智能社会研究

（双月刊）

2024 年
第 3 期
2024 年 5 月 10 日出版

2022 年 11 月 10 日创刊

总第 10 期

目　次

论文

研究报告

译文

书评

CONTENTS

THESIS

RESEARCH REPORT

TRANSLATED TEXTS

BOOK REVIEW

归因法:网络攻击来源归因规则*

德尔伯特·特兰 著**

裴 轶 强心语 译***

摘要:近年来,国际层面的网络攻击行为日趋增多,典型网络攻击如"震网病毒"事件、DNC 黑客攻击事件等。而网络攻击的溯源,即归因问题,始终是网络安全领域的重点、难点问题。长期以来,学术研究集中于突破归因的技术瓶颈,然而,本文认为这一研究路径系南辕北辙。网络攻击的应对难点不在于无法发现攻击痕迹,相反,当前并不存在技术障碍,真正的难点在于难以归责。构建一套法律体系(归因法)以认定责任主体、确定举证责任、解决国际争端,才是应对网络攻击的合理进路。本文通过研究现有程序规则,包括对抗制和纠问制的特点、举证责任、证明标准、国家责任理论以及关于提供保密证据的规则,阐述了如何构建一套法律体系来识别网络攻击来源。此外,通过对比研究既有的国际争端解决机构,本文探讨了归因法框架下的机构设置。归因法的探索,于当前的互联网时代有利于进一步丰富、完善国际法,维护网络空间国际秩序。

关键词:网络攻击归因 法律框架 国际法庭 国家责任 证据规则

---

* 本文原题为"The Law of Attribution: Rules for Attributing the Source of A Cyber-Attack",原文见 https://openyls.law.yale.edu/bitstream/handle/20.500.13051/7830/DelbertTranTheLawofAttrib.pdf?sequence=2,经授权翻译发表。论文原无摘要、关键词,中文版摘要系译者总结,关键词系编辑部根据论文大意总结而成,特此说明。

** 德尔伯特·特兰(D. Tran),耶鲁大学法学院。

*** 裴轶,北京理工大学法学院。强心语,北京理工大学法学院。

一、引言

网络攻击[①],尤其是大规模网络攻击,有可能在一些关键领域造成重大而广泛的危害。这些攻击包括针对核基础设施、商业实体、政府基础设施以及互联网基础设施本身的攻击。克拉珀指出,2013 年,在美国的国家威胁清单上,网络攻击威胁程度超过了恐怖主义。而且,对 DNC 的黑客攻击表明,此类网络攻击并没有减弱的迹象。网络攻击之所以持续不断,一方面可能是其成本相对较低(Boerbert, 2010),另一方面则在于其攻击源难以追踪。因此,网络攻击为国家行为者提供了肆无忌惮地从事恶意活动的绝佳场所,而不必担心归因或报复。

长期以来,国家归因[②]问题一直是网络安全领域的一个难题。匿名性是互联网的标志和优势之一,但同时也是这一令人困惑的问题的根源。尽管之前的大部分学术研究都集中在归因问题的技术障碍上,但本文试图重新审视这一问题,关注法律而非技术如何解决归因问题。技术归因放大了一个狭义的问题,即人们是否有可能纯粹通过技术手段保证将攻击归于责任主体。但是,法律学者和法律从业者都知道,责任问题很少仅通过单一的技术手段或证据形式来决定,责任的判断往往也不取决于确凿的有罪声明。[③] 法律判决往往基于大量直接或间接证据的积累,这些证据从整体上描绘了恶意行为的责任。同样的逻辑也适用于网络安全和归因。因此,真正的问题是如何构建一个证据和程序规则完善的法律体系。

尽管这一网络安全问题出现在政策与技术的交叉点上,但它也提出了一

---

① 本文所指的"网络攻击",既包括网络战争,也包括没有发生武装冲突,但仍应受到某种形式制裁的网络攻击,即使它们不值得以武力作为回应。

② 本文的"归因"一词,指识别网络攻击背后的行动者的过程。

③ Desert Palace, Inc. v. Costa, 539 U.S. 90, 99-100 (2003); Siegert v. Gilley, 500 U.S. 226, 236 (1991); Holland v. United States, 348 U.S. 121, 140 (1954).

个特别适合法律解决的问题。如果从根本上说法律涉及各方据以裁决争端的制度,那么网络攻击的归因问题正是法律可以解决的争端。法律程序还赋予结果以合法性,并以更强的制度影响力将这种解决方式正式化。在一个更具争议性和政治化的环境中,所有的报道都会被怀疑带有党派偏见,因此通过法律程序得出的结论更难被视为纯粹的“假新闻”。此外,一旦知道了网络攻击的罪魁祸首,就可以研究他们的战术和方法,威胁进行报复,采取反制措施纠正攻击行为,并建立和巩固适当的行为规范。但是,由于无法确定攻击来源,所有这些可能的应对措施都会受挫。在回答了一个关键的必要问题后,归因使法律得以出现:如果有的话,哪个国家应对网络攻击负责?

实际上,根据国际法,归因法将使针对另一个国家的某些制裁合法化,包括《联合国宪章》第五十一条——可能使用军事力量进行自卫。反之,如果一个国家未能证明其归因主张,那么根据国际法,它所实施的任何制裁都可能变得不合法或无效。归因的法律框架将提供一个重要的基石,使制度能够限制和纠正网络攻击所造成的伤害。

本文分几个部分来构想归因法。第二节首先回顾了归因问题:近期网络攻击造成的威胁、对此类攻击缺乏问责的问题,以及学者和政策制定者普遍认为阻碍网络攻击归属的一般技术障碍;然后,反驳了长期以来无法确定网络攻击归属的说法,指出归因的技术问题远比法律要求的范围狭隘,并说明归因如何反映了一个更容易解决的法律问题。第三节设想了国际归因法的框架:首先,它概述了评估国家对非国家行为者行为的责任承担的背景和重要考虑因素;其次,提出程序和法律规则,不仅是为了设想归因法的外观,而且是为了设想其程序规则如何与其实质内容建立适当和合理的关系。第四节讨论了归因法中最困难的因素:国家加入或参与这种法律框架的动机。虽然评估国家激励措施,涉及国际关系性质、国家间合作、国际秩序遵守等基础性问题,但是本文并不侧重讨论上述宏大命题;相反,本文将通过回顾、分析既有国际法庭的实践,探索归因法框架下的国际裁决模式。

二、国家归因问题

由于无法确定网络攻击的源头,行为者可以肆无忌惮地实施攻击,从而使制定国际法或条约来规范这种有害行为的努力失效。即使当前正式法源难以解决网络攻击,但是各国仍须确定攻击的来源,以便做出应对,包括制裁攻击者及其行为。换言之,归因是任何试图对恶意网络攻击实施规则或限制的关键先决条件。

目前的国际制度几乎没有明确规范或控制国家在网络黑客领域的行为,没有任何国际法律或条约明确规范网络攻击。虽然有学者指出武装冲突法的潜在适用性(Hathaway, Crootof & Levitz et al., 2012),但迄今为止,在应对网络攻击时,武装冲突法显然尚未被引用过。鉴于国际关系领域普遍存在不确定性,各国可能会规避风险,在对其他国家采取法律和外交行动时,对国际法的创新解释犹豫不决。因此,缺乏归因限制了制度和法律解决方案,使网络领域长期处于无法之境,未来网络攻击的范围和规模仍有升级和不确定性的可能(Condliffe, 2016)。

从更广泛的国际关系理论角度来看,归因有助于国际法的发展。很容易理解为什么自由主义理论家需要对网络攻击者进行归因,并以法律制度规制之,因为网络攻击对国内实体的附带影响为国内行为者创造了大量动机,鼓励国家行为者加入遏制此类攻击的国际框架(Moravcsik, 2014)。但即使是国际关系现实主义者也会承认,即使在没有总体国际法的情况下,国家也有必要通过归因来维持秩序。现实主义者的传统口号否认任何凌驾于国家之上的中央权威,并认为国家总是在寻求权力和促进自身利益(Mearsheimer, 2001)。虽然这种对国际关系的理解对国际合作或国际法构成了初步障碍,但现实主义逻辑并不完全排除合作,其中一个反驳理由就是互惠(Keohane, 1986)。互惠论的倡导者从博弈论出发,指出理性、自利的行为体在合作或叛

逃之间做出选择时,在反复进行博弈的情况下会最优化地选择合作。之所以选择合作,是因为博弈者在未来的“博弈”(或互动)中,会根据先前迭代中的决定对他人的行为进行惩罚或奖励(Axelrod, 1984)。因此,即使假定国家行为采用现实主义框架,互惠性也能使国际法在合作过程中形成,因为国际关系往往涉及国家间的重复互动,这些互动构成了国际关系博弈的“迭代”。

然而,互惠论假定国家可以准确地惩罚或奖励彼此的行为。虽然反措施可能促成这一互动,但正确使用反措施与正确归因密不可分。归因不仅是国家制裁负有责任的恶意行为者的基本要求,而且适当的归因对于国家声称合法使用制裁或反制措施也至关重要。法律的作用不仅在于决定冲突的结果,还在于使第三方对冲突结果的决定合法化(Weber, 1968)。法律的合法化功能在国际法和国际关系领域尤为明显,因为在这些领域,国家缺乏通过武力强制遵守的总体权威(Goldsmith & Posner, 1999)。因此,在互惠制度中,归因具有双重功能:确定不法行为者;使对第三方的正式或非正式制裁行为合法化。因此,归因问题是任何限制使用网络攻击的法律制度的关键性第一步。

(一) 为何归因如此困难

长期以来,网络攻击追踪溯源是网络安全领域的重点、难点问题。目前的许多学术研究都接受了这样一种传统观点,即互联网的技术架构使得归因成为一个极其困难的问题。归因问题引发了专家学者浩如烟海的讨论,如辛格等人(Singer & Friedman, 2014)将归因问题描述为网络领域“也许最棘手的问题”。

由于多种原因,很难将网络攻击归因于其源头。

首先,互联网的结构设计和跨网络信息传输的性质使归因变得复杂。当用户希望通过互联网进行某些操作时,例如在油管(YouTube)上搜索柯基犬的视频时,用户的计算机需要找到一种方法,与托管 YouTube 内容的机器进

行通信,并让该机器将柯基犬嬉戏的内容发送到原始机器上。这是如何实现的?每台机器都会被分配一个互联网协议(IP)号码作为“地址”(Grimmelman, 2017),这个地址通常是由互联网服务提供商或网络分配的,用户的电脑一般会从本地互联网路由器的地址开始,由路由器将请求转发到更广阔的互联网。

