



大会

Distr.: General
16 May 2022
Chinese
Original: English

拟订一项关于打击为犯罪目的
使用信息和通信技术行为的
全面国际公约特设委员会
第二届会议
2022年5月30日至6月10日，维也纳

会员国就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
的刑事定罪条款、总则及关于程序措施和执法的条款提交的提案和
材料汇编

增编



目录

	页次
五. 补充材料	3
导言	3
印度	3
牙买加（代表加勒比共同体）	13
马来西亚	22
新加坡	26
乌拉圭	29

五. 补充材料

导言

本增编载有 2022 年 4 月 14 日之后收到的会员国为拟订一项打击为犯罪目的使用信息和通信技术的全面国际公约特设委员会第二届会议提交的材料；材料没有按照主题划分章节。

印度

[原件：英文]
[2022 年 5 月 12 日]

背景

1. 网络空间是互联网上一个由人、软件、硬件和服务组成的复杂环境，与物理空间相比，具有鲜明而独特的特征。网络空间是虚拟的，无国界的，允许匿名。近年来，社交媒体和移动生态系统已成为重要的公共沟通渠道之一。最近，世界各地都认为，社交媒体的使用是犯罪分子和反国家分子实施网络犯罪的重要工具。与世界其他地方一样，由于网络空间无国界，加上可以即时通信，又能隐匿姓名，使用社交媒体和互联网实施网络犯罪的潜在可能在该国比以往任何时候都高。

2. 在全球信息和通信技术设备使用激增的同时，网络犯罪也成为一个大问题。技术的进步使人类依赖信息和通信技术来满足他们的所有需求。与传统犯罪不同，网络犯罪没有地域界限，网络犯罪分子是未知的，甚至是匿名的，这影响到包括普通公民在内的所有利益攸关方。下一节着重讨论全球发生的网络犯罪类型。

利用信息和通信技术实施的犯罪的分类

3. 网络犯罪是一个泛指术语，用于定义以计算机或计算机网络为犯罪活动工具、目标或场所的犯罪活动，从电子破坏到拒绝服务攻击无所不包。一般来说，网络犯罪可以分为“借助网络实施的犯罪”¹和“依赖网络实施的犯罪”。²此外，网络犯罪也可分为“针对人身的网络犯罪”、“针对财产的网络犯罪”和“针对政府的网络犯罪”。然而，最好使用“利用信息和通信技术实施的犯罪”这一定义，因为它也能够涵盖新的和新兴的技术。

¹ 例如盗窃、骚扰、剥削儿童、欺诈和诈骗，可以不用计算机而实施，但是在某些情况下要用计算机才能实施。

² 黑客攻击、勒索软件、分布式拒绝服务攻击和恶意软件、病毒传播和网络恐怖主义。

刑事定罪

4. 各缔约国应采取以下各点所规定的必要立法和其他措施，在其本国法律中将下列行为定为犯罪或同等条款。（下列清单是指示性的，还可以加上更多使用信息和通信技术实施的犯罪。）

4(a) 损坏计算机、计算机系统等

各缔约国应采取必要的立法和其他措施，在本国法律中规定，任何人未经计算机、计算机系统或计算机网络的所有者或任何其他负责人的许可而实施下列行为，均属犯罪：

(a) 访问或实现访问此类计算机、计算机系统或计算机网络或计算机资源；

(b) 从此类计算机、计算机系统或计算机网络下载、复制或提取任何数据、计算机数据库或信息，包括在任何可移动存储介质中保有或存储的信息或数据；

(c) 将任何计算机污染物或计算机病毒引入或致使引入任何计算机、计算机系统或计算机网络；

(d) 损坏或导致损坏任何计算机、计算机系统或计算机网络、数据、计算机数据库或驻留在此类计算机、计算机系统或计算机网络中的任何其他程序；

(e) 使或致使任何计算机、计算机系统或计算机网络中断；

(f) 拒绝或导致拒绝任何获得授权的人以任何方式访问任何计算机、计算机系统或计算机网络；

(g) 违反本法规定或根据本法制定的规则或条例，向任何人提供任何协助，以便利访问计算机、计算机系统或计算机网络；

(h) 通过篡改或操纵任何计算机、计算机系统或计算机网络，将一个人使用的服务记入另一个人的账户；

(i) 以任何方式破坏、删除或更改计算机资源中的任何信息，或降低其价值或效用，或对其造成有害影响；

(j) 窃取、隐藏、破坏或更改，或使任何人窃取、隐藏、破坏或更改计算机资源所用任何计算机源代码，意图造成损害。

4(b) 未能保护数据

各缔约国应采取必要的立法和其他措施，在本国法律中规定，法人拥有、经营或处理其拥有、控制或操作的计算机资源中的任何敏感个人数据或信息，若疏于实施和维护合理的安全做法和程序，从而给任何人造成非法损失或非法利得的，均属犯罪。

4(c) 篡改计算机源文件

各缔约国应采取必要的立法和其他措施，在本国法律中规定，任何人明知或故意隐藏、破坏或修改，或者明知或故意使他人隐藏、破坏或修改计算机、计算机程序、计算机系统或计算机网络所用的任何计算机源代码，而该计算机源代码是现行法律要求保存或维护的，均属犯罪，应受惩罚。

