美国顶尖智库在网络安全领域的研究态势分析

王 燕，高 芳
（中国科学技术信息研究所，北京 100038）

摘 要：分析美国顶尖智库在网络安全领域的研究态势，有利于掌握美国顶尖智库在该领域的研究现状和对美国网络安全战略的预判，为中国网络安全发展及智库建设提供借鉴。从时间和主题两方面分析了美国顶尖智库在网络安全领域的研究态势，采用隐含狄利克雷分布（Latent Dirichlet Allocation，LDA）主题模型对 2018—2022 年美国顶尖智库的研究成果进行主题挖掘，并结合政策事件对部分主题进行解读。结果表明，美国顶尖智库对网络安全的关注不断增强，研究成果主要集中在中美科技竞争、技术风险与治理以及网络安全人才培养等方面，在完善美国网络安全顶层设计、吸引人才等方面起到了重要的支撑作用，推动美国网络安全的发展。

关键词：美国；智库研究；网络安全；LDA 主题模型；政策研究
中图分类号：C932 **文献标识码**：A DOI：10.3772/j.issn.1009-8623.2023.08.002

1 研究背景

在信息时代，网络空间成为继海、陆、空、天之后的第五维空间。近年来，网络攻击和网络犯罪事件愈发频繁，网络安全已经成为影响国家安全的重要因素之一。狭义上，网络安全是指保护个人、组织或国家及其计算机系统、设备和数据免受网络攻击和未经授权的访问而采取的措施，广义上，其属于确保信息的机密性、完整性和可用性的相关理论、技术和方法等范畴[1]。20 世纪 70 年代以来，美国政府持续强调网络安全保护，颁布了一系列政策，将其作为国家安全的重中之重[2]。作为政策过程的重要参与者和政策制定的推动者，美国顶尖智库对美国公共政策的成熟和完善提供了重要参考[3-4]。其十分重视网络安全领域研究，通过发布研究报告和参与研讨会等方式直接或间接地将智库研究成果和建议等嵌入美国网络安全战略决策中[5]，智库文本作为智库研究成果的展现形式，充分体现了智库的战略思想与其对政策的预判[6]，因此，基于智库文本对美国顶尖智库在网络安全领域的研究态势进行分析，不仅有利于洞察美国顶尖智库在该领域的研究现状和对美国网络安全政策的影响，也能够发挥情报研究的前瞻性和先导性作用，对美国未来网络安全的布局和发展趋势进行研判，从而为中国在网络空间领域的政策制定和国际交流提供参考。

已有研究从不同角度对美国顶尖智库在网络安全领域的态势展开了分析，包括研究议题领域、美国对华网络安全议题的建构与认知以及在政策制定中的作用等。刘昊等[6]采用共词分析和社会网络分析方法对 2008—2016 年美国顶尖智库在网络安全的文本成果进行可视化分析，发现美国顶尖智库在网络安全领域的研究议题主要围绕安全防务与反恐、国际战略、关键基础设施和网络空间治理以及公共安全和法律等 4 个方面；韩娜等[5]选取了 2014 年以来美国顶尖智库的相关报告，采用文献分析法探究了其对涉华网络安全议题的建构，结果表明，大部分美国顶尖智库都将中国的网络安全发展视为主要威胁；霍淑红[7]探究美国顶尖智库对中

第一作者简介：王燕（2000—），女，在读硕士研究生，主要研究方向为科技战略与政策，重点领域情报分析。
通信作者简介：高芳（1980—），女，博士，研究员，主要研究方向为科技战略与政策、重点领域情报分析。
收稿日期：2023-05-23

美网络安全的认知变化，指出大部分智库在强调中美竞争必然性的同时，也表达了对中美关系恶化的担忧；鲁传颖[8]则指出美国顶尖智库通过构建平台、议程设置以及人才交流等方式，将其战略思想融入美国的网络安全决策中，并在中美两国网络外交中产生了重要的影响。随着技术的发展，自然语言处理在文本分析中起到重要的作用，共词分析、隐含狄利克雷分布（Latent Dirichlet Allocation，LDA）主题挖掘等也多被用于智库文本的研究[9-10]，以展现智库的研究现状，但了解智库在政策制定过程中的参与度和作用，还需要结合政策事件对结果进行统筹分析和阐释[11]，以展现智库情报的先决性和预见性。与此同时，在中美科技竞争环境下，美国顶尖智库对中美网络安全建设的看法和研究重点也需要深入探讨。

