澳大利亚战略政策研究所网络安全领域研究及对中国智库的启示 *

■ 朱敏[1] 张志强[2,3] 陈秀娟[4] 唐川[2,3]

[1] 江苏省公安厅 南京 210024
[2] 中国科学院成都文献情报中心 成都 610041
[3] 中国科学院大学经济与管理学院图书情报与档案管理系 北京 100190
[4] 南京师范大学新闻与传播学院 南京 210097

摘要：[目的/意义]自《关于加强中国特色新型智库建设的意见》发布以来，国内学者对西方知名智库进行了全面、深度的研究，取长补短，积极发展中国特色新型智库，但对除欧美之外的智库研究较少。因此笔者以澳大利亚权威智库澳大利亚战略政策研究所（ASPI）为研究对象，介绍了 ASPI 在网络安全与信息化领域的研究成果，为我国智库的发展提供借鉴。[方法/过程]本文主要使用了文献调研和网络调研的研究方法，介绍了 ASPI 的发展历程，梳理了近年来其在新兴科技领域的研究成果。[结果/结论] ASPI 共有 7 大研究领域，主要包括国防战略与国家安全、反恐、国际网络政策、国际计划、风险与应变、北部与澳大利亚安全以及战略警务和执法计划。在新兴科技领域，ASPI 极为关注与中国的合作和竞争关系研究。ASPI 在人员流动与合作机制、国际交流与合作、社交媒体利用等方面的经验值得国内智库学习和借鉴。

关键词：澳大利亚战略政策研究所 智库 网络安全
分类号：C932.8
DOI: 10.19318/j.cnki.issn.2096-1634.2020.04.11
开放科学（资源服务）标识码（OSID）

澳大利亚战略政策研究所（Australian Strategic Policy Institute，ASPI）是澳大利亚政府于 2001 年创建的一个独立、无党派的战略政策研究机构，侧重于国家安全、国防军事战略方向的研究，为政府提供新的想法，帮助政府就澳大利亚的未来发展做出更明智的决策。ASPI 是澳大利亚最为权威的智库之一，许多观点被广泛引用到对澳大利亚战略决策问题的公众讨论之中，对国际问题尤其是亚太问题的讨论也颇负盛名。其在《全球智库报告 2019》国防和国家安全领域全球智库排在第 13 位（共有 110 个智库参与排名），在外交政策和国际事务领域全球智库排在第 33 位（共有 156 个智库参与排名）。

本文以 ASPI 为研究对象，综合文献调研

* 本文系中国科学院政策研究课题“国际科技态势发展研究”（项目编号：ZYS-2020-03）及中国科学院文献情报能力建设专项项目“科技领域战略情报研究咨询体系建设”（项目编号：E0290001）研究成果之一。
作者简介：朱敏 (ORCID：0000-0002-6872-4270)，江苏省公安厅主任科员，硕士；张志强（ORCID：0000-0001-7323-501X），通讯作者，中国科学院成都文献情报中心主任，研究员，博士生导师，中国科学院特聘核心研究员，E-mail：zhangzq@clas.ac.cn；陈秀娟 (ORCID：0000-0002-8063-7647)，南京师范大学新闻与传播学院讲师，博士；唐川 (ORCID：0000-0001-5651-5052)，中国科学院成都文献情报中心副研究员，硕士。

和网络调研的研究方法，剖析 ASPI 的发展历程、人员构成、主要研究领域以及对网络安全领域的研究进展和趋势，以期为中国特色新型智库在未来更好地服务国家情报工作提供参考借鉴。

1 ASPI 总体发展情况

ASPI 由澳大利亚国防部于 2001 年 7 月 6 日创立，其发展主要经历了两个阶段：① 2001—2012 年期间，ASPI 主要关注传统国防领域，致力于提供与政策相关的研究和分析，以更好地帮助政府在战略和国防问题上进行决策，帮助公众进一步了解战略和国防问题；② 2012 年至今，彼得·詹宁斯（Peter Jennings）担任 ASPI 的执行主席，ASPI 的研究领域从高质量的国防研究扩展到了网络安全研究、治安维持和国际执法、边境安全等新领域，使得 ASPI 与政府、议会、行业和国际伙伴建立了密切的工作关系 [1]。

