零信任战略与美国网络安全的现代化*

刘国柱

【内容提要】 零信任是一种专注于资源保护的网络安全范式，其前提是信任永远不会隐式授予，而是必须持续评估。这一安全范式是随着互联网、物联网、大数据、云计算等数字应用场景的拓展而产生的。零信任架构的核心原则是通用身份验证、访问分割、最小信任授权、加密无处不在以及持续监控和调整。美国政府加速推进零信任战略，既是美国传统网络安全系统失能、网络安全理念和技术迭代的要求，也是数字时代大国竞争的组成部分，同时还是美国国防数字战略现代化的需要。美国政府加强基于顶层设计的网络安全宏观布局，明确实施零信任战略的关键事项，并确立了联邦政府推动零信任安全体系的基本原则。零信任安全框架的核心领域是关键基础设施、国家安全系统和国防系统，美国确立了以网络安全和基础设施安全局为轴心的推动零信任布局的“全政府”架构。零信任不仅仅是技术的转变，还是一种文化。零信任架构从以网络安全为中心转向以数据安全为中心。零信任不仅是网络安全防御战略，也是进攻战略，即在稳固自身安全的同时，无所顾忌地向对手发起攻击。美国在网络安全领域攻击性的增强，将给包括中国在内的世界其他国家的网络安全带来更大的压力。在这种情势下，中国政府机构、企业、网络安全工作人员须共同努力，打造中国自主可控、安全便捷的现代化网络安全体系。

【关键词】 零信任；关键基础设施；网络安全；数据战略

【作者简介】 刘国柱，浙江大学历史学院美国研究中心教授、非传统安全与和平发展研究中心研究员（杭州 邮编：310058）。

【DOI】 10.14093/j.cnki.cn10-1132/d.2023.06.001

【中图分类号】 D815；G323 【文献标识码】 A 【文章编号】 2095-574X（2023）06-0003-26

* 本文系中央高校基本科研业务费专项“战后美国科技创新体系的构建”的阶段性研究成果。作者感谢《国际安全研究》编辑部和匿名审稿专家的意见和建议，文责自负。

随着互联网、物联网、大数据、云计算等数字技术应用场景的不断拓展，传统上基于网络边界的安全保护日益转向以用户、设备和资源为中心的安全保护，零信任（Zero Trust）概念应运而生，并逐渐为企业和政府所接受。从特朗普政府时期美国便开始推动零信任安全布局，2020 年 8 月，美国商务部国家标准与技术研究院（National Institute of Standards and Technology，简称 NIST）推出了《零信任架构》（*Zero Trust Architecture*）报告，推动在美国使用零信任原则来规划企业和公共信息基础设施。2021 年 5 月 12 日，拜登政府颁布了《改善国家网络安全的行政命令》（Executive Order on Improving the National's Cybersecurity），标志着以构建“零信任架构”为核心的网络安全现代化进程进入了具体推进阶段。根据总统的行政命令，2021 年 6 月，美国国土安全部网络安全和基础设施安全局（Cybersecurity and Infrastructure Security Agency，简称 CISA）率先制定了《零信任成熟度模型》（*Zero Trust Maturity Model*）；2022 年 1 月 26 日，白宫管理与预算办公室（Office of Management and Budget）公布了《推动美国政府走向零信任网络安全原则》（*Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*）；2022 年 11 月 7 日，美国国防部公布了《国防部零信任战略》（*DoD Zero Trust Strategy*）。随着上述美国政府系列文件的公布，美国网络安全现代化战略趋于清晰化。

国内学术界已经开始关注零信任安全体系和美国零信任战略，并取得了一些颇有建树的研究成果。已有研究主要集中在以下三个领域：首先，从技术角度研究零信任安全架构和零信任安全体系，并分析其依赖的关键技术。[①] 其次，对美国零信任战略作出初步的判断，并形成了两种不同的观点。一种观点认为：这是美国政府“信息技术现代化”改革的一部分，属于渐进过程中的一环，目的不是为了发展零信任，而是资本炒作行为，违背了基本技术原理。[②] 另一种观点则认为，零信任是在传统信息技术边界消亡时对安全边界的重塑，是对原有安全能力体系的重新整合，目的在于使保障范围更加全域化。[③] 再次，对美国《国防部零信任战略》文本的解读，认为该战略的数据、应用程序、资产和服务提供安全保护，旨在为美国军

① 张泽洲、王鹏：《零安全架构研究综述》，《保密科学技术》2021 年第 8 期；唐敏璐、孟茹：《零信任安全体系研究》，《信息安全与通讯保密》2022 年第 10 期；余海、郭庆、房利国：《零信任体系技术研究》，《通信技术》2020 年第 8 期。

② 左晓栋：《零信任热中的冷思考》，《中国信息安全》2022 年第 2 期。

③ 肖新光、徐菲、赵超、李晓利：《从美方推动零信任战略过程看网络创新的规律特点》，《中国信息安全》2023 年第 3 期。

方推进零信任理念的发展提供指导。[①]

本文尝试在学术界已有的研究基础上，通过梳理传统网络安全体系向零信任安全架构的迭代，特别是零信任架构的主要逻辑特征，分析美国政府推动网络安全现代化的动因、基于零信任架构的联邦网络安全现代化战略谋划和布局以及美国零信任战略的特征等。

一 从传统网络安全到零信任安全理念

在当今世界互联互通不断增强的大环境下，信息安全已成为各国政府、企业、团体和个体关注的重点。由于物联网和云计算的快速发展，各种电子设备现在可以更加轻松地访问企业与公共网络。网络在为人们日常的工作、生活提供更多便利的同时，也增加了数据泄露和网络攻击的可能性。传统的维护网络安全方法被称为周界安全（Perimeter Security），其设计理念是：一个内部或受信任的网络由防火墙及其他安全防护措施将其与外部世界隔绝。这个边界内的（或通过远程方法连接的）人或端点，要比边界外的人或端点获得更高级别的信任。这些架构使得进入内部网络的人可以轻松地畅游内部网络，相应的用户、设备、数据和其他资源几乎完全不设防。网络攻击正是利用了这种设计，即首先获得对一个或多个内部端点或其他资产的访问权限，然后沿网络横向移动、利用其存在的弱点、泄露受控的信息并发起进一步的攻击。除此之外，随着网络扩展到包括大量的终端，用户需要从不同的地点访问，这种模式变得更加紧张起来。同时，对手还在继续寻找创造性的方法来绕过周界安全，例如操纵用户泄露其证书的网络攻击。这种网络扩张和对手的创造力要求防火墙必须不断调整，以应对不断扩大的授权进入网络的人员和可接受的进出网络的流量。

为解决传统网络安全框架的不足，零信任安全已经成为一种被广泛采纳的网络安全理念。在零信任安全架构中，所有设备和用户即使是网络中的设备和用户，除非得到验证，都被视为不可信。这决定了零信任安全的实施涉及对访问网络资源的设备和用户的持续监控和身份验证。

（一）零信任概念的发展历程

“零信任”一词最早是由斯蒂芬·保罗·马什（Stephen Paul Marsh）提出，他

① 孙宝云、齐巍：《美国国防部〈零信任战略〉解析》，《保密工作》2023 年第 3 期；李桢静、张小军、郝志超：《美国国防部〈零信任战略〉解读》，《信息安全与通讯保密》2023 年第 1 期。

在 1994 年 4 月于斯特灵大学（University of Stirling）发表的关于计算机安全的博士论文中，第一次使用了“零信任”这一概念。马什提出了一种信任的形式主义：它可以嵌入人工智能代理中，使代理能够作出基于信任的决策。[①] 马什的零信任概念在当时的网络安全领域并未产生多大的影响。2004 年，在由英国首席安全官组成的杰里科论坛（Jericho Forum）上，零信任作为一种安全设计概念被提了出来。英国的网络安全精英看到了由于云计算和移动计算的加速使用，访问和授权的方式正在发生变化，论坛提出了一个新的安全模型，这个模型适合于传统的周界安全环境已经失效，或变得不太重要，工作流程已经转移到云，移动终端正在成为应用程序访问的主要目标。论坛提出了一种名为“去边界化”的新安全概念，重点关注如何保护流入和流出企业网络边界的企业数据，而不是努力说服用户和企业将其保留在企业网络上。

