

数智时代网络安全的治理挑战与法治因应

——以新修订《网络安全法》为中心

李辉 李章乐 邹嘉诺

摘要:数智技术的快速演进使网络安全治理面临结构性压力。传统以静态防护和单一主体为中心的治理模式,已难以应对现实挑战。2025年新修订的《中华人民共和国网络安全法》为回应挑战提供了一个值得关注的制度样本。从“压力—弹性”视角来看,网络安全治理体系本质上是一个长期承受多重压力的制度系统。其治理效果取决于规则整合、主体协作、机制联动与治理边界共同形成的制度弹性水平。结合当前数智时代的治理实践,可以归纳出四类典型的协同治理问题,即规则碎片化、权责错配、机制割裂以及跨境协调不足。新修订的《中华人民共和国网络安全法》的制度设计,通过规则衔接、责任重构、机制嵌入,尝试调节治理压力、提升制度弹性。研究表明,网络安全治理正从以往的单一规制转向协同治理,其核心逻辑是在不确定环境中增强制度系统的承压与调适能力,法律在其中扮演着弹性工具的角色。这一分析不仅有助于理解数智时代网络安全治理的内在逻辑,也为反思国家安全领域中“安全—发展”关系的动态平衡提供了一个可延伸的观察视角。

关键词:数智时代;网络安全;“压力—弹性”视角;协同治理

中图分类号:C931 **文献标识码:**A **文章编号:**1673-0186(2026)09-0076-15

当前,大数据、云计算、区块链、智能算法等信息技术方兴未艾,网络空间正加速向数据驱动、智能主导、万物互联的新生态转变,为经济社会发展带来了历史机遇。然而,技术发展的“双刃剑”效应也日益凸显。面对数据跨境流动失控、算法黑箱与歧视、高级持续性威胁攻击^①、关键信息基础设施供应链脆弱等新型、复杂、系统性风险,传统的以被动防御和局部管控为主的

网络安全范式弊端已显。习近平总书记指出:“没有网络安全就没有国家安全,就没有经济社会的稳定运行,广大人民群众的利益也难以得到保障。”^[1]网络安全治理事关国家安全和经济社会发展,事关国家利益和人民群众的根本利益,是网络空间治理的首要任务。

当前,以部门分割、事后处置为特征的传统网络安全治理模式已难以适应风险形态的变化。

基金项目:国家社会科学基金重大项目“国家安全法治体系、战略体系、政策体系、风险监测预警体系的统筹建设研究”(25&ZD204);中央高校基本科研业务费专项资金资助项目“数字智能时代国家安全治理前沿问题研究”(2025bsky026)。

作者简介:李辉,中国人民公安大学研究生院教授、博士生导师,研究方向:国家安全治理、公安管理;李章乐,中国人民公安大学国家安全学院博士研究生,研究方向:国家安全治理;邹嘉诺,南京信息工程大学马克思主义学院助理研究员,研究方向:马克思主义与当代研究。

^①高级持续性威胁(APT, Advanced Persistent Threat)攻击指具有国家或相关背景的黑客组织基于政治、军事或商业等重大利益目的,针对如国家、组织或个人等特定目标进行的一系列隐蔽网络攻击行为。《国家网络安全知识百问》编写组.国家网络安全知识百问[M].北京:人民出版社,2020:128.

面对跨领域、跨主体、跨空间的安全挑战,构建多元参与、规则协同以及技术与制度相互嵌入的协同治理模式已成为网络安全治理的重要趋势。当前我国已逐步形成以《中华人民共和国网络安全法》(以下简称《网络安全法》)为基础,与《中华人民共和国数据安全法》(以下简称《数据安全法》)、《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)等法律相衔接的法治框架,并通过行政法规和规章、技术标准和行业规范不断细化补充,总体上确立起我国互联网信息管理的“四梁八柱”^[2]。然而在实际运行中,这套制度体系仍暴露出规则衔接不畅、主体责任错位、执行机制条块分割及跨境制度摩擦等结构性张力,致使协同治理的应然优势尚未充分显现。治理效能的提升不仅依赖于规则体系的完善或监管力度的加强,更取决于治理体系在持续风险扰动下,是否具备保持稳定运行与自我调节的能力。

为此,本研究引入“压力—弹性”(Pressure-Elasticity, P-E)的分析视角^[3],将网络安全治理视为一个在持续风险压力下寻求制度适应与能力提升的动态过程,考察我国网络安全治理体系所承受的内外压力来源,剖析法律规则、组织结构、运行机制及治理边界等要素所构筑的制度弹性。结合 2025 年新修订的《网络安全法》,探讨法律工具在缓解系统性压力与提升治理弹性方面的作用空间,以期理解数智时代网络安全协同治理的运行逻辑提供有益参考。

一、网络安全协同治理的“压力—弹性”视角

数智时代,网络安全治理的突出特征在于风险类型、传导方式与影响范围的系统性变化。以习近平同志为核心的党中央明确提出了“风险综合体”^[4]的概念,强调政治、经济、社会等各个领域的风险因素以及风险在境内和境外之间不是孤立出现的,而是会相互耦合叠加、传导演化,形成系统性风险,带来全域性冲击。如果防范

不及、应对不力,就会传导、叠加、演变、升级,造成比单体风险元素更加重大的后果^[5]。为更好地掌握协同治理在多元风险叠加背景下面临的结构性张力,有必要引入能够反映动态过程与系统特征的分析框架。

(一)从静态防护到动态调适:“压力—弹性”视角的引入

数智时代造就了前所未有的社会系统复杂性,包括演化复杂性、认知复杂性和调控复杂性^[6],使得风险挑战呈现出与以往截然不同的特点。在传统安全治理范式,风险往往被视为可以通过明确识别、分级防控和技术加固予以消除的对象,相应的治理目标更多聚焦于降低风险发生概率或减少直接损失。然而,数智时代的连通性、中心性和扩散性三种机制,放大了社会风险的规模^[7]。这种变化的核心在于,网络安全风险正在从“外部威胁”演变为深度嵌入治理对象本身的“内生压力”。随着云计算、大数据、人工智能、物联网等技术的广泛应用,网络空间逐渐演化为高度互联的技术生态。技术系统内部各节点之间的依赖关系显著增强,无论是算法漏洞、数据污染还是算力中断等任何一个节点的失效,都可能通过数据链路和算法链路迅速扩展。更关键的是,技术系统已不再是外在于经济社会活动的工具,而是构成经济社会运行的基础设施。风险由此不再被“隔离”在系统之外,而是内生于技术系统运行过程之中。在组织运行层面,平台化模糊了传统组织边界,导致数据控制权、算法决策权与实际责任承担主体不断分离。平台企业既是数据资源的聚合中心,也是风险扩散的重要节点。组织之间高度依赖的数据共享与业务协同,在提升效率的同时,也放大了风险传导效应。这种组织间的高度耦合,在软件供应链领域表现得尤为典型。一个软件系统往往由大量第三方组件、开源库、容器镜像、云服务接口等拼接而成,涉及从上游开源社区到商业供应商、再到最终部署的多个环节^[8]。这些组件往往由不同商业实体或社区维护,一旦某个上游环节

