MMXX

BIMUN

2020 北京国际模拟联合国大会

Beijing International Model United Nations 2019

背景文件

联合国预防犯罪和刑事司法委员会

议题：网络犯罪全球治理

青年使命 和合共生 | Harmony and Coexistence Mission of the Youth

目录

1. 欢迎辞

尊敬的各位代表：

你们好！

欢迎参加 2020 北京国际模拟联合国大会，感谢你们选择了联合国预防犯罪和刑事司法委员会，委员会全体学团成员在此欢迎你们的到来。祝愿你们能在本次大会中深入了解网络犯罪全球治理这一议题，并收获一份参与多边外交的全新体验。

步入 2020，我们迎来了一个新的十年。在这崭新的十年里，以联合国为首的多边外交平台将引领整个国际社会，共同为实现 17 个可持续发展目标而努力奋斗。

网络犯罪的全球共治是第 16 个可持续发展目标——和平、正义与强大机构中的重要议题，为此，在经社理事会以及毒品和犯罪问题办公室的指导下，联合国预防犯罪和刑事司法委员会开始寻求网络犯罪全球治理的新思路、新方法。

治理网络犯罪绝非易事。不同于传统犯罪，网络犯罪以其隐蔽性、危害性、传播性，以及不易预见性等多种特点给社会的安定与和谐带来了巨大的挑战。与此同时，在治理网络犯罪的道路上，除了技术要求较高等能力上的障碍之外，各国在主权平等框架之下的治理体系差异在一定程度上更加限制了国际社会在共同治理这一问题上的协调与平衡。

为破解议题中存在的诸多桎梏，我们将需要各位代表利用自己的智慧与担当，构建并完善网络犯罪治理体系，携手打造一个纯净、安全的网络空间。

我们相信各位代表能够在本次会议中为网络犯罪的全球治理选出一条最为可行的道路，期待大家的精彩发挥！

2020 北京国际模拟联合国大会
联合国预防犯罪和刑事司法委员会
主席团
2020 年 2 月

2. 委员会介绍

2.1 委员会历史

1992 年，根据联合国大会第 46/152 号决议，联合国经社理事会通过第 1992/1 号决议，正式设立了预防犯罪和刑事司法委员会。委员会是经社理事会下的一个职司委员会，同时也是联合国系统内制定预防犯罪和刑事司法政策的中央机构。委员会的前身最早可以追溯到专家咨询委员会，其于 1971 年被以技术工作为重点的犯罪预防和控制委员会所取代，使联合国在刑事司法政策方面的工作覆盖面更加广泛。随后，根据 1991 年在凡尔赛宫举行的一次部长级会议中达成的政治协议，成立预防犯罪和刑事司法委员会。[1]

2006 年，联合国大会通过第 61/252 号决议，进一步扩大了预防犯罪和刑事司法委员会的职权范围：委员会成为联合国毒品和犯罪问题办事处的理事机构，并负责联合国预防犯罪和刑事司法基金预算的批准，以及为世界范围内预防犯罪和刑事司法的领域提供技术援助。

2.2 委员会职权与职能

预防犯罪和刑事司法委员会的职权在于指导联合国在预防犯罪和刑事司法领域内的活动，并审查其在该领域的准则与规范，包括会员国对这些准则和规范的应用和执行情况。预防犯罪和刑事司法委员会通过决议和决定的方式行使其职权，委员会不仅是联合国预防犯罪和刑事司法方案的理事机构，而且是联合国犯罪大会的筹备机构。

预防犯罪和刑事司法委员会的职能在于：在预防犯罪和刑事司法领域同负有具体任务的其他联合国机构进行协调，例如同“联合国打击跨国有组织犯罪缔约方会议”和“联合国反腐败缔约方会议”进行协调；此外，该委员会还为成员国提供一个论坛，用于交流专业知识、经验和信息，制定国家和国际战略，并确定打击犯罪的重点。

委员会每年均举行年度例会，并在闭会期间定期召开会议。其通过决定和决议将大会成果落实为具体行动，同时向毒品和犯罪问题办公室提供政策指导。[2] 每年年底，委员会都会主持重新召开审议预算和行政事项的会议。

2.3 同其他委员会或方案的关系

2.3.1 经济及社会理事会

预防犯罪和刑事司法委员会是经及社理事会的职司委员会之一，同其他的 7 个职司委员会一样，委员会负责在特定领域开展相关工作，亦即负责“预防犯罪和刑事司法”领域的相

1　联合国：《预防犯罪和刑事司法委员会》，载于经社理事会官网，https://www.un.org/zh/aboutun/structure/ecosoc/ccpcj/mandate.shtml，2020 年 2 月 8 日登录；

2　联合国：《预防犯罪和刑事司法委员会》，载于毒品和犯罪问题办公室官网，https://www.unodc.org/unodc/en/commissions/CCPCJ/index.html?ref=menutop，2020 年 2 月 8 日登录；

关工作。

经社理事会规定了预防犯罪和刑事司法委员会的任务和首要工作：包括采取国际行动打击各国和跨国犯罪，如集团犯罪、经济犯罪、洗钱等；加强刑法在环境保护方面的作用；预防城市犯罪，如青少年犯罪与暴力；以及提高刑事司法管理体制的效率和公正性（见第1992/22 号决议）。[3]

2.3.2 联合国毒品和犯罪问题办公室

预防犯罪和刑事司法委员会是联合国毒品和犯罪问题办公室的理事会。委员会负责批准联合国预防犯罪和刑事司法基金的预算方案，此方案为促进全球预防犯罪和刑事司法领域的技术援助提供资源。[4]

2.3.3 联合国预防犯罪和刑事司法大会

预防犯罪和刑事司法委员会为每五年召开的联合国预防犯罪和刑事司法大会提供指导。委员会还审议大会成果并通过决议进一步确定后续措施。在该大会上，预防犯罪和刑事司法领域的政策制定人员和从业人员汇聚在一起，以帮助形成联合国预防犯罪和刑事司法议程和标准。[5] 上一届会议于 2015 年 4 月在多哈举行，会议批准了《多哈宣言》[6]。预期大会的下一次会议将于 2020 年年中举办。

3 联合国：《预防犯罪和刑事司法委员会》，载于经社理事会官网，https://www.un.org/zh/aboutun/structure/ecosoc/ccpcj/mandate.shtml， 2020 年 2 月 8 日登录；

4 同上；

5 联合国：《预防犯罪和刑事司法大会概况》，载于联合国预防犯罪和刑事司法大会官网，https://www.un.org/zh/events/crimecongress2015/about.shtml，2020 年 2 月 23 日登录；

6 编者注：多哈是众多国际多边会议的召开地，因此存在诸多的《多哈宣言》，需注意避免混淆；

3. 议题概述

虽名为“网络犯罪”，但其与“故意杀人罪”、“谋杀罪”、“抢劫罪”等由刑法典规范的具体罪名不同，网络犯罪一词并非法定概念，而是犯罪学意义上对一种新型犯罪的统称。由于这一领域的研究正处于起步阶段，关于网络犯罪确切而统一的定义尚没有形成[7]，我们也尚不能够在此通过下定义的方式给大家明确而又毫无争议地解释什么是网络犯罪。

因此，我们不妨换一种思路，即从描述性概述开始，用描述的方法刻画网络犯罪的大致模样，随后通过具体阐述其分类，以及构成网络犯罪的行为来具体了解何为网络犯罪。最后，我们再通过“全球局势”部分来了解国际社会在治理网络犯罪这一问题上的大致情况。

3.1 网络犯罪的描述性概括

网络犯罪是伴随着信息技术的发展、计算机的普及而出现的一种高智商、高科技犯罪，是计算机发展到高级阶段的产物。[8]

从词义解释上来看，网络犯罪可以拆分成“网络”和“犯罪”。

这里的“网络”不能简单理解成互联网，而应包括广义上的国际互联网、专业计算机信息网、企业计算机信息网等。而“犯罪”则表明了网络犯罪具有犯罪的一般特征。

通常，我们将网络犯罪描述为以网络作为本体、工具或地点的犯罪活动，其形式主要包括对计算机数据或系统进行攻击的行为，同时还包括为谋取个人利益或经济利益，或以对人身或财产造成损害为目的并与计算机有关的行为。

值得注意的是，常与网络犯罪相混淆的还有“计算机犯罪”一词。从本质上来说，计算机犯罪包含了网络犯罪。可以说，网络犯罪是典型的计算机犯罪，但它又不同于那些不以网络为对象、工具、或空间的计算机犯罪，仅仅针对计算机硬件或利用单台计算机而非网络实施的犯罪不属于网络犯罪。

简言之，网络犯罪是针对和利用网络进行的犯罪。从其本质出发，网络犯罪是破坏网络秩序，危害网络及其所承载信息的安全的行为。

相较于传统犯罪，网络犯罪具有以下的特点：

第一，网络犯罪成本低、传播快、范围广。

互联网的快速发展大大提高了网络的全球普及率，而网络犯罪恰以网络作为最重要的辅助手段。网络的互联互通在便利世界联络的同时也为犯罪分子提供了可乘之机。

网络犯罪的犯罪对象主要是网络信息系统及网络系统中存储、传输的信息[9]，信息作为一种无形财产，属于犯罪对象中“物”的范畴。由于在互联网中采集信息与散步信息的成本较为低廉，行为人可以利用网络的互联互通性，在任何地方的一台接入互联网的计算机上快速实现规模大、范围广的网络犯罪。

第二，技术性高、隐蔽性强、取证困难。

网络犯罪是专业性和高技术性的犯罪，是行为人在互联网络上通过编程、加密与解码等

7 编者注：在 2013 年 2 月对联合国毒品和犯罪问题办公室的研究问卷做出答复的国家援引的近 200 项国家法律中，不到 5% 的国家在法律条款的名称或范围中使用了“网络犯罪”一词。同时，也很少有国际或区域法律文书对网络犯罪给出明确的定义。各国立法更常提及“计算机犯罪”，“电子通信”等，而非“网络犯罪”；

8 吴俊，穆萍萍：《浅析网络犯罪同计算机犯罪之异同》，《法制与社会》，2008 年 11 月，第 340 页；

9 吴俊，穆萍萍：《浅析网络犯罪同计算机犯罪之异同》，《法制与社会》，2008 年 11 月，第 340 页；

专业技术实施的犯罪行为。其隐蔽性体现在犯罪实施成功之后，行为人可以通过一定的技术手段删除证据以逃避追查，以及相对于其他的犯罪，其在犯罪预备阶段不容易被识破等。电子证据易删除、易篡改、易丢失的特点，使网络犯罪的取证难度极高。值得一提的是，除了能够通过标准搜索引擎进行访问浏览的“表层网”以外，互联网结构中还存在无法通过常规搜索引擎进行访问浏览的“深网”，以及使用特殊加密技术刻意隐藏相关信息的“暗网”，行为人通常会借助暗网或者利用阻断电子证据传输等非法手段，阻碍警方获取网络犯罪证据。

第三，社会危害性较大。

由于网络犯罪具有成本低廉、传播速度快、传播范围广的特点，由于网络犯罪中涉及到以网络为工具的犯罪大多都以很多网络用户为目标，其传播快和范围广的特点也导致其一旦发生所造成的社会危害性便会比较大。除此之外，一些网络犯罪针对的是国际或政府互联信息网，一旦发生，泄露信息的流向和目的都导致所造成的社会危害性难以估量。《2018 年全球风险报告》[10] 首次将网络攻击纳入全球风险前五名，《2019 年全球风险报告》[11] 和《2020 年全球风险报告》[12] 也将数据欺诈或盗窃、网络攻击等技术类型的风险列入较可能发生的十大风险中。在 2018 年报告中，大规模网络攻击在发生概率排名中位列第三，且网络依赖性成为影响未来十年全球风险格局的第二大重要因素。该报告还提出，虽然绝大多数针对关键和战略系统的网络攻击并未成功，但是数量众多的网络攻击尝试也昭示着全球面临网络攻击的风险仍在上升。由于当前世界的关联性逐渐复杂，网络攻击不仅会造成孤立和突发的影响，也将带来更加剧烈而且不可逆的系统性冲击。

3.2 网络犯罪的分类

通过上文对网络犯罪的描述性概括，我们大致了解了网络犯罪的概念，下面我们将通过对其进行分类的方式从另一个角度了解网络犯罪。

3.2.1 从犯罪主体的角度分类

一般而言，犯罪主体的确定需要满足刑法上犯罪主体成立的条件，网络犯罪也不例外。犯罪主体是指实施危害社会的行为、依法应当负刑事责任的自然人和单位。网络犯罪的主体应是一般主体，既可以是单个的自然人，也可以是多人形成的集团或组织。

（1）自然人犯罪

从网络犯罪的具体表现来看，犯罪主体具有多样性。从本质上来说，不论年龄与职业，任何人都可以进行网络犯罪，但由于网络犯罪对相关技术水平的要求较高，因而从事网络犯罪活动的自然人，也多为掌握相关专业知识、拥有相关技术能力的行为人。在这种基础之上，自然人自身的专业素质、受教育程度、技术能力等因素都会影响其对社会所造成的危害。

（2）集团犯罪

集团犯罪是典型的有组织犯罪，其犯罪集团的内部成员之间具有相对合理明确的分工。

10 世界经济论坛：《2018 年全球风险报告》；
11 世界经济论坛：《2019 年全球风险报告》；
12 世界经济论坛：《2020 年全球风险报告》；

从犯罪的“成本—收益”角度分析，集团集团犯罪降低了犯罪成本，提高了犯罪成功率，更有利于诱发行为人继续从事网络犯罪活动。集团犯罪是网络犯罪的主流形态。据《网络犯罪综合研究》[13] 统计，超过 80% 的网络犯罪行为都源于某种形式的有组织活动。由于许多网络犯罪行为需要高度的组织化及专业化，传统的有组织犯罪集团极有可能广泛地参与到网络犯罪中，尤其是计算机诈骗、伪造身份等金融推动的网络犯罪。在集团犯罪中，由于犯罪集团的犯罪手法通常较为娴熟，且往往具有跨国性等特征，犯罪证据也相对更难被获取。因此，集团犯罪应为网络犯罪全球治理的重点和核心之一。

3.2.2 从网络在犯罪体系构成中的成分分类

随着计算机技术和互联网体系的发展，网络犯罪先后经历了以网络为本体的犯罪、以网络为工具的犯罪和以网络为空间的犯罪三个发展阶段，目前呈现出三个阶段交织并行的样态:

（1）以网络为本体

以网络为本体的犯罪需要专业的技术支持，一般指通过破坏计算机数据或系统的可用性、完整性、机密性，来实现局部网络系统或者区域内网络系统的瘫痪，或者通过前期破坏局部或者区域内的网络系统，为后期其他犯罪行为做好准备。

常见的以网络为本体的网络犯罪包括非法入侵、非法拦截、数据干扰、系统干扰、设备滥用等。

（2）以网络为工具

以网络为工具的犯罪是指仅利用网络为实现其一定犯罪意图的工具，其实施的具体犯罪行为不依赖网络也可以进行 [14]。这种类型的网络犯罪包含范围较大，是网络犯罪整治的一大重点。

以网络为工具的犯罪通常包括：通过网络实施的与儿童色情有关的犯罪、通过网络实施的盗窃罪和诈骗罪，以及与恐怖主义相关的传播、美化行为等。其中，网络诈骗或网络盗窃包括从个人或公司使用信息通讯技术窃取或非法获取有价值信息，黑客经常试图通过侵入计算机获取敏感信息和数据，他们越来越多地将金融、医疗、政府机构及在线零售商的数据库作为目标，并将从网络窃取来的数据资料放到在线的用来交易非法获得数据的国际交易市场进行交易，并获得利润。