作为专业术语，公认的“零信任/零信任安全”概念是在 2010 年由弗雷斯特公司（Forrester）的分析师约翰·金德维格（John Kindervag）提出的。金德维格认为，在今天的新威胁环境中，传统的基于周界的安全框架不再是一种有效的加强安全的方式，因为一旦攻击者攻破了防火墙，就可以访问防火墙内的所有资源。为此，金德维格提出了一种新的网络安全模型，并将其称为“零信任”：零信任的核心是一个简单的哲学，即安全专业人员必须停止像信任人一样信任数据包。相反，他们必须消除可信网络（通常是内部网络）和不可信网络（外部网络）的想法。在零信任中，所有网络流量都是不受信任的。因此，安全专业人员必须验证和保护所有资源，限制和严格执行访问控制，并检查和记录所有网络流量。

金德维格的零信任有三个基本概念：首先，无论位置如何，都能确保安全地访问。在零信任模型中，安全专业人员必须假设所有流量都是威胁流量，直到验证流量是经过授权、检查和安全的。其次，采用最小权限策略，严格执行访问控制。基于角色的访问控制是由网络访问控制和基础设施软件、身份和访问管理系统以及许多应用程序支持的标准技术。通过使用访问控制，安全专业人员将用户置于一个角色中，并基于该角色允许他们访问某些特定的资源。但是，零信任并未明确将访问控制定义为首选的访问控制方法。随着时间的推移，其他技术和方法也将随之发展，而重要的是最小权限和严格访问控制的概念。再次，检查并记录所有流量。在零信任中，只限制用户使用他们完成工作所需的资源。零信任不是相信用户会做正确的

① Stephen Paul Marsh, *Formalising Trust as a Computational Concept*, 1999, https://www.cs.stir.ac.uk/~kjt/techreps/pdf/TR133.pdf.

事情，而是验证他们正在做正确的事情。要做到这一点，就需要将“信任但要验证”原则转换为“验证而绝不信任”。零信任提倡两种获得网络流量可见性的方法：检查和记录。

金德维格提出的“零信任”概念，目的是为信息安全提供一个新的概念模型。零信任被设计成增量的和非教条的，它不是一个项目，而是一种思考信息安全的新方式，其目的是帮助建立一个关于信息安全未来的新对话，从而产生可行和有效的解决方案。金德维格为网络安全创建了革命性的零信任安全模型，因其对零信任安全模型具有超强的洞察力，被誉为“零信任之父”。[①]

随着网络安全问题的日益复杂化，以身份验证为基础的零信任安全理念和架构逐渐取得信息技术业界主流的认可。一些大型信息技术企业从不同角度设计了零信任安全模型。2010 年，谷歌公司在经历了“极光行动”（Operation Aurora）的网络攻击后，启动了一项为期六年的零信任“BeyondCorp”项目，这是一项全公司范围内的倡议，旨在以零信任模式重新构建谷歌公司的网络安全架构。BeyondCorp 的目标是使用户能够随时随地在任何设备上安全地工作，而无需使用虚拟专用网络（VPN）来访问组织的资源。BeyondCorp 有两个最重要的原则：第一，控制对网络和应用程序的访问。Beyond 为组织提供了一种自动化、可扩展的方式来验证用户身份、确认他们是授权用户以及符合应用规则和访问策略。第二，可见性。一旦用户有权访问机构的网络或应用程序，机构必须不断查看和检查所有流量，以识别任何未经授权的活动或恶意内容。否则，攻击者可以轻松地在网络内移动并在无人知晓的情况下获取他们想要的任何数据。BeyondCorp 作为一个成功的零信任模型，使零信任概念成为人们关注的焦点。

（二）零信任概念内涵与美国向零信任网络安全转型

零信任是一个动态的概念，其内涵随着网络技术的发展以及对网络安全认知的拓展而不断发展。无论是政界还是业界，都对零信任存在较为广泛的共识。参考谷歌、微软公司等美国主要信息技术企业的研究报告，可对零信任概念做如下定义：

零信任是一种专注于资源保护的网络安全范式，其前提是信任永远不会隐式授予，而是必须持续评估：从不信任，始终验证。零信任结构是实现企业资源和数据安全的端到端方法，包括身份（人和其他实体）、凭据、访问管理、操作、端点、

① John Kindervag, “No More Chewy Centers: Introducing the Zero Trust Model of Information Security,” September 14, 2010, https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf.

托管环境和相互连接的基础设施。

零信任安全架构假定漏洞是不可避免的或可能已经发生，因此它强调将访问限制为所必须的内容，并查找异常或恶意活动。零信任嵌入全面的安全监控；基于风险的细粒度访问控制；系统安全自动化以协调的方式贯穿信息基础设施的各个方面，以便专注于在动态威胁环境中实时保护关键资产特别是数据。这种以数据为中心的安全架构允许将最低权限访问的概念应用于每个访问决策，根据上下文几个因素的组合允许或拒绝对资源的访问。

尽管这一安全理念和架构被命名为“零信任”，但完全零信任是不可能实现的，它真正的意思是没有验证就没有信任。零信任的核心目的是构建国家或企业的信息技术基础设施，以实现这样的目标：即使对手成功地获得了对一台设备或用户凭据的访问权，他们通过网络实现目标的能力也将受到严重抑制，通过提供深度防御，避免对手的网络攻击造成更大的损失。根据上述定义，我们可以确定零信任的以下核心原则：

第一，通用身份验证。即所有用户、设备和服务的通用认证。任何实体（包括外部和内部的用户、设备、应用程序等）在组织的信息技术基础设施内部操作，或与组织的信息技术基础设施外部交互都要经过身份验证。

第二，访问分割。即所有的访问，无论是网络访问、数据访问还是应用程序访问等，都应该被分割成尽可能小的可访问区块，这样就没有单个实体（设备、用户、应用程序等）可以访问组织的整个或大部分网络、数据或应用程序，确保尽可能少的实体能够访问关键数据。

第三，最小信任授权。即只允许“需要知道”和可信任的实体访问资源，并将实体权限限制为执行其任务所需的最少数量的特权（访问、管理权限等）。这不仅包括最小化可以访问的内容，还包括可以访问多长时间以及从哪里访问。

第四，加密无处不在。零信任建立在假设网络不可信的基础之上，这意味着在任何发生通信的地方，都假定对手可能在监视。因此，无论是在组织的网络内部还是外部通信，都应该从端到端加密，以保护流动和静止的信息。

第五，持续监控和调整。即在组织基础设施上运行的所有实体都应受到监控，这包括所有网络流量、访问尝试和成功尝试以及正在运行的软件。监控包括所有网络和系统事件以及不同来源的交叉检查数据。

这五个原则共同构成了零信任的基本内涵，也是实现零信任安全目标的主要手段。零信任的主要目标是在攻击者试图通过组织横向移动以达到预定目标时破坏网

络杀伤链。零信任原则通过两种方式做到这一点。首先，窃听和侦察是困难的，因为端到端加密和通用认证限制了对信息的访问，而持续的监控可以识别异常通信。其次，横向移动减少，因为访问分割和最小权限授权阻止了受损实体访问关键资源。当横向移动受到限制时，内部威胁也会受到限制。①

美国是较早将零信任引入国家网络安全体系的国家，根据零信任安全的基本原则和美国网络安全体系的实际情况，联邦政府公布的《推动美国政府走向零信任网络安全原则》和美国国土安全部网络安全和基础设施安全局制定的《零信任成熟度模型》，② 确立了零安全架构的五大支柱：

第一，身份。对零信任来说，持续的可信用户认证最为重要，是一个机构零信任架构的核心组成。这包括使用身份、凭证和访问管理以及多因素认证等技术，并不断监测和验证用户的可信度，以管理他们的访问和权限，同时采取保障和保护用户互动的技术，如传统的网络网关解决方案等。支持零信任的最小权限访问，取决于确定接收访问用户身份的能力。零信任成熟度模型不再简单地使用密码来验证身份，而是在与服务或数据交互的整个过程中使用多种因素的组合来持续验证身份。

第二，设备。设备是指可以连接到网络的任何硬件资产，包括物联网设备、移动电话、笔记本电脑、服务器等。设备可以是机构拥有的，也可以是自带的。安全主体应盘点设备，保护所有机构设备，并防止未经授权的设备访问资源。设备的实时网络安全态势和可信度是零信任理念的一个基本属性。一些“记录系统”解决方案，如移动设备管理器，提供的数据可用于设备信任评估。此外，还应该对每个访问请求进行其他评估，如检查妥协状态、软件版本、保护状态、加密启用情况等。

第三，网络/环境。网络是指用于传输信息的开放通信媒介，包括机构内部网络、无线网络和互联网。安全主体应分割和控制网络，并管理内部和外部数据流。

---

① Microsoft, *Evolving Zero Trust: How Real-World Deployments and Attacks Are Shaping the Future of Zero Trust Strategies*, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT; Rory Ward and Betsy Beyer, *BeyongCorp: A New Approach to Enterprise Security*, https://static.googleusercontent.com/media/research.google.com/zh-CN//pubs/archive/43231.pdf; K.D. Uttecht, *Zero Trust (ZT) Concepts for Federal Government Architectures*, July 30, 2020, Lincoln Laboratory, MIT, https://apps.dtic.mil/sti/pdfs/AD1108910.pdf.

