从“合规防护”到“安全自主”

——欧盟网络安全政策范式转型及其影响*

丁　迪

内容提要：随着欧盟委员会《欧盟网络安全法》修订提案的提出，欧盟网络安全政策开始经历一场深刻的范式转型。在这一转型中，欧盟在政策目标、政策工具与因果认知三个层面的底层逻辑从“规则即安全”转向“自主可控方能塑造安全”。然而，受制于关键领域的能力差距、分权体制下的转化困境，以及战略自主与开放经济之间的张力，这一范式转型在政策实践中呈现出分层自主与可控依赖的状态。欧盟网络安全政策范式的转型，既深化了欧盟对自身脆弱性的认知，也在一定程度上加剧了跨大西洋关系的分化，以及全球数字治理的碎片化与阵营化。

关键词：欧盟网络安全　政策范式　范式转型　安全自主　技术主权

数字技术已成为大国博弈的核心场域，网络安全也已从技术治理议题扩展为关乎国家主权、经济命脉与国家安全的战略议题。长期以规则制定者形象立足于全球数字治理领域的欧盟逐渐意识到，当支撑规则运行的底层技术与基础设施掌握在他人手中时，再精密的规则也未必能够保障自身的安全。正是这一隐忧，促使欧盟的网络安全治理逻辑悄然发生一场看似平静却极为深刻的转变。这场转变并非一蹴而就，而是在一系列立法更迭与战略调整中逐步显现。要理解其性质与走向，须先回到欧盟网络安全治理的传统逻辑，考察它在何种基础之上建立、又

* 本文系2025年度国家社会科学基金青年项目"硅谷右翼对美国科技政策影响机制及启示研究"（项目批准号：25CGJ078）的阶段性成果。

因何而动摇,从而透过纷繁的立法表象,揭示这一转变的底层逻辑、现实限度及其深远影响。

一 问题的提出

欧盟对网络安全问题的理解并不局限于防范网络攻击,还包括保护网络与信息系统及相关主体免受网络威胁的活动。《欧盟网络安全法》(EU Cybersecurity Act)第二条将“网络安全”(Cybersecurity)正式界定为“为保护网络与信息系统、此类系统的用户以及其他受网络威胁影响的主体所必需的活动”。[①] 相应地,欧盟网络安全政策则可以界定为欧盟为保护网络与信息系统及相关主体免受网络威胁、维持系统安全与韧性而采取的一系列措施。在这一概念框架内,网络安全与数据安全相互交叉但并不等同。数据在网络与信息系统运行过程中面临的保密性、完整性和可用性风险属于网络安全问题;数据的权属配置、利用与流通则并不必然属于网络安全范畴,但相关活动涉及系统或数据安全时,二者的治理范围仍会交叉。同时,虽然随着国际安全环境与通信信息技术的不断演进,网络安全的概念框架不会轻易发生改变,但欧盟网络安全政策的内涵和治理边界则处于动态调整与变化之中。

传统上,欧盟主要凭借单一市场的规模与监管能力,将自身规则与标准外溢为全球性标准,从而在全球数字治理中占据独特地位。这种被称为“布鲁塞尔效应”的治理路径,构成学界理解欧盟数字治理的主流视角。[②] 在这一路径下,欧盟内部逐步形成了以原《网络与信息系统安全指令》(Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union,以下简称“原 NIS 指令”)和《欧盟网络安全法》为重要支柱,与

① European Union, “Cybersecurity Act,” April 17, 2019, Article 2(1), http://data.europa.eu/eli/reg/2019/881/oj.

② Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020, pp.25-66.

《一般数据保护条例》(GDPR)等数字规制相衔接的网络安全治理体系。这一体系综合运用法律义务、认证标准与跨境协调机制,重点规范经营实体的风险管理和事件报告,并推动成员国主管机关及技术机构之间的合作。相较于直接掌控底层技术和基础设施,其政策重心更多落在规则完善、合规执行与协调机制的建设上。然而,在特朗普第二任期内,美国在数字领域的单边主义及一系列胁迫性做法,进一步强化了欧盟对外部技术依赖和跨大西洋制度性信任脆弱的担忧。①

在此背景下,2026 年 1 月,欧盟委员会正式提出《欧盟网络安全法》修订提案(以下简称"CSA2 提案"),拟建立"可信信息和通信技术供应链框架"(Trusted ICT Supply Chain Framework),针对重要关键部门和其他关键部门的信息和通信技术供应链非技术风险,设计欧盟层面的协调评估与风险缓解机制。② 2026 年 1 月 22 日,欧洲议会以 471 票赞成、68 票反对、71 票弃权通过《关于欧洲技术主权和数字基础设施的决议》(European Technological Sovereignty and Digital Infrastructure),该协议指出,高科技产品和数字服务对外部供应链的高度依赖会给主权与韧性带来风险,并要求减少有害的战略依赖。③ 上述两个事件在欧盟网络安全政策的发展历程中具有标志性意义。一方面,这标志着对于网络安全问题认知与界定的重大调整,欧盟网络安全的政策视野已经由传统的网络与信息系统安全及市场主体合规,逐步扩展至数字产品、关键基础设施、信息和通信技术供应链及其外部依赖。另一方面,伴随着对网络安全问题认知的转变,欧盟对网络安全何以实现的政策逻辑也发生重要的变化。尽管《欧盟网络安全法》修订提案尚需经过后续的立法程序,其最终制度安排仍存在调整空间,但其蕴含的基本政策逻辑表明,欧盟网络安全治理的政策重心已由强调"规范他者行为"更多地转向"提升管控能力"。自 2020 年 12 月《欧盟数字十年网络安全战略》(The EU's Cybersecurity Strategy

① 周逸江:《美欧数字治理冲突下跨国科技公司监管博弈模式的重构》,载《欧洲研究》,2025 年第 6 期,第 36-59 页。

② European Commission, "Proposal for a Regulation for the EU Cybersecurity Act," January 20, 2026, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act.

③ European Parliament, "European Technological Sovereignty and Digital Infrastructure," January 22, 2026, https://www.europarl.europa.eu/doceo/document/TA-10-2026-0022_EN.html.

for the Digital Decade)将“韧性、技术主权与领导力”列为三大行动领域之一以来,强化供应链安全的《网络与信息系统安全指令 2》(Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union,以下简称“NIS2 指令”)(2022 年)、培育芯片产能的《欧洲芯片法案》(European Chips Act)(2023 年)、强化产品全生命周期网络安全要求的《网络韧性法案》(Cyber Resilience Act)(2024 年)、建立共同预警与应急机制的《网络团结法案》(Cyber Solidarity Act)(2025 年)等相关立法和政策,逐步构成新的网络安全政策框架。这一新框架与欧盟长期以来凭借规则塑造全球数字治理标准的传统路径之间存在明显的张力,对未来全球网络安全治理格局的走向必将产生深远的影响。

当前,学术界针对欧盟网络安全政策演变的研究,总体围绕两条主要分析路径展开。部分研究以“技术主权”“数字主权”等概念为切入点,分析欧盟数字化转型的政策目标、权力逻辑及其政策实践,较早捕捉到规则塑造、技术能力与战略自主之间关系的变化。但这类研究的对象多为欧盟数字治理或数字主权,较少专门从政策范式角度系统地解释网络安全领域中政策目标、政策工具与因果认知之间的关系。① 另有研究直接考察欧盟网络安全政策的演进,或从数字主权与战略自主的关系讨论欧盟规范性力量与地缘政治雄心之间的张力。这些研究已经超越单纯的技术或法条梳理,揭示了主权、安全、经济和规则输出之间的联动,但尚未以本文所采用的“政策目标—政策工具—因果认知”框架系统地判定欧盟网络安全政策是否发生范式转换。②

既有研究已经从数字主权、政策工具与地缘政治等角度揭示了欧盟网络安全

① 这一研究路径的代表性成果包括:蔡翠红、张若扬:《“技术主权”和“数字主权”话语下的欧盟数字化转型战略》,载《国际政治研究》,2022 年第 1 期,第 9-36 页;宫云牧:《数字时代主权概念的回归与欧盟数字治理》,载《欧洲研究》,2022 年第 3 期,第 18-48 页;史拴拴:《欧盟数字主权:生成逻辑、构建策略与现实挑战》,载《世界经济与政治论坛》,2022 年第 6 期,第 56-77 页。

② 这一研究路径的代表性成果包括:Helena Carrapico and Benjamin Farrand, “Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics,” *Journal of Common Market Studies*, Vol.62, 2024, pp.147-158; Dennis Broeders et al., “In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions,” *Journal of Common Market Studies*, Vol.61, No.5, 2023, pp.1261-1280。

政策的多重变化,但对政策目标、政策工具与因果认知三者关系的系统解释仍有推进空间。实际上,在网络技术格局变迁与地缘政治结构调整的双重作用下,欧盟政策目标的战略升级与政策工具的渐进式变革并不同步:目标层面的话语表述较快升级,工具层面的调整则相对渐进,二者之间的落差可被理解为欧盟决策者对“网络安全何以实现”这一根本问题的认知重构。若仅聚焦于话语分析,会高估政策转变的完成程度;若仅拘泥于文本解读,又会低估政策转变的深刻影响。如果缺少将政策目标、政策工具与因果认知相结合的整体性研究视角,就难以充分识别渐进立法表象之下的范式转向,也难以研判该转向的未来发展趋势。

据此,在研究欧盟网络安全政策的演进过程时,应当引入政策范式分析框架,着力突破现有立法文本的表层限制,厘清欧盟网络安全治理从旧有范式向新型范式转变的内在逻辑,系统阐释该转变的特征、运行机制与存在限度。在欧美战略关系持续调整、欧盟数字治理面临多重挑战的背景下,这一研究不仅有助于厘清欧盟数字治理的发展方向,也可为预判全球网络安全格局的发展趋势和制定应对方案提供学理层面的参考。

二 欧盟网络安全政策范式变迁分析框架

若要准确把握欧盟网络安全政策的演变,仅聚焦于具体目标或工具的调整和增减并不充分,而应当着眼于剖析政策形成过程中的认知与信念体系,将分散的政策目标、政策工具及其背后的因果认知整合为有机的整体展开分析。这一视角有助于透过繁杂的立法表象,辨识出渐进式变革是否反映整体政策逻辑的变迁。

(一)政策范式的概念及其分析功能

1993 年,霍尔(Peter A. Hall)通过借鉴库恩(Thomas Kuhn)的科学范式概念提出“政策范式”(Policy Paradigm)的概念。他将其界定为一个解释性框架,不仅规定了政策的目标,也规定了实现目标的工具,并界定了政策所要应对问题的性

质。[①] 在霍尔之后,达涅诺(Pierre-Marc Daigneault)对这一概念做了重要的方法论的精确化,主张研究者应同样关注政策制定者的观念与所采纳的政策,并在二者之间做尽可能严格的区分,以避免简单地把政策话语等同于政策实质。[②] 他的研究为政策研究的观念主义路径(Ideational Approach)提供了坚实的方法论支撑,在此基础上,本文进一步把政策范式界定为:由包括欧盟委员会、欧盟理事会、欧洲议会、欧盟网络安全局(European Union Agency for Cybersecurity,ENISA)等参与欧盟网络安全议程设定、立法和政策协调的核心政策制定者所构成的政策共同体共享的,关于政策目标、政策工具选择、政策所要处理问题性质的认知与信念体系。由此,政策范式本质上是一种政策认知体系,而具体的政策目标声明、政策工具选择、问题界定等均是这一认知体系的外化表现。

政策范式这一概念在政策研究领域具有极为重要的分析功能。其一,它将分散的政策工具整合为一个具备内在一致性的整体。在任何特定的政策领域,均存在数量繁多的法律、措施和工具。引入范式概念,能够探究这些分散的安排是否受同一套底层认知所统领,进而使政策研究的对象从分散的工具提升至整体逻辑层面。其二,它为识别政策的“深层变革”与“表层调整”提供了判断依据。在政策研究中,对于新立法或新工具引入的政策意义和战略走向的判断,往往缺乏理论支撑。政策范式概念的提出,揭示了政策共同体底层认知与信念体系的变化,为判断政策的战略走向提供了关键的理论工具。其三,它为不同政策领域、不同国家或地区的政策变迁比较提供了共同的分析维度,有助于研究者在更为宽泛的理论框架下系统地比较其异同。

政策范式分析框架具有一定的普遍性,也可用于分析其他国家或政策领域的深层政策变迁。但欧盟网络安全政策具有较强的跨领域性与渐进演化特征,使这一框架具有特殊的分析价值。自 2020 年以来,欧盟网络安全立法密集出台,政策

① Peter A. Hall, “Policy Paradigms, Social Learning, and the State: The Case of Economic Policy-making in Britain,” *Comparative Politics*, Vol.25, No.3, 1993, p.279.