本研究选择了美国的布鲁金斯学会（Brookings Institution）、战略与国际问题研究中心（Center for Strategic and International Studies，CSIS）、兰德公司（Rand Corporation）、卡内基国际和平基金会（Carnegie Endowment for International Peace）及美国外交关系协会（Council on Foreign Relations，CFR）5家智库作为分析样本，探究美国顶尖智库在网络安全领域的研究态势。根据宾夕法尼亚大学发布的《全球智库报告2020》（2020 Global Go To Think Tank Report）[12]，以上5家智库在国家安全智库榜单中位列美国前10，可以被称为顶尖智库；同时，这5家智库均设有网络安全相关专题，在网络安全领域进行了深入研究[5-7]。

基于以上5家智库近5年在网络安全领域的研究成果，本研究从时间和主题两个维度探究美国顶尖智库在网络安全领域的研究态势，采用自然语言处理方法对智库文本进行高频词共现分析和主题挖掘，并结合政策事件和智库文本针对相关主题进行解读，深度呈现美国顶尖智库在网络安全领域的研究态势和政策预判，探究中美竞争背景下美国顶尖智库如何推动和支撑美国在网络安全领域的持续发展，也为中国网络安全领域相关政策制定和智库建设提供借鉴。

2 1993—2022年美国政府网络安全战略文件及其核心观点

从20世纪90年代的克林顿时期，美国政府就认识到信息系统和网络基础设施安全对国家安全的重要性，此后，美国根据面临的网络安全挑战和国际形势不断调整和完善网络安全政策，经历了从全面防御到攻防结合、主动攻击再到美国优先的战略转变，形成了递进式和体系化的网络安全体系，并逐步占据网络空间主导地位[2]。

克林顿时期（1993年1月—2001年1月），美国网络安全政策以基础设施保护为重点，整体实施的是“适度安全型”战略，在加强保护的同时促进信息技术的发展，并于2000年4月发布了《保护美国的网络空间：国家信息系统保护计划1.0版》，首次将网络安全纳入国家安全战略框架。布什时期（2001年1月—2009年1月），“9·11”事件使得美国在继续保护关键基础设施的同时将重点转向网络反恐，通过发布一系列法律法规保障网络安全，在2003年出台了《确保网络空间安全国家战略》，首次将网络安全上升为国家战略，同时组建了总统关键基础设施保护委员会和国土安全部[6]。奥巴马时期（2009年1月—2017年1月），美国网络安全战略转向“主动攻击”和“网络威慑”，更具“攻击性”和“国际性”。2011年发布的《网络空间国际战略》则从经济、网络安全、执法、军事、互联网管理、国际发展及隐私保护7个方面阐述了美国日后推进的政策重点，强化国际合作，加深网络渗透，以实现美国在网络空间的主导地位。

特朗普时期（2017年1月—2021年1月），美国网络安全政策注重“美国优先”和“实用主义”，并将网络空间的大国博弈看作美国面临的主要挑战。2017—2019年，特朗普陆续签发4个总统行政令，以加强对关键基础设施的保护和增强美国网络安全人才建设。2017年12月发布的《国家安全战略》报告中“网络（cyber）”一词出现了46次，远高于以往同类文件，这意味着网络安全已经上升为国家安全的核心利益；2018年9月发布《美国国家网络战略》，从保护美国国土安全、美国人民和美国的生活方式、促进美国繁荣和以实力求和平及提升美国影响力4个方面明确了美国网络安全的4项支柱、10项目标与42项优先行动，这一系列文件从宏观上为美国在网络空间的持续发展指明了方向。这一时期，美国网络安全建设的重点除延续以往的保护关键基础设施外，还强调了数字经济和网络军事能力建设[13]，推进网络科技创新和人才

培养[14]。在国际上，美国将中国与俄罗斯视为其在网络空间中最重要的战略对手，并展开相关行动在数字空间遏制两国；同时建立以美国为中心的国际网络联盟机制，形成集体威慑[13]。2018年，特朗普宣布对华商品提高关税，掀起了中美贸易争端；为了限制中国高新科技发展，美国出台“实体名单”，对包括华为在内的70家公司进行出口制裁，中美两国的贸易竞争演化升级为科技竞争，而网络安全领域也成为中美科技竞争的重点。

拜登时期（2021年1月至今），美国网络安全政策重点在于防御体系的强化。“太阳风”（Solarwinds）、微软Exchange服务器等网络攻击事件接连发生，使得网络安全成为拜登上台后面临的首要任务。2021年3月公布的《临时国家安全战略指南》明确表示将网络安全作为第一要务；同年4月设立了国家网络总监办公室并任命前国家安全局副局长为第一任国家网络总监，主要负责网络安全政策和战略以及与行业和国际利益相关者的网络安全接触。随后在5月又发布了《改善国家网络安全行政令》，指出“保护网络安全是国家和经济安全的首要任务和必要条件”，旨在通过保护联邦网络、改善政府与私营部门之间的信息共享及增强美国的事件响应能力等提高国家网络安全防御能力。拜登政府还推进基于分层网络威慑的网络外交，一方面积极修复与盟友关系，另一方面将中国与俄国是视为主要威慑对象，推进“接触+遏制”的网络外交政策。2022年10月，美国白宫发布了《国家安全战略》，将加强国际合作、提升技术威慑能力及加快国际规则制定作为网络安全领域的施政重点，积极推动“网络外交”，表明了美国对国际合作和国际机制的重视；2023年3月2日，拜登签署《国家网络安全战略》，围绕建立“可防御、有韧性的数字生态系统”，提出了5大支柱共27项举措，更加突出和强调政府与行业的地位和作用。在这一阶段，拜登政府延续了特朗普的大国竞争策略，把中国视为美国“最严峻的竞争对手”。

