

Distr.: Limited
27 March 2019
Chinese
Original: English

全面研究网络犯罪问题不限成员名额

政府间专家组

2019年3月27日至29日，维也纳

报告草稿

增编

二. 初步建议和结论汇总表（续）

A. 执法和调查

1. 按照工作计划，本段载有会员国在会上题为“执法和调查”的议程项目2下提出的建议汇编。这些初步建议和结论是会员国提交的，列于此处并不表示已得到专家组核可。

三. 审议情况概要

A. 执法和调查（续）

2. 在随后的辩论中，专家组重点讨论了被控在数字环境中进行的犯罪活动的例子，刑事司法从业人员和调查人员对这些活动启动或进行调查及随后进行起诉都遇到了很大困难。这些例子主要包括网上欺诈、将互联网用于恐怖主义目的、利用暗网实施非法活动，以及滥用信息和通信技术对儿童进行性虐待和性剥削。此外还向专家组通报了网络犯罪与网络安全在概念上的相互依存关系，以及与网络犯罪有关的趋势和挑战，包括勒索软件攻击；用于实施欺诈的社交工程策略（网络钓鱼、鱼叉式网络钓鱼、语音钓鱼、短信欺诈）；利用 Colbalt Strike 平台攻击银行系统；物联网；加密货币挖掘和密码劫持；还有盗读银行卡和相关的犯罪。

3. 专家组会议再次讨论了是否需要一项关于网络犯罪的新的全球综合法律文书，还是各国应重在有效执行现行文书，包括《欧洲委员会网络犯罪公约》（《布达佩斯公约》）。一方面，有与会者认为不需要关于网络犯罪的新的全球综合法律文书，因



为《布达佩斯公约》已经为针对网络犯罪制定适当的国内和国际合作对策提供了适当的框架。据回顾,《布达佩斯公约》有 63 个缔约国,这表明该《公约》开放供非欧洲委员会成员加入。此外据称,该《公约》的第三方缔约国已经以《公约》为启发,统一国内实质性和程序性的立法标准。还有与会者表示,“统一国家标准”的概念不仅包括趋同和通用定义的情况,而且还包括国际规范对制定国家规章“有用”的情况。会上提到《布达佩斯公约》与其他区域文书互为补充,例如《非洲联盟网络安全和个人数据保护公约》(2014 年)和上海合作组织(上合组织)发布的“信息安全国际行为准则”。

4. 另一方面,有与会者指出,需要在联合国框架内制定一项关于网络犯罪的新的全球法律文书,以应对互联网技术的快速发展所带来的、现有机制并未涵盖的挑战,而且现有机制也并不是全世界所有国家都加入的。据强调,所设想的这样一项文书是在联合国牵头的进程框架内制定的,在这一进程中,所有会员国都可评估(或借鉴)《布达佩斯公约》和上述《非洲联盟公约》等现有文书,为高效努力达成网络犯罪全球对策确立自主权和责任。在这方面,提到了大会 2018 年 12 月 18 日关于“会员国打击为犯罪目的使用信息和通信技术行为所面临的挑战”的第 73/187 号决议,以及其中责成秘书长就会员国打击为犯罪目的使用信息和通信技术行为所面临的挑战征求会员国的意见,并根据这些意见提交一份报告,供大会第七十四届会议审议。在其他发言中,有与会者认为,《布达佩斯公约》没有解决联合国所有会员国的关切,其中规定的案文修正程序也很复杂,鉴于网络犯罪的不断演变性,这可能是一个不利因素。

5. 会上提到正在为通过《布达佩斯公约》第二项附加议定书进行谈判,其目的是就下列问题提供明确的规则和更有效的程序:更有效快速的国际合作条款;允许就索取用户信息的请求、保全请求和紧急请求与其他法域的服务提供商直接合作的条款;为跨境获取数据的现有做法提供更明确的框架和更有力的保障;以及保障措施,包括数据保护要求。

6. 还有与会者强调,《有组织犯罪公约》可用作应对网络犯罪挑战的有用工具,特别是考虑到这些挑战的跨国性质。会上建议考虑谈判制定《有组织犯罪公约》的一项附加议定书,特别处理网络犯罪问题。

7. 各代表团和专题主讲人向专家组介绍了各国为制定和实施打击网络犯罪的法律措施和程序措施所作的成功努力。对一些国家来说,《布达佩斯公约》和相应的能力建设项目是这一领域的基本构件。会上深入审议了国家一级的立法改革问题,包括此类改革的范围。有与会者提请注意,为确保听取不同利益攸关方的意见,需要有包容性和参与性的进程。有与会者提到,有必要在“法无明文不为罪”原则的基础上确保法律的确定性和明确性,还有必要在新的立法中使用“技术中性”的语言,以便与信息和技术领域的迅速发展保持一致。

