中外法学 Peking University Law Journal
Vol.31, No.4(2019)pp.871－890

国家安全法律义务的性质辨析

基于中澳两国法律的比较

周汉华*

摘 要 对我国宪法和国家安全法律进行系统分析可以发现，个人与组织的国家安全法律义务在性质上属于消极性、防御性义务，即当有危害国家安全的情形时，应承担保卫国家安全的责任。二战之后的特殊国际格局则使澳大利亚的情报活动与情报法律带有明显的攻击性特点。而澳大利亚宪法的特殊性又使其情报配合法律义务既包括消极性、防御性义务，也包括积极性、攻击性义务。因此，澳大利亚对于我国国家安全法律的一般性、原则性规定存在着自身的因素，认为这些规定会强制中国企业从事攻击性间谍活动，显然是不能成立的。

关键词 国家安全法律义务 宪法义务 消极性义务 情报配合活动

澳大利亚以我国国家安全法律要求个人和组织承担国家安全法律义务为由，宣称中国企业有义务应情报机关的要求在其设备中植入“后门”，并据此在世界上第一个禁止中国企业参与其5G网络建设。〔1〕对此，李克强总理在今年的“两会”记者会上予以坚决否认，阐明了中

* 中国社会科学院法学研究所研究员。

〔1〕 澳大利亚政府在给澳大利亚电信运营商发布的5G安全指导意见中明确提出：“有可能受到外国政府与澳大利亚法律冲突的法外指挥的供应商，可能会使电信运营商无法有效防护5G网络免于受到未经授权的访问或者干扰”。这一指导意见的发布，实际等于宣布禁止华为、中兴参与澳大利亚的5G网络建设。Government Provides 5G Security Guidance To Australian Carriers, 23 August 2018, https://www.minister.communications.gov.au/minister/mitch－fifield/news/government－provides－5g－security－guidance－australian－carriers; Angus Grigg and Lisa Murray, “Federal government bans Huawei, ZTE from 5G on security concerns”, Aug. 23, 2018. https://www.afr.com/business/telecommunications/federal－government－bans－huawei－zte－from－5g－on－security－concerns－20180823－h14cv0，最后访问日期：2019年4月8日。

国政府的法律立场。〔2〕中澳之间对中国法律的不同解读，涉及中国企业走出去的前途与未来，学界应当加强对国家安全法律义务性质的理论研究，为完善国家安全立法和规范相关执法活动明确原则与边界。本文试图通过对中澳两国法律的比较，从三个方面回答这一事件涉及的几个主要问题，包括如何理解国家安全法律义务的性质、国家安全法律义务与宪法义务的关系、情报活动的法律边界、法律责任规定对国家安全法律义务的限定、中澳法律差别在这场争论中的影响以及澳大利亚陷入偏见的可能路径等。

一、国家安全法律义务的宪法基础

(一)我国国家安全法律义务的宪法定位

我国宪法第 5 条规定："一切法律、行政法规和地方性法规都不得同宪法相抵触"。很多法律第 1 条均会规定"依据宪法，制定本法"。国家安全立法也不例外，比如《国家情报法》《国家安全法》《反恐怖主义法》《反间谍法》等均有这一规定。该规定表明：国家安全法律的原则、制度与规定等都必须符合宪法，如果规定含义不明，也需要依据宪法来进行解释。

我国国家安全法律确实都规定了个人与组织的国家安全法律义务，但这些条款大多比较简单、原则，因此容易成为攻击的对象。比如，《国家情报法》第 7 条、〔3〕第 12 条、〔4〕第 14 条〔5〕等均成为澳大利亚等国宣称中国企业承担的国家安全法律义务包括协助情报机关从事间谍活动的依据。〔6〕但是，这种攻击最大的错误在于忽视了国家安全法律的宪法基础，忽视了中国宪法对于义务的最基本定性。

纵观全球，宪法是否规定公民义务在各国的情况都不一样，也经历过变化。早期的一些成文宪法国家，如美国、瑞士、挪威等，在其宪法中并没有义务性规定。〔7〕法国大革命时期，有人主张在《人权宣言》中纳入人民的义务，但没有被采纳。〔8〕大革命后制定的法国 1795 年宪

〔2〕"这样做不符合中国法律，也不是中国行事的方法，现在不会有，将来也决不会有"，http://lianghui.huanqiu.com/2019/exclusive/2019-03/14549818.html? agt=15417，最后访问日期：2019 年 3 月 29 日。

〔3〕"任何组织和公民都应当依法支持、协助和配合国家情报工作，保守所知悉的国家情报工作秘密"。

〔4〕"国家情报工作机构可以按照国家有关规定，与有关个人和组织建立合作关系，委托开展相关工作"。

〔5〕"国家情报工作机构依法开展情报工作，可以要求有关机关、组织和公民提供必要的支持、协助和配合"。

〔6〕"中国的情报法提供了可以强迫华为协助国家情报活动的能力。国家情报法第 7 条使组织和个人有义务支持、协助和配合情报工作"；"在一种极端情况下，华为可能会被要求在其设备中植入'后门'，允许中国政府通过该后门进行间谍或破坏活动"。Tom Uren, "The technical reasons why Huawei is too great a 5G risk", 14 June, 2018. https://www.aspi.org.au/opinion/technical-reasons-why-huawei-too-great-5g-risk，最后访问日期：2019 年 3 月 20 日。该文作者是澳大利亚战略政策研究所(ASPI)国际网络政策中心高级分析师，该研究所由澳大利亚政府于 2001 年成立，由国防部部分出资，为澳大利亚战略和国防的独立智库。

〔7〕李勇："公民宪法义务与相关概念的关系"，《北方法学》2011 年第 2 期，第 114 页。

〔8〕王世杰、钱端升：《比较宪法》，商务印书馆 1999 年版，第 147 页。

法规定了个体对社会的义务，包括维护祖国、捍卫国家等基本义务。1919年的德国魏玛宪法更直接以“基本权利和基本义务”作为第二部分的标题，强调随着国家赋予公民以权利，公民对国家也负有责任，包括效忠国家、拥护政府、服兵役等基本义务。由于国家安危存亡，事关每个公民的利益，故早期许多国家宪法都明确规定公民保卫国家或服兵役的义务。其与公民的纳税义务一样，早已成为各国宪法的通例。〔9〕尽管二战以后发达国家的宪法几乎都不再规定公民的宪法义务，〔10〕但这并不意味着公民宪法义务的消失。〔11〕

我国从《共同纲领》〔12〕开始就规定公民的宪法义务，后来的四部宪法均以专章对公民的宪法权利与义务加以规定，并不断丰富。因此，规定公民义务是中国宪法的一个基本特点。〔13〕现行宪法第二章专门规定公民的基本权利和义务，明确全体公民都享有宪法和法律规定的权利，同时也必须履行宪法和法律规定的义务。宪法明确规定的义务包括：劳动的权利和义务、受教育的权利和义务、实行计划生育、抚养教育未成年子女、赡养扶助父母、遵守宪法和法律、保守国家秘密、爱护公共财产、遵守劳动纪律、遵守公共秩序、尊重社会公德、维护国家统一和全国各民族团结、维护祖国的安全、荣誉和利益、依照法律服兵役和参加民兵组织、依照法律纳税，等等。公民的国家安全宪法义务集中体现在宪法第54条，即“中华人民共和国公民有维护祖国的安全、荣誉和利益的义务，不得有危害祖国的安全、荣誉和利益的行为”。在非常短的一个条文中，两次出现“祖国的安全、荣誉和利益”，并不是同义反复、可有可无，而是有非常深刻的宪法内涵。从文本上解读，本条规定明显包含两层不同的意思。后半句指的是公民的积极（不作为）义务，不得有任何危害祖国安全、荣誉和利益的行为，义务边界清晰，规范的对象是公民本身，公民是守法对象；而前半句指的是公民需要承担消极义务，当第三人有危害祖国安全、荣誉和利益的情形时，挺身而出，承担维护国家安全、荣誉和利益的义务，公民是宪法规定的主体，是作为国家主人在承担保卫国家的义务。可见，公民的积极义务与消极义务分别体现在两个半句中，主客体关系、义务主体、义务性质、义务边界等均有不同，逻辑关系非常清晰。消极义务的发生，要以存在危害祖国安全、荣誉和利益的情形为前提，是对危害行为的回应，因此属于防御性、消极性义务，不是攻击性、积极性义务。简言之，作为国家的主人，公民要与危害国家安全、荣誉和利益的行为做坚决斗争。最为典型的消极义务，当然是对内协助执法、有效打击犯罪行为，对外抵御侵略、维护国家安全。但不论对内还是对外，消极义务都属于典型的防御性义务，这也是各国宪法或法律的通行规定。绝大部分

