论网络攻击在国际法上的归因

黄志雄

内容提要:大多数网络攻击的私人性和隐秘性特点,使得这类攻击在国际法上的归因成为一个较为复杂的问题。近年来,国际社会日益重视对这一问题的讨论,并提出了种种放宽甚至取消国际法上既有归因标准的主张。但是,这些主张在强调受害国维护自身网络安全需要的同时,忽视了其他国家受到无辜波及的风险,具有不同程度的片面性和局限性。对网络攻击确定国家责任的前提,是通过国际法进行负责任的归因,既不应使实际从事和控制网络攻击的国家逍遥法外,也不应扩大国家责任的范围而伤及无辜。联合国国际法委员会2001年《国家责任条款》中确定的归因规则,对于网络攻击的归因仍然发挥着不可替代的作用。

关键词:网络攻击　归因　国家责任　《国家责任条款》

黄志雄,武汉大学国际法研究所教授。

在近年来有关网络安全的讨论中,网络攻击的归因(attribution)问题日益受到重视。[1] 从国际法角度来说,归因的目的在于确定某一行为可否归于一个国家而成为该国的国家行为。就网络攻击而言,正确的归因是采取有效应对措施的重要前提:如果一起网络攻击通过归因被确定为国家行为,一般而言,这将涉及该国的国家责任以及受害国采取反措施的权利等问题。[2] 而完全由私人发起的网络攻击则通常属于网络犯罪行为,主要通过有

〔1〕 除学界的相关探讨外,目前国家间围绕网络空间国际行为准则的各种辩论和谈判也越来越多地涉及这一问题。例如,在联合国信息安全政府专家组2013年6月以协商一致方式通过的一份重要报告中,首次明确提出:"各国必须就可归因于他们的国际不法行为履行国际义务,且不得通过代理人实施此类行为。"参见 United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013), A/68/98, para. 23。而在2014年7月下旬举行的新一届专家组首次会议上,各国代表辩论的问题之一,就是有无必要围绕下文所述"转嫁责任"等主张制定新的网络攻击归因规则。

〔2〕 根据2001年《国家责任条款》第2条,一个行为要构成一国的国际不法行为并产生该国的国际法律责任,需同时具备以下两个要素:(1)该行为可依国际法归因于有关国家;(2)该行为与该国的国际义务不符。需要指出的是,即使一起针对他国的网络攻击被归因于一国,该攻击是否违背该国的国际义务还需加以具体分析。下文所关于网络攻击产生一国国家责任的表述,均假定有关攻击违反了该国的国家义务。

关国家国内法的管辖以及国家间的司法合作来加以应对。

不过,与国际法所关注的大多数行为相比,网络攻击在发起者的身份和源头追溯等方面有其复杂和特殊之处,由此提出的问题是:国际法上已有的归因规则可否适用于网络攻击?是否需要为此确立某些特殊的归因标准?对此,一些西方学者已有若干探讨,但其中多有似是而非、不无偏颇的观点。

我国学界对这一问题则鲜有关注,[3]尽管中国事实上是西方有关主张的主要"假想敌"之一。本文拟结合联合国国际法委员会 2001 年《国家责任条款》中的归因规则和相关国际实践,对网络攻击的归因问题加以分析,以期澄清某些带有误导性的主张,并阐明我国在这一问题上的应有立场。

一 网络攻击的归因:法律和技术层面

归因作为国际法上的一个基本问题,是一个用以"确定由自然人完成的某一行为(包括作为和不作为),是否可以根据国际法定性为'国家行为'"的法律过程。[4] 归因问题的重要性在于,国家作为一个虚拟的实体,不可避免地需要通过特定的个人来进行对内管理和对外交往。正如意大利国际法学家安齐洛蒂在近一个世纪前所指出的那样:"国家的行为仅仅是通过法律而归属于国家的个人的行为。"[5]因此,与国家在国际法上权利和义务有关的各种行为,通常都涉及这样一个问题:要将个人行为视同为国家行为,需要符合哪些条件或标准?这一问题,需要通过国际法上的归因规则来加以回答。

尽管国际法的几乎每一个领域都涉及归因问题,但有关归因规则主要是以习惯国际法的形式在国家责任法领域逐渐发展而来的。在此基础上,联合国国际法委员会 2001 年通过的《国家责任条款》(以下简称《条款》)[6]第一部分第二章,以 8 个条文(第 4—11 条)对有关归因规则进行了系统编纂。这些条款,构成了国际法上有关归因的一般规则。

概而言之,这些归因规则的总体原则是:"在国际层面上,唯一应归因于国家的行为是该国政府机关的行为,或者由这些机关所指挥、唆使或控制的其他人的行为。"[7]根据这一总体原则,《条款》第 4 条将一国国家机关的行为归因于该国。第 5—7 条则涉及可以归因于国家的三种特殊情况:经授权行使政府权力要素的个人或实体的行为(第 5 条);

---

〔3〕 就本文作者所见,截至 2014 年 8 月,国内学者中只有冷新宇的《网络攻击中国家责任的判别标准》一文(载《西安政治学院学报》2014 年第 2 期)对这一问题有较为系统的讨论。