3　研究设计

3.1　样本选择与数据采集

本研究主要从时间和主题两个维度分析美国顶尖智库在网络安全领域的研究态势，剖析美国顶尖智库在该领域的研究趋势和研究重点。

在数据获取时，以“cyber security”和“network security”等为关键词在智库官网进行检索，选择2018年1月1日—2022年12月31日的研究数据，以研究报告、论文等研究型成果为主[6]，采用八爪鱼工具对网页数据进行爬取，人工下载相关文件，共获取原始数据241条。

3.2　数据预处理与分析过程

首先，基于Python的自然语言工具包（NLTK）对文本进行预处理。NLTK是Python中进行自然语言处理的平台，可提供分析、词性标注、词干提取和词形还原等多种功能。其次，使用正则表达式过滤文本中的无效词汇；构建同义词典，统一同义词；基于NTLK中的停用词词典（stopword）和自定义的停用词词典，对文本进行分词、去停用词和词形还原及大小写归一等。

完成数据预处理后，采用TF-IDF算法提取文本的高频词，并选择排名前20位的高频词汇构建高频词共现矩阵，使用Gephi进行可视化[10]，以分析美国顶尖智库在网络安全领域的研究热点。LDA模型是一种经典的主题概率生成模型，相比基于相似度和词频的文本聚类方法，LDA模型更适用于规模较大的、多主题的文档数据集潜在主题识别[15]。因此，本研究使用LDA模型对美国顶尖智库在网络安全领域的研究文本进行主题挖掘，使用困惑度和手肘法确定最佳主题数。

完成主题聚类后，选取主题强度排名前3位的主题对美国顶尖智库在网络安全领域的研究态势进行分析。主题强度是指某时间段内主题的活跃程度，主题活跃程度越高，表明该主题受到的关注度也就越高[16]。具体计算公式如下。

$$TI_t^k = \frac{\sum_{d=1}^{M} p_d^k}{M} \quad (1)$$

其中，TI_t^k是指t时间段内主题k的强度，p_d^k表示第d篇文档中第k个主题的概率，M为文档数量。

4　结果与讨论

4.1　美国顶尖智库在网络安全领域的研究成果概况

本研究就美国顶尖智库在网络安全领域的发文量、关键词和文档主题进行分析。

美国顶尖智库的发文量代表其对该领域的关注度[10]，从图1可知，整体上发文量呈现稳步增长态势，这说明美国顶尖智库对网络安全的关注度

日益增强。从增长率可以看出，2019 年和 2022 年的发文量增长较多，2019 年 5 家顶尖智库发文量较 2018 年增长了 30.56%；在连续两年保持较为稳定的增长后，2022 年 5 家顶尖智库在网络安全领域的发文量又一次显著提升，增长率达到 20.00%。

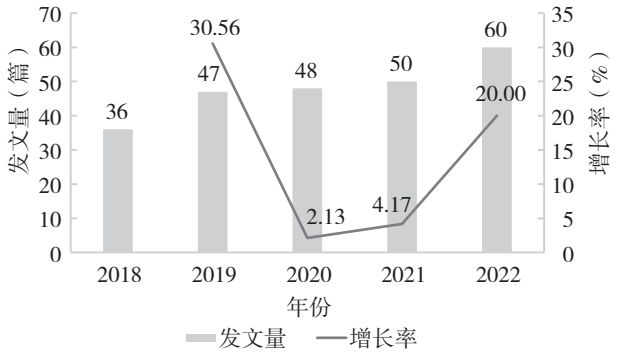

图 1　2018—2022 年美国顶尖智库在网络安全领域年发文量

从高频词（见表 1）和高频词共现图谱（见图 2）可以看出，美国顶尖智库在网络安全方面的研究重点主要有以下 3 个方面：一是不同领域的网络安全防御，如选举、金融、军事和关键基础设施等领域（“election”“financial_institutions”“military”“infrastructure”等）；二是网络安全相关技术及其风险治理（“technology”“data”“AI”“risk”等）；三是网络外交和国际关系，主要是中美关系（“China”）、美俄关系（“Russia”）和美欧关系（“EU”“NATO”）等。同时，“company”“government”等高频词的共现也体现了美国网络安全政策中政府主导、公私协同的特点[17]。