8. 讨论还围绕执法管辖权冲突产生的挑战展开,特别是下述情况,例如,服务提供商的总部设在一个法域,而数据控制人位于另一个国家,或者数据存储在另一个法域或多个法域。据指出,云计算的出现为刑事调查带来了更多的实际挑战和法律挑战。另据指出,对网络犯罪领域适用的管辖权依据采取灵活的做法可能是有益的,其中主要包括更多以提供信息通信技术服务之地为准,而不以数据所在地为准。

9. 专家组还强调，需要有适当的程序权力，以不仅获取与网络犯罪有关的电子证据，还有与各种常规犯罪形式有关的电子证据。这种电子证据可包括订户信息、内容数据或通信量数据等。据指出，由于在调查涉及电子证据的犯罪时遇到了匿名软件、高级加密和虚拟货币等新技术，调查人员可能需要采取新的战略，并考虑如何利用特殊侦查手段和远程数字取证来收集此类电子证据，同时确保此类证据在法庭上的可采性和使用。

10. 还着重讨论了如何在对网络犯罪采取有效执法对策的必要性与保护基本人权特别是隐私权之间取得平衡。共同点是，例如，数据保留条例可能是一种务实的办法，确保通信服务提供商能够更好地配合执法，从而在处理网络犯罪方面发挥更大的作用，但条件是这些法律在执行中有适当的程序保障措施和隐私保护措施。会上提到联合国人权事务高级专员关于“数字时代的隐私权”的报告，该报告已按大会第 68/167 号决议提交人权理事会（A/HRC/27/37）。

11. 专家组重申在跨国界调查和起诉网络犯罪方面开展国际合作的重要性。与会者承认，为获取或保全电子证据而提出的司法协助请求的数量正在迅速增加，目前的合作方式，特别是冗长的司法协助程序，不足以应对迅速而成功获取数据的挑战，因为此类证据不是固定不变的，只要“点击鼠标”即可转移或删除。

12. 会上列举了促进涉及电子证据的国际合作的不同做法，特别是业务上的做法，其中包括：合作国主管当局之间直接传递司法协助请求；更经常地使用因地制宜的国际合作工具，以保障电子证据的完整性，例如快速保全计算机数据；联合调查；使用电子手段传递司法协助请求，特别提到国际刑警组织以电子方式安全传输司法协助交流信息（e-MLA）的举措的潜在效用；24/7 网络联络点之间的信息共享；包括在国际刑警组织援助下，更经常地利用警察与警察之间的合作，以收集情报。还提到了欧洲打击网络犯罪中心（EC3），该中心是欧洲刑警组织在 2013 年设立的，目的是加强欧盟打击网络犯罪的执法对策。

13. 专家组还简短讨论了跨境获取数据的问题。据指出，总体而言，各国所采用的做法和程序，以及这些程序的条件和保障，在不同当事方之间差别很大。此外，还强调了嫌疑人的程序性权利、隐私上的考虑因素和对个人数据的保护、访问储存在另一法域的数据的合法性以及对国家主权的尊重。

14. 专家组强调，必须进行可持续的能力建设，以提高所有主管当局在业务层面的效力和技能，以应对网络犯罪带来的挑战。在这方面，发言者提到，国内外从业人员之间交流良好做法和经验是有益的。一些发言者提到在检察机关和执法当局内加强培训和能力建设，同时建立专门的打击网络犯罪机构或单位。在这方面强调指出，由于电子证据在常规犯罪调查中也越来越普遍，极有必要建立专门机构，利用特定专长、知识和业务技能调查这些犯罪。

15. 专家组进一步讨论了国家当局与私营部门特别是与通信服务提供商为加强数据的保全和获取而进行的合作。强调在国内这种合作日益重要，特别是在涉及严重犯罪的紧急情况下，同时也承认需要作出更多的努力，以确保在跨国案件中进行类似程度的合作。在这方面，提到通信服务提供商的“双重合规风险”，即考虑到有关各国的法律要求，如何平衡其对策。

四. 会议安排

B. 发言情况（续）

16. 下列国家的专家作了发言：阿尔及利亚、布基纳法索、加拿大、智利、中国、哥伦比亚、法国、印度、意大利、日本、科威特、毛里塔尼亚、荷兰、挪威和斯里兰卡。

17. 政府间组织欧洲联盟也作了发言。