〔4〕 Luigi Condorelli and Claus Kress, The Rules of Attribution: General Considerations, in James Crawford et al. (eds.), *The Law of International Responsibility*, Oxford University Press, 2010, p. 221. 当然,在现代国际法上,归因不仅仅适用于国家,而且也适用于政府间国际组织等其他具有国际法律人格的实体,但本文仅仅关注与国家有关的归因问题。

〔5〕 Dionisio Anzilotti, *Cours de droit international* (1929) (Paris, Panthéon Assas, 1999), p. 469, cited from Luigi Condorelli and Claus Kress, The Rules of Attribution: General Considerations, in James Crawford et al. (eds.), *The Law of International Responsibility*, Oxford University Press, 2010, p. 238.

〔6〕 Articles on the Responsibility of States for Internationally Wrongful Acts, Report of the ILC on the Work of its Fifty-third Session, UN Doc. A/56/10 (2001).

〔7〕 Commentaries to the Draft Articles on Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission at its fifty-third session (2001), Official Records of the General Assembly, Fifty-sixth session, Supplement No. 10 (A/56/10), Chapter II (Attribution of Conduct to a State), para. 2.

经另一国交由一国处置的机关的行为(第6条);国家机关越权或违反命令所从事的行为(第7条)。原则上,私人行为体的行为不能归因于国家,除非该行为受到国家的指挥或控制(第8条)。第9—11条同样规定了三种特殊情况:在没有有效政府的情况下事实上行使了政府权力的个人或团体所从事的行为(第9条);成为或建立了新国家的叛乱运动或其他运动所从事的行为(第10条);经一国认可和接受为该国行为的行为(第11条)。

上述早在网络空间形成之前就已经作为习惯国际法存在的归因规则,对于网络攻击在国际法上的归因问题是否同样适用?毕竟,网络攻击作为存在于虚拟网络空间的一类行为,与国际法所关注的大多数行为相比有着种种特殊属性。就本文探讨的归因问题而言,尤其值得注意的是网络攻击在以下两方面的特点。

第一,绝大多数网络攻击都是由私人行为体发起,其与特定国家之间的联系往往难以确定。互联网的普及,使得国家以外的各种行为体(包括个人和黑客组织等)能够轻松利用网络空间,开展各种活动并产生全球性影响。事实上,经披露的国家之间的网络攻击不仅数量很少,而且影响相对来说也小得多;相反,已知的绝大多数网络攻击都是由各种私人行为体发起的。[8] 在这个可以笼统地称为"黑客"的群体中,情况千差万别。他们有的独来独往、单兵作战,有的则形成了组织和协作程度各不相同的"黑客联盟";有的是基于政治立场、意识形态等原因对特定国家发起攻击(所谓"爱国黑客"就属于这一类),有的则是为了个人经济利益或者仅仅为了出名;他们多数独立于国家政府,但有的也与某些国家政府有着不同程度的联系,甚至听命于政府。在现有技术条件下,一个小小的黑客组织甚至一名"独狼"式的黑客就完全可以通过网络攻击对特定国家的网络基础设施或重要信息带来严重的安全威胁。但另一方面,由于攻击者通常并不在被攻击国境内,要确定攻击者与其所在国家之间的关系并将其绳之以法,往往面临国际刑事司法合作等方面的重重障碍。

第二,网络攻击通常具有高度的隐秘性,其发起者的身份确认十分困难。"在网上,没有人知道你是一条狗。"这一流传甚广的名言,体现了网络空间最主要的特征之一——匿名性。对于有经验的黑客而言,通过伪造IP地址、控制"僵尸网络"等手段,可以轻而易举地隐藏身份信息,包括攻击者是谁、攻击的真实源头位于何处等等。因此,调查和追溯网络攻击的源头(即所谓"技术归因")往往极其复杂、成本高昂且旷日持久。[9] 事实上,近年来国际上的一些大规模网络攻击(如2007年爱沙尼亚受到的网络攻击、2010年伊朗核设施受到的"震网"病毒攻击等)究竟是由谁发起,至今仍无定论。[10]

网络攻击的上述特点,会在多大程度上影响国际法上的归因规则对这类攻击的适用?在一些情况下,这种影响似乎不大。例如,只要能够证明,一起网络攻击是由一国的国家机关或经正式授权行使政府权力要素的个人或实体发起的,毫无疑问,该攻击将根据《条

〔8〕 Eric Jensen, Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, 38 *Stanford Journal of International Law* 207, 232 – 234 (2002).

〔9〕 David Clark & Susan Landau, Untangling Attribution, 2 *Harvard National Security Journal* 323, 324 (2011).

〔10〕 Duncan Holis, An E-SOS for Cyberspace, 52 *Harvard International Law Journal* 373, 397 – 399 (2011).