要将用户的请求发送到载有柯基犬的机器上,用户的机器就需要知道该机器的地址。用户的机器如何找到这个地址呢?从用户的角度来看,他或她可以在搜索栏中输入“www. youtube. com”。在机器端,这些可识别的名称会通过域名系统转换成机器地址或 IP 号,域名系统可以被视为一个将网站名称与 IP 号码相匹配的全局目录。一旦用户的机器知道了拥有大量柯基犬视频的网站地址,下一步就是将来自用户计算机的数据(从 YouTube 获取内容的请求)传输到 YouTube 上,YouTube 再将请求的数据发送到用户的计算机上。我们可以简单描述一下这个过程:请求(用户在地址栏输入的文本或点击网站链接的动作)在超文本传输协议(HTTP)层被转换成数据(数字),然后将数据传递给传输和网络层。在传输层,数据被分解成数据包大小的数据块,每个数据块都包含其目标地址,就像通过邮件发送的小信封。这些数据包在通往目的地的途中被传输到整个网络中的各个服务器(想象一下长途旅行中成千上万个可能的中转站),直到到达最终目的地,并被重新组合成来自 YouTube 的原始数据请求。在有 YouTube 内容的机器上,当 YouTube 将信息发送回用户时,这一过程会以相反的方向重复进行。

不过,两台计算机之间的这种通信过程并不要求知道请求(或黑客)的来源。YouTube 知道将其响应发送到哪里的唯一原因是,原始请求有意包含了它的地址,这样 YouTube 就能将数据发送回来。其他类型的活动,如向 YouTube 上传视频,则不需要在发送的信息中嵌入返回地址。因此,不需要数据传输的原始来源,我们的机器就能参与在线活动。我们通过互联网发送的数据包只需要知道它们的目的地,而不需要知道它们的来源。与邮局不同的

是,我们不需要返回地址,因为任何无法通过的数据都会丢失,人们只需一次又一次地尝试另一个请求,直到它通过为止。

其次,用户可以利用一些技术或程序应用来隐藏他们的网上活动痕迹(Greenemeier, 2011)。用户在互联网上进行的任何活动都会被记录其 IP 地址,因此用户可以选择使用代理服务器或"洋葱路由工具"来掩饰自己的 IP 地址(Feigenbaum, Johnson & Syverson, 2007)。参考邮局的比喻,为了掩盖寄信来源,寄件人可以把信交给朋友,让他们通过不同的邮局寄出,而非最近的邮局。寄件人还可以通过写下一个假的回邮地址来"欺骗"原始地址(Tanase, 2003)。一项实验证明,近三分之一的互联网用户可以在不被发现的情况下伪造他们的源 IP 地址(Beverly, Berger & Hyun et al., 2009)。

再次,即使可以重新设计互联网,对互联网上发送的每个数据位的源 IP 地址进行验证(Gallagher, 2013),这些地址也只能实现识别攻击源机器而非攻击者。攻击者可能会窃取或入侵他人的设备,或利用多人使用的公共设备或网络来进行网络攻击,这种情况数不胜数。例如,Mirai 僵尸网络攻击涉及恶意代理利用成千上万的其他设备,这些设备被代理收编为攻击工具(Meyer, 2016)。

最后,即使克服了所有技术问题,并确定是某个人发动了网络攻击,主权国家是否应对该个人的行为负责的问题依然存在。换句话说,网络攻击也提出了一个问题:国家何时可以为非国家行为者的不法行为负责?虽然这一法律难题最常出现在恐怖分子或集团的情况下(Clapham, 2015),但对黑客和网络攻击者来说,这个问题同样突出,因为他们通常没有制服或旗帜来表明他们是以任何特定国家的名义行事的。需要注意的是,这并不是归因问题的技术障碍,而是法律障碍。这一特别关切突出表明,有必要制定一种法律制度,以解决归因所带来的问题。

互联网的结构设计、掩饰在线活动的工具、仅能追踪于机器的限制以及将个人行为归责于国家的限制,这些因素构成了技术和法律方面的诸多障

碍,经常被认为是建立网络攻击监管法律制度的障碍(Waxman, 2011)。虽然以往的学术研究通常将归因的技术问题视为一个难以解决的难题,最好留给工程师去解决,但最近的学术研究认识到,归因问题可能并不是一项不可能完成的任务(Rid & Buchanan, 2014)。

(二) 技术归因问题是一种误导

尽管归因存在诸多技术障碍,但技术问题只是一种误导。这些技术障碍只是阻止我们得出一个非常狭隘的结论,即我们何时可以绝对肯定某个行为主体对网络攻击负责。然而,法律几乎从未按照绝对肯定这一几乎不可能达到的高标准来运作。即使是美国刑法,其著名的有利于被告的高举证责任也只要求在定罪前没有合理怀疑,而不是要求完全没有怀疑(Whitman, 2005)。从根本上讲,归因问题的核心是责任问题,而责任问题从根本上说是一个法律问题。即使在没有绝对因果关系确定性的情况下,法律也经常回答这个问题。因此,本文通过提出两个要点来解决归因问题:

第一,尽管归因存在障碍,但计算机科学家已经开发出一系列工具来追踪网络攻击,根据经验,大规模的国家攻击往往会留下足够的痕迹(或间接证据),引导鉴证专家找到攻击源。

第二,法律并不要求保证确定无疑,而只要求有足够程度的确定性,即某人应承担责任;无论是合理怀疑标准,抑或优势证据标准,法律已经构建了一套可应用于实践的归责方法。

一旦这两点确立,问题就不再是网络攻击是否可以归因,而是国际社会如何构建一套法律体系,制定必要的证据规则、程序、举证责任等。

关于第一点,强调归因的技术性质自然吸引了那些具有更强技术专长的人的兴趣,计算机科学家也相应地开发了一套工具来归因网络攻击。虽然这些方法都不可能单独提供万能的解决方案,但每种方法都提供了鉴证技术,可能会给任何特定案件带来一些启示,而且累积起来确实有可能在一定程度

上确定归因。就像可以通过鉴证证据(搜索指纹、识别笔迹等)追踪匿名信一样,也有办法利用间接证据来确定数字信息的传输和随后的网络攻击。本文所探讨的网络攻击——可能引发或要求国家做出反应的高调网络攻击尤其如此。由于其范围或规模更大,此类攻击往往更有可能留下痕迹。更大规模的行动也需要更多的资源,从而限制了有能力发动此类网络攻击的潜在对手的范围。

事实上,调查人员利用这些技术找出了最近两次重大网络攻击的罪魁祸首:“震网病毒”(Stuxnet)事件和 DNC 黑客攻击事件。下文将依次回顾每一次攻击,描述取证和间接证据的积累如何实现这些攻击的归因,从而证明归因的技术问题被夸大了这一讨论现状。

1.“震网病毒”(Stuxnet)事件

从 2009 年开始,伊朗的铀离心机开始失灵,且无人知晓原因。在一年的时间里,伊朗 6000 台离心机中有近 1000 台被摧毁。2010 年夏天,白俄罗斯的一家电脑安全公司受聘对伊朗的电脑进行故障排除,这些电脑一直神秘地死机。在调查中,这家公司偶然发现了一系列文件,这些文件后来被称为“震网病毒”(Stuxnet)。“震网病毒”被认为是“世界上第一个数字武器”(Zetter, 2015)。这是一个复杂的恶意软件,旨在渗透伊朗安全的核设施,感染操作核离心机的工业控制器,并通过操纵离心机内的压力水平和转子速度来摧毁这些离心机(Langner, 2013)。该病毒的设计意图是缓慢而渐进地造成这种破坏,从而降低被发现的可能性;它甚至包括一个操纵伊朗传感器的功能,以假装被操纵的功能在正常工作。

尽管人们试图掩盖其来源,但专家们得出的结论是,“震网病毒”是美国和以色列联合制造的。在“震网病毒”事件中,这一信息几乎是决定性的,因为很少有国家有动机和手段来攻击伊朗的核离心机。此外,攻击的规模往往会透露攻击者的信息。虽然高级持续威胁是最具威胁性的网络攻击形式,但其优势也成为其弱点。这是“震网病毒”攻击的另一个线索——代码中有四

个“零日漏洞”(对于私人黑客来说,这些漏洞的转售价值高达数百万美元),这再次暗示了攻击背后有强大的火力支持,几乎可以保证这种攻击来自某个国家。最后,细小的线索往往可以确定攻击的源头。通过“震网病毒”的代码,调查人员能够根据引用西门子设备的名称和 ID 编号发现其主要攻击目标——被操纵的目标是工业离心机控制器。鉴于目标的狭小性和投入的巨大资源,很容易推断出背后的国家。

2. DNC 黑客攻击事件

DNC 黑客攻击事件是国家行为者实施重大攻击的最新例证。美国情报部门坚称 DNC 黑客攻击来自俄罗斯。美国表示,尽管这一认定也依赖于机密情报,但在调查过程中咨询了几家私营网络安全公司,并提供了公开证据,证明攻击是俄罗斯所为。例如,他们注意到,DNC 黑客使用的渗透工具和编码与已知为俄罗斯联邦安全局(FSB,前身为克格勃)工作的俄罗斯黑客使用的工具和编码相同。这些分析人员还将 DNC 黑客攻击事件与 2015 年对德国议会发动攻击时使用的同一个 IP 联系起来。安全专家注意到用西里尔字母留下的数字签名。此外,安全专家注意到,DNC 黑客攻击事件在俄罗斯节假日期间停止了行动,他们的工作时间与俄罗斯时区一致(Meyer, 2016)。

当然,这些间接证据并非完全确凿,其中一些信息有可能是栽赃陷害。但法律体系长期以来一直能够分配惩罚和责任,即使责任仅来自间接证据。在 DNC 黑客攻击事件中,虽然可能有人植入了西里尔字母签名等线索作为障眼法,但黑客组织完全在俄罗斯时区和节假日内协调行动作为其伎俩的可能性要小得多,因为这种行动的协调成本很高,而且复杂程度非同寻常。最终,就像在刑事案件中一样,可以积累足够的证据来确定攻击的来源。

因此,问题不在于确定攻击的来源。挑战在于如何让其他国家相信,源头已经被正确识别。希望采取反制措施的国家需要让其他国家相信其归因的准确性,以确立其反制措施的合法性。出现这一问题,可能有两个主要原因:归因可能基于通过国家间谍活动或情报收集工作收集的数据,而国家可

能希望对这些数据保密(Sanger & Fackler, 2015);当国家有可信的事实依据来认定攻击行为时,它们可能不希望披露这些证据,因为网络攻击者可以从这些错误中吸取教训,避免在未来留下同样的痕迹(Brenner, 2007)。

虽然这些努力最终是基于间接证据的积累,但在许多法律领域,间接证据为支持法律判断提供了足够的可信度。例如,在侵权行为中,严格责任和事实自证原则表明,决定性的问题可能并不总是谁实施了某一行为,而是我们如何追究某一特定个人或实体的责任。而在不同情况下适用不同的责任标准,反映了法律在建立适当框架以解决此类冲突方面的灵活性。因此,在设计归因法时,这些问题将涉及对其他法律领域所援引的证据和因果关系的一般标准的一些调查。在这些领域中,法院已经使用了法律工具来建立足够的信任度,以将责任归于行为人。

