要素作用的意见》，对涉及国家安全的特殊个人信息数据，在保障安全的情况下依法依规进行数据开发使用，探索建设“原始数据不出域、数据可用不可见”的数据授权使用机制。三是在数据要素流通公私合作方面，培育合规高效、安全有序的第三方数据专业机构，为数据技术开发、数据服务扩展、数据人才培训等提供增值服务。四是围绕国防数据等重要数据的建设加强治理机制统筹，完善数据治理职能体系建设，强化数据监督管理。

3.2 完善国防网络安全与数据治理的“双重交互”体系

3.2.1 完善国防网络安全的“政府与公众预警交互”意识

从目前的国家网络安全事件的深入分析可知，境外机构对我国国防网络安全的攻击一般是从我国普通的人民群众入手，利用普通公民对国防网络相关知识的了解不足附加各种欺骗手段来进行信息收集。我国某些公民在信息收集的最基础层面被

收买或者引诱，境外机构利用收集到的信息进行大数据层面的深入分析。因此，要从根源处切断境外机构对我国国防网络安全的攻击，防范国防网络安全漏洞，应摒弃重视实体战场而不重视虚拟战场的传统观念[23]，必须抓好我国普通公民的国防安全意识问题，建立全民的反情报意识体系，才能最终形成牢固的国防网络防火墙[24]。

3.2.2 完善国防数据安全的“政府与企业合作交互”布网

政企交互合作的重点之一在于职能体系与监管层面的交互。依据《网络安全法》，我国的网络安全主管部门是国家网信部门，负责网络安全的统筹和监督。国家电信部门和公安部等其他部门在各自的职责范围内负责网络安全职能，人民政府网站的网络安全又要借助于国家其他的有关规定进行。网络关键基础设施的采购，由国家网信部门和国务院有关部门负责审查和数据出境评估。网络安全信息的收集、分析和通报，以及网络事件的评估和应急机制同样是由国家网信部门进行统筹。《数据安全法》则规定除了国家网信部门对网络安全数据进行协调统筹和监督之外，均由各地区、各领域内的各部门承担相应的数据安全监管职责。总体来看，现阶段立法对于网络安全与数据管理的职能体系上，对各个领域内的数据安全明确了主管部门和数据安全方针政策方面的职能划分，例如国家数据安全的决策议事、方针政策以及工作机制由中央国家安全领导机构负责，但是对于国家数据安全和网络安全方面的下位法制定、职能体系工作机制的细化与监管方案等还缺乏可操作性规则和配套制度建设。

具体而言，应当在《数据安全法》的指导下，对重要数据领域进行细分，将国防网络安全与数据的管理独立出来，重组一个具有相对独立权限的国防网络安全与数据治理部门。在职能监督与评估上，采取动态报告和定期报告相结合的方式进行。在特定网安与数字业务方面，可以通过公开招标的方式寻求最佳实践方案，同时由现有数字团队进行深入评估，例如美国DDS采取的评估方式是对过审公司发放技术挑战，要求相应私营公司在有限时间内给出解决方案，通过解决难题的方式来评估各个私营公司的数字技术能力。

政企交互合作的另一重点是网安人才体系交互。一方面可通过“旋转门”机制保障网络安全与数字技术人才体系的优化和更新。具体来说，通过“旋转门”人才机制至少确保有一定数量的国防网络数字人才来自于私营部门，范围可涵盖软件开发、信息工程师、数字工程师和产品经理等岗位，规定任职期限和考核标准，以确保人才的流动更新。另一方面人才支持体系离不开针对性的人才培养教育，必须建立广泛的网络安全人才素质培养基地。在高等教育阶段则进入专业技术与人才需求的联合培养轨道，针对性进行学科设置和专业素养教育，既可以满足国防部门对人才素质的考察需求，又能结合实际发展进行定制化培养。

最后，为了保证政企双重交互合作的效果，对与国防网络安全与数字领域有关的任何公私合作或者实践方案，都应当进行及时评估和审查，形式审查应当追随项目进行动态评估，对方案的审查应在事前、事中和事后分阶段进行，每年度还应当对所进行的公私合作项目进行报告。

参考文献:

[1] 112th Congress (2011-2012): national

defense authorization act for fiscal year 2013:H.R.4310[Z]. 2013.

[2] 116th Congress (2019–2020): national defense authorization act for fiscal year 2020: S.1790[Z]. 2019.

[3] 116th Congress (2019–2020): William M. (Mac) thornberry national defense authorization act for fiscal year 2021: H.R.6395[Z]. 2021.

[4] Cyberspace solarium commission white paper[R]. 2022.

[5] 6 U.S. Code § 665c – cybersecurity state coordinator[Z]. 2022.

[6] 115th Congress:national defense authorization act for fiscal year 2018: H.R. 2810[Z]. 2017.

[7] 胡晓剑. 美国《2018国防授权法案》网络安全条款解读[J]. 国际研究参考, 2018(3): 7–9.
HU X J. Interpretation of the cyber security provisions of the US National Defense Authorization Act of 2018[J]. International Study Reference, 2018(3): 7–9.