（3）以网络为地点

随着互联网的不断发展，新的犯罪形态即以网络为地点的犯罪逐渐增多。以网络为地点的犯罪行为依靠网络广大的受众群体和广泛的传播范围，实现其犯罪的目的，其强调以网络为犯罪行为的实行地。以网络为地点的犯罪与以网络为工具的犯罪的最大差别在于，前者不依赖网络无法施行，而后者不依赖网络也可实施。

常见的以网络为地点的犯罪行为包括网络造谣、网络诽谤、泄露或盗取用户个人网络信

13 联合国：《网络犯罪综合研究》，联合国毒品和犯罪问题办公室，2013 年 2 月；
14 编者注：例如诈骗行为不依赖网络也可以进行；

息等。这类犯罪行为通常不会造成很大的直接财产损害，但是通常会对人身权利造成较大伤害。

目前，针对以网络为地点的犯罪，大多数国家并没有明确的立法规定将其归为犯罪，但是就其特征和体现的危害后果来看，各国对是否有必要将其以犯罪论处还有所争议。

3.2.3 以犯罪行为与犯罪结果的所在地分类

犯罪地分为犯罪行为发生地和犯罪结果发生地。犯罪行为发生地，即犯罪行为的发生之处，具体包括犯罪行为的实施地、预备地、开始地、途经地、结束地等与犯罪行为有关的地点[15]；犯罪结果发生地，即犯罪结果产生之处，包括犯罪对象被侵害地、犯罪所得的实际取得地、藏匿地、转移地、使用地、销售地。

显然的，如果某一刑事案件的犯罪行为与犯罪结果的所在地均处同一国，该国当然具有管辖权。而如果某一刑事案件的犯罪行为与犯罪结果的所在地分处两国，则两国之间可能就司法管辖权的归属及适用问题产生冲突。

按上述犯罪地的分类，网络犯罪中的犯罪行为发生地往往直接被确定为行为人接入网络的地点。而由于网络犯罪行为人所有的犯罪行为均是通过互联网完成，所以网络犯罪在物理世界中的犯罪结果发生地通常难以确定。正是在这种基础上，网络犯罪中的大部分案件（尤其是跨国犯罪）都存在犯罪行为发生地与犯罪结果发生地不同的情况，这也直接导致各国的司法管辖权出现冲突。

针对这一情况，我们给出以下的案例进行阐释：

【例】以攻击公司计算机系统为例。

唐某（Thomas Tang）系 A 国公民，创办了唐氏集团，家底殷实。李某（Tony Li）系 B 国公民。因觊觎唐某殷实的家底，李某在家中（位于 B 国）非法利用网络技术攻击了唐某的个人计算机系统，通过互联网窃取其个人账户及密码，将其银行账户中的巨额财产占为己有。后唐某在旅游时发现自己的银行账户遭遇盗窃，于是立即报警处理。警方通过调查发现，唐某家中的计算机系统遭到了非法入侵，且有十足的证据表明位于 B 国的李某实施了该次犯罪。

李某的犯罪行为发生地为其自己家中（位于 B 国），该次犯罪的犯罪结果发生地为受攻击的计算机所在的唐某家中（位于 A 国），而这两地分处两国，因此在管辖权问题上就出现了争议。

A 国认为，A 国的司法部门具有保护性管辖权，即该犯罪行为侵犯了其公民（唐某）的重大利益（涉案金额达数千万），因而该案件应由 A 国进行管辖。而 B 国认为，由于案件发生在 B 国，B 国的司法部门具有属地管辖权，且犯罪嫌疑人李某为 B 国公民，B 国也同时具有属人管辖权，因而该案件应由 B 国进行管辖。因此在本案中就产生了国与国之间管辖权的争议。

从上述案例中我们可以看出，跨国网络犯罪所导致的犯罪行为地和犯罪结果地的区别导致了国家管辖权的纠纷。

15 编者注：犯罪行为有持续或者继续状态的，犯罪行为持续或者继续实施的地方都属于犯罪行为发生地；

3.3 构成网络犯罪的行为

犯罪行为是行为人所实施的违反刑法规定构成犯罪的行为，是刑法学中犯罪构成的基础和行为人承担刑事责任的根据。[16]

联合国毒品和犯罪问题办公室在针对网络犯罪的综合研究中将构成网络犯罪的行为分为三大类别[17]：

破坏计算机数据或系统的保密性、完整性和可得性行为
非法进入计算机系统
非法获取、截取或取得计算机数据
非法干扰计算机系统或数据
制作、传播或持有计算机滥用工具
破坏隐私或数据保护措施
与计算机相关的、为获得个人或经济利益、或造成损失的行为
与计算机相关的诈骗或伪造
与计算机相关的身份犯罪
与计算机相关的版权或商标犯罪
发送或控制发送垃圾邮件
与计算机相关的引起人身伤害的行为
与计算机相关的教唆或“诱骗”儿童的行为
与计算机内容相关的行为
与计算机相关的涉及仇恨言论的行为
与计算机相关的制作、传播或持有儿童色情制品
与计算机相关的支持恐怖主义犯罪的行为

各国针对网络犯罪的定义不同，其对构成网络犯罪的行为的规定也有所不同，为了方便各位代表对网络犯罪有进一步的了解，在此我们以《布达佩斯网络犯罪公约》为例，对构成网络犯罪的行为进行一个大致的了解。

《布达佩斯公约》[18]是欧洲委员会 26 个欧盟成员国及美国、加拿大、日本和南非等 30 个国家的政府官员共同签署的国际公约，是全世界第一部针对网络犯罪行为所制定的国际公约。

在《布达佩斯公约》中，网络犯罪的具体行为类别如下：

16 郭翔：《犯罪学辞典》，上海人民出版社，1989 年；

17 联合国：《网络犯罪综合研究》，联合国毒品和犯罪问题办公室，2013 年 2 月；

18 《布达佩斯网络犯罪公约》（Budapest Convention on Cybercrime），下称《布达佩斯公约》）又称《网络犯罪公约》，是全世界范围内第一部关于网络犯罪行为国际公约。其由欧洲理事会于 2001 年 11 月 23 日制定，在 2004 年 7 月 1 日正式生效。欧洲理事会另于 2003 年 1 月 28 日通过《网络犯罪公约补充协定：关于通过计算机系统实施的种族主义和仇外情绪的犯罪化》。 详情见 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185，2020 年 2 月 18 日登录；

表1 主要的网络犯罪行为

来源	分类	犯罪行为	备注
公约 条款 2	1计算机数据和系统的机密性、完整性和可用性相关的犯罪	非法访问 Illegal access	为获取计算机数据或其他非法目的，蓄意的、未经授权的非法访问，针对数据机密性或完整性
公约 条款 3		非法侦听 Illegal interception	利用技术手段截取非公开的计算机传输数据，针对数据机密性
公约 条款 4		数据干扰 Data interference	蓄意毁损、删除、破坏、修改或隐藏电脑资料的行为，针对数据机密性、完整性或可用性
公约 条款 5		系统干扰 System interference	通过输入、传输、破坏、删除、毁损、变造或隐藏计算机数据严重妨碍计算机系统功能，针对系统可用性
公约 条款 6		设备滥用 Misuse of devices	为以上犯罪行为提供设备，包括生产、销售、进口和发行等
公约 条款 7	2计算机相关的犯罪	计算机相关的伪造 Computer-related forgery	蓄意伪造数据，针对的是数据的真实性（公约中没有专门指出这个属性）
公约 条款 8		计算机相关的诈骗 Computer-related fraud	有诈骗意图的数据处理，其中包括干扰计算机正常功能
公约 条款 9	3内容相关的犯罪	儿童色情相关的犯罪 Offences related to child pornography	这个条款是欧洲情况，国内应该要严厉得多，不仅是儿童色情内容
公约 条款 10	4侵犯版权及相关权益的犯罪	Offences related to infringements of copyright and related rights	知识产权保护作为网络犯罪行为的单独一类，该分类只包含一种行为
公约 条款 11	5附加责任和制裁	尝试和协助或教唆 Attempt and aiding or abetting	尝试和协助或教唆上述犯罪行为的情况
公约 条款 12		法人责任 Corporate liability	对企业的附加制裁，不影响自然人的刑事责任，该项不计入犯罪行为[17]
补充协议 条款 3		通过计算机系统散播种族主义或仇外资料 Dissemination of racist and xenophobic material through computer systems	国内情况不太一样[18]

（对《布达佩斯公约》中相关罪名的概述 [19]）

3.4 网络犯罪治理的全球局势

全球范围内的法系主要由大陆法系和英美法系组成，此外还有伊斯兰法系等。大陆法系以法国、德国、日本法律为代表，英美法系以英国、美国、加拿大法律为代表。两大法系可以代表当前全球的两种主流立法思路和风格，因此，我们将从大陆法系和英美法系有关网络犯罪的法律规定来从立法角度进行探寻全球局势。

（1）大陆法系

大陆法系的一大特点是各国的法律制度具有相对完整的法律体系。这一体系以宪法为指

19 谢宗晓，刘琦：《< 布达佩斯网络犯罪公约 > 介绍及网络犯罪行为分析》，《中国质量与标准导报》，2017 年 6 月，第 54 页；

导，以私法（民法、商法）为基础，包含了刑法、刑事诉讼法、民事诉讼法以及行政法等在内的六大法律领域的法律、法令，被称为“六法全书”。

大陆法系十分注重成文法典的编纂，几乎每个国家在各个领域都制定了系统完整的法典。与编纂成文法典的传统相适应，大陆法系各个国家都十分注重对法典的解释工作，在对法律解释的基础上，进一步形成了法典解释学（注释学），由这种法典注释学，依次形成了各个部门法学。

德国作为大陆法系的代表，是首个在刑法范围内提出对网络行为进行规范和保护的国家。德国对网络犯罪的规制，主要是通过对本国刑法的修改来进行的。《第二部经济犯罪防治法》主要规定了非法获取数据罪、伪造证据资料罪、与计算机有关的诈骗罪、非法篡改数据罪、破坏计算机罪等罪名，并根据罪刑法定的原则，对于以上犯罪，在定罪量刑上根据情节轻重可分别判处两年以下或者五年以下自由刑或罚金，犯罪未遂也要受到相关处罚。而现行德国刑法中共规定了 9 个与网络犯罪相关的罪名，包括变更数据罪、破坏计算机罪、非法获取数据罪等。

日本作为又一大陆法系的代表性国家，在对网络犯罪的规制中受到了德国的深刻影响，也是以修正现行刑法典为主。在对日本现行刑法中有关计算机网络犯罪的规定修正之前，其主要是通过刑法中的传统条文来对网络犯罪进行相关规制。1987 年，日本通过“刑法部分条文修正案”的形式将网络犯罪的相关规定纳入到刑法。在日本现行刑法中，共有七条规定涉及到网络犯罪：通过破坏计算机网络等妨碍正常经营和业务罪、对公用文书进行破坏罪、对私用文书进行毁坏罪、虚假记载公正证书罪、伪造文书罪、违法提供和制作电磁记录罪、使用计算机网络诈骗罪。日本对于网络犯罪的相关规定仍然是在传统犯罪条文基础上的部分规定，多数是在传统规定上的适当延伸。目前，日本对侵犯网络信息系统和信息安全的犯罪行为，并没有做出与传统犯罪相区别的特殊规定，处罚基本上还是以自由刑和罚金刑为主。

大陆法系通常习惯于用法典的形式对法律规范做统一的系统规定，网络犯罪的具体形式也多用刑法典的方式加以呈现。尽管如此，大陆法系国家的法律规定也不能说是十分详尽，虽然以法典的形式能够较为系统地对网络犯罪进行规定，但是其无法应对互联网和网络犯罪快速发展新型态的趋势，无法囊括所有类型并及时作出修正。

（2）英美法系

英美法系国家信奉“法律本身是不可能完备的”，其通过对判例的技术性整理，形成具有很强的灵活性的判例法。但是，由于近年来世界各国沟通不断加强，各法系之间不断交融，英美法系也出现了制定实体法的趋势，确定性因素在整个法律系统中占有一定地位。

英美法系同大陆法系非常大的一点不同之处在于，英美法系同时以判例作为法律渊源，用于司法的适用。英美法系的国家，虽然很注重法律的解释，但更多在解释判例方面下功夫。

美国享受着计算机网络带来的便捷，但也是目前全球范围内网络犯罪发生最严重和最频繁的国家。为了应对日益严重的网络犯罪，美国通过立法规范最多、最全面的州立法和联邦立法作出应对。美国对网络犯罪的立法规制是从各州开始的。1978 年美国颁布的《佛罗里达计算机犯罪法》是美国历史上的第一部有关网络犯罪的法律。此后，其他各州纷纷效仿佛罗里达州的做法制定本州的网络犯罪法律。1984 年美国联邦政府颁布《非法入侵以及计算机诈骗与滥用法》，这是美国联邦第一部规制网络犯罪的成文法，后于 1996 年形成《计算机滥用修正案》，修正案还规定了美国联邦经济情报局对网络犯罪的特殊侦查权，后被纳入

《美国法典》。此外，美国联邦还陆续颁布了多部旨在规制和限制网络犯罪行为的法律，包括《正当通讯法案》、《国家被盗财产法》、《儿童色情预防法》等，通过各州和联邦的共同立法而构建起了一整套有效规制和惩处网络犯罪的法律法规体系。

不同于美国，英国所有有关网络犯罪的立法均是在全国范围内适用。英国最早关于网络犯罪的立法规定是从电子信息数据的角度对网络犯罪进行规制，即 1981 年修订的《伪造文书及货币法》。1984 年，英国在刑事证据法律范畴进一步提出了对网络犯罪的规制，规定电子记录的相关情报同样具有证明效力。但是，在此期间，英国并未将传统犯罪与计算机网络犯罪进行明确的区分，网络犯罪仅仅是被作为附着在传统犯罪之上一种新型的工具，对其的惩罚也仅仅只是在参照传统犯罪的规定处理，直到 1990 年出台的《计算机滥用法》才彻底改变了此种状况。

虽然英美法系的判例具有极大的灵活性，在社会生活和网络犯罪形式不断变化的同时，法律规范能够就此进行适当调整，促进法律规范的完善。但是，大多数英美法系国家的司法判例尚不完备，没有足够的判例作为依据支撑法官的判决。因此，英美法系的部分国家也十分注重通过制定实体法的方式来对网络犯罪进行规定。

4. 问题与挑战

4.1 立法及框架

4.1.1 定罪量刑缺少统一标准

根据国际刑事司法中的双重犯罪原则（亦称为相同原则），可引渡的犯罪必须是根据请求引渡国与被请求引渡国的法律，都认定为犯罪的行为，且行为人的行为必须构成重罪[20]。如今，许多严重的网络犯罪行为都具有跨国界的性质，因此要推进网络犯罪的全球治理，推动制定全球性的针对网络犯罪之定罪量刑的统一标准具有重大意义。

但与此同时，我们也不能忽略各国在立法上的独立权。

众所周知，各主权国家均享有独立权、平等权、自卫权，以及管辖权四大权利。其中，独立权确定了各国家有权在不受外界干扰的情况下，独立自主地管理本国对内事务以及对外事务（亦称之为“对内最高，对外独立”）。在对内的独立权中，各国有权自主制定国家的法律，他国不得干涉。

因此，如果要对网络犯罪的定罪量刑进行统一，各国只能通过友好协商的方式达成一致，并依靠各国的意愿积极履行相关责任。如何在这一形势下推进统一标准的制定是网络犯罪全球治理的一大难题。