表 1　美国顶尖智库在网络安全领域的研究成果排名前 20 位的高频词

序号	高频词
1	USA
2	China
3	EU
4	data
5	technology
6	risk
7	Russia
8	digital_trade
9	government
10	defense
11	election
12	financial_institutions
13	attack
14	company
15	DOD
16	threat
17	NATO
18	infrastructure
19	military
20	AI

续表

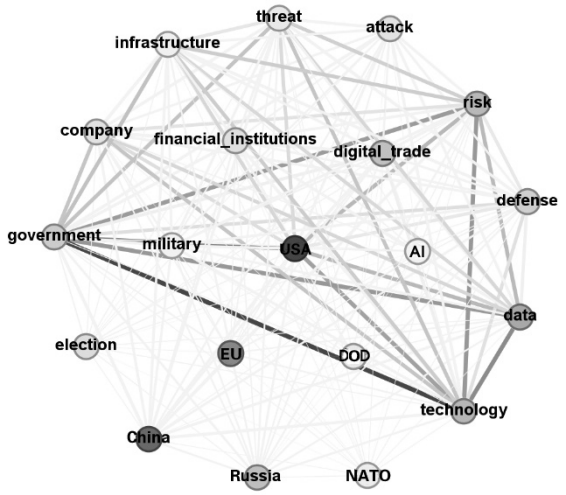

图 2　美国顶尖智库在网络安全领域研究的高频词共现图谱

困惑度评价曲线见图 3，当主题数目 K=8 时，曲线变化显著减缓，即到达真实聚类数，K 值再增加则得到的聚类回报会迅速变小，因此确定最终主题数目为 8，设置每个主题下输出前 15 个主题词，主题词分布和主题强度见表 2。按照主题强度进行排名，排名在前 3 位的主要有中美科技竞争、技术风险与治理和网络安全人才培养。本研究将结合文本分析等方法[10]，对上述 3 个主题的相关研究内容进行深入分析。

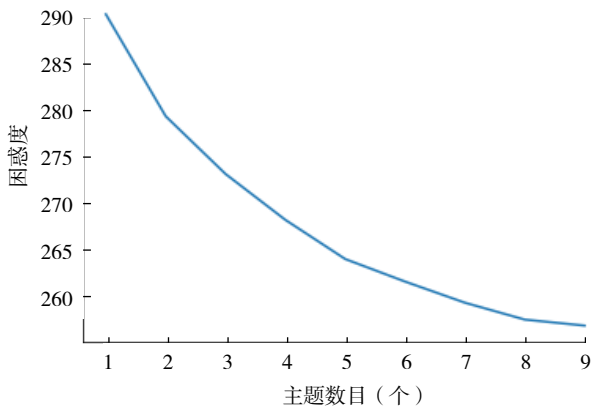

图 3　LDA– 困惑度评价曲线

4.2　中美科技竞争智库研究的内容比较

网络安全已经成为中美科技竞争的重点领域。整体而言，美国顶尖智库普遍承认中国的发展对美国的经济、技术和网络安全的领导地位带来了威胁和挑战，但无论是支持美国对中国的遏制策略还是支持中美两国合作，本质上都是以美国利益为先，从而确保美国在全球的领导地位。具体而言，主要政策主张和建议倾向主要可以划分为三大类。

第一类是兰德公司和战略与国际问题研究中心表现出较强的保守主义色彩，表示中国挑战了美国权威和以美国为首的世界秩序，并建议美国采取措施制裁中国。2018 年，兰德公司认为中国试图创建一种新的网络空间制度以获得主导权，这会影响全球网络空间的未来，建议美国通过加强多边主义以遏制中国的发展 [18]；同年，战略与国际问题研究中心也表示中国正在成为信息通信技术的全球领导者，挑战了美国主导的网络安全标准和国际秩序 [19]。这一阶段美国政府态度也趋于强硬，积极推进多边主义，联合多个国家共同维护以美国为主导的网络空间秩序，并采取“清洁网络”等计划限制中国信息通信技术的发展。但随着中美竞争的演化，两家顶尖智库也认识到中美竞争对美国技术创新和经济发展造成的损失，建议美国在制定政策时平衡好国家安全和经济利益 [20]。兰德公司提出可以允许高通公司等美国芯片制造商向中国手机制造商销售芯片，保证美国供应链经济健康发展，使美国对华为政策和美中两国之间的贸易问题分开探讨 [21]。但在关键领域，两家智库仍倾向于保持遏制策略，限制中国高新技术的发展。