ASPI 的组织架构如图 1 所示，ASPI 拥有两个研究项目，一是国防与战略计划，包括国防战略和能力小组、国际网络政策中心和战略家；二是国家安全项目，包括反恐政策中心、国际计划小组、战略警务和执法计划 / 北部安全小组以及风险与应变计划小组。

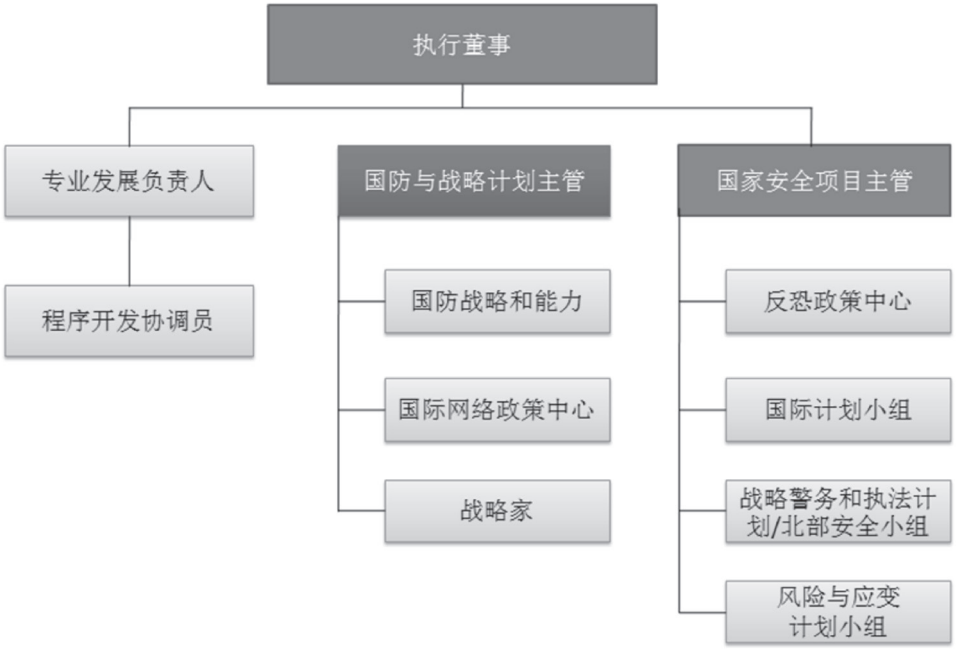

图 1 ASPI 组织架构
Figure 1 The organizational structure of ASPI

ASPI 由国防部提供部分研究经费，其他经费来源包括赞助、委托任务、会员计划、出版物销售、广告和活动注册费。2018 年度，ASPI 的经费收入为 530 万澳元，国防部的资助是 ASPI 的主要资金来源，占到总经费的 37%，委托收入占到了 32%，会员赞助和订阅占到了 25%，其他占 6%[2]。

ASPI 目前共有 40 位专家、18 位研究员和 17 名工作人员。成员主要来自政府部门、军队、教育界和媒体。ASPI 现任理事会主席肯·吉莱斯皮（Ken Gillespie）曾担任澳大利亚陆军总司令，拥有丰富的实践经验，在政府、国防、安全和商业领域拥有强大的人际联络网。现任执行主席彼得·詹宁斯（Peter Jennings）曾在国防和国家安全部门担任要职 [3]。其他成员的研究背景和身份背景分别见图 2、图 3[4]。

其中，从性别上来看，ASPI 研究人员中 42 人为男性，16 人为女性。身份背景构成上，有 25 人来自政府，约占总人数的 43%；11 人来自教育界，约占 19%；9 人来自企业，主要是撰稿人或编辑，约占总数的 16%；6 人来自军队；2 人在加入 ASPI 前是社会活动家或自由撰稿人。成员研究领域主要集中于国防安全、国土安全、军事能力、