〔9〕 李步云主编：《宪法比较研究》，韦伯文化国际出版有限公司2004年版，第580页。

〔10〕 对德国宪法不再规定宪法义务并不代表义务观念消失的分析，参见王锴：“为公民基本义务辩护——基于德国学说的梳理”，《政治与法律》2015年第10期，第117页。

〔11〕 王晖：“法律中的团结观与基本义务”，《清华法学》2015年第3期，第9页。

〔12〕 “中华人民共和国国民均有保卫祖国、遵守法律、遵守劳动纪律、爱护公共财产、应征公役兵役和缴纳赋税的义务。”

〔13〕 有学者认为，“广泛地引入具有一定道义性质的义务类型，是我国宪法有关基本义务规定的一个重要的规范特征”。林来梵：“论宪法义务”，《人大法律评论》2000年卷第2辑，第156页。

国家的宪法或法律都规定公民有服兵役、保卫国家以及针对违法犯罪行为承担作证或者协助打击犯罪的义务。〔14〕根据宪法第 54 条，每个公民都是国家安全、荣誉和利益的维护者、保卫者、防御者，都负有维护国家安全的义务，都要与各种形式的危害国家安全的行为作斗争。但是，该条规定的积极义务的边界是非常清楚的，并没有要求公民承担攻击其他主体（国家）的任何积极性义务。

因此，我国宪法对于防御性、消极性义务的明确规定，既符合各国通例，也与我国一直奉行的防御性国防政策、军事战略、核武器政策等一脉相承。中国在一系列文件中反复阐明奉行“独立自主的和平外交政策和防御性国防政策”。〔15〕“中国的国家利益、社会制度、对外政策和历史文化传统，决定中国必然实行防御性的国防政策。”〔16〕早在 1964 年，中国第一颗原子弹爆炸之后，中国政府就立即宣布中国发展核武器纯粹是防御性的，不首先使用核武器，不对无核国家使用核武器，不扩散核武器，主张世界上拥有核武器的国家全面彻底销毁核武器。这种原则一直坚持到现在。中国政府明确声明：“从拥有核武器的第一天起，中国就承诺无条件不对无核武器国家和无核武器区使用或威胁使用核武器”。〔17〕中国是世界上唯一一个承诺不首先使用核武器的国家，这体现了防御性国防政策的根本特点。解读中国的国家安全宪法义务，不能不看到这个根本性的立国特点。

王世杰、钱端升先生很早即指出：宪法中的权利义务规定“足以昭示未来的立法者以立法的方针，未来的行政者与司法者以行使行政权与司法权的轨范”。〔18〕国家安全法律将宪法规定的维护国家安全义务具体化为“支持、协助和配合”的义务，尽管比较原则，但仍然必须要以存在危害国家安全的行为为前提，并未改变宪法消极性、防御性义务的性质。所以，既不能将宪法上明确规定的消极性义务曲解为主动攻击性义务，更不能因为中国宪法与法律对于维护国家安全防御性义务的规定，就想当然地推论得出所有中国公民和组织都可能会成为其他主体（国家）攻击者的荒谬推论。如果这么推论，所有规定服兵役义务国家的公民都可能被视为潜在的侵略者，这显然是不正确的。正如有学者比较研究各国情况后所指出的，“设定义务的法律既须以法律形式为之，亦不得逾越宪法界限”。〔19〕中国宪法对于国家安全义务性质的明确界定，功能上类似于美国宪法第一修正案对于国会言论自由立法的边界的明确限定，其他立法均不能与之冲突或者抵触。〔20〕

〔14〕 根据荷兰学者马尔赛文的统计，世界上 1946－1955 年间 14 部宪法中有 78.6％规定了服兵役的义务，92.9％规定了服从宪法的义务。参见（荷）亨克·范·马尔赛文、格尔·范·德·唐：《成文宪法——通过计算机进行的比较研究》，陈云生译，北京大学出版社 2007 年版，第 192－193 页。

〔15〕 国务院新闻办公室：《中国的军事战略》（2015 年 5 月）。

〔16〕 国务院新闻办公室：《中国的国防》（1998 年 7 月）。

〔17〕 国务院新闻办公室：《中国的军控、裁军与防扩散努力》（2005 年 9 月）。

〔18〕 王世杰等，见前注〔8〕，第 67 页。

〔19〕 郑贤君：“基本义务的宪法界限：法律保留之适用”，《长白学刊》2014 年第 3 期，第 71 页。

〔20〕 由此可见，个别学者主张将宪法义务从宪法文本中清除出去的观点，显然是错误的。参见张千帆：“宪法不应该规定什么”，《华东政法大学学报》2005 年第 2 期，第 26 页。

抛开我国宪法谈国家安全法律义务，存在明显的前提错误。

进一步分析可以发现，针对宪法就（消极性）义务的规定，相关法律进行了具体落实。1979年《刑事诉讼法》第80条、1996年《刑事诉讼法》第110条、2012年《刑事诉讼法》第135条均对公民的协助义务进行了细化，规定任何单位和个人有义务按照人民检察院和公安机关的要求，交出可以证明犯罪嫌疑人有罪或者无罪的物证、书证、视听资料等证据。〔21〕在2013年棱镜门事件揭示出美国国安局大规模监控国外信息之后，面对非常严峻的安全形势，2014年4月15日，习近平总书记在主持召开中央国家安全委员会第一次会议时提出，坚持总体国家安全观，走出一条中国特色国家安全道路，并系统提出“11种安全”。为此，中国进行了较为系统的国家安全立法，先后制定了《反间谍法》（2014年）、《反恐怖主义法》（2015年）、《国家安全法》（2015年）、《网络安全法》（2016年）、《境外非政府组织境内活动管理法》（2016年）、《国家情报法》（2017年）、《核安全法》（2017年）等。〔22〕这些立法带有明显的回应性、防御性特点，目的都是为了维护国家安全，防范各种现实风险与挑战，制度设计方面也有高度的一致性。可以看到，不同法律对于单位和个人的执法配合义务都进行了明确，其立法意图都是一致的，都是基于维护国家安全的需要，以应对、化解国家安全危险为前提，将宪法义务法律化。〔23〕从这个角度看，诸如《网络安全法》第28条对网络运营者以及《反恐怖主义法》第18条对电信业务经营者、互联网服务提供者之执法协助义务的规定等，都是《宪法》《刑事诉讼法》上协助义务的衔接性规定以及在网络领域的具体化，并没有创设任何新的义务，尤其是没有创设所谓的攻击性义务或者要求企业从事间谍活动的义务。如果回到《网络安全法（草案）》第23条的表述，〔24〕就更能明确这种执法协助义务的性质与《刑事诉讼法》相互衔接的特点。

一个非常明显的现象是：这些法律义务规定，因为符合各国的通行做法，过去几十年一直没有受到过西方国家的指责。但是，随着中国国力增强，近年来，我国国家安全法律的制定或者修改突然都会成为集中攻击的目标。最为典型的个案，当属西方国家对我国《反间谍法》第13条的无理攻击，认为该条会让中国企业有义务应中国国家情报机关的

〔21〕 另外，根据一九八三年九月二日第六届全国人民代表大会常务委员会第二次会议通过的《全国人民代表大会常务委员会关于国家安全机关行使公安机关的侦查、拘留、预审和执行逮捕的职权的决定》，“国家安全机关，承担原由公安机关主管的间谍、特务案件的侦查工作，是国家公安机关的性质，因而国家安全机关可以行使宪法和法律规定的公安机关的侦查、拘留、预审和执行逮捕的职权”。

〔22〕 系统国家安全立法的情况，参见迟玉琢、马海群：“国家情报工作制度的基本构建逻辑”，《情报资料工作》2019年第1期，第24页。

〔23〕 例如，《反恐怖主义法》第9条规定，“任何单位和个人都有协助、配合有关部门开展反恐怖主义工作的义务，发现恐怖活动嫌疑或者恐怖活动嫌疑人员的，应当及时向公安机关或者有关部门报告”；《反间谍法》第21条规定，“公民和组织发现间谍行为，应当及时向国家安全机关报告”；《国家安全法》第11条规定，“中华人民共和国公民、一切国家机关和武装力量、各政党和各人民团体、企业事业组织和其他社会组织，都有维护国家安全的责任和义务”。