4(d) 借通信服务发送攻击性信息等

各缔约国应采取必要的立法和其他措施，在本国法律中规定下列行为为犯罪：任何人通过计算机资源或通信装置发送：

(a) 任何具有严重攻击性或威胁性的信息；

(b) 任何本人明知是虚假的信息，目的是利用此类计算机资源或通信装置持续地造成烦扰、不便、危险、阻挠、侮辱、伤害、刑事恐吓、敌意、仇恨或恶意；

(c) 任何电子邮件或电子邮件信息，目的是造成烦扰或不便，或在此类信息的来源方面欺骗或误导收件人或收信人。

4(e) 不诚实地接收被盗的计算机资源或通信装置

明知或有理由认为任何被盗的计算机资源或通信装置确是被盗的计算机资源或通信装置，而不诚实地予以接收或保留的人。

4(f) 盗用身份（假冒）

各缔约国均应采取必要的立法和其他措施，在本国法律中规定，任何人欺诈或不诚实地利用他人的电子签名、密码或任何其他独特识别特征的行为，均属犯罪。

4(g) 利用计算机资源冒名行骗（假冒）

各缔约国应采取必要的立法和其他措施，在本国法律中规定，任何人通过任何通信装置或计算机资源进行假冒欺诈，均属犯罪。

4(h) 侵犯隐私

各缔约国均应采取必要的立法和其他措施，在本国法律中规定，任何人在侵犯他人隐私的情况下，未经他人同意，故意或明知地抓拍、公布或传输他人隐私部位图像，均属犯罪：

(a) “传输”系指以电子方式发送视觉图像，以供一个人或多人观看；

(b) “抓拍”，就图像而言，系指以任何方式录像、拍照、拍摄影片或记录；

(c) “隐私部位”系指裸露或有内衣覆盖的生殖器、耻骨部位、臀部或女性乳房；

(d) “公布”系指以印刷或电子形式复制并公诸于众；

(e) “在侵犯隐私的情况下”系指一个人可以合理预期下述项目的情况下：

(一) 他或她可以私下脱衣，而不用担心其隐私部位正在被抓拍图像；或者

(二) 他或她的隐私部位的任何部分不会为公众看见，不管该人是在公共场所还是私人场所。

4(i) 网络恐怖主义

1. 各缔约国均应采取必要的立法和其他措施，在本国法律中规定下列行为为犯罪，即任何人：

(a) 通过下列行为意图威胁国家的统一、完整、安全或主权或在民众或任何一部分人中制造恐怖：

(一) 拒绝或导致拒绝任何获得授权访问计算机资源的人的访问；或者

(二) 未经授权或超越授权访问权限，试图渗透或访问计算机资源；或者

(三) 引入或导致引入任何计算机污染物；

通过此类行为，造成或可能造成人员伤亡或财产损害或破坏，或破坏对社会生活至关重要的供应或服务或明知可能对这种供应或服务造成损害或破坏，或对关键信息基础设施产生不利影响；或者

(b) 未经授权或超越授权访问权限，明知或故意渗透或访问计算机资源，并通过这种行为访问因国家安全或外交关系而受到限制的信息、数据或计算机数据库，或任何限制信息、数据或计算机数据库，有理由认为如此获得的此类信息、数据或计算机数据库可能被用于造成或可能造成对国家主权和完整、国家安全、与外国的友好关系、公共秩序、体面或道德等利益的损害，或事关藐视法庭、损害名誉或煽动犯罪，或为有利于任何外国、个人群体或其他人，实施网络恐怖主义罪。

2. 各缔约国应采取必要的立法和其他措施，在本国法律中规定，实施或共谋实施第1款(a)和(b)项所述罪行，均属犯罪。

4(j) 以电子形式的通信发布或传输淫秽材料

各缔约国应采取必要的立法和其他措施，在本国法律中规定下列行为为犯罪：任何人以电子形式发布或传输或导致发布或传输任何淫秽或引起淫欲的材料，或其效果往往会败坏和腐蚀可能（考虑到所有相关情况）会阅读、看到或听到其中所载或所体现的内容的人。

4(k) 以电子形式发布或传输含有露骨性行为等的材料

各缔约国应采取必要的立法和其他措施，在本国法律中规定，任何人以电子形式发布或传播或导致发布或传播任何含有露骨性行为或举止的材料，均属犯罪。

4(l) 以电子形式发布或传输描绘儿童露骨性行为等的材料

各缔约国均应采取必要的立法和其他措施，在本国法律中规定下列行为为犯罪，即任何人：

(a) 以任何电子形式发布或传输或导致发布或传输描述儿童从事露骨的性行为的材料；或者

(b) 创建文本或数字图像，以任何电子形式收集、搜索、浏览、下载、宣传、推广、交换或分发以淫秽、下流或露骨的性行为方式描绘儿童的材料；或者

(c) 培养、引诱或诱使儿童与一名或多名儿童建立网上关系，为了进行露骨的性行为，或在计算机资源上以可能冒犯理性成年人的方式这样做；或者

(d) 便利在线虐待儿童；或者

(e) 以任何电子形式记录自己或他人涉及与儿童发生露骨性行为的虐待行为，

前提是本节不延伸至任何电子形式的书籍、小册子、文章、著作、素描、彩画作品或形象：

(一) 事实证明，其出版理所当然，符合公共利益，因为此类书籍、小册子、文章、著作、素描、彩画作品或形象是科学、文学、艺术或学术兴趣所在或其他普遍受关注的对象，或者

(二) 为了真正的遗产或宗教目的而予以保存或使用。

“儿童”的年龄见该国国内立法中的定义。

4(m) 违反合法合同而披露信息

除本公约另有规定外，任何人，包括中间人，在根据合法合同条款提供服务时，访问了任何载有另一个人个人信息的信息材料，意图造成或明知他可能造成非法损失或非法利得，未经有关人员同意或违反合法合同，向任何其他他人披露此类材料。

5. 利用信息和通信技术实施的其他非法行为

在不影响（关于保护主权的条款）的情况下，缔约方应共同商定利用信息和通信技术实施的任何其他非法行为，以便开展本公约规定的合作。（考虑到信息和通信技术的进步，本公约中应有一项题为“其他非法行为”的条款）。

此外，还可以通过本公约扩展下列网络犯罪，就像联合国毒品和犯罪问题办公室文件³提到的刑事定罪一样：

- 非法访问
- 非法拦截：在没有权利的情况下，通过技术手段拦截向或从计算机系统或在计算机系统内部非公开传输计算机数据，包括电磁非法干扰
- 计算机滥用工具
- 身份犯罪
- 人身伤害
- 种族主义和仇外心理
- 支持恐怖主义罪
- 勒索软件

13. 所用术语

(a) “通信装置”系指手机、个人数字助理或两者的组合，或任何其他用于交流、发送或传输任何文本、视频、音频或图像的装置；

(b) “计算机”系指通过操纵电子、磁或光脉冲来执行逻辑、算术和存储功能的任何电子、磁、光或其他高速数据处理装置或系统，包括与计算机系统或计算机网络中的计算机连接或相关的所有输入、输出、处理、存储、计算机软件或通信设施；