二是在政治立场上处于中间位置的美国外交关系协会对美国遏制中国发展的策略提出了反对意见。从加强美国创新能力出发，为美国在中美竞争

表 2　美国顶尖智库在网络安全领域的研究成果主题分布

序号	主题	主题词	主题强度
1	虚假信息	election, Russia, social, USA, medium, norm, political, action, disinformation, attack, international_relations, EU, campaign, effort, response	0.1357
2	中美科技竞争	China, USA, technology, data, company, digital_economy, supply, risk, chain, software, government, industry, standard, Huawei, market	0.2797
3	金融安全	data, financial_institutions, risk, system, service, sector, technology, government, network, infrastructure, attack, institution, threat, company, development	0.0647
4	国际关系	EU, USA, defense, Russia, NATO, China, policy, cooperation, military, strategy, force, country, international, AI, region	0.0621
5	技术风险与治理	risk, data, service, technology, encryption, company, government, cloud, software, network, vulnerability, law, national_security, quantum, access	0.1703
6	关键基础设施保护	election, cloud, power, energy, risk, grid, supply, USA, software, framework, sector, service, infrastructure, chain, increase	0.1149
7	隐私保护	digital_trade, data, internet, USA, government, privacy, law, trade, online, access, country, encryption, user, policy, service	0.0773
8	网络安全人才培养	workforce, data, knowledge, program, industry, DOD, organization, incident, talent, education, researcher, personnel_management, career, training, technology	0.1419

中保持领先地位提出建议。美国外交关系协会表示，中国利用 5G 基础设施进行情报搜集和网络攻击，对美国的网络安全构成了严重威胁，但对华为等公司的技术限制可能会削弱美国的网络安全，美国更应该从技术措施、监管协调和外交关系等方面在制定全球规范和促进美国网络安全利益方面发挥领导作用[22]。美国外交关系协会指出，尽管中国的技术发展已经威胁到了美国的领导地位，但美国应该专注于发展自身实力，提高国家科技创新能力，超越中国远比放慢中国发展脚步更有效[23]，科技创新才是赢得未来的关键。

三是卡内基国际和平基金会和布鲁金斯学会对中美竞争态势表示担忧，希望中美加强合作。卡内基国际和平基金会指出，网络空间的安全和稳定发展取决于信息通信技术供应链的完整性，而以政治和商业利益为目的的干预行为破坏了供应链完整性[24]；布鲁金斯学会也表示，中美两国关系恶化使得通过外交手段解决网络安全问题的范围缩小，两国倾向于使用贸易和投资限制保护网络安全，这对全球贸易带来极大挑战[25]，鉴于中美两国的共同关切，双方可以就能源、电网等领域的网络安全问题达成共识，以应对未来挑战[26]。

4.3 技术风险与治理智库研究的内容比较

美国顶尖智库从新兴技术的优势和风险两个角度出发，探讨了新兴技术对网络安全的影响，一方面倡导对新兴技术的合理利用，另一方面强调技术风险治理，规范技术的开发和应用，同步推动新兴技术的应用。

一是倡导合理利用新兴技术以保护网络安全。战略与国际问题研究中心指出，技术应用能力与创新能力同等重要，如何利用人工智能等新兴技术推动经济发展、保障国家安全将是未来国际竞争的核心[27]。布鲁金斯学会分析了 5G 技术对网络安全的影响，提出改进网络安全保护确保 5G 技术的快速部署，利用人工智能和机器学习以保护软件是应对网络攻击的有效方法[28]。卡内基国际和平基金会认为人工智能技术在网络安全攻击的动态应对上拥有巨大潜力，它们可以帮助提高安全性能，加强对数字系统的保护，使其免受越来越多的复杂网络威胁，而利用人工智能的优势实现更广泛的网络安全防御，需要进一步完善相关政策和协调利益相关者[29]。

二是较为关注新兴技术带来的风险，建议从顶层设计和标准等层面规范技术应用和预防风险。兰德公司指出，无人机为恶意攻击者提供了漏洞和攻击渠道，美国国土安全部应该在政策层面制定一项无人机网络战略，在技术层面优先考虑关键技术漏洞以及反无人机系统的发展、监测无人机以区分合法和非法的使用行为[30]；战略与国际问题研究中心认为自动驾驶技术仍面临网络安全、隐私和数据保护等问题，相关政策和统一标准需要更新和改进[31]；美国外交关系协会认为人工智能和其他新技术将增加网络安全战略的不稳定性，而借助技术保护网络安全会导致更高程度的技术依赖，可能会产生不良后果，制定网络空间规范比网络威慑更加有效[32]。此外，兰德公司连续 3 年发布报告重点讨论了量子计算对当前网络加密系统造成的冲击，建议做好超前部署[33-35]。鉴于以上风险的担忧，美国政府也制定了一系列政策预防技术风险。《美国国家网络安全战略》要求在软件设计过程中和应用之前要先进行网络安全审查，以确保软件和硬件的网络安全；同时与盟友和伙伴国合作，推行负责任的国家行为规范。美国国家标准与技术研究院也发布《人工智能风险管理框架 1.0》，为人工智能开发过程中的可信度和安全性等提供参考[36]。美国网络安全与基础设施安全局（CISA）也发布相关报告，敦促利益相关者做好向后量子密码标准迁移的准备[37]。