② Pierre-Marc Daigneault, “Reassessing the Concept of Policy Paradigm: Aligning Ontology and Methodology in Policy Studies,” *Journal of European Public Policy*, Vol.21, No.3, 2014, pp.461-463.

工具不断扩展,日益与产业政策、供应链治理、关键基础设施保护和战略自主等议题相互交织。若仅停留在具体政策与工具层面的观察,既难以识别这些渐进变化背后政策共同体安全认知的系统性重构,又可能因现实政策成效有限而低估认知变化对未来政策走向的持续影响。引入政策范式框架,可以将分散的政策变化置于统一的认知逻辑中加以考察,识别渐进调整背后的整体性转变,从而更准确地把握欧盟网络安全政策变迁的性质及其发展方向。

(二)政策范式转型分析框架的构建

由于政策范式本质上是政策共同体共享的认知与信念体系,其变化不能仅由具体政策调整直接推断,而是需要通过能够反映政策认知的可观察证据加以识别。结合关于政策目标与政策工具的区分,以及达涅诺对政策范式认知属性的进一步操作化,本文根据欧盟网络安全政策研究的问题需要,将范式变化具体转化为三个相互关联的观察维度——政策目标、政策工具和连接二者的因果信念。本文分别从三个维度考察欧盟网络安全政策范式的变化,区分一般性的目标调整、工具增量与涉及基本认知变化的范式转换。

第一,政策目标维度所关注的是政策共同体针对"政策应当追求什么"形成的共同认知。此维度的观察对象涵盖政策宣示、官方战略文件、立法文本的目的条款和决策层的公开表述等。值得注意的是,政策目标并非处于同一层级,不同目标在抽象程度、战略地位与政策优先序上存在一定的差异。霍尔在其理论中明确将"政策目标层级"(Hierarchy of Goals)的变化视为政策变化的重要组成部分。[①]其对英国宏观经济政策的分析进一步表明,范式转型不仅体现为政策目标本身的变化,也可能表现为既有目标之间优先序的重新排列。因此,判断政策目标是否发生范式层面的变化,不能仅考察是否出现新的目标,还应关注相关目标在整体政策目标体系中的相对位置和优先级别是否发生实质性调整。

政策目标的稳定性,源于政策范式所形成的认知与规范约束。当政策共同体对政策问题的性质、政策使命和目标优先序形成共同认知后,既有的政策目标体

① Peter A. Hall, "Policy Paradigms, Social Learning, and the State: The Case of Economic Policy-making in Britain," pp.278-279, p.284.

系通常会保持较强的稳定性。① 当原有问题的界定仍能有效解释和回应主要政策风险时,新出现的问题通常可通过范式内部的目标调整或政策工具修正予以吸纳,并不会改变政策目标的基本层级结构。反之,当外部环境变化持续催生既有范式难以充分解释和应对的政策异常时,原有目标体系的认知基础便可能发生松动。更为重要的是,其他领域政策目标的变化,可能通过政策溢出与目标协调的路径对既有政策目标产生影响。② 在两方面因素的共同作用下,政策目标发生变动的可能性便会上升。

第二,政策工具维度所关注的是政策共同体针对“通过何种手段达成目标”形成的共同认知。这一维度的观察对象涵盖具体立法文本、监管框架、认证机制、产业政策、公共采购、危机响应机制等外在制度安排。在该维度中,还可以进一步对工具的参数设定、实施机制和工具之间的协同关系展开观察。正如当代政策科学在反思政策变迁测量方法时所指出的,国家治理手段的演进往往呈现出高度的制度黏性,政策组合内部的演化并不总是表现为旧工具的彻底废除与新手段的凭空创设。范式变迁的关键观察要点之一,在于工具集是否跨越传统的部门边界拓展至先前未覆盖的政策领域,以及既有工具的功能是否在新目标的引领下被重新界定。③ 判断政策工具是否在范式层面发生变化,不能仅仅考量政策是否新增了工具,还需审视既有工具的功能是否被重新定义,即原有的政策工具的功能是否在全新的战略统摄下经历了实质性的改变,从而服务于新的政策意图。

政策工具的选择建立在特定的政策目标、问题认知与政策情境基础之上。④ 当既有的政策工具能够有效地服务既定政策目标时,政策共同体通常缺乏对工具

---

① Yves Surel, “The Role of Cognitive and Normative Frames in Policy-Making,” *Journal of European Public Policy*, Vol.7, No.4, 2000, pp.495-512.

② Adrian Kay, “UK Monetary Policy Change During the Financial Crisis: Paradigms, Spillovers, and Goal Co-ordination,” *Journal of Public Policy*, Vol.31, No.2, 2011, pp.143-161.

③ Michael Howlett and Benjamin Cashore, “The Dependent Variable Problem in the Study of Policy Change: Understanding Policy Change as a Methodological Problem,” *Journal of Comparative Policy Analysis: Research and Practice*, Vol.11, No.1, 2009, pp.33-46.

④ Stephen H. Linder and B. Guy Peters, “Instruments of Government: Perceptions and Contexts,” *Journal of Public Policy*, Vol.9, No.1, 1989, pp.35-58.

体系进行实质性调整的动力。而当外部环境变化推动政策问题被重新界定,原有政策手段已不足以满足新的政策要求时,政策工具调整的压力便会随之上升。因此,政策问题与政策目标变化所形成的“目标—工具”失配是本文重点考察的政策变迁动力来源之一。① 但是,这种调整压力并不必然同步转化为现实政策工具的变化,其实际转化仍受制度结构、政策能力和资源条件等因素制约。② 这也将导致政策目标的快速跃迁与政策工具发展难以同步,进而使政策范式转型过程中出现“目标超前、能力滞后”的可能性。

第三,因果认知维度所关注的是政策共同体对于“为何特定工具能够达成特定目标”的共同信念。这一维度揭示了政策制定者关于“何种工具能够达成何种目标”的主观信念体系。正如当前国际政治经济学与网络性权力的前沿研究所揭示的,政策体系的演进往往源于底层逻辑的根本性变化。当外部技术依赖被用作胁迫工具且可被随时切断时,安全政策的着力点就会从约束行为转向储备安全能力。③ 在欧盟的网络安全与关键技术政策场域中,旧有的因果认知主要依赖通过规则对市场主体加以约束来实现整体安全;而新的逻辑则发生变化,仅仅依靠规则约束被认为不足以确保安全,在外部技术依赖被“武器化”的背景下,掌握关键技术能力和建立可替代选项成为维护自身安全的核心手段。由此可见,这一维度是政策范式概念中最具理论价值的枢纽部分,因果认知反映的是政策制定者关于目标如何达成、工具如何使用的根本性假设,这一维度在很大程度上决定了相关制度的功能设定与政策的战略走向。

因果认知的变迁,取决于既有认知能否持续对政策问题做出合理解释,以及政策实践能否持续产出符合既有认知预期的结果。当外部环境变化持续造成政策预期与现实结果之间的偏差,且该偏差被政策共同体识别为原有因果认知难以

---

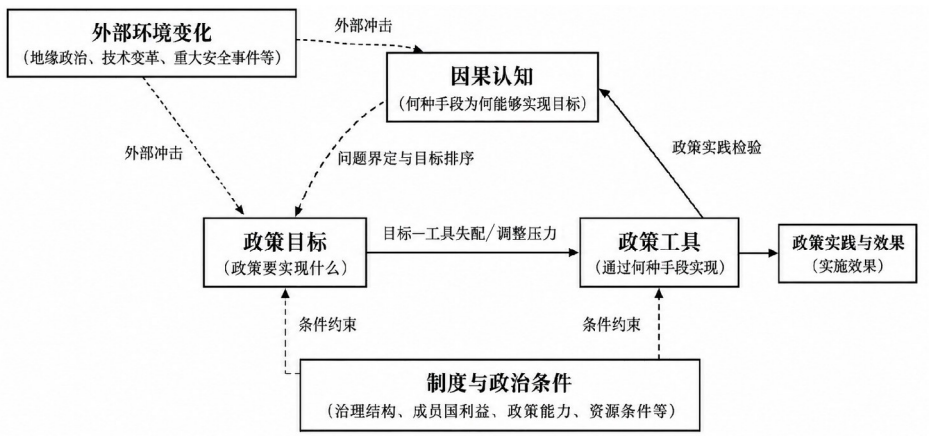
① Karoline S. Rogge and Kristin Reichardt, “Policy Mixes for Sustainability Transitions: An Extended Concept and Framework for Analysis,” *Research Policy*, Vol.45, No.8, 2016, pp.1620-1635.

② Xavier Fernández-i-Marín et al., “Studying Policy Design Quality in Comparative Perspective,” *American Political Science Review*, Vol.115, No.3, 2021, pp.931-947.

③ 米军等:《相互依赖武器化、网络结构演化和网络性权力——以半导体和国际金融网络的案例分析》,载《当代亚太》,2023 年第 6 期,第 30-60 页。

解释或应对的政策异常时,既有的问题界定与政策有效性认知便可能发生松动。但仅是原有的认知发生动摇,并不会自动导致范式转型。新的问题解释只有在既有制度结构、利益关系和政策过程的作用下逐步获得主要政策行动者的认可,并进入政策目标、政策话语及制度安排,才可能形成较为稳定的认知调整。① 因此,特定政策领域因果认知的变化往往并非孤立发生,而是与更高层级的战略认知和背景政策调整密切关联。

图 1 政策范式变迁的三维观察框架



注:图由作者自制。

上述三个观察维度并非相互独立,在外部环境和整体战略调整影响下会形成具有一定时序特征的互动关系。政策目标反映了政策共同体对于政策所要解决的核心问题及其优先序的基本判断;政策工具体现政策共同体对实现既定目标所需手段的判断。政策目标及其优先级的变化是推动政策工具调整的重要动力;因果认知则显示政策共同体关于特定政策工具何以能够实现既定目标的基本认知,通过目标与工具之间的关系来体现。三个维度变迁的动力机制同样存在紧密关

① Daniel Béland, “Ideas, Institutions, and Policy Change,” *Journal of European Public Policy*, Vol.16, No.5, 2009, pp.701-718.

联:当外部环境变化与更高层级背景政策调整推动政策问题重新界定时,既有政策目标的层级与优先序便可能发生变化;当新政策目标超出既有工具的功能范围,便会造成“目标—工具”失配,进而形成政策工具调整的压力,但这种调整压力能否转化为现实政策工具变化,还受制度结构、政策能力、利益格局和资源条件等因素制约。与此同时,外部环境变化所产生的政策异常以及整体战略认知的调整,也可能动摇支撑既有“目标—工具”关系的因果信念,并为其重构提供新的解释框架;而因果认知的变化,又会进一步强化对政策目标调整和工具变革必要性的认识。由此可见,三者之间既存在一定的传导关系,也存在政策实践形成的反馈机制(见图 1)。

(三)政策范式与现实政策的非对称关系

识别政策范式转型是预判政策走向的重要理论依据,但范式变迁并不完全等同于现实政策变迁。政策范式首先是一种认知层面的结构,指政策共同体关于“问题是什么、目标是什么、应当以何种工具实现目标”的共有理解;而现实政策则是这一认知结构在特定制度环境、能力条件和利益格局中的具象化的结果,这一过程在既有制度惯性、利益协调和能力约束的影响下可能存在时间上的滞后或转化程度上的差异,从而呈现出一种非对称性关系。

霍尔关于政策范式的经典研究,揭示了政策目标、政策工具和工具设定之间的层级性变化,并以英国宏观经济政策从凯恩斯主义转向货币主义为例,说明深层政策变迁往往伴随政策共同体认知体系的重组。但认知范式的变化未必会立即、完整地转化为现实政策变化,不能将政策认知层面的变化直接等同于制度层面的政策变化。政策范式变迁与政策变迁虽然密切相关,但属于两个分析层次,其关系并非完全对称。

这种非对称关系也体现在政策变迁的具体机制之中。既有研究表明,政策范式与制度安排的变化并不必然通过对既有结构的整体替代而实现。在观念层面,既有认知要素可以通过相互关系与相对权重的调整发生渐进式变化。[①] 在制度层

① Martin B. Carstensen, “Ideas Are Not as Stable as Political Scientists Want Them to Be: A Theory of Incremental Ideational Change,” *Political Studies*, Vol.59, No.3, 2011, pp.605-610.