(c) “计算机网络”系指一台或多台计算机或计算机系统或通信装置通过以下方式相互连接：

- (一) 使用卫星、微波、地面线路、有线、无线或其他通信媒体；
- (二) 终端或由两台或多台互连的计算机或通信装置组成的综合体，无论互连是否持续保持；

(d) “计算机资源”系指计算机、计算机系统、计算机网络、数据、计算机数据库或软件；

(e) “计算机系统”系指一种装置或一组装置，包括输入和输出支持装置，但不包括不可编程并能与外部文件结合使用的计算器，其中包含计算机程序、电子指令、输入数据和输出数据，可执行逻辑、算术、数据存储和检索、通信控制和其他功能；

(f) “计算机污染物”系指任何计算机指令集，其设计目的是：

- (一) 修改、破坏、记录、传输驻留在计算机、计算机系统或计算机网络中的数据或程序；或者

³ 资料来源：联合国毒品和犯罪问题办公室，《网络犯罪综合研究》，2013年2月草案，第22页。

(二) 以任何手段篡夺计算机、计算机系统或计算机网络的正常运行；

(g) “计算机数据库”系指以文本、图像、音频、视频的形式表示的信息、知识、事实、概念或指令，这些信息、知识、事实、概念或指令正在以形式化的方式准备或已经由计算机、计算机系统或计算机网络制作，并打算在计算机、计算机系统或计算机网络中使用；

(h) “计算机病毒”系指具有以下情况的任何计算机指令、信息、数据或程序：破坏、损坏、降低或从负面影响计算机资源的性能，或附着于另一计算机资源，并在程序、数据或指令被执行时或在该计算机资源中发生其他事件时运行；

(i) “损坏”系指以任何方式破坏、更改、删除、添加、修改或重新排列任何计算机资源。

(j) “计算机源代码”系指任何形式的计算机资源的程序列表、计算机命令、设计和布局以及程序分析。

(k) “网络安全”系指保护信息、设备、装置、计算机、计算机资源、通信装置和其中存储的信息免受未经授权的访问、使用、披露、干扰、修改或破坏；

(l) “数据”系指信息、知识、事实、概念或指令的表示，这些信息、知识、事实、概念或指令正在以形式化的方式准备或已经准备好，并且打算在计算机系统或计算机网络或云中处理、正在处理或已经处理，并且可以是任何形式（包括计算机打印输出、磁或光存储介质、穿孔卡、穿孔带）或存储在计算机的内部存储器中；

(m) “信息”包括数据、信息、文本、图像、声音、语音、代码、计算机程序、软件和数据库或微电影或计算机生成的缩微胶片；

(n) “法人”系指任何公司，包括从事商业或专业活动的公司、独资企业或其他由个人组成的社团；

(o) “合理的安全做法和程序”系指旨在保护此类信息免遭未经授权的访问、损坏、使用、修改、披露或损害的安全做法和程序，可以双方之间的协议中详加说明，或在任何现行法律中详细规定，在没有此类协议或任何法律的情况下，此类合理的安全做法和程序可由缔约国与其认为合适的专业机构或协会协商规定；

(p) “敏感个人数据或信息”系指缔约国可与其认为适当的专业机构或协会协商规定的个人信息；

(q) “电子邮件”和“电子邮件消息”系指在计算机、计算机系统、计算机资源或通信装置上创建、传输或接收的消息或信息，包括文本、图像、音频、视频和任何其他电子记录中的附件，可以与消息一起传输；

(r) “社交媒体中介”系指主要或唯一促成两个或更多用户之间在线互动并允许他们用其服务创建、上传、共享、传播、修改或访问信息的中介；

(s) “电子记录”系指以电子形式或缩微胶卷或计算机生成的缩微胶片存储、接收或发送的数据、记录或生成的数据、图像或声音；

(t) “发起人”系指发送、生成、存储或传输任何电子消息或致使任何电子消息发送、生成、存储或传输给任何其他的人，但不包括中间人；

(u) “财产”系指各种资产，无论是物质的还是非物质的、动产还是不动产、有形的还是无形的，包括银行账户中的资金、数字金融资产、数字货币（包括加密货币）以及证明对此类资产或其任何部分的产权或权益的法律文件或文书；

(v) “犯罪所得”系指通过实施本公约规定的犯罪或其他非法行为而直接或间接产生或获得的任何财产；

(w) “没收”在适用情况下还包括充公，系指根据法院或其他主管机关的命令永久剥夺财产；

(x) “上游犯罪”系指由其产生的所得可能成为本公约所定义的犯罪的对象的任何犯罪；

(y) “儿童色情制品”系指以任何方式显示儿童进行真实或模拟的露骨性活动，或主要为诲淫而显示儿童性器官的制品。

14. 面向数据的管辖权

面向数据的管辖权系指本国公民数据在世界任何地方被存储/处理/筛选/联合的国家应当对该数据具有更广泛的管辖权，而数据在哪里被实际存储/处理/筛选/联合则无关紧要。这种面向数据的管辖权将确保数据所有权以及隐私问题（公认的全球公民的基本权利）和人权的首要性。

（简要解释：在当前的场景中，基于威斯特伐利亚模型的经典管辖权在网络空间中并不适用，尤其是在涉及云资源会导致管辖权噩梦的场景中。例如，一个典型场景可能涉及已实施的网络犯罪，云中处理能力源自某个国家，存储聚合发生在另一个国家，云服务提供者在第三国注册，数据由服务提供者持有的用户（受害者和攻击者）可能是第四个国家的居民。显然，在这种情况下，根据传统的属地模式确定管辖权极其困难。鉴于上述情况，印度提议，公约采用面向数据的管辖权，而不是基于属地管辖权的模式。与隐私相关的数据所有权是全球公民的一项公认基本权利。欧洲法院承认这一点，它还据此承认了个人有被遗忘的权利。隐私权也与人权相关，众多国家在特设委员会中都已经提出这一点，面向数据的管辖权将有助于保护隐私权、基本权利和人权。）

