DOI：10.13317/j.cnki.jdskxb.2021.39

# 国际组织遭受网络攻击后的刑事管辖权研究

初北平，薛天赐

摘　要：近年来国际组织遭受网络攻击的现象愈发严重，国际组织“信息电子化”后也对“总部协议”中的刑事管辖权具有重要影响。对于东道国而言，按照现有“总部协议”中的管辖权安排，当攻击者位于领土之外时可能存在管辖权真空。对于成员国而言，当攻击者对国际组织基本职能产生严重影响时，将阻碍成员国的对外合作，侵犯成员国的国家利益，成员国应当有权依据保护性原则主张域外刑事管辖权。为了保障国际组织运营及其成员国权益，“总部协议”中的刑事管辖权规则应当进一步完善。

关键词：网络攻击；国际组织；刑事管辖权；总部协议

基金项目：国家社会科学基金重大项目(17ZDA145)

作者简介：初北平，大连海事大学法学院教授、博士生导师，法学博士，从事海商法、仲裁法、保险法研究；薛天赐，大连海事大学法学院博士研究生，从事海商法、国际法研究。

中图分类号：D993.9　　文章编号：1671－6604(2021)04－072－18

文献标识码：A　　开放科学(资源服务)标识码(OSID)：

国际组织①创建初期，在东道国“安全保障义务”下极少发生专门针对国际组织的刑事案件。但国际组织开始“信息电子化”进程后，由于网络自身的脆弱性、非对称性、隐蔽性等特点，网络攻击也转向国际组织，严重侵害国际组织的信息与信息系统，影响国际组织的日常工作，破坏成员国间相互合作的成果。网络犯罪对传统刑事管辖权提出挑战，应当重新审视国际组织管辖权安排的合理性，保障东道国与成员国的基本利益。

## 一、国际组织遭受网络攻击的管辖权迷雾

### （一）总部协议中现有的管辖权安排

管辖权是一种主权权利，是指：“描述一个国家或其他管理当局或机构的法律

① 本文所述的“国际组织”为政府间组织(IGO)，并不包括非政府间组织(NGO)。

权限的术语"①。而管辖则认为:"国家可以合法采取行动管制人或财产的范围,即国家可以界定与执行以及管制自然人与法人的合法权力。"②国际组织是国际法中的主体之一,由于国际组织不具有领土,因此国际组织本身并不享有管辖权,不能干涉本质上属于成员国国内管辖的事务。为了更好地实现组织职能,国际组织会设有常设机构并与东道国签订"总部协议"(Headquarters Agreement),其中包括国际组织与东道国之间的管辖权安排③。如果国际组织的特权与东道国的法律法规发生冲突,国际组织的特权将优先适用。国际法院认为国际组织享有法人地位④,从社会契约的角度,国际组织具有行政管理者与国际合同主体的双重身份⑤。对成员国而言,国际组织是行政管理者,享有条约缔结权,有权与其他国家缔结条约并享有一定的特权与豁免权。国际组织作为行政管理者,其管理范围应当仅限于国际组织的内部,因此有权制订内部的管理规则。为防止常设机构遭到不法侵害,东道国给予国际组织常设机构与外国使领馆相同的保护水平,在特殊情况下,如有关消防、卫生等事项不受特权约束。例如在1947年联合国驻纽约办事处与美国政府签订的"总部协议"中明确约定⑥,联合国可以授权和管理其总部,美国联邦、州和地方法院有权管辖联合国总部发生的行为和交易,并适用美国的相关法律,除非《联合国宪章》和"总部协议"中另有约定。《联合国宪章》和"总部协议"中的约定与美国法律法规相冲突的时候,以前者优先,但是,有关消防方面的法律法规除外。

在立法管辖权中,东道国享有常设机构所在地的立法管辖权,由于国际组织本身并不享有主权,因此不能对常设机构所在地行使立法权。国际组织特权来源于两个部分,分别是组织章程和管理规则。前者是成员国为国际组织实现部分职能而达成的协议,后者是保障国际组织日常运营而制定的管理性文件,两者均不是东道国的法律法规。在司法管辖权中,东道国通常对常设机构发生的行为和交易具有管辖权,并以东道国的法律法规为基础,国际组织的相关规则为例外。在法律适用方面,当组织章程、管理规则与东道国法律法规相冲突时,国际组织的相关规则具有优先性,并在司法审判中予以考虑。在执行管辖权中,未经国际组织许可,东道国不得擅自进入,除非涉及火灾或其他约定的情况,否则必须获得常设机构主要

① HAMID A G. Public international law: a practical approach[M]. Kuala Lumpur: Thomson Reuters-Sweet & Maxweel, 2019:141.

② 邱宏达. 现代国际法[M]. 台北:三民书局,2015:671.

③ ENEMO I P, OGWEZZY C M. The necessity of headquarters agreement under the law of international organisations[J]. International journal of advanced legal studies and governance, 2015, 5(1):20-21.

④ ICJ. Rep. 174[R]. 1949:16.

⑤ PARRY C. The Treaty-Making power of the United States[J]. British year book of international law, 1949(26):109.

⑥ Section 7& 8, "Agreement Between the United Nations and The United States of America Regarding the Headquarters of The United Nations" (No. 147).

负责人的许可,而常设机构也要向东道国保证不会成为避难所。

(二)网络攻击的本质是网络犯罪

在20世纪90年代家庭电脑全面普及之后,黑客攻击成为计算机犯罪的首要问题,并从个人受益转向威胁国家安全①。此时的网络犯罪被认为是从属于计算机犯罪,而网络攻击也被认为是计算机犯罪的一部分,《网络犯罪公约》与《打击信息技术犯罪的阿拉伯公约》都没有明确"网络攻击"的定义。在《网络犯罪公约》中,网络攻击属于对计算机系统和数据安全进行威胁和攻击的行为,公约并没有对此进行单独分类。在《打击信息技术犯罪的阿拉伯公约》中,虽然对网络犯罪做了全面扩张,但由于该公约采用犯罪结果地标准,作为犯罪行为的网络攻击并非该公约所关注的内容,同样没有对网络攻击做明确的定义。

网络攻击通常适用于三个领域:第一个是网络战中的网络攻击。国际组织可以成为网络战中的客体,但是由于国际组织本身并不享有主权,当国际组织遭受网络攻击时,不能以侵犯主权为由采取救济措施,即便达到低烈度的武装冲突程度,也是由东道国依据主权而采取反措施,国际组织本身并不能独立采取自卫权,因此不能适用网络战②。第二个是网络犯罪中的网络攻击。在网络犯罪中,网络攻击被认为是针对计算机信息系统,通过数字和网络技术相结合而实施的犯罪,包括非法访问信息系统,非法干扰信息系统,非法干扰数据库和非法拦截数据③。国际组织遭受的网络攻击主要是针对国际组织的信息和信息系统,因此以网络犯罪为主。第三个是网络恐怖主义中的网络攻击。网络恐怖主义作为恐怖主义在网络领域的延伸,包括为恐怖分子提供任何帮助④,是各国共同打击的严重暴力行为。网络恐怖主义的要素包括:关键基础设施、政治动机和在一般公众或特定人群的心中产生恐怖状态⑤。极端组织所发动的网络攻击通常不能令一般公众或特定人群产生恐怖状态,原因在于国际组织作为国家间的合作机制,需要实现成员国的部分职能,其所涵盖的信息通常为特定领域信息,具有一定的专业性而不具有普遍性。根据"《网络犯罪公约》关于通过计算机系统犯下的种族主义和仇外行为定为犯罪的附加议定书"的规定,特定人群是指以种族、肤色、血统、民族或宗教信仰划分的群体,具有一定的政治性,与具有专业性的特定人群

① NICHOLSON K J. International computer crime: a global village under siege[J]. New England international and comparative law annual, 1996(2):40-41.