款》第 4 条或第 5 条被归因于该国;[11] 如果发起该网络攻击的机关“经另一国交由一国处置”,或者该机关所从事的行为是越权或违反命令的,有关行为仍可根据《条款》第 6 条或第 7 条归因于该国。但是,实际情况通常并非如此简单,因为大多数网络攻击并不是由一国的国家机关(或经授权行使政府权力要素的个人或实体)发起,而由于网络攻击的隐秘性和技术归因的困难,很多时候甚至难以查证攻击者是隶属于一国国家机关的个人还是与一国政府无关的私人。由此,人们可以提出一系列问题,例如:

——如果受一国控制的私人行为体对他国发起网络攻击,在何种情况下(或者说,在该国的控制达到何种程度时)可以将该攻击归因于进行控制的国家,并追究该国的国家责任?

——如果一起网络攻击的发起者是与一国政府无关的私人行为体或身份不明者,是否可能将该攻击归因于攻击源头所在国,理由是该国未能采取措施来防止该网络攻击?

——同样地,如果一起网络攻击的发起者是与一国政府无关的私人行为体或身份不明者,是否可能将该攻击归因于攻击源头所在国,不论该国是否采取了必要措施来防止该网络攻击?

近年来多起被国外媒体大肆渲染的网络攻击事件,加大了西方国家对上述问题的关注。例如,根据一些媒体报道,美国五角大楼在 2007 年受到来自中国的网络攻击,爱沙尼亚在 2007 年受到的网络攻击主要来自俄罗斯,2008 年俄—格军事冲突期间格鲁吉亚则受到来自俄罗斯的网络攻击,但均无证据证明有关国家政府直接参与了这些攻击。[12] 鉴于直接调查和惩处攻击发起者存在较大困难,西方学者开始有针对性地提出为网络攻击的归因“量身定制”某些特殊规则的设想。[13] 那么,这些主张是否合理、可取?本文的随后几个部分,将分别加以分析。

二 私人网络攻击归因于国家:两种控制标准之争

如前所述,大多数网络攻击都是由私人行为体发起的,是否以及如何将这些私人发起的网络攻击归因于特定国家是一个日益重要的问题。原则上,国家不需要也不应当为私人行为体的行为负责,但与此同时,也不应允许国家“一方面事实上通过个人从事某些行为,另一方面又在这些个人违反国际法时将自身同这些行为切割开来”。[14] 如何在上述

〔11〕 2014 年 5 月 19 日,美国司法部以涉嫌通过互联网窃密为由,宣布对 5 名中国军人进行起诉。中国政府则严正声明,中国政府和军队及其相关人员从不从事或参与通过网络窃取商业秘密活动,美国的指责纯属无中生有、别有用心。中国外交部:《中方强力反击美方“起诉”中方人员》,http://www.fmprc.gov.cn/mfa_chn/fyrbt_602243/t1157508.shtml,2014 年 5 月 25 日访问。这里,两国的分歧在于中国军人是否利用互联网从事了有关行为这一事实问题,而不在于这些军人所从事的行为是否可以归因于国家。

〔12〕 Matthew J. Sklerov, Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Which Neglect Their Duty to Prevent, 201 *Military Law Review* 1,10 (2009).

〔13〕 《条款》第 55 条规定:“在且仅在一国际不法行为的存在条件或一国国际责任的内容或履行应由国际法特别规则规定的情况下,不得适用本条款。”因此,至少从理论上说,在《条款》的一般规则之外制定特别规则是没有问题的。

〔14〕 ICTY, Prosecutor v *Tadić*, Case No IT-94-1-A, Judgment, Appeals Chamber, 15 July 1999, para. 117.

两个不同的要求之间达成平衡,正是问题的关键所在。

《条款》第8条是关于私人行为如何归因于国家的主要条文,它规定:"如果一人或一群人实际上是在按照国家的指示或在其指挥或控制下行事,其行为应视为国际法所指的一国的行为。"前南斯拉夫国际刑事法庭(以下简称"前南刑庭")上诉分庭曾经在"塔迪奇案"中指出:该条文的目的,是"为了防止国家通过让个人来从事不能或不应由国家官员从事的活动,逃避其国际责任"。[15]

(一)关于国家控制私人行为的两种不同标准

第8条中的归因条件是国家对个人行为的"指示"(instruction)、"指挥"(direction)或"控制"(control)。这里,"指示"和"指挥"的含义相对明确,而"控制"这一用语则有着较大的解释空间。为了将有关个人的行为归因于国家,需要何种程度的国家控制?第8条本身没有对这一问题加以明确回答,但国际法院在1986年"尼加拉瓜案"中对此进行了讨论。[16] 在该案中,争议问题之一是受美国支持的尼加拉瓜叛乱者的行为可否归因于美国。

