欧盟网络制裁机制的国际法透视*

张　华

内容提要:欧盟网络外交近年来发展迅猛。随着恶意网络活动的日渐增多,欧盟在网络外交的框架下快速建立了网络制裁机制,并正式付诸实施。欧盟网络制裁的制度设计形式上与欧盟以往的制裁机制保持了一致,但存在法律方面的不确定性:“网络攻击”的界定过于宽泛;“严重后果”的适用难以客观化;回避网络攻击的归因与证据问题;过分强调审慎原则的规制效用;倡导集体制裁的倾向。这些问题将不同程度地制约欧盟制裁机制的顺利运作。由合法性角度观之,欧盟目前针对个人或实体的网络制裁措施尚无法以国际法上的还报或反措施来证立;由实效性角度观之,欧盟网络制裁机制的威慑和劝诫效果不宜过分夸大。有鉴于此,欧盟应谨慎使用网络制裁。现阶段,在欧盟网络制裁尚未扩大化的情况下,中国可以对欧盟的网络制裁机制保持适度的克制和警惕。

关键词:欧盟网络外交　网络制裁　合法性　实效性　国际法

欧盟网络外交近年来发展迅猛,成为欧盟对外关系中新兴的政策领域。继2019年欧盟正式建立网络制裁①机制后,2020年7月30日,欧盟首次针对第三国具体的个人、实体和机构实施网络制裁。引人注目的是,除俄罗斯和朝鲜的个人、实体和机构被列入制裁名单外,中国的2名公民和1家企业也赫然在列。中国外交部新闻发言人在7月31日主持例行记者会时,对欧盟的做法深表关切,并表示将密切关注有关动向。②10月22日,欧盟再次对俄罗斯个人和机构实施网络制裁。欧盟网络制裁有趋于频繁使用的可能。有鉴于此,笔者拟从国际法和欧盟法层面深入剖析欧盟最新建立的网络

* 本文系2020年国家社会科学基金重大项目“网络空间国际规则博弈的中国主张与话语权研究”(项目编号:20&ZD204)的阶段性成果。

① “制裁”(sanction)在欧盟法律体系中一般以“限制性措施”(restrictive measures)作为代称。虽然欧盟的法规和政策文件统一使用“限制性措施”,但不少欧盟官员在发表演讲时经常交替使用两者。本文为论述方便,亦采取交替使用的办法,仅在复述欧盟官方文件原始内容时,偶尔沿用“限制性措施”一词;在进行客观的法律分析和论证时主要使用“制裁”这一表述。

② 参见“2020年7月31日外交部发言人汪文斌主持例行记者会”,外交部网站,https://www.fmprc.gov.cn/web/fyrbt_673021/jzhsl_673025/t1803035.shtml,2020年8月1日访问。

制裁机制。具体而言,文章首先在概述欧盟网络外交近年来发展情况的基础上,厘清欧盟网络制裁机制赖以建立的政策背景和实质动因,继而依据欧盟部长理事会的相关法律文件,对欧盟网络制裁的核心制度和内容进行类型化分析;其次从国际法和欧盟法角度深入探讨欧盟网络制裁机制的法律不确定性,揭露其内在的法律缺陷;最后从合法性和实效性角度对欧盟网络制裁的实施进行前瞻性思考,并从法律层面提出中国方面的因应之道。

一 欧盟网络制裁机制的演化

出于对网络安全问题和外部网络威胁的关切,欧盟及其成员国近年来在网络外交方面不断加强资源整合和政策协调,成为当前全球网络空间治理进程中不容小觑的"欧洲力量"。受多方面因素的影响,欧盟在联合外交反应机制的框架下迅速建立和实施网络制裁机制,试图威慑和回应源自外部的恶意网络活动,引发国际社会的高度关注。

(一)欧盟网络制裁机制的发展进程

欧盟网络制裁机制是近年来欧盟网络外交政策不断演化的产物。2015 年 2 月 11 日,为响应《欧盟网络安全战略》,①欧盟部长理事会通过了关于网络外交的决议(简称《欧盟网络外交决议》),②正式启动了欧盟网络外交的建设进程。从内容来看,《欧盟网络外交决议》显示出欧盟意图在全球网络空间治理进程中彰显"规范性力量"的决心,其中合作与对话之类的积极措施构成欧盟网络外交的优先选项。

随着近年来全球网络攻击事件的频繁发生,欧盟网络外交开始聚焦恶意网络活动的反应措施。2017 年 6 月 19 日,欧盟部长理事会通过了"针对恶意网络活动的欧盟联合外交反应框架"的决议,③引进了所谓"欧盟网络外交工具箱"(Cyber Diplomacy Toolbox)。欧盟确认共同外交与安全政策(Common Foreign and Security Policy,CFSP)框架下的措施——包括必要时采取的限制性措施,适合针对恶意网络活动的欧盟联合外交反应框架。欧盟同时呼吁成员国、欧盟对外行动署和欧盟委员会进一步落实欧盟联合外交反应框架,并一道制定相关的实施指南。

① European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, "Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace," Brussels, 7.2.2013, JOIN (2013) 1 final.

② Council of the European Union, "Council Conclusions on Cyber Diplomacy," Brussels, 11 February 2015, 6122/15.

③ Council of the European Union, "Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities," Brussels, 7 June 2017, 9916/17.

2017 年 10 月 11 日,欧盟部长理事会下属的政治与安全委员会(Political and Security Committee,PSC)制定了《实施指南》,[①]列举了五类措施,包括预防性措施、合作性措施、稳定性措施、限制性措施,以及欧盟为成员国合法应对而提供的支持措施。在阐述限制性措施时,《实施指南》明确提出,欧盟在必要的情况下,为应对恶意网络活动,可以根据《欧洲联盟条约》第 29 条以及《欧洲联盟运行条约》第 215 条,对第三国、实体或个人采取限制性措施。限制性措施旨在改变被制裁国家、政府、实体或个人的政策或活动,主要包括旅行禁止、武器禁运和资产冻结。

2018 年 4 月 16 日,欧盟部长理事会通过了关于恶意网络活动的决议,[②]强烈谴责对信息和通信技术(Information and Communications Technologies,ICTs)的恶意使用,强调将信息和通信技术用于恶意目的属于不可接受的行为。部长理事会认为,“欧盟网络外交工具箱”有助于网络空间的冲突预防、合作和稳定。其规定了 CFSP 框架下的措施——包括限制性措施,以用于预防和回应恶意网络活动。2018 年 6 月 13 日,欧盟委员会和欧盟外交与安全政策高级代表发布了“提升恢复力和增强处理混合型威胁的能力”的联合通讯。[③] 该文件指出:“欧盟网络外交工具箱”中的措施——包括限制性措施——被成员国运用得越多,就越能发挥威慑作用。[④] 2018 年 6 月 28 日,欧洲理事会通过决议,强调应增强对源于欧盟境外的网络安全威胁的打击能力。欧洲理事会要求欧盟机构和成员国实施联合通讯中所提及的措施,包括网络攻击的归因和“欧盟网络外交工具箱”的实际运用。[⑤] 2018 年 10 月 18 日,欧洲理事会通过决议,[⑥]呼吁通过欧盟的制裁,提高对网络攻击的反应与打击能力。

在上述一系列政策文件“紧锣密鼓”式的呼吁下,2019 年 5 月 17 日,欧盟部长理事会通过了“针对威胁欧盟或其成员国的网络攻击采取限制性措施”的第 2019/797 号决定,[⑦]建立了针对自然人、法人、实体或机构的网络制裁机制。在此基础上,经欧

① Council of the European Union, “Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities,” Brussels, 9 October 2017, 13007/17.

② Council of the European Union, “Council Conclusions on Malicious Cyber Activities—Approval,” Brussels, 16 April 2018, 7925/18.

③ European Commission and High Representative of the Union for Foreign Affairs and Security Policy, “Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats,” Brussels, 13.6.2018, JOIN (2018) 16 final.

④ Ibid., p.8.