维和反恐和网络空间。其中，有 6 位学者从事中国国防、军事、科技相关的研究，有 3 位研究员来自美国的军方或政府，体现出 ASPI 对中国和美国的军事战略、国防科技的重点关注和研究倾向。

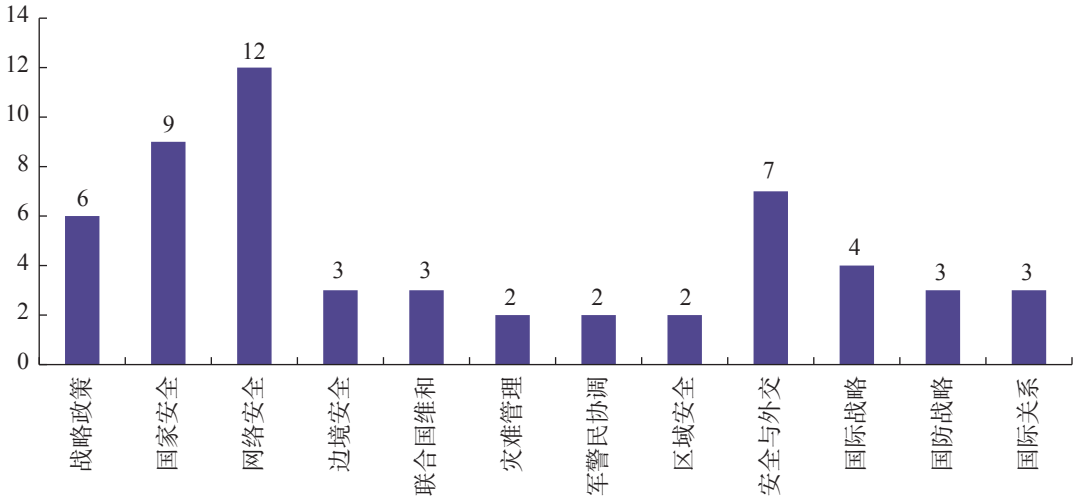

图 2 ASPI 成员专业背景分布

Figure 2 The professional background of ASPI’s members

备注：ASPI 成员中有 2 人负责程序开发，未参与研究领域统计。

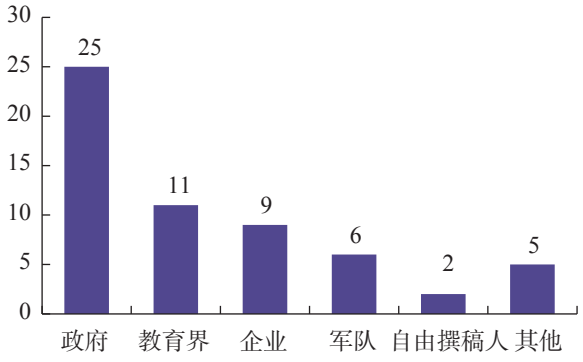

图 3 ASPI 成员身份背景分布

Figure 3 The identity background of ASPI’s members

2 ASPI 战略与政策研究主要领域及其成就

ASPI 的研究工作主要是以“项目”或“研究中心”的形式组织的，这些“项目”或“研究中心”类似于一个研究领域。ASPI 拥有 6 个项目和一个研究中心，分别是国防、战略与国家安全项目，反恐项目，国际网络政策中心，国际项目，风险与应变项目，北部和澳大利亚安全项目，战略警务和执法项目。这些项目和研究中心的详细介绍如下。