国际法院指出:尽管美国在资助、组织、训练、供给和武装尼加拉瓜叛乱者方面的作用(包括对叛乱者的军事或准军事攻击目标加以选择以及对叛乱者的整个行动进行谋划)是极为显著或决定性的,但这还不足以将叛乱者在尼加拉瓜从事的军事或准军事活动归因于美国,因为本案所涉及的违反国际法的行为完全可能是由叛乱团体的成员在不受美国控制的情况下从事的;"要使有关行为产生美国的法律责任,原则上需要证明美国对于……被指控违法的军事和准军事行动行使着有效控制(effective control)。"[17]根据这一原则,只有当一国不仅对某一团体进行了"总体上的控制",还对于该团体从事特定的行动发出了明白无误的指令时,所涉及的行动才能被归因于该国。在"波黑种族灭绝案"中,国际法院再次重申:主张存在有效控制的国家必须证明,有关控制是"针对被指控发生了不法行为的每一行动,而不是一般地针对从事了违法行为的个人或团体总体上的行动"。[18]

国际法院所采取的这一严格标准,受到了前南刑庭上诉分庭的批评。在"塔迪奇案"中,上诉分庭认为,整个国家责任法体系的逻辑要求国家对它在事实上或法律上控制的一切承担责任,而有效控制标准与这一逻辑不相符,因而是"缺乏说服力的"。[19] 上诉分庭进一步指出,为了将一个军事或准军事团体的行为归因于一国,应当证明的是此国家对该团体进行了全面控制(overall control),这种控制不仅体现为武装和资助该团体,还体现为协调或帮助其进行军事活动的整体筹划。"在此之外,并不要求国家就从事违法国际法

〔15〕 ICTY, Prosecutor v *Tadić*, Case No IT-94-1-A, Judgment, Appeals Chamber, 15 July 1999, para. 117.

〔16〕 International Court of Justice Reports of Judgments, *Case Concerning Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States), Merits, Judgment of 27 June 1986.

〔17〕 International Court of Justice Reports of Judgments, *Case Concerning Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States), Merits, Judgment of 27 June 1986, para. 115.

〔18〕 International Court of Justice Reports of Judgments, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v Serbia and Montenegro), Merits, Judgment of 26 February 2007, para. 400.

〔19〕 ICTY, Prosecutor v *Tadić*, Case No IT-94-1-A, Judgment, Appeals Chamber, 15 July 1999, para. 116.

的特定行为向该团体的首脑或成员发布指令。"[20] 根据全面控制标准,上诉分庭裁定,1995 年 7 月在斯雷布雷尼查对穆斯林族进行大屠杀的塞族共和国军受到了南斯拉夫联盟共和国(以下简称"南联盟")的控制。

在确定归因和国家责任方面宽松得多的全面控制标准,受到了一些学者的极力支持。具体就网络攻击而言,有的学者更是主张:鉴于这类攻击的私人性和隐秘性,在将有关攻击归因于国家时应当采用"全面控制"而不是有效控制标准,因为后者将使一国政府可以轻而易举地掩盖其信息战行动;"未来全面的法律机制应当为……网络攻击受害国提供充分救济,但如果有效控制成为决定网络攻击国家责任的主要范式,那么即便是最严重攻击的受害国也可能无法寻求正义。"[21]

(二)全面控制标准的局限性

上述赞同全面控制标准的主张貌似合情合理,实际上却经不起仔细推敲。

首先,国际法院在"尼加拉瓜案"中提出的有效控制标准和前南刑庭上诉分庭在"塔迪奇案"中提出的全面控制标准,实际上针对的是两个性质不同的问题——前者涉及的是国家责任问题(尼加拉瓜叛乱者的行为能否归因于美国并产生其国家责任),后者涉及的则是武装冲突的性质问题(南联盟对波黑塞族共和国军的控制是否足以使波黑战争成为国际武装冲突)。在处理后一问题(武装冲突的性质)时,全面控制标准也许是"可适用和恰当的",但在国家责任法领域,既有判例确认的仍然是有效控制而不是全面控制标准。[22] 因此,并不能简单地认为,有效控制标准被全面控制标准推翻和取代了。实际上,在上述两个案件之后的"波黑种族灭绝案"(该案涉及能否将波黑塞族共和国军的行为归因于南联盟并要求后者承担责任)中,国际法院再次确认了有效控制标准。

其次,从本质上说,《条款》第 8 条属于私人行为不归因于国家这一原则的例外,因此,对该例外加以狭义解释是更为合适的。[23] 正如国际法院在"波黑种族灭绝案"所言,国家责任法的一项基本原则是,国家仅仅对其自身的行为——亦即无论基于何种根据而代表国家采取行动的个人的行为——负责;"全面控制标准的主要缺陷在于,它扩大了国家责任的范围并远远超出了国家责任法的上述基本原则……该标准对于确定国家责任是不合适的,因为它把一国国家机关的行为与该国的国际责任之间必须存在的关联放宽到几乎难以延续的程度。"[24]

---

〔20〕 ICTY, Prosecutor v *Tadić*, Case No IT-94-1-A, Judgment, Appeals Chamber, 15 July 1999, para. 131.

〔21〕 Scott Shackelford, State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, in Christian Czosseck and Korie. Podins (eds.), *Conference on Cyber Conflict Proceedings 2010*, CCDCOE, 2010, pp. 202 – 204.

〔22〕 International Court of Justice Reports of Judgments, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v Serbia and Montenegro), Merits, Judgment of 26 February 2007, paras. 404 – 405.