4.1.2 犯罪客体的实时变化难以应对

网络技术的高速发展带来了各种新兴事物。在网络得以发展之前，各国刑法所保护的犯罪客体中的财产性权利通常为“有形客体”，也就是实在的、可见的客体，例如不动产和动产等。而在网络得以发展之后，各国刑法所保护的犯罪客体通常无法涵盖在网络犯罪中被侵害的各种“无形客体”，也就是虚拟的、看不见的客体，例如虚拟货币、个人数据等。

以虚拟货币为例，我们可以看出犯罪客体的实时变化给网络犯罪治理带来的巨大挑战：

虚拟货币一般是指在网络上流通的，具有一定价值的非真实的货币。随着时代的发展，大众所熟知的虚拟货币从游戏中可以用来购买各种装备的游戏币[21]，亦即第一类虚拟货币，逐渐发展为可以通过使用真实货币在各网络软件购买的第二类虚拟货币[22]，这一类的虚拟货币可以用来购买相关的网络增值服务。后来，随着网络技术的发展，又产生了第三类的网络虚拟货币，即诸如“比特币（BTC）”、“莱特货币（LTC）”等电子货币。这一类的虚拟货币具有更高的可流通性，在金融市场上也往往具有更高的价值。

在这三类虚拟货币的发展历程中，与之对应的网络犯罪也在逐渐成型。

就第一类虚拟货币而言，针对这种只在虚拟世界有其特定价值的游戏币，网络犯罪的危害性一般较小，无论从侵害的财产价值角度，还是从犯罪行为所侵害的人群范围角度而言，都不具有极高的危害性，因此从犯罪治理的必要性和犯罪治理的难度而言都尚不足以引起各层面的重视。

20 编者注：例如中国的刑法规定三年以上构成重罪；

21 例如摩尔庄园游戏中的摩尔豆；王者荣耀游戏中的金币等；

22 例如摩尔庄园游戏中充值米币，可以用来购买会员资格；在王者荣耀游戏中充值王者荣耀点券，可以用来购买皮肤等；

而在发展到第二类虚拟货币后，由于这一类的虚拟货币直接与现实中的真实货币挂钩，真实货币与虚拟货币可以单向转换甚至相互转换，因此针对这一类虚拟货币的网络犯罪的滋生速度远远高于针对第一类虚拟货币的网络犯罪。正是由于上述特点，针对第二类虚拟货币的网络犯罪的危害性有显著的提升，且由于网络发展的高度互联性，许多常用的虚拟货币（如Q 币等）是网络诈骗犯、网络盗窃犯的重灾区。对于这一类的网络犯罪，无论是从其侵害的财产价值角度，还是从犯罪行为所侵害的人群范围而言，都具有更高的危害性。因此，此阶段的网络犯罪治理已经开始引起了各层面的重视。

当发展到第三类网络虚拟货币后，由于这一类虚拟货币甚至可以直接当做一种真实货币在网络上进行金融投资或者作为一种新型货币直接被应用于生活中，针对这一类虚拟货币的网络犯罪行为的危害性是前两者所不可比拟的。遗憾的是，由于网络技术发展迅速，各国在立法层面通常无法迅速应对这种新局面，其对于这一类的虚拟货币，通常没有明确的法律定义，也进而难以对其进行管理，与之对应的网络犯罪治理也无从谈起。

上述是以虚拟货币的发展为例，展示了网络犯罪全球治理在犯罪客体的实时变化之下所面临的巨大挑战。

与虚拟货币相类似的，针对数据权利的网络犯罪、针对网络场所的网络犯罪等都面临着立法层面无法与之相匹配的问题，这也给网络犯罪的滋生提供了一片灰色地带。

4.1.3 针对电子证据立法的缺失

在当今网络犯罪立法领域，电子证据已经成为了重要一环，通常情况下，学界认为电子证据是指法律上确认的电子数据。但究其法律地位与效力，各国间的差异巨大。各国对电子证据均未有单独立法，甚至《证据法》都鲜有单列。全球目前只有《电子商务示范法》对电子证据有统一规定，其他情况下也没有国际统一规范，这也就导致了电子证据在全球范围内的效用存在差异。从而在网络犯罪跨国性的作用下，国际间电子证据的确认等问题限制了此类犯罪的解决。

4.2 执法与侦查

4.2.1 电子数据的新特征带来的挑战

电子数据的复杂性和高技术含量性意味着收集电子数据需要专业人员和技术知识做保障。而在实践中这些理论上的要求却很难实现。

基层侦查机关承担大量的刑事案件处理任务，但人员、技术和经费水平有限，再加上电子信息技术本身的发展速度较快，这就在取证主体合法和取证技术合法要求间造就了两难的局面。[23] 如果放开对取证主体的限制，就有可能对被调查对象包括隐私权在内的基本权利造成侵害，导致电子数据取证过程中权利侵害的问题出现。但另一方面，如果一味限制取证人员的身份资格，又可能因缺乏相应专业知识导致对电子数据的破坏甚至毁灭。而且无论是取证权限不合法，还是技术资质不合法，都会损害电子数据取证主体的合法性。

在电子数据的取证中，取证主体实际上呈现出了前所未有的多元化可能性，对传统的取证主体组成带来了很大挑战。一般来说，侦查权只能由各国公安机关、国家安全部门等国家

23 夷冰倩:《公安机关提取电子数据的法律规制》,《四川警察学院学报》, 2018 年第五期, 第 66-72 页;

专门机关的工作人员行使，其他人员无权进行搜查、扣押等取证工作，可是在司法实践中，具有侦查权的侦查人员往往没有掌握相关专业技术，掌握相关专业技术的人员又没有取证权限的问题在电子数据取证的过程中一直出现，而且越是复杂和隐蔽的数据存储，越是需要更多和更专业的技术人员进行发掘和收集，这也就对传统的侦查主体观念提出了新的要求。

与此同时，高技术含量性同时导致了国与国之间、部门与部门之间执法能力的差异。一般而言，欠发达国家并没有完整的网络监管体系与合适的网络监管能力，这给网络执法与国际合作带来了新的挑战。

4.2.2 部分取证工具、技术使用的合法合理性存疑

在对电子数据的合法性的规制和审查中，较为受到重视的是取证人员是否能够按照规范要求进行取证操作，但取证手段本身的合法性却不太关注。近年来，人肉搜索式信息获取受到的关注和争议不断增加，[24] 新型的远程操控、木马、黑客技术不断发展，使得犯罪门槛逐步降低，相关违法行为从高智商犯罪逐步降低为低门槛犯罪。与此同时，各国侦查取证部门的技术人员也从中感受到了便利 : 相比于公安机关内部自行开发类似的远程取证工具软件，直接借用不法分子编写的木马或黑客软件更为快捷便利和低成本，尤其是在科技水平欠发达的国家，执法部门并没有足够的能力开发真正有效、匹配网络犯罪领域最前沿的侦破软件。可是，“知法犯法”真的合理吗?

一般来说，使用这类技术和软件可能存在的合法合理性问题主要包含以下几个 :

第一，取证工具合法性问题：

从“合法性”的字面含义上来说，在取证过程中使用未经批准的工具或者技术是否违法，在立法与实务中本身就是一个模糊地带。法律规范往往没有规定这类工具软件本身的违法性，但是一般公民开发和使用这类工具的行为是被定性为不合法的，这就给侦查取证人员使用这类手段和工具的行为是否违法带来了疑问。

这种不确定性产生的最根本原因就是类似的手段或者工具具有隐私侵犯性。[25] 从法理上来说，具有隐私和公民权利侵犯性的取证行为是需要严格审批的，而侦查机关使用这些手段和软件来辅助侦查，从根本上来说是其实是缺少必要许可的。而且众所周知，对于公权力使用的方式和边界的规定目前还是较为模糊的，这需要对相关概念、行为方式等一系列问题的进一步明确。

第二，取证工具的安全性问题：

软件的安全、可靠与否也关系到整个电子数据取证过程的安全性。目前侦查机关使用盗版软件、破解软件进行的远程取证中，不乏木马软件，这些基本都是网络黑客开发的，很多黑客通过售卖这类软件换取不法收益，但是这些软件很多本身的安全性也没有保障，一些人在出售软件的同时在其中夹杂新的木马或者病毒程序，通过“黑吃黑”获取更多收益。如果侦查人员使用这些软件，就可能产生新的风险。

第三，缺乏审批监督要求：

在电子数据领域，虚拟的证据存在状态阻碍了有限现实空间中对证据实质真实的证明能力。在这种状态下，本应用第三方的监督与审批等程序对侦查取证工作进行监督，但从相关

24 王燃:《大数据时代个人信息保护视野下的电子取证——以网络平台为视角》,《山东警察学院学报》, 2015 第 5 期，第 126 页;

25 李强:《毒品犯罪案件侦查中电子取证存在的问题及对策》,《云南警官学院学报》, 2018 年第 2 期, 第 10 页;

的法律规定以及实践工作上来看，这一环节在新型的技术性领域实际是缺失的。各国对网络法的制定往往尚未完成，监督程序的设定进度更是难以匹配实际情况。

论其根本，各国刑事诉讼法本身鲜有从理论的高度对侦查行为的强制性做界定，而电子数据的虚拟属性又使得对其取证行为的隐私侵犯性很难通过一般性的方式予以界定，衍生出公权力与隐私权保护之间的界限和实际操作问题也难以避免。[26]

4.2.3 警方的侦查权难以落实

在前文中我们提到，网络犯罪具有隐蔽性高的特点。在犯罪预备阶段，这一特点显而易见。不同于传统犯罪的犯罪预备阶段，行为人通常要进行全方位的犯罪预备，这要求其在犯罪前期做好万全的准备，因此通常会留下痕迹。

例如传统的盗窃犯，在犯罪前，犯罪行为人通常需要以踩点的方式寻找合适的目标，这给警方的侦查带来了有效的信息，警方可以通过对可疑人员的摸排在犯罪预备阶段大致确定可能实施犯罪行为的嫌疑人的范围。

而对于网络盗窃犯，在犯罪前，犯罪行为人不需要通过实地的踩点寻找合适的目标，往往只需要利用同一台设备寻找合适的目标即可。由于网络的互动性强、隐蔽性高，警方通常无法在犯罪的预备阶段进行有效的侦查。

另外，在犯罪行为实施后，与之同理的，警方也往往会因为找不到明显嫌疑人线索等原因难以进行侦查。

这一问题在通过暗网进行的网络犯罪中体现的更为明显，即使各方对暗网所包含的信息基本为非法信息都心知肚明，但由于暗网的隐蔽性和无法追踪性，警方更加无法进行有效的侦查。因此，暗网的“蓬勃发展”是国际社会所面临的重大难题。

4.3 刑事司法问题

4.3.1 网络犯罪的司法管辖权缺少稳定性

管辖权是主权国家所拥有的四项基本权利之一，其基本内涵是主权国家所具有的，对人、事、物通过立法、行政、司法的途径进行管理的权利。

一般来说，被国际法普遍确定的管辖原则有四种，除了前文中提到过的保护性管辖权、属人管辖权，以及属地管辖权之外，还有普遍性管辖权。

显然，在这四种管辖权的共同基础上，针对发生在本国领土范围内[27]，或者由具有本国国籍的公民实施的网络犯罪，国家可以当然地享有管辖的权利，但对于跨国性质的网络犯罪，我们就不能一概而论了。

首先，在立法部分我们谈到了双重犯罪原则，这也是在保护性管辖权适用时所必须遵循的原则，即只有针对双方均认为构成犯罪的行为，一国才得以行使保护性管辖权。这进一步反映了推动制定全球性的统一标准具有重要意义。

其次，根据主权国家的独立性，一国不得干涉他国独立处理其主权范围内的事务。这意味着即使一国行使了保护性管辖权，另一国也没有义务予以配合，双方只能在友好协商的基

26 贾哀浩，姚强，韩笑晨：《电子证据的演进：从模式思维到制度理性—以司法实践中的发展为考察进路》，《郑州大学学报（哲学社会科学版）》，2014 年第三期，第 68 页；

27 编者注：包括在具有本国国籍的船舶、航空器、航天器中发生的网络犯罪；

础之上，就相关管辖问题达成一致。如果两国就相关管辖问题达成了长期一致，便会以签订引渡条约的形式予以体现。只有在签订引渡条约的情况下，国与国之间才会产生配合引渡的义务。

但是，如果国与国之间无法就管辖问题达成一致，那希望适用保护性管辖权的一方，无论在何种情况下，都不得在他国的领土范围内开展任何的执法行动。

综上我们可以看出，跨国性网络犯罪的全球治理，在一定程度上需要以各国的积极配合为基础，但基于政治因素，这种基础往往是不稳定的。这给网络犯罪的全球治理带来了问题与挑战。

4.3.2 执法组织及人员缺乏专业化

网络犯罪案件的检察和审判要求刑事司法系统实现专业化。这要求司法人员理解计算和互联网的概念，掌握网络犯罪法律框架得相关知识并具备在法庭上呈现和理解电子证据的能力。但在联合国毒品和犯罪问题办公室公布的相关资料中[28]，我们可以发现以下结论：

第一，各国的检察机构在网络犯罪领域的专业化程度往往要低于执法当局；

第二，发达国家的检察工作专业化程度要高于发展中国家。在大部分欠发达国家中，其检察人员严重缺乏 IT 技能，甚至有大量检察人员没有掌握任何 IT 技能。同时，他们在工作中，计算机设备的水平往往非常低，通常只配备了初级或中级计算机设备，甚至有大量没有配备任何设备情况的存在；

第三，在绝大多数国家，法院在网络犯罪领域的专业化程度极低，只有极少数国家设立了专业化的相关司法机构。因此，有大量网络犯罪案件都是由非专业法官审理的。与此同时，很多国家没有网络犯罪相关的法官培训制度，大量相关法官没有接受过任何网络犯罪的相关培训。

司法机关及其人员专业素质的参差不齐容易导致裁判标准及结果出现重大差异，在国际网络犯罪合作中产生许多困难。

4.3.3 各国司法能力建设存在巨大差异

由于各国的国情不同，网络犯罪活动在各国领域内滋生的程度也有所不同。在这种情况下，各国司法能力与国情的不相匹配会给网络犯罪的全球治理带来很大的困难。

对于大部分发达国家以及少部分发展中大国，其能够通过完善的司法体系建设来打击网络犯罪，司法能力能够与国情相匹配。而对于许多发展较为落后的发展中国家，甚至一些最不发达国家而言，由于其司法能力较弱，导致许多跨境的犯罪活动易于在这些国家境内展开，进而形成了独特的“避罪天堂”的国情。

针对这一问题，我们通过以下案例来予以描述：

【例】

发达国家 A 国的公民赵某某（Vincent Zhao）欲搭建一网络诈骗平台，通过网络赌球吸引网民前来消费，由于其本国打击网络犯罪氛围较浓，执法部门执法严格，司法部门司法体系成熟，故决定伙同李某某（Ann Li）以及潘某某（Ted Pan），前往司法体系不完善、打击网络犯罪能力较弱的太平洋岛国 B 国搭建相关网站，并在 A 国境内投放相关广告，吸引网民跨境消费。

28 联合国毒品和犯罪问题办公室：《网络犯罪研究调查问卷》。

由于 B 国缺乏相关监管，没有能力针对这一跨国网络犯罪行为进行相关打击。最终，三名犯罪嫌疑人在 B 国通过这一网络诈骗平台，一共非法获利两千余万元，并于 2019 年 7 月底被 A 国警方通过协议引渡的方式引渡回国、抓捕归案。