〔24〕 “为国家安全和侦查犯罪的需要，侦查机关依照法律规定，可以要求网络运营者提供必要的支持与协助。”

要求，允许利用其系统进行对其他国家不利的行为。〔25〕实际上，早在 1993 年，中国就制定了《国家安全法》，并在 1994 年制定实施细则，2015 年才将该法名称调整为《反间谍法》。《反间谍法》第 13 条的内容在原《国家安全法》《国家安全法实施细则》中已经存在，基本表述与内容几乎完全一致或基本相同，法律名称变化后只进行了个别文字调整和条文合并，立法技术更为简练，并增加了“依照规定”以及与《行政强制法》保持一致这样一些更能反映我国法治政府建设进步的控权性规定。然而，这样一条已经在中国法律、行政法规中存在二十多年、通过修订更为规范的规定，突然被西方国家曲解和妖魔化，这显然无法在中国法律规定本身找到任何根据。因此，有理由推断西方国家极有可能是根据自己的宪法制度与情报法律制度来猜测性地推导中国法律。这里以澳大利亚为例进行说明。

（二）澳大利亚宪法制度的特殊性

澳大利亚宪法制度独具特点，普遍认为其形成受到英国议会制度（威斯敏斯特）与美国联邦制度（华盛顿）两种不同宪法制度与法律传统的影响，〔26〕被认为是“华盛敏斯特”变种。〔27〕一方面，英国的议会至上原则在宪法中得到明确肯定，表明联邦和州议会可以通过任何想制定的法律，宪法与普通法的关系并不是那么明确、刚性；另一方面，美国的联邦制、三权分立原则与违宪审查制度等也得到确认，由澳大利亚高等法院（联邦最高法院）最终确定联邦议会通过的法律是否在联邦立法权范围内。〔28〕

同时，澳大利亚宪法既没有规定公民的宪法义务，也没有像多数国家宪法那样明确

〔25〕 美国众议院常设情报委员会在 2012 年的专门调查报告中最早提出中国国家安全法会让中国企业有义务从事间谍活动问题，随后不断被包括澳大利亚在内的其他方面援引作为依据。然而，通读该报告，上述结论缺乏任何法律分析，只是在脚注中简单援引中国国家安全法第 11 条作为理由。其实，第 11 条是有关行政检查的规定，“查验”是检查主体与检查对象双方之间的法律关系。稍微了解一点中国行政法知识就应该知道，行政检查与第三方执法配合义务没有任何关系，该条也未授权国家安全机关让检查对象承担执法配合义务，对第三方进行监控或者从事其他不利于第三方的行为。反间谍法真正涉及到公民或组织承担执法配合义务的条款应该是诸如第 4、19、20、21、22 条。可见，该委员会在援引中国法律条文上存在多重逻辑错误，不但对第 11 条做断章取义式解释，还对不同条款张冠李戴，武断援引。并且，该委员会的表述也非常不严谨，用非常主观的“看起来”作为整个判断的基础，极其不负责任。“看起来（It appears）中兴和华为有义务根据中国政府的任何要求允许中国政府使用或访问它们的系统用于国家安全伪装下的恶意目的”。House Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 3 (2012).

〔26〕 英美两种宪法传统及其对澳大利亚影响的具体分析，可见如，R. D. Lumb, “Fundamental law and the processes of constitutional change”, in Alice Erh－Soon Tay and Eugene Kamenka (eds), *LAW－MAKING IN AUSTRALIA*, Edward Arnold (Australia) Pty. Ltd. 1980, p. 77.

〔27〕 Patrick Keyzer, Christopher Goff, Asaf Fisher, *PRINCIPLES OF AUSTRALIAN CONSTITUTION*, LexisNexis Butterworths, Australia, 2017, p. 1.

〔28〕 Ibid., p. 11.

规定公民的权利，〔29〕或者像英国、加拿大、新西兰等国那样有一部具有宪法地位的人权法案，〔30〕导致其议会立法缺乏宪法上的刚性制约标准，〔31〕其违宪审查实践远远落后于美国、英国、加拿大、新西兰等国。〔32〕尽管有澳大利亚学者主张其宪法存在“隐含的人权法案”或对国家权力的宪法（原则）限制，但对于是否存在这种宪法授权（限制）以及究竟哪种权力受到宪法（原则）限制，存在很多不同看法，且不同解释都缺乏宪法文本支持，宣布某项具体法律违反宪法更难。〔33〕

由此，在议会至上且缺乏人权法案的宪法框架下，澳大利亚宪法以及宪法的（司法）实施机制对议会立法的制约自然就会滞后甚至缺位。尤其是澳大利亚情报领域的议会立法，如同后文将要阐述的，长期以来受宪法与法律制约更少，情报部门自由裁量空间极大，甚至可以法外行事。基于善意可以合理推论，习惯了这样的宪法制度和情报法律运作方式，当看到中国国家安全法律义务的一般性、原则性条款表述后，澳大利亚方面一些人很有可能会基于本能反应，以己度人，推定中国国家安全法律义务与澳大利亚的情报法律一样，不受任何宪法制约，包括从事各种攻击性活动的义务。

澳大利亚以中国国家安全法律规定为由禁止中国企业参与其5G网络建设，源于对中国宪法与法律的关系缺乏基本了解。脱离中国宪法文本对中国国家安全法律义务进行定性，得出简单的推论，既是对中国宪法具有最高法律地位这一宪法至上原则缺乏最基本的了解和尊重，〔34〕也忽视了两国宪法文本与制度的巨大差别，陷入到偏见之中。就澳大利亚法律而言，超出保卫国家安全范畴，强制第三方承担攻击性情报协助义务的宪法与法理依据何在，是无法回答的问题，亦根本无法从各国宪法实践中找到任何根据。从这种对比中，也可以进一步加深对我国宪法制度的认识，在推进合宪性审查工作中进一步让宪法权利和义务条款活起来、用起来、强起来，在宪法文本的基础上提供更加丰富

〔29〕 根据荷兰学者马尔赛文的统计，世界上1788－1975年间142部宪法中有85.9％规定了宪法与普通法的关系，90.1％规定了公民权利。马尔赛文，见前注〔14〕，第188－189页。

〔30〕 澳大利亚宪法对基本权利的保护仅仅局限于商务领域的“州际贸易自由”，其他领域均缺乏任何明确规定。James Crawford, *AUSTRALIAN COURTS OF LAW*, 3rd. ed. Oxford University Press, 1993, p. 197.

〔31〕 “很多国家宪法性的权利法案可以制约国会立法的内容，但澳大利亚联邦缺乏这样的立法，只有首都地区以及维多利亚州有法律明确承认立法不得超越特定的人权”。D. C. Pearce, R. S. Geddes, *STATUTORY INTERPRETATION IN AUSTRALIA*, LexisNexis Butterworths, 2014, 8th ed. p. 210.

〔32〕 具体对比分析可见，H. P. Lee, “A Federal Human Rights Act and the Reshaping of Australian Constitutional Law”, *University of New South Wales Law Journal*, Vol. 33, Issue 1, 2010, p. 88.

〔33〕 George Winterton, “Extra－Constitutional Notions in Australian Constitutional Law”, *Federal Law Review*, Vol. 16, Issue 3, September 1986, p. 223.

〔34〕 尽管中国宪法对宪法义务的规定有自己的特点，但就宪法的最高法律地位以及宪法与法律的相互关系而言，中国宪法与其他国家的宪法又没有本质的差别。澳大利亚学者通过对澳大利亚宪法实施实践的梳理，也承认对于比较宪法，既要看到不同国家的相同点，又要看到历史和制度环境的不同点，只有这样才能进行有意义的比较。Nicholas Aroney, “Comparative Law in Australian Constitutional Jurisprudence”, *University of Queensland Law Journal*, Vol. 26, Issue 2, 2007, p. 317.