2.1 国防、战略与国家安全项目（Defence, Strategy and National Security Program）

国防、战略与国家安全项目涵盖了 ASPI 在战略政策领域的传统核心工作，侧重于广泛的战略政策、全球和区域安全、澳大利亚国防军的作战需求，和澳大利亚国防能力的发展以及与国防资金和预算有关的问题。该项目广泛分析和研究战略趋势与军事之间的相互变化，包括：①权力变化对军事事务的影响；②常规武器和核武器在 21 世纪的作用；③经济、人口变化趋势的战略影响。该项目还分析研究澳大利亚国防军各个阶段的需求，包括：①确定未来作战能力的需求；②分析物资解决方案的竞争选择；③跟踪综合投资项目（Integrated Investment Plan）的项目进度；④探索与澳大利亚国防军人员有关的问题，如征兵、训练等；⑤评估国防军相对于地方军队的作战能力。此外，该项目还分析和评估澳大利亚的国防预算和支持国防军进行广泛活动所需的能力，包括：①短期和长期的国防资金；②国防工业的政策和能力；③项目管理策略；④国防经济趋势。近年来，ASPI 在该项目领域向政府提交了《国防物理科学和工程人员的能力》《计划购买 F-35 联合打击战斗机》《潜艇的战略价值》《部分中止对伊朗的制裁》等研究成果 [5]。

2.2 反恐项目（Counter-terrorism Program）

ASPI 于 2015 年启动该项目，并将之作为 ASPI 的重要研究领域。该项目旨在分析反恐环境，

包括政策、立法、恐怖威胁和国际问题并提供反恐政策建议、替代方案和竞争能力。该项目主要进行反恐主题的研究，促进利益相关方进行对话和讨论，并向政府、社区和行业利益相关者提供建议，尤其是如何开展反恐工作。近年来，ASPI 在该领域向政府提交了关于《2016 年刑法修正案（高危恐怖分子罪犯）条例草案》《2016 年严重有组织犯罪修正案》等研究成果 [6]。

2.3 国际网络政策中心（International Cyber Policy Centre）

ASPI 下属的国际网络政策中心（International Cyber Policy Centre，ICPC）在有关网络和新兴技术及更广泛的战略政策方面的研究处于全球领先地位。ICPC 通过开展原创性的研究，将不同专业知识、背景的研究人员聚集在一起，为公众提供信息并支持合理的公共政策。ICPC 在澳大利亚和海外为公共部门和私营部门提供研讨会、培训课程和大规模活动。ICPC 通过将世界一流的专家引入澳大利亚，丰富了有关网络和战略政策的全国性辩论 [7]。

2.4 国际项目（International Program）

ASPI 的国际项目探讨了维护国际和平和安全的挑战，这些项目既与澳大利亚直接相关，也对多边安全问题的国际研究工作做出了贡献。国际项目旨在：①加深澳大利亚和国际上对全球安全问题和多边和平行动的了解；②促进政府、私营部门和民间社会的主要利益相关方参与国际和平和安全有关的问题；③提供与澳大利亚面临的挑战和机遇相关的政策咨询，以促进和维护国际和平与安全。近年来，ASPI 在该领域向政府提交了《澳大利亚与非洲国家的贸易和投资关系》《印度洋领土的战略问题》《对外国投资的审查框架》等研究成果 [8]。

2.5 风险与应变项目（Risk and Resilience Program）

该项目包括在社区、地方政府机构、地区以及州和联邦政府层面建立抵御灾害的能力。该项目涵盖了所有危害、所有机构的问题、基础设施的弹性以及澳大利亚为“印度 - 太平洋”地区提供人道主义援助和救灾帮助。该项目有 4 个关键领域：①在全国范围内推广以建设抵御灾害能力为中心的有效的降低灾难风险的实践；②将弹性作为关键基础设施系统的设计因素；③促进关于如何产生和维持社区复原能力的辩论；④加强区域（东盟和大洋洲）灾害管理能力建设。近年来，ASPI 在该领域发布的《气候变化对澳大利亚国家安全的影响》被参议院外交、国防和贸易委员会采纳 [9]。