⑤ European Council, “European Council Meeting (28 June 2018) - Conclusions,” Brussels, 28 June 2018, EUCO 9/18, p.6.

⑥ European Council, “European Council Meeting (18 October 2018) - Conclusions,” Brussels, 18 October 2018, EUCO 13/18, p.2.

⑦ Council Decision (CFSP) 2019/797 of 17 May 2019 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or Its Member States, [2019] OJ L129 I/13.

盟外交与安全政策高级代表提案,部长理事会同时通过了第 2019/796 号条例,①其中规定了资产冻结措施。时隔一年多之后,2020 年 7 月 30 日,部长理事会又在 CFSP 框架下通过了第 2020/1127 号决定,②并制定了配套的第 2020/1125 号条例,③将制裁名单增加至第 2019/797 号决定的附件,首次启动了网络制裁。欧盟首批网络制裁的对象涉及中国、俄罗斯和朝鲜的 6 名公民、2 家企业和 1 家军事机构。10 月 22 日,欧盟部长理事会再次在 CFSP 框架下通过了第 2020/1537 号决定,④以及配套的第 2020/1536 号条例,⑤制裁 2 名俄罗斯公民和 1 家军事机构。从目前欧盟对恶意网络攻击的强烈反应来看,不排除未来它会更加频繁地采取网络制裁。

(二)欧盟网络制裁机制的发展动因

欧盟网络制裁机制的出台异常迅速。从 2015 年“欧盟网络外交”提出至今,在不到五年的时间内,欧盟即已完成了网络外交的“布局”,同时在很短的时间内建立了网络制裁机制,并付诸实施。归纳起来,推动欧盟网络制裁机制迅速出台的动因大致包括四个方面。

第一,贯彻《欧盟网络安全战略》和实施网络外交政策的需要。2013 年,《欧盟网络安全战略》将保护和促进一个单一、开放、自由和安全的网络空间作为核心目标。在擘画第五个方面的战略优先点和行动计划时,《欧盟网络安全战略》明确提出:将网络空间问题纳入欧盟对外关系和 CFSP,并使之主流化。⑥ 在此基础上,欧盟网络外交得以快速发展。根据“欧盟网络外交工具箱”,欧盟采取网络制裁措施的直接目的在于:向恶意网络活动释放信号,影响网络空间潜在攻击者的行为,以此加强欧盟及其成员国的安全。⑦ 与此同时,网络制裁亦服务于欧盟在全球网络空间治理进程中彰显“规范性力量”的需要。《欧盟网络外交决议》规定其网络外交很重要的一个方面在于:坚持现行国际法适用于网络空间,提倡“网络空间负责任国家行为规范”,强烈主

① Council Regulation (EU) 2019/796 of 17 May 2019 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or Its Member States, [2019] OJ L129 I/1.

② Council Decision (CFSP) 2020/1127 of 30 July 2020 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or Its Member States, [2020] OJ L246/12.

③ Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 Implementing Regulation (EU) 2019/796 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or Its Member States, [2020] OJ L246/4.

④ Council Decision (CFSP) 2020/1537 of 22 October 2020 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or Its Member States, [2020] OJ L351 I/5.

⑤ Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of Implementing Regulation (EU) 2019/796 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or Its Member States, [2020] OJ L351 I/1.

⑥ European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, “Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace,” pp.15-16.

⑦ Council of the European Union, “Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities,” p.5.

张国家对网络空间的国际不法行为应承担法律责任。① 相应地,采取与恶意网络攻击的范围、规模、期限、密度、复杂性和影响相称的制裁措施符合“欧盟和成员国在国际网络空间政策讨论进程中应发挥关键作用”这一战略定位。

第二,受到近年来外部网络攻击事件的刺激,欧盟从最初优先考虑积极措施转向积极措施与消极措施并举。从第 2020/1127 号制裁决定和第 2020/1537 号决定的附件所列举的制裁理由来看,促使欧盟接连两次实施网络制裁的网络攻击事件包括:2015 年针对德国联邦议会的网络攻击、2017 年的“WannaCry”和“NotPetya”网络攻击、2018 年针对禁止化学武器组织(Organization for the Prohibition of Chemical Weapons, OPCW)荷兰总部的未遂网络攻击,以及“云端跳跃行动”(“Operation Cloud Hopper”)网络攻击。在欧盟看来,这些网络攻击事件造成了严重后果,构成对欧盟及其成员国的外部威胁,只有诉诸网络制裁才能预防、阻止、威慑和回应持续的恶意网络攻击活动。

第三,荷兰、德国、英国、爱沙尼亚等个别欧盟成员国的极力推动。例如,荷兰在 2016 年担任轮值主席国期间出具了一份非正式文件,擘画了一系列针对网络攻击的外交反应措施。该文件得到了欧盟部长理事会下属的 PSC 的认可。后者请求欧盟对外行动署在此基础上进一步阐明相关措施,遂为 2017 年“欧盟网络外交工具箱”的出台提供了持续的动力。② 又如,在 2018 年英国索尔兹伯里(Salisbury)神经毒气袭击事件后,负责调查此事件的 OPCW 荷兰总部于 2018 年 4 月遭受未遂网络袭击,英国和荷兰为此呼吁制裁俄罗斯。再如,2020 年 6 月,就 2015 年德国议会遭受网络攻击这一事件,德国在欧盟内部提议制裁俄罗斯的个人和实体。2020 年 7 月 1 日,德国开始担任为期半年的欧盟轮值主席国。不无巧合的是,欧盟网络制裁于 7 月 30 日首次付诸实施,并于 10 月 22 日再度实施。

第四,受到美国网络制裁实践的启发。自 2014 年 11 月美国索尼影业公司据称遭到来自朝鲜的网络攻击以来,美国先后对朝鲜的若干个人和实体实施了一系列制裁。2015 年 4 月 1 日,时任美国总统奥巴马发布行政命令,宣布设立针对网络攻击的制裁制度。根据该总统行政令,美国网络制裁的对象是那些通过网络行为破坏国内重要基础设施和电脑网络系统、窃取商业机密或敏感信息的个人和实体。美国政府相关部门将有权对通过恶意网络行为威胁美国利益的个人和实体实施制裁措施,包括资产冻结

① Council Conclusions on Cyber Diplomacy, p.7.

② 有关荷兰在欧盟网络外交出台背景中的建设性作用,参见“Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace,” https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, last accessed on 1 December 2020。

和旅行禁止等。[①] 美国自此接连对朝鲜、俄罗斯和伊朗等国的个人和实体实施网络制裁措施。相关研究表明,欧盟与美国在经济制裁方面存在较强的协作关系。[②] 鉴于恶意网络攻击事件往往影响全球,美国与欧盟若干成员国近年来明显加强了联合归因方面的合作。[③] 欧盟在制裁法规中也表示需要在网络制裁方面与第三国加强协作,以确保制裁发挥最大的威慑效应。

二 欧盟网络制裁的法律制度设计

欧盟对外制裁分为两种:第一,联合国安理会授权的制裁;第二,自发性制裁,即在无联合国授权的情况下,欧盟自发采取的制裁措施。欧盟网络制裁机制即属于后者。作为 CFSP 框架下的一项政治工具,欧盟启动网络制裁的前提是欧盟部长理事会依据《欧洲联盟条约》第 29 条,以全体一致方式做出制裁决定。[④] 欧盟部长理事会的第 2019/797 号决定建立了欧盟的网络制裁机制,规定了资产冻结和旅行禁止这两类针对自然人、法人、实体或机构的制裁措施,亦即所谓的"定向制裁"(targeted sanction)。旅行禁止属于成员国专属权能的范畴,自然应由成员国自行决定实施方式。资产冻结则有所不同。根据《欧洲联盟运行条约》第 215 条,部长理事会应在 CFSP 制裁决定的基础上,经欧盟外交与安全政策高级代表和欧盟委员会联合提议,以特定多数方式通过配套的条例,规定资产冻结这一措施。[⑤] 与部长理事会第 2019/797 号决定一道制定的第 2019/796 号条例由此产生。以下将依据相关法律文件对欧盟网络制裁的法律制度设计进行类型化分析。