面,既有政策工具一旦嵌入法律体系、行政组织与执行程序,其整体替换往往受到制度惯性、协调成本与既有利益结构的制约。渐进制度变迁理论进一步指出,既有制度可能通过重新解释或重新部署而被赋予新的功能,也可能在原有制度基础上逐步叠加新的制度要素。① 由此,在新的政策目标逐步形成,而相应政策能力与制度工具尚未同步调整的情况下,既有工具可能继续存在,并通过适用范围或政策功能的调整承担新的政策任务,同时与新增工具共同构成新的政策组合。例如,在原 NIS 指令向 NIS2 指令的演进中,欧盟保留了风险管理、事件报告、监管与处罚等传统合规工具,同时通过扩展风险管理义务,将供应链安全明确纳入相关实体的法定责任范围。② 这一转变通过对既有合规框架的适用主体、责任范围和功能指向的进一步扩展与制度化,使既有合规工具更加系统地承担供应链风险识别与管理功能。可见,范式变迁在政策层面的表现,很多时候并不是简单的“旧工具消失、新工具取代”,而是“旧工具延续、新功能嵌入”。换而言之,范式转型并不必然表现为旧工具被新工具迅速替代,而可能首先表现为既有工具的延续、功能调整与新工具的渐进叠加。

正是这种非对称性,造成了政策范式与现实政策之间的持续张力。政策共同体即便已经形成新的问题意识和目标排序,既有制度结构、行政能力、利益格局和技术基础也未必能够同步调整。因此,政策转型常常是新目标已经确立,但旧工

---

① Wolfgang Streeck and Kathleen Thelen, “Introduction: Institutional Change in Advanced Political Economies,” in Wolfgang Streeck and Kathleen Thelen, eds., *Beyond Continuity: Institutional Change in Advanced Political Economies*, Oxford University Press, 2005, pp.24-26.

② 原 NIS 第 14、16 条已分别对基本服务运营者和数字服务提供商确立风险管理与事件报告义务,第 15、17 条规定了相应的监管与执法机制;此后,2018/151 号实施条例又要求数字服务提供商在安全管理中考虑“供应安全”,表明供应链因素在 NIS 时期已部分进入网络安全治理。NIS2 则进一步将供应链安全明确列为网络安全风险管理的基本措施。参见 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Arts. 14-17; Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems, Art. 2; Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, Arts.21, 23, 31-34。

具仍在运行;新逻辑开始统摄政策体系,但实际效果仍受制度条件与能力基础制约。据此,判断认知层面的政策范式是否已经形成,应主要依据问题界定、目标优先序和因果认知是否在核心政策主体及连续政策文本中获得较为稳定的表达,而判断政策转型的实现程度,则需要考察正式制度、政策工具和能力建设是否相应调整。这两者之间存在的张力和导致这一张力产生的结构性约束正是观察与分析欧盟未来网络安全政策走向的重要指标。

三 欧盟网络安全政策范式变迁分析

欧盟网络安全政策范式的转型并非单纯由网络安全风险增加所推动,而是外部技术与地缘政治环境变化、欧盟整体战略调整共同作用的结果。随着数字技术逐步成为大国竞争的核心领域,由关键技术、数字基础设施与全球供应链构建形成的相互依赖关系,开始显现出愈发突出的政治与安全属性。自 2013 年《欧盟网络安全战略》(Cybersecurity Strategy of the European Union)颁布以来,欧盟网络安全政策已逐步涵盖网络韧性、网络防御、产业与技术资源以及国际网络空间合作等多个领域。2020 年,《欧盟数字十年网络安全战略》提出“韧性、技术主权与领导力”等行动方向后,技术主权、供应链韧性和共同应急能力在整体政策体系中的战略权重进一步上升。此后,NIS2 指令、《网络韧性法案》《网络团结法案》等法规相继出台,进一步强化了供应链风险管理、数字产品全生命周期安全以及欧盟层面的共同监测、准备与危机响应能力。这一政策的演变过程并非仅是欧盟在应对新问题时做出的规则跟进,更体现了欧盟对“网络安全何以实现”这一问题的重新认识。

(一)政策目标的层级转移

2020 年前后,欧盟网络安全政策的目标体系发生了显著的层级性变化。这一变化的实质,不是某一具体目标的增减,而是多个既有网络安全目标层级位置的调整,这种层级转移主要体现在四个方面。

第一,目标性质从市场治理转向战略安全。2016 年,欧盟通过的《网络与信息

系统安全指令》的政策目标是“在联盟内实现网络与信息系统安全的高度共同水平”,其法律依据是《欧盟运行条约》第 114 条的内部市场条款。① 此时,网络与信息系统安全被欧盟视为数字单一市场正常运行的重要条件之一,政策重点更多体现为内部市场协调、风险管理与成员国间规则衔接。但是,2020 年 12 月 16 日,欧盟委员会与欧盟外交与安全政策高级代表联合发布《欧盟数字十年网络安全战略》,将网络安全行动方向重新定义为:“韧性、技术主权与领导力”“建立预防、威慑与响应的运行能力”以及“推进全球与开放的网络空间”。② 其中“技术主权”的提出,进一步把网络安全议题从内部市场治理领域提升至涉及欧盟整体战略地位的议题。③ 2021 年 3 月 22 日,欧盟理事会通过《关于欧盟数字十年网络安全战略的结论》(Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade),进一步将“在保持开放经济的同时实现战略自主,包括强化在网络安全领域做出自主选择的能力”列为正式政策目标。④ 由此,技术主权、战略自主与韧性等目标在网络安全政策体系中的优先级不断上升,欧盟网络安全政策的战略安全导向也随之日益凸显。

第二,目标对象从行为体合规扩展至关键基础设施安全。在原 NIS 指令时代,政策目标的核心对象是关键服务运营商与数字服务提供商等市场主体,只要这些主体采取“适当且相称”的安全措施并按要求报告事件,实体合规即可实现。但是,2024 年 10 月,《网络韧性法案》将政策目标的对象扩展至进入欧盟市场、属于该法适用范围的具有数字元素的产品本身,要求制造商履行编制“软件物料清单”(Software Bill of Materials,SBOM)、报告已被主动利用的漏洞和严重事件、持续

① European Union, “NIS Directive,” July 6, 2016, Article 1(1), https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

② European Commission and High Representative of the Union for Foreign Affairs and Security Policy, “The EU's Cybersecurity Strategy for the Digital Decade,” December 16, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018.

③ 张若扬、蔡翠红:《大国竞争背景下欧盟数字主权的复合构建——一种技术政治解读》,载《欧洲研究》,2026 年第 2 期,第 1-34 页。

④ Council of the European Union, “Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade,” March 23, 2021, https://data.consilium.europa.eu/doc/document/ST-7290-2021-INIT/en/pdf.

提供安全更新等义务。[①] 2026 年 2 月,欧盟委员会进一步推出 3.47 亿欧元的海底电缆安全投资与配套工具箱,将政策目标的对象进一步扩展至承载欧洲对外数据流的物理基础设施层面。[②] 这一政策覆盖范围的扩展,体现了欧盟网络安全政策目标在纵向维度上的扩展。

第三,目标内涵从内部秩序扩展至对外韧性。对内层面,欧盟网络安全政策主要聚焦于欧盟内部的市场秩序与基础设施保护,旨在消除成员国之间的规则碎片化,从而构建具备高度韧性的单一数字生态。对外层面,欧盟主要依靠其庞大的市场体量与规范制定能力,通过“布鲁塞尔效应”将欧盟标准外溢为全球事实标准,以制度性权力维护自身网络安全环境的长期稳定。2025 年 2 月 4 日,《网络团结法案》生效,在第 1 条第 2 款中明确把“为欧盟在网络安全领域的技术主权与开放战略自主做出贡献”列为立法目的。[③] 这一条例试图建立的欧洲网络安全预警系统、欧盟网络安全储备等机制,核心功能并非约束市场行为,而是在大规模网络威胁下确保欧盟能够维持整体运转、调动资源、快速恢复网络安全。随着跨境网络风险、供应链脆弱性和重大网络事件受到更多的关注,欧盟网络安全政策防御外部风险的维度被不断强化。在政策目标层面,防范跨境风险与提升重大网络事件的联合应对能力正逐渐获得更高的权重。

第四,目标表达从功能性目标上升至政治性目标。在原 NIS 指令时代,欧盟网络安全政策的目标表达是相对技术化的,“高度共同安全”“网络与信息系统安全”等表述均处于功能性目标层面。2026 年 1 月,欧盟委员会执行副主席亨娜·维尔库宁(Henna Virkkunen)在斯特拉斯堡正式提出《欧盟网络安全法》修订提案时,明确指出“网络安全威胁不仅是技术挑战,更是对欧洲民主、经济与生活

① European Union, “Cyber Resilience Act,” October 23, 2024, Articles 2, 13-14 and Annex I, Part II(1), https://eur-lex.europa.eu/eli/reg/2024/2847/oj.

② European Commission, “Commission Increases Submarine Cable Security with €347 Million Investment and New Toolbox,” February 5, 2026, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_327.

③ European Union, “Cyber Solidarity Act,” December 19, 2024, Article 1(2), https://eur-lex.europa.eu/eli/reg/2025/38/oj.

方式构成战略风险”。[①] 这一表述把网络安全的政策目标从技术安全议题上升为关乎欧洲整体生存方式的政治安全议题,网络安全问题也由低政治领域的非传统安全问题提升到高政治领域的国家安全问题,这从根本上改变了这一政策的政治属性。

虽然安全合规目标并未被废止,甚至在新的政策体系中得到强化,但 2020 年以来,网络安全韧性、技术主权与战略自主等战略性目标在政策体系中的地位明显上升。自《欧盟数字十年网络安全战略》将“韧性、技术主权与领导力”列为三大行动领域之一后,2021 年,欧盟理事会进一步将“在保持开放经济的同时实现战略自主”确立为网络安全战略的关键目标,并强调增强欧盟在网络安全领域自主选择的能力。这种变化折射出战略性目标的政策权重与统摄作用的提高,是欧盟网络安全目标体系内部优先序的重新调整。同时,这种调整也反映了欧盟政策制定者对网络安全环境、威胁来源及欧盟整体战略认知的改变。

(二)政策工具重组与拓展

随着政策目标层级的调整,欧盟网络安全政策工具在适用范围、功能定位和自身组合方式上也相应发生了明显变化。

第一,网络安全政策功能由实体风险管理进一步拓展至供应链风险治理。欧盟早期网络安全治理主要围绕实体风险管理与产品安全保障两个方面展开。前者通过风险管理、事件报告、监管与处罚等机制约束关键服务运营商和数字服务提供商的安全行为;后者则立足 2019 年《欧盟网络安全法》,逐步通过认证标准和安全要求提升信息通信产品、服务与过程的安全水平。因此,在原 NIS 指令所代表的早期治理时代,政策工具主要聚焦实体风险管理,并逐步延伸到产品自身的安全保障。

2020 年后,既有政策工具的法律形式被完整保留,但其功能定位在政策制定者的认知中发生了改变。NIS2 指令第 21 条明确将“供应链安全,包括各实体与其直接供应商或服务提供商之间关系的安全相关方面”列为十项强制性风险管理措

① European Commission, “Commission Strengthens EU Cybersecurity Resilience and Capabilities,” January 20, 2026, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_105.