从上述案例中我们可以看出，这样一种以跨国实施的方式来规避国家监管的网络犯罪，具有极高的社会危害性，打击难度大。各国在司法能力建设上的巨大差异导致了避罪天堂的产生，而这一情形又反过来影响到每一个国家。在全球范围内，如何针对性地提高那些被犯罪分子们当作避罪天堂的国家的司法能力，进而普遍性地打击网络犯罪，推动网络犯罪的全球治理，是给各国留下的一大问题。

4.4 国际合作

4.4.1 立法合作中的阻碍

在上述立法部分我们提到了立法层面存在的诸多问题，而解决这些问题的最好办法则是以国际合作的方式进行处理。在国际合作的过程中，也存在着诸多的问题。

在国际立法层面，我们首先需要明确的是，正如我们所强调过的，各国的主权决定了其在国内立法方面具有绝对的自主权力，因此全球性的针对网络犯罪定罪量刑的统一标准的制定只能基于各国的积极态度与积极配合。

值得注意的是，在共同标准的制定方面，《布达佩斯公约》作为世界上第一个也是唯一一个相关的国际公约，在全球标准制定方面起到了一定的积极作用。但是这样一个具有地区化特色的公约，在全球推广、全球适用方面遇到了巨大的阻力，诸多国家对此意见相左。

统一标准的制定所具有的重大意义我们已经有所了解，如何克服上述困难，推动制定全球统一标准，有待国际社会的共同解决。

4.4.2 行政合作中的阻碍

在网络犯罪的行政部分，我们谈到了电子证据的采集、取证工具的使用和警方的侦查权三部分。在治理跨国性的网络犯罪时，这三类问题与挑战无一不需要以稳定的国际合作作为基础，只有国与国之间有意愿进行合作且有所行动，相关的治理工作才能够落在实处。

在国际政治大环境波诡云谲的今天，影响各国作出行动的因素绝不仅有犯罪治理的必要性这一条，意识形态和国家战略才是起决定性作用的。在此基础上，即使各国都能意识到积极推动网络犯罪全球治理的必要性，但其往往还是需要基于各自的国家利益，站稳立场，谨慎行事，相关的行政合作也因此缺乏足够的推动力和稳定性。

4.4.3 司法合作中的阻碍

司法合作层面主要涉及司法能力建设和引渡的相关问题。

就司法能力建设问题来说，全球普遍的司法能力培养需要国际社会共同推动。无论是司法人员的能力培养，还是相关司法技术的支持，亦或是司法体系运行中资金的援助，都需要有足够的推动力。面对网络犯罪这一议题，国际社会的动力往往局限于网络犯罪所带来的危害足够巨大，在此基础上，各国才有必要共同努力，应对网络犯罪，治理网络犯罪。因而，

面对司法层面的国际合作缺少动力这一问题，需引渡的相关问题给各国在网络犯罪司法合作中带来了巨大挑战。

就引渡问题来说，各国的法律对于引渡是否设置前提条件大致可以区分成两种情况：第一种是引渡的条件是基于平等互惠的原则提出的，即请求引渡国是否能够在遇到类似引渡案件的时候同样能够及时给予请求方以平等的引渡待遇。这种承诺可以被认为是一种平等互惠的实践，甚至可以被认为是一种平等互惠的承诺，其不需要以成文的条约作为根据。第二种则是要求与该请求引渡国之间已经存在引渡相关条约，方可进行引渡。第二种情况也可以被称为“条约前置主义”。

从上我们不难看出，不论以何种方法设置引渡规则，国与国之间的平等互惠都是引渡可以进行的一大基础。同样的，由于政治考量等诸多因素，这一基础也不甚牢固。

另外，在国际司法合作中，追赃也是一个重要的组成部分。对电信诈骗跨国犯罪的追赃方法通常是直接缴获电信诈骗犯罪分子的违法存款和所得。然而，大部分的电信诈骗跨国犯罪活动往往是通过地下电子钱庄、国际电子汇兑等多种方式直接转移非法存款和所得，将非法存款和所得转移到不同国家和地区的多个银行账户中，单一国家的有关部门很难通过国外的银行账户来追回电信诈骗犯罪分子的非法存款和所得。

4.5 犯罪预防

“犯罪预防”是指致力于通过能够影响多重犯罪根源的干预手段，降低犯罪发生风险及其对个人和社会潜在有害影响的战略和措施。[29] 犯罪预防强调政府、组织、公民多方合作，借助多种途径实现犯罪预防的效果。网络犯罪自然也可以从犯罪预防的角度进行考虑。网络犯罪的犯罪预防由于网络犯罪的特殊性，形成了独特的挑战。目前，从犯罪学角度上认为当代犯罪预防的格局包括社会预防、刑罚预防、情境预防。

4.5.1 社会预防

社会预防是指通过对社会结构的调整与完善，使社会健康和谐地发展，消除或减少社会不良因素，防止社会失调和解组，从而达到控制和减少犯罪现象发生的社会活动过程。网络犯罪特殊的背景条件为社会预防增添了新的挑战：人们愈加普遍使用网络设备，导致产生大量潜在受害者和犯罪人员；更多的儿童和老人也成为了互联网用户。对于网络犯罪的社会预防，很多国家已经实现了一定程度的社会结构调整，但是对于全球大背景下大社会的社会预防，应该从哪些层面去做出何种具体的措施来减少社会的不良因素，如何使社会预防更好地落实到位，仍存在较大的挑战。

4.5.2 刑罚预防

在犯罪学中，刑罚除作为刑事责任的承担方式之外，还被当作一种预防措施进行研究。刑罚预防之目的主要在于规范公民行为、制止犯罪冲动、改善犯罪心理等。刑罚预防包括制定宣传刑罚、适用刑罚、执行刑罚三个基本途径。而对于网络犯罪，很多国家在该领域内的立法层面就存在很大的完善空间，而同时在立法司法实践中，刑罚能否得到充分有效地实行，所设立的刑罚又是否能真正起到犯罪预防的作用，都需要更多的考虑。

29 联合国经济及社会理事会关于促进有效犯罪预防行动的 2002 年第 13 号决议附件：《联合国预防犯罪准则》，2002 年 7 月 24 日，第 3 段；

需要明确的是，刑罚预防的功能是有限的，其威慑效果也只是暂时的，能否客观地运用刑罚来起到预防的作用，更是给各国的司法执法提出了挑战。在刑罚预防中，严酷的刑罚容易引起人们的反感与厌恶，同时可能激起人们的同情心，使得刑罚的威慑和预防作用大大降低。[30] 但对于网络犯罪而言，其犯罪途径众多，成本较低，过轻的刑罚不足以消除人们为了追求更大的利益而铤而走险的犯罪心理。

与此同时，不可否认刑罚对犯罪预防确实存在难以消除的负面作用。犯罪人常常被物化而不被当作正常人来看待，这不利于他们的再社会化。

刑罚预防的效果受到很多因素的影响，包括观念层面、制度层面、操作层面等的因素。从观念上来看，决策者的犯罪观和犯罪的对策观是否相匹配在司法实践中很重要。同时，在制度层面来看，有效执法是防控网络犯罪的关键，如何真正落实各国国内和国际的有效执法，也都是目前存在的问题和挑战。

因此，网络犯罪的刑罚预防不仅要从立法司法执法的角度去考虑，更要结合刑罚本身的一些弊端去探寻其更好的实践效果。

4.5.3 情境预防

情境预防通过建立一种特定的预防犯罪的环境，在犯罪已发区和高发区，采取减少犯罪机会的情景预防犯罪，包括但不限于增加犯罪困难、提升犯罪风险、降低犯罪收益等。通常来说，情境预防着眼于犯罪行为、被害人和犯罪机会。情境预防能够相对全面具体地分析情境与行为人地互动关系，变被动的犯罪预防为主动的犯罪预防，从效益整合的角度为预防措施提供新思路。

虽然情境预防具备着较大的优点，但是由于这种概念诞生于近 30 年前，所以对专业人才的依赖程度比较大，成本和工作量也相对比较大，为全球范围内的实践工作带来了困难。

4.5.4 公私合作推动犯罪预防

《联合国预防少年犯罪准则》明确强调，政府、各组织内部及各行政当局、社区公益组织、非政府营利性组织、工商部门和普通公民之间的合作和伙伴关系在日常的犯罪预防中发挥重要的作用。[31] 良好的犯罪预防一般从基本的原则（包括例如政府领导、合作和法治等）开始，然后进一步提出犯罪预防组织的形式（如制定犯罪预防行动计划等），并最终通过导向犯罪预防方法（如开发健全的犯罪预防知识库）和导向犯罪预防路径（其中包括如何减少发生犯罪的机会和强化犯罪目标等）的方式实施。

针对这一问题，我们通过以下案例予以描述。

【例】

2016 年 9 月，浙江绍兴市公安局警方成功侦破了一系列的互联网电信诈骗案，共刑拘网络违法犯罪嫌疑人一千余名。浙江绍兴市公安局警方在对国内外媒体详细介绍了案情时，着重向媒体提到了阿里巴巴安全部门的大力协助。这个安全部门集结了 2000 多人，共同组成了安全团队，在网络犯罪线索的提供、数据的分析、证据的收集等诸多环节方面，为网络

30　毛丹丹：《预防作为刑罚目的之正当性考察——一般预防与特殊预防》，硕士论文，东北师范大学，2011 年 5 月，第 15 页；

31　联合国：《联合国预防少年犯罪准则》，1990 年，第 7 条和第 9 条；

犯罪案件的最终侦查和破获提供了有力的支持。这就是许多地方媒体都在报道中提到的一个关键词 " 警企合作 "。[32]

从上述的案例我们不难看出，犯罪预防不仅需要政府的大力干预，私人部门等社会力量的支持和帮助也非常必要，尤其是在政府的力量难以保证犯罪预防专业化和针对化的实际情况下。如今的网络犯罪分子利用先进的互联网和计算机网络技术实施各种信息网络犯罪，其中的网络犯罪集团逐渐成型，组织严密，隐蔽性强，犯罪链条长且涉案网络广，犯罪的手段逐渐转型升级，变得愈加多样化，再加之犯罪对象覆盖面广，致使有关部门的破案难度日益增大。

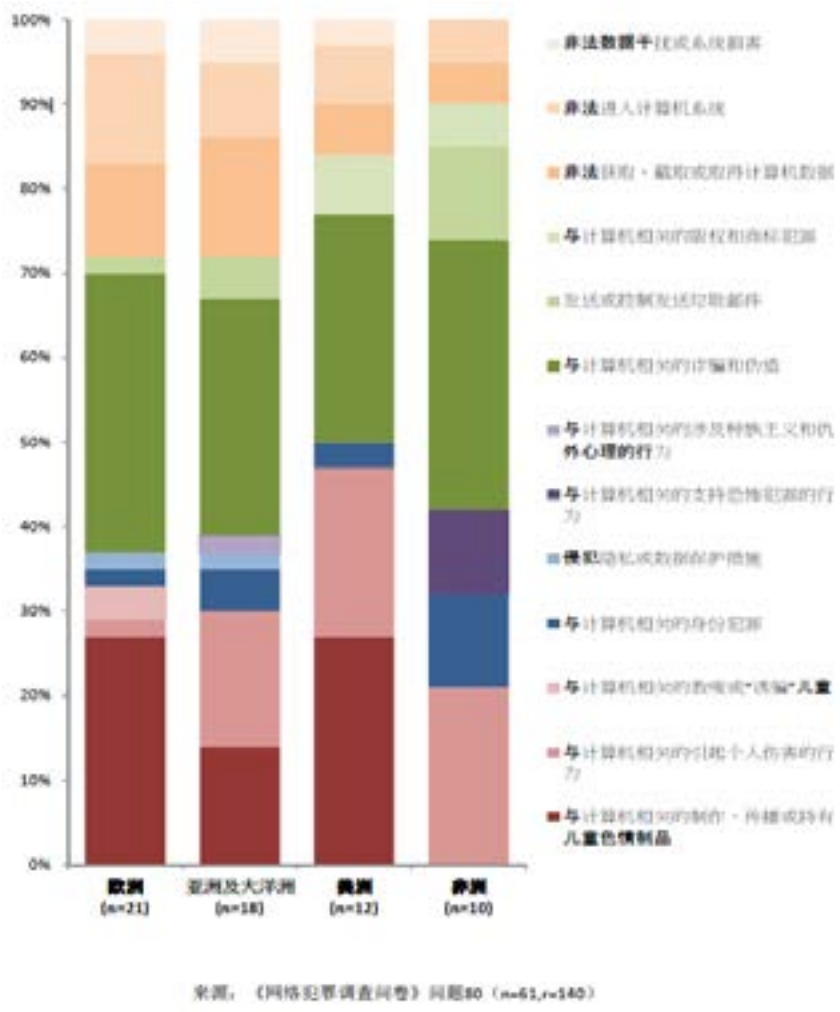
通过政府部门和私营部门合作，充分利用网络资源，从而有效地利用网络方法进行犯罪预防，是目前行之有效的一大方法。

32 刘潇潇：《信息网络犯罪之预防》，《社会与法治》，2018 年 2 月（下），第 216 页；

5. 现状及已采取的措施

5.1 网络犯罪现状和发展趋势

目前，网络犯罪行为主要分布在：金融导向行为，与计算机内容相关行为和破坏计算机系统行为三种行为。部分国家的执法部门认为，金融导向的犯罪行为，例如与计算机相关的诈骗、伪造等，占全部网络犯罪行为的约三分之一[33]。另一个占三分之一，在某些区域甚至达到一半的，为涉及计算机内容的犯罪行为，包括儿童色情、恐怖主义和侵犯知识产权。而破坏计算机系统行为，根据区域的不同，占比从 10% 到三分之一不等，但必然存在。网络犯罪的具体构成在各地区呈现出不同的状态，具体的构成如下图所示：



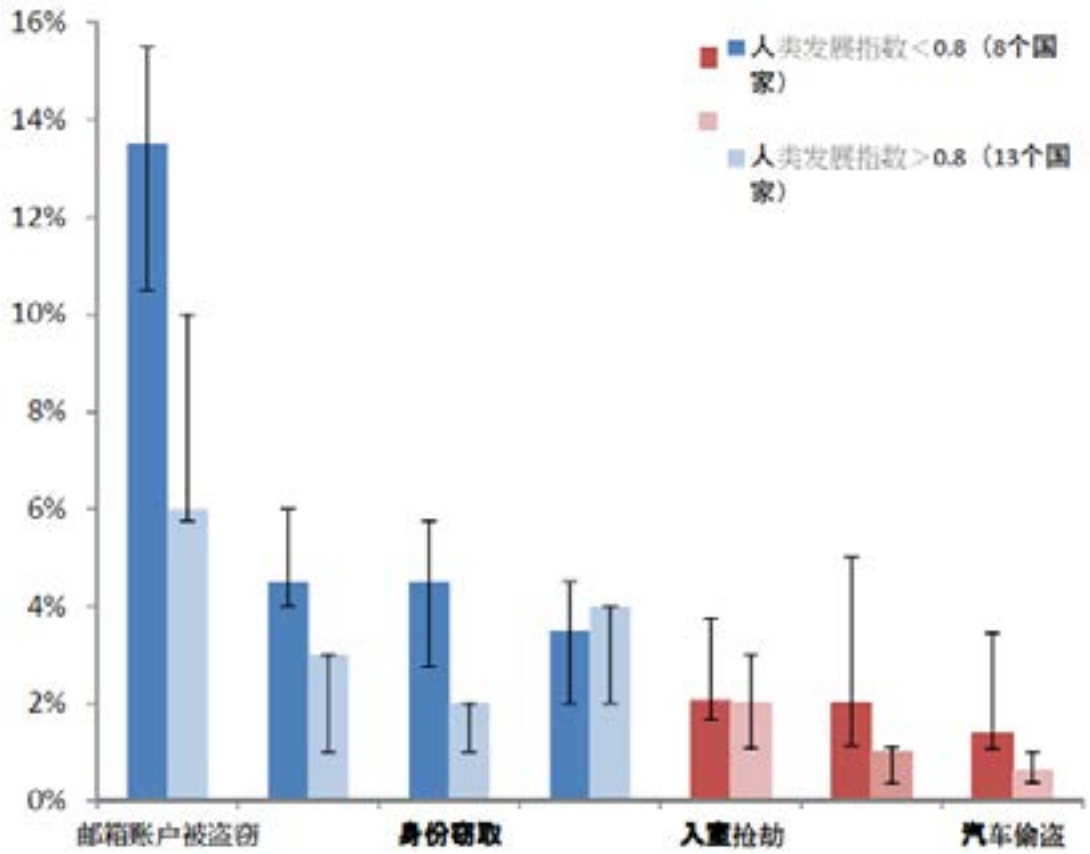
来源：《网络犯罪调查问卷》问题80（n=61,r=140）

（不同的网络犯罪类别在各地区的构成[34]）

33 联合国毒品和犯罪问题办公室：《网络犯罪综合研究草案》，2013 年 2 月，第 27 页；
34 联合国毒品和犯罪问题办公室，《网络犯罪综合研究草案》，2013 年 2 月，第 28 页；