(一)欧盟网络制裁的适用条件

触发欧盟网络制裁的前提是:网络攻击产生严重后果(significant effect),且构成对欧盟或其成员国的外部威胁。不仅如此,具有潜在严重后果的未遂网络攻击(attempted cyber-attacks),如果构成对欧盟或其成员国的外部威胁,也会导致欧盟的网络

① 参见"美国设立网络攻击相关制裁制度",中华人民共和国国家互联网信息办公室,http://www.cac.gov.cn/2015-04/02/c_1114844777.htm,2020 年 12 月 1 日访问。

② 刘建伟:《美欧经济制裁协作的特点、限度及其走向》,载《国际问题研究》,2019 年第 5 期,第 49-56 页。

③ 例如,2017 年 12 月,美国联合英国、丹麦等国就"WannaCry"网络攻击事件进行归因,将攻击来源锁定为朝鲜。同年,美国又和英国等 11 个国家开展联合归因,将"NotPetya"网络攻击的来源锁定为俄罗斯。2018 年 10 月 4 日,就此前 OPCW 总部和世界反兴奋剂机构遭受网络攻击事件,英国和荷兰联合发表声明,同时美国司法部起诉俄罗斯 7 名军事情报人员。这两起事件均被归因于俄罗斯。

④ 《欧洲联盟条约》第 29 条规定:就欧盟针对某一具有地理性质或主题性质的特殊事项应采取的方法,应由欧盟部长理事会以决定的方式做出规定。Consolidated Version of the Treaty on European Union, [2012] C326/13, Art.29.

⑤ Consolidated Version of the Treaty on the Functioning of the European Union, [2012] C326/47, Art.215.

制裁。甚至特定条件下“对第三国或国际组织的网络攻击”亦会激发网络制裁。[①] 欧盟制裁法规还特别就“网络攻击”“严重后果”和“外部威胁”做了较为细致的规定。其中,构成外部威胁的严重网络攻击包括:(1)源于欧盟境外,或在欧盟境外开展的网络攻击;(2)使用欧盟境外基础设施的网络攻击;(3)由欧盟境外自然人,或欧盟境外成立或运行的法人、实体或机构开展的攻击;(4)由欧盟境外自然人、法人或实体支持、指挥或控制的网络攻击。第四种情境意味着,如果有证据表明,欧盟境外自然人、法人或实体对欧盟境内的网络攻击提供了支持,或者是指挥或控制了网络攻击,那些在欧盟境内发动的网络攻击亦有可能激发欧盟的网络制裁。简言之,只要针对欧盟或其成员国的严重网络攻击具有外部因素,即有可能触发欧盟的网络制裁。

(二)网络制裁的方式

欧盟制裁的常规措施包括:金融制裁,即所谓的资产冻结,属于欧盟权能的范畴,由欧盟以条例的形式决定实施机制;武器禁运,理论上属于欧盟权能范畴,但事实上由成员国自主决定实施机制;[②]旅行禁止,即拒绝发放签证,拒绝入境或过境,属于成员国权能的范畴。广义上,欧盟制裁措施还包括中止贸易往来和行业合作。目前欧盟网络制裁的方式是旅行禁止和资产冻结。根据第 2019/797 号决定第 4 条和第 5 条,对于以下三种类型的自然人、法人、实体或机构,成员国应采取必要措施,以防止相关人员入境或过境,或者是冻结其资金或经济资源,具体包括:(1)对网络攻击或未遂网络攻击负有责任;(2)为网络攻击提供财政、技术或物质支持,或者是以其他形式介入网络攻击——包括计划、准备、参加、指示、援助或鼓励此类攻击,或者以作为或不作为的方式促成此类攻击;(3)与上述活动的自然人、法人、实体或机构有联系。[③]

(三)网络制裁的例外安排

欧盟网络制裁机制在规定旅行禁止和资产冻结的同时,还允许一些例外存在。就旅行禁止而言,这些例外包括:第一,欧盟成员国无拒绝其国民入境的义务;第二,当欧盟成员国为欧洲安全与合作组织(Organization for Security and Co-operation in Europe, OSCE)东道国时,不适用欧盟的限制性措施;第三,欧盟成员国负有国际法上的特定义

① 例如,根据欧盟第 2020/1127 号决定,欧盟之所以首次制裁俄罗斯公民和机构,原因是 2018 年 4 月俄罗斯 4 名军事情报人员试图对 OPCW 总部的无线网络开展网络攻击,只是由于荷兰情报部门的阻止而未遂。

② 《欧洲联盟运行条约》第 346 条规定:“任何成员国都可以采取它所认为必要的措施,以保护其与武器、军火或战争物资之生产或贸易相关的基本安全利益。”这一例外规定使得成员国可以自主决定有关武器禁运的实施机制,欧盟只是在 CFSP 框架下通过有关武器禁运的决定。

③ Council Decision(CFSP) 2019/797, Art.4(1).

务时,[①]亦不适用欧盟限制性措施。[②] 另外,欧盟成员国在特殊情形下还可以酌情免除旅行禁止措施。[③]

就资产冻结而言,成员国主管当局可以在其认为适当的条件下,授权解冻一些资金或经济资源,或者是允许获取一些资金或经济资源。这些例外情况主要涉及被制裁对象的基本生活需求、合理的服务费用和日常维持费用。此外,如果涉及外交使团、领事使团、国际组织或仲裁裁决的资金或经济资源,在满足特定条件时,资产冻结措施可以有所松动。[④] 最后,资产冻结亦不妨碍被制裁的自然人、法人、实体和机构支付制裁日期之前所达成的合同。

(四)通知与除名制度

根据第2019/797号决定,欧盟网络制裁名单的制定和修订程序是:在欧盟一个成员国或欧盟外交与安全政策高级代表提案的基础上,由部长理事会以全体一致方式通过决定。部长理事会应将制裁决定以及列入制裁名单的理由直接告知相关的自然人、法人、实体或机构,或者发布公报,并为其提供陈述意见的机会。当后者提交意见或者是新的实质性证据时,部长理事会应对此前的制裁决定进行审查,并通知相关的自然人、法人、实体或机构。[⑤] 这就为遭受欧盟网络制裁的个人和实体提供了"除名"的机会。申言之,由于网络攻击追踪溯源和国家归因存在技术、政治和法律方面的困难,不太可能精准确定网络攻击或未遂攻击的违法者,网络制裁机制中的除名制度就显得尤为必要。

由上述内容可见,除适用条件有所不同外,欧盟网络制裁机制中有关资产冻结、旅行禁止和例外安排的具体规定大体上沿袭了欧盟对外制裁的标准模式。[⑥] 欧盟对外制裁的经验累积使得欧盟可以"驾轻就熟"地出台网络制裁措施。当然,这也意味着在研判网络制裁机制相关法律问题时,欧盟其他制裁机制既有的经验和教训可以作为

① 第三种例外中,欧盟成员国的国际法义务涉及四个方面:作为政府间国际组织的东道国;作为联合国召开的国际会议的东道国;多边国际条约赋予特权与豁免时的义务;根据教廷与意大利1929年所缔结之《拉特兰条约》所产生的义务。

② Council Decision(CFSP) 2019/797, Arts.4(2), (3), (4).

③ 欧盟制裁决定规定了两类特殊情形。首先,欧盟成员国可以基于下述理由免除限制性措施:紧急人道主义需要,参加政府间会议,或者是联合国所主办或支持的国际会议,或者是成员国作为OSCE主席国所主办的国际会议。其次,当入境或过境对于履行司法程序为必需时,成员国亦可以免除限制性措施。Ibid., Arts.4(6), (7).

④ 具体而言,如果相关的资金或经济资源是从外交、领事使团或享有国际法上豁免权的国际组织的账户中缴纳或缴出,且支付被用于外交或领事使团或国际组织的官方目的之范围内,资产冻结这一措施可以有所松动。此外,对于涉及仲裁裁决的资金和经济资源,在满足特定条件时,成员国主管当局亦可以授权解冻一些资金或经济资源。

⑤ Council Decision(CFSP) 2019/797, Art.6.