的中国宪法实践。

二、国家安全法律义务的法律定位

(一)我国国家安全法律规定的是防御性执法配合义务

澳大利亚等国经常根据我国国家安全法律的某一条或几条原则性规定,无限加以放大,进而推论中国企业具有应情报机关要求从事间谍活动的义务。这种推论从多方面看都是不正确的。

首先,各国法律条文的解读都应当是一个整体,原则性规定必须放到整部法律中进行理解,否则会断章取义,得出不正确的结论。按照中国立法惯例,每部法律的第一章是总则,尤其第 1、2 条对于立法目的、依据与适用范围等的界定,是理解、适用整部法律的基础。比如,《国家情报法》第 1 条既明确了其制定依据是宪法,也明确了立法目的是维护国家安全和利益。《国家情报法》第 2 条更进一步具体明确了立法目的是为了"防范和化解危害国家安全的风险""维护国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益"。这一防御性的立法目的在第 11 条中表述得更为清晰,即国家情报工作涉及的情报属于"危害中华人民共和国国家安全和利益行为的相关情报",而不是一般情报。"任何组织和公民"的情报配合义务要以存在危害中国国家安全和利益的行为为前提,配合义务的履行是为了"防范、制止和惩治上述行为"。结合《国家情报法》第 1、2、11 条来理解第 7、12、14 条规定的任何组织和公民"支持、协助和配合"等义务,显然是消极性、防御性的配合义务,是针对危害中国国家安全行为的防御性义务,以存在危害中国国家安全的行为为启动条件,与宪法规定的维护国家安全义务完全一致。任何组织和公民承担的既不是一般义务,也不是无条件义务,更不是攻击性义务。中国企业在境外参与建设的 5G 网络等对中国国家安全并不构成危害,认为中国企业有义务应中国国家情报机关要求在其海外设备中植入"后门",或者以其他形式帮助中国国家情报机关监听或破坏他国的通信网络,实际上是认为中国企业需要无条件承担攻击性的一般义务,这是对《国家情报法》第 7、12、14 条的断章取义式理解,不符合该法的原意与立法目的。同理,《反恐怖主义法》第 18 条适用目的只能是为了"防范、调查恐怖活动",不是进行一般意义上的情报收集活动,不能被用于与反恐怖主义无关的目的,包括在境外从事不利于其他国家的行为。对此,国家安全法律均明确规定了"国家情报工作机构及其工作人员应当严格依法办事,不得超越职权、滥用职权,不得侵犯公民和组织的合法权益"。

其次,对于法律中原则性规定的解读,应根据立法说明等历史线索,进一步明确立法目的与意图。包括《国家情报法》在内的中国国家安全法律的防御性立法意图,在立法说明中可以得到进一步的证明。国家安全部部长陈文清代表国务院做的《关于〈中华人民共和国国家情报法(草案)〉的说明》对国家情报机关的职权进行了明确限定,"国家情报工作机构应当依法搜集、处理境外机构、组织、个人实施或者指使、资助他人实施,或者境内机构、组织、个人与境外

机构、组织、个人相勾结实施的危害中华人民共和国国家安全、利益的相关信息。国家情报工作机构应当为防范、制止和惩治境外机构、组织、个人在中国境内实施的危害我国国家安全、利益的行为提供情报参考或依据”。根据该立法说明,国家情报机关的职权范围(以及任何组织和公民的配合义务)受到三个方面的限定:①行为上必须有实施危害中国国家安全、利益的行为;②主体上必须是境外机构、组织、个人或者与境外机构、组织、个人相勾结的境内机构、组织、个人;③目的上是为防范、制止和惩治危害中国国家安全、利益的行为提供情报参考和依据。可见,制定国家情报法,是基于防御性的立法目的,并据此界定国家情报机关的职责范围和执法配合义务。《国家情报法》并未授权或者规定国家情报机关开展攻击性的情报活动,也没有授权国家情报机关可以要求任何组织和公民从事攻击其他国家的情报活动。中国企业在中国境外参与建设的通信网络对中国国家安全并不构成危害,从立法目的解释,中国国家情报机关不能根据《国家情报法》要求中国企业在其设备中植入“后门”,或者以其他形式帮助中国国家情报机关监听或破坏他国的通信网络。

再次,在全球互联互通的大背景下,原则性法律条款的解读应该充分考虑比较法与其他国家立法的普遍经验与做法。中国近年来的国家安全立法,普遍吸收、借鉴了国际社会尤其是发达国家的立法经验,并被立法者明确承认。〔35〕全国人大常委会法工委副主任郎胜所作的《关于〈中华人民共和国反恐怖主义法(草案)〉的说明》指出,该法的起草“同时还研究借鉴国外的有关立法经验”。近年来,国际社会越来越重视打击恐怖主义,欧盟、美国等国际组织和国家出于反恐怖主义工作需要,均通过立法强化网络运营商和服务商的执法协助义务。关于提供技术接口,欧盟、美国、德国、英国、荷兰、俄罗斯、日本、新西兰等国际组织和国家均有类似规定。例如,《布达佩斯网络犯罪公约》第20条第1款(“通讯数据实时收集”)规定:各缔约国应当采取必要的立法或者其他措施,授权主管机关在其管辖范围内采用技术手段收集和记录通过计算机系统传输的与特定通信相关的通信数据;授权主管机关强制服务提供者在主管机关采用技术手段收集、记录相关通信数据时提供配合与协作,以保证其技术上的可行性。公约第21条第1款(“内容数据截获”),针对主管机关采用技术手段收集和记录内容数据以及服务提供者的配合、协作义务方面,也作了类似的规定。1995年1月17日欧盟理事会通过的《合法截获电信决议》附录第三项规定:网络运营/服务商必须提供一个或者多个接口,以确保截获的通信以指定的格式通过特定的连接装置传输至执法监控设备。美国《1968年综合犯罪控制与安全街道法》第三章规定了犯罪侦查中的合法截获手段利用。〔36〕美国《1994年通信协助执法法》(CALEA)要求电信运营商(以及宽带服务商、VOIP)必须履行通信截获的执

〔35〕 比如,全国人大常委会法制工作委员会副主任郎胜在第十二届全国人民代表大会常务委员会第十五次会议上所作的《关于〈中华人民共和国网络安全法(草案)〉的说明》中明确承认草案起草“注意借鉴有关国家的经验,主要制度与国外通行做法是一致的”。

〔36〕 See, 1968 Omnibus Crime Control and Safe Streets Act, Title III.

法配合义务，第 103(a)条（“对提供协助的能力要求”）规定，电信运营商应当确保其设备、设施或者服务能够实施下列行为：根据法院命令或者其他的合法授权，迅速对某类通信进行隔离并且使政府能够对其实施监听；迅速对某类通信隔离并且使政府能够获取可用的呼叫识别信息；向政府发送监听到的通信以及能够确定身份的电话信息。关于解密义务，美国、欧盟、澳大利亚、法国、荷兰、新西兰等国家和地区也均对电信业务经营者、互联网服务提供者等提出了明确要求。例如，美国《1994 年通信协助执法法》第 103(b)(3)条规定，电信运营商为客户或者用户提供加密服务且掌握解密所需的必要信息的，负有解密或者协助政府解密的责任。欧盟理事会 1995 年《合法截获电信决议》附录第 3.3 项规定，如果网络运营/服务商对通信信息进行编码、压缩或者加密，执法机关有权要求网络运营/服务商提供被监控的通信的明文。英国《2000 年规制调查权力法》第三部分是对加密保护的电子数据的调查规定，指出如果情报部门、警察、海关合法掌握加密数据并且解密是由于国家安全、防止犯罪或是侦查需要，或是为了英国经济的良好发展，或是国家法定权力和职责合理有效履行之必需，且解密是唯一合理可行的手段，在有理由相信被要求解密的人掌握加密信息的密钥的情况下，可以书面形式要求这些人自己解密，在特殊情况下会要求他们提供解密密钥，但不要求他们提供仅用来作为电子签名的密钥。澳大利亚《2001 年网络犯罪法》附件 2（“电子储存数据相关执法权”）在《1914 年犯罪法》第 3L 条后加入了 3LA（“有计算机或计算机系统知识的人协助获取等”），规定执行官员可以请求治安法官发布解密命令，不执行解密命令的，监禁六个月。可见，类似于中国《反恐怖主义法》第十八条的关于电信业务经营者和互联网服务提供者向公安机关、国家安全机关防范、调查恐怖活动提供技术支持和协助的规定，在国际上是通行的，属于典型的执法配合义务。认为中国情报机关会利用类似规定要求中国企业在境外从事不利于外国利益的行为，是一种典型的双重标准，缺乏任何法理上的支持。

最后，中国国家安全法律规定的配合义务主体均是境内的电信业务经营者、互联网服务提供者、网络运营者或者其他公民与组织，不适用于中国境外的主体。中国企业在海外承担项目，进行网络建设，都会成立相应的当地法人，这些主体均不属于中国国家安全法律适用的对象，根本不存在执法配合义务的适用前提。

（二）澳大利亚国家安全法律义务包括主动攻击性义务

澳大利亚的情报机关从第一次世界大战开始就得到重视，〔37〕用于维护法律以及对付反战人士和澳大利亚共产党。〔38〕第二次世界大战中，作为同盟国成员，澳大利亚国防信号局（2013 年后改名为澳大利亚信号局）对美军信号情报局截获苏联通讯活动的维诺那计划提供

〔37〕 详细的介绍可见，*Royal Commission on Intelligence and Security Seventh Report — Australian Intelligence / Security Services* 1900—1950 by Jacqueline Templeton Volume I, p. 1, (Copy No. 25).