② 笔者之所以引证这两份文件，原因在于：首先，联邦政府作为美国最高行政当局有很强的权威性。其次，美国国土安全部网络安全与基础设施安全局是负责美国网络安全和基础设施保护的最重要机构，被称作网络安全领域的“国家协调员”，是美国国家网络安全体系的轴心。美国商务部国家标准与技术研究院、美国国防部的“零信任安全架构”，基本上是在上述两份文件的基础上设计的。

零信任网络常常被描述为“无边界”，但情况并非如此。零信任网络实际上是试图将周界从网络边缘移入，并将关键数据与其他数据进行分割和隔离。尽管是以更细化的方式出现，但周界仍然是一个现实。传统的网络安全基础设施——“城堡和护城河”相结合的防火墙模式——是不够的，周界必须与微分界一起向数据靠近，以加强保护和控制。

第四，应用程序和工作负载。保护和正确管理应用层以及计算容器和虚拟机是采用零信任的核心。拥有识别和控制技术的能力有助于作出更细化和准确的访问决定。因此，多因素认证是在零安全环境中为应用程序提供适当访问控制的关键部分。

第五，数据。机构数据应该在设备、应用程序和网络中得到保护。安全主体应对数据进行盘点、分类和标记，保护静止和传输中的数据，并部署检测数据泄露机制。对许多机构来说，开发一种全面、准确的方法来分类和标记数据将是一个挑战。随着各机构转向零信任架构，它们的心态必须转向“以数据为中心的网络安全方法”。①

美国政府确立的零信任安全架构的五大支柱，体现了零信任概念的基本理念：从不相信，始终验证。其强调了对用户身份和设备的持续验证，通过安全主体对网络的控制与分割，实现最小信任授权和对数据的保护。金德维格和网络技术企业的零信任安全概念或架构更多强调的是实现零信任安全目标的手段，美国政府的零信任安全架构则是明确将数据安全置于零信任安全的核心地位，体现了作为管理者的联邦政府与企业考虑问题角度的差异。同时，数据安全也是美国推动网络安全现代化最重要的动因之一。

二　美国政府推动网络安全现代化的动因分析

近年来，由于美国面临的网络安全环境日趋复杂，更新美国网络安全体系的呼声持续上升。从特朗普政府时期开始，一些美国联邦机构如国防部、商务部国家标准与技术研究院等，开始将思考方向转向零信任安全架构，并相继提出了各自的零信任发展战略和零信任架构。拜登就职不到 4 个月，便发布了《改善国家网络安全

① Executive Office of the President, Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf; Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model*, April 2023, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

的行政命令》，明确提出以零信任架构推动美国网络安全的现代化。美国政府加速推进零信任战略，既是网络安全理念和技术迭代的要求，也是数字时代大国竞争的组成部分，同时还是美国国防数字战略现代化的产物。

（一）美国传统网络安全防御系统的失能与网络安全现代化的必要性

信息技术发展与传统网络安全边界（周界）的脆弱性，使得网络安全传统信任模式和理念崩塌，催生出进行网络安全现代化的必要性。

当今的互联网环境是由一个相互连接的世界实现的，其主要特征是相互连通性、用户多样性、设备的丰富性以及应用程序和服务的全球性，这使得互联网世界更容易受到恶意活动的影响。传统的互联网、移动互联网、物联网、云计算等组成的混合网络环境日益复杂，加上各种恶意行为者威胁的快速升级和迭代，暴露了采用多层互不关联的安全技术的传统网络安全防御有效性不足，基于周界的网络防御已无法满足当前威胁环境下的网络安全需求。从网络犯罪分子到民族国家行为体，当代网络威胁行为体变得更持久、更隐秘、更微妙；网络恶意行为者已经展示了有规律地穿透网络外围防御的能力。这些内部和外部威胁行为者，成功地利用他们的权限危害个人用户、企业甚至国家经济安全。即使是最熟练的网络安全专业人员，在保护分散的企业网络免受越来越复杂的网络威胁时也面临着巨大的挑战。

近年发生在美国的典型案件有菲利普·卡明斯（Philip Cummings）事件[①] 和“太阳风”（SolarWinds）事件。[②] 这两个事件充分证明了传统的基于“围墙+卫兵”

① 1999 年到 2000 年，菲利普·卡明斯曾在一家名为 TeleData Communications, Inc.（TCI）的公司工作，为该公司以及 Equifax、TransUnion 和 Experian 等信用机构提供软件服务。因为他支持所有三个信用机构网络的软件，所以有权限访问所有客户的密码和订阅代码。在受雇于 TCI 期间，一个尼日利亚有组织犯罪集团的成员联系了菲利普·卡明斯，并为他提供的每一份信用报告支付 60 美元。卡明斯在技术上很有悟性，他给一台笔记本电脑预先编程，他的犯罪伙伴能够自动从三个信用机构下载信用报告。尽管卡明斯在 2000 年就离职了，但他及其同伙的犯罪活动持续了两年。2002 年，其中一家信用机构 Experian 的客户福特汽车信贷公司在不断接到许多消费者（这些消费者都是身份盗窃和欺诈的对象）的投诉后，卡明斯的犯罪行为才东窗事发。美国政府估计，卡明斯和他的犯罪同伙窃取了大约 3 万个身份，造成至少 270 万美元的直接经济损失。卡明斯事件是美国历史上最大的身份盗窃案。

② 太阳风公司（SolarWinds Corporation）是一家美国公司，为企业和美国联邦政府机构甚至一些重要国际组织开发软件，以帮助管理其网络、系统和信息技术基础设施。2020 年，该公司的软件 Orion 遭到黑客入侵，黑客获得了超级用户访问权限 SAML 令牌签名证书，该 SAML 证书又被用来伪造新的令牌，以允许黑客以受信任的最高权限访问网络，这次攻击的受害者包括网络安全公司 FireEye、多家财富 500 强企业，以及包括美国国务院、国防部、财政部、商务部、国土安全部和国家核安全委员会在内的多家美国联邦政府机构。这次攻击使用了太阳风系统库中的后门，由于证书受到信任，当太阳风系统更新时，恶意攻击难以被发现。

的模式（即设置防火墙区隔内外网，仅查验单次身份后便可在内网自由活动）已经严重失能。前者是凭借在内网中的身份认证就可以在“围墙”内部自由流动，后者则是攻击者成功越过防火墙，获得在“墙内”自由行动的权限，对网络安全造成恶意伤害。

近十年来，美国政府为强化维护国家网络安全的能力和政策，一直试图在原有的网络安全体系基础上，通过小修小补解决美国所面临的网络安全问题。2008 年，白宫管理及预算办公室发布了关于可信互联网连接的备忘录，该备忘录旨在优化个人外部连接，包括美国联邦政府目前正在使用互联网点的连接；2009 年，美国总务管理局（U.S. General Services Administration）也制定了《联邦身份、凭证和访问管理条例》（Federal Identity, Credential, and Access Management，简称 FICAM），该条例的目标是使正确的个人能够在正确的时间、以正确的理由访问正确的资源，与零信任安全的理念已经相当接近。所有这些程序都旨在限制授权方对数据和资源的访问。

上述美国不同政府部门加强网络安全的努力并未取得显著的效果，针对美国个人用户、企业和政府机构的网络攻击依然时有发生。根据美国联邦调查局（FBI）互联网犯罪投诉中心（IC3）2021 年的互联网犯罪报告，勒索软件团伙 2020 年侵入了美国多个关键基础设施部门至少 649 个组织的网络。“在 16 个关键基础设施部门中，IC3 报告显示，其中 14 个部门至少有 1 名成员在 2021 年成为勒索软件攻击的受害者。”[①] 针对关键基础设施的勒索案件涉及美国供水和废水处理系统、食品和农业部门、美国医疗保健和急救网络以及教育机构。巧合的是，在拜登发布《改善国家网络安全的行政命令》前几天，美国最大的燃料管道企业科洛尼尔管道公司（Colonial Pipeline）遭遇了境外勒索团伙的勒索软件网络攻击，导致公司暂时关闭所有运营管道，引发美国部分地区对停电和天然气、汽油、柴油等燃料供应的恐慌。