的组件存在可利用的漏洞,就会影响到供应链的各个层级。

面对技术快速迭代,网络安全治理逐渐形成由法律规范、行政规章、行业标准与平台规则共同构成的复合治理体系。然而,制度的多元化在扩大治理覆盖面并提高治理效能的同时,但规则重叠、监管交叉等问题也使风险部分转化为制度运行成本,从而使风险不仅成为治理对象,也成为制度运行过程中的内生压力来源。由此,数智时代网络安全风险已经从传统的外部冲击演变为深度嵌入治理体系本身的系统性压力。这种系统性压力使得网络安全风险不再固守于某一特定领域或环节,而是凭借技术生态的高度互联、平台组织的数据贯通以及治理规则的多重嵌套,形成跨域联动的风险综合体。风险综合体内在要素的相互交织、连锁联动、外溢放大效应,体现在各级各类风险挑战的类型特点、时空演化、引致后果等不同维度^[9]。在这种情况下,单纯依靠事前防范或事后处置,已难以支撑治理体系的长期稳定。

“压力—弹性”视角提供了一种有助于理解这种变化的分析思路。该视角强调,治理体系处于持续承受外部冲击和内部扰动过程之中,维持运转效能的关键不在于能否完全避免风险,而在于是否具备缓冲冲击吸收影响并在必要时实现适应性调整的能力。引入这个视角,并不意味着否定既有安全防护措施的必要性,而是试图解析,在高强度、不确定的压力持续存在时,治理体系如何维持基本功能并避免结构失衡。需要注意的是本研究所使用的“压力—弹性”分析视角,并非对既有韧性治理(Resilient Governance)理论的简单移植。既有韧性治理更多强调系统在冲击后恢复既有功能或实现自我调整的能力^[10],多聚焦于抽象系统或组织形态,对制度工具本身的作用机理分析有限。相较之下,“压力—弹性”视角在三个层面存在明显差异:在时间维度上,韧性治理关注“事后恢复”,而“压力—弹性”视角更侧重于“事中承压”,即压力持续作用

时,制度体系如何保持运转;在分析对象上,韧性治理侧重于将系统视为一个整体,而本研究则试图打开制度体系的内部结构,考察法律规则、运行机制等不同制度要素在承压过程中的变化;在功能逻辑上,韧性治理强调的是系统对环境的被动适应与恢复,而“压力—弹性”视角更关注风险压力在治理体系内部是如何分布的,以及不同制度安排如何通过结构性设计,来缓冲或者转移这些压力。因此,“压力—弹性”视角并非替代韧性治理,而是将分析焦点从“系统整体在冲击后的恢复”下移至“制度结构在压力中的运行”,以期理解网络安全协同治理的内在机理提供一个更具制度分析穿透力的观察框架。

在网络安全协同治理的具体情境中,“压力”并非外部因素的简单叠加,而更像是一种复合性扰动,包括技术演进速度、数据要素流动方式、平台化的组织结构以及国际环境变化等。“弹性”也不等于系统自发的恢复能力,而应该囊括法律制度之间的协调程度、组织结构的配适能力、运行机制的响应效率以及治理边界的调适空间等。此外,本研究所使用的“弹性”概念,并非指传统治理模式完全不具有的某种属性。事实上,任何相对成熟的治理体系都具备一定的规则调适空间和主体协作能力——行政自由裁量、分层级授权、多部门会商等制度安排,都在不同程度上赋予了传统治理以灵活性。然而,传统治理中的“弹性”更多是一种被动应对式的缓冲空间,其功能主要是在既定框架内吸纳偶发性的扰动。这种弹性建立在两个前提之上:其一,风险的来源和类型是可预期、可识别的;其二,治理体系的边界是相对清晰的,风险可以在既定框架内被定位和处置。然而,在数智时代,上述两个前提正在瓦解:风险的生成不再局限于可识别的外部威胁,而是深度嵌入技术运行、组织协作与制度安排之中;治理体系的边界也不再清晰,云计算模糊了物理边界,平台化模糊了组织边界,数据跨境流动模糊了法

域边界。在这种条件下,传统治理中的“弹性”空间反而可能成为问题。例如,过大的行政裁量权可能导致执法标准不一,分层授权可能造成责任分散,多部门会商可能延误应急响应。因此,本研究所讨论的“弹性”,不是传统治理中那种被动应对式的缓冲空间,而是指治理体系在面临不确定性、跨域性和持续性压力时,通过结构性制度安排实现主动吸收冲击、快速恢复功能,并在必要时进行适应性调整的能力。

基于这一区分,本研究主张数智时代的网络安全治理正在从“静态防护”走向“动态调适”,即当风险压力持续上升时,治理体系能通过制度安排将压力转化为结构调整的动力。“压力—弹性”视角的重点不在于抽象讨论系统如何适应环境,而是聚焦于一个更为具体的问题,即治理弹性究竟是通过哪些法律工具和制度安排,一步步生成并发挥作用的。

(二)网络安全协同治理的系统构成与弹性来源

从系统角度看,网络安全协同治理是由多种治理要素共同作用的综合过程^[11]。为便于分析,将这一治理体系分成几个相互关联、功能各异的子系统。

在规则层面,网络安全治理依托宪法原则、法律规范、行政规章以及技术标准等多层级规则,构成基本制度框架。法治与基础制度层是数智时代网络安全治理的第一个层面^[12]。规则系统为治理行为提供了合法性基础,并通过制度衔接、层级安排等手段,影响不同治理主体的行为预期。规则之间的协调程度,直接关系到制度运行的稳定性。

在主体层面,网络安全协同治理涉及政府部门、网络运营者、平台企业、技术服务机构以及用户等多元参与者^[13]。不同主体在资源占有、专业能力与风险承受能力等方面存在显著差异,他们之间的权责配置以及互动方式,直接决定了治理体系能否形成合力。

在机制层面,网络安全治理离不开一系列

运行机制,包括风险监测、信息通报、应急响应、执法处置等。这些机制将抽象的法律规则转化为实际行动,是治理体系应对突发事件和持续威胁的直接抓手^[14]。它们的运行效率,对整体弹性起着关键作用。

在空间层面,随着网络活动的跨境化与数据流动的全球化,网络安全治理已难以完全局限于一国法域之内^[15]。域外规则、国际制度以及跨境执法合作等外部条件都会影响国内治理效果。图1是用于解释制度功能和风险互动关系的分析框架,图中各个要素不是孤立存在,而是通过协作运转共同影响治理效果:当规则、主体、机制以及空间安排能够相互配合时,治理体系在遭受冲击后仍可正常运转;反之,就可能运行不畅,甚至面临严峻挑战。譬如,2025年9月,公安部公布的“护网—2025”专项工作行政执法典型案例中,贵州某单位政务服务系统因运营者、承建方、运维方等未落实网络安全主体责任,未采取监测、记录网络运行状态等技术措施,未按规定留存网络日志,未及时处置系统漏洞等安全风险,遭网络攻击后造成群众财产损失400余万元^①。