② 迈克尔·施密特.网络行动国际法塔林手册2.0版[M].黄志雄,等,译.北京:社会科学文献出版社,2017:183.

③ IGLEZAKIS I. The legal regulation of cyber attacks[M]. Rijn: Kluwer Law International BV, 2020: 15-16.

④ RAMESOVA K. Public provocation to commit a terrorist offence: balancing between the liberties and the security[J]. Masaryk university journal of law and technology, 2020, 14(1):131.

⑤ CULAPA A L. Cyberattacks, cyberterrorism and cyber-use of force: countering the unconventional under international law[J]. Ateneo law journal, 2004, 48(4):1087-1099.

有所不同。但随着“外国恐怖主义作战人员”的不断增多,恐怖主义的适用范围也在不断扩张。根据欧盟“DIRECTIVE 2017/541/EU”和“DIRECTIVE 2013/40/EU”的规定,对国际组织系统与数据进行非法干扰的网络攻击行为,如果是为了威胁国际组织工作人员的人身安全,强迫国际组织执行或放弃某一行动,严重影响国际组织的基本职能将被视为“恐怖主义”。因此,当国际组织遭受网络攻击时将存在两种认知,一种认为是网络犯罪行为,另一种认为是恐怖主义行为。

2016年9月,世界反兴奋剂机构(WADA)称一组俄罗斯黑客非法进入“世界反兴奋剂机构的反兴奋剂管理系统(ADAMS)”,窃取与里约奥运会相关的机密级医疗数据,并在网上发布,对世界反兴奋剂机构造成严重影响①。在2020年全球新冠肺炎大流行期间,世界卫生组织约450个有效的电子邮件地址和密码在网上遭到泄露,针对世界卫生组织工作人员的网络攻击事件激增,世界卫生组织遭受的网络攻击是平时的两倍②。与主权国家相比,国际组织并没有因为其特殊的国际法地位而免受网络攻击,反而因为在国际社会上具有较高的影响力,更加容易遭受网络攻击,有效治理针对国际组织的网络攻击问题已经刻不容缓。

(三)网络犯罪对传统刑事管辖权的改变

网络犯罪呈现出四个特点,分别是收益与成本之间的不对称性,违法行为发生地的隐秘性,行为地与结果地的跨国性,法律适用中的差异性。网络犯罪的这些特点导致网络犯罪在适用传统刑事管辖权原则时发生了激烈冲突,虚拟性的网络既弱化了其与领土之间的相互联系③,也不同于现实中的共享空间。网络是一个虚拟世界,不是一个自然界中存在的公共资源④。虽然各国在网络中存在共享空间,但是这个空间并不完全属于现实世界,不能将传统刑法中的管辖权规定直接适用于网络犯罪之中⑤。

在属地原则中,网络犯罪从“行为”和“结果”两个方面扩大适用范围,导致许多国家都可以主张管辖权。在属人原则中,网络犯罪的隐秘性将难以确定管辖权归

① WADA confirms attack by Russian cyber espionage group [EB/OL]. (2016-09-13) [2020-07-21]. https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group.

② Exclusive: elite hackers target WHO as coronavirus cyberattacks spike [EB/OL]. (2020-03-24) [2020-07-21]. https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN.

③ CASSIM F. Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study[J]. Potchefstroom electronic law journal, 2009, 12(4):38-42.

④ CHAPELLE B D L, FEHLINGER P. CHAPTER FIVE——Jurisdiction on The Internet: From Legal Arms Race to Transnational Cooperation[R]. A Universal Internet in a Bordered World: Research on Fragmentation, Openness and Interoperability. 2016:86.

⑤ ANZELMO E L. Cyberspace in international law: does the internet negate the relevance of territoriality in international law[J]. Studia diplomatica, 2005, 58(4):155.

属。在积极属人原则中,由于犯罪者隐匿真实身份,主张管辖权的国家可能并不真正享有管辖权,而真正享有管辖权的国家可能并未主张管辖权。在消极属人原则中,除网络恐怖主义外,网络犯罪通常不以国籍为标准实施犯罪,所侵犯的客体数量更多,同样陷入更加复杂的管辖权冲突之中。在保护性原则中,网络犯罪同样威胁着主权完整、国家安全与国家利益。法的滞后性与网络技术的超前性形成鲜明对比,需要确立保护性原则,扩张原有的保护性管辖范围。美国、马来西亚等国家已经确立保护性原则,防止网络犯罪侵害国家根本利益。在普遍性原则中,由于被国际法所认可的国际罪行较少,因此大多数网络犯罪并没有被视为国际罪行,包括网络恐怖主义行为,但这并不妨碍个别国家可以主张普遍性管辖,例如德国和比利时对网络传播儿童色情行为主张普遍性管辖①。

因此,在制订涉及网络犯罪管辖权范围的规则时,各国并不统一,部分国家在制订管辖权规则中过度扩张,导致无法实现执行管辖。部分国家在制订管辖权规则中过度保守,导致管辖权存在真空,需要构建更加适宜的网络犯罪管辖权规则。对于国际组织而言,应当重新审视总部协议中的刑事管辖权规则,进一步思索网络犯罪在适用总部协议时所发生的改变。

## 二、"网络攻击"下的东道国管辖权分析

大多数总部协议签订时间较早,受当时认知能力与技术能力的限制,无法预测网络攻击对刑事管辖权的影响,各国普遍接受一个国家应当对其领土范围内的行为和结果具有管辖权②,因此总部协议中的刑事管辖权通常以"主观属地原则"为主。基于网络犯罪虚拟性的特点,网络攻击者存在地理位置不确定性,这种不确定性将影响东道国是否享有管辖权。

### (一) 攻击者位于常设机构所在地时适用总部协议

当攻击者位于常设机构所在地时,东道国可以主张总部协议中的刑事管辖权。首先,东道国的刑事管辖权仅限于发生在总部地区的行为,根据"主观属地原则"的规定,当网络攻击行为发生在总部地区时东道国应当享有管辖权。其次,东道国的执行管辖权受到严格限制。总部协议中通常约定,在常设机构所在地,未经国际组织允许,东道国不得随意进入③。当东道国执行网络犯罪管辖权时,也必须获得国际组织的许可。再次,东道国管辖权仅限于领土范围之内。常设机构所在地虽然享有特权,但并不视为东道国放弃的领土,因此东道国有权依照属地原则而主张管辖权。最后,严格解释限制东道国的权力扩张。常设机构所在地是领土中的特殊

① BRENNER S W, KOOPS B J. Approaches to cybercrime jurisdiction [J]. Journal of high technology law, 2004, 4(1):28.

