法商研究 Studies in Law and Business
Vol. 42 No. 4(2025)

网络与信息法

超级平台国家安全自治及其监管

杨 永 红*

摘 要:随着超级平台渗透人类社会活动的方方面面,超级平台自治的私权力已扩张到传统国家公权垄断的国家安全领域。超级平台的崛起正在以新的方式塑造国家安全的治理。由于超级平台具有私人中介实体的法律地位,禁止一般监管与中介责任豁免原则成为超级平台自治的一般性原则,权力主体的错位使国家缺乏法律手段对超级平台公权私用进行监管。尽管欧盟对超级平台的监管已向强监管模式转向,但并未改变超级平台自治的一般性原则。因私主体进入公权领域而产生的结构性矛盾使美国能够借助非正式监管有效地影响超级平台国家安全自治,同时逃避公权所应受到的国内法与国际法的限制,在缺乏法律与领土限制的情况下隐蔽地实现了美国的长臂管辖。在私人第三方争端解决机构尚未构成对超级平台的有效限制、科技外交未能促成国际监督机制的情况下,美国超级平台的国家安全自治放大了美国的数字霸权。中国一方面,应积极支持我国大型平台的全球发展,并建设有中国特色的超级平台国家安全自治监管模式,以平衡美国数字霸权;另一方面,应在联合国框架下大力构建多利益攸关方参与的国家与私主体合治的国际监督机制,为构建网络空间命运共同体提供治理经验与发展基础。

关键词:超级平台 国家安全 平台自治 公权私有化

当今社会,拥有超大型网络平台(超级平台)的跨国科技公司已经变得极具影响力,正在积累以前只有国家才能享有的财富、国际影响和跨国利益。① 在技术与国家安全的交集上,拥有全球性互联网平台的商业巨头成为影响国家安全的重要力量。它们不仅仅是全球政治游戏的参与者,而且往往也是游戏舞台本身。这些“技术利维坦”②正越来越多地承担起国家在国家安全治

* 西南政法大学国际法学院、区域国别学院教授
基金项目:国家社会科学基金资助项目(22XFX009)

① See John W. Cioffi, Martin F. Kenney and John Zysman, Platform Power and Regulatory Politics: Polanyi for the Twenty-First Century, 27 New Political Economy, 820 (2022).

② 参见蒋慧:《数字经济时代平台治理的困境及其法治化出路》,《法商研究》2022 年第 6 期。

理方面的传统职能。[①]美国 2024 年 4 月以保护其国家安全为由通过的《保护美国人免受外国对手控制应用侵害法》(又称《Tiktok 强制出售法》)凸显了美国对超级平台国家安全自治的高度关注。

一、超级平台的法律地位与国家安全的平台自治

私人科技企业抓住发展主动权开启了平台时代,并以惊人的速度扩大规模,形成和积累了巨大的政治经济权力储备。[②]目前阿法贝塔、微软、梅塔、亚马逊、X 公司等跨国巨头统治着全球互联网超大型平台,长期在不同领域占据全球垄断地位。平台自治曾局限在私法关系中,但近年来日益向国家安全领域扩散,超级平台作为私主体的法律地位受到质疑。

(一)超级平台的法律地位

超级平台本质上是私人性质的商业实体,其对用户的自治权源自与用户之间的合同,但由于平台本身成为公共场所,其法律地位的定性直接影响到超级平台自治的责任与监管。美国法院的裁决显示超级平台因其私人身份而无须如政府一样承担保护个人言论自由的宪法责任。[③]1997 年美国法院宣布"监管广播媒体的特殊理由"不适用于"互联网的巨大民主论坛"。[④] 2017 年美国联邦最高法院指出,虽然社交媒体平台是信息、思想和沟通的公共场所,但是因其是私人商业的实体,故其拥有的言论自由同样受到政府保护。只有政府及与之相关的实体才有保护个人言论自由的义务,平台作为私人实体不能因剥夺某人的宪法言论自由权而承担责任。[⑤]同时,根据美国《通信规范法》的规定,包括网络平台在内的在线中介机构免于承担用户内容审核的责任,对平台自治的监管仅限于服务政府的重大利益,这使得平台自治权因其私人身份而很少受到监管限制。

在互联网诞生地的美国,因科技公司在平台时代拥有先天优势,平台私人中介实体的法律地位与美国的弱监管模式使平台能够通过商业行为顺利进入他国市场。欧盟、日本及英联邦国家等发达经济体因经济的开放性以及与美国的政治联盟而成为美国网络经济中的理想市场,在它们的帮助下,美国的一些网络平台迅速成为全球性超级平台。[⑥]这些国家与实体亦认可超级平台作为私人中介实体的法律地位。尽管欧盟近期通过数字立法为超级平台施加了一些公法上的义务,并通过人权保护与竞争法干预的路径加强政府监管,但是仍强调原则上应尊重平台作为中介

① See Laurie Clarke, Tech Ambassadors are Redefining Diplomacy for the Digital Era, https://techmonitor.ai/leadership/innovation/tech-ambassadors, 2023-06-29.

② See James Caporaso & Sidney Tarrow, Polanyi in Brussels: Supranational Institutions and the Transnational Embedding of Markets, 63 International Organization, 593 (2009).

③ See Orit Fischman-Afori, Global Digital Governance through the Back Door of Corporate Regulation, 33Fordham Intellectual Property, Media & Entertainment Law Journal, 720 (2023).

④ See Reno v. ACLU, 521 U.S. 844 (1997).

⑤ See Packingham v. North Carolina, 137 S. Ct. 1730 (2017).

⑥ See Dongsheng Zang, Revolt against the U.S. Hegemony: Judicial Divergence in Cyberspace, 39 Wisconsin International Law Journal, 1 (2022).