上述案例中,相关主体均未履行《网络安全法》规定的义务——制定网络安全事件应急预案,及时处置系统漏洞、网络攻击等安全风险。当各主体既未落实事前防护,又缺乏事中监测与事后应急能力,任何一处脱节都可能导致治理体系在高强度风险冲击下运转受阻。

(三)“压力—弹性”视角下协同治理问题的结构类型

治理体系的“安全”不是一种静态属性,而是在持续的风险冲击下维持基本功能稳定的动态过程。任何治理体系安全性的核心在于能否在风险冲击下保持核心功能的正常运转。当治理

①中华人民共和国公安部.公安部公布“护网—2025”专项工作6起行政执法典型案例[EB/OL].(2025-09-18).
<https://www.mps.gov.cn/n2254098/n4904352/c10237071/content.html>.

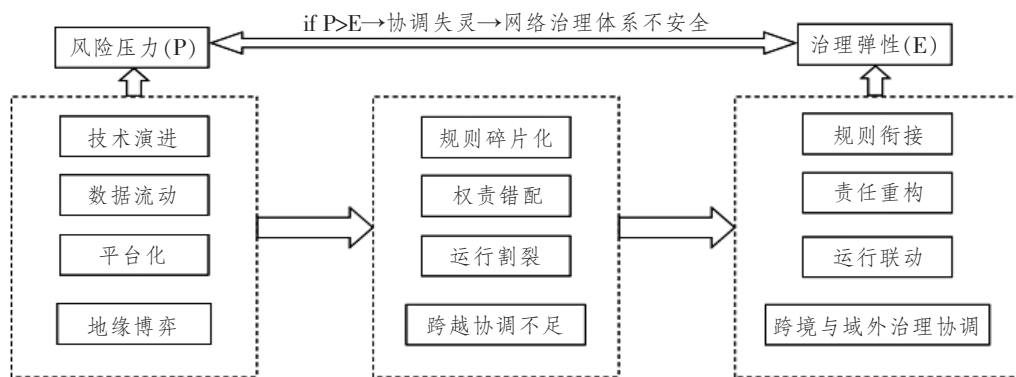


图1 治理“压力—弹性”分析框架

体系具备与压力相匹配的制度性缓冲能力时,压力处于弹性承载力范围之内,体系能够在冲击下维持基本功能;当压力持续累积且超出既有制度安排的调适空间时,治理体系便会进入弹性不足的状态——表现为响应迟滞、规则冲突、责任推诿或执行失衡。上述关系是一种结构性判断,而非精确的数学计算。本研究并不测量压力的数值和弹性阈值,而是通过考察压力来源的强度、持续性与扩散性以及弹性机制的存在与否、协调程度与响应效率,来综合研判治理体系是否处于弹性不足的状态。

在数智时代背景下,网络安全治理面临的压力具有多源性和叠加性特征^[16],其影响并不会平均分布于治理体系的各个层面,而往往集中表现为若干关键环节的弹性不足。对这些关键环节加以识别,有助于更有针对性地理解协同治理面临的现实困境。因而,本研究尝试从治理结构和治理空间两个维度,将网络安全协同治理中的相关问题进行划分,并对协同治理中弹性不足的集中表现加以归纳。

在治理结构维度上,协同治理结构性问题具体包括以下三类:一是规则层面。在现有制度体系中,不同法律、行政规章与技术标准在适用范围、调整对象和责任配置上存在差异,当规则之间缺乏有效衔接时,容易增加合规成本并削弱制度整体的引导能力。这种问题的根源,在于规则体系内部协调不足,弹性空间受限。二

是责任主体层面。多元主体参与本是协同治理的优点,但是如果权责划分不清、责任边界模糊,或者不同主体之间没有稳定的合作机制,“协同”反而可能导致责任分散,治理效率也随之下降。这类问题的根源,在于主体在压力情境下组织弹性不足。三是治理机制层面。即便在规则和主体安排相对明确的情况下,倘若风险监测、信息共享、应急响应和执法衔接等运行机制没有形成联动,那么面对突发风险或者复合风险时,治理体系还是会出现反应慢、处置脱节。这类问题,影响治理体系在压力冲击下能否快速响应。

在治理空间维度上,协同问题主要体现为跨境治理方面的外部约束。随着网络安全风险的跨境扩散,数字治理外溢性增强,国内治理效果逐渐受到域外规则冲突、执法协作不足以及国际制度博弈的影响^[17]。这类问题,更多体现为治理体系在外部环境变化时弹性边界的受限。

从上面的两类区分可以看出,四类协同问题处于不同的分析层面:前三类属于治理体系内部结构的问题,后一类则涉及外部空间条件对治理弹性的制约。正是在这两类维度的相互作用下,网络安全协同治理的“压力—弹性”关系才得以具体呈现出来。对这些问题类型做进一步分析,有助于为制度层面的回应提供更为清晰的参照。

二、网络安全协同治理的挑战

在“压力—弹性”框架下,网络安全协同治理中的诸多现实问题,可以被理解为治理体系的弹性不足。围绕前文所区分的内部结构维度和外部空间维度,本研究分别对四类协同治理挑战的具体表现展开分析,揭示内部逻辑,从而阐释挑战背后的结构性原因。

(一)规则层面:制度碎片化与弹性约束

在网络安全治理体系中,规则系统承担着界定权责、引导行为和稳定预期的基础性功能。然而,在数智时代风险快速演化的背景下,规则供给往往呈现出多层级、多来源并行推进的特征。当不同规则之间缺乏清晰的衔接与协调机制时,将压缩制度运行的弹性。

一方面,网络安全相关法律、行政法规与技术标准在调整对象、适用范围和责任指向上存在差异。例如,围绕数据安全、个人信息保护、算法治理等议题,不同规则体系分别从安全、权利或效率角度加以回应,这在一定程度上有助于风险的多维识别,但也容易在实践中形成合规逻辑分散、责任要求叠加的局面。尤其是,当跨行业经营主体企业的同一组数据需要适配不同行业标准时,则容易形成“多重标准适配”的难题^[18]。一旦被认定为“重要数据”,企业即面临本地化、安全评估等多重严格义务;若不同规则对同一活动的评估流程、主管机关要求不一,企业往往只能从严执行,极大提高合规成本,并陷入“漏判风险”或“过度合规”的两难境地。