〔23〕 Alexander Kees, Responsibility of States for Private Actors, in R. Wolfrum (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, Oxford, 2008 –), online edition, < www. mpepil. com >, visited on 12 April 2014, para. 14.

〔24〕 International Court of Justice Reports of Judgments, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v Serbia and Montenegro), Merits, Judgment of 26 February 2007, para. 406.

最后,就网络攻击的归因而言,全面控制标准同样缺乏法律依据。正如有学者曾经指出的那样:恰恰是因为确定网络攻击的源头存在很大困难,才更有必要采取有效控制标准,因为它可以防止一国被无辜指责从事了网络攻击;特别是在网络攻击受害国主张对攻击国行使自卫权的情况下,采用严格的有效控制标准更为重要。[25] 这里,应当看到,归因(以及使一国承担责任)本身不是目的,而是达到在各国间寻求正义这一目的的手段。

此外,在"塔迪奇案"中,前南刑庭上诉分庭也主张:应当对组织严密的军事或准军事团体和孤立的个人或非正式的团体加以区分,尽管全面控制标准适用于前者,但对于后者而言,仍有必要证明其特定的具体行为在事实上受到了控制。[26] 也就是说,即使是该上诉分庭也承认,对于孤立的个人或非正式的团体,在确定其行为可否归因于特定国家时,需要依照更为严格的有效控制标准来加以确定。这一点对于网络攻击的归因尤为重要,因为这类攻击大都是由"独狼"式的黑客或较为松散的黑客组织发起的。

三 私人行为体网络攻击的转嫁责任问题

(一)转嫁责任的提出

对网络攻击而言,经常存在并容易引发分歧的另一种情形是:如果一国受到的网络攻击是由另一国境内与政府无关的私人行为体发起,或者攻击来自另一国境内但攻击者身份难以查明,那么可否要求后一国家(即所在国)为有关攻击承担责任?在此情形下,由于网络攻击的隐秘性等特点,并没有证据证明存在《条款》第 8 条所指的国家对个人行为的指示、指挥或控制,从而难以根据国际法上的传统要求对网络攻击行为进行归因。有鉴于此,一些西方学者极力主张,应当通过"转嫁责任"(imputed responsibility)来解决这一问题。转嫁责任的基本含义是:如果一国未能采取必要措施预防从该国领土内发起的网络攻击,那么这些网络攻击将被转嫁于该国,并由此产生该国的国家责任。[27]

应当看到,在网络攻击受到普遍关注之前,与转嫁责任相类似的主张已经在国际法其他领域提出过。例如,一些学者认为,如果一国未能预防恐怖主义分子从其境内对他国发起攻击,该国应当对此承担"严格责任",而不需要遵守国际法上有关归因的传统要求。[28] 支持这一主张的学者大多认为,转嫁责任这一处于演进之中的新标准,是在"9.11"恐怖主义袭击之后开始逐渐形成的:由于阿富汗塔利班政府为基地组织提供了庇护场所,后者发起的"9.11"恐怖主义袭击随后被转嫁于塔利班,尽管并无迹象表明该政府对基地组织

---

〔25〕 Marco Roscini, World Wide Warfare-Jus ad bellum and the Use of Cyber Force, in Armin von Bogdandy and Rudiger Wolfrum (eds.), 14 *Max Planck Yearbook of United Nations Law* 85, 100 (2010).

〔26〕 ICTY, Prosecutor v *Tadić*, Case No IT-94-1-A, Judgment, Appeals Chamber, 15 July 1999, para. 116.

〔27〕 Matthew J. Sklerov, Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Which Neglect Their Duty to Prevent, 201 *Military Law Review* 1, 38 – 39 (2009); David E. Graham, Cyber Threats and the Law of War, 4 *Journal of National Security Law and Policy* 87, 93 – 96 (2010).

〔28〕 Vincent-Joel Proulx, Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?, 23 *Berkeley Journal of International Law* 615, 643 – 53 (2005).

行使着有效控制或全面控制。[29]

在表述转嫁责任的具体标准时,有关学者使用了所涉国家对特定不法行为"不愿意和不能够预防"、"容忍和不愿意预防"、"庇护和支持"等不同的措辞。不过,比较一致的看法是,转嫁责任是以国际法上国家对其领土内活动的审慎义务(due diligence obligation)为法律依据的。[30]在"科孚海峡案"中,国际法院对该义务作出的经典表述是:一国不应"在知情的情况下允许其领土被用于从事有损他国权利的行为"。[31] 这一义务的逻辑依据非常清楚:根据主权平等原则,所有国家都应尊重其他国家的领土主权,并有义务采取适当措施来保护他国的有关权利。一旦违反上述义务,将产生该国的国际责任。[32]