⑥ See Council of European Union, "Sanctions Guidelines," Brussels, 4 May 2018, Doc. 5664/18, pp.33-40.

重要参照。

三 欧盟网络制裁机制的法律不确定性

欧盟网络制裁的制度设计看似缜密,且形式上与欧盟以往的制裁机制大体上保持一致。但从国际法和欧盟法的角度仔细审视其内容以及相关的政策文件,仍然可以看出其中存在多个方面的法律不确定性。这些法律问题极有可能导致欧盟网络制裁机制在实践中被滥用,进而激化欧盟与第三国的矛盾。

(一)"网络攻击"的界定过于宽泛

根据欧盟制裁法规,"网络攻击"包含四种未经授权或不合法的网络行动:进入信息系统、信息系统干涉、数据干扰和数据拦截。① 其中,"信息系统干扰"是指那些妨碍或中断信息系统运行的网络活动。"数据干扰"是指删除、损坏、恶化、改变或阻止一信息系统的数据,或者使此类数据无法获取。这类恶意网络活动还包括窃取数据、资金、经济资源或知识产权。"数据拦截"是指通过技术手段,拦截非公共性质的数据传输。② 欧盟对"网络攻击"的上述界定很大程度上受到西方所提倡的"网络空间负责任国家行为规范"的影响。但是,对照目前国际社会有关此类规范的有限共识,③似乎欧盟对"网络攻击"的界定过于宽泛。

例如,欧盟制裁法规将窃取数据、资金、经济资源或知识产权之类的数据干扰活动亦界定为"威胁成员国的网络攻击",据此可激发网络制裁。④ 但实际情况是,目前国际社会对于"网络空间负责任国家行为规范"是否涵盖此类非公共性质的数据干扰活动尚存争议。而导致 2017 年第 5 届联合国信息安全政府间专家组(United Nations Groups of Governmental Experts,UNGGE)进程失败的一个重要原因就在于此。美国在此进程中曾极力主张"网络空间负责任国家行为规范"中应增加一项新的规定:"各国不应通过网络手段窃取知识产权、商业机密和其他敏感商业信息用于获取商业利

① Council Decision(CFSP) 2019/797, Art.1(3).

② Ibid., Art.2.

③ "网络空间负责任国家行为规范"最初由西方国家提出,相关规范在中俄等国向联合国秘书长提交的《信息安全国际行为准则》中亦有所体现。目前这一概念涵盖的规范内容在西方存在不同的版本。UNGGE2015 年报告在"负责任国家行为规范"部分列举了 11 项规范,代表了国际社会迄今为止有关这一概念的有限共识。See Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,22 July 2015,A/70/174.

④ 根据欧盟部长理事会第 2020/1127 号决定,欧盟首次网络制裁的动因是 2018 年前后的"WannaCry"和"NotPetya"网络攻击事件,以及 2019 年"APT10"通过网络窃取知识产权事件。欧盟方面认为,前者造成了欧盟及其他国家严重的损害和经济损失,后者损害了欧盟的完整性、安全性和经济方面的竞争力。

益”。此举引发了各国代表之间的分歧。① 欧盟制裁法规也将“窃取数据、资金、经济资源或知识产权”视为“构成外部威胁的严重网络攻击”,与美国立场如出一辙。这一定程度上超越了国际社会有关“网络空间负责任国家行为规范”的有限共识。从2015年UNGGE报告中所列举的“网络空间负责任国家行为规范”,以及2017年UNGGE进程中的相关争论来看,欧盟制裁法规有关“网络攻击”的界定过于宽泛。实事求是而言,当前不同国家、地区、行业对“网络攻击”的定义都不一致,②就连“关键基础设施”“基础公共服务”“关键国家功能”等概念的内涵和外延也无法获得统一。这些因素都有可能导致欧盟制裁法规中有关“网络攻击”之定义的条款出现解释和适用问题。

另外,欧盟网络制裁甚至适用于未遂网络攻击——如果此未遂网络攻击具有潜在的严重后果,且构成对欧盟或其成员国的外部威胁的话。那么问题在于,由于网络攻击本身具有很强的隐秘性和匿名性,在网络攻击并未奏效的情况下,如何准确识别攻击者的来源?又如何准确判断其具有严重后果?从欧盟回避网络归因的一贯立场,以及下文所述的“严重后果”标准适用时的法律不确定性来看,将网络制裁扩大适用于未遂网络攻击,存在滥用制裁的可能。

(二)“严重后果”的适用难以客观化

触发欧盟网络制裁的网络攻击必须是产生严重后果的外部网络攻击。《网络行动国际法塔林手册2.0版》规定网络攻击构成使用武力或武力攻击时,采取了“规模与后果论”。③ 欧盟制裁法规亦采取此种理论,并试图将之量化。第2019/797号决定第3条列举了有关决定网络攻击之严重后果的7种因素,包括:(1)对经济和社会活动、基础服务、关键国家功能、公共秩序或公共安全等造成扰乱的范围、规模、影响或严重程度;(2)受影响的自然人、法人,实体或机构的数量;(3)相关成员国的数量;(4)导致经济损失的数量;(5)违法者自身或为他人所获得的经济收益;(6)盗取数据的数量或性质,或者是数据泄露事件的规模;(7)所获取的商业敏感数据的性质。这显示出立法者将“严重后果”的标准客观化的努力,对于欧盟机构决定是否采取网络制裁措施具有一定的指导意义。

尽管如此,“严重后果”的判断仍难免落入主观化的窠臼。这是因为,欧盟成员国承受网络攻击的能力并不一样,加之成员国准备状态的不同,网络攻击对成员国产生

① 关于美国的相关主张,以及2017年UNGGE进程中的争论,参见黄志雄:《网络空间负责任国家行为规范:源起、影响和应对》,载《当代法学》,2019年第1期,第64页。

② 朱雁新:《数字空间的战争——战争法视域下的网络攻击》,中国政法大学出版社2013年版,第68-72页。

③ [美]迈克尔·施密特主编:《网络行动国际法塔林手册2.0版》,黄志雄等译,社会科学文献出版社2017年版,第335-341页。

的影响也不尽相同。即使相关成员国认为外部网络攻击的规模和后果极其严重,其他成员国也未必会持同样立场。考虑到欧盟制裁决定的做出需要部长理事会成员的全体一致,成员国对网络攻击严重程度的不同认识将有可能制约欧盟制裁决定的做出。更何况网络攻击的影响和后果可能在短期内无法显现,欧盟制裁法规中并未提及网络攻击的长期影响。至于相关成员国的数量要求为何,欧盟制裁法规也未提供量化标准——事实上也无法做到量化。因此,从欧盟制裁法规中有关"严重后果"标准的措辞和非穷尽式列举来看,关于"外部网络攻击是否对欧盟或其成员国产生严重后果"这一问题的答案注定是主观判断,因个案而定。①

另外一个相关的问题是,欧盟网络制裁在适用于未遂网络攻击时,如何从规模和后果角度来衡量此类网络攻击的严重程度?尤其是在网络攻击并未奏效的情况下,损害后果与未遂网络攻击之间的因果联系如何判断?这同样难以证明。② 再者,既然网络攻击并未奏效,欧盟在严重后果缺失的情况下仍实施网络制裁,这是否有违欧盟法中的比例原则?③ 考虑到该原则在以往欧洲法院涉及制裁的判例法中频繁适用,欧盟对未遂网络攻击实施网络制裁恐怕会遭到比例原则方面的"诘难"。