② RYNGAERT C. Jurisdiction in international law[M]. Oxford: Oxford University Press, 2008:75.

③ ZOLLER E. The national security of the United States as the host state for the United Nations[J]. Pace yearbook of international law, 1989(1):135-137.

区域,在 Klinghoffer v. S. N. C 一案中[①],美国第二巡回法院认为,位于纽约的联合国总部所在地并不是真正意义上的美国领土,而是美国放弃控制权的中立场所。东道国不能主张常设机构所在地的全部主权,解释总部协议时应当采用严格解释[②],防止国际组织与东道国之间通过扩张性解释来影响彼此间的权力,总部协议只适用于常设机构所在地发生的网络攻击行为。

(二)攻击者位于领土范围之内时适用东道国属地原则

如果攻击者在东道国领土上发动针对国际组织的网络攻击,东道国应当享有管辖权。东道国所主张的刑事管辖权不是源于总部协议的约定,而是东道国刑事立法中的管辖权,这是东道国主权绝对性的体现,国际组织不得干涉。各国可以通过国内立法确定网络犯罪的范围,既可以将传统刑事犯罪延伸到网络领域,也可以单独划定网络犯罪的适用范围[③]。虽然东道国有权制订网络犯罪的管辖权规则,但是由于网络犯罪具有跨国性的特点,在制订网络犯罪管辖权时,应当适当参考现有的国际规则。

主权权利应当具有独立性和绝对性,主权独立性体现在两个方面,对外要求一个主权国家应当具有国际交往能力,对内要求一个主权国家对其范围内的人口和领土享有控制权。这种国家控制权就包括管辖,即一个国家依照相关法律法规,对其领土或公民的管理行为。主权绝对性体现为绝对权威,让·博丹在《共和六书》中阐述主权理论时认为,一家之主在管理家庭成员中具有绝对权威,通常为丈夫、父亲或奴隶主。而国家同家庭一样,国家的主权者也应当具有绝对权力,这种绝对权力不能扩张到上帝所制定的律法之中,主权者的绝对权力也要受制于其所做出的承诺,要受法律的约束。古典时期的格劳秀斯、孟德斯鸠认为主权也应当置于法律体系或宪法规则的范围之内,而在国际主权观念中,国王与国王之间的关系并不会存在阻碍,他们都应当遵守上帝律令和自然法则,即便上帝消失,其管辖依旧存在,并存在于高级法的形式之中[④]。因此,管辖权作为一种主权权利应当具有独立性与绝对性[⑤],并受法律法规的约束[⑥]。特别是在国际交往中,管辖权作为一种受限的权利,也应当受到国际公约或国际协定的约束。

---

① Klinghoffer v. S. N. C. Achille Lauro Ed Altri-Gestione Motonave Achille Lauro in Amministrazione Straordinaria, 937 F. 2d 44, 51 (2d Cir. 1991).

② SCHERMERS H G, BLOKKER N M. International institutional law: unity within diversity[M]. Boston: Koninklijke Brill NV, 2018:1075.

③ Report of the commonwealth working group of experts on cybercrime[R]. Commonwealth Law Bulletin, 2014, 40(3):517.

④ 篠田英朗. 重新审视主权——从古典理论到全球时代[M]. 戚渊,译. 北京:商务印书馆,2004:40.

⑤ Omar v. Geren, 689 F. Supp. 2d 1, 7 (D. D. C. 2009), aff'd sub nom. Omar v. McHugh, 646 F. 3d 13 (D. C. Cir. 2011); The Schooner Exch. v. McFaddon, 11 U. S. 116, 136, 3 L. Ed. 287 (1812)

⑥ JENSEN E T. Cyber sovereignty: the way ahead[J]. Texas international law journal, 2015, 50(2—3):283.

属地原则是现有网络犯罪公约中所承认的基本原则之一。涉及网络犯罪管辖权的国际公约有两个,分别是《网络犯罪公约》和《打击信息技术犯罪的阿拉伯公约》。《网络犯罪公约》确立了属地管辖和属人管辖,根据第22条规定,公约同时承认各国可以根据自身需求确立不同的管辖权规则,并采用国家协商的方式解决管辖权冲突问题。《网络犯罪公约》在全球网络犯罪问题上达成部分共识,属地原则已经被各成员国所接受,基本覆盖欧美大部分国家。《打击信息技术犯罪的阿拉伯公约》确立了属地管辖、属人管辖、保护性管辖以及管辖权冲突规则。根据公约第30条第3款的规定,当成员国发生管辖权冲突时,保护性管辖优先于属地管辖,属地管辖优先于属人管辖,属地管辖在中东地区也得到了广泛认可。在部分示范法中同样认同属地原则,如加勒比共同体的"网络犯罪/电子犯罪:示范政策指南和立法文本"、北约的《塔林手册2.0版》等。虽然网络犯罪的虚拟性扩大了属地原则的适用范围,但属地原则作为网络犯罪管辖权已经被大多数国家接受,当攻击者位于东道国领土范围之内时,东道国有权依据属地原则主张网络犯罪管辖权。

(三)攻击者位于领土范围之外时可能存在权利真空

如果攻击者在东道国领土范围之外发动网络攻击,攻击者若是东道国国民,东道国可以通过属人原则主张刑事管辖权。攻击者若不是东道国国民,则须采取其他原则主张管辖权,而属地原则是最为基础的原则①。由于总部协议中未确立"客观属地原则",因此东道国原则上不享有刑事管辖权。

攻击者在境外对国际组织实施网络攻击通常有四种目的,首先是强迫国际组织积极或消极实施某些行为,其次是阻碍国际组织实现基本职能,再次是具有某些政治诉求,最后是实现攻击者的个人利益。前三种针对国际组织实施的犯罪行为通常被视为恐怖主义行为,恐怖主义犯罪以政治或意识形态为主要目的,旨在影响公众舆论并最终改变国家体制②。例如《欧洲制止恐怖主义公约》第3条规定,如果强迫国际组织履行或不履行某些行为,或者严重破坏及阻碍国际组织的基本职能都将被视为恐怖主义犯罪。虽然总部协议具有优先性,但国际组织不应当对东道国的国家安全构成威胁,总部协议不应当侵害东道国的主权,因此总部协议要让位于国家安全。如果东道国给予国际组织的特权与东道国国家安全相冲突,也应当以国家安全为准。例如在1988年,亚西尔·阿拉法特先生受到联合国的邀请,