15. “管辖权”可定义如下：

1. 各缔约国均应采取必要措施，在下列情况下确立对根据本公约确立的犯罪的管辖权：

(a) 犯罪在该缔约国境内实施或在该缔约国境内有影响；或者

(b) 犯罪发生在犯罪时悬挂该缔约国国旗的船只上或已根据该缔约国法律注册的航空器内。

2. 在不违反本公约的情况下，缔约国在下列情况下还可以对任何此种犯罪确立其管辖权：

(a) 犯罪系针对该缔约国国民和法人；或者

(b) 犯罪者为该缔约国国民和法人或在其境内有惯常居所的无国籍人；或者

(c) 犯罪发生在其境外，目的是为了在其领域内实施根据本公约确立的犯罪；

(d) 犯罪系针对该缔约国；或者

(e) 犯罪实施针对的目标是位于其境内的计算机资源；

(f) 犯罪涉及其国民的数字/电子数据，无论该数据的物理存储/处理/筛选/联合在何处。

3. 为本公约的目的，各缔约国应采取必要措施，在被指控犯罪人在其领域内而其仅因该人系其本国国民而不予引渡时，确立其对根据本公约确立的犯罪的管辖权。

4. 各缔约国还可采取必要措施，在被指控犯罪人在其领域内而其不引渡该人时确立其对根据本公约确立的犯罪的管辖权。

5. 如果根据本条第 1 款或第 2 款行使管辖权的缔约国被告知或通过其他途径获悉任何其他缔约国正在对同一行为进行侦查、起诉或审判程序，这些缔约国的主管机关应酌情相互磋商，以便协调行动。为根据本条进行磋商，缔约方应考虑面向数据的管辖权，即属于利用信息和通信技术实施的网络犯罪或非法行为的受害者的数据。

6. 在不影响一般国际法准则的情况下，本公约不排除缔约国行使其依据本国法律确立的任何刑事管辖权。

17. 搜查和扣押以电子方式存储或处理的信息

1. 各缔约国应采取必要的立法和其他措施，授权其主管机关搜查或以类似方式访问：

(a) 计算机系统或其一部分以及其中存储的计算机数据；

(b) 其境内可以存储计算机数据的计算机数据存储介质。

2. 各缔约方应采取必要的立法和其他措施，确保其主管机关根据第 1 款(a)项搜查或以类似方式访问某一特定计算机系统或其一部分，并有理由认为所搜寻的数据存储在其领土内的另一计算机系统或其一部分中，且此类数据可从初始系统合法访问或取用时，主管机关应能快速地将搜查或类似访问扩大到该另一系统。

3. 各缔约方应采取必要的立法和其他措施，授权其主管机关扣押或以类似方式取得根据第 1 款或第 2 款访问的计算机数据。这些措施应包括有权：

- (a) 扣押或以类似方式取得计算机系统或其一部分或计算机数据存储介质；
- (b) 制作并保留这些计算机数据的副本；
- (c) 保全/维护计算机数据的完整性。

4. 各缔约方应采取必要的立法和其他措施，授权其主管机关命令任何了解计算机系统运行或为保护计算机数据而适用的措施的人，在合理的情况下，提供必要信息，以便能够采取第 1 款和第 2 款所述的措施。

18. 实时收集流量数据

1. 各缔约国均应采取必要的立法和其他措施，授权本国主管机关：

- (a) 应用技术手段在缔约国本国境内收集或记录；
- (b) 迫使服务提供者在自身现有技术能力范围内：
 - (一) 应用技术手段在缔约国本国境内收集或记录；或者
 - (二) 配合并协助主管机关实时收集或记录本国境内借助计算机系统传输的与指定通信有关的流量数据。

2. 若缔约国由于其国内法律制度的既定原则而不能采取本条第 1 款(a)项所述的措施，则可转而采取必要的立法和其他措施，确保在本国境内应用技术手段实时收集或记录与本国境内传输的指定通信有关的流量数据。

3. 各缔约国均应采取必要的立法和其他措施，责成服务提供者对行使本条规定的任何权力以及与之相关的任何信息保密。

19. 收集内容和元数据

1. 各缔约方应采取必要的立法和其他措施，无需司法协助条约迅速提供元数据。拥有此类元数据的服务提供者应据执法机构的直接要求，通过各国指定的节点机构提供此类信息。

2. 各缔约方应采取必要的立法和其他措施，迅速提供内容数据。这种快速数据共享机制将根据本公约予以制定。

20. 拦截内容数据

1. 各缔约国均应就本国法律将确定的一系列严重犯罪采取必要的立法和其他措施，授权本国主管机关：

- (a) 应用技术手段在本国境内收集或记录；
- (b) 迫使服务提供者在自身现有技术能力范围内：
 - (一) 应用技术手段在本国境内收集或记录；或者

(二) 配合并协助主管机关实时收集或记录本国境内借助计算机系统传输的指定通信的内容数据。

2. 若缔约国由于其国内法律制度的既定原则而不能采取本条第 1 款(a)项所述的措施, 则可转而采取必要的立法和其他措施, 确保在本国境内应用技术手段实时收集或记录与本国境内传输的指定通信有关的内容数据。

3. 各缔约国均应采取必要的立法和其他措施, 责成服务提供者对行使本条规定的任何权力的事实和与之相关的任何信息保密。

21. 快速保全已存储的计算机数据

1. 各缔约国均应采取必要的立法和其他措施, 使本国主管机关能够命令或通过类似手段实现快速保全以计算机系统存储的指定计算机数据, 包括流量数据和内容数据, 特别是在有理由认为计算机数据极易丢失或被修改的情况下。

2. 若缔约方实施上述第 1 款, 命令个人保全其拥有或控制的指定已存储计算机数据, 则该缔约方应采取必要的立法和其他措施, 责成该人在必要长的期限内保全并维护该计算机数据的完整性, 最多不超过 180 天, 以便主管机关寻求予以披露。缔约国可以规定该命令嗣后可进行延期。

3. 各缔约国均应采取必要立法和其他措施, 责成保管人或其他保全这些计算机数据的人在缔约国本国法律规定的期间对执行此类程序事宜保密。

4. 各缔约方应设立一个协调节点, 让另一国可以通过该节点执行此类保全请求。

牙买加 (代表加勒比共同体)

[原件: 英文]
[2022 年 5 月 12 日]

第一章. 总则

第 条. 总则

本公约的宗旨如下:

1. 促进和加强各项措施, 以更高效率和更有效力地预防和打击针对信息和通信技术系统及计算机数据的机密性、完整性和可用性的犯罪和其他非法行为。

2. 促进、便利和支持国际合作和技术援助, 以防止和打击针对信息和通信技术系统及计算机数据的保密性、完整性和可用性的刑事犯罪和其他非法行为。

3. 促进、便利和支持在追回本公约所述刑事犯罪和其他非法行为所得资产方面的国际合作和技术援助。

第 条.适用范围

1. 本公约根据其规定，应适用于预防、侦查和起诉刑事犯罪，促进、便利和支持在预防和打击利用信息和通信技术实施刑事犯罪方面的国际合作，以及冻结、扣押、没收和返还根据本公约确立的这类犯罪的所得。
2. 为实施本公约的目的，除本公约另有规定外，根据本公约规定确立的刑事犯罪不一定对人身、财产和国家造成损害或伤害。

第 条.保护主权

1. 缔约国应以符合各国主权、主权平等和领土完整以及不干涉其他缔约国或其他国家内政原则的方式履行其根据本公约所承担的义务。
2. 本公约的任何规定均不赋予一缔约国在另一缔约国或另一国领域内行使管辖权和履行根据该另一缔约国或另一国国内法以及根据国际法和义务规定专属于该另一缔约国或其他国家主管机关的职能的权利。

第二章. 刑事定罪

第 条.非法/未经授权访问计算机系统或数据

各缔约国均应采取必要的立法和其他措施，将故意和无权情况下访问整个计算机系统或其任何部分的行为定为刑事犯罪。缔约国可规定犯罪行为实施方式是违反或违背安全措施，意图获取计算机数据或有其他不诚实意图，或者涉及与另一计算机系统相连的计算机系统。（根据《布达佩斯公约》第 2 条——非法访问）

第 条.非法/未经授权拦截

1. 各缔约国均应采取必要的立法和其他措施，将无权或未经授权故意对计算机系统或数据实施拦截定为刑事犯罪，条件是此类拦截以技术手段实施，意在拦截流量数据和通过信息通信技术处理的、并非供公众使用的数据，包括载有这类计算机数据的计算机系统的电磁发射。
2. 缔约国可规定犯罪出于不诚实意图，或者涉及与另一计算机系统相连的计算机系统。

第 条.非法干扰数据

1. 各缔约国均应采取必要的立法和其他措施，将无权或未经授权故意输入、破坏、删除、损坏、更改或抑制计算机数据的行为定为刑事犯罪。
2. 缔约国可保留规定第 1 款所述行为造成严重损害的权利。

第 条.非法干扰系统

1. 各缔约国均应当采取必要的立法和其他措施，将无权或未经授权通过输入、传输、破坏、删除、损坏、更改或抑制计算机数据而故意妨碍信息和通信技术系统运行的行为定为刑事犯罪。
2. 各缔约国可保留对第 1 款所述涉及或影响关键基础设施的行为加重处罚的权利。

第 条.滥用装置/恶意软件/计算机程序

1. 各缔约国均应采取必要的立法和其他措施，将无权却故意实施的以下行为定为刑事犯罪：
 - (a) 生产、销售、采购使用、进口、分销或以其他方式提供：
 - (一) 主要为实施根据相关条款（未经授权/非法访问、未经授权/非法拦截/干扰数据/干扰系统）确定的任何刑事犯罪而设计或改装的装置，包括计算机程序；
 - (二) 计算机密码、访问代码或能够访问整个信息、通信和技术系统或其任何部分所凭借的类似数据，意图将其用于实施相关条款（未经授权/非法访问、未经授权/非法拦截/干扰数据/干扰系统）所确立的任何刑事犯罪；
 - (b) 拥有上文(a)(一)或(二)项所述物品，意图将其用于实施各条款（未经授权/非法访问、未经授权/非法拦截/干扰数据/干扰系统）所述的任何刑事犯罪。缔约国可依法规定在刑事责任发生之前拥有若干此种物品。
2. 如果本条第 1 款所述的生产、销售、采购使用、进口、分销或以其他方式提供或拥有并非为了实施根据相关条款（未经授权/非法访问、未经授权/非法拦截/干扰数据/干扰系统）确立的刑事犯罪，例如是为了经授权测试或保护计算机系统，则本条不应解释为追究刑事责任。
3. 各缔约国可保留不适用本条第 1 款的权利，但该保留不得涉及本条第 1(a)(一)款所述物品的销售、分销或以其他方式提供。

第 条.与内容有关的犯罪

1. 各缔约国均应采取必要的立法和其他措施，将无权而故意实施的下列行为定为刑事犯罪：
 - (a) 通过信息和通信技术系统制作儿童性剥削和性虐待材料；
 - (b) 通过信息和通信技术系统提供儿童性剥削和性虐待材料；
 - (c) 通过信息和通信技术系统分发或传输儿童性剥削和性虐待材料；
 - (d) 通过计算机系统/信息和通信技术系统为自己或他人获取儿童性剥削和性虐待材料；