(三)回避网络攻击的归因与证据问题

欧盟网络制裁的一个典型特征是竭力回避网络攻击的国家归因问题。例如,欧盟第 2019/797 号决定序言部分强调:应将定向制裁措施(targeted restrictive measures)与"国家归因"——即将网络攻击的责任归因于一国——区分开来。前者不等于国家归因,因为归因是基于个案而采取的主权政治决定。在将网络攻击归因于第三国方面,每一个成员国均可以自由做出其决定。④ 在此前欧盟酝酿网络外交政策的过程中,欧盟亦反复强调定向制裁与国家归因之间的差别。例如,"欧盟网络外交工具箱"指出:"归因于一国或非国家行为体仍然是一种主权政治决定,这一决定基于各种来源的情报,并且应当根据国际责任法来确定"。⑤ 相关的《实施指南》在擘画有关援引欧盟联合外交反应措施的流程时,对恶意网络活动的归因问题进行了较为详细的阐释。但

① 例如,在德国的推动下,欧盟于 2020 年 10 月 22 日对俄罗斯军事情报人员和机构实施第二次网络制裁。其主要理由是:2015 年 4 月和 5 月期间德国议会信息系统遭受数日的网络攻击,一些议员和德国总理默克尔的电子邮箱账户受到影响。就此实例来看,似乎欧盟有关"严重后果"的认定门槛较低。

② 根据欧盟第 2020/1127 号决定,欧盟制裁俄罗斯个人和实体的原因是俄罗斯军事情报人员针对 OPCW 荷兰总部的未遂攻击。欧盟的理由是:这一攻击"如果成功,将会损害 OPCW 的网络安全和正在进行中的(关于索尔兹伯里事件)调查工作"。从欧盟的推定中很难看出此未遂网络攻击有何潜在的"严重后果"。

③ 关于欧盟法中的比例原则的详细论述,参见高秦伟:《论欧盟行政法上的比例原则》,载《政法论丛》,2012 年第 2 期,第 87-91 页。

④ Council Decision (CFSP) 2019/797, Recital 9.

⑤ Council of the European Union, "Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities," para.4.

是,《实施指南》的阐释重点是成员国如何在归因方面进行努力和协调,因为“恶意网络活动的归因问题仍然是在各种情报的基础上,基于个案而做出的主权政治决定。每一个成员国都可以在这方面自由做出自己的判断”。①

从表面上看,目前欧盟网络制裁的对象限于自然人、法人、实体或机构,尚未针对第三国,似乎没有归因的必要。而且欧盟一再强调其无意因为制裁个人或实体而影响欧盟与第三国之间的关系。就欧盟决策者的角度而言,欧盟定向制裁是一种模糊化策略,即在不要求将恶意网络活动精确归因于第三国的情况下,径自对能够识别的个人和实体直接实施制裁。至于这些个人和实体的行为能否归因于国家,并非欧盟网络制裁机制考虑的重点。欧盟的直接目的是迫使遭受制裁的个人和实体改变不法行为,间接目标也许是在不刺激第三国的情况下对第三国发出一定的警示。

但事实上,迄今为止引起欧盟强烈关注的网络攻击事件大多与第三国存在一定的联系。或者是因为这些网络攻击是由国家机关的工作人员发起和实施,或者是由国家机关通过“代理人”来间接实施网络攻击。因此,在具体的网络攻击事件中,欧盟决定制裁第三国的自然人、法人、实体或机构,往往涉及国家机关工作人员,或者是国家指挥或控制的人员和实体。② 这就等于向第三国或相关的行为体传达信号,隐晦地表明网络攻击有归因于第三国的可能——只是出于避免双边外交关系的恶化,欧盟选择制裁具体的个人和实体。更何况从欧盟有关审慎原则(due diligence)的强调来看,源自于第三国领土上的个人和实体的网络攻击有可能导致领土国的国际法律责任,甚至可直接归因于领土国。③ 因此,就法律适用的角度而言,实际上在欧盟做出制裁决定之前不可能不适当考虑国家归因的问题。而且只有严肃认真地对待归因问题,才能避免制裁措施的滥用。从确保制裁实效性的角度而言,归因也是欧盟决策时不能回避的一环。目前无论欧盟借口归因属于成员国的主权权能范畴,抑或出于避免激化双边关系的考虑而采用实用主义托词,其实都不符合第三国在法律适用方面的关切。

另外值得注意的是,欧盟认为归因的证据不宜公开。在《实施指南》中,欧盟指出:“在采取适当的反应之前,欧盟成员国并无披露归因所依赖之证据的国际法义

---

① Council of the European Union, “Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities,” p.13.

② 欧盟在 2020 年先后两次以恶意网络活动为由制裁俄罗斯的公民和机构。这些俄罗斯公民是隶属俄罗斯联邦武装力量总参谋部情报总局(Main Directorate of the General Staff of the Armed Forces of the Russian Federation,GRU)的军事情报官员——其中包括 GRU 的负责人,遭受制裁的机构是 GRU 下属的特种技术中心(Main Centre for Special Technologies,GTsST)。

③ 近年来有不少国际法学者主张,在依据传统的归因标准无法将非国家行为体的网络攻击行为直接归因于一国的情况下,如果非国家行为体发起网络攻击的领土国未恪守审慎原则,那么该领土国需要对非国家行为体的网络攻击承担国际法律责任。See Luke Chircop, “A Due Diligence Standard of Attribution in Cyberspace,” *International and Comparative Law Quarterly*, Vol.67, 2018, p.645.

务”。当然,“成员国可以选择与其他成员国分享证据,以使得欧盟的联合外交反应措施发生效力,或者令其他成员国信服,并一道对恶意网络攻击做出反应”。① 众所周知,关于网络归因的证据是否需要公开的问题,目前国际社会存在很大的争论。② 欧盟的立场实际上不利于全面预防和阻止恶意网络活动。

(四)过分强调审慎原则的规制效用

欧盟网络制裁的另一个典型特征是异常重视审慎原则。③ 在“欧盟网络外交工具箱”中,欧盟提倡对“负责任国家行为规范”的尊重,“确认恶意网络活动可能构成国际法上的不法行为,并强调国家不得开展或蓄意支持有悖其国际法义务的 ICTs 活动,不得蓄意允许他人利用其领土,使用 ICTs 实施国际不法行为”。④ 欧盟及其成员国强烈支持“现存国际法适用于网络空间”这一共识,并怀有“积极支持自愿的、非约束性的网络空间负责任国家行为规范的发展”的坚定承诺。⑤ 在《实施指南》中,欧盟的表述亦反映出对审慎原则的超常重视。欧盟指出:“欧盟在本框架下的措施是用来防止或回应恶意网络活动,这类活动可能源于一国或非国家行为体,或从一国领土上过境——如果该国蓄意允许其领土被用于此类活动,或蓄意支持此类活动。”⑥《实施指南》中还阐释了一国需要为恶意网络活动承担国际法律责任的情形:“当恶意网络活动是由一国开展,或一国需要为在其指挥或控制下的非国家行为体的网络行动负责,或者一国将非国家行为体的行为承认和接受为其自身的行为时,欧盟及其成员国可以动用本框架下的所有措施——包括针对该国的限制性措施”。⑦ 不仅如此,欧盟还表示:“当一国蓄意允许其领土被用于有损欧盟或其成员国的恶意网络活动时,本框架下的措施可用于诱导此国家,使之确保其领土不被用于此种活动”。⑧

---

① Council of the European Union, “Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities,” p.14.

② 例如,英国检察总长赖特(Jeremy Wright)在伦敦查塔姆研究所(Chatham House)代表英国阐述有关“国际法适用于网络空间”的立场时,指出:国际法并不要求国家在所有情况下都应披露其做出归因决定的相关信息,亦不要求其必须公开归因。See Jeremy Wright, “Cyber and International Law in the 21st Century,” Speech Delivered on 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century, last accessed on 26 December 2020.

③ 有关网络空间审慎原则的详细阐释,参见张华:《非国家行为体之网络攻击的国际法律责任问题——基于审慎原则的思考》,载《法学评论》,2019 年第 5 期,第 162-169 页。

④ Council of the European Union, “Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities,” para.2.

⑤ Ibid., para.3.

⑥ Council of the European Union, “Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities,” p.5.

⑦ Ibid.

⑧ Ibid.