〔38〕 See, e.g., Frank Cain, “Australian Intelligence Organizations and the Law: A Brief History”, *University of New South Wales Law Journal*, Vol. 27, Issue 1, 2004, p. 296.

了协助，发挥了重要的作用。〔39〕二战结束之后，世界马上进入冷战，美国、英国、加拿大、澳大利亚、新西兰五国组成信号情报交换联盟——五眼联盟。根据秘密协议，澳大利亚国防信号局的任务就是监听北亚、中国、印尼等地区的通讯联络，一直带有非常鲜明的主动性、攻击性色彩。〔40〕这些情报机关的一些重大项目或活动，包括维诺那计划在内，长期处于保密状态，不仅一般公众不知情，即使美国、澳大利亚等国的政府领导人很长时期也不知情。〔41〕这导致的后果之一是情报活动的滥用，监控对象从国外延伸到国内。

1972 年水门事件曝光以后，美国相继制定《隐私权法》《阳光下的政府法》《外国情报监控法》，并修改《信息自由法》，既严格规范在美国国内进行的情报活动，保护美国公民的权利，也一定程度上开始规范针对外国的情报监控活动。〔42〕但是，美国官方一直等到冷战结束后的 1997 年，才由根据《1994－1995 财年对外关系授权法》特设的保护与减少政府秘密委员会，正式对外承认维诺那计划等保密项目，并提出改革情报工作监督的一系列建议。〔43〕随后，主要发达国家普遍出现了一轮减少政府秘密、推动信息公开、加强对情报活动立法控制的浪潮。然而，2001 年发生的 911 事件，又重新改变了西方国家立法与情报监控走势。五眼联盟以反恐和国家安全为由，普遍加大了监听的力度与范围，将很多企业与个人纳入监听对象。〔44〕美国 2001 年通过的《爱国者法》第二章集中规定了“强化监控程序”方面的内容，授权政府机构可以为了调查外国情报与国际反恐目的获取第三方“商业记录”和其他有形载体，尤其第 215 条授权联邦调查局可以大规模秘密地从电信服务提供商、互联网服务提供商等组织或个人处获取信息。〔45〕这导致后来斯诺登事件所反映的美国国家安全局超出国家安全范围、无节制大量

〔39〕维诺那计划的具体情况介绍，可见（美）约翰·厄尔·海因斯、哈维·克莱尔：《维诺那计划——前苏联间谍解密》，吴妍妍、吴锡林译，群众出版社 2004 年版，第一章。

〔40〕Frank Cain, supra note 38, p. 306.

〔41〕有学者因此称这些情报机关为地下帝国。Geoffrey de Q. Walker, “Underground Empire: Intelligence Agencies and the Rule of Law”, *Federal Law Review*, Vol. 20, Issue 2, 1991, p. 293.

〔42〕具体情况参见：Peter P. Swire, “The System of Foreign Intelligence Surveillance Law”, *George Washington Law Review*, Vol. 72, Issue 6, August 2004, p. 1306.

〔43〕The Commission on Protecting and Reducing Government Secrecy, *REPORT of the COMMISSION ON PROTECTING AND REDUCING GOVERNMENT SECRECY*, LX, A－2 (1997).

〔44〕澳大利亚国会 2003 年通过了该国立法史上争议最大立法之一的《2003 澳大利亚安全情报局立法修正（恐怖主义）法》，赋予该局各种超常规特别权力。具体分析与批评参见：Lisa Burton; Nicola McGarrity; George Williams, “The Extraordinary Questioning and Detention Powers of the Australian Security Intelligence Organisation”, *Melbourne University Law Review*, Vol. 36, Issue 2, 2012, p. 415.

〔45〕对美国 1978 年《外国情报监控法》制定及适用演变的介绍，以及 2001 年《爱国者法》对适用目的的扩大化修订分析，参见：William Funk, “Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma － A History”, *Lewis & Clark Law Review*, Vol. 11, Issue 4, Winter 2007, p. 1099.

使用第三方数据监控外国人与侵犯本国公民权利之现象。〔46〕斯诺登披露的秘密资料同时也揭示了澳大利亚信号局监听包括印尼总统在内的印尼重要人物通讯的事实。〔47〕

澳大利亚情报法律的变化充分体现了上述国际趋势。2000 年之前，尤其是冷战结束之前，澳大利亚、加拿大、美国、英国等五眼联盟情报相关的法律规定都比较分散，也很简略，情报工作受到的法律限制很少。〔48〕2000 年前后，这几个国家普遍出现了情报工作法律化的现象，法律规定更为细致，体现了要加强对情报活动法律控制的意图。〔49〕澳大利亚《2001 年情报服务法》作为澳大利亚情报活动的最基本立法，就是其中的表征。

该法缘起于上世纪九十年代中期围绕澳大利亚秘密情报局发生的一场争议。澳大利亚秘密情报局相当于英国的军情六处，设立于 1952 年（澳大利亚政府 1977 年才公开承认机构的存在），负责秘密从事外国情报收集工作。1993 年，因为前任探员的爆料，秘密情报局成为社会关注的焦点，被媒体指控为经常法外行事、越权收集澳大利亚公民的材料等。为此，澳大利亚决定对秘密情报局进行司法调查，并任命了专门的调查委员会。尽管调查委员会的最终结论认为秘密情报局并非处在监督体系之外，但仍然提出了加强控制和责任以及提高内部组织和管理等系统性改革建议。其中的关键建议之一是通过国会立法，既为秘密情报局提供法律基础，又加强国会监督。〔50〕基于这份建议，形成了该法草案，并由时任外交部长于 2001 年 6 月 27 日提交给国会，同年 9 月 29 日通过，10 月 29 日开始实施，随后又根据形势变化经历了很多次修正。该法体现了澳大利亚加强对情报活动控制的精神，引入了三项主要的改革：①为澳大利亚秘密情报局和澳大利亚信号局提供了国会立法依据，改变了两机构过去依据部门委任立法运行的状况，由此使该法成为情报活动的基本法律；②扩充了澳大利亚安全情报局、秘密情报局和澳大利亚信号局的权力，也加强了各自的内部管理和控制，包括司法部长与内设总法律顾问的控制；③设立了统一监督安全情报局、秘密情报局和澳大利亚信号局的国会联席委员会，以代替过去分别设立的安全情报局国会联席委员会（1988 年设立）和情报服务联席委员

〔46〕 See, e.g., *LIBERTY AND SECURITY IN A CHANGING WORLD: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 20 (12 December 2013). 其他发达国家的类似趋势，can see, e.g., Christian Schaller, "Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law after Snowden", *German Law Journal*, Vol. 19, Issue 4, July 2018, p. 941.

〔47〕 Ewen MacAskill & Lenore Taylor, "Australia's spy agencies targeted Indonesian president's mobile phone", *THE GUARDIAN* (U.K.) (Nov. 17, 2013), https://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone，最后访问日期：2019 年 4 月 11 日。

〔48〕 比如，根据美国 1947 年《国家安全法》，美国总统 1981 年发布的《12333 号行政命令》第 2.7 条授权执法机关可以与私营企业（以及学术机构）依合同方式进行合作，授权范围非常广泛。

〔49〕 See, e.g., Ashley S. Deeks, "Confronting and Adapting: Intelligence Agencies and International Law", *Virginia Law Review*, Vol. 102, Issue 3, May 2016, p. 623.

〔50〕 Commission of Inquiry into the Australian Secret Intelligence Service, *Report on the Australian Secret Intelligence Service* (Public Edition), March 1995, p. 195.