此外，值得注意的是，执法部门和私人部门对于网络犯罪有关风险和威胁的认识并不是完全一致的。执法部门通常认为本国最常见的网络犯罪行为是风险最高、对本国威胁最大。而对于私营部门来说，他们普遍认为破坏计算机系统和其他网络犯罪行为相比，威胁要大得多。这种认识可以被解释为：对于私营部门来说，破坏计算机系统所造成的损失要大于其他两种网络犯罪行为。具体而言，私营部门主要关注的网络犯罪有：“非法获取和盗窃知识产权”、“入侵网银”、“企图入侵顾客数据系统”、“员工泄密”和“拒绝服务（Denial of Service）攻击”。[35]

从受害百分比方面来看，网络犯罪的个人受害率要远高于传统犯罪，而且与国家发展水平呈现反相关。具体信息如下图所示：



（网络犯罪的受害率与国家发展程度因素的关系对比[36]）

最后，除上述情况外，《网络犯罪综合研究草案》[37]还就全球网络犯罪局势给出了以下几个关键结论：

欧洲私营部门企业报告显示侵入和网络钓鱼导致的数据泄露受害率为 2%-16%。

这些罪行所用的犯罪工具已辐射至全球，如僵尸网站。2011 年全球有超过一百万互联网协议地址（IP 地址）被用于指挥和控制僵尸网站服务器。

35 联合国毒品和犯罪问题办公室：《网络犯罪综合研究草案》，2013 年 2 月，第 30 页；
36 联合国毒品和犯罪问题办公室：《网络犯罪综合研究草案》，2013 年 2 月，第 32 页；
37 联合国毒品和犯罪问题办公室：《网络犯罪综合研究草案》，2013 年 2 月，第 26 页；

政府致力于清除的互联网内容包括儿童色情和仇恨言论，但也包括诽谤和批评政府的言论，因此有时激发对人权法的担忧。

一些评估显示，侵犯版权的互联网通讯约占全球总量的 24%。

5.2 国际社会的共同行动

5.2.1 网络犯罪全球治理项目

发生在无边界的网络空间，并与有组织犯罪集团逐渐深入的参与相复合，使得网络犯罪本质复杂。犯罪的实施者和受害者往往位于不同国家，其影响也波及了全球各地的社群。这使得采取紧急、动态且国际化的措施变得十分重要。为此，根据大会第 65/230 号 [38] 以及预防犯罪与刑事司法委员会（Commission on Crime Prevention and Criminal Justice）第 22/7 号 [39]、第 22/8 号 [40] 决议，网络犯罪全球治理项目（Global Programme on Cybercrime，下称项目）被授权建立。该项目通过能力建设和技术援助等方式帮助会员国治理网络犯罪。项目资金来源为澳大利亚、加拿大、日本、挪威、英国和美国政府的捐款。

项目旨在通过支持会员国预防和打击网络犯罪来灵活应对发展中国家的确定需求。项目在 2017 年的主要关注地区是中美洲、东非、中东和北非及东南亚和太平洋地区，项目的主要目标有：

在强有力的人权框架内，提高对网络犯罪，尤其是儿童性剥削和性虐待的调查、起诉和审判的效率；

将政府整体对网络犯罪的长期应对，包括国家协调、数据收集和有效的法律框架有效化和持续化，以达到可持续的应对和提高威慑力的目的；

随着公众对网络犯罪风险了解的增加，加强政府、执法机构和私营部门之间的国内和国际交流。[41]

5.2.2 网络犯罪开放式政府间专家组

联合国大会在其第 65/230 号决议 [42] 中依据《萨尔瓦多宣言》（the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World）第 42 段 [43] 要求预防犯罪与刑事司法委员会组建网络犯罪开放式政府间专家组（Open-ended

38 联合国大会：《第十二届联合国预防犯罪和刑事司法大会》，A/RES/65/230，2010 年 12 月；

39 预防犯罪与刑事司法委员会：“Strengthening international cooperation to combat cybercrime”， Resolution 22/7， 2013；

40 预防犯罪与刑事司法委员会：“Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime”， Resolution 22/8，2013；

41 UNODC：“Global Programme on Cybercrime”， official website， https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html，2 月 8 日登录；

42 联合国大会:《第十二届联合国预防犯罪和刑事司法大会》，A/RES/65/230，2010 年 12 月，第 3 页；

43 联合国大会:《第十二届联合国预防犯罪和刑事司法大会》，A/RES/65/230，2010 年 12 月，第 10 页；

Intergovernmental Expert Group on Cybercrime，下称专家组），在网络犯罪全球治理项目开始前，专家组已经开始全面研究会员国、国际社会和私营部门在网络犯罪问题上的对策。该专家组是目前联合国框架下探讨打击网络犯罪国际规则的唯一平台。[44]

专家组的第一次会议于 2011 年一月 17 日至 21 日在维也纳召开，在本次会议上，专家组回顾之前对一系列主题研究并确定了研究的基本范式。之后，在其第 67/189 号决议中，大会赞赏地注意到了专家组对于网络犯罪的全面研究，鼓励专家组努力完成现有工作并在合适时机加以介绍[45]。主题研究包含了八个章节：1. 连接性和网络犯罪；2. 全球情况；3. 立法和框架；4. 定罪；5. 执法调查；6. 电子证据和刑事司法；7. 国际合作；8. 预防[46]。

专家组的第二次会议于 2013 年 2 月 25 日至 28 日召开，在本次会议当中，除其他会议内容外，专家组注意到毒品和犯罪问题办公室在专家组主持下，依据大会第 65/230 号决议编写的网络犯罪综合研究草案以及会员国、国际社会和私营部门对此的回应。专家组的第三、四、五次会议分别于 17 年 4 月 10~13 日、18 年 4 月 3~5 日、19 年 3 月 27~29 日召开，第六次会议预定于 2020 年 4 月 6~8 日召开。[47]

5.2.3 布达佩斯网络犯罪公约

《布达佩斯网络犯罪公约》（Budapest Convention on Cybercrime）于 2001 年 11 月 23 日于布达佩斯签订（下称《布达佩斯公约》）。《布达佩斯公约》由欧洲委员会（Council of Europe）在法国斯特拉斯堡起草，欧委会观察员国加拿大、日本、菲律宾、南非和美国积极参与。2004 年 7 月 1 日，《公约》正式生效，截止 2019 年 9 月，共有 64 个国家批准了《布达佩斯公约》，另有四个国家签署了公约但尚未批准。

《布达佩斯公约》的附加议定书《种族主义与仇外议定书》（Protocol on Xenophobia and Racism）于 2006 年 3 月 1 日生效。批准了该议定书的国家必须将通过计算机系统散布种族主义和仇外内容以及因种族主义或仇外心理引起的威胁和侮辱定为犯罪。

《布达佩斯公约》是关于网络犯罪的第一部区域性的国际条约，也是目前在网络犯罪问题上唯一具有约束力的国际文书。该公约是缔约国在治理网络犯罪的立法层面的指南，以及缔约国之间进行国际合作的框架。其主要内容涉及侵犯版权、计算机相关诈骗、儿童色情制品和侵犯网络安全的行为。同时还包含一系列权力和程序（powers and procedures），例如对于计算机网络的调查和拦截。其序言中指出，《公约》的主要目标是确立保护社会免受网络犯罪侵害的共同刑事政策，特别是通过出台合适的法律以及促进国际合作。该公约的主要目的有：

1. 协调各国在网络犯罪领域的实质性刑事法律要素；

---

44 宋冬:《打击网络犯罪国际合作形势与展望》，载于《网络空间战略论坛》，2018 年 6 月刊，第 31 页;

45 联合国毒品和犯罪问题办公室，“Open-ended Intergovernmental Expert Group Meeting on Cybercrime”，official website，https://www.unodc.org/unodc/en/cybercrime/egm-on-cybercrime.html，2 月 8 日登录;

46 联合国毒品和犯罪问题办公室，“Open-ended Intergovernmental Expert Group Meeting on Cybercrime - meetings”，official website，https://www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html，2 月 8 日登录；

47 联合国毒品和犯罪问题办公室，“Open-ended Intergovernmental Expert Group Meeting on Cybercrime - Background information on the Comprehensive Draft Study on Cybercrime”，official website，https://www.unodc.org/unodc/en/cybercrime/egm-on-cybercrime/meetings.html，2 月 8 日登录；

2. 给予国内刑事程序法律效力，以调查和起诉此类犯罪、通过计算机系统进行的或与电子证据相关的其他犯罪；

3. 建立快速有效的国际合作机制。[48]

虽然《布达佩斯公约》在打击全球网络犯罪方面作出了诸多贡献，但是仍不能满足众多发展中国家的需求，因此受到了这些国家强烈的反对。在发展中国家的视角下，其具体问题有以下：

1. 成员国组成存在局限性：

《网络犯罪公约》的签署国大多局限于欧洲范围之内，除美国、日本等积极参与谈判并发挥实质性影响外，其他域外国家尤其是广大发展中国家对公约内容毫无话语权，其规定一般仅在欧洲范围内适用而无法成为全球标准。

2. 公约的加入程序复杂：

公约第 37 条规定，非欧委会成员国加入公约须由部长委员会征得缔约国的一致同意，然后在部长委员会的投票中获得 2/3 以上多数的支持，并取得列席委员会投票的缔约国代表的一致支持，方可获邀请加入公约。受制于繁琐的加入程序等因素，拓展缔约国的进程十分缓慢。

3. 公约内容存在局限性：

公约规定的网络犯罪罪行侧重于技术性犯罪，即以网络为犯罪对象的犯罪（如非法入侵、非法拦截、数据干扰、系统干扰、设备滥用等），与当前“传统犯罪网络化”的形势不相适应。除上述技术性犯罪外，公约规定的其他罪行，包括网络儿童色情、侵犯知识产权犯罪等，多为美欧发达国家关切的罪行，而发展中国家重点关注的网络成人色情、网络赌博等罪行均未纳入公约。

另外，公约构建的国际合作机制也易受各国有关国家主权、安全以及公共秩序主张的影响，实际效果有限。公约第 27 条第 4 款对司法协助规则进行了规定：“被请求方除了可基于第 25 条第 4 款的情形（现有司法协助文书的安排）拒绝请求外，还可基于以下情形拒绝协作：a. 被请求方视请求中的罪行为政治犯罪或与政治相关的犯罪；b. 被请求方认为请求的执行可能损害其主权、安全、公共秩序以及其他重要利益。”因此，一国可以公约的上述情况为借口，对拒绝合作的原因进行模糊处理，进而拒绝他国的司法协助请求。

5.2.4 网络犯罪数据储存中心

预防犯罪与刑事司法委员会第 22/8 号[49]决议指出:“网络犯罪数据储存中心（cybercrime repository，下称中心）是由毒品和犯罪问题办公室设置的储存网络犯罪相关法律与经验教训的中央数据库，设立这一数据库是为了促进对司法能力与需求的持续评估及提供和协调技术援助。”

中心下设判例法数据库（Case Law Database）、立法数据库（Database of Legislation）和经验教训数据库（Lessons Learned Database）三个数据库，分别记载有关网络犯罪的不同内容。判例法数据库主要记载有关网络犯罪和与电子证据相关的判例以及

48 Council of Europe Treaty Office， “Details of Treaty No.185 Convention on Cybercrime”， official website， https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185，2 月 8 日登录；

49 同上；

成功的执法行动记录，使用者可以了解会员国法院是如何处理有组织犯罪案件的。立法数据库主要包含网络犯罪记录和法律程序，可以按国家、网络犯罪类型和具体程序进行搜索，意在说明会员国是如何通过国内立法条款界定、禁止各类不法行为并将其定罪的。经验教训数据库包含预防和打击网络犯罪的国家政策和战略。[50]

同时，中心还作为打击犯罪信息与法律网络共享平台（Sharing Electronic Resources and Laws On Crime， SHERLOC）的一部分存在，该网站旨在促进《联合国打击跨国有组织犯罪公约》（the UN Convention against Transnational Organized Crime）及其三项议定书执行方面信息的传播。[51]

5.3 各国的行动

“在过去的十年中，制定打击网络犯罪的国际和地区文书方面出现了极大的发展。这包括具有约束力和非约束力的文书。这些文书可分为五类，包括在以下背景中制定或受到启发而制定的文书：（一）欧洲委员会或欧洲联盟；（二）独立国家联合体或上海合作组织；（三）非洲政府间组织；（四）阿拉伯国家联盟，以及（五）联合国。所有文书之间都存在大量交互影响，特别是《布达佩斯公约》制定的概念及方法。”[52]

各法系内国家在网络犯罪方面所采取的措施及其基本框架可以说是相似的，因此，笔者将以法系作为划分标准对各国的行动加以介绍。

5.3.1 英美法系国家

英美法系的两个代表性国家英国和美国，尤其是美国，在网络犯罪有关领域的制度框架较为完善。属于英美法系的其他国家如加拿大、澳大利亚、新西兰、南非等也都加入了《布达佩斯公约》，而如印度、巴基斯坦等国更是除此之外没有加入其它相关国际文书。因此，海洋法系国家的有关措施大多是在《布达佩斯公约》框架下的。笔者将着重介绍美国和英国。

美国联邦政府在网络犯罪治理领域中发挥着重要作用，其对联邦网络信息系统保护和协助非联邦网络信息系统保护都至关重要。在现有制度下，所有联邦政府机构对自己的网络信息系统负有直接责任，有些部门对部分关键基础设施也承担着一定的责任。在美国本土，至少有 50 项立法和 13 个判例直接或间接与网络犯罪有关。[53]

在 2015 年出台《网络安全保护法案》和《网络安全信息共享法案》之前，美国国会关于网络犯罪的有关立法常见措施为在国土安全部（Department of Homeland Security， DHS）或其他部门下设立一个专门机构。2015 年出台的《网络安全保护法案》（National Cybersecurity Protection Act）和《网络安全信息共享法案》（Cybersecurity Information Sharing Act）中，对网络安全有关事务做出了非常详细的规定，不管是从立法总体框架还是从立法深度上看，相关方面的法律保护都取得了很大的进步。[54]