三、归因法

既有的法律和程序体系包含了大量可借鉴的材料,提出了许多制度特征和设计,供我们在勾勒归因这一法律制度时参考。国际归因法在设计其结构和组成部分时必须解决几个问题。本节将首先讨论是否有可能制定一套跨实体法的归因规则,以及与此相关的问题,即这一归因法将用于何种目的。这些答案为该体系的整体结构和框架奠定了基础,而整体结构和框架将涉及设计选择,如是否优先选择对抗制而非纠问制,以及制度设计的其他关键方面。然后,本节将讨论界定实体法界限的关键程序规则。这些规则包括举证责任、评估国家对非国家行为者的行为所负责任的标准,以及证据和管理敏感性的规则。虽然这些规则是程序性的,但它们对案件的潜在结果有着巨大的影响,因此必须制定适当的程序,以确保兼顾程序正义与实质正义。

(一) 跨实体法的归因法

是否有可能制定一部跨实体法的归因法,即无论归因所证明的法律或政

治行动如何,该法的规则都能适用,这是构建归因法首先要解决的问题。举例而言,归因法可能会根据应对网络攻击所采取的反制措施的严厉程度而改变其严格或灵活的标准。

从广义上讲,归因法背后可能有几个目的,通过归因的法律主张,可能有理由采取几类后续制裁或应对措施:第一,在确定攻击的归属后,可以对网络攻击的责任国进行负面的经济惩罚,如经济制裁;第二,被归咎于发动攻击的国家可能会被剥夺积极利益,因为它将无法参与未来的国际条约或协议;第三,归因可以成为黑客反击措施的理由(Holzer & Lerums, 2016);第四,归因可以成为军事回应的理由。这些可能的归因对策可进一步分为两类:单边行动或多边行动(表1)。

表1　　归因对策的进一步分类

	单边行动	多边行动
拒绝外交接触/协议	拒绝参与目标国家可能寻求的贸易协定、条约或其他双边协定;拒绝外交接触	拒绝加入更广泛的贸易协定或条约
负面经济惩罚	经济制裁;废除现有的贸易协定	多边制裁机制
网络对抗措施	反击黑客	联合制造网络攻击,如“震网病毒”
军事对策	有针对性的军事打击等	联合军事力量

虽然这些选择提出了国家在网络攻击归因后可能采取的一系列实际和政策应对措施,但就制定归因规则而言,这些应对措施对我们如何设计归因规则的影响,可从两个主要方面加以考虑:单边行动还是多边行动;惩罚的“严重”程度。

第一个问题,归因是用来发起单边行动还是多边行动,实际上对归因法的整体理论影响相当小。这主要是因为归因法背后的目的在单边和多边反应中通常是一致的——在国际社会看来,归因是惩罚的正当理由。无论一个国家是否希望通过自己的单边行动或多边行动来惩罚网络攻击者,归因都是

为了在国际社会第三方的眼中使这种行为合法化。

唯一的例外是在多边承诺无法保证的情况下,受害国不仅需要说服其他国家报复是合理的,而且需要说服其他国家参与报复。这些情况可能会使归因法理论向更严格的要求倾斜,因为其他国家可能会要求对归因有更大的信心,然后才会投入自己的资源来应对没有直接影响到它们的网络攻击。

对信任差距的担忧有两种回应:直接遭受攻击的国家对正确识别攻击来源有着极高的兴趣,这意味着信任差距可能并不取决于归因的确定性,而更多地取决于国家加入多边行动的一般动机;仅仅存在一个多边机构,要求非受害国做出反应,似乎就意味着这种机构联系的来源本身就足以促使这些国家加入实施惩罚的行列,而无须更严格的归因制度的额外保证。例如,如果国家有义务对网络攻击做出多边回应,那么作为一个法律问题,或作为确保未来合作的理性利益问题,它们受到约束这一事实可能足以证明一个国家有理由决定与受害国一起对网络攻击来源做出多边回应(Loomis, 2008)。因此,单边/多边的区别很可能不会改变制定一套跨实质性归因规则的可能性。

对网络攻击可能采取的反制措施的严重性可能会对单一的跨实体归因法造成更重要的影响。更严重的反制措施可能需要更严格的程序规则,使这些规则取决于一国应采取的反制措施。虽然这一直观原则在抽象情况下似乎是正确的,但在网络安全的具体背景下以及上文详述的国家可能采取的应对措施中,这一原则值得探讨。根据可能采取的反制措施的严重程度,应对措施可大致排序如下(从高到低):军事力量、网络反措施(或“黑客反击”协议)、经济制裁和外交惩罚。

虽然军事力量涵盖各种可能的行动,但这些行动仍可归类为应对网络攻击的最严厉的可能对策。鉴于军事行动的一般成本和冲突升级的危险(Nye, 2021),各国越来越少选择动用军事力量。此外,国际法明确规定全面禁止使用武力。尽管如此,政界人士和军方领导人都表示,可能会对外国网络攻击做出军事反应(Williams, 2016);在对黑客攻击采取可能的反制措施时,特别

是当网络攻击严重到足以被归类为武力行为时,这仍是保留选项(Schmitt,1999)。军事行动的幽灵很可能会引发国际社会的高度关注,并对正确确定网络攻击来源的信心提出极高的要求。考虑到2003年美国因妄称伊拉克拥有大规模杀伤性武器而发动的对伊拉克的入侵已声名狼藉,这一点尤其如此。

另一类反制措施,即网络黑客攻击(Chulov & Pidd, 2011),也可能达到与使用军事力量相关的严重程度。虽然网络黑客攻击可能涵盖比军事力量更广泛的一系列活动,但一些学者认为,网络攻击有可能造成与传统动能军事攻击一样大的破坏,有时可被定性为国际战争法下的武力(Graham, 2010)。如果网络黑客攻击在某种程度上被认为等同于国际军事力量,那么这类反制措施也可能需要一套特定的程序规则,以证明在这些高风险情况下的归因是合理的。

对更严格的程序规则和更严肃的反制措施的需求,并不会导致制定一部关于归因问题的跨实体法的计划失败,因为法律可以通过修改相关的程序规则或要求来引发特定的惩罚。以美国的版权法进行对比,其中的条款可以根据侵犯版权行为的严重程度,规定民事赔偿、加重民事赔偿或刑事责任。这三种对侵权行为的惩罚都依附于版权法的一般体系,但具体的惩罚取决于被告的违法意图。回到归因法,其可以根据应对网络攻击的救济措施的严厉程度,来调整举证标准,这并不影响归因法的构建可能性。

鉴于有可能制定一部关于归属问题的跨实体法,下一步就是概述这一体系的主要特征,首先是将形成整个法律结构的基本要素。

1. 对抗制或纠问制

一个需要面对的主要设计选择是,归因法是在对抗制框架下运行(如美国、英国的法律制度)(Strier, 1992–1993),还是在纠问制框架下运行(如大多数欧洲、亚洲和南美洲国家的法律制度)(Kötz, 2003; Langbein, 1985; Tomlinson, 1983)。选择对抗制框架还是纠问制框架,在很大程度上反映了

法律程序的理念,而这一理念又决定了该系统的规则和整体设计。对抗制法律框架的主要特点是,公正的决策者(法官或陪审团)根据当事人及其代理人提供的证据和论据对争议做出判决(Hay & Spier, 1997),这种制度依赖于对抗双方提供证据和论据。而纠问制框架则将法官定位为主要的事实认定者和调查者,当事人及其律师在收集证据方面发挥的作用却相对有限。

虽然许多纠问制诉讼制度仍保留了一些“对抗”特征,但将重点从当事人转移到法官对整个法律制度产生了关键性的连锁反应。正如约翰·朗宾(J. Langbein)所指出的,德国法院的纠问制设计极大影响了德国民事诉讼程序的其他方面,如为诉讼的各个阶段设定了更为灵活的顺序。相比而言,对抗制为原告和被告陈述或参与诉讼的各个环节设定了固定的顺序,而“在德国的诉讼程序中,法院会对整个案件进行审理,不断寻找案件的关键点,即可能决定案件胜负的法律问题或事实问题”。因此,纠问制诉讼程序的灵活性使得审判过程具有连续性,可以通过多个时间点对问题进行重新审理。此外,朗宾还指出,纠问制对证人以及他们在法庭上提供事实或证据时所扮演的角色有重大影响。在对抗制中,提供证人、准备证人、直接质证和交叉质证主要由双方负责。在纠问制诉讼制度中,法官负责传唤证人并在法庭上主导对他们的询问。这只是对抗制诉讼制度或纠问制诉讼制度在影响法律机构民事诉讼程序的整体特征方面的两个例子。因此,在构建归因法时,应从一开始就确定这一制度选择。

无论哪种制度,都各有理由。主张对抗制的人赞美对抗制盘问的优点,认为它是揭露谎言的最有力工具;在这种制度下,当事人专门负责提出和获取证据,而事实认定者专门负责从给定的证据中得出推论,这种制度效率较高(Marcus, 1992);他们还指出纠问制法官可能会预先判断案件的结果,忽略可能进一步揭示争议的关键证据或论据。主张纠问制的人则指出,过度的立场之争和作秀可能会使对抗制程序最终扭曲事实和证据(Frank, 1949),并使该制度偏向于那些拥有更多资源和更优秀律师的当事人(Hadfield, 2000)。

在这些反反复复的争论中,学者们采用了许多理论和经验模型来检验这两种制度的有效性。一些模型表明,这两种制度在产生准确或理想结果的能力上差别不大(Froeb & Kobayashi, 2001);而另一些模型或研究则认为,结果取决于个人所衡量的特定数据(Lind & Tyler, 1988; Parisi, 2002)。通常认为,虽然两种法律模式之间的争论由来已久,而且在短期内也很可能无法解决,但每种模式都有其适合运作的情形。朗宾尽管赞成纠问制的普遍效力,但他承认对抗制在刑法中可能有其独特的理由。

本文认为,对抗制模式更适合归因问题,概因纠问制的优势在国际背景下化为乌有。首先,纠问制依赖于一个预先存在的、中央集权的司法当局,它可以被信任为客观地寻求真相,而国际领域缺乏这样的机构;其次,由于归因往往依赖于技术证据,而证据往往是通过间谍活动或其他秘密情报收集活动获得的,因此在归因争端中当事方几乎总是最有能力获得和提出此类证据。

纠问制依赖司法机构来推动其程序,这在很大程度上是国际背景下的一个弱点。虽然确实存在一些国际法院,但这些法院的管辖权并不完整,或者是专门处理专业问题,无法涵盖这里提出的归因问题。国际法院(ICJ)是当前国际框架内可能存在的最佳司法选择,因为它一般会广泛考虑主题事项(Thirlway, 2016)。然而,即使是国际法院,其影响力也是有限的;只有在国家同意适用国际法院的情况下,国际法院才能解决国家间的争端。例如,在国际法院对尼加拉瓜诉美国一案做出不利于美国的裁决后,美国退出了国际法院的强制管辖(Kahn, 1987)。此外,国际法院的强制执行权也受到限制。纠问制假定了对主导大部分诉讼程序的司法机构合法性的高度信任,而在国际法背景下,国家主体不太可能参与一个更多由法院而非当事人本身主导的程序。

其次,纠问制假定法官有足够的专业知识来寻找解决案件的相关信息,包括知道应该寻找哪些(专家)证人以及如何对他们进行询问。但在归因问题上,这种能力推定可能不成立。鉴于网络攻击和归因的技术性质,当事人