这一系列事件使美国政府认识到，渐进式的改进无法解决今天美国所面临的复杂的网络安全问题，“为了跟上今天动态和日益复杂的网络威胁环境的步伐，联邦政府必须采取果断措施，使其网络安全方法现代化，包括增加联邦政府对威胁的可见性，同时保护隐私和公民自由。”“联邦政府必须采取安全最佳实践；向零信任体系结构推进；加快安全云服务的发展，包括软件即服务（SaaS）、基础设施即服务（IaaS）和平台即服务（PaaS）；集中和简化对网络安全数据的访问，

① Federal Bureau of Investigation, *Internet Crime Report 2021*, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

以推动分析、识别和管理网络安全风险；并对技术和人员进行投资，以满足这些现代化目标。”[①] 总之，日趋复杂的网络安全问题是美国政府加速推动零信任安全体系的最主要推动力。

（二）数据权力凸显了大国竞争时代数据保护在网络安全中的核心地位

随着数字时代的到来，全球数字经济急速发展，数据作为数字经济的核心要素，已经成为关键性的资源，数据就是权力（Data is Power）。在全球金融危机之后，传统贸易增长趋于平缓，取而代之的是跨境数据流动的爆炸式增长。以带宽衡量，跨境数据流量从 2008 年到 2020 年增长了约 112 倍。[②] 数字时代的全球经济犹如一台永动机般的数据机器，不仅在消费数据、处理数据，同时还在产生新的数据。与全球经济的其他要素相比，数据与权力更加紧密地交织在一起。

首先，数据是创新的重要来源。超级计算、云存储和机器学习的巨大进步，使得数据对创新变得更加重要。人工智能、无人驾驶等新一轮科技革命塑造的技术和产业，无不依赖数据的驱动。

其次，数据驱动着国家经济和产业结构的转型。以在数字技术开发与利用方面走在世界前列的美国为例，20 世纪 80 年代，美国位居世界 500 强的企业多是包括埃克森美孚石油、通用、福特、摩根大通、花旗银行等传统金融和制造业企业。但上述企业的优势地位现在已经被亚马逊、苹果、谷歌、脸书和微软等数字企业所取代。这批在数字时代走在世界前列企业的重要成功秘诀就是它们将来自几十亿人和数以千万计组织的大量数据转化为客户的新经济价值。

再次，数据同样也是国家安全领域备受重视的要素。2019 年 6 月 4 日，白宫管理与预算办公室发布的《联邦数据战略》，将数据视为“一种战略资产”。[③] 数据通过推动生产力的发展，提升了支撑美国军事力量的经济实力。用谷歌前首席执行官、美国人工智能国家安全委员会（The National Security Commission on Artificial Intelligence）主席埃里克·施密特（Eric Schmidt）和美国国防部前副部长罗伯特·沃克（Robert Work）的话说：数据赋能的人工智能将是“几代人以来造福人

① The White House, *Executive Order on Improving the National's Cybersecurity*, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

② Matthew J. Slaughter and David H. McCormick, “Data Is Power: Washington Needs to Craft New Rules for the Digital Age,” *Foreign Affairs*, Vol. 100, No. 3, 2021, p. 54.

③ Office of Management and Budget, *Federal Data Strategy—A Framework for Consistency*, June 4, 2019, https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf.

类的最强大的工具”，但它也将被用于“追逐权力”。[①] 正因如此，数据成为美国推动的大国竞争的重要领域。[②]

美国不仅将中国视为基于数据分析与利用的平台经济的最主要竞争对手，而且还是美国网络安全领域的最主要“威胁”。

在数字经济领域，美国走在世界的最前列，但紧随其后的不再是传统的发达国家而是中国。根据联合国贸易与发展会议（UNCTND）发布的研究报告，数字经济中的财富创造高度集中在中美两国。中美两国占与区块链技术相关的所有专利的75%，占全球物联网支出的 50%；亚马逊、微软、阿里巴巴、谷歌和华为等公司则占据了全球 80%以上的云计算市场。全球七大超级数字平台——微软、苹果、亚马逊、谷歌、脸书、腾讯和阿里巴巴占全球前 70 家最大数字平台总市值的 2/3。[③] 从近年的情况看，除了中国，其他国家连与美国进行竞争的机会都没有，美国自然视中国为数据竞争场域的最主要对手。

美国政府认为，中国近年来加大了通过合法和非法渠道收集外国数据的力度。美国国土安全部颁布的《数据安全商业警告：涉华数据服务及设备商业风险》报告，指责中国“资助的数据盗窃不仅加速了外国竞争对手在中国国内市场份额的减少，还加速了中国技术在国际市场的主导地位——包括航空航天、半导体、机器人、人工智能系统、生物识别、网络智能、基因组学、药物和可持续/绿色能源材料等领域”。[④] 拜登政府颁布的《国家网络安全战略》，也指责包括中国在内的所谓“具有修正主义意图”的国家积极利用先进的网络能力，“威胁美国的国家安全和经济繁荣”，“对政府和私营部门网络构成了最广泛、最活跃和最持久的威胁”。[⑤]

① Matthew J. Slaughter and David H. McCormick, “Data Is Power: Washington Needs to Craft New Rules for the Digital Age,” *Foreign Affairs*, Vol. 100, No. 3, 2021, p.57.

② 相关分析详见刘国柱、尹楠楠：《印太经济框架下美国与东南亚的战略互动：以数字经济场域为聚焦》，《南洋问题研究》2023 年第 1 期；杨楠：《美国数据战略：背景、内涵与挑战》，《当代美国评论》2021 年第 3 期。

③ United Nations Conference on Trade and Development, *Digital Economy Report 2019*, https://unctad.org/system/files/official-document/der2019_en.pdf.

④ U.S. Department of Homeland Security, *Data Security Business Advisory: Risks and Considerations for Businesses Using Data Service and Equipment: From Firms Linked to the People's Republic of China*, https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

⑤ The White House, *National Cybersecurity Strategy*, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

加强对数据的保护是美国零信任战略的核心。拜登发布的行政命令也强调:“联邦政府必须充分利用权力和资源来保护和保障其计算机系统的安全,无论它们是基于云的、内部的还是混合的。保护和安全的范围必须包括处理数据的系统(信息技术),以及运行系统的重要机器(操作技术),这些系统确保我们安全。”① 这也从另一个侧面体现了零信任战略与数字时代大国竞争的关系,即通过零信任战略的推进,确保美国在数据竞争场域的优势地位。

(三)零信任与美国国防数字战略的现代化

美国国防系统在世界上最早实施数字化转型,基于互联网的信息技术在此过程中发挥着至关重要的作用。随着世界主要大国均在致力于提高信息战能力,为应对日益严峻的挑战,美国国防部于 2019 年 7 月制定了 2019—2023 财政年度的《国防部数字现代化战略》。该报告认为,现代战场空间已经延伸到太空和网络空间,预计这些领域对手的能力将在未来的战略环境中扩展,从而加剧所有领域内和跨领域的竞争。为了在新的数字作战环境中保持和扩大美国的军事优势,美国军队必须具有适应性和创新性,并能够在多个地区和所有领域无缝运用其能力。尽管网络安全威胁持续存在,但敏捷、有弹性、透明、无缝和安全的信息技术基础设施和服务至关重要,必须能够将数据转化为可操作的信息,并确保执行任务的可靠。但是美国在常规和战略武器方面的优势,正在被网络空间内的复杂攻击以及针对内部人士的情报行动所弱化甚至抵消。美国国防部提出了“网络安全优先,网络安全至上”(Cyber First, Cyber Always)的理念,在一个有争议的网络空间中保卫美国国防系统,要求“每个网络、系统、应用程序和企业服务都必须通过设计实现安全,并在整个收购生命周期中进行网络安全管理”。②

显然,美国国防系统同样面临着日益复杂的网络安全问题。随着网络规模和复杂性的增长,需要大量的快速数据传输,以保持对数字和物理战场的态势感知。这种快速的数据传输对国防部未来能力的发展和增强态势感知至关重要。应用于国防部系统的人工智能和机器学习将依赖于这种数据流,反过来又会促成从弹性卫星群到网状网络的一系列新技术和任务。在这个不断扩大的网络中,每一个增加的端点

① The White House, *Executive Order on Improving the National's Cybersecurity*, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

② Department of Defense, *DoD Digital Modernization Strategy*, July 12, 2019, https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF.