施之一。[①] 这使欧盟能够通过规范相关实体,将监管范围由实体自身的网络安全管理进一步延伸至其与直接供应商和服务提供商之间的安全关系,从而增强对供应链风险的识别与管理能力。《网络韧性法案》附件 I 第二部分第 1 项,进一步要求制造商“识别和记录具有数字元素之产品中所含的漏洞与组件,包括以常用且可机读的格式编制软件物料清单,至少覆盖产品的顶层依赖”,这一要求提升了欧盟对相关数字产品内部组件及其直接软件依赖关系的识别和可追溯能力。这一政策工具功能上的调整,使传统产品安全治理由侧重市场准入进一步延伸至供应链风险识别与产品全生命周期管理,并将网络安全要求覆盖至产品的设计、开发、生产和后续维护等环节,标志着欧盟网络安全治理理念的一次重要转变。

第二,网络科技产业政策被纳入网络安全政策体系。除了对既有工具的功能重新编码之外,欧盟还将原本不属于网络安全治理范畴的政策工具纳入治理体系,实质性拓展了网络安全政策的边界。这一现象主要表现在欧盟打破了传统上的政策壁垒,将产业政策工具深度嵌入网络安全治理体系中。欧盟相关的战略和政策显示,关键技术制造能力与物理数字基础设施的安全韧性被视为实现网络安全与技术主权的重要基础。例如,2023 年 9 月,《欧洲芯片法案》拟调动数百亿欧元投资,为“综合生产设施”与“开放欧盟代工厂”建立认定框架,试图降低供应中断和关键技术受制于人的风险。随着大规模产业扶持手段被逐步用于强化关键信息基础设施、降低供应链依赖和提升网络安全能力,部分科技产业政策被嵌入欧盟网络安全治理体系,进一步拓展了其网络安全政策工具箱。[②]

产业政策工具的引入,实质性地打破了网络安全治理的传统边界。相较于早期主要将产业技术资源作为网络安全能力建设的一项战略任务,欧盟近年来明显提升了产业投资、产能建设和基础设施能力建设的力度,通过具体立法、财政投入和项目机制将早期的战略表述落实为网络安全治理实践,产业政策工具与网络安

① European Union, “NIS 2 Directive,” December 14, 2022, Article 21(2)(d), https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

② Rocco Bellanova et al., “Digital/Sovereignty and *European Security* Integration: An Introduction,” *European Security*, Vol.31, No.3, 2022, pp.337-355; European Union, “Chips Act,” September 13, 2023, Articles 13-16, https://eur-lex.europa.eu/eli/reg/2023/1781/oj.

全政策之间制度衔接更为直接,网络安全政策的外延也被进一步扩展。政策工具的扩展与重新组合通常意味着治理目标与问题界定对工具适配提出了新的要求。① 在欧盟网络安全政策场域中,这种政策工具的结构性扩张,在很大程度上反映了政策制定者对网络安全复杂性与维护安全路径认知的改变。

第三,网络安全治理中的欧盟层级协调与共同应对能力进一步强化。网络安全治理的决策与协调机制逐步由成员国分散实施,向更强的欧盟层级统筹与共同治理发展,成为欧盟网络安全政策功能拓展的重要表现之一。以 5G 供应链安全为例,2020 年,欧盟 5G 安全工具箱主要由成员国根据共同风险评估框架,对高风险供应商采取限制措施。② 2026 年 1 月,《欧盟网络安全法》修订提案则进一步计划在欧盟层面建立风险评估与缓解机制,构建可信信息和通信技术供应链框架。③ 这一框架若获通过,将进一步提升欧盟层面在关键信息和通信技术供应链风险评估与缓解方面的制度能力。同样,在原 NIS 指令框架下,欧盟层面的网络安全合作主要侧重于成员国之间的战略协调、信息交换与跨境事件协作,具体应急资源和响应能力仍主要分布于成员国层面。在此基础上,2025 年 2 月 4 日,《网络团结法案》生效,进一步强化了欧盟层面的共同应对能力,通过创设“欧洲网络安全预警系统”“网络安全应急机制”以及“网络安全事件审查机制”三大政策工具来协调欧盟整体网络安全系统的运转,以便快速识别威胁,跨国调动资源,构建集体干预能力。④ 这一系列制度安排表明,在成员国继续保留主要治理权限的同时,欧盟层面的网络安全协调、风险识别和共同应对能力正被不断强化。多层治理体系中,欧盟层级功能也由政策协调进一步向资源支持和跨境响应拓展。

---

① Michael Howlett, “The Criteria for Effective Policy Design: Character and Context in Policy Instrument Choice,” *Journal of Asian Public Policy*, Vol.11, No.3, 2018, pp.245-266.

② European Court of Auditors, “Special Report 03/2022: 5G Roll-Out in the EU: Delays in Deployment of Networks with Security Issues Remaining Unresolved,” 2022, https://www.eca.europa.eu/en/publications/SR22_03.

③ European Commission, “Proposal for a Regulation for the EU Cybersecurity Act,” Recital 132, Articles 98(1), 99 and 103.

④ 孙频捷:《韧性悖论:2025 年欧盟网络安全态势综述》,载《中国信息安全》,2026 年第 1 期,第 73-78 页;另参见 European Union, “Cyber Solidarity Act,” Article 1(1)。

由此可见,欧盟实现网络安全目标的政策路径正在发生较为明显的变化。通过对既有政策工具的功能拓展,将安全治理延伸至产品全生命周期;通过引入产业政策工具,来进一步扩大网络安全治理的边界;通过强化欧盟层面的协调与共同应对机制,来增强网络安全政策的系统性与一致性。这些变化提升了欧盟网络安全政策的治理范围与制度能力。更为重要的是,政策工具变化所呈现出的政策路径调整,为进一步考察欧盟关于网络安全风险来源及维护安全路径认知的变化提供了重要的经验基础。

(三)政策因果认知的重塑

政策目标的层级转移与政策工具的功能转换,深刻反映了欧盟政策制定者关于“网络安全何以可能”在因果认知层面的变革。这一认知的重组是政策范式变迁最深层、最重要的表现。2020 年之前,虽然欧盟网络安全政策已经包含韧性建设、能力合作和产业技术资源等多种政策路径,但以原 NIS 指令为代表的市场规制体系,仍将通过风险管理、事件报告等义务规范市场主体行为作为提升网络与信息系统安全水平的重要实现路径。这一政策逻辑的本质是通过市场纠偏来保障网络安全。例如,2013 年,NIS 指令提案的影响评估将关键企业网络安全措施不足、信息不对称和事件透明度不足等列为影响网络与信息系统安全的重要问题,并据此主张通过风险管理、事件报告等强制性义务提高安全水平。① 同样,GDPR 通过数据控制者和处理者的安全处理、数据泄露通知与合规责任机制强化个人数据安全,也是这一逻辑在个人数字权利保护问题上的延续。但是,2020 年之后,欧盟决策者对网络安全的认识发生了转变,供应链风险管理、产业与技术能力、基础设施韧性以及共同应对能力等因素在安全实现路径中的政策权重明显上升。这一政策逻辑重组,具体呈现在三个方面。

第一,安全风险的关注焦点由“市场失灵”转移到“对外依赖”。在“合规防

① European Commission, “Impact Assessment Accompanying the Document Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Level of Network and Information Security across the Union,” SWD(2013) 32 final, Strasbourg, February 7, 2013, p.21, 25, pp.39-41.

护”范式下,网络安全风险主要归因于安全投入不足、信息不对称导致的市场失灵。在这一解释下,风险被视为一种可由外部规则矫正的市场偏差,治理的任务就是以合规义务弥补市场的供给缺口。原 NIS 指令对运营商设定风险管理与事件报告义务,正是这一认知的制度体现。但是随着地缘政治博弈的深化发展,原本被视为正常市场分工的外部技术依赖则被视为新的风险敞口。2026 年 1 月 22 日,欧洲议会通过的《关于欧洲技术主权和数字基础设施的决议》(European Parliament resolution of 22 January 2026 on European technological sovereignty and digital infrastructure)指出,欧盟在数字产品、服务、基础设施和知识产权方面对非欧盟国家的依赖超过 80%,对关键领域的过度依赖可能损害欧盟竞争力、民主韧性与安全表示关切,这标志着“过度依赖是一种风险”正式成为欧盟的官方判断。① 换而言之,对外部供应链的依赖不再是一个中性的经济事实,而成为安全风险的来源本身。更为重要的是,对外技术依赖的安全属性开始受到欧盟更为系统的关注。对外依赖的风险判断不仅取决于供应方的政治属性,也取决于依赖是否高度集中、缺乏替代性以及是否可能被工具化。由此,具有较高脆弱性的关键依赖逐渐成为欧盟网络安全风险评估与缓解机制的重要关注对象。

第二,安全手段由依赖“规则约束”转变为强调“整体韧性支撑”。以原 NIS 指令为代表的内部市场规制路径仍较为强调规范市场主体行为,以提升网络与信息系统安全水平。但在 2020 年的《欧盟数字十年网络安全战略》框架下,安全路径已开始由单一合规环节扩展为多环节复合协同的模式。规则约束虽然仍被视为实现网络安全的重要路径,但欧盟对网络安全实现机制的认识已经大幅扩展为强调规制、投资、产业技术能力与集体行动机制的共同作用,实现网络安全的政策逻辑由以市场规制为重要支点,进一步扩展为规制约束、供应链韧性、能力建设与共同响应相结合的多元路径。2026 年 5 月,维尔库宁接受媒体采访时指出,技术主权意味着降低有风险的依赖,应从半导体供应链到云服务的关键领域增强欧洲自

① European Parliament, “European Technological Sovereignty and Digital Infrastructure,” Recital B and para.3.

身能力,[①]这正是此种认知转变的典型体现。与此同时,欧盟通过“数字欧洲计划”(Digital Europe Programme)为由国家网络中心和跨境网络中心组成的欧洲网络安全预警系统提供资金支持。2021—2024 年,欧盟用于各级网络安全运营中心的建设与运行资金已超过 1.94 亿欧元。[②] 这说明在政策实践中,合规约束需要辅以公共资金支持的技术与组织能力,才能抵御系统性的安全冲击。在欧盟决策者眼中,当下的网络安全必须依靠规则、能力与协调等多重环节共同建构的整体韧性来实现。

第三,安全内涵由防御性安全转变为自主性安全。虽然欧盟较早便认识到安全自主能力的重要性,但是其早期网络安全的核心含义依然是“保护系统、抵御和处置威胁、恢复功能”。2020 年之后,增强对关键技术和基础设施的自主选择能力、降低战略性依赖对欧盟行动空间的约束,则成为网络安全政策中更受关注的目标。纵观近年来欧盟有关网络安全政策与战略文本,这种自主性安全体现在技术、战略、应对和评估四个维度之中。具体而言,技术自主指欧盟在关键技术领域须具备一定规模的本土供给能力、多元可替代来源以及可信伙伴合作网络;战略自主指防范外部技术依赖对欧盟政策选择形成限制,同时具备降低高风险依赖的能力;应对自主指重大网络安全事件发生后,欧盟拥有可自主调配的应急资源,并能够通过欧盟与成员国之间的协调机制实现跨境响应;评估自主则指欧盟已形成独立的风险识别、供应商评估与政策判断机制。在 5G 安全工具箱中的多供应商战略、《欧洲经济安全战略》对经济依赖武器化风险的识别、《网络团结法案》建立的共同检测与应急支持机制,以及 5G 协调风险评估和可信信息和通信技术供应链框架所体现的自主风险判断能力,均是欧盟网络安全政策强化“自主性安全”逻

① Luca Bertuzzi, “Technological Sovereignty Is Not About Isolation, EU Digital Chief Says,” Euronews, May 21, 2026, https://www.euronews.com/my-europe/2026/05/21/technological-sovereignty-is-not-about-isolation-eu-digital-chief-says.

② European Union, “Cyber Solidarity Act,” Article 3(1), (3); European Commission, “Digital Europe Programme Fuels Digital Transformation and Skills Development across Europe,” December 18, 2025, https://digital-strategy.ec.europa.eu/en/news/digital-europe-programme-fuels-digital-transformation-and-skills-development-across-europe.