50 The Cybercrime Repository， “About Us”， official website， https://sherloc.unodc.org/cld/about-us/index-cybrepo.html?lng=en，2 月 8 日登录；

51 SHERLOC， “关于我们”， 官方网站， https://sherloc.unodc.org/cld/v3/sherloc/?lng=zh，2 月 8 日登录；

52 联合国：《网络犯罪综合研究草案》，2013 年 2 月，第 20 页；

53 李小林：《美国网络安全立法研究及启示》，硕士论文，导师：齐爱民，重庆大学 ,2016 年；

54 李小林：《美国网络安全立法研究及启示》，硕士论文，导师：齐爱民，重庆大学，2016 年；

在美国国会通过的所有有关法案中，《网络安全信息共享法案》（下简称《法案》）的地位是最重要的。该法案的目标有三个：

建立一个鼓励私营企业自愿与联邦政府共享信息，从而帮助联邦政府加强防御的法律框架；

使国土安全部成为与私营企业交接的主要平台，并使其成为联邦政府与私营企业实现网络信息共享的主要门户；

努力平衡个人身份信息的保护与私营企业的信息保护的冲突。

《法案》同时也注重对于个人的保护，在个人隐私保护方面有以下要点：

个人信息处理。当企业与联邦政府分享有关数据时，在分享之前必须审查和评估这些数据，如与特定个人的网络安全相关，则必须删除这部分信息。此外，任何美国公民在其个人信息已经或将要被联邦政府共享时，必须及时给予其通知。

监督制度。司法部长需起草并定期修改与公民自由和隐私的有关方针，该方针对存储、使用和传播有关数据进行规定。隐私和公民自由委员会应每两年向国会和总统提交一个报告，报告需提供有关《法案》对个人隐私和公民财产影响的评估，并对有关问题提出相应指导方针。

终止期限。法案在十年后失效。[55]

2016 年推出的《网络安全国家行动计划》（Cybersecurity National Action Plan，CNAP），在总结奥巴马七年多执政经验的基础上对美国在数字时代面临的问题提出了策略方针。CNAP 指出“试图伤害美国的罪犯、恐怖分子和国家都已经认识到对美国的在线攻击要比直接攻击更容易”。因此，美国目前对网络犯罪主要有三个关注点：1. 持续扩大破坏性；2. 网络恐怖主义；3. 部分国家干涉选举。[56]

英国至少有 10 部法律的 14 个章节直接或间接与网络犯罪有关，但在 SHERLOC 网站的判例法数据库 [57] 中没有有关判例。与美国的 50 余项法案大多是作为专门针对网络犯罪问题的议案提出不同的是，英国部分有关法律（如 1978 年保护儿童法案 Protection of Children Act 1978，1907 年百慕大刑法典 Bermuda Criminal Code Act 1907，1988 年版权、设计与专利法 Copyright， Designs and Patents Act 1988） 通常并不是针对网络犯罪进行直接规定。换言之，英国对于网络犯罪有关案件的处理更多是基于对法律进行解释的方式进行。例如 1981 年伪造与仿造法规定，如一个人为自己或他人使用、伪造假冒工具，并且引诱他人接受仿造品作为真品，他就违反本法。而网络犯罪中伪造他人信息进行诈骗和通过伪造的工具让别人相信自己行为的合法性，则是明显违反本法的。[58]

在履行《布达佩斯公约》方面，英国通过立法形式或者直接执行《公约》的内容，与欧洲委员会成员国携手治理网络犯罪。不过英国对在网上传播种族主义和侮辱性语言这一方面的规定与《公约》并不完全一致。此外，英国政府还出台了多部《英国网络安全战略》（下简称《战略》）对英国信息安全建设做出了战略部署和具体安排。《战略》的一个愿景是在自由、公平、透明和法治等核心基础上，构建一个安全而具有活力和恢复力的网络空间，并以此促进经济增长和社会价值产生，通过实际行动促进经济繁荣、国家安全及社会稳定。

《战略》的四个战略目标分别是：应对网络犯罪，使英国拥有世界最安全的网络空间之一；使英国面对网络攻击拥有更强的恢复力，并保护其在网络空间中利益；帮助塑造一个可

55 李小林：《美国网络安全立法研究及启示》，硕士论文，2016 年 4 月，重庆大学，第 28 页；
56 李恒阳：《美国网络安全面临的新挑战及应对策略》，《美国研究》，2016 年 04 期；
57 SHERLOC: Case Law Database- crime type- cybercrime， official website，2 月 8 日登录；
58 古丽阿扎提·吐尔逊：《英国网络犯罪研究》，《中国刑事法杂志》2009 年 07 期；

供英国民众安全使用的、开放的、稳定的、充满活力的网络空间；构建跨界的知识技能体系，以对所有网络安全目标提供基础支持。[59]

5.3.2 大陆法系国家

大陆法系的代表国家有：法国、德国等欧盟国家以及中国。由于欧盟国家均加入了《布达佩斯公约》，在有关制度方面与美英等国差距不大，因此本部分将主要介绍欧盟整体和中国的有关制度。

在 2012 年前后，欧洲民众对于信息网络犯罪的担忧达到了前所未有的地步，民调显示 74% 的受访者认为自己成为网络犯罪受害者的风险正在增加。为重建公众对信息网络的信心，继法国、德国、英国等欧洲国家推出各自的网络安全战略之后，欧盟委员会于 2013 年发布了一份整个欧盟层面的网络安全战略，旨在通过各成员国政府、私营企业和公民的共同努力，使欧盟拥有世界上最安全的网络环境。

一，完善管理体制，推动信息共享。

欧盟是一个超国家组织，因此其网络安全管理体制分为欧盟和成员国两个层面：在欧盟层面，2004 年 3 月 10 日成立了欧洲网络与信息安全局（ENISA），其职责主要有：

分析网络安全威胁，并向欧盟委员会及成员国提供结果；

促进欧盟委员会和成员国间合作，提供相关咨询和援助；

协助欧盟委员会开展国际合作，

在成员国层面，各国相关部门如通信部、内政部、国防部等，负责制定相关政策并与其他公共机构和私营部门协作，识别信息安全威胁并积极采取应对措施。

二，提升恢复能力以应对网络攻击。

为提升欧盟及成员国防范、监测和应对网络安全事件的能力，增强遭受攻击后的恢复能力，欧盟委员会为欧盟整体和成员国制定了行动路线：

在欧盟层面，计划扩大 ENISA 在应急响应方面的职能，并建立紧急情况协调响应机制，增强网络攻击事件发生后的应对能力，并制定了通信供应和数据服务在数据保护方面的有关标准。

在成员国层面，欧盟敦促：尚未出台有关战略的国家尽快出台相关文件；成员国指定相关问题主管机构，并建立计算机应急响应小组（CERT）；通过各类方式提高公众的网络安全意识；对不同人开展不同内容的有关培训，培养专业人才队伍。

三，强力打击犯罪，力推《布达佩斯公约》。

作为全球第一个针对网络犯罪的国际公约，《布达佩斯公约》为其各成员国共同打击网络犯罪提供法理依据，同时也成为欧盟谋求网络犯罪领域领导地位的工具。一方面，欧盟极力敦促尚未批准该公约的成员国尽快批准并执行该公约，同时贯彻和执行网络犯罪相关指令；另一方面，欧盟和美国、日本等国家也在积极呼吁国际社会以该公约为基础，制定应对网络犯罪的国际框架和准则。

中国网络犯罪治理立场可以认为主要是从话语平台与话语策略出发的。话语平台被认为是决定网络犯罪治理逻辑的根本因素，在这方面中国更倾向于国际性的平台，如联合国。近年来，联合国在网络犯罪治理中的“中流砥柱作用”被中国政府反复提及。2016 年 6 月 26 日，中俄就网络犯罪相关问题达成七点共识，其中第六点明确：加大工作力度，预防和打击利用

59 刘权：《信息安全的英国之鉴》《中国经济和信息化》，2012 年 10 期；

网络进行恐怖及犯罪活动，倡议在联合国框架下研究建立应对合作机制，包括研究制定全球性法律文书。与欧盟、美国和日本等国家不同，中国唯一加入的有关国际文书为《上海合作组织国际信息安全领域协定》，并与俄罗斯一同主张重新建立一个联合国框架下的合作机制。中国对于《布达佩斯公约》的态度也较为冷淡，并不赞成在其机制上进行修改作为全球化的机制存在。[60]

5.3.3 伊斯兰法系国家

伊斯兰法系国家大多加入了《阿拉伯国家联盟打击信息技术犯罪公约》（Arab Convention on Combating Information Technology Offences，下称《阿盟公约》），而作为非阿拉伯国家的伊朗、马来西亚等国并未加入任何有关国际文书。《阿盟公约》的目的是加强阿拉伯国家之间在打击信息技术犯罪方面的合作，以抵御此类犯罪的威胁，进而保护阿拉伯国家的安全和利益及其社区和个人的安全。《阿盟公约》描述了其涵盖的信息技术犯罪、程序规定及缔约国之间的法律和司法合作机制。

《阿盟公约》在其第二章与第三章就非法访问、非法拦截、滥用信息技术手段等罪行做出了明确定义，并明确了网络犯罪有关程序规定及其适用范围。《阿盟公约》的第四章就法律与司法合作做出了明确的规定，其核心内容为：

要求缔约国将其法律管辖权限扩大到所有第二章所规定任何罪行；

确定相关犯罪罪犯的引渡标准；

规定各国间调查和收集相关电子证据的互助模式及跨国管辖标准；

技术合作与技术援助的有关标准；

要求各国成立 24 小时工作的特别部门管理网络犯罪的技术建议、

此外，值得注意的是，沙特阿拉伯等国引起国际社会关注的网络犯罪通常为对油田及有关设施的网络攻击。

5.4 国家间的执法合作

由于从理论层面讲解执法合作对于理解来说存在较大困难，因此我们将选取几个经典的执法合作案例以供参考。

【案例一：破坏 ZeroAccess 僵尸网络】[61]

2013 年 12 月，欧洲刑警组织的欧洲网络犯罪中心和美国联邦调查局一起，同与包括微软数字犯罪小组和 A10 网络公司在内的私营部门合作破坏了 ZeroAccess 僵尸网络。ZeroAccess 僵尸网络是一种恶意软件，感染了超过 200 万台使用 Microsoft Windows 系统的计算机。

ZeroAccess 僵尸网络是最具弹性和持久性的僵尸网络之一，并且预计可以抵挡外界破坏。感染了 ZeroAccess 僵尸网络的计算机会执行比特币挖掘或点击欺诈（clickfraud）。比特币挖掘涉及使用计算机进行计算以获取比特币的过程。点击欺诈则是一种计算机劫持

60 蔡高强，焦园博：《论联合国框架下网络犯罪国际治理的中国立场》，《中央民族大学学报（哲学社会科学版）》，2019 年 46 期 02 版；

61 编者注：本案例在 SHERLOC 数据库中编号 No.CYB001R；

技术，它将受感染的计算机的网络访问重定向到包含广告的网站，这些广告按点击数向 ZeroAccess 付费。比特币挖矿和点击欺诈产生的收入被控制僵尸网络的网络犯罪分子获得。欧洲刑警组织表示，ZeroAccess 僵尸网络所产生的活动估计每月使广告主花费 270 万美元。

由于该僵尸网络的复杂性和弹性，这一举措并未完全消灭 ZeroAccess 僵尸网络，不过严重影响了其运行。欧洲刑警组织和有关的私营部门正在努力通知计算机被感染的人并提供提供信息，以教育公众如何保护自己免受 ZeroAccess 僵尸网络的侵害。

这一行动证明，与私营部门的合作对于抵御恶意软件和僵尸网络的威胁至关重要。执法部门和私营部门之间的情报共享有助于识别与恶意软件相关的 IP 地址。这种合作导致了对有关服务器的搜寻和缉获，使僵尸网络遭到破坏。[62]

【案例二：美利坚合众国诉 Steven W Chase】[63]

被告 Steven W Chase 先生于 2014 年 8 月 19 日至 2015 年 3 月 4 日之间是 Playpen 网站主要管理人，该网站专门交易儿童色情内容。在该网站上，用户能够以匿名方式聊天，并交换和购买儿童性虐待内容的图像。网站的内容根据受害人的年龄和性别以及所涉及性行为分为不同的“标牌”（boards）。

2014 年 12 月，Chase 出现疏漏使得 Playpen 的 IP 地址暴露给了意大利执法机构。这一 IP 地址显示其位于美国，因此通知了美国联邦调查局。2015 年 1 月，FBI 与美国司法部儿童剥削与淫秽科，FBI 外地办事处以及许多国家的外国对口机构共同实施了“奶嘴行动”，该行动旨在识别 Playpen 网站的用户并将他们绳之以法。2015 年 2 月 19 日，FBI 执行了对 Chase 先生房屋的搜查令并逮捕了他。搜索过程中对一台计算机进行的法医检查发现了数千张儿童性剥削的有关图像。2016 年 9 月 16 日，联邦陪审团裁定 Chase 先生与儿童色情和剥削儿童有关的多项指控成立。2017 年 5 月 1 日，他被判处 30 年有期徒刑。

另外两个 Playpen 网站的管理员分别是美国印第安纳州的 46 岁的 Michael Fluckiger 和美国肯塔基州的 47 岁的 David Browning。他们在 2015 年 12 月因为剥削儿童组织服务被判有罪，并于 2017 年初被判处 20 年徒刑。[64]

本案件之所以意义重大，是因为 Playpen 网站的规模以及调查导致的对儿童性犯罪者的逮捕、起诉和定罪的数量。该网站有来自世界各地的 150,000 多名用户，并被 FBI 认为是世界上最大的儿童色情网站。FBI 的调查规模和影响范围都是空前的，此案在当时被认为是 FBI 在起诉使用匿名 Tor 服务人员方面的最成功的案例。

截止 2017 年 5 月 4 日，“奶嘴行动”已经在美国境内已经逮捕了 350 人，起诉了 25 名儿童色情制品的制作人、51 名对儿童进行性虐待的人，查明或营救了 55 名遭受性虐待的美国儿童。同时，“奶嘴行动”还导致了 548 起国际逮捕，包括 358 起在欧洲的逮捕行动，并对美国境外 296 名遭受性虐待的儿童进行了识别或营救。

该案意义重大的另外一个原因，是其表明了涉及对儿童的性虐待和散布儿童色情制品的人如何变得越来越老练，并使用技术手段保护其身份以阻止执法调查。换言之，该案也表明执法部门在查明这类罪犯并将其绳之以法方面所面临的挑战。

EC3 负责人 Steven Wilson 评论说：“对儿童进行性虐待的人正变得越来越具有法医学

62 SHERLOC: Operation: Disruption of the ZeroAccess botnet, UNODC No.: USAx151, https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/xxx/2013/operation_disruption_of_the_zeroaccess_botnet.html?lng=en&tmpl=sherlock, 2 月 20 日访问；

63 编者注：本案例在 SHERLOC 数据库中编号 USAx151；

64 同 29；

意识，并积极使用最先进的匿名和加密形式来避免被发现。执法部门需要能够使用适当手段来应对这种对我们孩子的威胁。互联网没有边界，也无法识别边界。我们需要在受害者的权利与隐私权之间取得平衡，如果我们遵循 19 世纪的法律原则，那么我们将无法在最高层次上有效地应对犯罪。”[65]FBI 特工 Dan Alfin 表示，“奶嘴”行动只有在 FBI 国际合作伙伴和外地办事处的支持下才能取得成功。[66]

