联合国网络犯罪政府间专家组第五次会议
书面评论意见

一、一般性评论

网络犯罪的跨国性、匿名性、智能化，以及电子证据的不稳定、易灭失，给各国执法、调查及刑事司法带来巨大挑战。现有国际法律框架下的双边司法协助等国际合作机制需要适应这些挑战。一些跨境调取电子证据的实践，对主权等国际法基本原则、正当程序保障及个人数据保护的影响令人担忧。国际社会迫切需要加速推进国际立法，协调各国打击网络犯罪法律和实践，为上述问题提供被普遍接受的解决方案。

联合国网络犯罪政府间专家组撰写的《网络犯罪问题综合研究报告草案》，提出制定与电子证据调取权相关的国际示范条款、电子证据国际合作文书、有约束力的网络犯罪问题全球性法律文书等，值得关注和讨论。中方支持联合国网络犯罪政府专家组按照2018至2021年工作计划继续开展工作，交流在网络犯罪执法与调查、电子证据与刑事司法方面的做法和经验，并按时向联合国预防犯罪委提出工作建议。

二、中国在网络犯罪执法与调查方面的实践

在立法层面，中国修改《刑法》，新增“拒不履行信息网络安全管理义务罪”、“非法利用信息网络罪”和“帮助信息网

络犯罪活动罪”，并拟于今年发布司法解释，为加强打击网络犯罪帮助行为和预备行为提供法律依据。

中国出台规定，明确网络犯罪案件“犯罪地”包括网站服务器所在地、网络接入地、网站建立者、管理者所在地，被侵害的计算机信息系统或其管理者所在地，犯罪嫌疑人、被害人使用的计算机信息系统所在地，被害人被侵害时所在地，以及被害人财产遭受损失地等，有利于强化对网络犯罪的管辖。

在执法层面，中国执法机关去年针对侵犯公民个人信息、黑客攻击、网络诈骗、网络赌博、网络色情、利用网络组织考试作弊等网络犯罪开展专项打击行动。

在国际合作层面，中国执法机关收到并处理来自国际刑警、司法协助和双边警务渠道的案件协查请求和情报通报1000余起，与70余个国家和地区构建了执法协作网络。

从中国打击网络犯罪执法与调查的实践看，当前主要面临三个突出困难：

一是网络犯罪的隐蔽性增强，犯罪分子身份溯源难。网络犯罪分子大量利用代理服务、VPN服务、网络加密等方式隐蔽真实身份，导致执法机关难以有效追踪犯罪人真实身份。

二是跨国取证需求增多，但国际合作渠道不畅。大量境内嫌疑人利用境外网络资源实施犯罪，很多关键证据都在外国。中国跨国取证主要通过司法协助和警务合作等渠道，但由于各国法律制度不同、协作效率不高等原因，往往程序繁琐，用时较长。

三是网络犯罪链条化、有组织化趋势加剧，增加执法与调查难度。网络犯罪形成黑色产业链条，各个环节均寄生了大量分工协作、利益共享的专业犯罪团伙，共同完成从准备、组织、实施犯罪、销赃分赃的整个犯罪过程，查处起来十分困难。

三、中国在网络犯罪电子证据与刑事司法方面的实践

继 2012 年将电子证据规定为法定证据种类后，中国又先后发布了两个专门的电子证据规范性文件，明确电子证据是指案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据，开放式列举了一些常见电子证据，特别是进一步细化了电子证据的取证、采信规则。

在电子证据取证方面，规定了收集、提取、检查、侦查实验、检验、鉴定等系列取证手段，以及各种取证手段的具体实施要求。

在电子证据采信方面，确立了审查判断电子证据真实性、完整性、合法性、关联性的具体程序和标准，设置了对瑕疵证据的处理规则，明确了对电子证据的非法证据排除规则。即，被篡改、伪造或无法确定真伪的电子证据，有增加、删除或修改情形，真实性受到影响的电子证据，以及其他无法保证电子证据真实性的情形不能作为定案根据。

实践中，电子证据取证和运用方面主要存在以下困难：一是随着云计算等信息技术的发展，越来越多的电子证据存储在云端，很难对其进行封存、扣押，特别是一些案件数据量很大，收集和分析任务艰巨。二是电子证据天然的无形性、

易篡改等特点，使其容易被更新、修改或清除，如何确保真实性、完整性成为问题。三是犯罪嫌疑人成功作案后，常将原始文件记录删除，造成电子证据链条不全、证明力弱，难以证明案件事实。

四、建议

执法与调查

各国进行网络犯罪执法与调查应尊重和保障人权，遵守本国法律关于刑事程序保障的规定。

各国应重视加强对帮助行为、预备行为的调查和执法，以应对网络犯罪日益加剧的链条化趋势。

各国应就云计算、暗网等对网络犯罪执法与调查的影响进
行讨论，共同研究可行的应对之策。

鼓励各国通过立法明确网络服务提供者配合防范网络犯罪和协助执法与调查的义务。例如,鼓励网络服务提供者采取技术措施和其他必要措施，防范网络犯罪；制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险，保障网络安全。

电子证据范围

各国应制定或完善立法，承认电子证据的证据能力，规定电子证据的定义和范围。

各国可考虑在本国立法中将以下数据规定为电子证据：登录日志等传输数据、电子邮件等内容数据、用户注册信息等用户数据；其他案件发生过程中形成的，以数字化形式存

储、处理、传输的，能够用于证明案件事实的数据。

电子证据取证能力

鼓励各国采取措施加强网络犯罪电子证据取证能力建设，培养法律素养和技术知识兼备的专业团队，加强在这方面的经验共享和培训合作。鼓励联合国毒品和犯罪问题办公室在这一领域发挥作用。

电子证据取证手段

鼓励各国在本国立法中规定扣押、封存原始存储介质、现场提取、远程勘验、调取等电子证据取证手段。鼓励各国通过计算电子证据完整性校验值、锁定网络应用账号、采取写保护措施等防增加、删除、修改手段“冻结”电子证据。

鼓励各国制定电子证据取证的技术规范和标准。

各国应确保电子证据取证符合正当程序原则。

电子证据采信规则

各国应在本国电子证据相关立法中规定判断电子证据真实性、完整性、合法性、关联性的规则，并在适用原始证据、传闻证据及非法证据排除等传统证据规则时考虑电子证据的特殊性。

跨国调取电子证据

各国跨国调取电子证据应尊重证据所在地的国家主权，遵守正当程序，尊重相关个人和实体的正当权利，不得采取侵入性和破坏性技术侦查手段跨国获取电子证据。

鼓励各国针对调查网络犯罪、调取电子证据的需要，协商通过优化程序等方法，进一步畅通司法协助和执法合作渠

道。

各国应考虑制定与电子证据调取权相关的国际示范条款，以及联合国框架下有约束力的打击网络犯罪全球性法律文书，并在其中纳入各方普遍接受的获取境外电子证据条款，为解决跨国调取电子证据问题提供规范。