和数据传输都会为对手创造新的机会。随着攻击面的扩大，周界安全将越来越不堪重负，并且可能会允许更多未经授权的用户溜进美国国防网络系统。如果不改变网络安全战略，国防部将面临损害其数据、网络和业务的风险。

为克服这些挑战，美国国防部在《国防部零信任战略》中提出要尽快落实零信任原则，在零信任基础上建立更加强大的网络安全框架，并要求美国整个国防系统，“以‘永不信任，始终验证’的心态来保障设备、应用程序、资产和服务的安全”。必须确保“当对手试图攻破我们的零信任防御体系时，他们会发现再也无法在我们的网络中来去自如，更无法妨碍我们向作战人员提供最大限度的支持”。[①]

三　美国政府基于零信任的联邦网络安全现代化战略布局

针对美国联邦机构、私营部门和个人频频发生的网络攻击事件，暴露出美国现有的网络安全防御体系以及网络危机应急能力的不足。美国政府认为，必须更加积极地构建零信任网络安全生态系统，保护美国关键数据资源的绝对安全，并积极培育美国社会的零信任网络安全共识。从联邦政府到国防部、国家安全局等美国政府机构，相继发布了推动在美国联邦机构和美国社会构建零信任安全体系的战略性文件。拜登政府加强了基于顶层设计的网络安全宏观布局，确立了实施零信任战略的关键事项；明确了联邦政府推动零信任安全体系的基本原则；将关键基础设施、国家安全系统和国防系统作为推动零信任安全框架的核心领域；确立了以网络安全和基础设施安全局为轴心的推动零信任布局的“全政府”架构。

（一）美国政府基于顶层设计的零信任网络安全体系宏观布局

拜登政府通过颁布《国家网络安全战略》和《改善国家网络安全的行政命令》两份重要文件，对推动以零信任为核心的网络安全现代化进行了宏观布局。

1．拜登政府确立了网络安全现代化的总体目标

拜登政府网络安全现代化的总体目标是：“建立一个可防御的、有弹性的数字生态系统，在这个生态系统中，攻击系统比保护它们的成本更高，敏感或私人信息得到安全和保护，并且事件或错误都不会导致灾难性的系统性后果。”[②] 为此，联

① Department of Defense, *DoD Zero Trust Strategy*, October 21, 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf.

② White House, *National Cybersecurity Strategy*, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

邦政府将通过使美国的网络系统更具防御性和弹性，以更好地支持关键基础设施的防御。美国政府承诺：致力于通过长期努力实施零信任架构战略，并使信息技术和在线数字操作技术基础设施现代化来改善联邦网络安全。通过美国政府的示范作用，联邦网络安全将成为美国关键数字基础设施的基本模型，用于成功构建和运行安全且有弹性的系统。

2．明确了联邦政府推动零信任安全框架的路径

为推动联邦网络安全系统现代化，明确了联邦政府推动零信任安全框架的路径。新的《国家网络安全战略》要求，联邦政府各个部门必须更换或更新无法抵御复杂网络威胁的信息技术和在线数字操作技术系统，包括授权白宫管理与预算办公室，以零信任安全战略指导联邦文职行政部门（FCEB）实施多因素身份验证、加密数据、了解整个攻击面、管理授权和访问并采用云安全工具。白宫管理与预算办公室还将领导制定一项为期多年的计划，以加速联邦文职行政部门网络安全的现代化，消除所有无法在十年内实施零信任架构战略的遗留系统，或者以其他方式减少那些在规定时间内无法被替换系统的风险。此外还使用更安全的技术取代遗留系统，包括通过加速向基于云的服务的迁移，提升整个联邦政府的网络安全态势，进而提高联邦网络安全系统为美国公私部门及民众提供数字服务的安全性和弹性。

3．确立了在不同领域推动零信任安全框架的工作重点

根据联邦政府的网络安全战略和总统行政命令，确立了在不同领域推动零信任安全框架工作重点。白宫管理与预算办公室先后发布了五项关于保护关键软件、日志记录、端点检测和响应、零信任架构和软件供应链的政策备忘录。这些政策包括：

M-21-30，即“通过增强的安全措施来保护关键软件”备忘录。以美国商务部国家标准与技术研究院发布的指导和安全标准，通过增强的安全措施保护关键软件。[①]

M-21-31，即“提高联邦政府与网络安全事件相关的调查和补救能力”的备忘录。规定了日志管理、配置和企业级集中的详细要求，并且提供了一个成熟度模型，对最关键的软件类型和需求进行优先级排序。[②]

M-22-01，即“通过端点检测和响应，改进联邦政府系统中网络安全漏洞和事

① Office of Management and Budget, “M-21-30, Protecting Critical Software Through Enhanced Security Measures,” August 10, 2021, https://whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf.

② Office of Management and Budget, “M-21-31, Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents,” August 27, 2021, https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf.

件的检测”备忘录，要求联邦政府各部门加速采用强大的端点安全解决方案，这是零信任架构的一个重要组成部分，端点检测和响应将端点数据（如工作站、移动电话和服务器等联网计算设备）的实时连续监控和收集，与基于规则的自动响应和分析能力相结合。[①]

M-22-09，即“推动美国政府走向零信任网络安全原则”备忘录，提出了美国政府推动零信任网络安全原则：假定组织范围内的任何人或设备都是不可信的，将联邦政府迁移到新的网络安全范式，并将各机构的重点放在加强其限制和持续验证人和设备访问政府数据的能力上。[②]

M-22-18，即“通过安全的软件开发实践来增强软件供应链的安全性”。旨在启动政府范围内的转变，要求各机构使用以安全方式开发的软件。最大限度地降低在机构网络上运行未经验证的技术所带来的风险，提高联邦技术对网络威胁的抵御能力。[③]

此外，在联邦政府公布了“关于促进美国在量子计算领域的领导地位，同时降低对脆弱密码系统风险的国家安全备忘录”后，白宫管理与预算办公室与美国国土安全部网络安全和基础设施安全局、商务部国家标准与技术研究院、美国国家安全局等部门合作，为各机构制定要求，优先考虑并确定它们在最敏感的系统中使用加密技术的位置，因为这些系统很容易被未来的量子计算机解密。[④]

（二）美国政府推动零信任安全战略的核心领域

美国政府推动的零信任安全战略主要集中在关键基础设施、国家安全系统和国防部系统三个领域。

---

① Office of Management and Budget, “M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response,” October 8, 2021, https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf?ref=hackernoon.com.

② Office of Management and Budget, “M-22-09, Moving the U.S. Government toward Zero Trust Cybersecurity Principles,” January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

③ Office of Management and Budget, “M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices,” September 14, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf.

④ The White House, “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Minigating Risks to Vulnerable Cryptographic System,” May 4, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

1．关键基础设施

保护关键基础设施的安全，是拜登政府国家网络安全战略的第一支柱。随着物联网、工业互联网、云计算和各种信息技术迭代的加速，传统的物理世界与数字世界的分野已经被打破，万物互联变得越来越普遍。传统的基础设施如电网、油气管道、工厂、金融企业、城乡水处理设施以及其他关键的基础设施逐渐淘汰旧的模拟控制系统，在线数字操作技术正在被引入越来越多的行业和社会治理机构。以超大容量、超高速度、超低延迟为主要特征的新一代移动通信技术，更是带动了众多支持民用和军用的基础设施如无人驾驶、远程医疗等系统。

上述基于互联网技术的经济与社会活动，推动越来越多的公共基础设施处于在线状态，使得网络攻击对政府工作、企业日常运转和公众日常生活等方面更具破坏力和影响力。美国政府必须让民众认识到“保护构成我们关键基础设施的系统和资产对我们的国家安全、公共安全和经济繁荣至关重要”，要对关键基础设施及其所提供的“基本服务的可用性和弹性充满信心”。[①] 零信任安全框架就是要为这些关键基础设施的所有者和运营商提供基础级别的安全性和弹性，让网络上的恶意行为者难以实现他们的目的。

拜登政府保护关键基础设施的一个重要举措就是扩大公私合作。代理国家网络主管肯巴·沃尔登（Kemba Walden）指出：“我们对关键基础设施的所有者和运营商寄予更多期望……因为互联网现在基本上是全球公域。因此，我们对私营部门、非营利组织和行业的合作伙伴期望更高。”[②] 这意味着美国将重构网络契约，至少在网络安全领域让美国私营企业承担更大和更多的责任。

2．国家安全系统

自网络安全问题出现以来，国家安全系统（National Security System, 简称 NSS）一直是美国政府给予特别关注的领域。拜登政府颁布了《改善国家安全、国防部和情报系统网络安全的备忘录》，授权负责运作“国家安全系统委员会”（Committee on National Security Systems，简称 CNSS）的国家安全局局长，制定并发布关于与 CNSS 云迁移和运营相关的最低安全标准和控制指南，要求拥有或运营国家安全系统的每个行政部门或机构负责人应根据其法定权限，更新现有机构计划，优

① The White House, *National Cybersecurity Strategy*, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023. Pdf.