① 东道国虽然确立"被动人格原则",但国际组织的工作人员享有特殊的国际法地位,在履行国际组织职责时处于"中立地位",对国际组织的信息和系统进行的破坏行为,并不会威胁工作人员的个人安全,其损害结果只涉及国际组织,因此并不能适用"被动人格原则"。

② 在某些国家和地区(如印度尼西亚),实施恐怖主义的目的如果是基于政治目的则被视为政治犯罪,将生命财产所造成的严重破坏视为实现政治目标的一种手段。详见BORGERS M J. Framework Decision on Combating Terrorism: Two Questions on the Definition of Terrorist Offences. *New Journal of European Criminal Law*, 2012, 3(1):76-79。

但美国基于国家安全原因拒绝提供签证,认为其所参加的组织涉嫌发动针对美国的恐怖主义行为①。当网络攻击者基于政治诉求而对国际组织实施网络攻击时,将构成恐怖主义行为,严重威胁东道国的国家安全,东道国的国家安全将优先于总部协议,享有网络攻击管辖权。例如欧盟"Directive (EU) 2017/541"号指令第19条规定,如果犯罪行为是在另一个会员国的领土上发生的,那么任何会员国都可以扩大其管辖范围。

如果针对国际组织的网络攻击是实现攻击者的个人利益,没有对国际组织构成严重损害,则应当适用一般网络犯罪,不能适用于恐怖主义犯罪②,总部协议将具有优先性。由于总部协议并不包含客观属地原则,因此东道国并不享有管辖权。首先,总部协议中并不包括客观属地原则,解释总部协议通常采用严格解释,应当严格限定在主观属地原则范围之内。其次,客观属地原则将扩张东道国管辖权,如果东道国依据客观领土原则而享有管辖权,东道国管辖权将扩张至国际组织所有事务之中,干涉国际组织的日常事务,影响国际组织独立性。再次,东道国在常设机构所在地并不是绝对权威,常设机构所在地是东道国主权下的特殊区域,东道国在常设机构所在地上绝对权威受限,并让位于总部协议中的特权。最后,东道国无法实现管辖权。东道国的执行管辖权必须获得国际组织许可。东道国给予国际组织的是执行管辖权中的特权,东道国在电子取证过程中所涉及的电脑、服务器与数据库均处于国际组织的实际控制之下,同样享有东道国给予的特权,东道国不应实施执行管辖权。因此,当攻击者单纯为个人利益而对国际组织实施网络攻击时③,由于总部协议签订时间较早,刑事管辖权不能适用客观属地原则,可能存在管辖权真空的情况。

## 三、"网络攻击"下的成员国管辖权分析

国际组织作为国际合作机制,在成员国之间的权限划分过程中,如果涉及国际组织内部安全将视为共同权限,任何一个成员国均有权维护国际组织的合法利益;如果仅仅涉及成员国的国家安全,则该成员国将享有唯一责任④。因此当国际组织遭受网络攻击的时候,对内安全影响将导致东道国的专属管辖变为成员国的共

① Statement by the Legal Counsel concerning the determination by the Secretary of State of the United States of America on the visa application of Mr. Yasser Arafat[R]. A/C.6/43/7, 1988.

② MALISZEWSKA-NIENARTOWICZ J. A new chapter in the EU counterterrorism policy: the main changes introduced by the directive 2017/541 on combating terrorism[J]. Polish yearbook of international law, 2017(37):193.

③ 如在亚太地区港口国检查组织APCIS系统中,如果船东基于个人利益,阻碍访问系统,篡改相关数据,实现逃避检查的情况时,则属于上述所指的基于个人利益对国际组织实施网络犯罪的情况。

④ BIGNAMI F. EU law in populist times: crises and prospects[C]//Gilles de Kerchove, Christiane Höhn. The EU and international terrorism: promoting free movement of persons, the right to privacy and security. Cambridge: Cambridge University, 2020:277.

同管辖。

(一) 成员国享有网络主权

网络最初被视为"自由之地",各国不应当在网络空间中行使主权,网络应当作为去"主权化"的全球公域①。但随着网络犯罪等问题不断涌现,对网络空间进行治理势在必行,"网络主权"的概念由此产生并获得大多数国家的认同②,"网络主权"是现实空间主权在网络空间的延伸。

第一,主权内容随着时代的发展有所改变③。当让·博丹系统阐述主权理论后,直到签订"威斯特伐利亚和约"才确立了主权是一种平等权利。联合国成立后,《联合国宪章》第2条进一步丰富主权平等原则,包括对内完全自主,对外完全独立。在国际法治理念不断深入,科学技术不断进步的背景下,主权外延在《芝加哥公约》《南极条约》《外层空间条约》《联合国海洋法公约》中不断扩张,并应与社会发展相适应。而当全球进入"5G时代"后,主权也自然扩张到被誉为第五疆域的网络空间。"塔林手册2.0版"也认为,成员国基于领土原则对网络活动行使的主权权利具有正当性,不能因为成员国缔结的"组织宪章"早于主权与时代发展,就否认成员国在网络空间中享有主权权利。

第二,安全领域中的"网络主权"已经达成共识。虽然欧美发达国家与中俄等新兴国家在互联网治理中存在认识上的差异,但对于网络安全问题,各国都承认享有主权,并可以依据主权行使管辖权。俄罗斯在2019年通过了《俄罗斯互联网主权法案》,规定俄罗斯的互联网活动只能适用俄罗斯联邦法律,所有交换数据与过境数据及其所有者或持有者均受俄罗斯管辖,保障互联网中的公民宪法权利与国家安全,确保俄罗斯境内的互联网与公共通信网络的完整性、安全性与稳定性。我国《国家安全法》第25条规定:"国家建设网络与信息安全保障体系,提升网络与信息安全保护能力,加强网络和信息技术的创新研究和开发应用,实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控;加强网络管理,防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为,维护国家网络空间主权、安全和发展利益。"

第三,网络主权是国家利益的体现。各国对网络犯罪的认识和界定有所差异,希望在制订规则中维护自身利益④。美国、欧盟、俄罗斯和我国在各自的立法实践中存在一定的冲突与矛盾,网络主权概念由浪漫主义向现实主义过渡,各国开始积极主张网络主权。一方面在治理模式中对弈。美国在全球治理互联网问题上提出

① BARLOW J P. A Declaration of the Independence of Cyberspace[EB/OL]. (1996-02-08)[2021-01-31]. https://www.eff.org/cyberspace-independence.

② SCHMITT M N, VIHUL L. Respect for sovereignty in cyberspace[J]. Texas law review, 2017, 95(7): 1667-1668.

③ 程卫东. 网络主权否定论批判[J]. 欧洲研究, 2018, 36(5): 66.

④ 初北平. "一带一路"多元争端解决中心构建的当下与未来[J]. 中国法学, 2017(6): 72-90.