另一方面,规则更新节奏与技术变迁速度之间的错位,也会削弱制度体系的调适能力。在有些领域,规则通过原则性条款或授权性规定为技术发展预留空间;但在另一些领域,规则越细化、越固定,后续调整起来就越困难。当不同规则在稳定性与灵活性之间采取的策略不一致时,整体规则系统的弹性协调便面临挑战。目前来看,关于算法透明度、公平性、可问责等义务,分散在《互联网信息服务算法推荐管理规定》《生成式人

工智能服务管理暂行办法》等文件中,各个文件的要求重点和尺度并不统一。算法推荐与生成式人工智能在应用场景、技术机理和风险特征上存在客观差异,分别制定规则具有合理性。但是在缺少高位阶统一标准的情况下,多元规则并存会增加企业合规成本与衔接难度。当技术迭代带来新型算法风险、构成新的扰动压力时,现有的分散且原则化的规则很难提供及时、一致的响应框架。这恰恰说明,现有法律体系在动态整合与精准适应方面存在弹性不足的问题。

从“压力—弹性”视角看,这类问题的关键在于规则体系内部协同不足,从而限制了整体弹性。当外部风险压力持续上升,不同规则之间缺乏衔接,无法在规则层面实现有效分流或者缓冲,压力将会转化为合规标准冲突与执法尺度不一带来的制度摩擦。这种摩擦并不是直接源自外部风险压力,而是内生于规则体系自身的协调问题,这本质上反映了技术快速演进过程中,立法如何在保障安全底线与促进创新发展之间寻求动态平衡的价值难题。

(二)责任主体层面:多元主体参与下的权责错配

协同治理强调多元主体共同参与网络安全事务,但多元并不必然等同于协同。在实践中,如果各方权责划分不清,协作机制又不够稳定,协同治理反而可能演变为责任推诿与效率下降的状态。

从纵向层级来看,网络安全治理涉及中央至地方的多个行政部门及其下属机构,不同部门在监管重点、执法资源和风险认知方面都存在差异。协调机制一旦不足,就容易出现政策传导偏差,治理压力在上下级之间往复传递,难以被有效消解。从横向协同来看,首先,同级职能部门之间职责交叉、主导权不明,削弱了制度响应与问责机制的执行效能;其次,政府、企业与平台的专业能力、风险承受能力本就不对等,这使责任分配更加复杂。特别是在平台化环境中,平台既是风险的承担者,也是治理的重要节点^[19]。如

果平台的责任边界缺乏明确界定,既可能导致过度合规,也可能削弱实际治理效果。此外,用户和社会组织在网络安全中的角色,往往更多体现为被动接受规则或事后维权,在风险预防和早期识别中发挥的作用有限。这种参与结构,限制了治理体系通过分散风险、共享信息来提升整体弹性的可能性。

从“压力—弹性”的角度来看,责任主体层面的协同问题,实质上反映了包含政府监管部门与平台企业在内的多元治理体系在压力情境下弹性不足。尤其当平台这一关键节点的权责边界模糊不清时,一旦风险集中爆发,权责错配就容易加剧治理困难,使多元主体之间难以形成稳定的协作关系。

(三)治理机制层面:运行割裂与响应迟滞

相较于规则和主体之间的协同,治理机制更能直接影响网络安全治理体系面对风险冲击时的反应能力。在数智时代,网络安全风险往往具有突发性、隐蔽性和复合性特征,这对风险监测、信息共享和应急处置的协同联动提出了更高要求。

实践中,不同治理环节之间的衔接不足,是机制层面常见的协同挑战。以应对高级持续性威胁(APT)事件为例,这类攻击给网络安全治理体系带来的扰动压力是多方面、持续久、高强度的。压力不仅源于攻击本身的潜伏周期长、隐蔽性强并具有极强的攻击目标定向性^[20],更来自应对过程中所需的跨层级、跨部门、跨地域乃至跨境的协同需求。如果风险监测和执法处置之间的信息流通不畅,可能会延误响应时效;如果应急响应与常态监管机制之间缺乏联动,也容易在突发事件中反应迟滞。技术系统不兼容、数据共享壁垒以及程序衔接繁琐,均有可能进一步加剧上述困难。据国家互联网应急中心(CNCERT)监测,2024年境外APT组织对我国重要单位实施网络攻击事件超过600起。然而在应急处置实践中,“有的单位在发生网络安全事件后,不知道该不该报、向谁报、怎么报,甚至出现瞒报、

迟报等问题,导致有的事件未得到及时有效处置,危害扩大或产生不良社会影响,同时,国家层面也无法全面掌握网络安全态势,难以有效组织开展联防联控工作。”^[21]风险监测、信息通报与应急处置之间的链条在关键环节上断裂,使本可被早期识别和控制的风险,最终演变为实质性危害。值得注意的是,机制层面的协同问题,并非完全源于执行力度不足,往往与制度设计中对稳定性和可控性的强调有关。在部分情形下,为避免权力滥用或误判风险,治理机制被设计为多重审核和分段运行,在常态下有助于规范运作,但是在高强度风险冲击下,这种制度惯性反而可能压缩应急反应的弹性空间,加剧协同治理难度。

(四)跨境与域外治理:外部空间约束与弹性边界

与上述三类内部结构性问题不同,跨境与域外治理协同问题本质上体现为治理体系在外部空间面临的弹性约束。随着数据跨境流动和网络活动全球化程度的加深,网络安全风险的生成与扩散已超出单一法域的制度边界。

从规则上看,不同国家和地区在数据保护、网络安全和数字治理方面的制度取向存在显著差异。域外立法和长臂管辖的扩张,让国内治理主体在合规选择上面临更为复杂的制度环境^[22]。在执法层面,跨境取证、协助调查和裁决执行等环节仍存在较高门槛,限制了治理措施真正发挥作用^[23]。这些因素共同构成影响国内网络安全治理弹性的外部约束。以中国科技企业“出海”的具体实践为例,跨境协调所面临的外部扰动集中体现在几个方面:数据跨境流动的“高标准”趋势持续强化、数据治理“国家安全化”取向日益明显,全球化与数据本地化之间的结构性张力则进一步加剧了这一矛盾;在技术供应链与算力层面,少数国家将出口管制与科技制裁政治化,通过“实体清单”与不断扩大的管制清单,对高端芯片、云计算等关键算力资源实施“断供”,意图切割全球产业链;而在规则话语权层面,部分发达

国家凭借先发优势将专利嵌入国际标准,构建“专利池”以抬高市场准入门槛,并通过频繁的“专利流氓”诉讼实施“法律围堵”^[24]。规则冲突、地缘博弈与供应链安全等问题的相互叠加,对中国企业与国家的数字主权及发展利益构成了系统性冲击。

此外,跨境与域外治理协同问题,反映了网络安全治理在全球层面的结构性不平衡。外部环境的不确定性上升时,国内治理体系的弹性边界随之受到挤压,内部结构性问题由此更容易被放大。

通过区分内部结构维度与外部空间维度,可以看到,上述四类协同问题并非彼此孤立,而是在“压力—弹性”关系中相互作用。正是在这种多维张力的交织下,协同治理的复杂样态得以呈现。对不同形态的系统分析,揭示了治理实践中亟待解决的问题。