服务提供者的合同自由，其私人中介实体的法律地位并未发生变化。①

（二）国家安全的平台自治

超级平台私人中介实体的法律地位来自用户的平台治理权，超级平台利用技术先占进行自我赋权，②使“平台自治＋政府监管”成为超级平台治理的全球通用模式。当前，超级平台控制了全球信息流，几乎世界上每一个重大的地缘政治事件都与它们的行动有关。③

1.左右选举

宣传与话语权一直以来是政治参与的重要工具，现代通信技术和社交媒体平台的结合为政治讨论和政治活动创造了一种恰适的工具。2016 年的美国总统选举被视为超级平台对现实社会政治生态影响的标志性事件。2018 年曝光的脸书－剑桥分析公司的数据丑闻显示，超级社交平台所拥有的大量数据带来了操纵个人意见、影响选情的权力。④ 防止、识别和应对这种干扰的负担在很大程度上落在了平台身上。国家虽然可以因为超级平台没有阻止社交媒体上的错误信息或数据滥用而惩罚平台企业，但是无法阻止网络平台出现错误信息或滥用数据。通过国家安全自治，超级平台已形成了一种在很大程度上不受国家控制的大规模政治影响力，形成左右选举的效果。

2.塑造舆论

平台上的政治内容通常是由各种政治和媒体行为者（包括记者、活动家、政治战略家、民选官员和公民本人）创建的。超级平台对呈现给个人用户的内容进行编辑和排序以及对某些内容的推广和抑制，不仅影响单个内容，还影响平台上的整个内容流。⑤ 超级平台使用的算法使其只展示用户最可能感兴趣的内容、个性化用户可访问和消费的内容，并以有组织的方式向用户提供内容。平台技术、平台的可供性和算法以及平台治理塑造了平台用户的可见内容，使平台对用户拥有说服能力，且平台可能将这种能力出售给出价最高的人（包括广告商、政府或政党）。⑥ 谷歌搜索作为全球最热门的搜索网站之一，垄断了全球大部分的搜索平台，其搜索清单往往能决定用户看到的信息。维基百科则主导了全球大部分的网络百科平台，垄断了大量事件的全球叙事。⑦由于全球性超级平台大多系美国科技企业拥有，它们也成为美国向全球推行其价值观的有效工具。

3.防止恐怖及暴力活动

恐怖主义组织与暴力组织往往利用超级平台在全球冲突热点地区从事跨国恐怖主义和其他

---

① See Orit Fischman－Afori, Global Digital Governance Through the Back Door of Corporate Regulation, 33 Fordham Intellectual Property, Media & Entertainment Law Journal, 720 (2023).

② 参见马治国、占妮：《数字社会背景下超级平台私权力的法律规制》，《北京工业大学学报》（社会科学版）2023 年第 2 期。

③ See Kristen Eichensehr, Digital Switzerlands, 167 University of Pennsylvania Law Review, 665 (2019).

④ See Case Study on Cambridge Analytica Embezzling on Facebook Users Data, https://legaldesire.com/case－study－on－cambridge－analytica－embezzling－on－facebook－users－data/, 2025－04－22.

⑤ See 2023 Facebook Algorithm Guide: Overview & Best Practices, https://tinuiti.com/blog/paid－social/facebook－algorithm/, 2024－04－22.

⑥ See Natali Helberger, The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power, 8 Digital Journalism Volume, 842－854 (2020).

⑦ See Most Popular Websites Worldwide as of November 2024, https://www.statista.com/statistics/1201880/most－visited－websites－worldwide, 2025－04－22.

暴力活动,超级平台虽然已经采取一些审查措施,但是并未有效防止平台被暴力组织与恐怖主义组织利用。[①]面临一系列的政治、监管和公众压力,超级平台不得不应对因其产品和服务所带来的负面安全影响。[②]脸书、微软、推特和油管等平台企业在 2017 年成立了全球互联网反恐论坛,旨在应对影响平台的重大恐怖袭击,在指定的工作框架内与政府机构就反恐、选举诚信等问题定期举行会议。[③] 哈希行业数据库系其重要工具,该数据库允许成员为恐怖分子创建"数字指纹",并与其他参与的公司共享该数据。[④]与政府相比,超级平台针对在线威胁提供潜在技术解决方案,扮演一种不同于政府的角色,被寄望能够有效阻止恐怖袭击。

4. 解释和适用与安全相关的国际法

超级平台国家安全自治的作用还在于应对发生在世界各地的国际罪行、与国际罪行的认定及构成安全威胁情势的决定,并判断是否需要采取强制措施、判断强制执行后外国政府可能会做出的反击、应对政府的更迭所带来的安全问题等。例如,超级平台介入的缅甸罗兴亚少数民族问题、[⑤]以色列与哈马斯的冲突都涉及种族灭绝罪、反人类罪等国际罪行,[⑥]超级平台参与的美国在阿富汗撤军后的政府更迭问题则牵涉关于政府承认的国际规则。[⑦]

尽管超级平台已成为国家安全治理的重要参与者,但平台的自治权来自其与用户之间达成的合同,他们之间可能产生的冲突或争议的解决通常适用合同法规则而非公法规则。因超级平台私人中介实体的法律地位并未发生改变,故私权力进入传统的公权领域所带来的结构性问题也日益突出。

二、超级平台国家安全自治的能力建设与治理驱动力

超级平台自治从私法领域扩张至国家安全领域后,超级平台不得不强化国家安全治理能力的建设,并建立专门团队以适应治理需求。

(一)超级平台国家安全自治的能力建设

随着超级平台参与国家安全治理,它们必须加强自己的国家安全自治能力建设,而最便捷的

---

① See House of Commons Home Affairs Committee, Hate Crime: Abuse, Hate and Extremism Online, Fourteenth Report of Session 2016 - 17, HC 609(UK); Scott Shane, In 'Watershed Moment,' YouTube Blocks Extremist Cleric's Message, New York Times, 2017-11-12.

② See Steven Levy, Facebook: The Inside Story, Blue Rider Press, 2020, p.6 .

③ See Evelyn Douek, The Rise of Content Cartels, 20-04 Knight First Amendment Institute, https://knightcolumbia.org/content/the-rise-of-content-cartels, 2025-04-22.

④ See Google Public Policy, Update on the Global Internet Forum to Counter Terrorism, https://blog.google/around-the-globe/google-europe/update-global-internet-forum-counter-terrorism/, 2025-04-22.

⑤ See Hum. Rts. Council, Rep. of the Independent International Fact-Finding Mission on Myanmar, UN Doc. A/HRC/39/64, 2018.

⑥ See Elizabeth Culliford, Facebook Deploys Special Team as Israel-Gaza Conflict Spreads Across Social Media, REUTERS, 2021-05-19.

⑦ See Cristiano Lima, The Technology 202: Facebook, Twitter, YouTube Face High-Stakes Question of Whether to Recognize Taliban, Washington Post, 2021-08-17.