"多利益相关方模式",既要制衡利益相关方去除中央集权,确保每一个参与者的共同权利与责任,又与非政府组织"互联网名称与数字地址分配机构"(ICANN)关系密切,背离利益相关方的治理准则①。我国与俄罗斯在治理互联网的过程中更加青睐于政府间组织,既从国家主权的角度提升政府在治理中的权威性,又从中央集权的角度限制自由主义在网络领域中的无序发展,确保本国在网络空间中的国家利益②。另一方面是数据权属的相互掠夺。在云计算与大数据的时代,拥有和掌握数据开发、传播和控制的国家将获得网络空间的竞争优势③,各国基于自身利益,采用"数据存储地标准"或"数据控制者标准"。欧盟地区将数据保护作为一项基本权利,在"一般数据保护条例"(GDPR)中确立适用欧盟地区的所有自然人、所有数据操作以及所有个人数据④,建立具有保护管辖色彩的"最低限度的联系"原则并扩张条例适用范围⑤。美国则通过"存储通信法"(SCA)确立了对内数据管理,如果法院对法律程序进行修改或撤销,必须考虑到美国利益⑥。而"澄清海外合法使用数据法"(CLOUD Act)则授权执法机构获取美国公司控制的境外数据,但欧盟提出该法案与"一般数据保护条例"发生潜在冲突⑦。成员国的国家利益除了体现在网络治理与资源掠夺中,同样不能忽视在传统主权中的国家利益,特别是信息电子化后,可能涉及成员国的国家利益。

(二) 成员国基于国家利益受损而享有域外管辖权

组织章程中通常并不包括管辖权安排,成员国并不享有管辖权。国际组织遭受网络攻击被视为恐怖主义行为后,成员国的管辖规则从传统的主观属地原则和积极属人原则扩张到客观属地原则与消极属人原则,成员国应当享有域外管辖权。

第一,网络攻击侵犯了成员国的国家基本利益。主权国家有权对外开展交流与合作,国际合作是一个主权国家的固有权力,不应当受到任何形式的干扰和破坏。"美国国家利益委员会"在2000年发布的《美国国家利益报告》中将"国家利益"分为四个等级,将"对外合作维护国际体系"视为"至关重要"的国家利益之一,

① ZHANG X B, XU K. A study on cyberspace sovereignty[J]. China legal science, 2016, 4(5): 47-49.

② 郎平. 主权原则在网络空间面临的挑战[J]. 现代国际关系,2019(6):46-48.

③ 齐爱民,盘佳. 数据权、数据主权的确立与大数据保护的基本原则[J]. 苏州大学学报(哲学社会科学版),2015,36(1):64-70.

④ ZHAO B,CHEN W Q. Data protection as a fundamental right: the european general data protection regulation and its exterritorial application in China[J]. US-China law review, 2019, 16(3):99-102.

⑤ 邵怿. 论域外数据执法管辖权的单方扩张[J]. 社会科学,2020(10):119-129.

⑥ 18 U.S. Code § 2703(h)(3)(A)

⑦ European Data Protection Board. EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection [EB/OL]. (2019-07-12)[2021-01-01]. https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

并提出“网络恐怖主义”可能对关键基础设施造成损害进而影响国家安全①。如果国际组织受外部因素影响不能发挥其应有职能,成员国的对外合作将受到不应有的阻碍和干预,成员国在网络活动中的主权独立性受到了外部干预,网络攻击将干预成员国的政府职能,严重损害成员国的国家基本利益。当国家基本利益遭受严重损害时,成员国应当享有域外管辖权②。《塔林手册 2.0 版》规则 10 第 3 款规定:“一国可以就外国国民实施的旨在严重损害本国基本国家利益的网络活动行使域外立法管辖权。”成员国如果主张域外管辖权应当基于“合理联系”原则,“合理联系”原则主要包括两个方面③,一个是行使管辖权的国家与管辖事件之间具有密切关联。国际组织是国家间相互合作的结果,成员国与国际组织之间具有直接联系。德国宪法法院在审理 Manfred Brunner and Others v. The European Union Treaty 一案中提出④,成员国建立欧盟,以便于共同行使成员国的部分职能,并在一定程度上行使其主权,国际组织与成员国的主权之间具有直接联系。当国际组织遭受网络攻击时,其最终结果是成员国的对外合作受到外部因素的阻碍和干预,成员国与网络攻击之间应当具有关联性。另一个是行使管辖权的国家与受管辖事件之间有国际法所认可的利益。当国际组织遭遇网络攻击时,国家间的对外合作被迫中断,国际组织无法履行其应有职能,成员国网络主权独立性受到外部实质性干预,从而影响成员国的国家利益。《打击信息技术犯罪的阿拉伯公约》第 1 条中明确规定,制订公约的目的之一就是为了保障阿拉伯国家联盟的利益,因此这一利益逐渐被国际法接受,成员国应当享有域外管辖权。

第二,国际规则认同国家行使域外管辖权。成员国基于保护原则而主张域外立法管辖权时应当享有一定的自由度⑤,但不能违反国际法中的禁止性规定。《网络犯罪公约》采取开放性原则,没有禁止成员国设立域外管辖。《打击信息技术犯罪的阿拉伯公约》第 30 条第 1 款 e 项规定,如果犯罪是部分、全部或者已经实现对国家利益造成重大影响,各成员国应当做出承诺,以采取必要的程序将其权限扩张到本公约第二章所述的罪行中。《塔林手册 2.0 版》则直接规定域外管辖属于网络管辖权的一般规则,认为各国有权制订域外立法管辖权和域外执行管辖权。此外《防止及惩治恐怖主义公约》《上海合作组织反恐怖主义公约》等国际公约均承认域外管辖权,因此成员国主张域外管辖权有一定的合理性。

第三,成员国的域外管辖权并不影响东道国主权。成员国在规制网络活动中,

① The Commission on America's National Interests. America's National Interests[R]. 2000:5, 48.

② 联合国. 联合国大会第 61 届大会正式记录补编第 10 号[R]. A/61/10,2007:390.

③ 曹亚伟. 国内法域外适用的冲突及应对——基于国际造法的国家本位解释[J]. 河北法学,2020,38(12):81-101.

④ Manfred Brunner and Others v. The European Union Treaty, [1994] 1 C. M. L. R. 57, quotation 52.

⑤ BLAKESLEY C L, STIGALL D E. The Myopia of U. S. v. martinelli: extraterritorial jurisdiction in the 21st century[J]. George Washington international law review, 2007, 39(1):24.