4.4 网络安全人才培养智库研究的内容比较

美国顶尖智库就形成体系化的网络安全人才力量达成共识，重点关注人才的吸引、留用和多样性等关键问题。美国智库则提出网络安全人才应在质量上占据优势，从人才教育和培训等方面持续发力，培养高技能人才。

一是需要强有力的政策吸引和留用人才，扩大人才库。卡内基国际和平基金会指出，随着各国更积极地吸引优秀科学家，美国需要考虑采取新的方法留用外国研究人员，可以通过双边协调加强关键领域的人才流动和国际合作弥补国内人才不足的缺陷[38]；美国外交关系协会也表示美国创新环境的核心优势一直是源源不断的国内科学、技术、工程和数学（STEM）人才，以及美国吸引世界各地优秀人才的能力。在中美竞争环境下，美国需要强有力的政策吸引和留住人才，例如，制定一

项国防教育法案以扩大科学、技术、工程和数学方面的人才输送渠道，关注教育和培训中的公平性和多样性，为进入专业技术部门的学生减免学费，为在美国毕业的外国留学生提供便利以及允许移民在美国生活和工作等措施提升美国的科技竞争力[23]；战略与国际问题研究中心也指出可以通过定向培养、提高人才多样性（族裔、性别、地域和专业的多样性）等方式以扩大网络安全人才库[39]。美国相关部门也通过提高薪酬、增设奖学金项目等吸引网络安全人才。2021 年 8 月，美国国土安全部公布了网络安全人才管理系统以实现招聘和留用人才的灵活性，将给予网络安全专业人员最高可达 25.58 万美元的薪资，在更具有竞争力的地区薪资最高可增加至 33.21 万美元[40]。美国国土安全部、网络安全和基础设施安全局等机构也设立了荣誉计划等奖学金项目[41]。

二是提高人才质量，培养高技能人才。战略与国际问题研究中心指出美国无法在人才数量上超越中国，在人才质量上占据优势是保持竞争力的关键[42]；聚焦网络安全人才培养，美国需要加强基础教育和实践学习，通过提高学术卓越中心标准、加强校企合作和企业内部的再培训等措施夯实基础、培养技术型人才[43]。兰德公司也探究了网络运营官留用和招聘的潜在驱动因素，技术能力的深入、职业愿景的明确性以及持续培训等是员工选择留用与否的重要因素[44]。《美国国家安全战略》将网络安全人才的培养作为 27 项举措之一，明确提出由国家网络主任办公室（ONCD）领导制定并监督国家网络劳动力和教育战略的实施，提高人才的多样性，增加获得网络教育和培训途径的机会以提升人才质量，继续保持网络安全人才优势，推进人才体系建设。

5　结论

本研究基于智库文本分析了美国顶尖智库在网络安全领域的研究态势，并结合政策事件和文本分析对相关研究主题进行了探讨，以深入了解美国顶尖智库在网络安全领域的研究态势，为中国智库建设和网络安全领域发展提供借鉴。主要结论如下：一是从发文量看，美国顶尖智库对网络安全的关注日益增强，且反映了美国政府的关注程度；二是从研究内容看，美国顶尖智库在网络安全领域的研究主要聚焦八大主题，最受关注的细分领域主要是中美科技竞争、技术风险与治理及人才培养。三是从决策支撑效果看上，美国顶尖智库始终不断追求在网络安全领域的实力提升，推动以美国为中心的全球网络空间秩序、探索新兴技术的应用和风险防范、推出新的政策吸纳高科技人才和团队以维持美国竞争力。美国顶尖智库的研究成果和建议也已经成为美国政府决策的重要参考依据，在完善美国网络安全顶层设计、吸引人才等方面起到了重要的支撑作用。■

参考文献：

[1] The Cybersecurity and Infrastructure Security Agency. What is cybersecurity[EB/OL]. [2023-04-26]. https://www.cisa.gov/news-events/news/what-cybersecurity.

[2] 胡璇 , 程德斌 , 冷昊 , 等 . 美国网络安全发展现状及制度体系建设研究 [J]. 电子产品可靠性与环境试验 , 2022, 40(5): 73-79.