方法就是向政府学习。[①] 目前已有超级平台招聘美国政府前国家安全官员等专业人员组成专门团队，适用美国政府管理国家安全的政策与规则。2019年，脸书聘用美国前国务院法律顾问担任其总法律顾问，而其公共政策部门全球威胁破坏负责人的职位则由美国前国家安全委员会情报总监担任。[②] 谷歌则聘请美国前国务院官员贾里德·科恩。[③]这些官员将美国政府国家安全治理的方法和思维模式移植到超级平台中，并模仿美国政府创建了类似的情报分析、政策研究和外部联络机构。脸书目前约有40 000人致力于维护安全，而美国国务院外交服务人员的总数仅约为15 600人。[④] 同时超级平台还与政府的利益相关者建立了关系，弥补他们在线下世界中的盲点。美国超级平台和美国政府建立了以事件为中心特定合作和与专门机构常态合作两种模式，接受美国政府对平台国家安全自治的指导。

超级平台通常利用政府提供的信息设置自己的黑名单，通过为其用户设置标准和规则，创建、暂停和终止与用户的关系等方式，或利用技术手段改变用户行为等方式进行国家安全自治。尽管平台治理缺乏政府的强制力，但主要技术平台的选项列表及它们在现代社会中的作用仍然赋予它们足够的限制性权力，并有能力对个人和团体实施有实质影响的制裁。[⑤]

（二）超级平台国家安全自治的驱动力

在实践中，超级平台国家安全自治鲜有来自法律的正式授权，而更多的是与政府进行非正式合作，在政府缺位的情况下平台会替代政府进行治理，平台利益与政府利益冲突时平台会挑战政府权力，在少数情况下也会基于平台利益涉足国家安全事宜。

1.基于政府的授权

美国赋予平台企业在内容和用户管理方面几乎不受限制的自主权。平台对内容的审查权被美国法院视为私主体的宪法权利。[⑥] 但与美国任何私主体一样，平台的权利受到法律限制。例如，当美国政府根据《反恐怖主义和有效死刑法》指认伊朗革命卫队为外国恐怖组织时，脸书立即从照片墙（Instagram）上删除伊朗革命卫队关联账户发布的内容，尽管平台并不清楚其发布内容是否构成对恐怖主义的实质支持。[⑦]政府网络部门还可以通过获得法院命令指令平台删除内容、协助刑事调查、对用户实施制裁。由于这些超级平台的全球性，它们的执行行为会使美国制裁在

① See Elena Chachko, National Security by Platform, 25 Stanford Technology Law Review,55－140 (2021).

② See Jennifer Newstead to Join Facebook as General Counsel and John Pinette Becomes Vice President of Global Communications, https://about.fb.com/news/2019/04/newstead－and－pinette－join－facebook/, 2025－04－22.

③ See Google's Diplomatic Edge, https://www.techtransparencyproject.org/articles/googles－diplomatic－edge,2025－04－22.

④ See Meta: Our Progress Addressing Challenges and Innovating Responsibly, https://about.fb.com/news/2021/09/our－progress－addressing－challenges－and－innovating－responsibly/, 2025－04－22; Julie Nutter, The Foreign Service by the Numbers: Where We Stand, The Foreign Service Journal, https://afsa.org/foreign－service－numbers,2025－04－22.

⑤ See Elena Chachko, National Security by Platform, 25 Stanford Technology Law Review, 55－140 (2021).

⑥ See Zhang v. Baidu.com, Inc., 932 F. Supp. 2d 561 (S.D.N.Y. 2013).

⑦ See Golnaz Esfandiari, Instant Ban for Iran's IRGC On Instagram: Social－Media Giant Blocks, https://www.rferl.org/a/instant－ban－for－iran－s－irgc－on－instagram－social－media－giant－blocks－commanders－sites/29886908.html, 2025－04－22.

全球适用。[①] 在相当长的一段时间里,欧盟与美国一样对平台自治干预较少,明确了平台自治的禁止一般监管义务与中介责任豁免义务。《欧盟数字服务法》首次明确了超级平台打击包括仇恨言论或恐怖主义内容和非法歧视性信息等非法内容的法律义务,规定超大型平台有义务识别、分析、评估平台上存在的非法内容传播、损害欧盟基本利益等系统风险并采取有效的风险缓解措施(第 34 条和第 35 条)。这些数字法的实施往往依赖于平台自治,目前有不少超级平台修订了其平台自治规则以符合《欧盟数字服务法条例》的相关规定。

需要强调的是,平台自治以私主体的合同自由和言论自由为基础,在实践中超级平台通过正式的法律授权进行国家安全治理的情形较少。

2.与政府的非正式合作

在美国,超级平台自治很大程度上不受宪法和政府法定义务的约束,其内容审查行为几乎不受司法审查。[②] 政府将平台作为自己的长臂干预工具,如此政府可以规避法律程序和法律义务而推进某些行动,还可避免受到司法审查。向平台就迫在眉睫的威胁提出警告可能比通过政府渠道动员笨拙的跨部门流程来应对威胁效率更高、效果更好。非正式合作还可以规避来自政府内部的反对。“密苏里州诉拜登案”[③](以下简称“拜登案”)凸显出美国政府各部门是如何威胁、鼓励、说服、诱导超级平台进行国家安全自治活动的。欧盟也存在类似的互联网转介单位,[④]其职责也是非正式地联系平台,在没有立法授权的情况下要求超级平台删除国家认为危险或非法的内容。[⑤]

当政府机构将平台作为国家安全治理的变通办法时,政府与超级平台呈现出一种复杂的非正式“公共权力与私人权力共享”的动态关系。这意味着政府可借平台自治行使政府权力并不受法律限制、不承担法律责任。为此,越来越多的国家专门设置互联网转介单位,以一种更系统化的方式巩固了非正式监管的兴起。[⑥]

3. 填补政府职能空缺

超级平台国家安全自治的范围之所以相当广泛,部分原因在于政府缺位、政府不作为以及政治领导层与国家安全官僚机构之间的内部紧张关系。例如,在新冠疫情期间,各超级平台自行采取措施打击关于新冠感染的虚假信息;在美国国会骚乱发生后,一些超级平台自行批量关停鼓励暴力的用户账号;在美国退出阿富汗时政策模糊的情况下,超级平台也自行采取行动,拒绝承认塔利班政府。

4. 挑战政府权力

从前面三种模式可以看到,虽然在某些国家安全治理领域,超级平台与本国政府机构之间形成了互惠互利的共生关系,但是有时二者也会发生冲突。超级平台与特朗普政府之间就曾经出

① 参见杨永红:《次级制裁及其反制——由美国次级制裁的立法与实践展开》,《法商研究》2019 年第 3 期。

② See Danielle Keats Citron, Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age, 80 Southern California Law Review, 241 (2007).