辑的典型表现。同时,必须指出,欧盟的“自主”并不意味着完全自给或单独行动,而是强调在保持对外合作的同时,仍然具备替代、选择、判断和响应能力。这种内涵的转变表明,欧盟已经将掌握网络安全的主动权视为实现网络安全政策目标的重要基础。

因果认知所关注的并非只是“何为安全”,而是“风险为何产生,以及何种手段能够实现安全”。2020 年以来,关键依赖、产业与技术能力、基础设施韧性和共同应对能力在欧盟安全实现逻辑中的重要性明显上升,表明其因果解释正由以规制纠偏为重要支点,进一步向规制、能力建设、依赖管理与共同应对相结合的多元逻辑扩展。这一因果认知的变化,是判断欧盟网络安全政策范式变迁的重要依据。

(四)从“合规防护”到“安全自主”的政策范式转型

在欧盟的网络安全政策议程中,战略安全的权重进一步上升,政策工具的外延也随之扩展。这些变化在制度层面表现为相关立法的持续更新以及政策工具的重组与拓展。更为重要的是,在认知层面,欧盟政策制定者对网络安全风险、治理目标及安全实现路径的理解也产生了变化。这一政策目标、工具组合与因果认知的渐进变迁,共同推动了欧盟网络安全的政策范式转型,并将持续影响其未来网络安全政策的演进方向。尽管其政策目标的变化主要表现为多重目标的叠加与层级位移,政策工具的调整体现为扩展与重组而非简单替代,因果认知的变化也更多表现为认知重心的转移而非原有路径的彻底否定,但正是这种渐进累积、相互嵌套的调整,使政策目标、工具组合与因果认知之间的关系发生了系统性重构。正如渐进制度变迁理论所揭示的,深层变迁并不必然以制度断裂或要素替代的形式出现,也可以通过既有要素的叠加、转换与重新排序逐步实现。欧盟网络安全政策正在经历的,正是这种渐进而具有结构性意义的范式转型。鉴于政策的渐进变迁并非线性替代,而是不同目标、工具与因果认知的叠加、嵌套与重组。为识别这种渐进变化中不同治理逻辑的相对差异,本文采用理想类型方法,将欧盟的两种政策逻辑概括为“合规防护”与“安全自主”。

本文将早期政策中以内部市场规制、主体合规义务和认证机制为代表的一类政策取向界定为“合规防护”理想类型。“合规防护”范式下的政策,主要通过统一

安全规则、设定风险管理和事件报告义务、实施监管与认证,提高市场主体和数字产品的基本安全水平。[①] 原 NIS 指令对关键服务运营商设定风险管理和事件报告义务,《欧盟网络安全法》通过统一的欧盟网络安全认证框架提高信息和通信技术产品、服务和过程的安全水平,均体现了这一规制取向。

然而,随着数字化程度和跨部门互联依赖不断加深,欧盟网络安全风险日益呈现跨境化、系统化和地缘政治化特征。2020 年,欧盟委员会在原 NIS 指令评估中明确指出,数字化转型扩大了网络威胁对象,攻击来源更加多样、手段更加复杂,而原有制度同时存在覆盖范围有限、成员国和行业之间韧性水平不一致、联合态势感知不足和缺乏共同危机响应等问题。[②] 2022 年,KA-SAT 卫星网络遭受攻击进一步显示,网络攻击可以与军事冲突相结合,并跨越国界影响多个欧盟成员国,使网络安全风险超出单一企业合规和单一成员国处置能力的范围。[③] 与此同时,战略自主、技术主权及地缘经济转向等更高层级的战略认知不断向网络安全领域传导。2020 年,《欧盟数字十年网络安全战略》首先将“韧性、技术主权和领导力”三大行动领域之一。[④] 此后,“战略自主”更加明确地向数字和技术领域延伸。2021 年的《战略前瞻报告》以欧盟的“行动能力与行动自由”为核心,将数据

---

① 需要说明的是,“合规防护”并非欧盟官方提出的政策概念,而是本文为比较 2020 年前后政策变化,对 2020 年前欧盟网络安全政策中以内部市场规制、主体合规和认证机制为突出特征的一类认知与政策取向所作的理想类型归纳。它并非对这一时期全部网络安全政策的完整描述,也不意味着当时欧盟将规则约束视为实现安全的充分条件。2013 年,欧盟网络安全战略已经将网络韧性、网络防御、产业与技术资源以及国际网络空间政策纳入治理体系,原 NIS 指令也通过国家战略、合作组和 CSIRTs 网络等机制强化成员国能力建设与跨境协作。

② European Commission, “Executive Summary of the Impact Assessment Report Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148,” SWD(2020) 344 final, Brussels, December 16,2020, p.1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0344.

③ Council of the European Union, “Russian Cyber Operations against Ukraine: Declaration by the High Representative on Behalf of the European Union,” May 10, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/.

④ European Commission and High Representative of the Union for Foreign Affairs and Security Policy, “The EU's Cybersecurity Strategy for the Digital Decade,” Part II.

管理、人工智能和前沿技术能力建设列为增强“开放战略自主”的重点领域。[①] 2022 年的《战略前瞻报告》在新的地缘政治环境下,进一步将关键物资供应、前沿技术以及网络安全纳入增强欧盟韧性与开放战略自主的政策框架。[②] 2023 年,《欧洲经济安全战略》进一步将供应链韧性、关键基础设施的物理与网络安全、技术安全与技术泄漏,以及经济依赖武器化或经济胁迫列为四类广泛且非穷尽的经济安全风险。[③]

由此可见,2020 年成为欧盟网络安全政策范式转型的重要节点。在此节点前(2017 年前后),自主性理念开始进入网络安全议程,但欧盟仅仅提出目标,并没有在政策工具上进行重大调整,只能说是处于政策范式转型的理念酝酿阶段。2020 年之后,随着跨境性、系统性和地缘政治性风险上升,原 NIS 指令所暴露的制度局限进一步加大政策调整压力,欧盟的一系列战略报告将技术主权、开放战略自主和经济安全等战略认知与网络安全紧密联系在一起,表明其对网络安全问题的认知发生了改变。随着提升供应链韧性、产业技术能力、关键基础设施安全和共同应对能力等战略性目标获得更高的政策权重,欧盟网络安全治理开始由以规制纠偏为重要支点,进一步向规则制定、能力建设、依赖管理和共同应对相结合、以强化欧盟对网络安全议程控制能力为目标的复合型安全路径发展。

基于上述变化,本文将 2020 年以来逐步强化的一类网络安全政策取向概括为“安全自主”理想类型。“安全自主”范式强调主体对安全议程的控制能力,而不是在数字技术领域实现封闭式自给,也并非否定合规规则的治理价值。这一范式的基本逻辑是,网络安全不仅需要规则的规制,也依赖欧盟在关键安全事项上保持

---

① European Commission, “2021 Strategic Foresight Report: The EU’s Capacity and Freedom to Act,” September 8, 2021, Section III(3), https://commission.europa.eu/strategy-and-policy/strategic-planning/strategic-foresight/2021-strategic-foresight-report_en.

② European Commission, “2022 Strategic Foresight Report: Twinning the Green and Digital Transitions in the New Geopolitical Context,” June 29, 2022, Sections V(1), V(3) and V(10), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0289.

③ European Commission and High Representative of the Union for Foreign Affairs and Security Policy, “European Economic Security Strategy,” June 20, 2023, Section 2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0020.

必要的选择、判断和行动能力。这种“自主性”具体体现为关键技术和服务具有一定的本土能力或可替代来源,关键外部依赖不会过度压缩政策选择空间,欧盟能够形成自身的风险识别与评估机制,并在重大网络安全事件中拥有可调动的共同应对资源。区别于“合规防护”理想类型主要强调通过规则约束和主体合规降低安全风险,“安全自主”范式是一种以“自主掌控”为底层逻辑的治理模式,强调在规则治理的基础上增强自身对网络安全风险及其后果的自主控制能力。

表 1 欧盟网络安全政策范式比较

	“合规防护”	“安全自主”
政策目标	以提升网络与信息系统安全水平、协调市场规则和强化主体责任为重要政策取向	在既有安全目标基础上,更加突出韧性、技术主权、关键依赖管理和自主行动能力
政策工具	以风险管理、事件报告、监管认证等规制工具为重要支点,同时辅以能力建设和跨境协调机制	在延续规制工具基础上,进一步引入供应链治理、产业投资、基础设施建设和共同响应等复合工具
因果认知	将规范主体行为、改善风险管理和信息披露视为提升网络安全的重要实现路径	更加强调规制、技术能力、依赖管理、供应多元化和共同响应等多种机制共同塑造安全
安全内涵	主要强调网络与信息系统的保护、风险防范、事件响应与功能恢复	在防护与韧性基础上,进一步强调保持必要的技术替代、政策选择、风险判断和危机响应能力

资料来源:作者根据 2013 年《欧盟网络安全战略》、原 NIS 指令、2020 年《欧盟数字十年网络安全战略》、NIS2 指令、《关键实体韧性指令》、《网络团结法案》及 2023 年《欧洲经济安全战略》等整理。①

① “合规防护”与“安全自主”均为本文为分析欧盟网络安全政策变化而建构的理想类型,并非欧盟官方政策术语,也不对应两个彼此截然分离的历史阶段。“合规防护”主要提炼 2020 年前欧盟网络安全政策中较为突出的市场规制与主体合规取向,但这一时期已经存在韧性建设、网络防御、产业技术能力和跨境协作等政策要素;“安全自主”则用于概括以 2020 年为关键转折点,此后逐步强化的政策取向,主要表现为战略性目标权重上升、工具组合进一步扩展以及风险来源与安全实现路径的因果认知重组。二者之间体现的是政策重心和要素组合的渐进调整,而非旧范式被新范式整体替代。

通过对比不难发现,欧盟网络安全政策范式变化的核心,在于欧盟政策共同体对“安全从何而来”这一根本问题认知的变化。驱动这一变化的主要因素有两个。

一方面,数字技术竞争加剧、供应链风险上升和技术依赖日益凸显的政治属性,改变了欧盟对网络安全风险来源的认知。更为重要的是,随着数字平台、人工智能等技术日益成为支撑经济社会运行的基础设施,作为这些技术底层支撑的网络安全问题也迅速成为国家安全的焦点,进而加速了这种认知变化的进程。尤其是 2025 年以来,跨大西洋关系不确定性上升、美国关键技术出口政策出现较大调整、欧盟对美国云服务和先进芯片等数字基础设施仍保持较高依赖的背景下,外部技术依赖所包含的供应中断和政策约束风险更加受到欧盟的重视。① 欧盟逐渐认识到,关键技术、数字基础设施和供应链对外部主体的高度依赖,并非单纯的市场结构问题,而可能转化为制约其安全、韧性与自主行动能力的战略脆弱性。2026 年 6 月 3 日,在欧盟“技术主权一揽子计划”发布时,欧盟委员会主席冯德莱恩明确指出,欧洲不能继续依赖他人提供维持关键公共服务和基础设施运行的核心技术。②

另一方面,欧盟整体战略方向的调整也在一定程度上带动了其网络安全威胁认知的变化。自战略自主逐步向数字与技术领域延伸以来,“技术主权”“战略自主”等上位战略目标不断融入网络安全政策体系。《欧盟数字十年网络安全战略》与《网络团结法案》都明确了“自主性”的重要地位。外部依赖越来越被重新界定为可能限制欧盟自主判断、自主决策和自主行动能力的安全风险。由此,欧盟网络安全政策目标的层级结构也随之调整,供应链韧性、关键能力与战略自主在既有市场开放、竞争力和基本权利等目标之外获得了更高的政策权重,并更加系统

① 欧盟委员会对 2025 年美国 AI 芯片限制的答复表达了这种担忧,详情参见 European Commission, “Answer Given by Executive Vice-President Virkkunen on Behalf of the European Commission,” P-000495/2025, March 25, 2025, https://www.europarl.europa.eu/doceo/document/P-10-2025-000495-ASW_EN.pdf。

② European Commission, “Commission Proposes Tech Sovereignty Package to Strengthen Europe’s Digital Autonomy and Resilience,” Press Release IP/26/1187, Brussels, June 3, 2026, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1187.