不应当侵犯东道国的网络主权,虽然主权在对外方面具有独立性,但也要受国际法的约束①。国际法院在"尼加拉瓜诉美国"案中指出②,《联合国宪章》第2条第7款中的"不干涉原则"可扩大解释为所有国家或国家间组织直接或间接干预其他国家的内部或外部事务,因此成员国主张域外管辖权时应当受"不干预原则"的约束。在域外执行管辖权中,成员国如果在其领土范围之外行使权力,必须获得合法授权,包括国家授权与国际法上的特权③。在国家授权下,成员国的域外管辖权只能来源于东道国,同时还受国际组织限制。国际组织的特权约束东道国管辖权,即便成员国获得东道国的国家授权,在执行管辖权中还需要获得国际组织的许可。而成员国对国际组织电子信息系统所采取的调查取证,并未对东道国网络产生影响,特别是远程取证方式并不视为侵犯东道国的网络主权④。在国际法的特权下,成员国的域外管辖权应当来源于国际公约和国际惯例。这种特权应当被国际法所认可,但受公约内容的限制。因主权利益受损而主张的域外管辖权已经被大多数国家接受,域外管辖权主要基于主权国家的国家安全、领土完整、主权权利以及政府职能方面可能造成的损失,而不是损害行为或损害结果所发生的地点。美国法院在United States v. Pizzarusso一案中指出⑤,保护性管辖所有的犯罪要素都发生在国外,这些行为对国家安全和政府职能产生"潜在的不利影响"(potentially adverse effect)。在法国、埃及和伊朗的司法审判中,如果侵犯主权利益,基于安全利益至上原则,法院可以进行缺席审判,否则国家将长期处于危险之中⑥。保护原则关乎国家基本利益,保护原则的域外管辖是领土管辖的例外情况⑦。但域外管辖权也不能无限扩张,《打击信息技术犯罪的阿拉伯公约》虽然允许基于国家利益受损而主张管辖权,但是根据公约第4条第2款的规定,各成员国在实施该公约时不能侵犯其他成员国主管机关依据国内法所享有的专属管辖权或职能,即便成员国享有管辖权也应当尊重其他成员国的主权权力。《防止及惩治恐怖主义公约》与《上海合作组织反恐怖主义公约》的域外管辖权范围也仅限于缔约国之间。因此,成员国如果主张域外管辖权,应当获得东道国与国际组织的授权,或者与东道国之间存在条约关系。但无论基于国家授权还是国际法上的特权,当国际组织遭受网

① 联合国. 从国际安全的角度来看信息和电信领域发展的政府专家组的报告[R]. A/68/98, 2013.

② ICJ. Rep. 14[R]. 1986:205.

③ 初北平,邢厚群. 海事法律规则的适用与创新——以无人潜航器法律适用困境为例的分析[J]. 南京社会科学,2020(5):76-81.

④ CHIRCOP L. Territorial sovereignty in cyberspace after tallinn manual 2.0[J]. Melbourne journal of international law, 2019, 20(2):373.

⑤ United States v. Pizzarusso, 388 F. 2d 8, 10-11 (2d Cir. 1968).

⑥ KHOZEIMEH M A, SHAYGANFARD M. Infringements liable to protective jurisdiction (Case study: islamic republic of Iran, France and Egypt's laws) [J]. Beijing law review, 2017, 8(3):313-319.

⑦ BLAKESLEY C L, STIGALL D. Wings for talons: the case for the extraterritorial jurisdiction over sexual exploitation of children through cyberspace[J]. Wayne law review, 2004, 50(1):127-128.

络攻击时,成员国主张的域外管辖权均不会影响东道国主权。

(三)国际组织"信息电子化"对成员国刑事管辖权的影响

成员国主张管辖权的基础是国家对外合作遭受外界阻碍,如果缺失这样的基础则成员国不得主张管辖权。网络攻击主要对国际组织的系统及数据产生重要影响,信息是国际组织向成员国传递的主要内容,也是国际组织对外宣传的重要帮手,"电子化办公"实际上就是将国际组织对内与对外所传递的信息转变为电子数据①,由门户网站或专业信息系统进行传输。国际组织的信息传递任务通常由秘书处负责,这些信息主要分为三类:

第一类是向外界提供有关该组织的相关信息,是国际组织对外宣传的工具,间接扩大该组织的国际影响力。当此类信息遭受网络攻击时并不能视为阻碍国际合作,这些信息不会对国际组织的运营造成直接影响,网络攻击没有直接对国际组织职能构成阻碍或威胁。因此,成员国不能基于阻碍国际合作而提出管辖权主张,东道国则可以依据国内法有关网络犯罪的规定主张管辖权,但在执行管辖权中需要获得国际组织的许可。

第二类是向外界提供国际组织所涉领域的信息,这些信息通常承载着国际组织的职能,是国家间相互合作的结果。这些信息分为两个部分,一个是具有公开性的专业信息,另一个是存储信息的专业信息系统。此类信息遭受网络攻击的话,将给成员国间相互合作造成直接损失。即便网络攻击只破坏某一成员国的数据或者影响该系统的部分功能,但对其他成员国来说,无法通过该系统获得准确的数据分析及结果,各成员国均受到实质性的影响。因此,当网络攻击侵犯专业信息或专业信息系统时,无论是否造成实际损失,应当视为网络攻击阻碍政府对外合作的职能,侵犯成员国国家利益,成员国都可以据此主张管辖权。

第三类是向成员国或特别专家提供资料,这些信息将有助于成员国提前了解会议议程,更好地开展国际合作。此类信息同样由两个部分组成,一个是具有保密性的内部信息,国际组织所提供的电子文本是国际组织和成员国之间的内部资料,甚至是具有法律约束力的文件。另一个是传输此类信息的办公系统,主要用于国际组织和成员国之间的文件传输。如果网络攻击破坏此类信息,就会对秘书处的日常工作造成影响,不利于实现国际组织的职能。依据保护原则,针对政府职能和国家安全的行为只要产生"潜在的不利影响",成员国都可以主张管辖权。因此当网络攻击破坏此类信息时,即便所侵犯的信息不具有法律效力,但由于该信息具有保密性,有可能对国际合作造成影响,成员国同样可以据此主张管辖权。

## 四、常设机构所在地刑事管辖权的完善与建议

总部协议中的传统刑事管辖权已不能完全适用于"信息电子化"后的国际组

① 方阁,初北平.海事网络安全风险保险的法律治理研究[J].江西社会科学,2020,40(5):179-191.

织,为平衡东道国与成员国之间的权益,应当进一步完善总部协议中管辖权安排。

(一) 国际组织应当享有常设机构所在地的数据所有权

网络对国际组织的日常运营产生重要影响,同时也对国际机制理论产生深远影响①,各国在网络空间中的相互博弈也影响着国际组织。网络空间与主权之间有三个层级,分别是物理层、逻辑层和社会层,东道国在物理层、逻辑层和社会层的主权也要受到总部协议的约束。

在物理层面,国际组织的计算机和服务器处于东道国的领土之上。东道国的领土主权在常设机构所在地是一种受限制的权利,国际组织的计算机和服务器通常位于常设机构所在地,这些实体物同样享有总部协议中东道国给予的特权和豁免。在逻辑层面,东道国并不享有网络协议与数据的专属权。对于网络协议而言,由于电子频率和根域名资源是一种稀缺资源,网络技术标准和域名地址分配不能专属于某个国家。国际组织所产生的数据通常存储于常设机构所在地,如果东道国采用"数据存储地标准",当对国际组织产生的数据主张权力时,常设机构所存储的数据享有总部协议中的特权与豁免。如果东道国采用"数据控制者标准",客体物的数据权属应当由数据控制者享有,实际控制者所在地将享有的数据主权,国际组织所产生的数据通常由常设机构实际控制,即便委托第三方公司进行数据维护和管理,数据所有权依旧归国际组织所有。在社会层面,东道国有权规制境内自然人和法人的网络活动,但受总部协议的约束。国际组织的电子数据视为国际组织文档的组成部分,应当由国际组织享有所有权。