2.6 北部和澳大利亚安全项目（The North and Australia’s Security Program）

该项目对澳大利亚北部的安全以及北部在促进澳大利亚更广泛的安全方面的关键作用进行了持续的重点研究。该项目着重于：①对北方在澳大利亚更广泛安全中的作用保持强烈的公共政策关注；②通过更新以 1980 年代“澳大利亚防卫”为基础的战略框架，发展北方和安全的现代化思维方式；③将北部放在除国防外的国家安全利益中进行广泛讨论，包括内政、边境安全和海关、太空、网络安全，人道主义和灾难响应，生物安全和能源安全 [10]。

2.7 战略警务和执法项目（Strategic Policing and Law Enforcement Program）

该项目研究了执法对于国家安全以及更广泛的战略政策的影响。主要研究领域包括：①分析执法问题以及其与国家安全问题之间的联系；②执法机构对澳大利亚国际目标的贡献；③执法机构的未来定位。近年来，ASPI 在该领域向政府提交了《2017 年澳大利亚国家安全立法修正案》《2017 外国影响透明度计划法案》《2017 年澳大利亚广播公司修正案（恢复短波电台）条例草案》等相关研究成果 [11]。

3 ASPI 在网络安全领域的研究重点与影响力

ASPI 的一个重要研究领域是网络，其下属的国际网络政策中心通过传统的实证研究，识别、追踪和阐释网络安全领域最重要的发展，并提出建设性建议，以适应未来的变化。近几年 ASPI 推出的有关网络安全领域重要研究成果如表 2 所示。

表 2 ASPI 涉网络安全领域代表性研究成果

Table 2 The main research output on cyber security distributed by ASPI

发布年月	报告名称	内容主题
201910	新的中俄高科技伙伴关系	大数据和人工智能
201907	在 IT 和 OT 融合时代保护关键的国家基础架构	基础机构安全
201905	黑客与民主	网络舆论
201904	绘制中国的科技巨头	网络安全
201904	澳大利亚外交数字化	外交安全
201904	华为和 Telefunken：通信企业和不断发展的电力战略	通信安全
201812	澳大利亚的网络安全未来	网络安全
201810	华为与澳大利亚的 5G 网络	5G、中国
201806	网络空间中的威慑	网络威慑
201804	澳大利亚的网络攻击能力	网络攻击
201803	物联网的不安全因素	物联网
201711	量子技术及其在国防中的应用	量子技术
201705	澳大利亚的网络安全战略：实施与进展	网络安全
201705	数字时代的外交安全	外交安全
201703	澳大利亚 - 美国网络安全对话	网络安全
201611	网络规则与澳大利亚的隐私部门	网络治理
201607	网络空间中的威慑：不同领域、不同规则	网络威慑
201605	网络空间与武装力量：网络攻击能力的基本原理	网络战
201512	下一代互联网时代的澳中网络关系	中澳关系

3.1 重视中国网信政策及应对策略

ASPI 这几年发布的网络安全与信息化（简称“网信”）领域的重要研究成果中，有 40% 涉及中国。ASPI 围绕中国的微博外交、大数据与隐私等话题开展了研究，并向澳大利亚提出相关建议。

2015 年 12 月，ASPI 发布了《下一代互联网时代的澳中网络关系》，报告提到网络安全是国家安全的首要问题，而 ICT（Information and Communications Technology）网络对于澳大利亚的数字未来和经济繁荣至关重要，呼吁中澳双方进行更为紧密的对话，以便在面对共同的网络威胁时互相合作 [12]。

2018 年 5 月，ASPI 发布了《中国的微博外交与审查制度》，建议澳大利亚政府建立微博社交账号，扩大其在中国的影响力，同时呼吁外国政府应为其在中国的社交媒体账户建立并发布明确的使用条款 [13]。

此外，近两年，ASPI 发布了 5 篇分析中国在网信领域政策及龙头企业的报告，ASPI 认为，中国科技公司无疑为全球技术行业做出了重要而宝贵的贡献，为世界各地的人们提供负担得起的、高质量的设备和服务。但 ASPI 也对与中国公司合作过程中所带来的政治和安全隐患表示担忧，特别是在诸如 5G 等关键基础设施领域，以及可能涉及敏感或双重用途的技术。ASPI 呼吁澳大利亚政府加深对形成、限制和驱使中国公司全球行为的独特国家环境的了解，与中国的科技巨头接触时做出更明智的决定 [14-17]。