③ See State of Missouri v. Biden, 23-30445 (5th Cir. Sep 08, 2023).

④ See EU Internet Referral Unit-EU IRU: Monitoring Terrorism Online, EUROPOL.

⑤ See Elena Chachko, Administrative National Security, 108 The Georgetown Law Journal,1063 (2020).

⑥ See Rabea Eghbariah & Amre Metwally, Informal Governance: Internet Referral Units and the Rise of State Interpretation of Terms of Service, 23 Yale Journal of Law and Technology, 542 (2021).

现对抗情势。2020年5月28日,时任美国总统特朗普在两次被推特标记其推文后,签署了“防止在线审查”的行政命令,试图削弱社交媒体对在线言论的审查权。[①] 2021年1月美国国会骚乱后,推特、脸书、谷歌等美国十几家社交媒体公司联合对特朗普进行“封杀”。可见国家秩序失控或政府处理不当或政府与网络平台之间的利益和政策出现不一致的时候,平台权力可能直接挑战政府公权。特别是在超级平台领导人奉行美国价值观时,由于价值观、文化、信仰等多方面差异,超级平台与外国政府更容易产生权力冲突。例如,由于印度政府对超级平台提出的国家安全治理的要求遭到超级平台的怠慢或拒绝,因此超级平台被印度批评为“双标”甚至“数字殖民主义”。[②]

5.服务于平台利益

超级平台实行私人企业董事长负责制,其权力集中在少数超级平台的领导人,这与互联网初期所规划的去中心化的自由世界形成了巨大反差。公权力的私有化无限放大个人权力,甚至代行了原来由国家机构执行的部分公共服务和公共政策,同时其商业实体追逐利润的本质与公共权力存在不可调和的矛盾。例如,马斯克最初对以色列与哈马斯在加沙冲突中的反应引发了大广告客户如苹果、迪士尼、IBM等撤离X平台,[③]这又迫使马斯克违反平台政策而允许以色列外交部关联账户发布宣传广告。[④]这凸显了平台作为商业私人实体以商业利益最大化为决策出发点与国家安全治理需要承担的社会公共责任之间不可调和的矛盾。而推特在2020年10月屏蔽《纽约邮报》关于拜登之子的负面信息,显示出超级平台国家安全自治被滥用于维护私人利益,[⑤]暴露了超级平台国家安全自治缺乏正当监管的重大风险。

超级平台的国家安全自治因发生在其日常自治活动中而具有高度的偶然性和动态性,自治范围的起伏不仅取决于平台的目标和优先事项,在很大程度上还取决于其利益与政府特别是母国政府的特定国家安全和外交政策优先利益的耦合度,这使得监管对于防止超级平台滥用权力甚至威胁他国国家安全意义重大。

三、超级平台国家安全自治的监管模式

基于超级平台私人实体的法律地位,对超级平台的自治监管应以政府公权力监管为主。但由于国家对超级平台技术私权力最初奉行一般不监管原则,导致政府在技术私权进入公权领域的时候缺乏有力的法律工具对其进行监管。由于缺乏国内法与国际法限制,公权私用导致的权

① See Preventing Online Censorship, Executive Order 13925 of May 28, 2020.

② See Lauren Frayer & Shannon Bond, India and Tech Companies Clash over Censorship, Privacy and Digital Colonialism, https://www.npr.org/2021/06/10/1004387255/india-and-tech-companies-clash-over-censorship-privacy-and-digital-colonialism, 2025-04-22.

③ See Chance Townsend, X Advertisers that Have Reportedly Pulled Ads Recently: See the List, Including Disney and Apple, https://mashable.com/article/advertisers-pulling-ads-on-twitter-x, 2023-11-18.

④ See Tarek Ali Ahmad, Musk's X Platform Allows Israeli State Media to Run ad Campaigns Despite Ban, https://www.arabnews.com/node/2392981/media, 2025-04-22.

⑤ See Jeremy Herb, et al., Twitter Execs Acknowledge Mistakes with Hunter Biden Laptop Story but Say No Government Involvement, https://edition.cnn.com/2023/02/08/politics/twitter-hearing-house-oversight/index.html, 2025-04-22.

力滥用问题亟须第三方监督。

(一)政府监管典型模式

数字主权和技术主权的行使并不禁止超级平台自治,[①]政府对超级平台国家安全自治的监管目的在于防止超级平台滥用自治权。

1. 美式弱监管范式

在美国,私营部门不受公共部门义务的约束。美国政府对超级平台的监管受到宪法和体制的结构性限制。[②]同时,由于担心对技术使用的限制会制约技术发展的速度,美国法院通常对平台的政府限制采取谨慎态度。[③]从 1997 年第一个涉及互联网与《美国联邦宪法第一修正案》之间关系的"里诺案"[④]到 2017 年"帕克汉姆案"[⑤],美国联邦最高法院一直支持超级平台享有广泛的平台自治权且不受其他适用于传统媒体作为具有宪法价值的私人机构的义务的约束。

政府对私人商业实体的监管通常是从消费者保护、反垄断与责任承担三方面进行的。在消费者保护和反垄断领域,美国联邦政府针对超级平台尚无正式立法的现实,相关的监管实践还是基于传统法规。例如,2024 年 3 月美国司法部依据《谢尔曼法》对苹果公司提起反垄断诉讼。[⑥]在责任监管领域,《通信规范法》使包括网络平台在内的在线中介机构免于承担用户内容审核的责任,这不仅有效地将网络平台与传统公司无法摆脱的风险敞口隔离开来,还将其与一系列法律风险和潜在责任隔离开来。[⑦]美国的弱监管模式导致美国联邦政府在超级平台国家安全自治上缺乏强有力的监管手段,因而不得不通过非正式路径干预超级平台国家安全自治。