三、制度回应:作为治理弹性工具的新修订《网络安全法》

在“压力—弹性”框架下,网络安全协同治理中的四类协同问题,集中反映了治理体系在不同维度上的弹性约束。将2025年新修订的《网络安全法》置于治理体系运行的具体情境中,考察新修订的《网络安全法》及其相关制度安排,如何作为法律工具嵌入治理结构,可对前述协同治理挑战形成回应与解释。《网络安全法》的修订是对以大数据、生成式人工智能等技术为核心驱动力的数智时代所衍生出的外部压力升级和治理弹性不足的法治回应。在“压力—弹性”视角下,法律不再被理解为单向度的规制手段,而应视之为化解压力、重构弹性的制度装置。

(一)规则整合与制度衔接

针对规则层面因价值取向协调不足而产生的制度摩擦,新修订的《网络安全法》在立法理念上首先确立了统筹高质量发展和高水平安全的基本导向。这次修法贯彻落实了习近平总书记

关于网络强国的重要思想和总体国家安全观,力求把握好数字化、智能化背景下发展和安全之间动态平衡、相互促进的辩证统一关系。价值层面的统合,为化解不同法律间因调整对象差异而产生的衔接张力确立了顶层依据。修法将原第十八条拆为两款,并增加一条作为第二十条,既明确“国家支持人工智能基础理论研究和算法等关键技术研发,推进训练数据资源、算力等基础设施建设”“国家支持创新网络安全管理方式,运用人工智能等新技术,提升网络安全保护水平”,又同步强化全链条风险防控机制,要求“完善人工智能伦理规范,加强风险监测评估和安全监管,促进人工智能应用和健康发展”^①。可以看出,修法兼顾了风险防控与主动适应技术演进趋势的双重目标。然而,这一修改设计的内在张力同样值得关注。修改并未对主体内容作实质性重构,而是聚焦于法律责任的局部完善。这种“小切口”思路虽然减少了修法阻力,却也意味着治理体系的结构调整仍需依赖后续立法。另外,人工智能条款在立法过程中亦存在争议。审议过程中,部分代表委员认为草案第二十条“国家支持人工智能基础理论研究和算法等关键技术研发”与《网络安全法》关联度不强,部分表述甚至超出法律适用范围^[25]。这一争议折射出深层制度难题——当一部以安全为核心功能定位的基础性法律开始增设“支持研发”等促进性条款时,其规范边界究竟应延伸至何处?“安全法”与“产业促进法”的功能区分,仍是一个尚未完成的立法课题。

在制度衔接上,修订通过引入弹性化规则工具,在一定程度上回应了上述张力,提升了法律体系的协同性。一方面,修订通过原则性规定和衔接条款,例如,新法第二十条关于人工智能研发与安全监管并重的原则性规定、第二十三条

^①中央网络安全和信息化委员会办公室,中华人民共和国国家互联网信息办公室.中华人民共和国网络安全法[EB/OL].(2025-12-29).https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm.

关于网络安全等级保护与数据分类管理的衔接安排,在规范层面初步搭建了网络安全、数据安全与个人信息保护之间的协调框架,增强了不同规则体系之间的衔接基础。这种处理方式多部法律之间的协同运行搭建了制度接口,从而在一定程度上缓解规则碎片化对治理弹性的挤压。另一方面,修订引入了分类分级管理、差异化合规要求以及授权性条款等弹性化规则工具,为监管部门根据风险变化和技术发展预留了动态调整的空间。这种制度设计并不是要放松安全要求,而是试图通过减少刚性规则之间的直接冲突,避免合规压力在规则层面无序叠加,让制度体系在承压状态下仍具备一定的自我调适能力,但是弹性设计仍面临落地挑战。法律文本虽然确立了方向和框架,但是规则之间的实际衔接操作、跨部门的协调等,仍可能在运行中被转化为新的压力源。从“压力—弹性”视角看,当前的制度设计,旨在提升治理体系在规则层面的整体弹性,使外部风险不至于过度集中在制度摩擦上。

(二) 责任配置与角色分化

针对责任主体层面的协同挑战,新修订的《网络安全法》从责任配置和角色分化入手,重新梳理了多元主体之间的权责关系。理解这一制度设计,需要同时把握其分层逻辑与结构性张力。

在制度逻辑上,此次修法在延续国家主导治理的同时,更加注重在制度层面体现不同治理主体的功能差异。根据全国人大常委会法制工作委员会在修正草案说明中的阐述,此次修法坚持“分类施策”原则,科学设置不同类型违法行为的法律责任^[26]。宪法和法律委员会审议报告进一步明确,修法旨在“完善法律责任制度”^[27]。

在政府层面,修订明确了各部门的监管职责边界和协作机制,为部门之间的协调提供了制度基础。在企业 and 平台层面,修订通过区分一般网络运营者、关键信息基础设施运营者以及特定服务提供者的责任类型,构建了一个分层次、差异化的责任体系。例如,新法第六十一条尤其强

化了对关键信息基础设施运营者的义务要求与法律责任——基于其在经济社会运行中的特殊地位,法律对其设定了更高标准的网络安全保护责任和更严格的法律后果^[28]。后续审议中对此予以肯定,认为修法“通过提升罚款限额上限、明确处罚程序、强化供应链安全、压实个人责任等,提升了法律的威慑力和执行力”^[29]。而对于一般网络运营者,则依据规模、业务类型及风险等级划定相应责任范围,避免“一刀切”带来的监管僵化。然而,这一分层责任配置的结构张力同样值得关注。一方面,设定罚款上限的处罚模式可能会削弱法律的威慑作用;另一方面,差异化责任配置在“分类”层面实现了制度创新,但在责任与风险实际匹配层面仍有待完善。此外,责任标准的提高也可能加剧大企业与中小企业之间的能力鸿沟。

修订虽在制度层面明确了网络运营者的义务,但并未详细规定如何履行这些义务,因而义务的履行仍需依赖配套制度与技术手段的支撑。具体而言,网络运营者应当按照网络安全等级保护制度的要求,从不同维度落实安全保护义务。例如,在制度层面,制定内部安全管理制度和操作规程,确定网络安全负责人,落实网络安全保护责任。在技术层面,采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施;实施数据分类,推进重要数据备份和加密。另外,还应该建立网络运行状态监测与网络安全事件记录机制,并按照规定留存相关的网络日志不少于六个月。这些义务的履行不能仅靠法律条文的原则性规定,还需要行业标准、技术指南和第三方评估等配套机制的协同支撑。未来应在《网络安全法》的框架下,进一步制定分行业、分场景的细化指引,将法律的原则性要求转化为可操作、可评估的具体标准。