有理由认为,由一个普通法院来牵头提供事实和证据不太可靠。即使可以通过由具有技术专长的法官组成的合议庭进行诉讼来解决这一问题,但这些法官在确定特定争议中的确切事实方面所处的相对地位仍会有所欠缺。当涉及他们在确定某一特定争端中有争议的确切事实方面的相对立场时,这些法官仍然显得力有不逮。法官可能不那么熟悉每个国家的网络能力和行动,也不熟悉可能支持一国指控另一国对网络攻击负责的基本证据。由于围绕网络攻击和网络安全的许多证据也可能来自秘密情报行动(Connolly, 2016),因此对抗制将更为合适,因为当事方本身最有能力提出或决定何时提出某些敏感证据。

对抗制为归因法提供了一个总体框架。这种制度将有一个公正的裁决者,并将在很大程度上由当事人在法律论证和提供事实与证据两方面驱动。因此,这种体系将包含与美国法律体系类似的程序排序,从启动到发现再到提出论据,其中的论据将围绕当事人各自的论证阶段进行安排。

2. 证明标准

有了对抗框架,接下来要做的就是确定对抗双方如何成功证明其归因主张。换言之,就是确定成功证明主张的举证责任。“举证责任”一词通常指两个不同的概念:说服责任和举证责任(证据)(Fleming, 1961)。由于本节大部分内容涉及在对抗制诉讼中当事人的举证责任,因此此处使用的“举证责任”一词指的是说服责任。广义地说,说服责任涉及裁判者在收到案件中提出的所有相关事实和论据后,对得出法律结论的信心。

举证责任也许是对案件实体结果影响最大的程序规则。罗伯特·贝尔顿(Belton, 1981)将举证责任描述为“美国法律体系中最重要的程序概念之一”,因为“它通过指示事实认定者对特定类型案件的事实结论的正确性应具有的信心程度,帮助实施实体法”。毕竟,根据当事人的举证责任,同一套事实可能会导致完全不同的结果。

一些学者批评举证责任之间的分级在法官或陪审团的心目中没有明确

的区别。然而,这些批评都是在理论层面提出的;支持这些论点的经验证据,往往是基于要求个人对各种举证责任进行抽象定义的调查。但是,关于这些举证责任含义的调查答案可能并不是结论性的,因为这些术语的含义在实践中总是结合具体的事实来理解的(Kaplow, 2012)。因此,对"清晰且有力"的特定含义缺乏共识可能并不反映事实认定者在特定案件中的实际共识。在特定案件中,一组事实认定者可能都同意一方当事人的证据已确立了"清晰且有力"的证据。此外,考虑到举证责任在实践中对案件结果所产生的经验性影响,这些否定举证标准作用的论点似乎并不具有说服力(Devine, Clayton & Dunford et al., 2000)。鉴于举证责任对一个法律体系的诉讼程序所具有的重要影响,确定归因法中举证责任的适当高度就显得尤为重要。

举证责任有三种经典标准:优势证据标准、清晰且令人信服标准,以及排除合理怀疑标准。优势证据标准直截了当地要求事实认定者相信事实(或法律结果)存在的可能性大于不存在的可能性,大致上将举证责任平均分配给双方。美国最高法院将清晰且令人信服标准描述为中间标准,该标准对说服力的要求略高于优势证据标准,但仍低于排除合理怀疑标准。最后,排除合理怀疑标准代表了最高的举证责任,旨在确保尽可能保护被告免受错误判断的可能性。

虽然这种举证责任的范围已经确立,但何时适用某种标准的规范性依据却不那么明确。詹姆斯·弗莱明(J. Fleming)写道:"在任何特定问题上,在两种意义上分配举证责任都没有令人满意的检验标准。"罗伯特·贝尔顿(R. Belton)也表达了类似的观点:"法院尚未制定出任何普遍规则或一套政策考虑因素,供法院在确定如何在双方当事人之间分配这三种责任时参考。"诚然,优势证据标准长期以来一直是美国民事诉讼的标准,合理怀疑也同样是美国刑事司法诉讼的主要规则。然而,这些标准与各自的诉讼程序联系在一起,主要是法律传统层面的原因,缺乏特定的理由,特别是民事诉讼程序中适用的标准。这一点在将美国的法律制度与其他国家的法律制度进行对比

时尤为明显。一些具有纠问制传统的国家,如德国,对其法院所面对的所有法律问题,无论事由如何,均采用合理怀疑标准(Clermont & Sherwin, 2002)。因此,任何一种特定的法律制度都会采用不同的举证责任。在归因问题上,如何选择适用哪种举证责任呢?

虽然在选择举证责任标准时可能没有单一的检验标准,但有一些一般原则确实影响着这种选择。例如,政策依据、公平性以及相关事件实际发生的可能性等考虑因素。弗莱明认为,类似的公平、便利和政策性总体原则推动着为举证责任设定标准的决策。除了这些更为普遍的原则之外,弗莱明还承认其他考虑因素的相关性,如一方当事人获得证据的相对机会、一方当事人的论点偏离普遍经验的程度,以及可能将举证责任作为不利论点的障碍的实质性考虑因素。

虽然贝尔顿和弗莱明的描述似乎符合常规,但也没有提供太多有益的启示。公平、便利和政策性作为宽泛的理由,几乎适用于任何法律解释,也适用于任何方向。

相反,路易斯·卡普洛(Kaplow, 2012)将这些考虑因素置于一个更具体的参照框架内,通过经济学分析来探讨举证责任,即每种举证责任如何才能最好地实现法律制度的目标。举证责任被具体视为调整两种主要概率结果的工具:对实施有害行为的人施加责任的概率,以及对适当行为的人施加错误责任的概率。在卡普洛看来,举证责任必须在阻止有害行为和避免扼杀有效行为之间取得平衡。按照这一思路,考虑非对称错误成本至关重要,因为这些错误的计算往往决定了程序规则如何倾斜竞争环境,包括如何设定举证责任。

最典型的例子就是刑事处罚,因为“宁可让 10 个有罪之人逃离处罚,也好过让无罪之人遭受痛苦”,所以我们认为“有利于被告的刑事诉讼规则”是合理的,包括高举证责任。就归因而言,错误成本似乎没有那么明显地偏向一方或另一方(Gersen & Vermeule, 2016)。让一个网络攻击国逍遥法外是否

比惩罚一个无辜的国家更好?假设网络攻击的严重程度足以上升到武装力量的水平,并假设反制措施的范围小于军事打击,那么网络攻击的危害是否不如军事打击严重,这一点并不一定清楚,尤其是如果后者应该受到相称性规则的限制。

就归因法而言,优势证据标准最适合实现归因制度的总体目标。在军事行动是对网络攻击的唯一回应(或威胁)的情况下,举证责任应提高到合理怀疑标准。作为基本的举证责任,以证据优势来证明归因似乎最合适,主要有两个原因:首先,较低的举证责任产生较低的证据门槛,增加了产生法律判决的机会,从而增加了责任风险,提高了对有害行为的威慑;其次,它将说服责任大致平等地分配给各方,挑战双方以最佳方式提供有关网络攻击起源的信息和证据。

虽然可以设想一种更低的举证责任(如严格责任),但优势标准是最可取的平衡点,因为它规定必须提供一定程度的信息以确立表面证据确凿的案件,然后根据对双方所提供信息的比较分析做出判决。这一要求鼓励控辩双方竞相提供信息。因此,优势证据标准能带来最佳的信息生产水平,而更广泛地提供有关国际网络攻击的更多信息,有助于解决困扰网络安全领域乃至更广泛的国际互动中的不确定性和交易成本问题(Li, Ou & Rajagopalan, 2010)。

批评者可能会反对说,优势证据标准对为自己辩护的国家来说是不公平的。毕竟,优势证据标准将责任平等地分配给了双方。但有人可能会说,与提出指控的国家相比,处于辩护地位的国家实际上处于弱势。不仅存在信息不对称的问题,因为提出归因指控的国家可能拥有(或声称拥有)支持其立场的秘密情报,而且扮演防御角色的国家基本上也被迫通过证明反事实来反驳指控,即它事实上没有发动网络攻击。鉴于进行归因可能需要复杂的技术技能,而一些国家可能缺乏拥有此类技能的人员,因此考虑到归因所带来的特殊挑战,一些国家可能根本没有资源来开展反击归因的工作。刑事或民事案

件中的个人可以提供不在犯罪现场的证明,而复杂的、由许多成员组成的国家则不同。一般来说,国家无法说明其全部职能,以显示其诚实。

反驳的理由是,个体在民事诉讼中作为被告时,经常会对自己的行为做出说明。虽然证明反事实确实很难,尤其是在黑客攻击的情况下,但这种反对意见假定将攻击归咎于国家的初步证据已经发生。如前所述,即使适用优势证据标准,这一任务仍是一项挑战。优势证据标准的传统表述是,一方需要以超过 50%的可能性证明其主张。但是,假设一个不可知论的事实调查者从 50%的概率线开始,并能被指控者推翻是不够的。虽然对抗制框架迫使事实调查者对双方的主张进行比较分析,但 50%的概率假设被告只是在否定原告的主张,而实际上被告经常会提出一个或多个反论点。

因此,案件的转折点不是原告陈述的概率真实性的严格角力,而是原告陈述的概率真实性与被告可能的反陈述的概率真实性之间的比例。就网络攻击而言,有人反对优势标准偏向原告,这就犯了贝叶斯概率论的错误;与其假定原告的归责指控绝对属实,不如将这些指控与潜在的概率进行比较,即全球众多潜在行为者中的任何一个都可能对攻击负责。然后,被告国可以参考任何技术或环境依据来怀疑归因。

此外,本应有利于指控国的信息不对称在实践中可能并不那么有利,因为事实认定者往往会对隐瞒信息的当事方表示更大程度的怀疑。这一点在国际法院审理的国家对国家的裁决中得到了具体研究。在这些裁决中,国际法院对通常以安全为由的证据隐瞒做出了回应,对间接证据做出了有利于无法获得被隐瞒证据的一方的宽松解释(Scharf & Day, 2012)。从逻辑上讲,国际法院行动背后的原则也适用于其他形式的国际裁决。考虑到许多国内法院倾向于从一方当事人隐瞒证据的事实中做出积极的不利推论,国际法院的回应对隐瞒证据做出了相当温和的反应(Nance, 2010)。因此,将优势证据标准适用于归因法时,不会造成原告的不公平优势。

一般来说,优势证据标准符合归因的目标,因为它提供了威慑和信息生

产的最佳平衡;较低的举证责任降低了归因的障碍(因此,增加了反制措施的潜力),同时仍然需要必要的说服力,以激励生产有关网络攻击的相关情报和信息。在提议或威胁以军事打击作为反制措施的情况下,归因法应将举证责任提高到合理怀疑标准,这与美国刑法采用该标准的原因相同。合理怀疑标准承认,伴随着如此严重的惩罚,错误率极不相称,正如错误的刑事处罚可能带来极不相称的、不可容忍的伤害一样,错误的军事冲突也会带来同样的伤害,而且范围和规模可能会成倍增加。

3. 将非国家行为体的网络攻击归因于国家:国家责任理论

迄今为止,归因法采用的是对抗制,遵循类似美国和英国法律制度的程序流程,包括提起诉讼的规则、申诉和答辩的前后顺序以及提供证据的对抗性发现框架。它还有一个一般的举证标准,用于确定一方何时成功证明另一国对发动网络攻击负有责任。但是,如果一个国家将责任归咎于碰巧在其境内活动的"非国家行为者",从而为自己辩护,使自己免于承担责任呢?法律是否应将非国家黑客的恶意活动归咎于国家?