近年来美国政府频频通过非正式方式干预超级平台在公共卫生安全、选举、舆论控制、外交政策、反恐等方面的自治。在"拜登案"中,美国白宫、卫生部、联邦调查局、国务院、网络安全与基础设施局等政府机构通过胁迫或重大激励或诱导或说服或鼓励等方式要求脸书、推特、油管和谷歌以"贴标签""降级"、删帖与关闭账户、"尚未达到删除阈值的页面更难在平台上找到"等方式参与平台国家安全自治,白宫甚至威胁将修改《通信规范法》确立的平台中立免责规则。而超级平台大多也顺从于政府的"胡萝卜加大棒"政策,与政府进行利益交换。该案初审法官认为平台在政府官员的指示下进行的内容审查违反《美国联邦宪法第一修正案》,牺牲私人和政府行为者的利益,为此发布了禁止政府胁迫、敦促、鼓励、施压或以任何方式诱导平台采取行动的命令。2023 年 9 月 8 日,该案上诉法院指出受国家监管并不能将私人行为归责于国家。只有国家强迫、重大鼓励等积极行为才能满足紧密联系测试要求,从而将私人行为归责于国家,为了区分"胁迫的企图"与"说服的企图",法院须考虑以下 4 个因素:(1)说话者的措辞和语气;(2) 该言论是否被视

① 参见杨永红:《美国域外数据管辖权研究》,《法商研究》2022 年第 2 期。

② See Orit Fischman-Afori, Global Digital Governance through the Back Door of Corporate Regulation, 33 Fordham Intellectual Property, Media & Entertainment Law Journal, 720 (2023).

③ See Packingham v. North Carolina, 137 S. Ct. 1730 (2017).

④ See Reno v. ACLU, 521 U.S. 844 (1997).

⑤ See Packingham v. North Carolina, 137 S. Ct. 1730 (2017).

⑥ See Justice Department Sues Apple for Monopolizing Smartphone Markets, Thursday, March 21, 2024, https://www.justice.gov/opa/pr/justice-department-sues-apple-monopolizing-smartphone-markets, 2025-04-22.

⑦ 参见张燕、张祥建:《平台权力的结构、扩张机制与异化效应》,《社会科学家》2022 年第 2 期。

为威胁;(3) 监管机构的存在;(4)谈话是否涉及不利后果。上诉法院认为“敦促、鼓励、施压”甚至“诱导”行动并不违反宪法,但若这种行为越界成为“胁迫”或“重大鼓励”则会导致违宪。[①]遗憾的是,最终美国联邦最高法院的裁决回避了政府隐蔽干预平台国家安全自治的合法性问题,以原告要求获得前瞻性救济的诉请与政府官员的行为之间缺乏具体联系为由裁定原告欠缺诉讼资格,推翻了上诉法院的裁决。[②]该裁决为平台用户追究政府非正式干预侵权责任设置了较高的证明责任,事实上关上了司法限制政府非正式干预的大门。

《Tiktok 强制出售法》试图通过禁令改变超级平台的非美国血统,表明美国已无法接受超级平台拥有非美籍母公司。该法对非美国国籍的超级平台的打压加强了美国超级平台的全球垄断地位,但正如美国联邦最高法院所指出的,该法对超级平台外国控制人的监管不等于对超级平台的自治进行监管,[③]故其并不影响美国对超级平台国家安全自治的弱监管。

美国的弱监管模式使得超级平台国家安全治理仍主要基于平台自治,政府主要利用其对超级平台的管辖权非正式干预超级平台的国家安全自治,并在美国法院的支持下规避美国法的限制。尽管在国家责任领域,根据《国家对国际不法行为的国际责任条款草案》第 5 条、第 8 条和第 11 条的规定,私人行为在或有国家的正式授权、或有国家控制私人行为、或有国家承认及接受的情况下可归因于国家,但是基于美国对超级平台治理的非正式监管的隐蔽性,超级平台的国家安全治理活动归因于美国政府存在现实障碍。超级平台的全球性使美国的非正式监管在缺乏法律与领土限制的情况下实现美国的长臂管辖,超级平台的私人身份导致国际法难以发挥维护其他国家的主权与国家安全的作用,从而进一步放大了美国的数字霸权。

2. 欧式强监管范式

2000 年《欧盟电子商务指令》第 15 条明确规定各成员国不可以保护用户的基本权利为目的要求平台承担一般的监管义务。在《欧盟一般数据保护条例》实施前,欧盟主要依据竞争法对超级平台自治进行监管。然而,作为欧盟最成熟的二级立法,欧盟反竞争法在削弱美国超级平台垄断地位上效果不明显。为终结“大而不倒”的平台时代,2024 年生效的《欧盟数字市场法》和《欧盟数字服务法》确立了超级平台“守门人”的法定义务。这对超级平台的优势可能产生一定的影响,但反竞争领域的监管主要是针对平台自治的运营方式,对其在国家安全治理方面的影响仍是间接的。

欧盟数字法亦重视用户人权保护。《欧盟一般数据保护条例》为保护用户的被遗忘权、可携带权、隐私权等权利,为平台设置了强制同意的法定义务。《欧盟数字服务法》突破性地为平台设置了内容审查义务,规定了平台对非法内容的删除义务,以及超级平台对通过传播、扩散非法内容或进行非法活动等方式滥用平台服务功能所带来的系统性风险与蓄意、通谋操纵平台服务对公民言论、选举程序、公共安全和未成年人保护产生可预见性影响的系统性风险进行评估与管控的义务。如果超级平台未能履行这些义务,欧盟委员会可通过违法调查程序对平台进行处理。[④]这标志着欧盟开始对超级平台国家安全自治进行监管。值得强调的是,《欧盟数字服务法》仍然

① See Murthy v. Missouri, 603 U.S. (2024).

② See Murthy v. Missouri, 603 U.S. (2024).

③ See TikTok Inc. and Bytedance Ltd., and Others v. Merrick B. Garland, 604 U.S. (2025).

④ 参见王燕:《社交平台私权力的公私二元规制》,《法商研究》2024 年第 1 期。

受到《欧盟运行条约》的限制,欧盟法院对欧盟委员会根据《欧盟数字服务法》作出的所有的罚款和惩罚性付款决定均有无限的审查权。尽管《欧盟数字服务法》明确了欧盟委员会相对严格的监管权,但它没有废除《欧盟电子商务指令》中的基本条款,而是延续了欧盟确立的禁止一般监管义务与中介机构责任豁免的一般原则,并受到欧盟法关于言论自由及其他传统法律原则的限制。