[8] 117th Congress (2021–2022): national defense authorization act for fiscal year 2022: S.1605[Z]. 2021.

[9] Subtitle a of title XXII of the homeland security act of 2002 (6 U.S.C. 651 et seq.) [Z]. 2002.

[10] 115th Congress (2017–2018): John S. McCain national defense authorization act for fiscal year 2019: H.R.5515[Z]. 2018.

[11] 吴沈括, 崔婷婷. 美国受控非密信息管理制度研究[J]. 中国信息安全, 2019(5): 87–91.
WU S K, CUI T T. Research on American controlled non-confidential information management system[J]. China Information Security, 2019(5): 87–91.

[12] 侯娜, 胥宝俊, 陈波. 美国2019财年国防预算解析[J]. 和平与发展, 2019(2): 19–34, 133, 134.
HOU N, XU B J, CHEN B. Analysis of US defense budget in FY 2019[J]. Peace and Development, 2019(2): 19–34, 133, 134.

[13] 李峥, 张磊. 美国《2019财年国防授权法案》主要特点及影响[J]. 国际研究参考, 2018(9): 21–24, 34.
LI Z, ZHANG L. Main features and influence of the national defense authorization act of FY 2019 in the United States[J]. International Study Reference, 2018(9): 21–24, 34.

[14] 罗仙, 张玲, 庞浩, 等. 从美国最新国防预算文件看网络空间发展新动向[J]. 信息安全与通信保密, 2021, 19(11): 117–125.
LUO X, ZHANG L, PANG H, et al. Trend analysis of U.S. cyberspace development based on its defense budget[J]. Information Security and Communications Privacy, 2021, 19(11): 117–125.

[15] 朱殿骅, 谢先达, 张允壮. 美国国防预算是如何制定的?[J]. 财政科学, 2017(10): 56–74.
ZHU D H, XIE X D, ZHANG Y Z. How is the defense budget made? analysis of defense budget process of the United States[J]. Fiscal Science, 2017(10): 56–74.

[16] 胡欣. 美国新国防授权法案的愿景与危险[J]. 世界知识, 2018(17): 74.
HUX. The vision and dangers of the New US Defense Authorization Act[J]. World Affairs, 2018(17): 74.

[17] 许洪波, 陈波. 面向国防安全的网络大数据分析与应用系统[J]. 大数据, 2015, 1(4): 29–37.
XU H B, CHEN B. Network big data analysis and application systems for national defense security[J]. Big Data Research, 2015, 1(4): 29–37.

[18] 魏凯. 对大数据国家战略的几点考虑[J]. 大数据, 2015, 1(1): 108–114.
WEI K. Some considerations on the China national big data strategy[J]. Big Data Research, 2015, 1(1): 108–114.

[19] 王贵松. 论法治国家的安全观[J]. 清华法学, 2021, 15(2):21–37.
WANG G S. On the security concept of a country ruled by law[J]. Tsinghua Law Review, 2021, 15(2): 21–37.

[20] 倪良. 关注网络国防是《国家安全法》对网络立法的基本要求[J]. 中国信息安全, 2015(8): 38–40.
NI L. Paying attention to cyber defense is the basic requirement of cyber legislation in the National Security Law[J]. China

Information Security, 2015(8): 38-40.

[21] 杨兵, 张锦. 网络国防信息安全力量建设探析[J]. 飞航导弹, 2016(12): 31-33, 38.
YANG B, ZHANG J. Analysis on the construction of network defense information security force[J]. Aerodynamic Missile Journal, 2016(12): 31-33, 38.

[22] 完颜邓邓, 陶成煦. 美国政府数据分类分级管理的实践及启示[J]. 情报理论与实践, 2020, 43(12): 172-177, 155.
WANYAN D D, TAO C X. The practice and enlightenment of American government data classification and hierarchical management[J]. Information Studies (Theory & Application), 2020, 43(12): 172-177, 155.

[23] 侯嘉斌. 从《网络安全法草案》看推动网络国防建设军民融合发展的路径[J]. 中国信息安全, 2015(11): 119-121.
HOU J B. On the path to promote the development of cyber national defense construction in integration of defense and civilian technologies from the perspective of the Draft Cyber Security Law[J]. China Information Security, 2015(11): 119-121.

[24] 李响, 马海群. 美国《国家反情报战略》演进分析[J]. 情报杂志, 2022, 41(5): 1-7.
LI X, MA H Q. Analysis of evolution of the USA national counterintelligence strategy[J]. Journal of Intelligence, 2022, 41(5): 1-7.

作者简介

齐鹏云(1993-), 女, 中国人民公安大学法学院博士生, 主要研究方向为数据法学与司法制度。

收稿日期: 2023-01-03
基金项目: 国家社会科学基金项目(No.21&ZD193)
Foundation Item: The National Social Science Foundation of China (No.21&ZD193)