地进入网络安全政策框架。

外部环境变化与整体战略目标的调整,共同促使欧盟政策制定者重新审视网络安全风险的来源,并进一步推动政策范式的调整。欧盟逐步认识到,在高度对外依赖的背景下,单纯完善规则体系无法适配新的安全风险。网络安全不再被单纯理解为规范市场主体行为的结果,而越来越被视为规则约束、关键能力、供应链韧性与自主行动能力共同作用的产物。这种认知变化的实质,是欧盟对“风险为何产生以及何种政策手段能够实现安全”这一因果关系的重新理解。欧盟网络安全政策范式的调整,正是在外部环境施压与整体战略变迁的共同作用下逐步演化而来。在外部战略环境不断发生变化的情况下,“安全自主”政策范式在欧盟网络安全政策场域中的权重会进一步提升,对未来欧盟网络安全政策走向产生重要影响。

四 范式变迁下欧盟网络安全政策转型的限度

欧盟网络安全政策呈现的“安全自主”范式特征,核心在于强化欧盟在网络安全领域的选择、判断与行动能力。当前,其政策调整已逐步出现“完善规则、建设能力、培育替代选项与提升集体韧性”并行推进的复合取向。不过,这一政策转型仍受多重客观条件的制约。欧盟立法与治理结构的复杂性、关键技术领域的能力差距、安全治理目标与开放经济原则之间的张力,都将对这一转型构成一定程度的限制。

(一)高度对外依赖下的能力限度

欧盟网络安全“合规防护”政策范式在外部安全条件上隐含着类似于霸权稳定论中“善意霸权”(Benevolent Hegemon)的假设。[①] 在这一假设下,美国主导的安全与技术秩序总体上能够为欧洲提供稳定的外部公共产品和可信赖的安全环境。

① “善意霸权”(benevolent hegemon)概念源自金德尔伯格(Charles P.Kindleberger)的霸权稳定论,但其核心思想非常清楚,国际体系需要一个愿意承担超额成本、提供公共产品并维持体系稳定的领导国。参见 Charles P. Kindleberger, “Dominance and Leadership in the International Economy: Exploitation, Public Goods, and Free Rides,” *International Studies Quarterly*, Vol.25, No.2, 1981, pp.242-254。

但当这种安全环境变得不再可靠,欧盟计划“将网络安全主动权掌握在自己手中”,并试图在关键技术节点上具备本土供给或可信多元化能力时,其在关键数字技术领域的能力不足便成为一种难以规避的客观约束,限制了新范式下网络安全政策的全面转型。

目前,欧盟网络技术对外依赖集中在云计算、互联网基础设施、人工智能等关键领域。2026 年 1 月 22 日,欧洲议会对欧盟在云基础设施、半导体、人工智能与网络安全等关键领域对非欧洲行为体的过度依赖表示特别关切,明确承认“欧盟对非欧盟国家在关键数字产品、服务、基础设施和知识产权方面的依赖度超过 80%”,并指出技术权力正日益集中于非欧洲企业手中,限制了欧洲在创新、竞争与维护其数字经济、社会与民主自主控制方面的能力。① 欧洲云基础设施服务市场的发展格局更直观地呈现了欧盟在数字技术领域的对外依赖。据 2025 年 7 月协同研究集团(Synergy Research Group)发布的数据,亚马逊、微软与谷歌合计掌握欧洲云基础设施市场约 70%的份额,而思爱普(SAP)、德国电信(Deutsche Telekom)、法国 OVH 云计算公司(OVHcloud)等本土供应商合计市场份额仅占约 15%。② 即使到 2030 年,欧盟若按《欧洲芯片法案》所设立的目标,将其全球半导体市场份额由约 10%提高至 20%,也仅意味着欧盟半导体生产与产业能力得到增强,并不等同于实现全产业链技术自主或供应安全。③ 同时,Gaia-X 等欧洲数据与云基础设施合作计划的市场落地相对缓慢,迄今未能改变欧洲云市场由美国超大规模云服务商主导的格局。

究其根源是欧盟在过去十余年间未能对底层数字基础设施投入足够资源。正如德拉吉(Mario Draghi)在其受欧盟委员会委托完成的《欧洲竞争力的未来》报告中指出的,欧盟在数字技术领域与美国、中国之间已经形成明显的能力差距。以软件与互联网领域为例,欧盟企业在全球领先研发企业相关支出中的占比仅为

① European Parliament, “European Technological Sovereignty and Digital Infrastructure”.

② Synergy Research Group, “European Cloud Providers’ Local Market Share Now Holds Steady at 15%,” July 24, 2025, https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15.

③ European Commission, “Chips Act,” September 13, 2023, Recital 23.

7%左右,而美国和中国分别约为71%和15%;在技术硬件与电子设备领域,欧盟所占比重约为12%,也明显低于美国的40%和中国的19%。① 欧盟在新兴技术领域日益落后,对外国技术的依赖不断加深。有研究指出,欧盟一方面将数字主权和技术自主作为治理目标,另一方面又不得不在高度全球化的半导体生产体系中寻求能力提升,由此形成自主目标与相互依赖现实之间的持续张力。② 这种为提升自身技术安全能力而不得不更加依赖外部力量,但外部依赖又被视为一种安全隐患的现象,构成一种"自主困境"。在网络安全治理领域,欧盟事实上正面临着这一困境的挑战。这并不意味着欧盟无法提高自主能力,而是表明其现实政策目标更可能表现为降低高风险依赖、扩大替代来源并提升关键环节的控制能力,而非实现全产业链或全技术体系的完全自主。③

这一物质性约束折射出范式重构与政策变迁之间的非对称关系,政策共同体对"安全从何而来"的认知可以通过观念转变而相对快速地完成重组,但建立在物质性基础之上的实际能力建设却难以同步跟进。范式重构可以改变政策工具的组织方式,却不能立即改变欧盟技术能力的存量结构,欧盟可以在规则层面设定最严格的安全标准、要求提高供应链的可追溯性,但在供给层面仍难以为这些规则提供完全自主的技术支撑。这在若干高资本投资、高技术集中度的关键技术领域对新范式构成重要的能力约束,这种约束也深刻影响了范式转变在机制与战略层面的限度。

(二)政策转化约束下的机制限度

政策工具要发挥功能必须依托欧盟机构与成员国对不同形式立法的及时实

---

① Mario Draghi, "The Future of European Competitiveness, Part A: A Competitiveness Strategy for Europe," European Commission, September 9, 2024, p.16, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en; Mario Draghi, "The Future of European Competitiveness, Part B: In-depth Analysis and Recommendations," European Commission, September 9, 2024, pp.76-78, https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en.

② Linda Monsees, "The Paradox of Semiconductors—EU Governance Between Sovereignty and Interdependence," *Cambridge Review of International Affairs*, Vol.38, No.1, 2025, pp.3-21.

③ European Commission, "Strengthening Europe's Tech Sovereignty," last updated on June 23, 2026, https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty.

施。然而,欧盟并非主权国家,而是一个权力在超国家机构与成员国之间分割共享的复合体。在网络安全这一与国家安全高度相关、由欧盟与成员国分层治理的领域,权限配置具有明显的分层性。除了欧盟层面的顶层立法外,成员国仍承担大量具体执行、监管和应急响应职责。欧盟网络安全政策转型通常难以脱离既有立法、机构和成员国执行体系,让欧盟完全放弃传统的制度体系而另起炉灶并不现实,它需要在既有欧盟立法及成员国实施框架内,通过对原有工具的重组与功能的重新编码来推进转型。正因如此,这种“修修补补”式的制度演化方式也是新范式落实的重要制约因素。

首先,政策转化过程复杂,延迟新规范的落地施行。政策议程和战略认知的调整可以较快地通过战略文件、决策者表述和立法倡议来实现,在最终立法确认后获得稳定的共识。但其制度化和能力建设却需要经历立法协商、成员国国内法转化、监管机构调整以及具体执行机制建立等多个环节,因而明显滞后于政策目标的变化。以《关键实体韧性指令》(Critical Entities Resilience Directive,以下简称“CER 指令”)为例,按照第 26 条第 1 款规定,各成员国应最迟于 2024 年 10 月 17 日完成相关国内立法并向欧盟委员会通报转化措施。但包括卢森堡、荷兰、西班牙、瑞典在内的多个成员国均未能在法定期限内履行这一义务。[①] 这种大范围、持续性的转化迟滞至少说明欧盟多层治理结构本身会增加从欧盟立法到成员国执行之间的制度转换成本。CER 指令并非单一领域的技术性规范,而是横跨能源、交通、金融、卫生、数字基础设施等多个关键部门,需要成员国重新协调主管机关职责,并处理其与既有关键基础设施保护制度及部门性规则之间的衔接关系。[②] 由此可见,政策认知与规范目标的调整可以在欧盟层面较快完成,而其制度化和

① European Union, “Critical Entities Resilience Directive,” December 14, 2022, Article 26(1), https://eur-lex.europa.eu/eli/dir/2022/2557/oj; European Commission Representation in Malta, “April Infringements Package: Key Decisions,” April 29, 2026, Section 3, “Migration, Home Affairs and Security Union—Referrals to the Court of Justice,” https://malta.representation.ec.europa.eu/news/april-infringements-package-key-decisions-2026-04-29_en.

② Marcos Julien Alexopoulos et al., “Examination of the Critical Infrastructure Resilience Directive from the Maritime Point of View,” *Journal of Common Market Studies*, Vol.63, No.2, 2025, pp.667-678.

操作化则受到多层级治理结构、国内制度嵌入和部门协调成本的制约,二者之间的时间落差很难完全消除。

其次,政策转化机制在落地过程中存在制度稀释与效能降低的问题。NIS2 采用“最低限度协调”(Minimum Harmonisation)方式,仅设定安全要求的底线,允许成员国自主提高标准并自行设计实施细则。这一规定使成员国已经完成或正在推进的转化安排在主管机关、处罚标准、登记与事件报告流程、部门覆盖范围等方面存在差异。① 这种差异使欧盟统一网络安全框架在实际落实过程中出现不均衡性。欧盟所追求的在网络安全领域实现“统一掌控”的目标,在这种较大的制度差异下存在被稀释的风险。同时,成员国的能力差距进一步削弱了政策施行的效能。欧盟网络安全局(ENISA)的评估显示,成员国在政策实施、漏洞披露、监督措施、研发与教育等方面存在明显差异。② 在网络安全领域,整体安全水平往往取决于最薄弱的环节,制度安排与执行能力的不均衡是欧盟网络安全政策统一实施和共同韧性提升的重要制约因素。

再次,政策功能重组时新旧逻辑的张力,导致部分规定难以落实。新范式并未废止旧工具,而是在保留其法律形式的前提下为其注入新功能,这使得旧工具的原有逻辑与被赋予的新使命之间可能存在一定的张力。NIS2 第 21 条供应链安全条款是典型代表。其法律形式仍是要求受规制实体履行合规义务的传统规制工具,但其功能已进一步延伸至关键供应链风险管理,并要求与欧盟层面的“关键供应链协调安全风险评估”相衔接。③ 然而,此类合规义务主要在企业可管控的供应关系中发挥作用。受规制实体可通过供应商评估、合同约束、采购调整等方式降低直接供应商带来的风险,但企业难以依靠自身行为改变关键供应链上游的市场结构、供应商国别来源及其受第三国法律与政治权力影响等战略属性。尤其是

---

① John Timmons and Joe Devine, “NIS 2: One Year Later,” White & Case LLP, October 20, 2025, https://www.whitecase.com/insight-alert/nis-2-one-year-later.

② European Union Agency for Cybersecurity, “2024 Report on the State of Cybersecurity in the Union,” December 3, 2024, p.22, https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union.

③ European Union, “NIS 2 Directive,” Article 21(2)(d) and (3).