会,以加强国会监督。2005 年,该委员会更名为国会情报与安全联席委员会。

对于第三方主体的执法协助义务,该法规定非常隐秘,也十分简略,但从其中仍然可以看到第三方必须承担相关义务的法律规定。比如,根据该法第 7(1)条,澳大利亚信号局负责境外信号情报收集(以及网络信息安全),可以与合同服务提供者签订协议,由后者提供服务。根据该法 38C 和 38D 条款的授权,信号局既可以聘用合同服务提供者协助履职,也可以借调其雇员到澳大利亚境内外的其他组织工作一定时间。从中可以看出,该法通过非常简单的一般性条款,明确了各种第三方合同服务提供者的协助义务。至于协助义务的范围和形式等,则完全由具体的合同条款确定,这当然会包括协助从事攻击性的情报活动。由此,该法规定的合同制度等于为情报协助工作撑起了一把巨大的保护伞。

进入后冷战时代,随着信息技术的发展,国际关系格局发生深刻变化,各国普遍要求进一步增强国家安全机关的权力。2013 年,澳大利亚国会情报与安全委员会发布完善澳大利亚国家安全法律的报告,其中一个重要目标是实现业界协助义务的现代化。〔51〕 随后,澳大利亚稳步推进一系列立法与修法工作,完善第三方对于执法机关与情报机关的协助义务。2015 年,澳大利亚国会不顾来自各方面的反对,通过了《1979 电信(截获与获取)法》修正案,强制要求互联网服务提供商与电信运营商留存用户元数据二年,包括用户姓名、位置、电话号码、电子邮件详细情况、短信、使用的社交媒体和网址、设备地址、接收方的通讯情况以及其他数据,供至少 21 个政府机关使用。

2018 年 12 月,澳大利亚通过了充满争议的《电信与其他立法修正(协助与获取)法》(以下简称为"协助与获取法"),对包括电信法、刑法典、行政决定(司法审查)法、独立国家安全立法监督法、电信(截获与获取)法、澳大利亚安全情报局法、监控设备法、海关法等在内的众多法律进行一揽子修正,进一步对情报机关以及执法机关获取"指定的通讯提供者"的加密通讯信息与数据进行了广泛的立法授权,系统强化了第三方的执法协助义务。

根据该法,为获取特定使用者的加密信息与数据,情报机关以及执法机关可以通过采用下述三种方式之一要求第三方提供执法协助:①技术协助请求(TAR)。这些属于自愿性质的请求,由澳大利亚安全情报局(ASIO)局长,澳大利亚秘密情报局(ASIS)局长,澳大利亚信号局局长,或者包括澳大利亚联邦警察(AFP)、澳大利亚犯罪委员会(ACC)以及州和领地警察等"截获机关"首席长官签发,可以绕过强制性通知的监督规定,请求获取指定的通讯提供者的通讯与数据,并由通讯提供者自愿决定是否提供协助;②技术协助通知(TAN)。这些属于强制性通知,只能由澳大利亚安全情报局(ASIO)局长或者截获机关首席长官签发,要求指定的通讯提供者使用现有的截获或者解密能力,提供获取通讯信息的渠道;③技术能力通知(TCN)。这些属于强制性通知,要求指定的通讯提供者建设基础设施,以满足后续的技术协助通知的要

〔51〕 Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 2013, p. 49.

求。技术能力通知只能由澳大利亚安全情报局(ASIO)局长或者截获机关首席长官提出请求,由司法部长经通讯部长同意后签发,以书面方式送达通讯提供者,并留出 28 天的提出异议机会。签发请求或通知的机关还可以与指定的通讯提供者签订合同,明确提供者提供协助的具体义务。

第三方的协助义务既可以是行为,也可以是物,范围非常广泛。根据修改后的《电信法》第 317E 条的规定,清单中的权力主要包括:①撤除一种或者多种由第三方使用或者代为使用的电子防护措施;②提供技术信息;③安装、维护、测试或者使用软件或设备;④保证以特定格式提供根据令状或授权获取的信息;⑤协助或者促成执行令状或授权、协助或者促成有效接收令状或授权相关的信息;⑥促成或者协助获取第三方合法活动的客体,包括设施、用户设备、数据处理装置、标明的传输服务、提供标明的传输服务衍生或附属的服务、电子服务、提供电子服务衍生或附属的服务、用于或可能用于与标明的传输服务相关的软件、用于或可能用于与电子服务相关的软件、可以安装在已经或者可能与电信网络互联的计算机或其他设备上的软件;⑦协助测试、修改、开发或维护某种技术或能力;⑧通知第三方合法活动的特定变化或有影响的发展,只要这种变化与执行令状或授权相关;⑨修改或促成修改第三方所提供服务的任何特征;⑩以第三方或者另一个第三方所提供的服务来替换或促成替换第三方所提供的服务。需要注意的是,权力清单只适用于强制权力。如果情报机关或执法机关行使的是非强制性的权力(技术协助请求),则根本不受权力清单的任何限制。

协助与获取法对于协助义务的适用范围规定也非常广,既包括维护澳大利亚的国家安全、外交关系、经济利益,也包括协助打击(最高刑期三年以上有期徒刑)严重的澳大利亚国内犯罪以及协助打击外国刑法规定的严重犯罪,还包括协助维护与电子信息存储与传输相关的信息的安全性和完整性,其范围远远超出我国国家安全法律对于国家安全法律义务适用条件的限制性规定。因此,第三方的协助义务既包括防御性协助义务,必然也包括攻击性协助义务。〔52〕第三方秘密履行协助义务后,必须对整个过程保密,不得泄露任何消息。同时,第三方执行技术协助通知或技术能力通知的行为获得法律责任豁免,免于承担任何民事责任。

协助与获取法对于承担协助义务的"指定的通讯提供者"的范围界定同样非常广,明确列举的义务主体包括十五大类,如电信运营商、传输服务商、传输服务中间商、一个或多个终端用户在澳大利亚的电子服务提供商(及其辅助服务商)、研发、提供或者更新用于或可能用于提供传输服务或电子服务的软件商、制造、提供、安装、维护或者运行设施的主体、为设施制造或者提供部件的主体、将设施与电信网络连接的主体、制造或者提供在澳大利亚使用或者可能在澳

〔52〕 代表用户数字权利的国际非政府组织"现在公开"对适用范围规定的可能滥用进行了全面的分析。Access Now, Comments to the Department of Home Affairs, 7 (10 Sep, 2018), https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/the-assistance-and-access-bill-2018, 最后访问日期:2019 年 5 月 6 日。该网站汇集了所有对法案的反馈意见,除另行注明,后面介绍的立法意见均可在该网站查到。

大利亚使用的用户设备的主体、制造或者提供在澳大利亚使用或者可能在澳大利亚使用的用户设备的部件的主体、安装或者维护在澳大利亚用户设备的主体、制造、提供、安装或维护数据处理设备的企业等。同时,该法规定执法机关可以直接接触这些第三方组织中的个人,如工程师或者信息技术管理员,而不是必须首先经过该组织本身。批评者普遍认为,该法所规定的"指定的通讯提供者"可以包括向澳大利亚的任何人提供任何类型的在线服务或者通讯设备的任何人,而根据法律要求开设的"后门"可能会被罪犯或其他恶意当事方钻漏洞,危害所有用户的隐私和安全。〔53〕

为平息各界的批评,防止执法协助活动导致信息系统风险增大或者弱化对其他一般用户的保护,该法对请求与通知所要求的内容进行了一定的限制。根据该法规定,情报机关与执法机关不得要求指定的通讯提供者以电子保护的形式实施或者建设系统弱点或系统脆弱性,包括开发新的解密能力,降低系统认证或加密的有效性,或可能对任何其他人(非特定目标对象)所拥有的任何信息的安全造成危害以及可能导致未经授权的第三人可以获得安全信息等。然而,这些限制性条款并不能真正消解包括脸书、苹果、谷歌等企业在内的全球信息产业界的忧虑。〔54〕尽管澳大利亚政府极力否认,但业界与消费者团体普遍认为,协助与获取法为强制企业安装"后门"提供了法律依据,澳大利亚由此成为世界上第一个如此立法的国家。〔55〕

协助与获取法还明确规定执法与情报机关可以要求提供者在外国履行通知要求的配合义务。根据修订后的《电信法》317ZB(5)的规定,如果提供者证明在国外履行通知要求的配合义务会违反外国法律,也只能作为免除其民事(罚款)责任的抗辩理由,无法免除其他责任。对此,澳大利亚律师委员会提出了强烈的批评,认为这样规定会使很多需要报告守法情况的组织面临各种信誉与金融风险,不是真正的避风港。〔56〕这样的规定,实际上是迫使各种组织在国

〔53〕 Brian P. Bartish, "Controversial Australian Encryption Act Denounced by Privacy and Cryptography Advocates", https://www.dataprivacymonitor.com/international－privacy－law/controversial－australian－encryption－act－denounced－by－privacy－and－cryptography－advocates/,最后访问日期:2019 年 5 月 30 日。

〔54〕 代表全球软件行业的软件联盟在其立法后评论建议中指出,法律目前对于"系统弱点"和"系统脆弱性"的界定过于模糊、宽泛,应进一步明确其含义,并澄清技术能力通知不会被用来制造技术弱点。The Software Alliance, "RIVIEW OF THE TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACESS) ACT 2018－BAS COMMENTS", 5 (12 Feb., 2019).