② Divid E. Sanger, “New Biden Cybersecurity Strategy Assigns Responsibility to Tech Firms,” March 2, 2023, https://www.nytimes.com/2023/03/02/us/politics/biden-cybersecurity-strategy.html.

先考虑采用和使用云技术的资源。同时，要根据国家标准技术研究院和国家安全系统委员会的零信任框架体系，在可行的情况下采用零信任架构；还规定在本备忘录发布之日起 180 天内，各机构应对国家安全系统静止数据和传输数据实施多因素认证和加密，并要求所有联邦机构使用国家安全局批准的、基于公共标准的加密协议。

备忘录要求，国家安全局局长应与国家情报总监、中央情报局局长、联邦调查局局长以及国防部相关部门负责人协调和制定一个框架，以处理与国家安全系统商业云技术相关的网络安全和事件，确保国家安全系统各机构、国家安全局局长和云服务提供商之间的有效信息共享。①

3．国防部网络

鉴于国防领域的特殊性，国防部在美国网络安全现代化体系中有突出的地位。白宫要求美国国防部制定与美国国家安全战略、国防战略和国家网络安全战略保持一致的、具有前瞻性的部门网络战略，以做到深入了解威胁行为者，识别和暴露恶意软件，并在恶意活动影响其预定目标之前将其破坏。

国防部零信任框架必须优先支持和加强国防部所有级别的战斗人员关键作战能力，适用于所有军事多域作战（网络、空间、空中、地面和海上）和支持业务资产。零信任通过确保美国军队的数据、应用程序、资产和服务的安全性，以实现战术环境中通信频谱中的制信息权。

国防部构想了一个可扩展的、弹性的、可审计的和可防御的环境，其核心是为国防部的数据、应用程序、资产和服务提供安全保护。其重要步骤如下：

第一，采用零信任文化。以零信任安全架构和思维方式，指导整个国防部零信任生态系统的信息技术设计、开发、整合和部署。国防部所有工作人员都要理解和接受零信任思维和文化，接受相关培训，并支持将零信任技术集成至国防信息环境中。第二，加强国防部信息系统的安全和防御。国防部网络安全实践采纳并实施零信任，以实现国防部信息系统的弹性。第三，技术加速。国防部基于零信任的技术部署速度等于或超过行业发展速度，以保持在不断变化的威胁环境中的领先地位。国防部信息企业及各机构应与零信任工作保持一致，包括开发测试、确保可互操作的标准和资产。第四，零信任授权。国防部执行零信任框架要集成部门与机构间的

① The White House, “Memorandum on Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems,” January 19, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/.

流程，从而实现零信任的无缝、协调执行。这要求部门与机构级的流程和资源必须重新设计或同步零信任原则和方法。[①]

（三）构建全政府全社会网络安全协调机制

面对越来越复杂和严峻的网络安全形势，特朗普政府开始加强联邦政府内部不同机构之间、联邦政府与地方政府之间网络安全方面的协调。2018 年 11 月 16 日，特朗普签署了《2018 年网络安全和基础设施安全局法案》，将美国国土安全部的“国家保护和计划局”（NPPD）更名为“网络安全和基础设施安全局”。该局负责加强各级政府的网络安全和基础设施保护，并与美国各州协调网络安全计划，提高各级政府的网络安全水平，防范个人和有组织黑客对美国关键基础设施的攻击。[②] 该局在加强跨部门合作，增强国家在网络空间的弹性等方面发挥着越来越重要的作用，被视为“联邦网络安全团队的四分卫”。[③]

拜登政府同样看重网络安全和基础设施安全局在美国网络安全体系中的地位和作用，将其视为“关键基础设施安全和弹性的国家协调员”。拜登政府的《国家网络安全战略》继续加强该局与美国其他风险管理机构的协调，使联邦政府能够实现与美国所有关键基础设施所有者和运营商的完美协作。为实现这一目标，美国政府在网络安全和基础设施安全局建立了联合网络防御协作组织（JCDC），以整合联邦政府以及私营部门和国际合作伙伴的网络防御规划和运营；加强国家网络调查联合特遣部队（NCIJTF）协调执法和阻止其他破坏行动的能力；重振网络威胁情报集成中心（CTIIC）在协调情报收集、分析和合作伙伴关系方面的作用。[④]

根据美国《国家网络安全战略》的精神，网络安全和基础设施安全局制定了《CISA 战略计划：2023—2025》，利用该机构的召集权限和关系管理能力，扩大和强化与利益相关者的合作伙伴关系，加强全国性运营协作和信息共享机制。

第一，确立了优化利益相关者参与伙伴关系活动的合作计划和行动。为更好体现合作伙伴关系的价值，网络安全和基础设施安全局在美国联邦机构、风险管理机

---

① Department of Defense, *DoD Zero Trust Strategy*, October 21, 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf.

② 115 Congress, Public Law 115-278, https://www.govinfo.gov/content/pkg/PLAW-115publ278/pdf/PLAW-115publ278.pdf.

③ 四分卫是美式橄榄球（又称美式足球）中的一个战术位置，属于进攻组的一员，位于中锋的后面、进攻阵型的中央。通常发挥临场指挥的作用，大部分的进攻由四分卫发动。

④ The White House, *National Cybersecurity Strategy*, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

构以及更广泛的利益相关者群体中规划、优先考虑和协调利益相关者参与零信任战略行动。

第二，将区域办事处完全纳入网络安全和基础设施安全局的运营协调。网络安全和基础设施安全局区域办事处工作人员对于成功推广零信任网络安全起到至关重要的作用，通过加强总部与提供全国接触点的区域工作人员之间的整合，建立协调总部各部门和地区之间参与活动的流程，相互支持运营关系管理。

第三，向利益相关者开放网络安全和基础设施安全局项目、产品和服务的政策。通过为联邦机构的利益相关者提供必要的洞察力，以便就资产、系统和企业层面的网络和物理基础设施降低风险，对其防御和恢复能力作出及时、明智的决策。

第四，加强与合作伙伴的信息共享。为了提高利益相关者的态势感知能力，网络安全和基础设施安全局加强了与外部合作伙伴的多向沟通，包括及时报告事件以及共享威胁和漏洞、情报和情报需求以及其他信息和数据。[①]

从特朗普政府时期启动，拜登政府持续推进，大致形成了以零信任安全为原则的美国网络安全现代化框架。美国联邦机构也在紧锣密鼓地推进这一进程，以期在网络安全现代化领域走在世界各国前列，为美国网络安全打造坚固的盾牌。

四　美国零信任网络安全战略的特征

经过特朗普和拜登两届政府的努力，美国实现零信任安全战略的路线图被勾勒出来，零信任安全战略的特征逐渐清晰。总体来看，美国零信任网络安全战略呈现出以下几个基本特征：

（一）零信任是一种文化

零信任不仅仅是一种技术，而且还是网络安全设计方法的转变，这是一种文化。作为一套不断发展的网络安全模式，零信任架构将防御从静态的、基于网络的边界转移到用户、资产和资源上。零信任架构的核心假设是：不会仅仅根据资产或用户的物理或网络位置（即局域网与互联网）或对资产的所有权（企业或个人拥有的资产）给予资产或用户隐含的信任。这一理念的转变是当前遗留的身份验证和安全机制的一个重大变化，也是一个重大的文化变革。正如美国《国防部零信任战略》所指出的，国防部保护和保障美国国防部信息设备，不能仅靠技术解决；它需要改变

① Cybersecurity and Infrastructure Security Agency, *CISA Strategic Plan 2023-2025*, September 2022, https://www.cisa.gov/sites/default/files/2023-01/StrategicPlan_20220912-V2_508c.pdf.