技术依赖度较高的关键供应链节点,企业层面的供应链风险管理与欧盟降低战略性依赖的宏观政策目标之间,存在明显张力。在云计算领域,少数大型供应商占据主导地位的市场结构,与数据迁移费用、兼容性不足以及技术、合同和组织转换的障碍相互叠加,导致了云服务生态锁定效应。欧盟《数据法》(Data Act)明确指出,高额数据迁出费用和其他不合理转换费用会抑制客户更换服务商,而互操作性不足以及技术、合同和组织性障碍又会进一步限制数据、应用和业务功能在不同云环境之间迁移。① 企业即使希望通过更换或增加供应商来分散风险,也会因较高的转换成本和对既有技术生态的依赖而难以在短期内实现。

最后,分布式执行高度依赖成员国的政策转化能力,这种能力的显著落差将进一步削弱政策转型的成效。新范式下的诸多工具,无论是 NIS2 的供应链审查,还是关键基础设施保护义务,其有效性都取决于成员国国家网络安全机构及相关组织的实际执行能力。但欧盟 27 国在制度转化进度上存在明显差距。例如,NIS2 要求成员国最迟于 2024 年 10 月 17 日完成国内法转化,但直到 2025 年 5 月,仍有 19 个成员国因未向欧盟委员会通知完整转化措施而收到说明理由意见;2026 年 7 月,欧盟委员会仍因爱尔兰、西班牙、法国和荷兰未通报完整转化措施,决定将这四国诉至欧洲法院。② 由于网络基础设施和供应链在欧盟内部具有高度关联性,部分成员国在制度转化和政策执行上的迟滞,可能严重影响欧盟治理体系的完整性与一致性。

在欧盟分权体制下,传统框架内的渐进性变革是较为稳固的政策转型路径,但对于一场深度的范式转型而言也是一种限制因素。范式与认知可以在布鲁塞

① European Union, “Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data (Data Act),” Recital 88, Articles 23, 29, https://eur-lex.europa.eu/eli/reg/2023/2854/oj.

② European Commission, “Commission Calls on 19 Member States to Fully Transpose the NIS2 Directive,” May 7, 2025, https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive; European Commission, “Commission Refers Ireland, Spain, France and the Netherlands to the Court of Justice for Failing to Transpose the Rules on Cybersecurity,” July 8, 2026, https://digital-strategy.ec.europa.eu/en/news/commission-refers-ireland-spain-france-and-netherlands-court-justice-failing-transpose-rules.

尔的战略文件中较为快速地实现转变,但其施行却必须穿越 27 国分散立法与差异化执行的重重关隘。范式跃迁与制度层面的迟滞落地之间的结构性落差,构成欧盟网络安全范式在机制层面的重要限制因素。

(三)发展与安全张力下的战略限度

欧盟单一市场的根基建立在货物、服务、人员与资本自由流动的原则之上。这一原则不仅是欧盟内部市场的法律基础,也是欧盟在全球数字治理中所秉持的核心价值主张。① 然而,以安全为由限制特定供应商或要求供应链可替代,与这一开放经济原则存在张力。更为重要的是,对安全自主这一概念的认知在欧盟成员国之间也并不统一。法国主张欧盟应在关键技术领域增强自主能力、减少对非欧洲技术供应商的依赖;而部分中东欧国家则担忧过度强调自主可能削弱跨大西洋关系。② 2026 年年初以来,尽管跨大西洋关系的剧变在很大程度上推动了欧盟内部战略自主共识的凝聚,但成员国之间在自主的程度、战略方向与议题优先级上仍存在分歧。③ 如何在“安全限制”与“开放发展”之间保持平衡,仍是范式转型中欧盟必须解决的难题。④

更深层的战略张力来自欧盟对外关系的多元定位。一方面,欧盟与美国在数字政策领域已经存在明显的结构性紧张关系。欧盟将关键外部技术依赖及第三

① 关于欧盟“开放战略自主”概念中“开放性”与“自主性”之间的张力分析,可参见 European Commission, “2021 Strategic Foresight Report: The EU's Capacity and Freedom to Act,” Section I。

② Élysée, “Conclusion of the 26th Franco-German Ministerial Council,” July 17, 2026, https://www.elysee.fr/en/emmanuel-macron/2026/07/17/conclusion-of-the-26th-franco-german-ministerial-council; Government of Poland, “Stronger EU in a Turbulent World: Contribution to the Discussion on the Concept of EU Strategic Autonomy,” September 16, 2021, pp. 1-3, https://www.gov.pl/attachment/5c18adea-7778-4d83-9edb-9f680a1cc633.

③ Foo Yun Chee, “EU Plan to Phase-Out High-Risk Tech Draws Fire from China's Huawei,” CNBC (Reuters), January 20, 2026, https://www.cnbc.com/2026/01/21/eu-plan-to-phase-out-high-risk-tech-draws-fire-from-chinas-huawei.html.

④ 2026 年 6 月欧盟电信理事会讨论显示,各成员国总体认同减少数字价值链中的战略依赖,同时又普遍强调保持开放、创新和公平竞争。参见 Council of the European Union, “Transport, Telecommunications and Energy Council (Telecommunications), June 9, 2026,” Section “Technological Sovereignty of Europe's Public Administrations,” June 9, 2026, https://www.consilium.europa.eu/en/meetings/tte/2026/06/09/。

国供应商可能带来的供应链风险纳入网络安全治理,美国贸易代表办公室则将欧盟的云服务网络安全认证方案以及部分成员国针对关键数据和云服务提出的所有权、数据存储管辖等加强安全自主性的要求列入贸易壁垒评估范围。① 另一方面,欧盟在网络安全之外的能源、防务、关键技术合作等议题上仍存在不同形式、程度不一的对美结构性依赖。这种“既要保持战略自主、又要维系跨大西洋合作”的双重定位,使欧盟在安全自主路径的推进上始终面临“走多远”“走多深”的战略困境。过于激进的自主化,如对美国数字企业实施具有明显排他性的本地化要求、市场准入限制或监管措施,可能引发美国通过贸易调查、关税措施以及双边贸易谈判施加反制压力,更可能加剧跨大西洋裂痕;而过于克制,又难以掌握安全主导权。这一两难处境,正是欧盟新范式难以避免的战略性约束。

(四)“有限自主”转型下欧盟网络安全政策的总体评价

在能力、机制与战略的三重约束下,欧盟网络安全政策只能实现“有限自主”。欧盟已经形成了清晰的战略调整意愿,亦有具体的政策行动,但物质基础的不足、自身体制的局限与战略目标的内在张力,使其在实践中难以完全摆脱对外部技术与供应链的依赖。其转型由此陷入一种“认知已然成型、实践诸多阻碍”的困境。但是跨大西洋关系的剧变与技术胁迫的现实,又使其无法退回传统“合规防护”政策路径,只能寻求一种有限的政策平衡。

欧盟网络安全政策的现实形态可以概括为“分层自主下的可控依赖”。2026年5月,欧盟委员会负责技术主权、安全与民主的执行副主席维尔库宁明确为技术主权划定了限度,指出技术主权“不意味着隔绝”,而是降低有风险的依赖、在关键节点建立替代选项。2026年,西班牙电信执行董事长马克·穆尔特拉(Marc Murtra)在巴塞罗那经济圈会议上强调,推动欧洲技术自主意在减少对海外市场的

① Office of the United States Trade Representative, “2026 National Trade Estimate Report on Foreign Trade Barriers,” March 31, 2026, p.190, https://ustr.gov/sites/default/files/files/Press/Releases/2026/National%20Trade% 20Estimate%20Report%202026.pdf.

过度依赖,而非走向孤立。[①] 在这一政策基调下,欧盟对不同领域采取分层治理策略,在关键基础设施控制层、敏感数据处理、加密技术等战略性领域,积极推动供应链审核,并提升自身技术能力,力求最大限度摆脱依赖;[②]而在多数应用层服务、消费类产品与非敏感数据处理领域,则长期保持开放,并容忍一定程度的依赖。[③] 这种"有选择地管理对外依赖"的安排,既是欧盟主动的选择,也是其在客观约束下的策略性妥协。具体而言,欧盟网络安全政策呈现出三个特征。

第一,在政策效能上,新型政策难以在短期内覆盖全部战略目标。安全自主范式为欧盟设定了一套层次分明、定位高远的目标体系,即将涉及安全领域的核心技术、供应链与基础设施纳入欧盟可控范围。近年来,欧盟已在制度设计层面推动供应链风险管理和跨境危机协同机制建设。例如,2026 年,信息和通信技术供应链安全工具箱建立了共同的风险识别、评估与缓解框架;[④]《网络团结法案》则设立了欧盟网络安全储备和跨境应急支持机制。但这些制度的实施程度并不一致:信息和通信技术供应链安全工具箱本身属于非约束性框架;《网络团结法案》实施时间较短;《网络韧性法案》的主要义务也要到 2027 年 12 月才全面适用。而

---

① Telefónica, "Marc Murtra: 'European Sovereignty Requires Simplifying Regulation, Building Our Own Technology and Accepting the Risk to Fail'," June 3, 2026, https://www.telefonica.com/en/wp-content/uploads/sites/5/2026/06/pr_marc_murtra_cercle.pdf.

② 相关政策参见 European Commission, "Communication on the Implementation of the 5G Cybersecurity Toolbox," June 15, 2023, https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox; NIS Cooperation Group, "EU ICT Supply Chain Security Toolbox," February 13,2026, https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security; European Commission, "Proposal for a Regulation of the European Parliament and of the Council Establishing a Framework of Measures for Strengthening Europe's Cloud and AI Ecosystem (Cloud and AI Development Act)," COM(2026) 502 final, Brussels, June 3, 2026, Articles 16, 29 and Annex II, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026PC0502。

③ 相关政策参见 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, "European Economic Security Strategy," JOIN(2023) 20 final, Brussels, June 20, 2023, Sections 1 and Section 3.3, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023JC0020; European Commission, "Cloud and AI Development Act," Shaping Europe's Digital Future, 2026, https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act。

④ NIS Cooperation Group, "EU ICT Supply Chain Security Toolbox," February 13, 2026, https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security.

在云服务、先进芯片等资本密集、市场集中度高且替代周期较长的关键领域,欧盟既有的能力差距仍然限制其自主目标的实现水平。“安全自主”目标在短期内仅能实现局部覆盖,无法达成全面落地。

第二,在政策转型上,各成员国政策落地实施进度落差较大,难以在短期内形成政策合力。欧盟多层治理结构意味着统一政策目标需要经过成员国国内立法、监管机构调整和具体执行等多个环节,可能产生实施时点、监管强度和能力建设上的差异。虽然最低标准、欧盟委员会监督和跨境协作机制能够在一定程度上缓解这种分化,但“欧盟层面的自主目标”与“成员国层面的执行能力和政策选择”之间的协调成本始终存在。这也会延缓政策工具的统一实施和整体能力的形成。

第三,在可持续性问题上,“安全自主”范式的长期推进需要持续的产业投入、技术积累与政治支持。欧盟已经将投资、监管改革和集体行动响应同时纳入网络安全战略框架,说明这一转型本身具有较高的资源与制度需求。尤为关键的是,“安全自主”政策范式在很大程度上是由外部战略环境与欧盟顶层战略调整驱动,其政策的制定与实施受自身整体战略与政治环境影响较大,在当前动荡变化的国际环境下,其可持续性难以保障。

总体而言,新范式下欧盟网络安全政策的实际效能、内部协调与可持续性仍受到现实条件制约。欧盟更多以局部自主替代全面自主,以分层执行落实统一目标,以渐进推进实现长期转型。欧盟并非放弃“安全自主”,而是在技术能力、制度结构与相互依赖约束下形成“有限自主”。这一现象也说明,在高度集中且相互依赖的全球技术体系中,即使具有较强市场和制度能力的行为体,其技术自主仍存在明显的限度与边界,而那些体量更小的国家在大国技术竞争中则更加难以摆脱对外技术依赖的局面。

五 欧盟网络安全政策范式转型的现实影响

作为全球最大数字单一市场中最活跃的规制性力量,欧盟在网络安全政策范式上的转型意味着其治理逻辑的根本变化,必将对欧盟自身的网络安全态势、跨

大西洋网络安全合作和全球数字治理格局产生深远影响。

(一)范式转变引发新的结构性风险与隐患

网络安全政策范式的转变,对欧盟自身网络安全态势的影响是双重而非单向的。新范式构建了一套远比“合规防护”时代更为立体的制度架构,使欧盟首次具备透视供应链、识别关键物资依赖、协调集体应对的潜在能力,其实质是为欧盟搭建掌控整体网络安全态势的制度性框架。然而,欧盟在寻求更多管理权限的同时,也导致新的结构性安全隐患产生。