(e) 在计算机系统/信息和通信技术系统或在计算机数据存储介质中拥有儿童性剥削和性虐待材料。

2. 就上文第 1 款而言，“儿童性剥削和性虐待材料”一词应包括视觉上描绘以下内容的材料：

- (a) 儿童参与露骨性行为；
- (b) 貌似儿童的人参与露骨性行为；
- (c) 表现未成年人参与露骨性行为的逼真图像。

3. 就上文第 2 款而言，“儿童”一词系指十八(18)岁以下的任何人，除非适用儿童的法律规定成年年龄低于 18 岁。（《儿童权利公约》，第 1 条）

第 条.侵犯隐私/未经同意传播色情图像

1. 各缔约国均应采取必要的立法和其他措施，将无权而故意实施的下列行为定为刑事犯罪：

(a) 明知图像对象未同意，发布、分发、传输、销售、提供或宣传某人的私密图像；

(b) 发布、分发、传输、销售、提供或宣传某人的私密图像是为了骚扰或伤害图像对象。

“私密图像”的定义

2. 在本条中，“私密图像”是指以任何方式，包括摄影、影片或录像，对一个人进行的视觉记录：

(a) 其中该人裸体，其生殖器官、肛区或乳房暴露，或正进行露骨的性活动；

(b) 就此而言，在录制时，存在引起对隐私产生合理期望的情况；及

(c) 就此而言，在实施犯罪时，图像对象仍带有合理的隐私期望。

第 条.知识产权

各缔约国均应采取必要的立法和其他措施，将利用信息和通信技术故意实施并具有商业规模的侵犯缔约国立法所界定的版权和相关权利的行为定为刑事犯罪。

与计算机有关的罪行

第 条.与计算机有关的作假

1. 各缔约国均应采取必要的立法和其他措施，将无权而故意输入、更改、删除或抑制计算机数据，造成不真实的数据，意图使其在法律上被视为真实的数

据或将其作为真实数据处理的行为定为刑事犯罪，而不论该数据是否可直接阅读和理解。

2. 缔约国可以规定在刑事责任发生之前存在欺诈意图或类似的不诚实意图。

第 条.与计算机有关的欺诈

1. 各缔约国均应采取必要的立法和其他措施，将无权或未经授权通过以下方式故意实施的造成他人财产损失的行为定为刑事犯罪：

- (a) 对计算机数据的任何输入、更改、删除或抑制；
- (b) 对计算机系统运行的任何干扰；

具有欺诈或不诚实意图，为自己或他人获取经济利益。

第 条.未完成罪

1. 各缔约国均应采取必要的立法和其他措施，将以共犯、协助者、教唆犯、唆使者或共谋者等任何身份参与根据本公约确立的犯罪定为刑事犯罪。

2. 各缔约国可采取必要的立法和其他措施，将实施根据本公约确定的犯罪的任何未遂和中止定为刑事犯罪。

3. 各缔约国应采取必要的立法和其他措施，将为实施根据本公约确定的犯罪进行预备的行为定为刑事犯罪。

第 条.法人责任

1. 各缔约国应采取符合其法律原则的必要措施，凡任何自然人，在法人机构中担任领导职务的，不论是作为个人还是作为法人机构的一部分行事，凭借下述权力为法人利益实施根据本公约确立的刑事犯罪的，就确定该法人参与此犯罪的责任：

- (a) 法人代表权；
- (b) 代表法人作出决定的授权；
- (c) 在法人内部行使监督或控制的授权。

2. 除本条第 1 款已经规定的情况外，各缔约国应采取必要措施，确保能够追究法人的责任，条件是因为第 1 款所述自然人不受监督或控制，所以该自然人可以根据法人明示或默示授权行事，为该法人的利益实施根据本公约确定的刑事犯罪。

3. 在不违反缔约国国内法的情况下，法人责任可以是刑事责任、民事责任或行政责任。

4. 此种责任不应影响实施刑事犯罪的自然人的刑事责任。

5. 各缔约国均应特别确保使依照本条应当承担责任的法人受到有效、适度和劝阻性的刑事或非刑事制裁，包括金钱制裁。

第 条.制裁和措施

1. 各缔约国均应使实施根据本公约确立的刑事犯罪受到与罪行严重程度相称、有效、适度和劝阻性的制裁，包括剥夺自由。
2. 各缔约国均应确保使依照第...条（法人责任）应当承担责任的法人承受有效、适度和劝阻性的刑事或非刑事制裁或措施，包括金钱制裁。

第三章. 程序法和执法

第 条.程序规定的范围

1. 各缔约国均应采取必要的立法和其他措施，为刑事侦查或诉讼的目的确立本章所规定的权力和程序。
2. 除第...条（拦截通信）另有规定外，各缔约国均应将本条第 1 款所述权力和程序适用于：
 - (a) 根据本公约条款（刑事定罪规定）确立的刑事犯罪；
 - (b) 利用信息、通信和技术系统实施的其他刑事犯罪；
 - (c) 收集刑事犯罪的电子形式的证据。
3. 各缔约国可保留仅对保留中规定的刑事犯罪或刑事犯罪类型适用相关条款（实时收集数据）所述措施的权利，条件是此类犯罪的范围不超过缔约国适用相关条款（拦截内容数据）所述措施的刑事犯罪的范围。
4. 如果缔约国由于其在通过本公约时已生效的立法的限制，无法对在服务提供者计算机系统内传输的通信适用相关条款（实时收集数据）和相关条款（拦截内容数据）所述的措施，而该系统：
 - (i) 正在为一个封闭用户群的利益运行；
 - (ii) 不使用公共通信网络，也不与另一个公共或私人计算机系统连接；则该缔约国可保留不对此类通信适用上述措施的权利。
5. 各缔约国均应考虑对这种保留加以限制，以便能够最广泛地适用各条款（实时收集数据和拦截内容数据）所述措施。

第 条.条件和保障措施

1. 各缔约国应确保本条所规定的权力和程序的确立、实施和适用符合其国内法规定的条件和保障措施，其中应规定保护人权和自由，包括其根据 1966 年《公民及政治权利国际公约》和其他适用的国际人权文书所承担的义务而产生的权利。

2. 鉴于有关程序或权力的性质，这种条件和保障措施除其他外还应酌情包括司法监督或其他独立监督、适用的正当理由以及这种权力或程序的范围和期限限制。
3. 在符合公共利益，特别是健全司法的范围内，各缔约国应考虑本条规定的这些权力和程序对第三方的权利、责任和合法利益的影响。

第 条. 加快保全计算机数据

1. 各缔约国均应采取可能必要的立法和其他措施，使其主管机关能够下令或以类似方式迅速获取、收集和保全指定的计算机数据，包括流量数据，特别是在有理由认为这些数据特别容易被删除、修改或丢失的情况下。
2. 如果缔约国执行上述第 1 款，命令某个人（包括法人）保全其所拥有或控制的指定已存储计算机数据，则该缔约国应采取必要的立法和其他措施，要求此人在必要长的期限内保全和维护计算机数据的完整性，但最长不超过该缔约国国内法规定的期限，以便主管机关能够寻求披露这些数据。缔约国可以规定，此种命令嗣后可以延期。
3. 各缔约国应采取必要的立法和其他措施，要求负责保全信息之人对在本国法律规定的期间采取此类程序事宜保密。
4. 本条所述权力和程序应根据相关条款（程序规定的范围、条件和保障措施）确定。