思维方式和文化，从国防部的领导到任务操作员，涵盖所有的国防部信息设备用户。“虽然保护数据是零信任的核心，但成功实施我们的零信任框架需要整个部门理解和接受零信任文化。”① 美国国防部发布的《2023 年国防部网络战略》（概要）表示，国防部将采取行动培育网络安全文化和网络意识。“我们将建立这样的期望：高级军事和文职领导人在网络安全问题上具有基本的流畅性。美国防部将开发、资助和实施不同级别的专业军事和民事教育的技术课程，重点是将军和高级行政人员领导力课程。更广泛地说，我们将确保各级军人适当了解网络问题，将网络教育要求纳入委任来源和入伍培训计划的课程中。”②

与任何新举措一样，员工的理解与支持对于零信任接受度至关重要。机构首先要建立用户意识，教育员工了解采用零信任背后的原因。具有网络安全意识的员工才能了解零信任，愿意接受它，并在日常工作中严格执行零信任的相关规则。由于威胁形势总是在不断变化，维持零信任环境需要持续创新。为了保持领先地位，政府机构需要了解形势正在如何变化，并不断适应这些变化。这不仅需要更新它们的能力和架构，还需要更新它们的用户意识和培训内容。一旦员工和用户意识到网络攻击者可以利用的常见攻击向量或弱点，以及涉及可以诱骗用户泄露其身份验证信息精心设计的骗局，他们将自动了解新的增强安全措施的必要性。零信任首先是一种文化，已经成为美国联邦机构的一种普遍认知。美国卫生与公共服务部（HHS）在推动联邦政府零信任战略时，一开始就使开发团队成为零信任和网络实践的一部分。其手段是，通过对以零信任为中心的员工进行培训——“零信任 101”培训，宗旨是对每个人进行零信任教育，并使该系统的所有用户成为零信任的一部分，以便他们能够适应这些概念。美国卫生与公共服务部官员反复强调，在实施零信任安全架构时，真正的改变不是技术，而是组织内部的“文化改变”，③ 即构建强大、稳定和深入人心的安全文化。

（二）零信任网络安全以数据安全为中心

保护穿越和存储在网络中的数据是任何网络价值的一个主要部分。保护所有的数据，无论是静态的还是动态的，都是零信任架构的主要支柱。有助于这种保护的

① Department of Defense, *DoD Zero Trust Strategy*, October 21, 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf.

② U.S. Department of Defense, *2023 Cyber Strategy of the Department of the State* (*Summary*), https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

③ Grace Dille, “Zero Trust is a ‘Cultural Change’, not a Tech Change, HHS Official Says,” April 14, 2022, https://www.meritalk.com/articles/zero-trust-is-a-cultural-change-not-a-tech-change-hhs-official-says/.

关键技术包括加密、虚拟私人网络和数据丢失预防功能。通过依靠零信任架构，强调识别高价值的数据，并对其进行优先保护。同时在零信任架构的支持下，各级操作人员也会相信访问的数据、部署的资产、使用的应用程序和提供的服务都是安全且有弹性的。麻省理工学院林肯实验室的专家古普雷特·巴蒂亚（Gurpreet Bhatia）在谈到作为一种文化变革的零信任安全理念时认为："零信任要求不仅要保护我们的设备和其他电子产品，还要保护我们皇冠上的宝石——数据，这是一种真正的新方法，我们将数据置于宇宙的中心，用正确的机制、控制、政策和治理来包围和保卫它，以确保我们能够做所有我们需要做的事情……能一路顺利完成使命。"①

根据上述理念，《国防部零信任战略》要求国防部信息企业建立零信任能力，该能力必须在由七个零信任支柱及附加因素构成的组织架构内进行开发、部署和运行，以确保标准化执行。这些支柱为国防部零信任安全模型和零信任体系架构奠定基础，而附加因素则是跨领域、非技术的能力和活动，涉及文化、治理和国防部零信任资产组合管理办公室的其他要素（如零信任培训等）。该模型的核心是支柱内所有能力必须以整合方式工作，以有效地保障数据支柱的安全。②

（三）零信任是一个动态的渐进的过程

实现零信任架构是一个过程，而不是基础设施或流程的大规模替换。零信任安全战略要求美国联邦机构应逐步实现零信任原则下的流程变更和技术解决方案，以保护其最高价值的数据资产。以美国国防部为例，《国防部零信任战略》目标级零信任（The Target level ZT）是保护国防部数据、应用程序、资产和服务安全，管控已知威胁带来的风险所必须采取的行动和零信任能力的最小值。虽然国防部零信任框架将随着时间的推移而完善和适应，但目前的战略背景要求将重点放在加快对零信任核心能力和技术的投资上，国防部及其相关部门必须尽快达到目标级零信任。

随着目标级零信任的实现，国防部零信任资产组合管理办公室（ZT PfMO）将监督执行情况，并在国防部减轻当前风险的情况下，引导向更先进的零信任发展。着眼于继续向新一代安全体系架构的发展，为解决恶意攻击者给国防部带来的新型威胁，ZT PfMO 还可能修改此策略对目标级零信任的定义。

实现上述目标并非意味着零信任安全框架的完善与结束，零信任安全架构将随

① Maria Briggs, "Changing the Culture of Cybersecurity with Zero Trust," April 18, 2023, https://www.dau.edu/News/Changing-the-Culture-of-Cybersecurity-With-Zero-Trust.

② Department of Defense, *DoD Zero Trust Strategy*, October 21, 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf.

着对手攻击的接近、向量因时间的推移而发生变化，攻击面的保护需要继续调整和完善。

（四）零信任安全架构与美国现有的网络安全架构相辅相成

美国现有的联邦网络安全政策和指导与零信任架构的规划、部署和操作相互交叉。当零信任架构与现有的网络安全政策和指导方针相辅相成时，其将会加强联邦机构的安全态势，并防范常见威胁。

首先，零信任架构的部署涉及围绕指定任务或业务流程制定访问策略。系统拒绝对资源的所有网络访问，只允许通过连接的终端进行访问，但对于一个联邦机构来说，执行任务的风险是可以接受的。必须确定和评估与执行既定任务有关的风险，并接受或减轻风险。为此，美国国家标准与技术研究院开发了风险管理框架。零信任架构可能会改变企业定义的授权边界，并减少对网络外围防御的依赖。但风险管理框架中规划的整个过程在零信任架构中不会改变。

其次，零信任架构与国家标准与技术研究院的隐私框架。保护用户的隐私和私人信息是国家安全系统的主要关注点，为此，美国国家标准与技术研究院制定了供联邦机构使用的隐私框架。零信任的核心需求之一是企业应该在其环境中检查和记录流量，其中一些流量可能包含私人信息或存在相关的隐私风险。国家标准与技术研究院的隐私框架正在帮助开发一个正式的流程，以识别和减轻企业在开发零信任架构时的任何与隐私相关的风险。

再次，零信任架构与联邦身份、凭证和访问管理体系结构。主题配置是美国零信任架构的一个关键组成部分，零信任架构需要有强大的主题提供和身份验证策略。美国管理与预算办公室发布了关于改善联邦政府身份管理的备忘录，呼吁所有联邦机构成立一个身份、凭证和访问管理办公室，管理与身份发放和管理有关的工作。鉴于零信任安全架构严重依赖于精确的身份管理，意味着联邦推动零信任安全体系必须要整合该机构的身份、凭证和访问管理政策。

此外，联邦政府的可信互联网连接 3.0、国土安全部持续诊断和缓解计划、国家网络安全保护系统、云智能和联邦数据战略等，都可以与零信任安全架构交互操作、相辅相成，共同推动美国网络安全的现代化。[①]

（五）零信任不仅是美国网络安全的防御战略也是网络进攻战略

一方面，通过构建以零信任架构为基础的现代化网络安全体系，为美国以互联

① National Institute of Standards and Technology, *Zero Trust Architecture*, August 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

网为基础的数字系统打造一个坚硬的“外壳”，让竞争对手和网络攻击者——无论是国家行为体还是非国家行为体，都难以攻破美国无数层保护伞保护下的关键基础设施和关键数据，以避免对美国互联网、物联网、云计算造成系统性的破坏；另一方面，在确保美国自身网络安全系统稳固的情况下，美国可以在网络安全领域无所顾忌地向对手发起攻击。从这个角度看，美国推动的零信任网络安全战略，与里根政府推动的战略导弹防御计划有异曲同工之处，颇有网络安全领域的“星球大战计划”味道。