[3] 黄雯 , 温芳芳 . 美国智库的成果传播及其对北极决策的影响 : 以传统基金会、卡内基国际和平基金会和外交关系委员会为例 [J]. 情报杂志 , 2020, 39(2): 27-34.

[4] 蒋观丽 , 文少保 . 美国智库如何影响政府教育决策 : 以布鲁金斯学会布朗教育政策中心为例 [J]. 现代教育管理 , 2019(7): 123-128.

[5] 韩娜 , 杨念奔 , 石斌 . 美国智库对涉华网络安全议题的建构及启示 [J]. 情报杂志 , 2022, 41(7): 34-40.

[6] 刘昊 , 张志强 , 田鹏伟 , 等 . 美国一流智库在网络安全领域的研究成果分析 : 基于文本量化的视角 [J]. 图书与情报 , 2017(3): 124-33.

[7] 霍淑红 . 美国主要智库对中美网络安全问题的认知分析 [J]. 智库理论与实践 , 2020, 5(5): 80-88.

[8] 鲁传颖 . 美国智库在网络安全政策决策机制中的作用及特点 [J]. 现代国际关系 , 2015(7): 42-49, 64.

[9] 韩娜 , 邹初妤 , 王建军 . 冷战后西方智库涉华安全话语主题演变研究 : 基于西方五大智库的 LDA 分析 [J]. 智库理论与实践 , 2022, 7(4): 113-123.

[10] 张誉曜 , 陈媛媛 . 美国著名智库文本成果研究 : 以人工智能领域为例 [J]. 图书馆论坛 , 2021, 41(2): 152-160.

[11] 张誉曜 . 关键词视角下的美国智库文本研究 [D]. 乌鲁木齐 : 新疆师范大学 , 2021.

[12] MCGANN J G. 2020 Global go to think tank index report[R/OL]. [2023-04-18]. https://repository.upenn.edu/

think_tanks/18/.

[13] 李恒阳 . 特朗普政府网络安全政策的调整及未来挑战 [J]. 美国研究 , 2019, 33(5): 41-59, 5-6.

[14] 刘子林 . 特朗普政府网络安全政策研究 [D]. 北京 : 外交学院 , 2022.

[15] 刘微 , 王慧 , 雷蕾 , 等 . 北京市科技金融政策供需匹配研究 : 基于 LDA 政策文本计量方法 [J]. 经济问题 , 2023(1): 52-60.

[16] 李华东 , 伊惠芳 , 刘细文 . 基于文献计量和主题模型的对撞机技术发展态势研究 [J]. 世界科技研究与发展 , 2022, 44(3): 342-353.

[17] 肖杰 . 2021 年上半年美国拜登政府网络安全政策分析 [J]. 中国信息安全 , 2021(6): 81-84.

[18] Rand Corporation. China and the international order[EB/OL]. [2023-03-11]. https://www.rand.org/pubs/research_reports/RR2423.html.

[19] Center for Strategic and International Studies. How Chinese Cybersecurity Standards impact doing business in China[EB/OL]. [2023-04-18]. https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.

[20] Center for Strategic and International Studies. The costs of U.S.-China semiconductor decoupling[EB/OL]. [2023-03-11]. https://www.csis.org/blogs/new-perspectives-asia/costs-us-china-semiconductor-decoupling.

[21] Rand Corporation. Securing 5G: A way forward in the U.S. and China security competition [EB/OL]. [2023-04-18]. https://www.rand.org/pubs/research_reports/RRA435-4.html.

[22] Council on Foreign Relations. Securing 5G networks: challenges and recommendations[EB/OL]. [2023-04-18]. https://www.cfr.org/report/securing-5g-networks.

[23] Council on Foreign Relations. Innovation and national security: keeping our edge[EB/OL]. [2023-03-11]. https://www.cfr.org/report/keeping-our-edge/.

[24] Carnegie Endowment for International Peace. ICT supply chain integrity: principles for governmental and corporate policies[EB/OL]. [2023-04-18]. https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974.

[25] Brookings Institution. Cybersecurity, digital trade, and data flows: re-thinking a role for international trade rules [EB/OL]. [2023-04-26]. https://www.brookings.edu/research/cybersecurity-digital-trade-and-data-flows-re-thinking-role-for-international-trade-rules/.

[26] Brookings Institution. Secure power: gigawatts, geopolitics, and China's energy internet [EB/OL]. [2023-04-26]. https://www.brookings.edu/research/secure-power-gigawatts-geopolitics-and-chinas-energy-internet/.

[27] Center for Strategic and International Studies. National security implications of leadership in autonomous vehicles [EB/OL]. [2023-04-02]. https://www.csis.org/analysis/national-security-implications-leadership-autonomous-vehicles.