这对归因法和网络安全法来说是一个特殊的问题,因为进行网络攻击的成本相对较低,这为无数非国家行为者提供了选择(Nye, 2010),他们可能出于各种动机采取行动。所有与简单归因攻击相关的典型问题都有可能进一步削弱黑客个人与可能将该行为者与国家联系在一起的任何指挥链或控制基础设施之间的联系。因此,归因法必须解决一个不可避免的结果,即追踪到黑客个人,并面对如何为法律责任目的将此人与国家联系起来的问题。

国家责任理论是一个超越网络攻击领域的法律问题,此前在其他情况下也曾涉及。国际法已经有了将非国家行为者的恶意行为归咎于国家的国家责任理论,2001 年《国家对国际不法行为的责任条款草案》规定了国际法院追究国家对非国家行为者责任的方式。《国家对国际不法行为的责任条款草案》第四、八条随后被国际法院认定为习惯国际法,法院、评论家和其他利益方也广泛承认这些条款阐述了习惯国际法中国家责任理论的标准观点。例

如,《塔林手册》第 1 版和最近发布的第 2 版都大量借鉴了联合国国际法委员会的条款草案,在网络攻击的背景下提出了国家责任理论的概念。

《国家对国际不法行为的责任条款草案》认为,如果非国家行为者是作为国家机关行事,或在国家的指示、指令或控制下行事的,则该非国家行为者的不法行为可归于国家。第四条规定:

1. 任何国家机关,不论行使立法、行政、司法职能,还是任何其他职能,不论在国家组织中具有何种地位,也不论作为该国中央政府机关或一领土单位机关而具有何种特性,其行为应视为国际法所指的国家行为。

2. 机关包括依该国国内法具有此种地位的任何个人或实体。

正如第四条评注所明确指出的,第四条也适用于可被视为事实上的国家机关的个人。同时,第八条也认为,如果非国家行为者是“按照国家的指示、在国家的指挥或控制下行事”,则其行为可归于国家。第四、八条所述国家责任的条件,一般被理解为检验国家是否控制了个人行为者的标准。这些控制测试反过来又与国际法院等在裁决中采用的控制测试相呼应。

然而,关于国家责任的现行国际法也存在一些局限性。例如,奥娜·哈撒韦等人(Hathaway, Crootof & Levitz et al., 2012)批评现行框架产生了不正当的激励机制,只要国家保持最低限度的监督,就可以将非法任务交给非国家行为者,从而逃避责任。他们还认为,控制测试实际上抑制了控制无赖或恶意行为的努力,因为实施控制的尝试可能会产生足够程度的控制,使国家对非国家行为者做出的不法行为负责,尽管国家努力对其进行监管。彼得·马格里斯(Margulies, 2013)批评了适用于网络攻击归责任务的国家责任理论的范围,提出条款草案的控制测试要求具体、全面控制的高标准,这样的标准将是排除国家指挥非国家行为者进行网络攻击的非常重要的例子。

这些意见不仅是批评性的,也是建设性的。哈撒韦等人(Hathaway, Crootof & Levitz et al., 2012)、马格里斯(Margulies, 2013)提议进行调整,以弥补国家责任规则中的这些缺陷。马格里斯建议采用“虚拟控制测试”,即“当

一个国家资助和装备一个私人实体或个人,而该私人实体或个人随后参与网络攻击时,该国家就有责任证明其对网络攻击不负有责任”。根据这一检验标准,马格里斯似乎要求有一些初步证据表明被指控的国家与非国家实体有关联。然而,这种建议的国家责任方法与哈撒韦等人所描述的现行制度下的国家责任方法存在一定的风险,即政府与非国家行为者之间的任何现有关系都可能附带责任,这反而会激励政府放弃对其范围内的非国家行为者的任何控制。马格里斯可能会反驳说,“资助和/或装备”的要求意味着虚拟控制测试只要求政府在对此类实体提供实质性支持的情况下行使此类监督,政府自然有动机在各种情况下资助非国家实体,而在政府这样做的情况下,就应该推定期望监督。这一论点的问题在于,马格里斯对“资助和/或装备”非国家实体的定义过于模糊,这些术语潜在的广泛范围实质上抹杀了对将个人不法行为归咎于国家能力的限制。

当然,这些问题很容易通过更具体地界定这些术语来解决。另外,哈撒韦等人提出的为国家责任主张提供积极辩护的建议也可以补充解决不正当激励的问题。他们提出了一项类似的广泛义务,即代表国家“确保尊重”《日内瓦公约》第一条,确保其范围内的非国家行为者不参与网络攻击。虽然这种方法同样会引起人们对激励国家保持距离而不是进行监管的担忧,但他们提出了这样的观点来解决这一担忧:如果国家能够证明他们采取了“合理的措施”来防止违反国际法,那么国家就应该有一个积极的辩护理由。

通过将这些建议纳入程序规则,归因法不仅可以推进国家责任理论,而且可以用哈撒韦等人、马格里斯提出的同样新颖的解决方案成功应对网络攻击归因的新挑战。通过虚拟控制测试结合“合理注意”的肯定性抗辩,非国家行为者与他们所联系的国家之间建立起更为合理的联系,应允许归因法将个人的网络攻击归于国家,同时允许国家在采取善意措施防止不法行为时,以适当的方式保护自己免于承担责任。

4. 敏感情报及其举证规则

假设一个国家遭受了网络攻击,并希望提出法律指控,将攻击归因于另

一个国家。在目前的情况下,国家已经知道了提起诉讼的程序,以及起诉和答辩、简易判决辩论和出示证据的前后顺序。在最后一步,国家遇到了一个问题:如果国家所依赖的证据有很大一部分来自秘密情报,那该怎么办?此外,国家可能有看似合理的事实依据来确定攻击的归因,但可能出于正当理由不想披露这些证据,因为网络攻击者可以从这些归因点中吸取教训,避免在未来留下相同的线索。归因法面临的挑战是,如何协调提出此类证据的必要性与国家对其机密情报及其来源保密的愿望。

对抗制在一定程度上解决了这一难题:由于当事人可以控制指控的推进,一种答案是干脆将这一问题置之不理。根据成本效益考量,该观点认为,这种披露是寻求对网络侵犯者进行指控的代价,完全由国家来权衡指控的利益与披露其秘密情报能力信息的成本。这种方法的问题在于,它假定网络攻击的成本纯粹是受攻击国家的内部成本。然而,如果我们将网络攻击理解为一种普遍的、全球性的、反复出现的现象(Hackett, 2016),而且一个国家的网络攻击行为如果不加制止,就会在未来对其他国家进行网络攻击,那么归因行为(以及它能够采取反制措施阻止未来的攻击)就会产生积极的外部效应,而上述观点则忽略了这一问题。

因此,归因法应努力兼顾国家的保密和归因利益,找到一种既能允许国家将敏感情报作为证据提出,又能对公众保密的方法。这并不是法院第一次在法庭上处理敏感情报的作用问题。长期以来,法院一直在国家的敏感安全关切与法院的公共角色之间寻求平衡,并开发了许多管理工具来保护听证会上产生或使用的信息。归因法可以纳入两个主要程序,以满足国家保护机密信息的愿望:首先,法院可以制定单方面和不公开审理证据的程序;其次,当法院的记录包含机密信息时,法院可以封存这些记录。

当有必要在法庭上证明某项主张时,一些国家的法院采用这种程序来确保机密信息的安全。在美国,1978 年的《外国监视情报法》(FISA)设立了外国情报监视法院,负责审查联邦执法人员和情报人员的监视令申请。外国情

报监视法院的诉讼程序是单方面和秘密进行的,其裁决很少公开(Clarke,2014)。这些程序性举措并不局限于专门法院。美国《机密信息程序法》允许美国法院在审理刑事案件时对机密信息进行单方面和秘密审查,以确定该证据是否对公平审判或刑事正当程序的要求至关重要(Manget,2006)。一般来说,在向联邦法院提起民事诉讼时,《联邦民事诉讼程序规则》第二十六条允许在有充分理由的情况下封存法庭记录。

其他国家也有类似的程序来保护审判程序或证据。英国于2013年通过了《司法与安全法》,规定了秘密材料程序(CMPS),即只有法官和经过专门安全审查的辩护律师才有权接触案件中涉及的任何敏感情报的秘密法庭听证会。同样,荷兰的《受保护证人法》也规定了一项特别程序,由特别治安法官听取荷兰两大情报机构代表的意见,以决定某些信息是否应保密,或某些证人的身份是否应匿名。这种证据在荷兰的行政、民事和刑事案件中都有使用,而且这种程序与美国的情报监视法庭一样,主要是单方面和不公开进行的,但在特别法官评估敏感情报时,案件当事人有可能在场。德国和西班牙则禁止在审判中使用秘密证据,但有时也允许根据秘密证据提供证词或匿名信息。

单方面程序和不公开程序在许多方面有利于归因法。增加这些类型的程序为系统创造了灵活性,使事实认定者能够逐案分析敏感情报引起的问题。尤其是单方面程序,它可以使事实认定者与当事人就信息披露问题进行谈判,因为当事人可能倾向于高估披露自己信息的成本,这是一种损失规避(Kahneman, Knetsch & Thaler, 1991)。不公开程序允许敏感证据获得充分的证据价值,同时更普遍地降低了信息披露的成本。

在法律程序中制定保密规则也是有代价的。法律程序的透明度往往会赋予其更强的合法性,而保密则可能会破坏这种合法性。此外,如果归因法的首要目标之一是在国际社会眼中证明反制措施的正当性,那么秘密听证会可能会让国际社会中的许多人对反制措施的正当性产生怀疑。

这一棘手问题关系到法院或法律判决的权威来源。诚然,司法程序的公开展示可能因其透明度而有助于程序的合法性,但这并不意味着这种公开性对司法合法性的约束力具有决定性作用。毕竟,前面讨论过的国家都成功地将保密措施纳入其法律体系,而没有损害其法律裁决的合法性(Butler, 2013)。当然,这些机构并不是一开始就采用不公开的诉讼程序,其中大多数机构也不是将大部分案件都置于不公开的诉讼程序之后。社会之所以接受某些记录的保密,可能是因为这些司法机构已经通过长期的普遍公开诉讼程序建立了合法性。

如果公众普遍信任国际机构及其国内法院,这种信任就会转化为对国际法院的支持(Voeten, 2013)。这一结论与法学界对权威的更广泛的解释是一致的,即主张权威的是法院的职务或机构,而不仅仅是纯粹的说服力(Raz, 1985)。毕竟,在美国,提交给联邦上诉法院的绝大多数案件都是通过未公开的"无意见"命令终止的,这表明法律争议的解决并不要求法律程序有一个纯粹透明的窗口(Raz, 1985)。

事实上,尽管使用了秘密程序,其他国际法院仍保持了其合法性。例如,欧洲人权法院在"A 诉联合王国案"[①]中就遇到了这一问题,欧洲人权法院在该案中审查了联合王国允许根据包含"秘密材料"的证据拘留个人的程序。国内和国际法院积累的这些经验表明,归因法可以采用不公开和单方程序的方法。当然,这些程序必须审慎使用。尽管如此,有了审查保密材料的程序,国家就可以在声称归因时提出敏感情报,同时又能保护情报的机密性。

(二) 归因法法律框架的总结

总之,拟议的归因法具有以下特点。第一,它基于对抗制而运行,在这种机制中,诉求和记录都主要由诉讼各方形成。第二,与对抗制框架相一致的是,程序规则以典型的对抗制法律程序的前后方式对案件的各个阶段进行时

① A v. United Kingdom, 49 EHRR 29 (2009).