拜登政府新版《国家网络安全战略》公开表达了美国网络安全战略的攻击性：“美国将使用国家权力的所有工具来瓦解和摧毁威胁我们利益的行为者”，让恶意行为者无法发动持续的网络活动和威胁美国的国家安全或公共安全。[①] 联邦执法机构率先将国内法律机构与私营企业以及国际盟友和合作伙伴进行整合部署，以破坏在线犯罪基础设施和资源，包括从摧毁名声不佳的僵尸网络到没收从勒索软件和欺诈活动获取的加密货币。同样，国防部和情报界致力于将其全方位的互补权力用于防止破坏活动。

拜登政府网络安全战略中的攻击性是 2018 年美国国防部网络安全战略“防御前置”的延续，“防御前置”强调采取先发制人的行动，授权美国网络安全人员在美国境外的网络上运行，在威胁到达美国国内网络之前发起攻击。很明显，所谓的“防御前置”就是打着防御旗号的攻击性行为。

美国在网络安全领域的攻击性行动并非仅仅针对世界上所谓的“恶意行为者”，被美国视为不同领域的竞争对手也在美国的攻击范围内。美国在网络安全领域的历史并不光彩，斯诺登所披露的美国中央情报局的“棱镜计划”，即是美国对其他国家进行网络攻击和监控的缩影。拜登上台以来，美国对中国重要机构的网络攻击也呈上升趋势。2022 年 6 月，美国国家安全局特定入侵行动办公室（TAO）对包括西北工业大学在内的中国网络目标实施了上万次的恶意网络攻击，控制了相关网络设备（网络服务器、上网终端、网络交换机、电话交换机、路由器、防火墙等），疑似窃取了高价值数据。[②] 2023 年 7 月 26 日，武汉市应急管理局地震监测中心报警称，该中心部分地震速报数据前端台站采集点网络设备被植入后门程序。经国家

① Department of Defense, *DoD Zero Trust Strategy*, October 21, 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf.

② 国家计算机病毒应急处理中心：《西北工业大学遭美国 NSA 网络攻击事件调查报告（之一）》，https://www.cverc.org.cn/head/zhaiyao/news20220905-NPU.htm。

计算机病毒应急处理中心和奇虎 360 公司组成联合调查组调查取证，在该单位的网络中发现了技术非常复杂的后门恶意软件，该软件与美国情报机构常用的攻击性软件有相似之处，具有很强的隐蔽性。通过对恶意软件的功能和受影响的系统判断，攻击者的目的是窃取地震监测相关数据，具有明显的军事侦察目的。[①] 美国在网络安全领域攻击性的增强，将给包括中国在内的世界其他国家的网络安全带来更大的压力。

结　语

美国推动基于“永不信任，始终验证”原则的零信任网络安全战略，无疑将会有效提高美国的网络安全水平。由于网络的分割和用户被授予有限的访问权，实施零信任架构将减少漏洞的影响。较小的漏洞影响将减少业务中断并保持较低的修复成本。分割是限制漏洞影响范围的关键技术，将访问限制在只有个别用户需要访问的网络区域，有助于减少漏洞的影响。通过严格授予的访问权限，将最大限度地减少网络攻击者的攻击面，潜在入侵者获得未经授权的访问将变得更加困难。这种更高级别的安全性在当今的技术环境中尤为重要，因为网络威胁不仅更加普遍，而且也变得更加复杂。

零信任是美国网络安全现代化的重要组成部分，但并非全部。作为美国网络安全整个链条中的一环，零信任更多体现在网络安全的“软性”领域。正如美国联邦机构普遍认知的，零信任不仅仅是技术，更主要是一种文化。但在大国竞争的格局中，美国政府对于网络安全“硬”的一面也同样重视。特朗普政府推出并为拜登政府所沿用的“清洁网络”（Clean Network）计划，号称“以国际公认的数字信任标准为基础”，“解决专制恶意行为者对自由世界构成的数据隐私、安全、人权和原则性协作的长期威胁”。“清洁网络”所涵盖的清洁载体、清洁商店、清洁应用程序、清洁的云、清洁电缆、清洁路径，既包括零信任安全架构所涉及的硬件，也触及零信任安全架构相关的软件。[②] 二者共同构成了完整的美国网络安全现代化体系。

网络安全也是中国国家安全的重要组成部分，习近平总书记指出：“没有网络

① 邵艺博：《外交部发言人回应武汉市地震监测中心遭受网络攻击》，《新华每日电讯》2023 年 7 月 27 日，第 7 版。

② Department of States, *The Clean Network*, https://2017-2021.state.gov/the-clean-network/index.html.

安全就没有国家安全。”[①] 与美国相比，中国面临着更为复杂和严峻的网络安全形势。面对互联网技术领先国家网络安全现代化形成的压力，中国更应增强忧患意识，做到未雨绸缪，积极构建中国现代化的网络安全体系。可喜的是，基于零信任架构的网络安全理念已被中国政府机构和网络安全企业接受。2019 年 9 月 27 日，工业和信息化部公布了《关于促进网络安全产业发展的指导意见（征求意见稿）》，将零信任安全列入“着力突破网络安全关键技术”。2019 年 7 月，由腾讯公司牵头的“零信任安全技术参考框架”获 CCSA 行业标准立项。2021 年 7 月，腾讯公司牵头起草中国第一部《零信任系统技术规范》，填补了国内零信任领域的技术标准空白，同时该规范也入选了中国电子工业标准化技术协会团体标准。基于零信任的网络安全试点工作也已经启动。

作为数据大国，中国社会正在加速向数字化和智能化转型。但中国信息化发展存在着不充分、不平衡的特点，尤其是不同行业和领域之间差异较大。在信息安全领域，不仅大量存在无效防护和防护缺失的情况，而且从政府机构到企业再到个人，信息安全意识普遍亟待提高。这就要求政府机构、企业、网络安全工作人员共同努力，牢牢把握国际网络安全发展的脉动，打造中国自主可控、安全便捷的现代化网络安全体系。

【来稿日期：2023-09-17】
【修回日期：2023-10-15】
【责任编辑：谭秀英】

① 中共中央党史和文献研究院编：《习近平关于总体国家安全观论述摘编》，中央文献出版社 2018 年版，第 166 页。

Abstract

[Abstract] Zero Trust is a cybersecurity paradigm based on the premise that trust is never implicitly granted but must be continuously validated. This security paradigm that focuses on resource protection has emerged with the expansion of digital applications such as the Internet, Internet of Things, big data and cloud computing. The core principles of Zero Trust architecture include universal identity verification, access segmentation, least trust authorization, pervasive encryption, continuous monitoring, and adaptation. Identity, devices, networks, applications and workloads, as well as data constitute the pillars of Zero Trust architecture. The U.S. government is accelerating the implementation of distinct Zero Trust capabilities and activities, driven by the need to modernize its traditional cybersecurity systems, adapt to evolving cybersecurity concepts and technologies, and compete as a major player in the digital age. Zero Trust architecture is also crucial for the modernization and informatization of the U.S. defense digital strategy. The U.S. government has strengthened its top-level cybersecurity layout, outlined key initiatives for implementing its Zero Trust strategy, and highlighted basic principles in advancing its Zero Trust security system at the federal government level. As a result, key infrastructure projects, national security systems and defense systems are regarded as core areas for the implementation of Zero Trust architecture, which has contributed much to the establishment of a "whole-of-government" framework with the Cybersecurity and Infrastructure Security Agency as the pivot. Giving more attention to data security than cybersecurity, Zero Trust is not only a technology issue, but also a matter of culture concerning the shift in cybersecurity design approaches. At the same time, Zero Trust is both a cybersecurity defensive strategy and an offensive one, allowing organizations to secure themselves and launch attacks against their adversaries without hesitation. The United States is greatly enhancing its offensive capabilities in the field of cybersecurity, which will put greater pressure on other countries. Against this backdrop, collaborative efforts are called for from Chinese government agencies, enterprises, and cybersecurity professionals to build a modern, autonomous, and secure cybersecurity system in China.

[Keywords] Zero Trust, key infrastructure, cybersecurity, data strategy

[Author] LIU Guozhu, Professor, Institute of World History and Research Center for Non-Traditional Security and Peace Development, Zhejiang University (Hangzhou, 310058).

[Abstract] Defence technology cooperation serves as an important manifestation of