65 同 29, Commentary and Significant Features；
66 同 29, Investigation, Comments；

6. 可能的解决思路

6.1 发挥国际公约机制的作用

国际公约具有约束力，能有效打击网络犯罪。自 2011 年联合国预防犯罪和刑事司法委员会召集网络犯罪政府专家组至今，专家组仅举行了五次会议，其中第二次会议和第三次会议之间经历了长达四年的停滞。造成专家组工作进程较缓的主要原因是各国对待制定治理网络犯罪的国际规则的态度存在较大差异。世界各国在“需要一个治理网络犯罪的全球性公约”这一目标上达成共识，但如何实现该目标，国际社会主要有两种不同思路：一是美国、日本和欧委会成员国所倡导的，将原有的《布达佩斯公约》“原封不动”地继续进行推广，或者经过“小修小补”后吸纳更多的国家加入其中；二是中国、俄罗斯等发展中国家所倡导的，在联合国框架下“另起炉灶”，构建新的国际规范。

在本章的后续内容中，我们将会把上述两种思路延伸为“路径一：推广或扩充现有的区域性公约”和“路径二：在联合国框架下构建新公约”，并进行具体阐述和可行性分析。

6.1.1【路径一：推广或扩充现有的区域性公约】

首先声明，由于《布达佩斯公约》是目前影响范围最广、同时争议最大的区域性公约，所以我们会将其作为典型分析路径一，暂不讨论其他区域性公约。

经简化，路径一既包括照搬《布达佩斯公约》，将其直接推广成为全球性公约的方式[67]；也包括保留《布达佩斯公约》的基本框架进行内容扩充，将其间接推广成为全球性公约的方式[68]。结合背景文件第五章“现状与已采取措施”的相关论述，我们将路径一的优劣总结如下：

其优势包括：第一，基本框架成熟，《布达佩斯公约》对定罪、程序法、国际合作等内容均做出规定；第二，内容可更新，可以通过发布实施指南、制定议定书等方式使《布达佩斯公约》与时俱进；第三，准入门槛高，有利于保障《布达佩斯公约》内容的高标准和有效性；第四，一定程度上可以节约时间和资源。

其劣势包括：第一，时代局限性，欧洲理事会近二十年来仅针对《布达佩斯公约》编制两份议定书，导致内容不能适应治理网络犯罪的时代需求；第二，条款不公平性，《布达佩斯公约》并不能平等地维护所有缔约国利益，部分条款在非欧盟国家存在侵犯司法主权之嫌；第三，签约封闭性，非欧盟成员国加入《布达佩斯公约》的门槛高，缔约过程不开放。

通过对比可以发现，《布达佩斯公约》的主要优势和劣势其实是辩证统一的。不可否认的是，美国、日本，以及欧盟成员国等发达国家坚持将《布达佩斯公约》推广成为全球性公约，是从国内政治、经济、安全等维度出发做出的最佳选择，也是国家利益至上的行为体现。截

67 将这一方式命名为路径一（a）；
68 将这一方式命名为路径一（b）；

至 2020 年 1 月，《布达佩斯公约》已有 64 个正式缔约国[69]，且已对 140 余个国家[70]的网络犯罪立法工作产生了指导性影响。2019 年，贝宁、布基纳法索、巴西等 3 个国家被邀请加入《布达佩斯公约》，待完成所有成为缔约国的内部程序后，也将与其他 64 国一同开展包括电子证据获取便利在内的打击网络犯罪方面的合作[71]。鉴于《布达佩斯公约》缔约国众多，加之上文提到的优势和劣势，将该公约推广成为全球性公约是一条虽然简单但阻力较大的可选路径。

阿尔巴尼亚	安道尔	亚美尼亚	阿根廷	* 澳大利亚	奥地利
阿塞拜疆	比利时	波黑	保加利亚	* 佛得角	* 加拿大
* 智利	* 哥斯达黎加	克罗地亚	塞浦路斯	捷克	丹麦
* 多明尼加	爱沙尼亚	芬兰	法国	格鲁吉亚	德国
* 加纳	希腊	匈牙利	冰岛	* 以色列	意大利
* 日本	拉脱维亚	列支敦士登	立陶宛	卢森堡	马耳他
* 毛里求斯	摩尔多瓦	摩纳哥	黑山	* 摩洛哥	荷兰
北马其顿	挪威	* 巴拿马	* 巴拉圭	* 秘鲁	* 菲律宾
波兰	葡萄牙	罗马尼亚	圣马力诺	* 塞内加尔	塞尔维亚
斯洛伐克	斯洛文尼亚	瑞士	西班牙	* 斯里兰卡	* 汤加
土耳其	乌克兰	* 英国	* 美国	\	\

表格 1 《布达佩斯公约》缔约国[72]

* 巴西	* 布基纳法索	* 贝宁	俄罗斯	* 南非	* 突尼斯
* 哥伦比亚	* 尼日利亚	瑞典	爱尔兰	\	\

表格 2 《布达佩斯公约》观察员国[73]

2019 年 11 月 18 日，联合国大会表决了俄罗斯等 46 个国家共同提交的题为“打击为犯罪目的使用信息和通信技术行为”的决议草案，该决议草案以 88 票赞成、58 票反对、34 票弃权获得通过[74]。根据该决议草案内容，“联合国大会决定设立一个代表所有区域的不限成员名额特设政府间专家委员会，以拟定一项关于打击为犯罪目的使用信息和通信技术行为的全面国际公约[75]（以下简称“新公约”）。”在这一背景下，路径一（a）前景渺茫，而

69 Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY，Cybercrime， T-YC Committee， Council of Europe， https://www.coe.int/en/web/cybercrime/parties-observers， 2020 年 2 月 4 日登录 ;

70 Benin invited to accede to the Budapest Convention on Cybercrime， T-YC News， T-YC Committee， Cybercrime， Council of Europe， https://www.coe.int/en/web/cybercrime/-/benin-invited-to-accede-to-the-budapest-convention-on-cybercrime， 2020 年 2 月 4 日登录 ;

71 Budapest Convention: Brazil invited to accede， T-YC News， T-YC Committee， Cybercrime，Council of Europe， https://www.coe.int/en/web/cybercrime/-/budapest-convention-brazil-invited-to-accede， 2020 年 2 月 4 日登录；

72 * 非欧洲委员会成员国，下表同；

73 Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY，Cybercrime， T-YC Committee， Council of Europe， https://www.coe.int/en/web/cybercrime/parties-observers， 2020 年 2 月 4 日登录；

74 A/74/401 号报告，联合国大会第三委员会，2019 年；

75 A/RES/74/247 号决议，联合国大会第三委员会，2019 年；

路径一（b）仍存在可能性，但也是道阻且长，国际社会需要取之精华、弃之糟粕：一方面，要保护《布达佩斯公约》的可更新性，促使世界各国在网络犯罪立法上进一步趋向兼容性和一致性；另一方面，要吸取其它已有国际规范的经验，努力破除《布达佩斯公约》的时代局限性、条款不公平性和签约封闭性。

6.1.2【路径二：在联合国框架下构建新公约】

路径二仅指在不依赖《布达佩斯公约》等已有区域性公约的前提下，在联合国框架内制定全新的打击网络犯罪的全球性公约。这一路径的优劣十分突出：其优势在于联合国这一多边外交平台能保障公约制定过程的民主、透明和多边参与，可以反映更多国家普遍关注的问题；劣势在于工程量巨大，需要耗费大量时间和资源。接下来，我们将对路径二的可能性进行分析，并讨论假若采取路径二，新公约可能具备的指导思想和基本框架。

可行性一：联合国已通过相关决议

俄罗斯、中国等发展中国家长期倡导这一路径，并得到越来越多国家的认可与支持。2004 年，中国等国首次在联合国预防犯罪和刑事司法委员会上便提出，希望在联合国机制下制定一部专门打击网络犯罪的国际公约。2017 年，俄罗斯向联合国大会提交《联合国打击网络犯罪国际合作公约草案》[76]。

正如上文所述，联合国大会已经以 88 票赞成对 58 票反对、34 票弃权通过了关于构建新公约的决议。换句话说，在俄罗斯、中国等发展中国家的不断推动下，在联合国框架下构建新公约的路径已获得世界多数国家的支持，联合国将为此分配资源，捐助国也需要为发展中国家的参与提供帮助。

阿塞拜疆	安哥拉	佛得角	塞内加尔	塞尔维亚	斯里兰卡
贝宁	南非	尼日利亚	俄罗斯		

表格 3 投赞成票的《布达佩斯公约》缔约国和观察员国

通过对比《布达佩斯公约》缔约国、观察员国名单和 A/RES/74/247 号决议表决情况，可以发现仅有阿塞拜疆等 10 个国家在此表决中投赞成票，其中大部分为非欧洲委员会成员国、发展中国家，这更加直观地反映了美国、欧洲委员会成员国等《布达佩斯公约》缔约国同俄罗斯、中国等发展中国家之间的意见分歧。

可行性二：联合国制度框架的优越性

一方面，联合国善于协调各国矛盾。作为最具代表性和权威性的国际组织，联合国已成功推动《联合国气候变化框架公约》等全球性公约的签订，将其选做推动打击网络犯罪国际合作的平台，既有利于牵制和平衡各国的利益偏好，保障新公约的广泛代表性和中立性，也有利于监督世界各国对新公约的执行情况。

另一方面，联合国现有资源十分丰富。联合国毒品与犯罪问题办公室在打击跨国犯罪、网络犯罪等方面有着丰富的实践经验，包括但不限于组建政府间专家组、设立资料库和基金[77]，相关研究涵盖立法、司法等多个方面; 国际电联在推动网络犯罪全球研究上也成绩斐然，这些经验都将在新公约的制定过程中发挥积极作用。

76 Draft United Nations Convention on Cooperation in Combating Cybercrime， The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland， https://www.rusemb.org.uk/fnapr/6394， 2020 年 2 月 5 日登录；

77 具体内容可参考背景文件第五章“现状及已采取的措施”；

关注点一：新公约的指导思想

第一，新公约应当是系统的，兼具国家层面和国际层面。国家层面上，既要重视政策制定，通过完善立法、加强司法等方式打击政治、经济、社会、技术等各维度可能发生的网络犯罪行为，避免成为全球网络犯罪治理的最弱环节；又要重视公众意识培养，动员社会各行业从业者发挥优势，参与网络犯罪治理。国际层面，应加强合作，通过包括但不限于分享数据信息、开展技术援助的方式共同提高打击网络犯罪的能力。

第二，新公约应该是全面的，涵盖几乎所有网络犯罪形式。对旧的犯罪形式，如非法进入、非法截取、电脑诈骗等，不能只是解释现有的含糊不清的法律，而要制定具体、清楚的条款，以确保在司法审判过程中可以给网络犯罪人员以确定罪名。对新的犯罪形式，如僵尸网络、网络钓鱼、信息盗用等，要进行充分调研，吸取各国好的立法、执法经验，在新公约中加以定罪。

第三，新公约应当是尊重国家主权、保护用户利益的。在新公约面前，不论国家政治体制、意识形态、经济实力、技术水平存在何种差异，任何国家都不应以此为由侵犯他国主权；亦不论公民性别、种族、宗教信仰、受教育程度存在何种差异，任何用户都不应以此为由侵犯他人利益。新公约需要对管辖权等权利进行限制，保护包括个人信息在内的计算机数据。

关注点二：新公约的基本框架

具体法律措施将是运用新公约预防和打击网络犯罪的关键所在。新公约需要保留《布达佩斯公约》等区域性公约已经强调的定罪、程序法、国际合作等实质内容，并且结合背景文件第四章“问题与挑战”的相关内容、俄罗斯于 2017 年提交的《联合国打击网络犯罪国际合作公约草案》的具体内容和《网络犯罪综合研究（草案）》的研究成果，考虑制定加入、生效、修改、保留、退出等具体条款，并在实体规则、管辖权、电子证据、引渡制度、财产损失的追回程序、网络服务供应商的责任与义务、预防等方面进行革新和补充。

在联大决议表决通过成为既定事实的前提下，在联合国框架下构建新公约或是最理想的路径选择。新公约的框架和内容将成为新一轮辩论的焦点，考虑到各国之间的利益纠纷和意见分歧，新公约的生效和推广道阻且艰。

6.2 发挥国际会议和国际组织机制的作用

在俄罗斯、中国等发展中国家的积极推动下，构建新公约已成为多数国家在未来一段时间内所共同关注的核心目标；但与此同时，由于《布达佩斯公约》缔约国众多，且在很长一段时间内发挥着积极效用，故部分国家想用新公约将其取代还需要经历更多的积极探索。因此，新公约能不能获得世界各国的普遍认可和加入，仍有诸多不确定性。

这种情况下，寻求短期的、可快速生效的合作机制也是一个可行的解决路径。具体来说，世界各国可以利用双边或多边的国际会议机制、国际组织机制，以发展中国家间、发达国家间或发展中国家和发达国家间的合作为基础，在坚持己方立场的同时多交流、多合作，以达成示范条款、备忘录或谅解等成果性文件，为将来新公约的生效和推广投石问路。

6.2.1 发挥国际会议机制的作用

长期以来，国际会议平台是各国推动合作、协调关系、缓解冲突、维护国际秩序的场所，能够发挥单个主权国家难以起到的独特作用。鉴于网络犯罪已成为全球性的非传统威胁，诸

多国际会议都已将打击网络犯罪列入议题单当中。无论是多边机制还是双边机制、无论是政府间还是非政府间、无论是全球性还是区域性，这些会议都存在着国际会议机制所共有的作用和缺陷。我们通过以下三个案例来予以描述：

【案例一】

亚洲 - 非洲法律协商组织（AALCO，以下简称“亚非法协”）是一个政府间、区域性的多边会议机制，成员国均为亚洲和非洲国家。2014 年，中国在亚非法协德黑兰年会上提出，希望在协会框架下增加“网络空间国际法”的议程，受到了亚非国家的欢迎，该倡议由会议一致通过[78]。2015 年，亚非法协北京年会上决定设立一个开放式的网络空间国际法工作组，专门从事保护网络空间国家主权、大家网络犯罪国际合作等问题的研究工作[79]。目前该工作组已召开两次工作会议，其中 2017 年会议上，与会成员提出应鼓励各国开展相关立法工作，或是要制定一份打击网络犯罪国际合作的国际法规则。

【案例二】

“伦敦进程”（London Process）是一个全球性的多边会议机制，也是世界上迄今为止唯一一个专门针对网络安全和网络空间治理问题的多边会议，目前已在伦敦、布达佩斯、首尔和海牙举办了四次会议，与会国数目均超过 60 个，且多为欧美发达国家。“网络犯罪”是“伦敦议程”的五大议题之一[80]，故四次会议均涉及了打击网络犯罪的国际法规则问题，《布达佩斯公约》依然适用、无需以条约形式制定新的规则成为了会议的主流声音。会议“价值观辩论”的色彩非常浓厚，至今“伦敦进程”未出台任何成果性文件。值得一提的是，“伦敦进程”邀请了行业代表、非政府组织代表、智库代表等参与辩论。

【案例三】

中美打击网络犯罪及相关事项高级别联合对话是一个政府间的双边会议机制。从 2015 年建立至今，该机制已开展了三次会议。会议具有较高的集中性和延伸性，内容包括但不限于网络诈骗、商业窃密、网络军火交易、网络色情传播。会议还取得了一系列合作成果，包括但不限于：网络保护、热线机制、信息共享、案件合作和成立专家组会议[81-82]。