间排序。第三,在进入案情实质阶段时,指控国必须以优势证据证明其归因主张,除非指控国希望采取军事反制措施。如果一个国家没有披露其计划采取的反制措施,或者这种选择尚不确定,那么案件可以按照优势证据标准进行审理,但这不足以成为日后采取军事行动的理由。第四,为履行举证责任,各国可选择采用不公开审查、单方听证和封存记录等程序,以使用敏感证据证明其主张。第五,也是最后一点,证明归因主张的国家需要具体证明攻击与受国家指使或控制的个人有关,其中控制测试将根据马格里斯主张的"虚拟控制测试"进行善意解释。与此同时,国家将有积极的抗辩理由,证明其在监管相关非国家行为者方面尽职尽责。

四、实施归因法的模式

随着归因法框架的制定,如何才能使这一理论更加充实和生动呢?本节将讨论归因问题中政策性较强的方面,主要探讨机构设置问题:在哪里进行判决,由谁来判决?当然,国家遵守国际制度或法律的问题本身就是一个宏大的讨论主题(Goldsmith & Posner, 2005)。从康德哲学(Tesón, 1992)到理性选择理论(Guzman, 2002),对国际法和国际制度的结构性解释不一而足。在刑法(Simmons & Danner, 2010)、环境法(Brodansky, 1999)和人权法(Simmons, 2009)等几乎所有领域,都出现过关于国家遵守特定主题的讨论。

虽然本文可以就国家参与的动机提出一般性的结构分析,但国家合作或遵守的问题既是一个法律问题,也是一个政治问题。为了对国家如何参与到这样一个法律框架中提出一个完全具有预测性的主张,我们的建议必须借助于:国际关系,既包括广义的理论层面,也包括针对当前历史时刻的具体分析;行为经济学,分析激励机制、成本以及不同参与者的行为概率;对许多参与者的具体历史和心理分析,这些参与者可能是建立这样一个法律制度的重要因素。

全面回答国际履约挑战所提出的问题超出了本文的范围。相反,本文采取了一种更为温和的方法,即通过调查各种其他形式的国际裁决来讨论国家参与的一般激励因素。因此,本文研究了三个国际裁决的例子:国际法院、世界贸易组织争端解决机制,以及像美国—伊朗求偿法庭这样的特设系统。每个机构都反映了不同的国际裁判方法,为国际机构如何成功促使各国参与其体系提供了范例。国际法院提供了将归因法纳入具有广泛属事管辖权的现有框架的选择,世界贸易组织争端解决机制反映了一个具有专门主题的裁决体系,而美国—伊朗求偿法庭则是一个特设的、国家对国家的方法的典范,它可以更灵活地解决两个特定国家之间的冲突,但缺乏创造更持久的法律权威的力量。

(一) 国际法院

国际法院是国际法律机构的典范。国际法院于 1946 年根据《联合国宪章》成立,是 20 世纪大部分时间内唯一存在的国际法院(Dupuy, 1999)。因此,国际法院不仅是创建新的国际法律体系的典范,而且还提供了一个可纳入归因法的现有典例。一般而言,国际法院拥有广泛的属事管辖权,可审理向其提出的任何国际法指控,只要该指控是在双方同意的情况下提出的。将归因法纳入国际法院的好处,是将归因法附着在一个已有公信力、机构历史以及充分发展的规则和资源的现有机构上。

在国际法院成立之前,人们曾多次尝试建立国际机构来解决国与国之间的争端。例如,1899 年海牙和平会议后成立了常设仲裁法院(PCA)(Kolb, 2014)。尽管名为“常设仲裁法院”,但它并不是一个永久性的常设法院,而是提供了一个行政组织,各国可以从候选人库中挑选仲裁员,并建立自己的法庭来解决争端。尽管常设仲裁法院提供了一套程序规则,但这些规则只是默认规则,缔约国自行选择制定的规则将推翻这些规则。1899 年常设仲裁法院成立后,1907 年召开了一次后续会议,包括美国在内的几个州提议成立一个

真正的常设法院。

虽然1907年的提案在当时未能获得支持,但第一次世界大战造成的破坏推动了建立国际法院的进程,最终形成了国际法院的前身——常设国际法院。在25年的任期内,常设国际法院做出了32项判决,所有判决均已执行。在此期间,常设国际法院还发表了27项咨询意见,其中大多数咨询裁决都得到了各国的遵守或采纳。总之,常设国际法院为后来的国际法院奠定了成立的基础。

国际法院是随着1946年《联合国宪章》的制定而成立的,其模式沿袭自常设国际法院。国际法院由安全理事会和联合国大会选出的15名法官组成。这些法官通过单独选举产生,任期9年,选举的重点是法官个人而非其国家的代表。国际法院还纳入了一系列规则,以确保其司法机构的独立性,其中包括:要求法院成员庄严宣誓在履行职责时保持公正的规则;国际法院进一步努力消除潜在的利益冲突,禁止其成员在担任法院法官期间"行使任何政治或行政职能,或从事任何其他专业性职业"。

《国际法院规约》第三十四至三十八条规定了国际法院的管辖权,使其有理由审议有关下列事项的所有法律争端:条约的解释;任何国际法问题;任何一经确定即构成违反国际义务的事实的存在;因违背国际义务而应做出的赔偿的性质或程度。

虽然国际法院目前尚未审理有关网络攻击的国际争端,但网络攻击和归因法当然涉及属于国际法院职权范围的法律问题。网络攻击有可能上升到违反第二条第四款的武装力量的程度,同时也有可能违反国家主权和中立的理论。归因作为网络攻击的一个必然附属问题,牵涉到此类国际法问题。

基于以上概述,下文将进一步讨论国际法院的成立因素,以及对构建、实施归因法的启示。我们很难将国际法院(及其前身常设国际法院)的创立与促成这两个机构诞生的历史割裂开来。毫无疑问,第一次、第二次世界大战推动了国际法院的创立,也对与之相关的国际组织的创立产生了重要影响。

作为一个历史问题,它们似乎在讲述国际法因国际悲剧而产生的故事。这一历史叙事既令人鼓舞,又令人不安。说它令人鼓舞,是因为它表明各国有可能创建新的国际法和国际机构,以应对网络攻击和全球网络安全等当代挑战。令人忧虑的是,可能只有当这些挑战发展到导致国际灾难或造成广泛伤害的事件时,各国才不得不创建此类机构。当然,这种广义的概括并不是实际执行归因法的全部。毕竟,像爱沙尼亚网络攻击这样更加本地化的事件已经刺激了像共同制定《塔林手册》及其续篇这样的团体,暗示了先发制人而非被动执行国际法的可能性。

(二) 世界贸易组织争端解决机制

实施归因法的第二种模式是通过世界贸易组织争端解决机制这样的机构。与国际法院模式不同的是,世界贸易组织的争端解决体系是一种将裁决程序附于一个具有特定主题的国际机构的模式。采用这种模式的好处是,通过一个专门的事实认定机构来执行归因法,这些机构可能最有能力解决证据和技术的技术复杂性问题,而国家及其专家正是通过这些证据和技术将恶意数字活动追溯到其创造者的。

世界贸易组织是根据《马拉喀什建立世界贸易组织协定》成立的,该协定是 1994 年乌拉圭回合谈判达成的几项协定之一。世贸组织的成立总体上是为了促进和监督全球贸易,而世贸组织的争端解决体系是《马拉喀什建立世界贸易组织协定》第三条明确规定的职能之一,旨在帮助该机构实现这一目标。与此同时,《关于争端解决规则与程序的谅解》(DSU)对世贸组织争端解决程序的结构和程序做出了更精确的规定。根据《关于争端解决规则与程序的谅解》第一条,争端解决程序可适用于一些特定协定下的争端,包括 1994 年《多边货物贸易协定》和《与贸易有关的知识产权协定》。

争端解决程序由争端解决机构(DSB)管理,该机构负责监督世贸组织争端解决小组的运作及其裁决的执行。专家组的实际职能由《关于争端解决规

则与程序的谅解》规定的规则决定。这些规则包括设立裁决专家组的规定、专家组的组成、专家组程序以及每个专家组如何执行其裁决程序的各种其他基本规则。例如,《争端解决谅解书》规定了启动争端解决小组的条件,指出争端解决机构应在申诉方"以书面形式"提出请求时设立一个解决小组,而且这种请求"应说明是否进行了磋商,确定有争议的具体措施,并简要概述申诉的法律依据,足以清楚地说明问题"。此外,《关于争端解决规则与程序的谅解》还对专家组的成员构成进行了规范,规定了专家组成员不得来自争端当事国(除非双方另有规定)。在决策过程方面,《关于争端解决规则与程序的谅解》的条款还要求专家组为其决定制定具体的时间表,规定了具体的审查阶段和这些具体阶段的程序,并规定了专家组可以审查或咨询的信息类型。因此,《关于争端解决规则与程序的谅解》规定了一个全面的裁决制度。

这样一个机构在促使国家参与和遵守方面的有效性引起了学术界的关注。关于国家参与的问题,一个更加专业化的论坛可能会引起这样的担忧,即在该主题领域拥有既得利益的强国可能会将这样一个机构仅仅作为一种施展其影响力的手段。例如,查德·鲍恩(Bown, 2005)的一项实证研究表明,一个国家的报复能力、法律能力以及在国际政治经济关系中的作用对衡量该国参与争端解决体系的可能性具有重要意义。鲍恩的研究结果让人担心,专门机构可能只是强国将其在某些领域(如贸易或网络安全)的主导权制度化的工具。当然,这个问题可能只是国际力量不对称的一个特征,也可能是财富不平等更普遍地影响法律的结果。