(二)对转嫁责任的质疑

由此看来,将私人行为体从事的网络攻击"转嫁"到攻击行为发生地国,并据此追究该国的国家责任,这一主张似乎能够在现代国际法上找到明确的法律依据。但事实上,转嫁责任与违反审慎义务所产生的责任之间有着"差之毫厘,谬以千里"的重要区别。从概念上说,后一责任是基于国家有义务预防或惩罚私人行为体所采取的某些行为这一国际法义务,换言之,该责任的基础是有关国家的不作为;而转嫁责任则是将私人行为体的行为归因于所谓"庇护国",而使该国作为不法行为的行为国承担责任。[33] 更重要的是,这两种责任的形式和严重程度通常也有很大差别。

试举一例:在某些私人行为体从甲国境内对乙国发起武力攻击的情况下,如果甲国被认为违反了预防有关攻击的义务,那么乙国可以要求甲国承担相应的法律责任,但是,却不能因自身受到的武力攻击而对甲国行使武力自卫权,因为甲国并非该武力攻击的发起国;但如果有关武力攻击按照转嫁责任被归因于甲国,那么乙国就完全可以对甲国进行武力自卫。

美国在"9.11"事件后通过阿富汗战争对塔利班政府进行的军事打击,常常被认为是转嫁责任在国际实践中获得支持的一个重要例证。不过,尽管就这一具体事例而言,美国对塔利班政府采取军事行动的合法性得到了大多数国家明示或默示的承认,但未来类似的恐怖主义行为是否也构成《联合国宪章》第 51 条所指的"武力攻击"、受害国可否同样援引该条行使武力自卫权,在国际法上并未得到原则性的回答。相反,阿富汗战争有着明

---

〔29〕 David E. Graham, Cyber Threats and the Law of War, 4 *Journal of National Security Law and Policy* 87, 96 (2010); Nicolas Tsagourias, Cyber Attacks, Self-defence and the Problem of Attribution, 17 *Journal of Conflict & Security Law* 229, 242 (2012).

〔30〕 Timo Koivurova, Due Diligence, in R. Wolfrum (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, Oxford, 2008 -), online edition, <www.mpepil.com>, visited on 28 April 2014.

〔31〕 International Court of Justice Reports of Judgments, *The Corfu Channel Case* (The United Kingdom v. Albania), Merits, Judgment of 9 April 1949, p. 22.

〔32〕 2013 年出版的《关于可适用于网络战的国际法的塔林手册》(简称《塔林手册》),在其规则 5 中针对网络空间的行为提出:"一国不应在知情的情况下允许位于其领土内或处于其政府排他性控制下的网络基础设施被用于从事有害和非法地影响其他国家的行为。"See Michael Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge University Press, 2013), p. 26.

〔33〕 James Crawford and Simon Olleson, The Nature and Forms of International Responsibility, in Malcolm Evans (ed.), *International Law* (3rd edition), (Oxford University Press, 2010), p. 454.

显的特例性质,它对于今后类似事件的"先例效果"颇为值得怀疑。[34]

此外,一国领土不应被用于从事对他国有害的行为这一义务的具体内容还存在很大争议。本质上说,这一义务针对的是国家的特定行为(即采取必要措施对私人行为体可能在该国领土上从事对另一国有害的行为加以防范),而不是特定结果(即确保该国领土上不发生对他国有害的行为)。但是,国家究竟应当采取哪些具体措施来履行该义务并防止产生转嫁责任?根据一些西方学者的观点,应当予以评估的因素至少包括:该国是否通过立法将有关攻击确定为犯罪行为;该国是否积极地对从事有关攻击的个人进行了调查和起诉;如果该国缺乏相应能力对从事网络攻击的个人进行调查和起诉,其是否向他国寻求援助来履行相应的国际义务;该国是否积极地对受害国的调查和起诉予以了合作。[35] 但是,这些观点在理论上和实践中都尚未形成任何共识。

就网络攻击而言,国家要对利用本国领土范围内网络基础设施从事的各种行为加以有效监控,其技术难度远远超出对传统私人行为特别是军事行为的监控难度。同时,由于所谓"数字鸿沟"的存在,不同国家在网络空间的技术能力也存在极大差别。因此,依据何种标准对一国领土范围内发起的网络攻击实行转嫁责任,将是一个更为复杂和有争议的问题。正如有学者曾经指出的那样:"即使对于传统的动能武器攻击,国家在何种情况下构成'不愿意和不能够预防'也没有得到充分界定,确定网络攻击源头方面的挑战使得这一概念在网络空间的适用更为困难。"[36]

综上所述,尽管根据现有国际法规则,如果一国未能采取必要措施防止其领土被用于从事对他国有害的行为,那么该国的确应当对其不作为承担相应的法律责任,但以国家的此种审慎义务为由主张对从一国领土内发起的网络攻击实行转嫁责任,则不仅在法理上有"挂羊头卖狗肉"之嫌,也极有可能在实践中进一步加大国家之间的分歧和对立,因而是不可取的。

四 "自上而下归因"主张及其危险性

一种更为激进的观点认为,由于网络攻击的隐秘性,现有"自下而上"的应对策略(即在确定攻击源头包括攻击者身份的基础上,通过归因来确定国家责任)已被证明是不成功和低效率的;对国家安全政策制定者而言,知道"谁应负责"比"是谁干的"更为重要,为此应当采取"自上而下"的策略,使国家"对自其领土上或由其公民发起的攻击承担责任"。[37]

上述"自上而下归因"的观点,与转嫁责任颇有相似之处,即均主张基于网络攻击是从哪一国家领土发起这一事实来确定国家责任。但是,二者之间的区别也是不可忽视的。

---

〔34〕 Anna Oehmichen, Force Qua Terrorism: International Law in the Wake of 9/11, in Sanford Silverburg (ed.), *International Law: Contemporary Issues and Future Developments*, Westview Press, 2011, pp. 455 - 456.