〔55〕 Lily Hay Newman, AUSTRALIA'S ENCRYPTION－BUSTING LAW COULD IMPACT GLOBAL PRIVACY, Dec. 07, 2018. https://www.wired.com/story/australia－encryption－law－global－impact/,最后访问日期:2019 年 4 月 24 日。The Australian Communications Consumer Action Network, Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 4 (2018). http://accan.org.au/our－work/submissions,最后访问日期:2019 年 5 月 5 日。

〔56〕 Law Council of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill* 2018: Parliamentary Joint Committee on Intelligence and Security, 8 (18 October 2018). https://www.lawcouncil.asn.au/resources/submissions/telecommunications－and－other－legislation－amendment－assistance－and－access－bill－2018,最后访问日期:2019 年 5 月 3 日。

外更为积极地履行通知要求的配合义务。

协助与获取法还规定了双边执法配合义务,即外国政府也可以要求提供者履行配合义务。根据修改后的《电信法》,只要外国法律规定的是最高三年以上有期徒刑的严重犯罪,就可以签发技术协助请求或者上述两种不同类型的通知,要求提供者协助执行外国生效的刑法,这等于为五眼联盟之间的协助渠道打开了方便之门。在五眼联盟之间,因为地缘优势,澳大利亚负责截获源自亚洲的电子情报并与其他几个成员共享,相互之间存在各种持续的合作机制。〔57〕另外,如果外国政府要求司法部长安排获取存储在计算机中的数据,司法部长可以授权相关执法官员根据《2004 年监听设备法》27A 的规定,针对违反外国法律、最高可能判处三年以上有期徒刑的刑事违法行为的调查或者调查程序,申请获取计算机(内容)的令状。

如果说《2001 年情报服务法》还只是原则性、隐秘地规定了第三方的执法协助义务,那么协助与获取法则全面、系统地架构了第三方协助义务的整体框架,赋予不同情报机关与执法机关向众多第三方提出请求或通知的制度。因此,该法自草案颁布之后,就在澳大利亚国内外引发广泛批评。〔58〕澳大利亚人权委员会是根据联邦议会立法于 1986 年设立的独立法定组织,通过司法部长向联邦国会报告。该委员会就协助与获取法向国会提交报告,历数该法的五大主要弊端:①签发技术协助通知和技术能力通知缺乏司法授权要求,只要满足相关的行政程序即可签发,不能有效制约权力滥用;②为避免产生"系统弱点"和"系统脆弱性"而对协助请求或通知的限制过于模糊,难以发挥制约作用;③可以提出协助要求的"相关立法目的"范围过广;④该法附件五授予澳大利亚安全情报局强制协助权力的范围过广;⑤该法附件二、附件五规定的"掩盖曾经秘密获取过信息的事实"的权力范围过广。〔59〕

(三)简单的比较结论

通过上述比较分析可以合理推断,澳大利亚完全可能是以自己的情报收集与配合收集法律规则来套用中国情况,认为中国情报机关可能会根据国家安全法律来要求中国企业协助进行情报收集工作。但是,中国国家安全法律与澳大利亚情报法律有如下几个重大的差别:①澳大利亚情报机关从事的是(军事)情报收集工作,背景是五眼联盟之间的最初秘密协议,本身带有保密性、全面性和主动性。相反,中国国家安全法律是为维护国家安全的立法,是为了防范

〔57〕 Ashley Deeks, "Intelligence Communities, Peer Constraints, and the Law", *Harvard National Security Journal*, Vol. 7, Issue 1, 2015, p. 8.

〔58〕 联合国促进与保护观点与表达自由权特别报告人也专门针对草案公开发布了系统批评性的评论意见,包括强迫制造"后门"问题。Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 (REFERENCE: OL AUS 5/2018).

〔59〕 Australian Human Rights Commission, Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Submission 56), 2 (22 February 2019). https://www.humanrights.gov.au/our-work/legal/submission/telecommunications-and-other-legislation-amendment-assistance-and-0,最后访问日期:2019 年 5 月 6 日。

和化解危害国家安全的各种现实风险，打击恐怖主义等各种违法犯罪活动的立法，属于防御性立法，不是为（军事）情报收集工作提供依据。两国立法目的、立法时机与制度初衷等完全不同；②澳大利亚情报立法明确授权其情报机关从事境外情报收集活动，并非常笼统地规定了情报机关与第三方之间的合作机制，情报机关与协助从事情报活动的第三方收集的显然不只局限于维护国家安全的防御性情报。相反，如前所述，中国国家安全法律规定的都只是针对危害中国国家安全的防御性协助义务，是宪法义务的法律具体体现；③澳大利亚《2001 年情报服务法》与协助与获取法既没有像某些澳大利亚法律那样规定有“前言”或“立法目的”，可以帮助明确具体条款的含义，〔60〕也没有类似于中国法律中“总则”类的限制性规定。〔61〕 因此，其情报收集的范围要远远大于中国《国家情报法》总则所规定的“为防范、制止和惩治危害中国国家安全、利益的行为提供情报”之范围。必须看到，中国与澳大利亚两国政治制度、法律制度存在多方面重大差别，不能因为澳大利亚情报法律规定了覆盖范围广泛的情报收集与配合情报收集制度就简单推断、怀疑中国立法也规定了同样的制度；④就立法技术而言，澳大利亚情报法律不论是在实体规则部分还是后面将要看到的法律责任部分，均比我国国家安全法律要严格、严密得多，被普遍认为在世界上赋予了政府机关前所未有的权力去干预技术公司的运行。〔62〕要求第三方在海外承担攻击性情报协助义务的场景在澳大利亚法律中能够得到充分的实现，而在我国国家安全法律中既无这一立法意图，也无法找到相应的法律依据和威慑保障。

三、违反国家安全法律义务法律责任的比较

无责任追究，施加义务则毫无意义。从哪些行为会被追究法律责任，也能从末端倒推国家安全法律义务的性质与边界。

对于会被追究法律责任的违法行为类型，我国国家安全法律规定的两个特点非常突出，正好能够再次证明本文前面的基本论点。首先，受到西方国家指责最多的（承担间谍活动协助义务）一般性条款，如《国家情报法》第 7、12、14 条，《国家安全法》第 77 条，《反间谍法》第 20 条等，在法律责任中均缺乏对应条文。也就是说，不履行这些一般性协助义务不会产生任何不利法律后果。其次，国家安全法律追究法律责任的义务均是具体列明的具体执法配合义务，不是一般性义务，这再次体现了国家安全法律义务防御性、消极性的特点。

〔60〕 对于澳大利亚法律中“前言”与“立法目的”作用的分析，可见如，D・J・Gifford, Kenneth H・Gifford, *HOW TO UNDERSTAND AN ACT OF PARLIAMENT*, 8th. Ed. 1994. The Law Book Company Limited., Chapter 10, Chapter 11.