3.2 关注研究新兴技术带来的网络安全威胁

信息技术发展迅猛，新兴技术层出不穷，这些技术为网络安全带来机遇的同时也带来了挑战。ASPI 针对量子计算、5G、人工智能、物联网进行了深度分析，探讨了这些技术带来的网络安全威胁，结合目前澳大利亚的网络现状和法律法规，

呼吁政府和行业进一步讨论并共同努力利用新技术、更新法律法规来提高网络安全性。

3.3 专注研究澳大利亚国家层面的网络安全战略

ASPI 主要的研究内容是国家安全、国防战略，其在网络领域的研究也集中于网络安全和网络威慑，尤其是国家层面。2017 年 3 月，ASPI 发布了《澳大利亚 - 美国网络安全对话》，这次对话探讨了亚太地区的合作问题、打击网络犯罪和促进数字经济发展 [18]。同年 5 月还发布了《澳大利亚的网络安全战略》，评估了政府在 2016 年 4 月 21 日发布的网络安全策略的实施状况，并提出了改进策略 [19]。2018 年 12 月，ASPI 发布了《澳大利亚的网络安全未来》，构想了一个信息孤岛的互联网世界以及在这种零散的互联网世界中存在的大国博弈，并指出政府应该对这种情况的发生准备应急预案。ASPI 专注于澳大利亚的网络安全，积极为政府部门的网络安全策略出谋划策，有效推动了澳大利亚网络安全的发展 [20]。

4 ASPI 发展对我国相关智库的启示与建议

4.1 建立与决策部门之间的人员流动与合作机制

尽管多数智库都强调自己的独立性和透明性，但研究是否能够真正发挥作用离不开政府的支持与参与。因此，与政府保持良好的合作、加强人员流动是极为必要的。政府和智库之间保持交流和合作既能够促进智库开展有针对性的研究，又能够使政府获得更多的合理建议。国外智库的一大特点是，通过旋转门制度加强与决策部门之间的联合与合作。ASPI 由澳大利亚国防部成立，主要的资助也来自于国防部，每年承接大量国防部关于国防战略相关的研究。ASPI 大量的研究人员来自于政府，其历任执行董事曾在国防部和国家安全部门担任要职，与政府部门建立了良好的关系。ASPI 的年度报告显示，ASPI 的高级研究人员经常与澳大利亚的议员和高级官员们进行政策讨论。此外，ASPI 的成员们还积极参加政府咨询委员会和各类专家小组，仅 2018 年，ASPI 的成员应邀参加了国家复原能力工作组、国防与战略研究中心、国防大趋势研究、亚太减少灾害风险部长级会议等 11 项重要活动。ASPI 的研究工作对澳大利亚政府部门的决策形成了强力支撑。

在我国，智库与政府部门之间的沟通和交流渠道并不畅通，政府部门有时自以为是，官僚化倾向突出，不乐于听取智库的声音，也不建立与智库沟通的渠道；智库即使有意愿也难以与政府部门沟通，更不了解相关政府部门的战略考虑。二者相互之间的人员流动更是比较困难，基本上是政府官员退休后到一些智库兼职。为此，要建立智库与决策部门间的常态化沟通与成果报送机制，政府部门要建立面向专业化智库的咨询机制，智库需要主动加强与政府相关部门的交流沟通，通过“内参”、专家咨询等形式向政府部门提供咨询建议，二者相互合作，可以促进决策的科学化、民主化和智库决策咨询工作的专业化和高质量化。

4.2 加强国际交流访问和合作以提升智库国际影响力

提升国际影响力，掌握国际话语权是智库发展的重要任务。为了提升其国际影响力，ASPI 的主要做法包括：① ASPI 通过交流、访问、共同撰写出版物与多家智库保持合作伙伴关系；② ASPI 还利用人员之间的交流访问提升其国际影响力，ASPI 雇佣了多名来自其他研究机构的客座研究员，加深了其对国内外国防和国家安全事务的了解；③ ASPI 积极参与国际对话，ASPI 在 2018 年参与了 10 次国际对话；④ ASPI 的员工积极参与各类国际会议，在 2018 年度，他们在超过 15 个重要国际会议上发言。