〔35〕 David E. Graham, Cyber Threats and the Law of War, 4 *Journal of National Security Law and Policy* 87, 96 (2010).

〔36〕 Laurie Blank, International Law and Cyber Threats from Non-State Actors, 89 *International Legal Studies* 406, 416 (2013).

〔37〕 Jason Healey, Beyond Attribution: Seeking National responsibility for cyber attacks, http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF, visited on 20 February 2014, p. 1.

转嫁责任的基本理念是一国在未能采取有效措施阻止私人从该国境内对他国发起网络攻击时,而需要承担由此"转嫁"(归因)而来的国家责任;而"自上而下归因"主张则仅仅关注攻击是从哪国领土(或由哪国公民)发起,而对于所涉国家是否存在"不愿意和不能够"、"庇护和支持"等因素几乎不加考虑。

篇幅所限,本文对此主张仅略加讨论。早在 18 世纪中期,瓦特尔就正确地指出:"即使是那些进行了最佳管理的国家或者最为警觉、最绝对的主权者,也不可能随心所欲地雕塑其主体的所有行为,并使之时刻处于完美遵行该国义务的状况。因此,将公民所从事的每一不法行为都归咎于其国家或主权者是不公平的。不应泛泛地主张,由于某一损害是其他国家的一名成员所从事的,我们就受到了该国的损害。"〔38〕而在我们当前所处的互联网时代,鉴于确定网络攻击是从哪一国家领土发起的技术困难以及一国控制源于该国领土的网络空间活动的困难,瓦特尔所指出的问题更加彰显,因而"自上而下归因"的不合理性也更为显而易见。

还应注意的是,对网络空间的很多行为而言,确定其领土归属不仅存在技术上的困难,而且其结果常常具有很大误导性。例如,在 2007 年爱沙尼亚受到的大规模网络攻击中,技术专家们发现攻击来源于一个庞大的"僵尸网络",涉及位于 178 个国家的大约 8.5 万台电脑,其中绝大多数电脑是在被黑客入侵和操纵的情况下,无辜和毫不知情地卷入了有关攻击。〔39〕正是因为注意到了通过领土归属进行"自上而下归因"的危险性,美国学者霍利斯提出了如下质疑:"考虑到美国被视为网络威胁的最大来源国(中国其次),如果对某一攻击源头的调查最终确定为美国境内的一台电脑,美国应当对此承担何种责任?"〔40〕2013 年出版并产生了较大影响的《塔林手册》也指出:"(网络攻击)行为发生的地点和有关行为人所处的地点不影响是否产生国家责任的认定。"〔41〕总之,在迄今为止关于网络攻击归因问题的讨论中,"自上而下归因"是一种最为极端、充满强权色彩的主张,它朝着完全取消国际法上的归因要求迈出了极为危险的一大步。

五 结语:对网络攻击进行负责任的归因

网络安全已经成为世界各国的共同关注事项。受害国对网络威胁加以有效回应并使加害国承担责任,这无疑是一个正当的要求。但是,落实国家责任的前提是通过国际法进行负责任的归因,即在查明网络攻击相关事实的前提下,运用合理的法律标准来确定有关攻击与特定国家之间的内在联系,既不应使实际从事和控制网络攻击的国家逍遥法外,也

〔38〕 Emerich Vattel, *The Law of Nations or*, *Principles of the Law of Nature Applied to the Conduct and Affairs of Nations and Sovereigns* (Béla Kapossy and Richard Whatmore eds.), Liberty Fund, 2008, Book II, Chapter VI, para. 73.

〔39〕 Eneken Tikk et. al, *International Cyber Incidents: Legal Considerations*, CCDCOE, 2010, pp. 20 – 23; Nicolas Tsagourias, Cyber Attacks, Self-defence and the Problem of Attribution, 17 *Journal of Conflict & Security Law* 229, 233 (2012).

〔40〕 Duncan Holis, An E-SOS for Cyberspace, 52 *Harvard International Law Journal* 373, 401 (2011).

〔41〕 Michael Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge University Press, 2013), p. 33.