第 条. 快速保全和部分披露流量数据

1. 各缔约国均应就根据相关条款（快速保全计算机数据）应予保全的流量数据采取必要的立法和其他措施，以便：
 - (a) 确保无论一个还是多个服务提供者参与了相关信息的传输，都可快速保全流量数据；
 - (b) 确保迅速向缔约国主管机关或该主管机关指定的人员披露足够数量的流量数据，使缔约国能够确定服务提供者和通信的传输路径。
2. 本条所述权力和程序应根据相关条款（程序规定的范围、条件和保障措施）确定。

第 条. 提交令

1. 各缔约国均应采取必要的立法和其他措施，授权其主管机关在有合理理由相信已经实施或正在实施刑事犯罪时，命令：
 - (a) 本国境内的某个人（包括法人）提交其拥有或控制的、存储在计算机系统或计算机数据存储介质中的计算机数据；
 - (b) 在该缔约国境内提供服务的服务提供者提交其所拥有或控制的与此类服务有关的用户信息。

2. 本条所述权力和程序应根据相关条款（程序规定的范围以及条件和保障）确定。
3. 就本条而言，“用户信息”一词系指服务提供者掌握的除流量数据和内容数据之外与其服务用户有关的任何信息，基于这些信息有可能确定：
 - (a) 使用的信息和通信服务类型、采用的技术规定和服务期；
 - (b) 可从服务协议或安排中获取的用户身份、邮政地址或地理地址、电话和其他接入号码，包括互联网协议地址，以及账单和付款信息；
 - (c) 对服务协议或安排有影响的信息和通信设备的位置信息。

第 条. 搜查和扣押以电子方式存储或处理的信息

1. 各缔约国均应采取必要的立法和其他措施，授权其主管机关在有合理理由相信已经实施或正在实施刑事犯罪时，搜查或以类似方式访问：
 - (a) 信息和通信技术系统或其一部分以及其中存储的计算机数据；
 - (b) 在本国境内的可能存储了计算机数据的计算机数据存储介质。
2. 各缔约国应采取必要的立法和其他措施，确保若其主管部门根据第 1 款(a)项搜索或以类似方式访问某一特定计算机系统或其一部分，并有合理的理由认为所查找的数据存储在其境内的另一计算机系统或其一部分内，且从初始系统可以合法访问或初始系统可以取用这种数据，则主管部门应能迅速扩大搜索或以类似方式访问该另一系统。
3. 各缔约国应采取必要的立法和其他措施，授权其主管机关扣押或以类似方式取得根据第 1 款或第 2 款访问的计算机数据。这些措施应包括有权：
 - (a) 扣押或以类似方式取得计算机系统或其一部分或计算机数据存储介质；
 - (b) 制作并保留这些计算机数据的副本；
 - (c) 维护相关已存储计算机数据的完整性；
 - (d) 使被访问的计算机系统计算机数据无法访问或移除。
4. 各缔约国均应采取必要的立法和其他措施，授权其主管机关命令了解计算机系统的运行情况或了解为保护其中的计算机数据而适用的措施的任何人，在合理的情况下，提供必要的信息，以便能够采取第 1 款、第 2 款和第 3 款所述措施。
5. 本条所述权力和程序应根据相关条款（程序规定的范围，及条件和保障措施）确定。

第 条. 实时收集流量数据

1. 各缔约国均应采取必要的立法和其他措施，授权其主管机关在有合理理由认为已经实施或正在实施刑事犯罪时：

- (a) 在该缔约国境内应用技术手段收集或记录;
 - (b) 迫使服务提供者在其现有技术能力范围内:
 - (c) 在该缔约国境内应用技术手段收集或记录; 或者
 - (d) 配合并协助主管机关实时收集或记录与该国内通过计算机系统传输的指定通信有关的流量数据。
2. 如果缔约国根据其国内法不能采取第 1 款(a)项所述的措施, 则可转而采取必要的立法和其他措施, 确保在本国境内应用技术手段, 实时收集或记录与在其境内传输的指定通信有关的流量数据。
 3. 各缔约国应采取必要的立法和其他措施, 责成服务提供者对行使本条规定的任何权力的事实以及与之有关的任何信息保密。
 4. 本条所述权力和程序应根据相关条款(程序规定的范围, 及条件和保障措施)确定。

第 条.拦截内容数据

1. 各缔约国均应针对拟由本国法律确定的一系列严重刑事犯罪采取必要的立法和其他措施, 授权其主管机关在有合理理由认为已经实施或正在实施刑事犯罪的情况下:
 - (a) 在该缔约国境内应用技术手段收集、记录或存储,
 - (b) 迫使服务提供者在其现有技术能力范围内:
 - (c) 在该缔约国境内应用技术手段收集、记录或存储, 或者
 - (d) 配合并协助主管机关实时收集或记录在该国内通过计算机系统传输的指定通信的内容数据。
2. 如果缔约国根据其国内法不能采取第 1 款(a)项所述的措施, 可以转而采取必要的立法和其他措施, 确保在其境内应用技术手段, 实时收集或记录关于其境内指定通信的内容数据。
3. 各缔约国应采取必要的立法和其他措施, 要求服务提供者对行使本条规定的任何权力的事实以及与之有关的任何信息保密。
4. 本条所述权力和程序应根据相关条款(程序规定的范围, 及条件和保障措施)确定。

马来西亚

[原件：英文]
[2022年4月20日]

第一章. 总则

第1条. 宗旨声明

本公约的宗旨是：

- (a) 促进和加强更有效率和效力地预防和打击/制止网络犯罪的措施；
- (b) 推动和便利国际合作；
- (c) 支持能力建设和技术援助，使会员国能够增强自身应对网络犯罪的能力；
- (d) 确保在执法权益和尊重基本人权之间达成适当平衡。