归根结底,即使存在对某些国家的参与偏向,如果法律体系的价值不仅仅在于为一方或另一方裁决诉求,而是在于法律制度带来的积极外部效应,即在国家间创造更大的可预见性与合作,那么参与的偏向可能是一个可以容忍的代价。其他实证研究表明,此类法律确实提供了这些积极的外部效应。例如,迈克尔·贝克特尔等人(Bechtel & Sattler, 2015)发现,申诉方和签署申诉方向世贸组织提出的申诉的被动第三方所获得的经济利益差别很小。这

些结果表明,“较弱”的国家可以选择搭乘“较强”国家的便车,从贸易增长中获益,而且裁决程序产生的外溢效应可能会使更多国家受益。如果世贸组织的争端解决程序能够有效地促使争端各方遵守规定,那么这一程序所产生的遵守规定的情况以及随之而来的积极的外部效应,很可能说明国际裁判制度是成功的。

世界贸易组织的争端解决机制不仅提供了一个国际裁判的范例,也为某些法律制度如何被纳入国际机构并获得更广泛的认同提供了一个实用的经验。在《私权、公法:知识产权的全球化》一书中,苏珊·塞尔斯(Sells, 2003)追溯了《与贸易有关的知识产权协议》如何被纳入世贸组织结构的历史。在这一历史叙事中,塞尔斯提请人们注意“这场戏剧中的核心角色”——“总部设在美国的 12 名知识产权委员会成员”,该委员会由代表不同行业的 12 名首席执行官组成。因此,集中游说在将某些监管制度落实到国际法中,以及在动员各国充当此类制度的有力倡导者方面可以发挥突出作用。鉴于网络攻击对私营商业实体构成的风险越来越高,以雅虎网络攻击为例,商业公司肯定有机会在游说中发挥突出作用,以成功地将拟议的归因法等国际制度制度化。

(三)大规模赔偿委员会(美国—伊朗求偿仲裁庭)

实施归因法的第三种模式是通过特设法庭,如 1981 年成立的美国—伊朗求偿仲裁庭。美国—伊朗求偿仲裁庭是纯粹双边大规模求偿委员会的一个范例,它是通过两国之间的条约而产生的。与前两种模式不同的是,法庭制度是针对双方之间的一系列具体指控要求而产生的。这种方式的优点是灵活性强,可以根据具体情况和所涉各方的具体要求来实施。但其不足在于效力范围有限,这种效力受限既体现在管辖当事方,也体现在仲裁庭可审理的历史事件方面。

该仲裁庭是解决伊朗人质危机协议的一部分(Mosk, 1987)。在 1979 年

的革命中,伊朗人袭击了美国驻德黑兰大使馆,劫持了 69 人(Sahimi, 2009)。虽然一些人质获释,但仍有 52 人被关押了 444 天。《阿尔及尔协议》帮助促成了美国和伊朗之间的协议,伊朗将释放美国人质,以换取美国取消贸易制裁并解冻伊朗的一些资产。重要的是,《阿尔及尔协议》还试图解决美国公民对伊朗提出的以及伊朗公民对美国提出的大量私人指控。《阿尔及尔协议》解决这些问题的方式,是将其从诉讼转为仲裁——因此成立了法庭。

《指控解决宣言》正式成立了法庭,包括其管辖权、组成和仲裁规则等条款。在管辖权方面,法庭仅限于审理两类指控:美国国民对伊朗的指控和伊朗国民对美国的指控,以及构成该国民指控标的物的同一合同、交易或事件所引起的任何反诉;美国和伊朗因双方之间的货物和服务购销合同安排而对对方提出的官方指控。在确定裁决人时,《指控解决宣言》确定仲裁庭由 9 名成员组成:美国任命 3 名,伊朗任命 3 名,然后由这 6 名成员任命仲裁庭的最后 3 名成员。

在程序方面,仲裁庭采用了联合国国际贸易法委员会的仲裁规则。这些规则又制定了一套全面的程序,对审理的各个阶段做出规定,包括进行质证和出示证据的方法。这些规则还为仲裁庭适用各种程序机制提供了很大程度的灵活性和自由裁量权,如何时或如何纳入专家证据(Bockstiegel, 1986; Straus, 1986)。因此,纳入贸易法委员会的规则提供了一个实例,说明如何将先前存在的一套规则纳入或借鉴到特定的特设裁决机构中,这反过来又为特设机构如何对归因法采取同样的做法提供了类似的可能性。

总体而言,美国—伊朗求偿仲裁庭成功地处理了双方的大量求偿。美国提出的几乎所有索偿都得到了裁决,那些有利于美国索偿者的索偿要求都得到了全额支付(Brower, 1992)。伊朗方面,美国于 2016 年同意支付 17 亿美元的和解金,以解决伊朗的一项长期指控。因此,一种观点认为,该仲裁庭发挥了重要作用。举例而言,仲裁庭自成立以来已处理了 3900 余起案件,这些案件总体上涵盖了美伊两国间除少数大型、复杂指控外的所有案件。除了处

理的案件数量,理查德·莫斯克(Mosk, 1987)等人还称赞仲裁庭有能力切实、成功地执行一整套裁决案件的程序规则,这些规则有助于有效地处理复杂的案件,其程序"可作为未来法庭的指南"。事实上,仲裁庭还在其他方面发挥了指导作用。克里斯托弗·吉布森等人(Gibson & Drahozal, 2006)的研究表明,美国—伊朗求偿仲裁庭的裁决已被解决投资争端中心法庭援为先例,这表明特设法庭的裁决仍可在其裁决的直接争议之外产生更广泛的影响。

然而,以临时方法提出归因指控是有局限性的。尽管美国—伊朗求偿仲裁庭的裁决已被其他法庭引用,但对仲裁引用的更普遍调查表明,仲裁法庭对案例的引用往往因背景不同而有很大差异。虽然《国际货物销售合同公约》和国际商会对先前裁决的引用相对较少,但体育仲裁法庭和域名仲裁系统在其裁决中对先例的引用几乎无处不在。在归因问题上,很容易看到这些裁决会走向前者的道路。鉴于网络攻击归因案件的事实差异很大,从网络攻击的类型到国家对支持归因的证据的保密程度,法庭很可能不愿意过多地依赖以前的案例,因为它们可能存在事实差异。

特设法庭在建立参与激励机制方面也面临着特殊的挑战。由于特设法庭经常产生于双边协定,它们依赖于各国拥有(或相互视为拥有)相对平等的地位。此外,它们还取决于特定的历史背景。在这种背景下,每一个国家都对另一个国家有足够的不满,从而提供了首先成立这样一个法庭的动机。在网络攻击的背景下,这种情况当然有可能发生,各国可能相互进行了网络攻击,但很难想象一个国家会主动承认自己的责任,并带着有序解决的愿望与对方接触。尤其难以想象,在这种情况下,各国拥有足够平等的影响力,从而产生迫使双方坐到谈判桌前的局面。虽然前两种模式确实只能对已经发生的攻击进行裁决,但常设司法机构本身就代表了一种时间上的持久性,使其裁决能够对未来投下更大的影响。因此,特别模式虽然在可能需要它的特定事实情况下最有效,但在执行归因法方面却是一个不太有效的模式。

五、结论

在描述国际法院的起源时,罗伯特·科尔布(R. Kolb)将其发展历程分为三个部分:组织全面的仲裁司法计划;试图建立一个永久性和强制性的“仲裁法院”;建立一个与国际联盟有联系的机构法院——常设国际法院。

至关重要的是,创建这一制度的第一步是创建法律方案。每迈出一步,法律的愿景就会逐渐变得更加具体,直到这一愿景成为实际的法律制度。本文提出的归因法旨在描绘国家如何通过法律应对网络攻击威胁的愿景。当然,与最初的国际法院概念相比,归因法是一个更为温和的制度。但这仍然是一个重要的制度,而且由于之前的国际法机构所奠定的基础,这一构想变得更有可能。

本文设想了一个将网络攻击归因于责任国的法律框架,并提出了允许国家合法提出这种主张的程序规则。通过采用对抗制,归因法可使双方平衡就这一不确定主题的举证责任。通过默认的举证责任——以优势证据证明标准归因,归因法可以解释证明归因的技术困难,允许法律承认间接证据何时足以将攻击与其来源联系起来。此外,通过使用虚拟控制测试,归因法可以更广泛地要求国家对与其有联系的非国家行为者负责,并允许禁止抗辩,为对此类行为者实施适当程度监督的国家创造安全港。最后,允许对证据进行单方面和不公开审查的程序规则将照顾到国家对其敏感情报的保密性的关切,同时也保留了在提出归因指控时使用相关证据的能力。

通过这些规则,归因法旨在使网络攻击背后的源头透明化。长期以来,网络攻击一直被蒙上一层神秘的面纱而不受控制,国家长期以来一直可以逃避实施此类攻击的责任(Kaplan, 2016)。虽然像美国这样的国家行为体可能曾一度认为自己在网络战领域拥有不成比例的优势,但网络攻击的日益扩散可能已经超出了任何一个国家的控制范围,不仅威胁到国家的安全,还威胁

到其私人和民间机构的稳定。随着不安全和不确定性的代价与日俱增,各国可能很快就会认识到需要法律机构通过相互问责来约束它们。

然而,近年来国际结构似乎出现了一些裂痕。随着英国脱欧等事件的发生,以及唐纳德·特朗普和玛丽娜·勒庞(M. Le Pen)等支持保护主义政策的个人的日益活跃,过去几十年来作为国际法发展主要特征的国际机构似乎正在退缩。保护主义的威胁因网络攻击的兴起而加剧,尤其是网络攻击在潜在干扰选举政治和国内机构合法性方面的恶性用途。所有这些威胁加在一起,似乎会破坏人们对国家主权和国际法的能力和稳定性的信心。

我们很容易被当下的政治风云所迷惑,而忽视了更长远的发展道路。但是,当今日益加剧的不确定性更加提醒我们需要进一步发展国际法,而不是进一步退缩。想象我们可能实施的新法律框架是一个步骤。但法律理论只是一部分,光有理论是不够的,除非这种理论能够解决、契合现实问题。归因法所规定的程序规则不仅规定了指控成功所必须满足的技术特征,还规定了与之相伴的实际成本。这样,它就将法律制度的成本具体化,以权衡无人管理现状下的不确定性成本。也许国家及其选民可以容忍一个没有法律来遏制网络安全威胁的世界。但如果对归因法可能带来的代价有了更明确的认识,国家可能很快就会意识到,无限制的网络攻击所造成的破坏代价太大,不容忽视。

参考文献

Axelrod, R. 1984, *The Evolution of Cooperation*, New York: Basic.

Bechtel, M. & T. Sattler 2015, "What Is Litigation in the World Trade Organization Worth?" *International Organization* 69(2).

Belton, R. 1981, "Burdens of Pleading and Proof in Discrimination Cases: Toward A Theory of Procedural Justice." *Vanderbilt Law Review* 34(5)

Beverly, R., A. Berger & Y. Hyun et al. 2009, "Understanding the Efficacy of Deployed Internet Source Address Validation Filtering." http://Perma.Cc/Ys79-Zpjr.

Bockstiegel, K.-H. 1986, "Applying the Uncitral Rules: The Experience of the Iran-United States Claims Tribunal." *Berkeley Journal of International Law* 4.