从上述案例我们不难看出，国际会议机制侧重于立场表达和意见交换。部分国家会将国际会议视作一个“演说平台”，借机宣传本国的立场和理念，力求获得更多国家的认可和肯定。更多国家会在国际会议上交流意见和看法，以加强彼此之间的了解和信任，从而为开展更深层次的政治、经济、文化、法律合作奠定基础。此外，国际会议机制的准入门槛设置灵活，有效的扩大了参与讨论的行为体范围，非政府组织、智库、网络服务提供商等非国家行为体能够在网络犯罪全球治理中发挥越来越重要的作用。

国际会议机制也存在不可回避的缺陷。第一，多边会议“务虚”大于“务实”，通过阅读案例二会发现，“伦敦进程”注重国家对于价值观的宣传和维护，价值观冲突使得会议处

78 Resolution of 54th Annual Session on International Law in Cyberspace， AALCO， http://www.aalco.int/54thsession/Cyberspace%202015. Pdf， 2020 年 2 月 5 日登录；

79 Resolution of 55th Annual Session on International Law in Cyberspace， AALCO， http://www.aalco.int/54thsession/Cyberspace%202015. Pdf， 2020 年 2 月 5 日登录；

80 黄志雄：《2011 年“伦敦进程”与网络安全国际立法的未来走向》，载《法学评论》，2013 年，第 4 期，总第 52-57 页；

81 第二次中美打击网络犯罪及相关事项高级别联合对话取得七项成果，中华人民共和国中央人民政府，http://www.gov.cn/xinwen/2016-06/15/content_5082555.htm，2020 年 2 月 6 日登录；

82 第三次中美打击网络犯罪及相关事项高级别联合对话联合成果清单，中华人民共和国中央人民政府，http://www.gov.cn/xinwen/2016-12/09/content_5145730.htm，2020 年 2 月 6 日登录；

于拉锯状态，以致没有任何成果性文件产出。第二，多边会议缺乏持续性和稳定性，目前除“伦敦进程”外，所有的多边会议都是将网络犯罪作为维护网络安全或是促进互联网技术发展的子议题，缺少讨论网络犯罪的专门性国际会议。第三，多边会议的成果作用有限，这是由两方面因素造成的：一方面，与会国的立场“一边倒”，亚非法协的成员国主要是发展中国家，在国际合作的主体思路上与中国较为相似，主张建立全球性的国际法规则，而“伦敦进程”的主要与会国是美欧等发达国家，推广《布达佩斯公约》便是“最佳选择”；另一方面，暂且不论多边会议达成共识、发布成果性文件的可行性，即使出台了成果性文件，也不具有法律约束力和强制力。第四，双边会议便于取得成果，但成果难以向其他国家推广。

综上，如果希望继续发挥国际会议机制的作用，可以考虑在开展新的、巩固现有的双边会议机制之外，建立讨论网络犯罪全球治理的专门性多边会议，为主张不同路径的国家搭建一个平等交流的平台，推动研究和制定体现与会国利益和需求的示范条款。随着相关领域的多边会议逐渐增多，国家间的交流与合作范围将出现越来越多的交集，各国便可以通过互动推动示范条款、谅解等获得更大范围的认可。

6.2.2 发挥国际组织机制的作用

为应对网络犯罪造成的危害，国际组织也在依靠现有的组织平台积极推动网络安全和网络犯罪领域的规制、标准、制度建设[83]。除了上文已详细说明的网络犯罪全球治理项目、网络犯罪开放式政府间专家组、联合国预防犯罪与刑事司法基金和《网络犯罪公约》外，国际刑警组织、欧盟等国际组织也做出了诸多尝试，我们将作为案例给出，并分析国际组织机制的作用和缺陷。

【案例一】

国际刑警组织（INTERPOL）是世界各国联合打击刑事犯罪的全球性国际组织，是国际警察合作的主要渠道，共有 194 个成员国[84]。早于 2000 年，国际刑警组织便建成了反计算机犯罪情报网络[85]，用于收集计算机和网络犯罪活动的情报，为各国政府和企业提供技术支持。2015 年，国际刑警组织正式启动位于新加坡的全球创新综合机构（IGCI）[86]，专门预防和打击区域性和全球性的新型网络犯罪。国际刑警组织还在研究网络犯罪的形式与策略、加强公私合作、共享数据信息等方面做出了一系列努力。

【案例二】

欧洲联盟（EU）作为当今影响力最大的区域性国际组织，从上世纪 90 年代便开始进行网络犯罪内部治理行动。其设立了欧洲网络犯罪中心、欧洲网络与信息安全局等多个职能不同的实体部门，颁布了《关于打击计算机犯罪协议的共同宣言》等多项法律法规。同时，欧盟还与美国以及中国等发展中国家开展了多方面的外部合作。

相较于国际会议机制，国际组织机制具有更强的稳定性，在网络犯罪全球治理这一议题上，国际组织常采用举行定期会议、成立政府间专家组、建立实体机构等方式，推动世界各

83 于志刚：《全球化信息环境中的新型跨国犯罪研究》，中国法治出版社 2016 年版，第 267 页；

84 What is INTERPOL， Who we are， INTERPOL， https://www.interpol.int/Who-we-are/What-is-INTERPOL， 2020 年 2 月 6 日登录；

85 国际刑警组织准备建立反计算机犯罪情报网络，中国新闻网，http://www.chinanews.com/2000-07-02/26/36014.html，2020 年 2 月 6 日登录；

86 驻新加坡大使陈晓东对国际刑警组织全球综合创新中心进行工作访问，中国驻新加坡大使馆，http://www.chinaembassy.org.sg/chn/sgxx/sghd/t1429419.htm，2020 年 2 月 6 日登录；

国达成更多共识，为进一步构建全球性公约奠定基础。同时，联合国毒品与犯罪问题办公室、国际电信联盟、国际刑警组织等国际组织均能在各自的专业领域范围内发挥重要作用，通过政策研究、技术创新来提高成员国的立法、执法和刑事司法能力。

国际组织机制也存在一定缺陷。第一，除了联合国（主要机关、方案、基金、专门机构）和国际刑警组织外，其余参与治理网络犯罪问题的均是区域性组织，导致建立的机构具有地域局限性，且其制定的制度适用不广泛，难以满足解决全球性问题的需求。第二，国际刑警组织的职能有限，其主要发挥的作用在于协调多方合作和提供技术支持，并不能为治理网络犯罪提供法律制度层面的帮助。第三，受限于联合国的职权，其出台的宣言、决议、报告等文件并不具有约束力。

若想继续发挥国际组织机制的作用，一方面，可以考虑成立与现有机构职能不交叉、不冲突的实体性机构，就网络犯罪治理的某一细分方向开展实践；另一方面，可以推动相关国际软法的形成，而非一步到位构建全球性公约。

7. 针对各问题的国别立场分析

7.1 立法及政策框架议题

1. 各国网络犯罪立法趋同趋势明显

a）在应对网络犯罪的总体策略方面，各方均认同应采取系统、综合和整体的方式应对网络犯罪，强调应完善国内相关立法政策，加强应对网络犯罪的机制体制和执法能力建设，强化政府各部门之间的打击网络犯罪协作以及政府与互联网企业等的公私合作，加强应对网络犯罪的公共教育，提升全社会应对网络犯罪的意识和能力，不断整合和完善网络犯罪执法司法合作网络和机制等；

b）在应对新挑战方面，各国普遍关注云计算、大数据、物联网等新技术发展对打击网络犯罪带来的挑战，特别是如何制定有效规则，为跨境获取电子证据提供法律保障。欧洲委员会表示，其就该问题成立了相关的工作组，并正在谈判制定网络犯罪《网络犯罪公约》附加议定书。

2. 各国在一些具体问题的政策取向、优先目标以及手段方式上存在分歧

a）发展中国家认为，应从网络安全治理的总体视角审视网络犯罪应对问题，加强专家组与联合国等其他平台沟通与协调。

b）发达国家强调应严格区分两者，专家组应聚焦网络犯罪问题，网络安全问题则应由国际电联、联合国信息安全政府专家组等其他平台讨论。

7.2 国际公约的理念分歧

拥护“网络自由”

代表国家：美国

行动：美国《网络空间国际战略》的出台标志着“网络自由”的概念正式形成，“网络自由”也是该战略的核心词汇。这个概念的核心要点在于，通过对全球网络空间信息流动环境的塑造，将全球网络空间和最新的互联网应用作为实践美国外交政策的新工具。为此，美国偏向对“网络安全”做狭窄的定义，认为只有网络基础设施和存储在网络空间中的信息（特别是商业机密）的安全才是网络安全的范畴，在网络中传播的非经济类但可能对国家安全构成威胁的信息，原则上不属于网络安全的范畴。

拥护“网络主权”

代表国家：中国、俄罗斯

行动：2011 年 9 月 22 日，在由俄国家安全会议牵头组织的 52 国情报机构首脑闭门会议上，俄方提出了《确保国际信息安全公约》的草案。这个公约的内容为禁止将互联网用于

军事目的，禁止利用互联网推翻他国政权，同时各国政府可在本国网络自由行动。中俄等国向第 66 届联大提出的《信息安全国际行为准则》（草案）也提出：“重申与互联网有关的公共政策问题的决策权是各国的主权。对于与互联网有关的国际公共政策问题，各国拥有权利并负有责任”。上述文件草案都表明了网络主权的观点，这是中俄与欧盟在网络空间领域的最深刻分歧。[87]

7.3 各国对《网络犯罪公约》的看法

西方国家

态度：主张依照《网络犯罪公约》打击网络犯罪，无需制定新规则。这些西方国家认为打击网络犯罪，应坚持保护人权，强调言论自由与网络自由；在国际合作上强调跨境证据调查的时效性，削弱国家司法主权。

中国等发展中国家

态度：应协调好网络自由与网络主权的关系，网络应受到合理监管；跨境证据调查也应事先征得当事国的同意，尊重国家司法主权。在这种背景下，中国、俄罗斯等新兴国家认为《网络犯罪公约》存在弊端，需要在联合国框架下制定新的规则。

行动: 2013 年 4 月 26 日，联合国预防犯罪和刑事司法委员会第 22 届会议在维也纳闭幕，会议的主要亮点是巴西、俄罗斯、印度、中国、南非五国以“金砖五国”的名义向联合国提出了《加强国际合作，打击网络犯罪》的决议草案，要求进一步加强联合国对网络犯罪问题的研究和应对。[88] 2018 年 4 月 3 日至 5 日，在维也纳举行的联合国网络犯罪政府专家组第四次会议上，中国以及其他金砖国家、伊朗、埃及、阿尔及利亚、科威特等国从法理、技术和实务等角度予以反驳，强调《网络犯罪公约》系地区性公约，广大区域外国家未参与公约谈判，内容没有代表性；公约规定了苛刻的加入程序，需由欧洲委员会邀请并经过公约缔约国一致同意方可加入，不具有国际性公约所应具备的开放性。此外，公约成立“获取跨境数据工作组”，就跨境电子证据获取问题谈判制定新的附加议定书，也足以说明公约需要更新和补充，才能符合时代需要。这一进程应该通过在联合国这一最具代表性的平台谈判制定全球性文书的方式来进行，才能真正推动打击网络犯罪的国际合作。

87　于志刚：《缔结和参加网络犯罪国际公约的中国立场》[J]，政法论坛， 2015 年第 33 期（5），第 91-108 页；

88　蔡雄山：《网络犯罪的国际治理》[J]，方圆， 2014 年（4）: 第 32-33 页；

8. 需要代表思考的问题

1. 如何理解预防犯罪和刑事司法委员会与经社理事会以及毒品和犯罪问题办公室的关系?

2. 国际社会应如何合作，以解决犯罪行为发生地与犯罪结果发生地分处两国的网络犯罪?

3. 随着网络犯罪形式日趋多样，技术水平越来越高，各国应如何解决立法层面与执法能力的双重缺失?

4. 在双重归罪原则下，如何能保障国际司法合作的顺利进行?

5. 在各国网络相关法律差异巨大的情况下，如何能保证最终的罪、责、刑相适应?

6. 如何平衡国际法与各国网络相关法律的适用?

7. 为什么属于大陆法系的法德等欧盟国家与英美法系的美国等国家共同认可《布达佩斯公约》?

8. 为什么中国和俄罗斯对于修改《布达佩斯公约》持反对立场？试分析其深层原因；

9. 请对比《阿拉伯国家联盟打击信息技术犯罪公约》与《布达佩斯公约》在国际合作框架上的差异，并分析造成此等差异的原因；

10. 请对比国际会议机制和国际组织机制的优势和不足；

11. 请思考以联合国为框架的多边外交平台的局限性；

9. 推荐阅读

1. 国际条约：
《联合国打击跨国有组织犯罪公约》
《布达佩斯网络犯罪公约》
《阿拉伯国家联盟打击信息技术犯罪公约》
《上海合作组织国际信息安全领域协定》
《多哈协定》
《关于各国依联合国宪章建立友好关系及合作的国际法原则宣言》

2. 学术论文：
尹鹤晓：《电子数据侦查取证程序研究》；
蔡雄山：《网络犯罪的国际治理》；
黄志雄：《2011 年“伦敦进程”与网络安全国际立法的未来走向》
于志刚：《全球化信息环境中的新型跨国犯罪研究》
刘潇潇：《信息网络犯罪之预防》
夷冰倩：《公安机关提取电子数据的法律规制阴》
王燃：《大数据时代个人信息保护视野下的电子取证——以网络平台为视角》
李强：《毒品犯罪案件侦查中电子取证存在的问题及对策》
贾哀浩，姚强，韩笑晨：《电子证据的演进 : 从模式思维到制度理性—以司法实践中的发展为考察进路》
杨三朋：《论跨国网络犯罪中国际刑事司法合作的问题》
Von Bogdandy：《联合国法律要点年鉴》
Sierber：《掌控全球网络空间的复杂性》
Heller：《比较刑法手册》
Zweigert：《比较法律》

3. 联合国期刊：
联合国：《网络犯罪综合研究（草案）》

10. 附录 - 名词释义

犯罪分子：指经法院判决有罪的人，在感性化表达时亦可用；

行为人：指实施行为的人，在学理分析中常用；

犯罪对象：指犯罪包含的侵害行为所指向的人和物，是犯罪客体的具体表现；

犯罪客体：指刑法所保护而为犯罪行为所侵害的社会关系，如人身权利、财产权利；

犯罪预备阶段：指为犯罪准备工具、制造条件的行为阶段；

犯罪主体：指实施危害社会的行为、依法应当负刑事责任的自然人和单位；

自然人：亦即个体的人，与法人、非法人组织等为平等的法律概念；

人身权利：指与人身直接相关而没有经济内容的权益，例如隐私权、名誉权等；

保护性管辖权：是指一国针对在该国领土范围以外实施的、严重侵害该国国家或公民的重大利益的犯罪所实施的管辖；

属地管辖权：指国家对其领土范围内一切的人、物、事所享有的管辖权；

属人管辖权：指国家对具有本国国籍的人和物所享有的管辖权；

普遍性管辖权：指根据国际法的规定，对于某些特殊的国际犯罪，不论犯罪行为发生于何地，亦不论罪犯的国籍为何，各国均有权对犯罪行为进行管辖。

法系：指按照法律的特点和历史传统对各国法律进行分类的一种方法；

判例法：是指以过往的法院判决作为法律依据的司法形式，亦指过往判决本身；

成文法：国家机关依照一定的程序制定和颁布的，表现为条文形式的规范性法律文件；

私人部门[89]：指个人、家庭和私人所拥有的企事业单位，是公共部门的对称；

国际软法：指那些不能运用国家强制力保证实施的法律规范；

89 编者注：即“private sector”；