(二)"电子信息化"后常设机构所在地的刑事管辖权安排

1."联合国合作打击网络犯罪公约"对总部协议中刑事管辖权的影响。在《网络犯罪公约》与《打击信息技术犯罪的阿拉伯公约》生效之后,各国纷纷在国内法中确立网络犯罪的法律法规,但国家之间的利益冲突以及对网络犯罪的认知程度不同,导致司法实践中存在差异。为了缓和这种矛盾,一方面由区域组织在本区域内推行示范性立法,期望达成本区域内有关网络犯罪的协调一致。另一方面联合国也高度关注网络犯罪问题,在 2010 年《应对全球挑战全面战略的萨尔瓦多宣言》中提出应当对网络犯罪问题做全面研究,并在 2019 年底通过了"联合国合作打击网络犯罪公约草案"(下文简称"草案")。

在管辖权方面,"草案"明确各国在网络空间中享有主权权利,承认各国在网络空间中的管辖权,允许各缔约国在国内立法中确立网络犯罪管辖权:(1) 船舶和航空器在内的主观和客观属地原则;(2) 积极和消极属人原则,缔约国境内设有常设机构的法人、缔约国的外交使团或领事馆;(3) 保护原则,同时要求各缔约国所制定的网络犯罪管辖权不能违反一般国际法准则。"草案"首次纳入针对国际组织的网络犯罪问题,根据"草案"第 43 条第 2 款 a 项,缔约国有权管辖其领土上设有常

① 张丽华. 国际组织概论[M]. 北京:科学出版社,2015:32.

设机构法人的网络犯罪活动,因此当国际组织遭受网络攻击时,东道国享有网络犯罪管辖权。

虽然该“草案”承认东道国对国际组织网络犯罪管辖权的正当性,但并没有授予国际组织成员国以同样的权力。根据“草案”第43条第2款c项,缔约国有权确立针对本国网络犯罪行为的管辖权,承认各缔约国可以基于保护性管辖而主张网络犯罪管辖权。在这种情况下,管辖范围不再仅限于领土并扩张到领土范围之外。但是这项规定仅限于针对本国的网络犯罪行为,“草案”中规定的保护性管辖只是保护成员国的部分主权,即成员国对内主权,并不包含成员国对外主权。这种管辖权安排还是基于传统属地原则中的东道国“安全保障义务”,是传统东道国刑事管辖权在网络领域中的映射,并非基于网络主权的全面扩张。即便该“草案”不做上述约定,东道国依据剩余权力,实际上也享有基于属地原则的网络犯罪管辖权,“草案”事实上仅是对这种权利的阐述,因此这一规定不能完全解决国际组织遭受网络攻击时的管辖权问题,也不能有效打击针对国际组织的网络攻击行为。一方面,“草案”没有改善东道国消极行使管辖权的现状。即便国际组织已经遭受频繁的网络攻击并造成较为严重的破坏,但积极主张刑事管辖权的东道国却相对较少,“草案”并没有改变管辖权安排,甚至限制了其他成员国的合理主张。成员国无法依据“草案”而主张管辖权,不能提升对国际组织的有效保护。即便国际组织有权变更东道国,迁移总部所在地,但往往需要较多的时间和经济成本,这将阻碍国际组织的日常运营,甚至破坏国际组织已经取得的成果。因此绝大部分国际组织并没有轻易改变选址,而“草案”的这种规定不会改变东道国积极主张管辖权的局面。另一方面,“草案”对保护国际合作存在不足。鼓励“国际合作”是“草案”的重点内容之一,“草案”鼓励缔约国在打击信息通信技术犯罪、追回资产、多方参与、刑事诉讼程序、人员培训等方面开展合作,并在“草案”序言部分明确提出:“国际合作对打击信息通信技术犯罪至关重要”。在执法合作中,为更好地实现“草案”的目标,“草案”以示范法的形式创设了一套合作机制供各缔约国参考,同时鼓励各缔约国加强与国际或区域性组织之间的相互合作,对已经缔结的双边或多边协定进行修正。但是该“草案”并未对“国际合作”问题给予充分保护,特别是作为国家间合作成果的国际组织,“草案”并未给予更多的回应。当国际组织遭遇网络攻击而阻碍国际合作进程时,由于网络攻击针对的对象是国际组织并非成员国,网络攻击也不在成员国领土上,攻击者如果也不是成员国的国民,即便事实上网络攻击侵犯成员国主权,“草案”也没有赋予成员国以管辖权,完全由东道国决定是否行使管辖权。

2. 国内立法对总部协议中刑事管辖权的影响。由于“联合国网络犯罪公约草案”尚未生效,因此常设机构所在地的刑事管辖权与东道国和成员国的国内立法相关。对东道国而言,刑事管辖权应严格适用“主观属地原则”,在适用网络犯罪时可能存在权利真空,因此有两种修正路径,一是扩张刑事管辖权的适用范围,但这种方式将过度扩张东道国的管辖范围,形成东道国对国际组织事务的

“长臂管辖”。二是对网络犯罪管辖权做特别约定,但需要东道国具备较为完善的网络治理体系。对成员国而言,传统刑事管辖权主要与东道国有关,此前管辖权问题并未获得足够关注。在“网络犯罪”出现之后,域外管辖权成为各国治理网络犯罪的权利之一,各国纷纷在国内立法中确立域外效力。如果网络攻击的目的是为了破坏国际合作机制,则应当赋予成员国域外管辖权,国际组织的刑事管辖权将不再专属于东道国,管辖权多元化也有利于解决国际组织遭受网络攻击的实际问题。

以我国为例,由于大多数国际组织建立较早,与美国、荷兰、奥地利等国家相比,选择我国为东道国的国际组织并不多。但近年来我国的国际影响力不断提升,国际话语权逐渐提高,已经有“上海合作组织”“联合国外太空事务办公室”“亚太空间合作组织”选择我国为东道国并建立相应的信息平台。在现行立法中,我国《刑法》确立“保护性管辖”与“属人管辖”为一般原则,虽然管辖范围较广,但对我国政府参与国际组织活动的保护性立法相对较少。我国《驻外外交人员法》保障对我国驻外使领馆及参与国际组织工作人员的合法权益,但为驻华国际组织提供立法保护方面还存在问题。我国《反恐怖主义法》中将针对国际组织的犯罪行为视为恐怖主义,但却仅限于基于政治和意识形态的胁迫行为,并不包括阻碍国际组织实现基本职能的网络攻击行为,以及基于个人利益的网络攻击行为。我国《网络安全法》中明确我国享有网络主权,对“网络攻击”的性质及责任做出明确规定,但仅限于对国内“关键信息基础设施”造成损害的网络攻击行为,并未考虑境外人员对我国参加国际组织遭受网络攻击的损害,特别是基于个人利益而实施的网络犯罪情况。有学者也提出,应当基于我国的基本利益,建立以保护性管辖为基础的域外适用规则,强调域外行为损害本国基本利益,在网络安全中体现基于效果原则的保护性管辖权,将境外的特定行为纳入域外效力范围①。因此,东道国具备良好的法律体系,能够为国际组织提供有效的救济途径才是确保国际组织合法权益的基石。