从上述措辞来看,欧盟明显沿袭了 UNGGE 报告中有关审慎原则的表达,[①]体现了欧盟贯彻“网络空间负责任国家行为规范”的决心。这意味着,虽然目前欧盟的网络制裁属于针对自然人、法人、实体和机构的“定向制裁”,但不排除未来欧盟将网络制裁的对象扩大至第三国——不仅《实施指南》有关限制性措施的对象中明确提到了第三国,而且审慎原则为欧盟扩大制裁对象提供了潜在的法律依据。但问题在于,审慎原则目前在国际法上的地位和适用存在很大的不确定性。UNGGE 报告所列举之“网络空间负责任国家行为规范”也只是自愿的、非约束性的。[②] 欧盟在网络外交文件中热衷于推崇这类规范,沿用审慎原则的惯用表达,且不排除以此追究相关国家的法律责任,乃至采取制裁措施,显示出欧盟欲将“软法”转化为“硬法”的决心。但是,鉴于审慎原则在现行国际法体系中仍处于演进中状态,欧盟将“应然法”作为“实然法”来适用,恐怕会在制裁实践中引发法律争议。

(五)倡导集体制裁的倾向

欧盟网络制裁机制的适用范围广泛。除对欧盟或其成员国构成外部威胁的网络攻击外,针对第三国或国际组织的网络攻击如果造成严重后果,欧盟亦可以对此采取限制性措施——如果这对于实现《欧洲联盟条约》第 21 条中的 CFSP 目标为必需的话。《欧洲联盟条约》第 21 条规定了欧盟对外行动的目标,其中与 CFSP 密切相关的目标包括:(1)捍卫欧盟的价值、根本利益,安全、独立和完整;(2)巩固和支持民主、法治、人权和国际法的原则;(3)根据《联合国宪章》的宗旨和原则、《赫尔辛基最后文件》的原则以及《巴黎宪章》的目标,维护和平,预防冲突和增强国际安全。[③] 从中可以看出,由于 CFSP 的目标过于宽泛,在第三国或国际组织遭受网络攻击的情况下,欧盟对此采取制裁措施几乎没有限制。但是,考虑到国际法体系中单边制裁的合法性争议,[④]欧盟因第三国或国际组织遭受网络攻击而采取制裁恐有不妥。

就反措施的角度而言,欧盟或其成员国作为网络攻击的受害方,对负有责任的第三国采取网络制裁尚属合法。欧盟对相关的自然人、法人、实体或机构实施制裁也可谓“师出有名”——虽然不无合法性方面的争论。但在第三国或国际组织遭受网络攻

① 2015 年 UNGGE 报告第 12 段所列举的“网络空间负责任国家行为规范”中至少有两项涉及审慎原则,分别是:(c)各国不应蓄意允许他人利用其领土使用 ICTs 实施国际不法行为;(f)各国不应违反国际法规定的义务,从事或故意支持蓄意破坏关键基础设施或以其他方式损害为公众提供服务的关键基础设施的利用和运行的 ICTs 活动。

② “网络空间负责任国家行为规范”本质上属于国际软法的范畴,是为了弥补现行国际法的不足而提出的概念和制度。参见黄志雄:《网络空间负责任国家行为规范:源起、影响和应对》,第 65-66 页。

③ Consolidated Version of the Treaty on European Union, [2012] C326/13, Arts.21(a), (b), (c).

④ See Barry Carter, “Economic Sanctions,” in Rüdiger Wolfrum, ed., *Max Planck Encyclopedia of Public International Law*(*Vol.III*), Oxford University Press, 2012, pp.328-329.

击的情况下,欧盟及其成员国并非网络攻击的受害方。除非有条约特殊的规定,欧盟无论是在合法性层面,还是在正当性层面,其实都缺少采取制裁措施的空间。可以预料的是,欧盟因此制裁相关国家的自然人、法人、实体或机构,极易激化欧盟与相关国家之间的矛盾。①

考虑到欧盟未来有可能针对国家采取网络制裁措施,在第三国或国际组织遭受网络攻击的情境下,欧盟针对相关国家的网络制裁也许构成集体反措施。但众所周知,集体反措施在国际法上的合法性存在争论,②尚未被接受为普遍的国际法规则。因此,欧盟此类网络制裁的合法性其实也无法通过集体反措施来证立。

另外,欧盟网络制裁法规中的措辞近似于欧洲法院扩张欧盟对外权能时的"平行原则"(principle of parallelism)——当对外行动是实现欧盟内部权能的目标所必需时,欧盟因此享有隐含的对外权能。③ 从欧盟制裁法规的表述来看,这等于是扩大了欧盟在 CFSP 领域的权能,亦即在原本不属于欧盟对外权能的领域,由欧盟决定采取网络制裁措施。更何况,根据欧盟对外关系法的基本原理,"平行原则"原本就不能适用于 CFSP 领域。④ 因此,欧盟制裁决定中的这一规定有违欧盟对外关系法的根本原则——"授权性原则"(principle of conferral),⑤极有可能在欧洲法院招致司法审查之诉。

颇引人注目的是,为使欧盟的制裁措施发挥最大效用,欧盟第 2019/797 号决定第 9 条规定:"欧盟应鼓励第三国采取类似的限制性措施"。由于网络攻击溯源困难,加上国家归因存在技术和政治障碍,真正需要为网络攻击承担责任的行为体其实极易规避网络制裁。更何况网络空间缺乏物理边界,仅依靠欧盟的网络制裁并不足以威慑和劝诫违法者。因此,基于确保制裁实效性的考虑,欧盟提倡与第三国⑥联合制裁恶意网络攻击行为,以产生协同效应。同时,鉴于欧盟网络制裁机制的建立一定程度上受

① 例如,欧盟以 OPCW 荷兰总部的未遂网络攻击事件制裁俄罗斯军事情报人员和机构。俄罗斯外交部在第一时间表示"困惑和遗憾",并声称将依据外交对等原则进行反制。

② [英]安德鲁·克拉彭:《布赖尔利万国公法》,朱利江译,中国政法大学出版社 2018 年版,第 239-241 页。

③ 张华:《欧洲联盟对外关系法原理》,法律出版社 2016 年版,第 30-33 页。

④ "平行原则"不适用于 CFSP,而只适用于具有"超国家性"的欧盟政策领域。一个明显的例证是:《欧洲联盟条约》规定了 CFSP 的宪法性条款;《欧洲联盟运行条约》第 216 条第 1 款吸收了欧洲法院判例法中的"平行原则"。后者不涉及 CFSP。

⑤ 《欧洲联盟条约》第 5 条规定了"授权性原则",即"欧盟仅在由成员国在两部条约中赋予它的权能范围内行动,以实现两部条约规定的目标。两部条约未赋予欧盟的权能属于成员国所有"。

⑥ 对于欧盟而言,最有希望联手实施网络制裁的国家包含四类:欧洲经济区国家,即挪威、冰岛、列支敦士登;欧盟候选成员国,即土耳其、黑山、阿尔巴尼亚;与欧盟缔结有伙伴关系协定或稳定联系协定的国家,如乌克兰、摩尔多瓦、格鲁吉亚;其他相邻的欧洲国家,如瑞士。另外,英国退出欧盟后,亦将同欧盟一道积极实施网络制裁。

到美国实践的启发,不排除在美国制裁或起诉网络攻击行为体时,欧盟亦有可能采取类似措施。① 欧盟联合美国等其他国家一道制裁伊朗,并一度迫使伊朗在2015年改变核政策的成功先例也证明了集体制裁的功效。② 问题在于,欧盟和其他国家制裁伊朗是因为有安理会的决议授权在先,而自发性的网络制裁在国际法上的合法性不无争议。因此,欧盟倡导集体实施网络制裁也只能使用"鼓励"这类非强制性的措辞。