不应扩大国家责任的范围而伤及无辜。

与国际法所关注的大多数行为相比,网络攻击具有一些不可忽视的特殊属性,主要体现在:第一,绝大多数网络攻击的发起者是私人性质的黑客组织或个人,其与特定国家之间的联系往往难以确定;第二,网络攻击的隐秘性使得攻击者身份和源头的确定也极为困难。这些属性无疑加大了《条款》有关归因规则适用的难度。

正是为了克服这些挑战,一些西方学者提出了用"全面控制"取代"有效控制"标准、将私人行为体从事的网络攻击"转嫁"到攻击行为发生地国、实行"自上而下归因"等主张,其共同特点是放宽国际法上现有的归因标准,降低归因难度。

不难看出,网络攻击的特殊性主要体现在攻击源头、攻击者的身份及其与特定国家之间的联系等事实查明方面的问题;西方学者有关修改国际法上既有归因标准的主张,则可概括为试图"通过法律推定的方式克服这种事实上的不确定性"。[42] 然而,这并非解决网络攻击归因问题的正确途径。一个显而易见的问题是,这些主张在强调受害国维护自身网络安全的需要时,不同程度地忽视了其他国家受到无辜波及的风险。转嫁责任就是一个典型的例子:作为西方国家在国际法领域话语强权的体现之一,它大大突破了国家责任法上的现有归因规则,便于以网络攻击受害国自居的西方国家向其他国家(包括中国)施压甚至抹黑。鉴于西方国家近年来一再以各种捕风捉影的所谓"证据"指责中国支持网络攻击、渲染"中国网络威胁论",[43] 上述主张的片面性和危险性不应被低估。

事实上,国际法上有关归因规则的主要作用,在于明确某一行为能否根据国际法被定性为一国的国家行为,从而为认定该国是否承担国家责任奠定基础。所涉行为在事实方面的相对清晰,是有关归因规则得以适用的前提。就网络攻击而言,这类攻击在源头追溯等方面通常具有的不确定性应当通过国家间的互信和善意合作以及未来新的技术发展来加以解决,而不应成为一些国家根据其一己之私,动辄要求放宽甚至取消现有归因规则的理由。[44] 如果拨开网络攻击在事实查明方面的"迷雾",不难看到,这类行为在国际法上的归因与现实世界的其他行为并没有原则性的区别。

因此,回归到问题的本源,联合国国际法委员会《国家责任条款》中有关归因问题的一般规则(包括在国际法院判例中得到确立的"有效控制"标准),对于网络攻击的归因问题仍然可以充分适用,并且可以为负责任的归因提供必要的法律保障。而且,从正义原则的要求来看,正如有学者所言,恰恰是因为在确定网络攻击源头方面存在困难,才更有必

---

〔42〕 克尔杜拉·德勒格著:《别碰我的云:网络战、国际人道法与平民保护》,尹文娟译,载红十字国际委员会东亚地区代表处编译:《红十字国际评论——新科技与战争》,法律出版社 2014 年版,第 44 页。

〔43〕 例如,西方媒体曾广泛报道有关中国政府直接卷入针对美国的恶意网络攻击的"无可辩驳"的证据,但最终事实却并非如此。参见 Robin Geiß and Henning Lahmann, Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention, in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, CCDCOE, 2014, p. 626。

〔44〕 冷新宇在网络攻击归因问题上对美国政府和美国学者相关立场的评论可谓一针见血:他们之所以"更加倾向于降低责任的门槛,这个姿态背后的逻辑是易于指责对方,而对方因为技术能力远不如美国强大,所以抓不到美国政府承担责任的证据。"参见冷新宇:《网络攻击中国家责任的判别标准》,《西安政治学院学报》2014 年第 2 期,第 100 页。

要采取较为严格的归因标准,以防止其他国家被无辜地指责从事了网络攻击。[45]

总之,当前各种试图改变乃至抛弃国际法上现有归因标准的主张是既不可取也难以成立的。为了保证其他国家不会受到无辜波及,受害国必须正确地将网络攻击归因于真正的攻击者。因此,国际法上现有的归因标准不仅不应取消,相反还应通过加强国际合作来加以强化。

[**Abstract**] The attribution of cyber attacks under international law is an important and complicated issue, due mainly to the anonymous and private nature of most cyber attacks. In recent years, scholars from western countries have paid more and more attention to this issue, and have made various proposals to loosen and even abolish the existing attribution standards in international law, so as to facilitate the attribution of cyber attacks to states which arguably should be responsible. However, these proposals, while emphasizing the need of attacked states to ensure their cyber security, are largely biased and unfounded, in that they ignore the potential risk for innocent states to be unduly held responsible. The precondition of establishing state responsibility for cyber attacks is responsible attribution in accordance with international law so that, on the one hand, states actually engaged in cyber attacks are not be allowed to escape international responsibility and, on the other hand, the scope of state responsibility is not improperly expanded to negatively affect innocent states. In this respect, the attribution rules in the UN International Law Commission's 2001 Articles on State Responsibility have an indispensable role to play in the attribution of cyber attacks under international law.

(责任编辑:廖 凡)

〔45〕 Marco Roscini, World Wide Warfare-Jus ad bellum and the Use of Cyber Force, in Armin von Bogdandy and Rudiger Wolfrum (eds.), 14 *Max Planck Yearbook of United Nations Law* 85, 100 (2010).