2023 年 12 月 8 日,欧盟委员会正式对 X 平台启动违反《欧盟数字服务法》程序第一案。[①] 2024 年 7 月 11 日,欧盟委员会向 X 平台通报了其初步意见,认为该公司在与暗黑模式、广告透明度和研究人员数据访问相关的领域违反《欧盟数字服务法》。该案的发展进程体现了欧盟对超级平台国家安全治理的强监管模式。该模式对超级平台舆论领域的国家安全治理形成了较为明显的事后监管,当欧盟机构实施干预时争议信息已然传播并形成舆论导向,其监管难以改变已形成的舆论。同时欧盟对超级平台国家安全自治的监管仍然受到欧盟条约及禁止一般监管、中介责任豁免等规则的限制,其复杂的法律制度极有利于财力雄厚的超级平台,加之欧盟机构官僚作风突出,时间将成为欧盟监管最大的敌人。这在“欧盟委员会对谷歌反竞争案”[②]中表现得相当突出,该案从 2010 年欧盟发起对谷歌的反竞争调查到 2024 年 9 月 10 日欧洲法院审理终结,耗时长达 14 年。

欧盟及其成员国对平台自治的监管被限制在明确的法律规定范围内,一旦超出这个范围就只能非正式干预平台自治。欧盟的互联网转介单位通过与平台的沟通为欧盟主管当局提供战略和业务支持,主要在打击恐怖主义和暴力极端主义领域与平台合作,促进平台迅速有效地删除有关恐怖主义和暴力极端主义及仇恨言论等内容。欧盟互联网转介单位主要通过说服、鼓励、建议等方式利用超级平台自治实现其国家安全目标。2016 年欧盟通过超级平台同意的方式,以“行为准则”明确平台的关于仇恨言论的内容审查义务以解决非正式监管的透明度问题。脸书、微软、推特和油管等超级平台与欧盟共同签署了一项打击网上非法仇恨言论的行为准则。自 2018 年以来,多个超级平台加入该行为准则,在迅速审查和删除仇恨言论内容方面效果明显。[③] 该行为准则以尊重平台自治为基础,未引入政府问责制度,灵活地把政府机构对超级平台的说服结果契约化与透明化,似乎开辟了一条将非正式监管予以正式化与合法化的路径。

(二)第三方监督

超级平台商业实体的运行模式将其治权集中在少数人手中的同时,也意识到自治权力的合法性与权力监督问题。第三方监督的出现试图解决超级平台自治的法律监督问题及权力集中所带来的合法性问题。

1.第三方私人监管的有限性

由于人们担心科技平台权力的集中,脸书尝试将监督权还给人民。[④]脸书 2009－2012 年开始“新的治理模式”和“大规模民主进程”试验,将平台政策的变化交由用户投票决定。但由于参

① See Commission Sends Preliminary Findings to X for Breach of the Digital Services Act, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3761,2025－04－22.

② See C－48/22 P － Google and Alphabet v. Commission (Google Shopping).

③ See JHA Council 7 October 2021,Progress on Combating Hate Speech Online through the EU Code of Gonduct 2016－2019.

④ See Mark Zuckerberg, Standing for Voice and Free Expression Speech, Georgetown University, The Washington Post, 17 Oct. 2019 .

与投票用户占比仅为0.3%，试验随后被放弃。[①] 2018年扎克伯格宣布建立由专家组成的独立审查委员会。[②]审查委员会可以推翻平台的决定，其决定对脸书与照片墙拥有约束力。[③]审查委员会在一定程度上独立于超级平台，但梅塔公司深度参与审查委员会的建立，是其资金来源，且其审查标准是脸书和照片墙的社区规则及其价值观，这些都导致审查委员会作为第三方的独立性遭到质疑。从2021年起，审查委员会仅决定少数具有挑战性的案件。[④] 最著名的案例莫过于其支持脸书对特朗普的禁令，只要求脸书明确禁令的期限。[⑤] 事实上审查委员会的审查仍然代表着超级平台在数字空间的自我监管，属于非政府私人实体的横向治理模式，[⑥]且其监督仅针对脸书与照片墙，并无普遍意义。

欧盟亦对超级平台自治设立了第三方争端解决机构。根据《欧盟数字服务法》第21条的规定，用户有权选择庭外争议解决机构作为解决内容审核争议的替代方式。此类争端解决机构还可监督“无法通过内部投诉处理系统解决的投诉”。与梅塔公司参与的审查委员会不同，它必须由其成立地成员国的数字服务协调员认证，而且缺乏“将具有约束力的解决方案强加给各方的权力”，故此类机构可能会转而专注于促进平台与用户之间的谈判，以达成争端的解决。[⑦]尽管该机构独立于超级平台，但其决定因缺乏法律拘束力而难以对超级平台的自治权力构成有效限制。

2.国际监督的缺位

当下，国际安全与国家安全的界限日益模糊。协助国家选举自1991年起即成为联合国大会的工作内容之一。恐怖主义、国内武装冲突及一国发生的人道主义灾难等都成为联合国安理会所关注的国际安全问题。[⑧]超级平台的全球性与其治理的国家安全事项使超级平台权力的监督问题成为国际问题。但超级平台的自治活动系私主体行为，仅在有国家的正式授权、或受到国家控制、或被国家承认及接受的情况下才可能归责于国家并由国家对其活动承担国际责任。《联合国工商业与人权指导原则》(以下简称《指导原则》)虽然可适用于超级平台自治，但是其对国家义务与企业责任的内容进行了实质性区别，规定企业应自愿“避免侵犯他人的人权，并应解决其所

① See Anika Gauja, Digital Democracy: Big Technology and the Regulation of Politics, 44 University of New South Wales Law Journal, 959 (2021).

② See Mark Zuckerberg, A Blueprint for Content Governance and Enforcement, https://m.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/, 2025-04-22.

③ See Shannon Bond, Trump Suspended from Facebook for 2 Years, https://www.npr.org/2021/06/04/1003284948/trump-suspended-from-facebook-for-2-years, 2025-04-22.

④ See Jan Mazur & Barbora Gramblickova, New Regulatory Force of Cyberspace: The Case of Meta's Oversight Board, 17 Masaryk University Journal of Law and Technology, 3 (2023).

⑤ See Shannon Bond, Trump Suspended from Facebook for 2 Years, https://www.npr.org/2021/06/04/1003284948/trump-suspended-from-facebook-for-2-years,2025-04-22.

⑥ See Michael Cusumano, Annabelle Gawer and David Yoffie,Can Self-Regulation Save Digital Platforms? 30 Industrial and Corporate Change, 1259-1285 (2021).

⑦ See Digital Services Act, Article 21;David Wong & Luciano Floridi, Meta's Oversight Board: A Review and Critical Assessment, 33 Minds & Machines, 261-284 (2023).