四 欧盟网络制裁机制的反思与前瞻

从2017年《实施指南》明确提及限制性措施至今,欧盟网络制裁机制从无到有,并且正式付诸实施,不过3年左右的时间。这既是因为先前其他制裁机制的经验为欧盟网络制裁的制度设计提供了充足的"养料",也是因为欧盟内部就通过制裁来威慑与回应恶意网络活动这一点迅速达成了共识。可以看出,欧盟与成员国出于联合应对外部网络安全威胁的需要,迫切希望网络制裁发挥威慑效应,以迫使发动网络攻击的自然人、法人、实体或机构"改弦更张",或至少是对其发出警示信号。不过,从合法性和实效性的角度来看,欧盟网络制裁机制其实应谨慎使用。

(一)合法性

制裁在国际法上的合法性问题不无争议。③ 网络制裁在国际法上的法律依据为何?在联合国安理会尚未通过有关网络制裁的专门决议之前,欧盟单方面采取的网络制裁措施难以避免合法性方面的指摘。欧盟方面认为,其实施网络制裁的国际法依据是还报(retorsion)和反措施(countermeasures)。④ 问题是,在一般国际法上,无论是还报抑或反措施,都是发生在国与国之间的双边关系中。还报是指一国以不友好或不礼貌的行为对待另一国不友好或不礼貌的行为,将两者的行为孤立来看,其实都不涉及违反国际法的问题。⑤ 反措施是指受害国针对责任国不履行国际法义务的行为而采取的一种对抗性措施,意在迫使责任国履行国际法义务,或承担国际法律责任。⑥ 目前欧盟网络制裁的对象限于自然人、法人、实体或机构,尚未针对第三国,以还报和反

① 关于欧盟对外制裁中的美国因素,参见王磊、刘建伟:《欧盟对外制裁决策:制度设计与影响因素》,载《国际观察》,2016年第1期,第142-144页。

② 吕蕊、赵建明:《试析欧盟在伊朗核问题中的角色变化与影响》,载《欧洲研究》,2016年第6期,第52-55页。

③ 田斌:《经济制裁:有效与人道的权衡》,中国经济出版社2019年版,第57-58页。

④ 例如,欧盟安全研究院(EUISS)近期发布的研究报告指出,欧盟针对个人或实体的制裁属于国际法上"还报"的范畴,针对国家的制裁属于"反措施"的范畴。See Patryk Pawlak and Thomas Biersteker, eds., *Guardian of the Galaxy: EU Cyber Sanctions and Norms in Cyberspace*, Chaillot Paper, No.155, 2019, p.51.

⑤ [英]马尔科姆·肖:《国际法》,白桂梅等译,北京大学出版社2011年版,第895-896页。

⑥ 贺其治:《国家责任法及案例浅析》,法律出版社2003年版,第305页。

措施来证立“定向制裁”的合法性,难免有“张冠李戴”之嫌。反观之,如果认为还报或反措施构成欧盟网络制裁的国际法依据的话,那等于是暗示:欧盟关于网络制裁对象限于自然人、法人、实体或机构的立场不过是一种外交托词,关于网络制裁无须归因的辩解更是一种推卸责任的借口。

质言之,欧盟针对从事外部网络攻击的自然人、法人、实体或机构采取制裁措施,其实应当从管辖权的角度论证其合法性与否。从保护性管辖的角度①来看,理论上,欧盟及其成员国似乎可以对从事此类网络攻击的自然人、法人、实体或机构行使管辖权,这可以通过执法合作来实现,而无须擅自采取自力救济措施——单边制裁。但实际情况却是,欧盟似乎更倾向于通过单边制裁以遏制恶意网络活动。在国际法上缺乏有关网络制裁的一般性规定或特殊规定的情况下,欧盟单边制裁极有可能冲击第三国的管辖权,从而酿成国际争端。更加合法的方式应当是欧盟与具有管辖权的第三国通过网络执法合作,共同打击恶意网络活动。

不无讽刺的是,就网络执法的现实需要而言,网络制裁倒是有可能产生“适得其反”的后果。例如,成员国对涉及网络攻击的自然人实施旅行禁止,看似具有警示作用,但客观上也使得成员国执法机关无法在欧盟境内利用这些自然人入境或过境的机会实施抓捕行动。② 而在境外实施抓捕又会侵犯他国的管辖权,显然并不可取。因此,即使网络制裁措施短期内可以起到“突袭”和“威慑”的效果,但从法治的角度来看,应优先考虑采取常规的执法措施以应对恶意网络活动。或许只有在第三国不愿意或不能够与欧盟及其成员国开展网络执法合作的情况下,网络制裁才可以作为最后诉诸的措施,获得一定程度的正当性。

(二)实效性

欧盟实施网络制裁的战略考量是对从事网络攻击的相关行为体产生“突袭”和“威慑”效果。但从以往欧盟制裁的实践情况来看,欧盟制裁的实效性可谓“褒贬不一”。③ 在判断制裁机制的实效性时,理论界和实务界首先考虑的指标往往是制裁是否成功地迫使制裁对象改变了行为模式。④ 因为欧盟网络制裁刚刚付诸实施,目前从这方面判断其实效性为时尚早。但需要指出的是,根据相关学者的研究,制裁其实很

① 保护性管辖,是指国家可以对外国人在境外实施的危及相关国家安全的行为行使管辖权。参见[英]马尔科姆·肖:《国际法》,第522页。

② 例如,欧盟2020年10月22日第2020/1537号制裁决定中的旅行禁止措施涉及俄罗斯军事情报官员巴金(Dmitry Sergeyevich Badin)。问题是,在2020年5月,德国方面曾经对其发布了逮捕令。旅行禁止明显不利于逮捕行动。

③ 以欧盟制裁叙利亚为例,参见田斌:《经济制裁:有效与人道的权衡》,第144-146页。

④ See Barry Carter, “Economic Sanctions,” p.323.

少在改变制裁对象的行为模式方面发挥效用。① 就联合国安理会通过的制裁而言,大概只有10%的制裁产生了改变制裁对象的行为模式的效果。② 有鉴于此,不少学者提出了判断制裁实效性的替代性指标,其中最有影响力的两个指标分别是:限制被制裁对象获取资源,从而防止其开展不法行为;向外部和内部的受众发出警示信号。③

如果说短期内尚无法判断欧盟制裁条例是否成功限制被制裁对象获取资源的话,那么至少可以认为,欧盟列举网络制裁名单这一行为本身就已经对外发出了信号。但从实用主义角度来看,以发出警示信号作为判断欧盟制裁实效性的标准难免有"自欺欺人"之嫌——这似乎是在依据其他两种判断标准无法获得积极评价时的托词。最有说服力的标准应该还是制裁是否改变了制裁对象的行为模式,或者是限制了被制裁对象获取资源。需要指出的是,根据以往的制裁经验,资产冻结和旅行禁止有时非但不能产生威慑效应,反而会刺激制裁对象以及相关联的第三国采取更加严重的对抗性措施。④ 因此,欧盟网络制裁的实效性有待进一步观察,欧盟在列举制裁名单和实施制裁措施时,或许象征意义远大于实际意义。

另外,根据上文分析,由于欧盟网络制裁机制存在一系列的法律不确定性,可以预料,未来将会产生不少涉及欧盟网络制裁法规之解释或适用的争端。诸如网络攻击的定义、网络攻击的严重后果标准、网络攻击的归因和证据问题等,极有可能成为欧洲法院诉讼的主题。

更有甚者,一如其他欧盟对外行动,欧盟与成员国之间的权能划分问题,或多或少也会制约欧盟网络制裁机制的实施。由于欧盟的明示权能中并没有专门列举欧盟在网络外交方面的权能,因此,欧盟网络外交只能寄生于其他明示性的对外权能。目前欧盟之所以能够在网络制裁领域有所作为,既是因为网络攻击这一外部威胁促使欧盟内部迅速实现联动协调,也是因为其制裁机制在欧盟基础条约中有较为清晰的法律依据。⑤ 不过,从欧盟对外权能博弈的经验来看,一旦外部威胁消失,或者网络制裁涉及欧盟外交的其他领域,欧盟与成员国之间的权能纠葛难保不会"沉渣泛起"。例如,在网络归因和证据的采集方面,欧盟能否事实上做到完全尊重成员国的判断?或者个别

---

① [美]加利·克莱德·霍夫鲍尔等:《反思经济制裁》,杜涛译,上海人民出版社2019年版,第186-188页。

② Andreas Boogaerts, "A Symbiotic Relationship? Examining the Convergence of Views Between Practitioners and Scholars on Sanctions Effectiveness," *European Foreign Affairs Review*, Vol.23, 2018, p.230.