〔61〕 协助与获取法正文仅仅只有短短的三条，分别规定法律名称、不同修正的生效日期与附件法律地位，然后就是大篇幅的具体修改其他法律条文的五个附件。

〔62〕 StartupAUS, Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018, 1 (12 February 2019). https://startupaus.org/advocacy/submissions/，最后访问日期：2019 年 5 月 21 日。

而且国家安全法律规定的法律责任均限于行政法律责任,力度普遍较轻,一般是有限的罚款,情节严重的情况下才可能涉及到行政拘留。例如,《反恐怖主义法》第 82 条规定:“明知他人有恐怖活动犯罪、极端主义犯罪行为,窝藏、包庇,情节轻微,尚不构成犯罪的,或者在司法机关向其调查有关情况、收集有关证据时,拒绝提供的,由公安机关处十日以上十五日以下拘留,可以并处一万元以下罚款”。第 84 条规定:电信业务经营者、互联网服务提供者未依照规定为公安机关、国家安全机关依法进行防范、调查恐怖活动提供技术接口和解密等技术支持和协助的,由主管部门处二十万元以上五十万元以下罚款,并对其直接负责的主管人员和其他直接责任人员处十万元以下罚款;情节严重的,处五十万元以上罚款,并对其直接负责的主管人员和其他直接责任人员,处十万元以上五十万元以下罚款,可以由公安机关对其直接负责的主管人员和其他直接责任人员,处五日以上十五日以下拘留。第 91 条规定:拒不配合有关部门开展反恐怖主义安全防范、情报信息、调查、应对处置工作的,由主管部门处二千元以下罚款;造成严重后果的,处五日以上十五日以下拘留,可以并处一万元以下罚款。《反间谍法》第 29 条规定:“明知他人有间谍犯罪行为,在国家安全机关向其调查有关情况、收集有关证据时,拒绝提供的,由其所在单位或者上级主管部门予以处分,或者由国家安全机关处十五日以下行政拘留;构成犯罪的,依法追究刑事责任。”《网络安全法》第 69 条规定:网络运营者拒不向公安机关、国家安全机关提供技术支持和协助的,由有关主管部门责令改正;拒不改正或者情节严重的,处五万元以上五十万元以下罚款,对直接负责的主管人员和其他直接责任人员,处一万元以上十万元以下罚款。

另外,我国刑法没有不履行情报配合义务或国家安全法律义务而追究刑事责任的罪名或规定。刑法与情报相关的犯罪只有第 111 条规定的为境外窃取、刺探、收买、非法提供国家秘密、情报罪,不适用于不履行情报执法配合义务行为。刑法与国家安全工作相关的只有第 277 条规定的妨害公务罪第 4 款“故意阻碍国家安全机关、公安机关依法执行国家安全工作任务,未使用暴力、威胁方法,造成严重后果的,依照第 1 款的规定处罚”,这明显不包括不履行国家安全法律义务情形。换言之,在我国,违反国家安全法律规定的各种义务,均不会导致刑事责任。

对于不履行执法配合义务,包括证人不出庭作证,由于我国刑法至今都未规定任何法律责任,证人不出庭作证等现象长期无法解决。〔63〕 只有 2012 年修订后的《刑事诉讼法》第 193 条规定:经人民法院通知,证人没有正当理由不出庭作证的,人民法院可以强制其到庭,但是被告人的配偶、父母、子女除外。证人没有正当理由拒绝出庭或者出庭后拒绝作证的,予以训诫,情节严重的,经院长批准,处以十日以下的拘留。可见,我国消极性、防御性执法配合义务的履行,刑法一直都缺乏任何保障机制。

综合上述分析可以看到,遭到澳大利亚指责的我国国家安全法律一般性义务条款,实际只

〔63〕 可见如,潘新喆:“刑事证人拒不出庭作证原因探析”,《理论探索》2003 年第 1 期,第 76 页。

是一种倡导性宣示,并无相应的法律责任规定,更不可能产生迫使中国企业在境外从事间谍活动的后果。至于仅仅靠行政处罚支撑的具体执法配合义务,由于处罚力度有限,其实际执行功效也值得怀疑。指责中国通过国家安全法律强迫中国企业在海外从事间谍活动,显然故意扭曲和高估了中国法律的作用,是一种典型的借题发挥。

相反,澳大利亚对于法律责任的严厉规定,为执法机关留下了很大的执法空间,非常典型地体现出了与我国法律的差别。比如其《2001 年情报服务法》第 39 条之后的内容以极大篇幅规定对各种违法情形的制裁措施。其中的法律责任条款鲜明地体现出两个特点,正好与我国相反。一是以刑事制裁为主,以行政罚款为辅,威慑力度大;二是与我国国家安全法律对具体列举的违法情形予以处罚不同,澳大利亚的法律责任均围绕(包括合同方在内的)保密义务展开,即(合同方)任何人不得不当披露任何有关国家安全方面的信息,否则需要承担法律责任。由此,澳大利亚在实体法部分以非常简略的方式规定第三方的执法协助义务,在法律责任部分对执法协助的所有信息均作为保密信息加以保护,并以严厉的刑罚威慑使得履行协助义务的情况完全处于保密状态之中,形成完整的闭环。比如,第 40(1)(b)(ii)(iii)条规定,任何人只要泄露与澳大利亚信号局签署任何合同的信息,或者泄露是澳大利亚信号局合同方雇员、代理人的任何信息,均构成犯罪,监禁十年;第 40G 条规定,任何人只要违反与澳大利亚信号局签订的合同规定,复印、抄写、保留、移除或者以其他方式处理因为合同而获得的信号局的记录,构成犯罪,监禁三年。

协助与获取法同样系统规定了协助义务人的不同刑事法律责任和行政处罚(罚款)责任,并全面强化了追究责任的力度。修订后的《1997 年电信法》第 317ZF 条规定,指定的通讯提供者、指定的通讯提供者的雇员、指定的通讯提供者的合同服务提供方,或者指定的通讯提供者的合同服务提供方的雇员等,未经授权泄露任何与技术协助请求、技术协助通知、技术能力通知相关的任何信息的,均构成犯罪,监禁五年。通过刑事责任,澳大利亚使整个情报协助活动完全处于保密状态。对于第三方不履行配合义务的,附件三、附件四通过修改法律,对于知道密码而不开启设备的人扩展了最高刑的刑期,《犯罪法》规定可处二年到五年监禁,严重的可监禁十年,《海关法》则规定可处六个月到五年监禁,严重的可监禁十年。《1997 年电信法》第 317ZB 条规定:电信运营商、传输服务商以及其他指定的通讯提供者只要能够履行技术协助通知或技术能力通知的要求,就必须履行。电信运营商、传输服务商每次不履行义务,最高罚款 1 千万澳元;电信运营商、传输服务商之外的其他服务提供者,公司每次不履行义务罚款最高 1 千万澳元,个人最高罚款 5 万澳元。另外,经协助与获取法附件二修订的《2004 年监控设备法》第 64A(8)条规定:对于法官或行政上诉裁判所成员签发的获取计算机内容的令状,有义务协助获取的人如果不执行命令的,构成犯罪,处监禁十年,还可以并处 600 计算单位的罚金。

因此,从法律责任角度进行比较分析,再一次证明中澳两国法律对于执法协助义务的不同处理,揭示两国法律的根本性差别。澳大利亚对中国法律的解读不但不符合中国法律的实际,

也无意中将自己的各种做法大白于天下。〔64〕事实上，随着信息全球化进程的不断加深，更为理性、健康的做法应当是在理解和尊重他国法律制度的基础上，求同存异，积极寻求最大公约数，以促进合作。澳大利亚上述“以小人之心度君子之腹”的做法，既曲解了中国法律，也无益于国际合作。

Abstract: Based on comprehensive analysis of Chinese Constitution and national security laws, this article argues that the legal obligations of individuals and entities under China's national security laws are in essence reactive and defensive, i.e., they shall undertake responsibility to safeguard the country when national security is threatened. In contrast, Australian intelligence activities and intelligence laws have always been offensive, by their nature, due to special international circumstances after the World War II. Moreover, with its unique characteristics, the Australian Constitution allows its intelligence laws to impose both reactive/defensive obligations and proactive/offensive obligations. Therefore, looking at general or principal clauses in Chinese national security laws, the Australia observers would misinterpret them based on its own experiences, claiming that these stipulations would force Chinese companies to conduct offensive espionage activities. This is completely groundless.

Key Words: National Security Laws; Constitutional Obligations; Reactive Obligation; Intelligence Activity

（学术编辑：彭 錞）
（技术编辑：马 超）

〔64〕 澳大利亚信息产业协会在对协助与获取法草案评论时指出，“草案不仅仅只是对付犯罪分子，它把全体澳大利亚人置于危险之中”。实际上，通过比较分析可以看到，澳大利亚情报法律是把全世界人民置于危险之中。The Australian Information Industry Association, Submission to the Parliamentary Joint Committee On Intelligence and Security (PJCIS) on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 2 (Oct., 2018). https://aiia.com.au/__data/assets/pdf_file/0009/91395/AIIA－response－to－the－PJCIS－into－the－Assistance－and－Acess－Bill－12－October－2018.pdf，最后访问日期：2019 年 5 月 26 日。