通常情况下，我国智库不强调、不追求国际化，基本上都是国内型的机构。因此，在全球智库国际化发展的趋势下，我国智库的普遍问题是缺乏国际化发展的意愿和能力。缺乏国际化能力的智库，难以承担时代赋予的第五种力量的作用。应鼓励国内智库国际化发展，可以借鉴 ASPI 的做法，在加强学术、人才交流的同时，积极参与和主办各类国际对话、国际会议等，提升其国际影响力。

4.3 重视使用社交媒体扩大智库的社会影响力

在新媒体和自媒体时代，信息传播方式发生了革命性变化。一个不善于传播的智库，难以建立社会影响力，而社会影响力又是智库追求的重要发展效果。ASPI 非常善于使用社交媒体，其

通过官网、博客、出版物、活动预告、媒体活动等多种形式引起公众讨论从而影响政府决策。在2018 年，ASPI 举办了 142 次公共活动，包括圆桌讨论、大师班、研讨班等，来自澳大利亚和国际的众多学者参与其中进行讨论。ASPI 善于利用媒体发声，ASPI 的工作人员每周都会接受广播或电视采访就研究领域提供意见。2018 年全年，ASPI 的工作人员共进行了数百次访谈。在社交媒体方面，ASPI 的网站 2018 年的访问量为 59 万次，推特和脸书的关注人数为 2 万多，YouTube 拥有 6 万次的观看。

相较于 ASPI，我国的智库难以适应新媒体、自媒体时代的传播环境，仍然囿于象牙塔式的发展方式，在公众心中的形象太过于“束之高阁、无人问津”，难以在群众中形成热烈的关注和讨论。要证明自身的价值和意义，就必须重视对外传播，注重媒体公关以及传播策略 [21]。现在我国互联网日益普及化，网民人数达 8 亿多，居世界之最。国内智库要学会借助网络化的新媒体传播工具，积极参与，通过网络化传播智库的研究成果等形式，积极发挥引导社会思潮和社会进步的正能量作用，积极扩大智库的社会影响力。

参考文献：

[1] ASPI. About US[EB/OL]. [2020-03-27]. https://www.aspi.org.au/about-aspi.

[2] ASPI. 2019-2023 Corporate plan[EB/OL]. [2020-03-27]. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-09/ASPI%20Corporate%20Plan%202019-2023.pdf.

[3] ASPI. Peter Jennings[EB/OL]. [2020-03-27]. https://www.aspi.org.au/bio/peter-jennings.

[4] ASPI. Our people[EB/OL]. [2020-03-27]. https://www.aspi.org.au/our-people.

[5] ASPI. Defence, strategy and national security program[EB/OL]. [2020-03-27]. https://www.aspi.org.au/program/defence-strategy-and-national-security-program.

[6] ASPI. Counter-terrorism program[EB/OL]. [2020-03-27]. https://www.aspi.org.au/program/counter-terrorism-program.

[7] ASPI. International cyber policy centre[EB/OL]. [2020-03-27]. https://www.aspi.org.au/program/international-cyber-policy-centre.

[8] ASPI. International program[EB/OL]. [2020-03-27]. https://www.aspi.org.au/program/international-program.

[9] ASPI. Risk and resilience program[EB/OL]. [2020-03-27]. https://www.aspi.org.au/program/risk-and-resilience-program.

[10] ASPI. The North and Australia's Security Program [EB/OL]. [2020-03-27]. https://www.aspi.org.au/program/north-and-australias-security-program.

[11] ASPI. Strategic policing and law enforcement program[EB/OL]. [2020-03-27]. https://www.aspi.org.au/program/strategic-policing-and-law-enforcement-program.