第一重安全隐患源于范式转变所带来的战略透支。欧盟在自身能力尚未发展成熟时提升安全目标,试图重新审视并调整原有的供应链结构,其战略意图在某种程度上超出了现实能力的承载范围。“安全自主”范式要求欧盟对关键技术、供应链与基础设施实现自主掌控,但欧盟的实际能力并未实现同步增长;与此同时,旧范式所依赖的外部技术供给已被重新界定为必须摆脱的风险,而本土替代方案尚无法填补该缺口。这最终可能导致欧盟一方面承担着远高于以往的安全承诺,另一方面却不切实际地重构供应链,战略意图与实际能力之间的差距不仅没有因转型而缩小,反而进一步扩大,构成事实上的战略透支。

第二重安全隐患来自成员国政策转型不均衡导致的制度盲区。原有政策体系经过长期磨合,各成员国已基本构建起一套虽不算先进,但体系相对完整、运行状态稳定的合规治理架构。而新范式所要求的供应链审查、关键依赖识别、集体危机应对等举措,复杂度远高于传统管理模式,对各成员国的技术能力、行政资源与专业人才队伍提出了更高要求。在这一高门槛的筛选下,成员国之间的能力差距将被放大,部分成员国不仅难以充分履行新范式下的义务,其原本完整稳定的治理体系在改革进程中还出现大量过渡性空隙与监管盲区,反而提升了欧盟网络安全的脆弱性。

第三重安全隐患来自政策目标与政策工具集多元化和复合化带来的高昂协调成本。新政策范式下,欧盟网络安全治理覆盖的范围大幅增加,所需政策工具也更为复杂,有效协同也更为困难。随着网络安全治理范围和工具组合的不断扩展,企业合规成本可能随之上升。有欧洲电信行业组织(Connect Europe)警告,新

增监管要求可能给欧洲电信行业带来数十亿欧元的额外成本。[①] 这种高昂的协调与合规成本使得原本并不充分的欧盟安全治理资源变得更加紧缺,从而削弱欧盟整体的治理能力。

综合来看,政策范式转型对欧盟自身网络安全态势的影响是双重的。一方面,新工具集的引入与既有工具的功能重新编码,实质性扩大了欧盟的管理选项,为安全自主奠定了制度基础;另一方面,这种转型在改善欧盟网络安全的同时也会引发新的安全隐患,有可能加剧欧盟整体网络安全的脆弱性。

(二)欧美网络安全关系分化博弈加速演进

范式转型对跨大西洋网络安全合作的影响,体现为合作模式从“依赖共生”向“分化博弈”的转变。在“合规防护”范式下,跨大西洋网络安全合作建立在欧盟规则供给与美国技术供给的功能性互补之上。欧盟通过 GDPR 等规则塑造全球数字治理标准,美国通过其科技产业为欧盟提供底层技术基础设施,两者形成一种隐性的“规则—技术”分工。

但在“安全自主”范式下,这一前提的两端同时被动摇。一方面,美国政府将欧盟在“安全自主”思路下形成的法律规范视为一种“非关税贸易壁垒”,并向欧盟施压,迫使其放弃;另一方面,美国将技术依赖作为胁迫欧盟改变自身政策的“武器”的做法,再一次证明了传统上基于“盟友互信”的欧美技术共享已不再可靠。2025 年 10 月 15 日,欧盟安全研究所(EUISS)发布专题报告《低信任:在特朗普 2.0 下驾驭跨大西洋关系》,直言不讳地指出,特朗普第二任期以来,欧美在防务、贸易、技术发展等多个领域的合作已被大幅削弱。[②]

---

① 参见 Connect Europe, “Connect Europe Statement on the Cybersecurity Act,” Press Statement, Brussels, January 20, 2026, https://connecteurope.org/news/connect-europe-statement-cybersecurity-act; Jennifer Baker, “Pricey and Protectionist: New Cybersecurity Rules under Fire from the Start,” EU Perspectives, January 26, 2026, https://euperspectives.eu/2026/01/cybersecurity-act-faces-legislative-challenges/。

② Giuseppe Spatafora et al., eds., *Low Trust: Navigating Transatlantic Relations under Trump 2.0*, Chaillot Paper No.187, European Union Institute for Security Studies, October 15, 2025, https://www.iss.europa.eu/publications/chaillot-papers/low-trust.

在网络安全领域,该转变主要体现为:欧盟正通过《网络团结法案》、欧盟网络安全储备、可信信息和通信技术供应链框架等工具,提高欧盟在网络安全危机中的自主应对和行动能力。例如,欧盟通过《欧洲芯片法案》、海底电缆安全工具箱等政策工具,增强底层基础设施的本土建设能力;通过CSA2提案下的可信信息和通信技术供应链框架,建立针对包含美国供应商在内的第三国技术供给的可信度审查机制。上述政策表明供应中断、关键依赖和第三国供应商风险已经被纳入欧盟网络安全治理的视野,其治理目标转变为:在外部供给可能受到扰动的条件下,通过增强本土能力、供应多元化和风险缓解机制维持必要的网络安全行动能力。这些举措标志着跨大西洋网络安全关系正逐步从"高度互信基础上的功能性互补"转向"低信任条件下的安全博弈"。

此类分化博弈一经启动,便呈现自我强化的发展态势。欧盟为降低对美国的技术依赖所推行的可信供应链审查、本土产能建设和公共采购方向调整,客观上压缩了美国科技企业在欧洲的市场空间。这些举措很容易诱发美方的反制与政治施压,而美方的反制又会印证欧盟"外部依赖不可倚仗"的判断,推动欧盟更为坚定地推进技术自主进程。自主诉求与外部反制形成相互刺激的态势,可能会导致难以逆转的螺旋上升态势,推动欧美网络安全博弈持续加速演化。

(三)全球数字治理的日益碎片化与阵营化

欧盟政策范式的转变,正在推动其全球数字治理角色发生调整,并可能进一步改变欧盟数字规则的对外作用方式。长期以来,欧盟依托其庞大而开放的单一市场、较强的监管能力和统一而严格的规则体系,促使外部主体为进入欧盟市场而调整自身行为和标准,因而居于全球数字规则创制链条的重要位置。这种规则外溢不仅推动了部分欧盟标准在域外被采纳,也在数据保护、平台治理和数字市场监管等领域促进了跨国规则趋同,为全球数字治理规范的形成提供了重要制度参照。

在"安全自主"范式下,欧盟的政策逻辑不再仅将网络安全界定为技术风险与市场行为治理问题,而是进一步聚焦关键技术、基础设施和供应链的控制权,以及该控制权可能受外部政治权力影响的风险。当外部依赖被认定为可能在国家间

竞争中转化为战略脆弱性时,供应商来源、控制关系、第三国法律环境及外部政治影响等非技术因素便被纳入网络安全风险判断的范畴,欧盟网络安全治理的地缘政治属性也随之增强。2026 年,欧盟委员会《欧盟网络安全法》修订提案明确指出,信息通信技术供应链安全不仅取决于产品和服务本身的技术安全属性,还需要纳入依赖关系与外部干预风险的考量。① 这一逻辑已在 5G 供应商治理领域显现。欧盟委员会对华为、中兴的风险认定并未局限于产品是否符合统一技术标准,而是进一步依据 5G 工具箱设定的供应商风险标准,将非技术性脆弱性、外部影响及长期依赖等因素纳入评估框架,并于 2023 年明确认定两家企业相较其他 5G 供应商具有所谓的“更高风险”。② 这意味着,欧盟在部分领域的技术准入正逐步从主要依据产品和服务自身安全性的“技术合规”判断,转向“技术合规+政治安全可信”的双重判断,供应商的地缘政治属性由此成为影响市场准入的核心因素之一。传统依托统一标准与开放市场来扩大规则影响力的治理模式,也被安全化逻辑所重塑。更为重要的是,一旦政治关系、第三国法律环境和战略立场等非技术因素持续进入技术准入与供应链治理,不同国家和地区完全可能依据各自的安全判断形成差异化、排他性的“可信供应链”体系。这种基于政治安全判断的差异化准入难以完全通过统一技术标准实现互认,从而可能削弱全球数字规则的普遍适用性与相互兼容性,强化全球数字治理圈层化与制度碎片化趋势。

这一负面影响很可能通过政策示范效应被进一步放大。欧盟长期秉持开放、多边、规则导向的治理理念,是该理念的倡导者,其政策选择因而具有较强的国际示范意义。当欧盟自身也开始将供应商“可信性”、来源及第三国控制关系纳入技术供给风险评估时,可能进一步强化在大国技术竞争和地缘经济分化背景下的网络安全治理地缘政治化趋势,进一步增加全球网络空间治理按照政治属性的差异

① European Commission, “Proposal for a Regulation for the EU Cybersecurity Act,” Recital 132, Article 103(4), Article 105(2)(b).

② European Commission, “Commission Announces Next Steps on Cybersecurity of 5G Networks in Complement to Latest Progress Report by Member States,” June 15, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3309.

而形成不同治理圈层的可能性。一旦网络安全治理由依托规则对接的协作模式，滑向以阵营边界划分的对峙格局，全球性治理合作的开展也随之变得更为困难。

六 结语

当前欧盟网络安全政策正处于由“合规防护”范式向“安全自主”范式渐进转型的阶段。就政策目标维度而言，欧盟在合规达标这一基础性目标之外，进一步确立了“将网络安全主动权掌握在自己手中”的安全自主目标；就政策工具维度而言，原有合规规制工具得到保留与强化，但其制度功能正被重新定位，与产业政策、供应链审查、集体危机响应等新增工具协同形成复合型政策体系；就因果认知维度而言，掌握核心能力、识别高风险依赖、建立可替代方案以实现安全的全新认知，正成为推动欧盟网络安全政策发展的主要动力之一。

传统上，“布鲁塞尔效应”被视为欧盟维持其全球数字治理影响力的重要机制，然而规则的有效性最终仍需以技术能力作为支撑，倘若技术依赖被域外国家“武器化”，规则将不再是欧盟可单方面定义并强制推行的工具，反而会陷入受他国牵制的不利处境。基于这一认知，欧盟政策共同体开始重新界定“安全”与“权力”的关系。欧盟理事会等网络安全决策主体已经明确认识到，网络安全的实现无法依托单一规则供给，必须构建在多维度自主能力的物质基础之上。这种针对“规范性权力底层支撑”的根本性认知重构，正是欧盟治理范式调整的核心内涵。

但从实际运行状态来看，本次范式重构并未实现欧盟决策层理想表述中所预设的完善水平。欧盟立法与治理结构本身具备复杂性特征，这决定了其难以在短期内完成根本性政策调整，仅可在既有制度框架的边界内，通过工具重构与功能转码推进深层战略变革。受体制约束形成的发展路径，叠加关键技术领域存在的能力缺口、成员国执行能力的差异化特征，以及安全自主目标与开放经济原则之间的内在张力，最终使得本次范式重构呈现为“有限自主约束下的转型困境”。欧盟既清晰彰显了推进战略调整的明确意愿，也暴露了特定制度环境对其变革路径的客观限制。这种限制使得欧盟在关键基础设施、敏感数据、加密技术等战略领

域坚持高度自主的发展方向,而在多数应用层级与非敏感领域仍维持一定程度的外部依赖。该复合形态是欧盟在结构性约束条件下必须直面的现实。

就中国而言,欧盟此次政策转向的影响具有双重属性。一方面,作为该转向的直接成果,《网络韧性法案》规定的“软件物料清单”义务与 CSA2 提案提出的可信信息和通信技术供应链框架,可能推高适用范围内中国企业进入欧盟市场的合规成本。另一方面,欧盟此次转向所折射出的跨大西洋分歧,为欧洲在对华政策中保持独立判断、推动中欧在非敏感领域开展务实合作创造了一定的空间。中国可借助这一契机,推动中欧围绕网络安全认证、漏洞披露、软件物料清单等技术议题开展对话。同时,欧盟网络安全政策范式的转向,为中国构建自身网络安全治理体系提供了参考与启示。当前网络安全治理正逐步演变为规则治理与政治权力博弈深度纠缠的复合问题。中国可考虑持续完善合规规则体系,同时在关键技术环节培育替代方案,推动规则建设与能力建设深度融合,方能在持续演进的国际网络安全秩序中保持战略主动。

(**作者简介**:丁迪,同济大学政治与国际关系学院副教授;**责任编辑**:蔡雅洁)