③ Francesco Giumelli, *How EU Sanctions Work: A New Narrative*, Chaillot Papers, No.129, 2013, pp.18-19.

④ 例如,自2014年开始至今,针对克里米亚问题和东乌克兰问题,美国、欧盟及其盟友先后对俄罗斯实施制裁。此举非但没有迫使俄罗斯让步,反而促使俄罗斯对美国和欧盟采取了反向制裁措施。参见吴大辉:《制裁与反制裁:欧俄相互经济加害难长久》,载《当代世界》,2016年第10期,第14-17页。

⑤ 《欧洲联盟运行条约》第215条第1款承袭原《欧共体条约》第301条,为欧盟制裁第三国提供了法律依据;第215条第2款由《里斯本条约》引进,为欧盟制裁自然人、法人、实体或机构提供了法律依据。

成员国的判断是否就足以确保在欧盟部长理事会决策时实现一致,因而可以通过新的网络制裁决定?这些问题的答案仍有待长期观察。

综上所述,尽管欧盟网络外交奉行“尊重国际法,并且不得侵犯基本权利和自由”原则,①但基于上述合法性与实效性这两个层面的考量,欧盟网络制裁理应谨慎使用。由整个国际关系背景观之,欧盟或许可以借此在网络空间治理的商谈进程中彰显“规范性力量”。② 但过于急切地追求“规范性力量”的欧盟对外行动亦有可能产生负面效应。就网络制裁而言,如果欧盟和美国一样,在制裁实践中长期奉行单边主义和双重标准,将制裁对象限于西方阵营的“假想敌”——例如俄罗斯、朝鲜和伊朗,③又无视网络对话之类的积极措施的话,那么其网络外交的公正性和实效性将难以维系。久而久之,欧盟网络制裁将一定程度地削弱欧盟的“规范性力量”,而非起到建设性作用。欧盟在其他对外政策方面“毁誉参半”的制裁实践可谓“殷鉴不远”。④

五 结语:中国的应对

中国在网络安全问题方面的一贯立场为:“中国是网络安全的坚定维护者,也是黑客攻击的受害国之一,始终依法打击在中国境内或利用中国网络基础设施发起的网络攻击”。⑤ 由于欧盟首次网络制裁即涉及中国公民和企业,本文在全面和深入剖析欧盟网络制裁机制的基础上,有必要再扼要阐述一下中国方面的因应之道。对于当前本国公民和企业遭受欧盟制裁这一异常事件,中国短期内不妨保持适度的克制。形式上,欧盟目前对外声称网络制裁的对象限于个人或实体,并不存在国家归因的问题。无论其真实目的为何,至少欧盟在表面上释放出来的善意为双方的对话和沟通留有余地。中国的合理反应措施应当是加强与欧盟方面的沟通与协调,建立高级别的网络安全对话机制,与之开展良性的网络外交。

对于当前遭受欧盟网络制裁的中国公民和企业而言,可以谋求在欧盟制裁机制的

① Council of the European Union, “Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities,” p.5.

② “规范性力量”这一术语经常被用于描述欧盟对外行动的现实影响力,或者是欧盟自成一类的国际身份。参见严骁骁:《反思“规范性力量欧洲”:理论与实践》,上海人民出版社 2019 年版,第 4-6 页。

③ 有学者在 2020 年 6 月统计,自 2015 年 4 月 1 日奥巴马政府设立网络制裁机制以来,美国已经对来自俄罗斯、伊朗和朝鲜的 96 个公民和企业实施了网络制裁措施。See Stefan Soesanto, “The Case Against EU Cyber Sanctions for the Bundestag Hack,” https://www.lawfareblog.com/case-against-eu-cyber-sanctions-bundestag-hack, last accessed on 1 December 2020.

④ 例如,欧盟以违反人权为由的自发制裁实践存在明显的双重标准和实效性问题,详见张华:《欧洲联盟对外关系法中的“人权条款”问题研究》,法律出版社 2010 年版,第 193-210 页。

⑤ 在 2020 年 7 月 31 日外交部例行记者会上,就欧盟对涉嫌从事网络攻击的两名中国公民和一家中国企业实施制裁这一问题,外交部发言人汪文斌再次阐明了中国的立场,并对此事件做了相关评论。

框架下,利用其中的“除名”制度,或者通过欧盟或成员国法院提起司法审查诉讼。以成员国层面的诉讼为例,遭受制裁的公民或企业可以在成员国法院挑战成员国实施措施的同时,质疑欧盟制裁法规中存在的法律不确定性。此时,成员国法院需要请求欧洲法院就欧盟制裁法规的相关问题发表初步裁决,从而实现对欧盟制裁法规的间接司法审查。就欧盟层面的诉讼而言,遭受制裁的公民和企业可以在欧洲法院系统,以侵犯基本权利和自由等诉因直接提起废除之诉,挑战欧盟相关法规和制裁措施的效力。值得一提的是,在迄今欧洲法院受理的CFSP案件中,个人或实体挑战欧盟制裁法规和措施之效力的案件占绝大多数,其中不乏成功“维权”的典型。① 因此,在无法通过“除名”制度获得权利救济的情况下,遭受制裁的个人和实体可以尝试诉诸欧盟法院的司法审查机制。

当然,诚如上文分析所见,由于欧盟极力推崇“网络空间负责任国家行为规范”,尤其是其中的审慎原则,②不排除欧盟未来有针对国家采取网络制裁的可能。目前中国虽然无须为本国公民和企业遭受欧盟网络制裁而反应过度,但不能没有“未雨绸缪”的意识。鉴于近年来欧美频繁出台单边制裁法案,中国公民和企业遭受外国制裁措施影响的概率明显增加,中国除针对个案采取对抗性的制裁措施外,不妨考虑制定相应的“阻断法案”,③以系统性地遏制或削弱欧美“甚嚣尘上”的单边制裁倾向。对于欧盟最新的网络制裁机制,中国应保持一定的警惕,不排除在国际法允许的范围内适时采取反措施。

最后,基于未来预防争端的考虑,中国也许可以在网络攻击的溯源和证据采集方面,加强与欧盟及其成员国的执法合作,甚至考虑与欧盟成员国开展联合归因的工作,预先促使欧盟及其成员国基于事实做出独立、理性的判断,避免其径自诉诸带有惩戒性和对抗性的制裁措施。如此既可以从源头上消除欧盟实施网络制裁的诱因,同时又可以推动欧盟通过对话合作等积极措施谋求网络争端的和平解决,避免加剧网络空间的紧张对抗,共同维护网络空间的安全与稳定。

(**作者简介:**张华,南京大学法学院副教授;**责任编辑:**宋晓敏)

① 根据学者统计,个人或实体在欧洲法院系统中往往基于以下原则获得权利救济:辩护权、有效的司法保护、对基本权利无理由或不相称的限制、阐明制裁理由的义务、明显的评估错误、违反合法预期和滥用权利。See Luca Pantaleo, “Sanctions Cases in the European Courts,” in Paul Eden and Matthew Happold, eds., *Economic Sanctions and International Law*, Hart Publishing, 2016, p.172.

② 欧盟外交与安全政策高级代表博雷利在2020年7月30日发表的有关欧盟网络制裁的声明中,亦再次“浓墨重彩”地表达了欧盟及其成员国推广“网络空间负责任国家行为规范”和审慎原则的决心。See Declaration by the High Representative Josep Borrell on behalf of the EU: European Union Response to Promote International Security and Stability in Cyberspace, 30 July 2020.

③ 有关欧盟制定阻断法案以应对美国单边制裁的经验,以及对中国立法之启示的相关论述,参见叶研:《欧盟〈阻断法案〉述评与启示》,载《太平洋学报》,2020年第3期,第62-65页。