[12] Simon Hansen. Australia–China cyber relations in the next internet era[EB/OL]. [2020-03-27]. https://www.aspi.org.au/report/australia-china-cyber-relations-next-internet-era.

[13] Fergus Ryan. Weibo diplomacy and censorship in China [EB/OL]. [2020-03-27]. https://www.aspi.org.au/report/weibo-diplomacy-and-censorship-china.

[14] ASPI. Huawei and Australia's 5G network[EB/OL]. [2020-03-27]. https://www.aspi.org.au/report/huawei-and-australias-5g-network.

[15] Rick Umback. Huawei and Telefunken Communications enterprises and rising power strategies[EB/OL]. [2020-03-27]. https://www.aspi.org.au/report/huawei-and-telefunken-communications-enterprises-and-rising-power-strategies.

[16] Danielle Cave, Samantha Hoffman, Alex Joske. Mapping China's technology giants[EB/OL]. [2020-03-27]. https://www.aspi.org.au/report/mapping-chinas-tech-giants.

[17] Samantha Hoffman. Engineering global consent: The Chinese Communist Party's data-driven power expansion [EB/OL]. [2020-03-27]. https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

[18] Liam Nevill, Zoe Hawkins, Tobias Feakin. The Australia–US Cyber Security Dialogue[EB/OL]. [2020-03-27]. https://www.aspi.org.au/report/australia-us-cyber-security-dialogue.

[19] Liam Nevill, Zoe Hawkins. Australia's cyber security strategy: Execution&evolution[EB/OL]. [2020-03-27]. https://www.aspi.org.au/report/australias-cyber-security-strategy-execution-evolution.

[20] Frank Smith, Aim Sinpeng, Ralph Holz. Australia's cybersecurity future(s)[EB/OL]. [2020-03-27]. https://www.aspi.org.au/report/australias-cybersecurity-futures.

[21] 张志强，苏娜．国际智库发展趋势特点与我国新型智库建设 [J]. 智库理论与实践，2016, 1(1): 9-23.

作者贡献说明：

朱　敏：搜集、整理资料和数据，撰写文章；

张志强：指导论文框架，总结启示，修改文章；

陈秀娟：搜集整理资料，修改文章；

唐　川：修改文章。

Research on Cyber Security Achievements of Australian Strategic Policy Institute and Its Inspiration to Think Tanks in China

Zhu Min[1] Zhang Zhiqiang[2,3] Chen Xiujuan[4] Tang Chuan[2,3]

[1]Jiangsu Provincial Department of Public Security, Nanjing 210024

[2]Chengdu Documentation and Information Center, Chinese Academy of Sciences, Chengdu 610041

[3] Department of Library Information and Archives Management, School of Economics and Management, University of Chinese Academy of Science, Beijing 100190

[4]School of Journalism and Communication, Nanjing Normal University, Nanjing 210097

Abstract: **[Purpose/significance]** Since the publication of "Opinions on Strengthening the Construction of New Type Think Tanks with Chinese Characteristics", a number of scholars have conducted comprehensive and in-depth research on well-known western think tanks, learned from others' strong points and filled in the gap. However, they pay less attention to think tanks other than Europe and the United States. Therefore, the article introduces the famous think tank in Australia, Australian Strategic Policy Institute(ASPI), to provide a reference for the development of think tanks in China. **[Method/process]** This article mainly uses the case study method and statistical analysis method, introduces the development course of ASPI, and sorts out its research results in cyber security in recent years. **[Result/conclusion]** ASPI has seven research areas, including defense, strategy and national security program, counter-terrorism program, international cyber policy, international program, risk and resilience program, the north and Australian security, and strategic policing and law enforcement program. In network security, ASPI pays great attention to cooperation and competition relationship with China. ASPI's experience in personnel mobility and cooperation mechanisms, international exchanges and cooperation, and utilization of social media is worth learning for domestic think tanks.

Keywords: Australian Strategic Policy Institute think tank cyber security

收稿日期：2020-03-04 修回日期：2020-03-28