3. 确立成员国间的管辖权冲突规则。通常情况下,总部协议中的“争议解决机制”将优先于组织章程中的“纠纷解决机制”。国际组织确定管辖权冲突规则时应当分为两种情况,一种情况是东道国与成员国之间的管辖权冲突,另一种情况是除东道国外的成员国之间所发生的管辖权冲突。

东道国与其他成员国之间的管辖权冲突,本质上是东道国与国际组织之间的管辖权争议,不能视为成员国间的管辖权冲突,因为国际组织的管辖权问题已经通过总部协议确认,因此应当适用总部协议中的“争议解决机制”。例如《加拿大政府与环境合作委员会之间的总部协定》第 18 条规定:“关于解释和适用本协议或任何补充协议所发生的任何争议,当事方未能通过谈判或其他方式解决时,应当交由三

① 廖诗评. 中国法域外适用法律体系:现状、问题与完善[J]. 中国法学,2019(6):20－38.

名仲裁员组成的法庭做最后决定。执行董事指定一名仲裁员,加拿大外交部长指定一名仲裁员。两名仲裁员再共同指定一名仲裁员。"①根据联合国驻纽约办事处"总部协议"第8条规定:"如果两名仲裁员未能就共同指定仲裁员事宜达成一致,则由国际法院院长指定。"因此,东道国依据"领土原则"的管辖权主张将优先于其他成员国的域外管辖权。

当成员国间发生管辖权争议时,将涉及组织章程中所设立的"纠纷解决机制"与相关国际公约中"管辖权冲突规则",由于网络攻击的客体是国际组织,管辖权冲突实质上是成员国之间的内部争议,并不是缔约国之间国内立法中的管辖冲突,因此原则上应当适用国际组织章程中的"纠纷解决机制",两者之间是一种排他关系。主张管辖权的成员国如果缔结了同一个涉及管辖权冲突的国际公约,可以适当参考公约中的管辖权冲突规则,但决定权并不在于成员国,而是纠纷解决机制中的权力机构,如大会、仲裁庭等。国家间存在天然的利益冲突,在"囚徒困境"的博弈中,国家间相互合作将比国家间彼此割裂带来更多的收益。纠纷解决机制作为一种组织化安排,本身就提供了一套成本较低的解决方案,而在解决成员国间矛盾与冲突的过程中,适当参照成员国共同缔结的国际公约将更有利于解决矛盾,容易达成共识,进一步降低成本②。因此,如果成员国都是《打击信息技术犯罪的阿拉伯公约》的缔约国,则在"纠纷解决机制"中适当参考该公约第30条第3款规定的管辖权冲突规则。如果成员国都是《网络犯罪公约》的缔约国,可以在"纠纷解决机制"中适当参考该公约第22条第5款的规定,由成员国在适当的情况下先进行相互协商③,再适用组织章程中的"纠纷解决机制"。"联合国合作打击网络犯罪公约草案"没有对管辖权进行优先性排序,而是为缔约国提供"引渡协议",积极促进缔约国主张管辖权,更加重视对犯罪行为的有效打击。根据"草案"第43条和第48条,当发生管辖权冲突时,各缔约国应当进行协商,协调彼此间的行动。公约鼓励各缔约国采用"引渡"的方式解决管辖权冲突,如果缔约国之间没有"引渡协议",根据"草案"第48条第4款,缔约国可以依据"草案"请求引渡。如果缔约国拒绝引渡请求,则主张引渡的缔约国确立享有管辖权,而拒绝引渡的缔约国,无论其行为是否发生在该国境内,均应及时起诉该行为人。域外执行管辖权是主权的一个排他属性,国家在境外行使权利,必须经过他国同意或国际法上的特定授权。而东道国与国际组织之间,东道国在执行管辖权中放弃绝对权力,授权国际组织自由支配所享有的特权,东道国在这一问题中并不享有完整的权利,国际组织中的"纠纷解决机制"是解决成员国间管辖权冲突的唯一途径。因此,国际组织在修订组织章程时,应当对可能遭受网络攻击的情况予以充分考虑,首先,正视攻击者位于东道国管辖

① Article18,"Headquarters Agreement Between the Government of Canada and the Commission for Environmental Cooperation" (E101916-CTS 1997 No. 27.).

② 饶戈平.国际组织与国际法实施机制的发展[M].北京:北京大学出版社,2013:57-61.

③ 郭旨龙,丁琪,高严.网络犯罪公约的修正思路[M].北京:中国法制出版社,2016:171.

范围之外时可能存在的权力真空,有必要确立并承认成员国享有域外管辖权,保障国际组织的有序运行。其次,确立管辖权冲突规则,国际组织应当合理预见成员国间可能存在的管辖权冲突,强调国际组织内部纠纷解决机制是解决管辖权冲突的唯一途径。再次,重视国际公约的指引作用,在纠纷解决机制中充分考虑成员国间共同缔结的国际公约,尽快达成共识,提升纠纷解决机制效率。最后,充分借鉴"联合国网络犯罪公约草案"中"引渡协议"模式对解决管辖权冲突的实效作用,成员国间可能没有共同缔结的国际公约,但可能存在共同参加的国际组织,其他国际组织针对相同问题所做的安排同样具有参考价值。联合国作为全球最大的国际组织,几乎涵盖所有国家,虽然其所制定的"草案"尚未生效,但"草案"中的内在价值同样有助于解决成员国间的管辖权冲突。

(责任编辑:潘亚莉)

# On the Criminal Jurisdicition after the Cyber-attacks on International Organizations

Chu Beiping, Xue Tianci

(School of law, Dalian Maritime University, Dalian 116023, China)

**Abstract**: In recent years, the cyber-attacks on international organizations were on the rise. The "E-information" of international organizations also impacted the criminal jurisdiction in the "Headquarters Agreement". For the host country, there may be a jurisdiction vacuum when the attacker is from outside its territoryaccording to the jurisdiction arrangement in the existing "Headquarters Agreement". For the member states, they should have the right to assert extraterritorial criminal jurisdiction on the basis of the principle of protectionwhen the attacker affects the basic functions of international organizations, hinders the foreign cooperation of the member states and infringes their national interests. So, to protect the operation of international organizations and the rights and interests of their member states, the criminal jurisdiction rules in the "Headquarters Agreement" should be improved.

**Key words**: cyber-attack; international organization; criminal jurisdiction; Headquarters Agreement