此次修订通过引入多层次的责任配置和引导性条款,系统性地拓展了协同治理的组织基础。在不削弱国家监管权威的前提下,法律明确鼓励行业组织、技术机构及社会力量参与治理。

当风险集中出现时,能够通过分散承压点来增强整个治理体系的弹性,这一点以人工智能为代表的新兴技术领域尤为明显。修订首次在基础性法律中设立了专条,一方面表明支持技术研发的立场,另一方面也要求完善伦理规范与安全监管。该条款不仅为技术发展提供了法律依据,更重要的是确立了国家引导、行业与社会协同参与的治理框架。实际上,这是以法律形式明确了多元主体在应对新兴技术系统性风险中的共同责任,利用制度设计来确保具体场景的多元利益相关者实现风险共担的动态治理^[30],为后续构建“基础法+专门法”的协同治理体系奠定了基础,构成了一种对技术风险演化趋势的前瞻性制度安排。

(三)机制嵌入与运行联动

针对治理机制层面因标准不一,程序烦琐而导致的跨部门协同响应迟滞,新修订的《网络安全法》主要以跨部门联动的运行优化为导向,间接回应机制嵌入难题。梯度化处罚优化了跨部门协同执法的裁量基准,在源头上减少跨部门衔接摩擦。具体而言,法律依据危害程度将违法行为细分为“一般违法”“拒不改正或情节严重”以及“造成特别严重影响或后果”等梯度,并匹配相应强度的处罚。在缺乏此类梯度化标准的情况下,不同部门对同类违法行为的定性和处罚往往存在显著差异,这不仅增加了企业的合规不确定性,更提升了跨部门联合执法的协调成本。梯度化设计通过明确不同违法情形对应的法律后果,使各执法部门在协同行动中形成统一的判断框架,从而在一定程度上减少因标准不一导致的衔接摩擦。在此基础上,修订还明确引入了《中华人民共和国行政处罚法》中关于从轻、减轻或不予处罚的适用规则。这使得网络安全执法既能保持必要的威慑力度,又能体现过罚相当、包容审慎的现代法治理念^[31],确保了执法尺度在整体法治框架内的一致性。

这种梯度化标准对跨部门协同执法具有积极意义。其一,它使有限的执法资源能够向防

范和处置具有系统性、重大性危害的网络安全事件集中,有助于提升监管的精准化水平。其二,梯度化设计为创新型中小企业提供了适度的容错空间,有助于在安全底线之上营造规范有序又充满活力的发展环境^[32]。其三,该机制通过为不同违法情形预设明确的法律后果,在一定程度上缓解了因程序僵化导致的响应迟滞,使治理体系在面临突发或复合型风险时具备更强的短期响应能力。

然而,上述效果的产生高度依赖于若干配套机制的协同运行,而这一点恰是此次修法的制度供给相对薄弱之处。梯度化处罚的直接功能在于统一执法尺度,其向“运行联动”的转化,尚需经由信息共享标准、跨部门联合执法程序等一系列配套机制才能实现。修法虽然确立了处罚的梯度框架,却未对风险监测结果如何转化为执法启动依据、不同部门在应急状态下如何实现信息实时共享、联合执法的牵头主体与协调程序如何确定等关键问题作出实质性规定。这意味着,在缺乏配套实施规则的情况下,梯度化设计的规范效应仍可能因部门间的信息壁垒与程序分歧而被稀释。

此外,修法本身也蕴含着若干结构性张力。其一,裁量权的精细化与裁量权的规范化并非同一概念。梯度化设计在赋予执法机关更大裁量空间的同时,也增加了裁量权滥用的潜在风险,尤其是在“特别严重情形”的认定标准尚付阙如的背景下,不同地区、不同部门的执法尺度差异可能以新的形式再现。目前,地方层面已有《新疆维吾尔自治区网络安全管理行政处罚裁量权基准适用规定》《上海市公安局关于网络安全管理行政处罚的裁量基准》等规范性文件,这些地方探索为细化裁量标准积累了有益经验,但也反映出各地在违法情形分级、处罚幅度设定、从轻减轻条件等方面存在差异。这种差异在单一法域内或许尚可容纳,但在跨地域经营的网络平台面前,则可能转化为选择性执法与合规预期不稳的制度风险。其二,责任分层的精细化可能

无意中固化而非缩小大企业与中小企业之间的能力鸿沟——即便法律设定了差异化的责任梯度,中小企业因资源约束而难以达到基本合规要求的情形并未获得制度性纾解,过高的合规门槛反而可能使其陷入“违法常态”。其三,修法确立的梯度化框架与《数据安全法》和《个人信息保护法》中的处罚规定在逻辑上具有一致性,但具体处罚幅度的衔接、竞合情形下的法律适用规则等,仍需后续立法或司法解释予以明确,否则跨法适用的协调成本可能从执法前端转移至司法后端。

从“压力—弹性”视角审视,此次修法在机制层面的制度创新具有方向上的合理性。它通过梯度化设计使法律工具能够在不同强度的风险压力下释放差异化的规制效果。但同时也应清醒地认识到,从“处罚梯度统一”到“运行机制联动”之间,仍存在显著的制度落差。填补这一落差,有赖于国家网信部门会同相关主管部门尽快制定配套的行政处罚裁量基准实施细则,明确“一般违法”“情节严重”“特别严重影响或后果”的判定标准,并同步建立跨部门执法信息共享平台与应急联动程序。唯有如此,梯度化设计的制度红利才能从纸面走向实践,真正转化为治理体系在机制层面的弹性提升。

(四)域外适用与规则衔接

针对跨境与域外治理协同挑战,新修订的《网络安全法》在坚持以国内治理为主的同时,逐步加强了对境外的制度回应。法律明确了域外适用情形和跨境数据流动的基本规则,为国内治理体系应对外部不确定性提供了制度支点。

在规则层面,修订并没有试图单靠本国法律解决国际规则冲突,而是通过原则性规定和程序性要求,让国内制度在跨境治理中具备更高的可识别性与可对接性。具体来看,原第七十五条修改为第七十七条,内容调整为:“境外的机构、组织、个人从事危害中华人民共和国网络安全的活动的,依法追究法律责任;造成严重后果的,

国务院公安部门 and 有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。”^①旧法仅对“危害关键信息基础设施的活动”适用域外管辖,而且要求“造成严重后果”。在“活动范围”和“危害结果”的双重限定下,很多境外主体实施的网络攻击行为难以被完全覆盖。新法则把适用范围从“危害关键信息基础设施”扩展为“危害中华人民共和国网络安全的活动”。进言之,所有境外主体实施的网络攻击、数据窃取、非法控制等危害我国网络安全的行为,都可以依法追究。扩大规制范围后,我国就能对境外各类网络安全威胁行使管辖权,对跨境网络攻击形成更强的威慑力。

这次修订进一步明确了我国网络安全监管的域外适用情形,不仅扩大了法律的管辖范围与威慑效果,也清晰宣示了我国在网络空间的主权立场与司法态度。此举为应对跨境网络攻击、数据非法出境等日益突出的安全威胁提供了直接有力的法律武器,增强了我国在全球网络治理中的主动性与规则塑造能力,体现出我国增强维护和塑造国家安全的战略主动^[33]。