Boerbert, W. 2010, "A Survey Of Challenges in Attribution." https://api. semanticscholar. org/CorpusID:2445682.

Bown, C. 2005, "Participation in WTO Dispute Settlement: Complainants, Interested Parties, and Free Riders." *The World Bank Economic Review* 19(2).

Brenner, S. 2007, "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare." https://api. semanticscholar. org/CorpusID:72953571.

Brodansky, D. 1999, "The Legitimacy of International Governance: A Coming Challenge for International Environmental Law?" *American Journal of International Law* 93(3).

Brower, C. 1992, "Lessons to Be Drawn from the Iran-U. S. Claims Tribunal." *Journal of International Arbitration* 9.

Butler, A. 2013, "Standing up to Clapper: How to Increase Transparency and Oversight od FISA Surveillance." https://heinonline. org/HOL/LandingPage? handle=hein. journals/newlr48&div=8&id=&page=.

Chulov, M. &H. Pidd 2011, "Defector Admits to WMD Lies that Triggered Iraq War." http://Perma. Cc/W46Q-Yz2S.

Clapham, A. 2015, "Human Rights Obligations for Non-State-Actors: Where Are We Now?" in F. Lafontaine &F. Larocque eds., *Doing Peace the Rights Way: Essays in International Law and Relations in Honor of Louise Arbour*, Cambridge: Intersentia.

Clarke, C. 2014, "Is the Foreign Intelligence Surveillance Court Really A Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate." *Stanford Law Review* 66.

Clermont, K. &E. Sherwin 2002, "A Comparative View of Standards of Proof." *The American Journal of Comparative Law* 50(2).

Condliffe, J. 2016, "Security Experts Agree: The NSA Was Hacked." https://www. technologyreview. com/2016/08/18/70386/security-experts-agree-the-nsa-was-hacked.

Connolly, K. 2016, "German Spy Chief Says Russian Hackers Could Disrupt Elections." http://Perma. Cc/N5Em-3Gvc.

Devine, D., L. Clayton &B. Dunford et al. 2000, "Jury Decision Making: 45 Years of Em-

pirical Research on Deliberating Groups." *Psychology, Public Policy, and Law* 7(3).

Dupuy, P. 1999, "The Danger of Fragmentation or Unification of the International Legal System and the International Court of Justice." *International Law and Politics* 31.

Feigenbaum, J., A. Johnson & P. Syverson 2007, "A Model of Onion Routing with Provable Anonymity." *Financial Cryptography and Data Security* 4886.

Fleming, J. 1961, "Burdens of Proof." *Virginia Law Review* 47(1).

Frank, J. 1949, *Courts on Trial: Myths and Reality in American Justice*, Princeton: Princeton University Press.

Froeb, L. & B. Kobayashi 2001, "Evidence Production in Adversarial VS. Inquisitorial Regimes." *Economics Letters* 70(2).

Gallagher, S. 2013, "Turkish Government Agency Spoofed Google Certificate 'Accidentally'." http://Perma.Cc/L5Zy-2Tvv.

Gersen, J. & A. Vermeule 2016, "Thin Rationality Review." https://michiganlawreview.org/journal/thin-rationality-review.

Gibson, C. & C. Drahozal 2006, "Iran-United States Claims Tribunal Precedent in Investor-State Arbitration." *Journal of International Arbitration* 23(6).

Goldsmith, J. & E. Posner 1999, "A Theory of Customary International Law." *The University of Chicago Law Review* 66(4).

Goldsmith, J. & E. Posner 2005, *The Limits of International Law*, https://doi.org/10.1093/oso/9780195168396.001.0001.

Graham, D. 2010, "Cyber Threats and the Law of War." *Journal of National Security Law & Policy* 4.

Greenemeier, L. 2011, "Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers." http://Perma.Cc/Fy47-Jcyn.

Grimmelman, J. 2017, *Internet Law: Cases and Problems*, https://www.semaphorepress.com/InternetLaw_overview.html.

Guzman, A. 2002, "A Compliance-Based Theory of International Law." *California Law Review* 90(6).

Hackett, R. 2016, "Why A Hacker Dumped Code Behind Colossal Website-Trampling Bot-

net." http://Perma. Cc/Bg6V-Dj8U.

Hadfield, G. 2000, "The Price of Law: How the Market for Lawyers Distorts the Justice System." *Michigan Law Review* 98(4).

Hathaway, O., R. Crootof & P. Levitz et al. 2012, "The Law of Cyber-Attack." *California Law Review* 100(16).

Hay, B. & K. Spier 1997, "Burdens of Proof in Civil Litigation: An Economic Perspective." *The Journal of Legal Studies* 26(2).

Holzer, C. & J. Lerums 2016, "The Ethics of Hacking Back." https://ieeexplore. ieee. org/document/7568877.

Kahn, P. 1987, "From Nuremberg to the Hague: The United States Position in Nicaragua v. United States and the Development of International Law." *The Yale Journal of International Law* 12(1).

Kahneman, D., J. Knetsch & R. Thaler 1991, "Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias." *Journal of Economic Perspectives* 5(1).

Kaplan, F. 2016, *Dark Territory: The Secret History of Cyber War*, New York: Simon & Schuster.

Kaplow, L. 2012, "Burden of Proof." *The Yale Law Journal* 121.

Keohane, R. 1986, "Reciprocity in International Relations." *International Organization* 40(1).

Kolb, R. 2014, *The Elgar Companion To The International Court Of Justice*, https://lawcat.berkeley. edu/record/369760.

Kötz, H. 2003, "Civil Justice Systems in Europe and the United States." *Duke Law* 1.

Langbein, J. 1985, "The German Advantage In Civil Procedure." *University of Chicago Law Review* 52(4).

Langner, R. 2013, "To Kill A Centrifuge." http://Perma. Cc/8G3X-Gr9K.

Li, J., X. Ou & R. Rajagopalan 2010, "Uncertainty and Risk Management in Cyber Situational Awareness." https://www. academia. edu/89056610/Uncertainty_and_Risk_Management_in_Cyber_Situational_Awareness#:~:text = The% 20uncertainty% 20challenge% 20exists% 20in% 20all% 20three% 20phases, uncertainty% 20in% 20these% 20three%

20aspects%20are%20slightly%20different.

Lind, E. &T. Tyler 1988, "The Social Psychology of Procedural Justice." *Contemporary Sociology A Journal of Reviews* 18(5).

Loomis, A. 2008, *Leveraging Legitimacy In Securing U. S. Leadership: Normative Dimensions Of Hegemonic Authority*, Ph. D. Thesis of Georgetown University.

Manget, F. 2006, "Intelligence and the Criminal Law System." *Stanford Law &Policy Review* 17.

Marcus, M. 1992, "Above The Fray or into the Breach: The Judge's Role in New York's Adversarial System of Criminal Justice." *Brooklyn Law Review* 57(4).

Margulies, P. 2013, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility." *Melbourne Journal of International Law*, *Melbourne* 14(2).

Mearsheimer, J. 2001, *The Tragedy of Great Power Politics*, New York: W. W. Norton & Company.

Meyer, J. 2016, "Why Experts Are Sure Russia Hacked The Dnc Emails." http://Perma. Cc/Vlk7-Dcby.

Moravcsik, A. 2014, "Liberal Theories of International Law." in J. Dunoff & M. Pollack eds., *Interdisciplinary Perspectives on International Law and International Relations: The State of the Art*, Cambridge: Cambridge University Press.

Mosk, R. 1987, "Lessons from the Hague: An Update on the Iran-United States Claims Tribunal." *Pepperdine Law Review* 14(4).

Nance, D. 2010, "Adverse Inferences about Adverse Inferences: Restructuring Juridical Roles for Responding to Evidence Tampering by Parties to Litigation." https://www. bu. edu/law/journals-archive/bulr/documents/nance. pdf.

Nye, J. 2010, "Cyber Power." http://Perma. Cc/3Mcy-3Bn5.

Nye, J. 2021, "Soft Power: The Evolution of A Concept." https://doi. org/10. 1080/2158379X. 2021. 1879572.

Parisi, F. 2002, "Rent-Seeking Through Litigation: Adversarial and Inquisitorial Systems Compared." *International Review of Law and Economics* 22(2).

Raz, J. 1985, "Authority, Law and Morality." *The Monist* 68(3).

Rid, T. & B. Buchanan 2014, "Attributing Cyber Attacks." *Journal of Strategic Studies* 38(1-2).

Sahimi, M. 2009, "The Hostage Crisis, 30 Years on." http://Perma.Cc/M42L-Gtkw.

Sanger, D. & M. Fackler 2015, "N. S. A. Breached North Korea Networks Before Sony Attack, Officials Say." http://Perma.Cc/P3Bb-Kabj.

Scharf, M. & M. Day 2012, "The International Court of Justice's Treatment of Circumstantial Evidence and Adverse Inferences." *Chicago Journal of International Law* 13(1).

Schmitt, M. 1999, "Computer Network Attack and the Use of Force in International Law: Thoughts on A Normative Framework." *Columbia Journal of Transnational Law* 37.

Sells, S. 2003, *Private Power, Public Law: The Globalization of Intellectual Property Rights*, Cambridge: Cambridge University Press.

Simmons, B. & A. Danner 2010, *Credible Commitments and the International Criminal Court*, Cambridge: Cambridge University Press.

Simmons, B. 2009, *Mobilizing for Human Rights: International Law in Domestic Politics*, New Haven: Harvard University.

Singer, P. & A. Friedman 2014, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford: Oxford University Press.

Straus, M. 1986, "The Practice of the Iran-U. S. Claims Tribunal in Receiving Evidence from Parties and from Experts." *Journal of International Arbitration* 3.

Strier, F. 1992-1993, "What Can the American Adversary System Learn From An Inquisitorial System of Justice?" https://heinonline.org/HOL/LandingPage?handle=hein.journals/judica76&div=30&id=&page=.

Tanase, M. 2003, "IP Spoofing: An Introduction." http://Perma.Cc/5Ege-9Rdv.

Tesón, F. 1992, "The Kantian Theory of International Law." *Columbia Law Review* 92.

Thirlway, H. 2016, *The International Court Of Justice*, DOI: 10.1093/law/9780198779070.001.0001.

Tomlinson, E. 1983, "Nonadversarial Justice: The French Experience." *Maryland Law Review* 42(1).

Voeten, E. 2013, "Public Opinion and the Legitimacy of International Courts." *The Journal*

Theoretical Inquiries in Law https://doi.org/10.1515/til-2013-021.

Waxman, M. 2011, "Cyber-Attacks and the Use of Force: Back to The Future of Article." *The Yale Journal of International Law* 2(4).

Weber, M. 1968, *Economy and Society: An Outline of Interpretive Sociology*, [S. L.]: [S. n.].

Whitman, J. 2005, *The Origins of "Reasonable Doubt": Theological Roots of the Criminal Trial*, New Haven: Yale University Press.

Williams, K. 2016, "Clinton: Treat Cyberattacks 'Like Any Other Attack'." http://Perma.Cc/L4Ju-4Jzk.

Zetter, K. 2015, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Taipei: Crown.