⑧ See Yang Yonghong, Sovereignty in China's Perspective, Frankfurt am Main, Germany, 2017, pp.28-31.

涉及的不利人权影响”。[①] 2018 年联合国特别报告员大卫·凯伊曾建议将国际人权法纳入超级平台的内容管理规则,并称因超级平台在全球公共生活中发挥着极其重要的作用,故亟须采纳和执行《指导原则》。[②]但是这往往取决于超级平台的意愿且属于其自治的内容,无法解决超级平台在国际法上主体适格性的问题。即使超级平台将国际人权法纳入其社区规则,超级平台是否遵循国际人权法进行治理以及如何治理仍缺乏国际机制的监督。

一些国家认识到超级平台已经拥有对其他主体的支配性力量且正在获得国家安全领域的主体性权力地位,开始向硅谷派出外交官,期望能够通过外交途径影响超级平台国家安全自治。2017 年,丹麦向美国硅谷派出全球首位科技大使,负责与谷歌、脸书、微软、苹果等超级平台在包括网络安全和虚假信息、打击网上恐怖主义等重要问题上的合作。[③]法国、爱沙尼亚、荷兰、保加利亚、奥地利、英国、美国等纷纷任命技术大使。[④] 2022 年 6 月,联合国任命阿曼迪普·吉尔为其技术特使,[⑤]欧盟任命驻美数字事务高级特使。[⑥]集中全球超级平台的硅谷已约有 20 位科技大使与特使,硅谷所在的旧金山有超过 70 个领事馆。[⑦]硅谷已成为科技外交的中心。科技外交似乎类似于政府通过非正式渠道干预超级平台自治,但由于其干预来自超级平台非母国政府与国际组织,因此更像国际非正式监管。由于这些国家与国际组织缺乏美国与超级平台之间的权力结构关系,因此此类国际非正式监管作用极为有限。

无论是美国的弱监管还是欧盟的强监管模式,二者都以中介机构责任豁免与禁止一般监管义务原则为基础,这使得超级平台国家安全自治仍以平台自治为主导。[⑧]由于涉国家安全事项的时效性极强,数字新兴立法作为欧盟二级立法仍然受制于欧盟法律体系,加之超级平台强大的技术优势与雄厚的财力,欧盟强监管模式仍将面临有效性问题。而美国通过非正式干预对超级平台国家安全自治产生重大影响,导致美国数字霸权在国家安全领域的扩张。美国的非正式监管极易被滥用于维护美国的国家利益或私人利益,亟须独立第三方的监督。但第三方私人监督相

---

① U.N. Special Representative of the Secretary－General, Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework, Principles 11, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011).

② See David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HCR/38/35 (Apr. 6, 2018).

③ See Office of Denmark's Tech Ambassador, The TechPlomacy Approach, https://techamb.um.dk/the－techplomacy－approach, 2025－04－22.

④ See U.S. Department of State, Nathaniel C. Fick－－ Ambassador at Large Bureau of Cyberspace and Digital Policy, https://www.state.gov/biographies/nathaniel－c－fick/, 2025－04－22.

⑤ See Amandeep Singh Gill, Secretary－General's Envoy on Technology Office of the Secretary－General's Envoy on Technology, https://www.un.org/sg/en/content/profiles/amandeep－gill, 2025－04－22.

⑥ See Gerard de Graaf, Senior Envoy for Digital to the U.S. and Head of the EU Office in San Francisco, https://www.eeas.europa.eu/sites/default/files/documents/Bio_Gerard%20de%20Graaf%20New%20SF%2008.2022_0.pdf, 2025－04－22.

⑦ See What is Tech Diplomacy and Why Does it Matter? World Economic Forum, https://www.weforum.org/agenda/2023/02/what－is－tech－diplomacy－experts－explain/, 2024－04－22.

⑧ See Pat McGrath, Facebook Probed by Australian Electoral Commission over Mysterious Political Ads, ABC News, 2019－02－26.

对弱势且缺乏国际监督机制，导致对超级平台国家安全自治的监管及监督效果并不明显。

四、应对超级平台国家安全自治的中国路径

尽管中国平台企业价值规模已位居世界第二位，但中国几乎没有全球性超级平台，如在中国搜索市场占据首位的百度2024年的全球份额仅占1.15%。[①] 我国应积极将本国在线平台发展成为全球性超级平台，建设有中国特色的超级平台国家安全自治监管机制，并参与构建全球性超级平台的国际监督机制，防止超级平台的国家安全自治被滥用于国家与个人私利。

（一）建设有中国特色的超级平台国家安全自治监管模式

如果一个国家没有超级平台，就可能因没有超级平台治理话语权而落入美国数字霸权的封锁。因此，作为新兴的网络大国，中国应积极推动中国大型平台的海外发展以平衡美国的数字霸权。在这一过程中，一方面，要吸取美国和欧盟发展和监管超级平台的经验与教训。例如，政府的弱监管模式更有利于平台的全球发展，而主导超级平台国家安全自治的能力建设和通过非正式手段监管超级平台国家安全自治将有效地影响平台的国家安全治理。另一方面，要结合我国的国情，建设具有中国特色的超级平台国家安全自治监管模式。(1)我国在支持互联网企业海外发展时可采取弱监管模式以利于我国平台的全球发展，打消运行地政府对我国借平台权力影响该国国家安全的顾虑，将我国监管模式限制于我国领土，避免挑战运行地政府公权力，消除西方国家对我国科技企业的“技术威权主义”[②]抹黑。(2)我国可通过指导超级平台国家安全自治的能力建设，将中国国家安全治理理念与对外关系准则贯穿于平台自治，贯彻尊重他国主权、不干涉他国内政、反对数字霸权的根本立场，使平台在海外国家安全自治中不仅能够维护中国的国家安全，而且还维护中国一贯尊重他国主权、不干涉他国内政、不称霸的国际声誉。(3)建立政府与超级平台定期与不定期的交流机制，通过非正式方式使超级平台在国家安全自治中随着国家安全情势的变化有能力发现并解决涉及国家安全的问题。(4)鼓励超级平台自觉将国际人权条约纳入其平台治理规则，不断提高平台声誉。(5)在我国特有的人民调解制度的基础上打造对超级平台自治进行监督的第三方机制，降低超级平台滥用国家安全自治权的风险，由此解决全球性超级平台国家安全自治的合法性问题。

（二）构建联合国框架下多利益攸关方国际监督机制

由于超级平台的私人商业实体的法律地位，相关国际监督机制的构建面临主体适格的法理障碍，可以借鉴互联网名称与数字地址分配机构多利益攸关方政府与私主体合治的模式解决该法理障碍。该模式旨在扩大来自全球各地的不同群体的参与，包括私营部门、民间社会、学术领袖、互联网专家和企业及政府。在目前互联网名称与数字地址分配机构多利益攸关方管理模式中，尽管政府是其中重要的利益攸关方，但是互联网的产生与发展历史导致该社群内围绕技术精英建立的互联网技术和标准组织早已成为国际互联网治理的主体，且逐渐演绎出去政府中心的自下而上的工作方式和互联网文化，政府在该社群中作用有限。由于历史的原因，美国仍然能够

① See Search Engine Market Share Worldwide, https://gs.statcounter.com/search-engine-market-share, 2025-04-22.