总的来说,此次修订方向彰显出立法者统筹国内国际两个大局的战略思维。既要用法治来引导和规范国内新技术、新业态的发展,又注重构建与我国国力地位相匹配、与安全形势相适应的涉外网络法律制度,从而在动态发展的内外部环境持续筑牢国家网络安全屏障。从“压力—弹性”视角看,域外适用和规则衔接并不是无限扩张治理边界,而是在外部空间约束下,通过法律工具把弹性边界明确出来,让国内治理体系在面对外部压力时具备更为稳定的制度预期。统筹推进国内法治和涉外法治,严格依照法定权限、法定程序开展国家安全执法司法,引导人民群众自觉遵守国家安全法律法

^①中央网络安全和信息化委员会办公室,中华人民共和国国家互联网信息办公室.中华人民共和国网络安全法[EB/OL].(2025-12-29).https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm.

规,为推进国家安全体系和能力现代化奠定坚实法治保障^[34]。

《网络安全法》的修订,从规则整合、责任重构、机制嵌入与域外衔接等几个方面回应了网络安全协同治理的挑战。这些调整并非旨在消除风险本身,而是在承认风险长期存在的前提下,提升网络安全治理体系的弹性。从“压力—弹性”角度看,新法就像是数智时代里应对协同治理难题的“弹性工具”,其作用在于提供制度依据和规则框架,而不是治理能力的全部。法律文本只是法治的一环,如果说法律规范体系重在解决“有什么法”的问题^[35],那么法治的完整实现,还需解决“法怎么用”“法怎么用好”“法依靠什么运行”的问题,也就是说,执法、司法、守法等各个环节都需要协同推进。

在执法层面,修法确立的原则性义务不能停留在纸面上,需要转化为一线执法人员可操作、可检验的具体标准。监管机关应加快制定分行业、分场景的执法指引,将安全保护义务、重要数据保护、人工智能安全评估等原则性规定细化为具体的检查指标与裁量基准。同时,应依托修法明确的梯度化处罚框架,建立常态化的执法协作机制,推动网信、公安、工信等多部门形成统一执法逻辑,避免碎片化。司法层面,修法为网络安全民事侵权、行政争议与刑事追责提供了更为清晰的法律依据。司法机关应通过典型案例的裁判,进一步明确网络运营者的安全保护义务边界、数据泄露中的过错认定标准以及平台责任的具体构成要件,以司法裁判的示范效应填补法律原则与实践之间的落差。在跨境数据纠纷、算法侵权等新型案件中,法院应积极发挥司法解释的功能,逐步形成与修法精神相契合的裁判规则。守法层面,法律的实效最终取决于治理主体对规则的认同与遵从。修法以弹性条款释放了包容审慎监管信号,应借此引导企业从“被动合规”转向“主动治理”,通过行业标准引导与激励机制等手段,让网络安全内化为企业日常运营。同时,加强公众宣传,让多元主体真正成为治理弹性的

贡献者。

因此,《网络安全法》的修订不应被视为制度建设的终点,而应被理解为一项制度升级的起点。法律文本确立了方向与框架,但治理弹性的真正生成,还取决于执法精细化、司法专业化与守法自觉化的持续推进。唯有在“有法可依”的基础上,进一步实现“有法必依、执法必严、违法必究”的制度闭环,才能使修法的制度红利转化为实实在在的治理能力。

四、结论与展望:从网络安全法治到国家安全治理弹性

进入数智时代,网络安全早已不只是技术议题,而是慢慢渗透到经济运行、社会治理乃至国家安全体系的基础性问题。面对风险的高度不确定性与持续变化的技术环境,我们需要的法治体系是既能守住安全底线,同时又不阻滞创新发展的脚步,而这一点正是当下网络安全法治建设的核心难题。

本研究从“压力—弹性”角度出发,分析了网络安全协同治理在复杂动态环境下的实际运行逻辑。网络安全协同治理的关键并不在于彻底消除风险,而在于治理体系能否在多重压力下保持基本稳定,并具备必要的调适与恢复能力。本研究把网络安全协同治理中比较突出的问题归纳成四类——规则层面、责任主体层面与治理机制层面集中反映了治理体系内部结构在承压条件下的弹性不足;跨境与域外治理层面,更多是外部环境变化对治理体系弹性边界的制约。这四类形态并不是彼此割裂的,而是在“压力—弹性”关系中互相影响,最终共同决定了协同治理的实际效果。

从制度回应来看,新修订的《网络安全法》通过规则整合、责任配置、机制嵌入与域外衔接等一系列制度创新,着力于优化治理结构,从而提升整个体系面对多重压力的弹性能力。这也在提醒着我们,网络安全乃至国家安全的法治功能定位,应该超越传统视域下静态规则集合或单一

规制工具的定位,转而强调法律在治理体系中的结构性角色——法律通过协调各方力量、调节风险压力的分布,提供了制度基础,从而深度参与治理弹性的建构过程。认识到这一点,我们就能跳出西方“安全—发展”二元对立的分析范式,将两者放在动态平衡和系统调适的框架中重新审视,从而更全面地阐释“统筹发展和安全”的理论逻辑与实践逻辑。

在方法论层面,“压力—弹性”视角可以往外延伸至更广阔的国家安全治理领域。网络安全治理所呈现的高复杂性、强不确定性与显著外溢性等特征,在科技安全、数据安全、能源安全等诸多国家安全领域中同样存在。风险往往是系统生成与扩散的,传统上依赖某个部门或单一工具的治理模式日益乏力。引入“压力—弹性”框架,能够帮助我们从动态复杂系统的角度,审视不同安全领域之间的内在关联与联动效应,进而理解制度安排在面对多重风险叠加时,如何实现缓冲和自我调整。然而,这种视角外推,并不意味着简单套用具体制度经验,更多的是提供一种分析复杂治理问题的工具性视角。

需要指出的是,本研究仍存在一定的局限。受研究篇幅与研究方法所限,本研究主要从规范分析和制度解释的角度展开讨论,尚未对治理弹性的实际运行效果展开充分的实证检验。关于跨境与域外治理的分析,更多侧重制度层面的结构性约束,对国际实践中具体差异与动态博弈的探讨尚显不足。未来研究可以在此基础上,进一步结合案例研究或定量分析方法,对网络安全协同治理中弹性机制的运行效果进行实证考察;同时,也可从比较法或国际政治经济学的综合视角出发,深化对跨境网络安全治理问题的理解。通过多方法、多视角的交叉研究,有助于进一步丰富网络安全治理与国家安全法治研究的理论内涵。

参考文献

[1]彭波,张璁,倪弋.迈出建设网络强国的坚实

步伐——习近平总书记关于网络安全和信息化工作重要论述综述[N].人民日报,2019-10-19(1).