[28] Brookings Institution. Why 5G requires new approaches to cybersecurity: racing to protect the most important network of the 21st century [EB/OL]. [2023-04-18]. https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

[29] Rand Corporation. The artificial intelligence and cybersecurity nexus: taking stock of the European Union's approach [EB/OL]. [2023-04-18]. https://carnegieeurope.eu/2022/09/15/artificial-intelligence-and-cybersecurity-nexus-taking-stock-of-european-union-s-approach-pub-87886.

[30] Rand Corporation. How to analyze the cyber threat from drones: background, analysis frameworks, and analysis tools[EB/OL]. [2023-04-18]. https://www.rand.org/pubs/research_reports/RR2972.html.

[31] Center for Strategic and International Studies. Driving the future of av regulations: barriers to large-scale development[EB/OL]. [2023-04-18]. https://www.csis.org/analysis/driving-future-av-regulations-barriers-large-scale-development.

[32] Council on Foreign Relations. Confronting reality in cyberspace:foreign policy for a fragmented internet[EB/OL]. [2023-04-26]. https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace.

[33] Rand Corporation. Securing communications in the quantum computing age: managing the risks to encryption[EB/OL]. [2023-03-11]. https://www.rand.org/pubs/research_reports/RR3102.html.

[34] Rand Corporation. Preparing for post-quantum critical

infrastructure: assessments of quantum computing vulnerabilities of national critical functions[EB/OL]. [2023-03-11]. https://www.rand.org/pubs/research_reports/RRA1367-6.html.

[35] Rand Corporation. Commercial and military applications and timelines for quantum technology[EB/OL]. [2023-03-11]. https://www.rand.org/pubs/research_reports/RRA1482-4.html.

[36] The White House. Remarks of Dr. Alondra Nelson at the launch of the NIST AI risk management framework[EB/OL]. [2023-03-11]. https://www.whitehouse.gov/ostp/news-updates/2023/01/26/remarks-for-dr-alondra-nelson-at-the-launch-of-the-nist-ai-risk-management-framework/.

[37] The Cybersecurity and Infrastructure Security Agency. Preparing critical infrastructure for post-quantum cryptography[EB/OL]. [2023-03-11]. https://www.cisa.gov/news-events/alerts/2022/08/24/preparing-critical-infrastructure-post-quantum-cryptography.

[38] Carnegie Endowment for International Peace. U.S.-Japan technology policy coordination: balancing techno nationalism with a globalized world[EB/OL]. [2023-04-26]. https://carnegieendowment.org/2020/06/29/u.s.-japan-technology-policy-coordination-balancing-technonationalism-with-globalized-world-pub-82176.

[39] Center for Strategic and International Studies. A shared responsibility: public-private cooperation for cybersecurity[EB/OL]. [2022-03-11]. https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity.

[40] The Record from Recorded Future News. DHS launches new effort to attract cybersecurity talent[EB/OL]. [2023-03-11]. https://therecord.media/dhs-launches-new-effort-to-attract-cybersecurity-talent/.

[41] The U.S. Department of Homeland Security. Cybersecurity student programs [EB/OL]. [2023-03-11]. https://www.dhs.gov/homeland-security-careers/cybersecurity-student-programs.

[42] Center for Strategic and International Studies. How China's human capital impacts its national competitiveness[EB/OL]. [2023-04-26]. https://www.csis.org/analysis/how-chinas-human-capital-impacts-its-national-competitiveness.

[43] Center for Strategic and International Studies. The cybersecurity workforce gap [EB/OL]. [2023-04-18]. https://www.csis.org/analysis/cybersecurity-workforce-gap.

[44] Rand Cooperation. Attracting, recruiting, and retaining successful cyberspace operations officers cyber workforce interview findings[EB/OL]. [2023-03-26]. https://www.rand.org/pubs/research_reports/RR2618.html.

Analysis of American Top Think-tank's Research on Cybersecurity

WANG Yan, GAO Fang

(Institute of Scientific and Technical Information of China, Beijing　100038)

Abstract: This study aims to analyze the research trends of American top think-tanks in the field of cyber-security from both time and theme perspectives, in order to better understand the current state of the research and predict the direction of American cyber-security strategy, and provide reference for China's cyber-security development and think-tank construction. This study analyzes the research results of American top think-tanks of cyber-security from 2018 to 2022 using the LDA topic model, and interprets relevant topics with policy events. The study found that the focus of American think-tanks on cyber-security is constantly increasing, with research results mainly focusing on Sino-U.S. technology competition, technology risks and governance, and cyber security talent cultivation. They have been committed to maintaining and enhancing America's competitiveness in cyberspace, and their research results and suggestions have played an important role in the development and promotion of American cyber security.

Keywords: the United States; think-tank research; cybersecurity; LDA topic model; policy research