② 参见李艳：《美国强化网络空间主导权的新动向》，《现代国际关系》2020年第9期。

在互联网名称与数字地址分配机构多方利益攸关方模式下保持主导地位,这也是美国坚持互联网名称与数字地址分配机构多利益攸关方模式而反对构建联合国框架下多利益攸关方模式的核心原因。互联网名称与数字地址分配机构多利益攸关方模式的出现有其历史的偶然性,但目前创立一个新兴的超级平台国家安全治理国际监督机制的偶然性因素并不存在,因此中国可倡导发展中国家发起建立一个联合国框架下多利益攸关方模式对全球性超级平台进行监督。中国一贯坚定支持以联合国为核心的国际法体系,建立一个联合国框架下的多利益攸关方国际监督机制弥补超级平台国家安全治理监管机制的不足。这既符合发展中国家的利益,也符合在网络空间构建人类命运共同体的目标。

2005 年联合国大会(以下简称"联大")突尼斯会议通过的《信息社会突尼斯议程》对互联网多利益攸关方治理模式进行了具体阐释,并要求联大组织召开新的多利益攸关方政策对话论坛。联大因此在 2006 年组织联合国互联网治理论坛,成立了由来自所有 5 个联合国区域集团的政府、私营部门、民间社会、学术和技术群体的 50～55 名成员组成的多利益相关方咨询专家组,讨论与互联网相关的公共政策问题。中国可推动发展中国家以该论坛为基础,提出一个对全球性超级平台国家安全治理进行国际监督的方案,由该论坛的多利益攸关方咨询专家组进行讨论并提出修改建议,构建由政府、超级平台、技术专家、法律专家、国际组织、非政府组织及平台用户群体代表等多方参与的国际监督机制。同时,可通过联合国与超级平台签署契约的模式,使联大管理下的独立多利益攸关方监督机制成为现实,以有效防止超级平台国家安全自治被滥用于谋求国家与个人私利,遏制美国数字霸权。

五、结 论

超级平台在日常运营中获得的跨越主题与地域限制的支配性权力,成为干预政治运行和社会治理的"技术利维坦"。它们拥有大量的资源并凭此获取影响选举、反恐、舆论及涉安全的国际法适用等国家安全领域的治理权。美欧法律对私营中介实体进行保护的传统精神使责任豁免原则与禁止一般性监管原则主导了超级平台国家安全自治及监管,这导致超级平台国家安全自治的法律约束相当有限。尽管欧盟近期通过数据立法对超级平台赋予内容审查与风险评估等法定义务,但由于并未改变一般性规则,加之欧盟一直以来的官僚作风和国家安全具有较强的时效性,监管的实际效果不尽如人意。美国的非正式监管则一定程度上推动了美国数字霸权的形成。一方面,前美国官员负责的超级平台国家安全自治,将美国政府的工作方式推向全球。另一方面,超级平台受到美国法的管辖,使得美国拥有控制超级平台权力的全球性地位。目前美国非正式监管的偶然性、隐蔽性及其与美国政府权力的密切关联使美国能够利用非正式监管对全球性超级平台的国家安全自治产生实质影响,逃避国内法与国际法的限制。超级平台的全球性与商业性,可能导致其将自身利益与美国利益及美国价值观凌驾于其他国家利益和公共利益之上。被西方学者寄以厚望的第三方私人监督机制仅对少数超级平台有部分作用,且不具有一般性。而欧盟的庭外争端解决机构也因缺乏法律强制力而影响有限。超级平台的私人商业主体身份使其成为美国政府长臂干涉他国内政、侵犯他国权益的行为难以通过国际法追究其国际责任。同时联合国人权理事会的《指导原则》的软法性质及其对国家安全领域的低影响力,无法形成对超级平台国家安全自治的有效监督。近年来兴起的科技外交虽然可对超级平台国家安全自治形成

非正式的国际影响，但由于缺乏权力结构关系而难以对超级平台国家安全自治形成国际监督。为了保护发展中国家的国家安全利益，结合目前超级平台国家安全自治实际情况，一方面，应积极推动我国在线平台的全球发展，并建设具有中国特色的超级国家安全自治监管模式，平衡美国数字霸权；另一方面，联合发展中国家推动国际社会在联合国互联网治理论坛构建多利益攸关方的国际监管机制，提升广大发展中国家超级平台国家安全自治能力建设，为构建网络空间命运共同体提供治理经验与发展基础。

Abstract: With the permeation of superplatforms into all aspects of human society, platform autonomy has expanded to traditional national security fields. Global superplatforms have already become important players in national security governance. Due to its legal status as a private intermediary entity, prohibiting general supervision and exemption from responsibility for intermediaries limit government regulation of platform national security governance. The EU has significantly strengthened its regulatory powers in recent years, however, the timeliness of national security issues and the EU's bureaucratic system will continue to affect the effectiveness of its oversight of superplatforms. USA government mainly intervenes in the national security governance of superplatforms through construction of autonomy capabilities of superplatforms and informal monitoring. While third party private dispute settlement institutions have not yet constituted effective restrictions on superplatforms, and technology diplomacy has little impact on national security governance of superplatforms, U.S. superplatform's self－governance on national security expands the U.S. digital hegemony. Consequently, China should actively support Chinese platforms to develop globally, and build monitoring model regarding superplatform self－governance on national security in Chinese way, so as to ballance the U.S. digital hegemony. Meanwhile, China should promote the construction of a multi－stakeholder regulatory model under the United Nations and provide foundation for building a community with a shared future in cyberspace.

Key Words: superplatform, national security, platform governance, privatization of public powers

责任编辑　　何　艳