[2]支振锋.网络安全风险与互联网内容治理的法治化[J].改革,2018(1):44-46.

[3]李晓玲,修春亮,孙平军,等.安全导向的屯垦戍边地区城镇化转型研究——以新疆南疆四地州为例[J].地域研究与开发,2016(5):67-71,80.

[4]习近平.在党的十八届五中全会第二次全体会议上的讲话(节选)[J].求是,2016(1):3-10.

[5]陈刚.系统推进国家安全风险综合体治理[N].学习时报,2026-01-07(7).

[6]王芳,郭雷.数字化社会的系统复杂性研究[J].管理世界,2022(9):208-221.

[7]向静林,艾云.数字社会发展与中国政府治理新模式[J].中国社会科学,2023(11):4-23,204.

[8]王江,姜伟,张璨.开源软件供应链安全风险分析研究[J].信息安全研究,2024(9):862-869.

[9]钟开斌.构建新安全格局:逻辑起点、理论指引与实践进路[J].人民论坛·学术前沿,2023(19):5-14.

[10]杨立华,刘华宇,马壹.韧性治理:含义、范式变迁和一个新整合框架[J].治理研究,2025(3):4-26,2,158.

[11]张凌寒.迈向系统深化与协同治理的网络安全法治新阶段[J].中国网信,2026(1):65-67.

[12]吕宪栋,白延涛,班元浩.数字经济时代网络安全治理:制度逻辑、治理框架与发展路径[J].价格理论与实践,2025(8):76-81,263.

[13]中国科学院学部重大咨询项目子课题“信息技术支撑网络社会治理现代化战略研究”课题组,管晓宏,房超,等.数字政府赋能网

- 络治理的挑战与应对[J].国家治理,2023(16):51-55.
- [14]周辉,姜伟.健全网络生态治理长效机制[J].红旗文稿,2026(4):8-12.
- [15]鲁传颖.全球网络安全形势与网络安全治理的路径[J].当代世界,2022(11):48-52.
- [16]钟开斌.统筹发展和安全:理论逻辑、历史逻辑与实践逻辑[J].天津行政学院学报,2025(4):28-36.
- [17]张邦辉,林旭凌.全球数字治理的理论困境、根源解析与中国方案[J].理论探索,2025(6):76-86.
- [18]王桂芳.大国网络竞争与中国网络安全战略选择[J].国际安全研究,2017(2):27-46,149.
- [19]赵忠璐,李红权.从“不可无”到“无不可”:平台化风险及其治理——基于行动者网络理论[J].东北大学学报(社会科学版),2023(5):90-98.
- [20]Chen T M, Zheng C B, Zhu T T, et al. System? level data management for endpoint advanced persistent threat detection: Issues, challenges and trends[J]. Computers & Security, 2023, 135: 103485.
- [21]严寒冰.规范网络安全事件报告筑牢数字空间安全防线[J].平安校园,2026(1):76-80.
- [22]霍政欣.中国企业应对非传统涉外法律风险的道与术[J].中国应用法学,2026(1):53-69.
- [23]冯俊伟.《联合国打击网络犯罪公约》框架下跨境取证制度的发展[J].苏州大学学报(哲学社会科学版),2026(1):65-74.
- [24]张欣,周密,肖允丹,等.中国科技企业“出海”:战略机遇、风险挑战与法律应对[J].数字法治,2025(4):10-26.
- [25]张子璇.全国人大常委会会议分组审议网络安全法修正草案二审稿 筑牢未成年人网络安全防线[N].检察日报,2025-10-27(2).
- [26]王瑞贺.关于《中华人民共和国网络安全法(修正草案)》的说明——2025年9月8日在第十四届全国人民代表大会常务委员第十七次会议上[J].中华人民共和国全国人民代表大会常务委员会公报,2025(6):804-805.
- [27]黄明.全国人民代表大会宪法和法律委员会关于《中华人民共和国网络安全法(修正草案)》审议结果的报告——2025年10月24日在第十四届全国人民代表大会常务委员第十八次会议上[J].中华人民共和国全国人民代表大会常务委员会公报,2025(6):806-807.
- [28]梁思雨.基于《中华人民共和国网络安全法》修改视角的关键信息基础设施保护法治进阶研究[J].中国信息安全,2026(2):46-49.
- [29]舒颖.网络安全法修正草案初审:加大处罚力度强化法律衔接[J].中国人大,2025(19):22.
- [30]季卫东,赵泽睿.法律如何实现动态治理——人工智能不确定性的立法应对[J].学术月刊,2025(3):98-109.
- [31]中央网信办网络法治局.认真贯彻实施网络安全法切实筑牢国家网络安全屏障[J].中国网信,2025(11):18-20.
- [32]张恒军,杜龙钰.生成式人工智能环境下的网络空间安全治理新进路[J].新媒体与社会,2024(2):49-59,401-402.
- [33]傅小强.增强维护和塑造国家安全战略主动——“十五五”时期全面推进国家安全体系和能力现代化[J].国家治理研究,2026(2):20-30.
- [34]陈一新.提升护航高质量发展的国家安全能力[J].求是,2026(8):47-51.
- [35]周叶中.法治体系论——学习习近平法治思想关于法治体系论述[J].求是,2026(7):38-42.

Governance Challenges and Legal Responses to Cybersecurity in the Digital Era: Centered on the Revised Cybersecurity Law

Li Hui Li Zhangyue Zou Jianuo

Abstract: The rapid evolution of digital and intelligent technologies has placed structural pressure on cybersecurity governance. Traditional governance models centered on static protection and a single governing actor are increasingly inadequate to address real-world challenges. The revised Cybersecurity Law of 2025 offers a noteworthy institutional example in response to these challenges. Drawing on the “Pressure-Elasticity” perspective, the cybersecurity governance system can be viewed as an institutional system enduring multiple pressures over time. Its effectiveness depends on the resilience level shaped collectively by rule integration, stakeholder collaboration, mechanism coordination, and governance boundaries. Focusing on governance practices in the digital-intelligent era, this study identifies four key challenges in collaborative governance: fragmented rules, misaligned responsibilities, disconnected mechanisms, and inadequate cross-border coordination. By analyzing the institutional design of the revised Cybersecurity Law, it examines how legal frameworks address governance pressures and enhance institutional resilience through rule harmonization, responsibility restructuring, and mechanism embedding. Research shows that cybersecurity governance is transitioning from singular regulation toward collaborative governance, with its core goal being to strengthen systems’ capacity to withstand and adapt to pressure within uncertain environments—where law functions as a tool for enhancing resilience. This analysis contributes to understanding the operational logic of cybersecurity governance in the digital age and provides an extendable perspective for reflecting on the dynamic balance between security and development in national security domains.

Key Words: Digital and Intelligent Era; Cybersecurity; “Pressure-Elasticity” Perspective; Collaborative Governance

(责任编辑:易晓艳)