第2条. 术语使用

在本公约中：

- (a) “儿童”系指18岁以下的任何人；
- (b) “主管机关”系指经国内法授权下令、授权或承担执行本公约所规定的有关刑事侦查或诉讼措施的司法、行政或其他执法机关；
- (c) “计算机”系指单台执行逻辑、运算、存储和显示功能的电子、磁力、光学、电化学或其他数据处理设备，或者一组此类相互连接或相关的设备，包括与这类单台设备或一组相互连接或相关的设备直接相关或与之一起运行的任何数据存储设施或通信设施，但不包括自动打字机或排字机，或者便携式手持计算器或不可编程或不包含任何数据存储设施的其他类似设备；
- (d) “网络犯罪”系指根据本公约确立的犯罪；
- (e) “数据”系指以适合在计算机上使用的形式正在编制或已编制的信息或概念的表现方式；
- (f) “功能”包括在计算机上输入、输出或在计算机内部进行的逻辑、控制、运算、删除、存储、检索和通讯或通信；
- (g) “程序”系指代表指令或语句的数据，其在计算机上被执行后，使计算机执行某种功能。

第3条. 适用范围

1. 本公约除非另有规定，应适用于预防、调查和起诉本公约所规定的犯罪。
2. 本公约如有规定，还可适用于收集刑事犯罪的电子形式的证据。

3. 就本公约所涉事宜提供和开展技术援助和能力建设。

第4条. 保护主权

1. 缔约国在履行本公约规定的义务时，应恪守国家主权平等、国家领土完整和不干涉他国内政原则。
2. 本公约不授权一缔约国在另一国领土内行使管辖权或该另一国的国内法规定专属于其主管部门的职能。

第二章. 刑事定罪和执法

第5条. 未经授权访问

各缔约国应采取必要的立法和其他措施，将任何人故意实施的任何类型未经授权访问存储在计算机中的任何程序或数据的行为定为刑事犯罪。

第6条. 未经授权拦截

各缔约国应采取必要的立法和其他措施，将任何人故意实施的任何类型未经授权拦截任何数据或通信的行为定为刑事犯罪。

第7条. 干扰数据

1. 各缔约国应采取必要的立法和其他措施，在国内法中规定，没有权利却故意实施的破坏、删除、损坏或更改计算机数据的行为，属于刑事犯罪。
2. 缔约国可保留权利，规定第1款所述行为产生严重危害。

第8条. 妨碍计算机、程序或数据

各缔约国应采取必要的立法和其他措施，将以干扰、中断、抑制、阻碍、防止访问或损害的方式故意实施严重妨碍计算机程序或数据的行为定为刑事犯罪。

第9条. 滥用数据、程序或计算机

各缔约国应采取必要的立法和其他措施，将无权而故意实施的生产、改写、销售、采购使用、进口、给予、分销、供应或以其他方式提供任何数据、程序或计算机的行为定为刑事犯罪。

第10条. 儿童色情制品相关犯罪

1. 将无权而故意实施的下列行为定为刑事犯罪：

(a) 制作、生产或指导制作或生产任何儿童色情制品，旨在通过计算机系统予以分发的行为；

(b) 在筹备制作或生产儿童色情制品的过程中，或在筹备指导制作或生产儿童色情制品的过程中，或在制作或生产儿童色情制品的过程中，或者在指导制作或生产儿童色情制品的过程中，利用儿童或导致儿童被利用，旨在通过计算机系统予以分发的行为；

(c) 通过计算机系统，交换、发布、印刷、转载、销售、租赁、分发、展示、广告宣传、传输、促销、进口、出口、传送、给予或提供任何儿童色情制品的行为；

(d) 通过计算机系统获得、收集或寻求任何儿童色情制品的行为；

(e) 通过计算机系统参与本人明知或有理由认为与任何儿童色情制品相关的任何业务或接受其收益的行为；

(f) 通过计算机系统访问或个人持有或控制任何儿童色情制品的行为。

2. 就第 1 款而言，“儿童色情制品”一词采用《儿童权利公约关于买卖儿童、儿童卖淫和儿童色情制品问题的任择议定书》所下的定义。

第 11 条. 犯罪未遂及帮助和教唆

1. 各缔约国应采取必要的立法和其他措施，根据国内法确定，以任何身份，诸如共犯、助手或教唆犯，教唆或参与本公约规定的犯罪，均属刑事犯罪。

2. 各缔约国可采取必要的立法和其他措施，根据国内法确定，实施本公约规定的犯罪的任何未遂，均属刑事犯罪。

3. 各缔约国可采取必要的立法和其他措施，根据国内法确定，为实施本公约规定的犯罪进行预备的行为，均属刑事犯罪。

第 12 条. 法人责任

1. 各国应采取与其法律原则一致的必要措施，确定法人参与本公约规定的犯罪的责任。

2. 在不违反缔约国法律原则的情况下，法人责任可以是刑事责任、民事责任或行政责任。

3. 法人责任不影响实施犯罪的自然人的刑事责任。

4. 各缔约国尤其应确保根据本条规定被追究责任的法人受到有效、适度 and 劝阻性刑事制裁或非刑事制裁，包括金钱制裁。

第 13 条. 起诉、判决和制裁

1. 各缔约国应让实施本公约规定的犯罪的行为受到制裁，制裁应考虑到犯罪的严重程度。

2. 各缔约国应努力确保行使其国内法规定的任何法定裁量权，就本公约所涵盖的犯罪起诉有关人员，应最大限度发挥惩治这些犯罪的执法措施的效力，并适当考虑到吓阻实施此类犯罪的必要性。
3. 就本公约规定的犯罪，各缔约国应根据国内法采取适当措施，同时考虑到辩方的权利，力求确保就保外候审或上诉的裁决施加的条件要考虑到确保被告出席后续刑事诉讼的需要。
4. 各缔约国应确保法院或其他主管机关在考虑早释或假释被判定犯有本公约所涵盖犯罪的人的可能时，要谨记此类犯罪的严重性。
5. 本公约的任何规定概不影响以下原则，即根据本公约规定的犯罪、适用的法律辩护或其他决定行为合法性的法律原则均留给缔约国国内法予以说明，并且应根据该国内法起诉和惩罚此类犯罪。

第三章. 刑事诉讼程序和执法

第 14 条. 程序措施的范围

1. 各缔约国应采取必要的立法和其他措施，确立本章所规定的以刑事调查或诉讼为目的的权力和程序。
2. 除非另有明确规定，各缔约国应将本条第 1 款所述权力和程序适用于：
 - (a) 根据本公约所定义的犯罪而确定的刑事犯罪；
 - (b) 通过计算机系统实施的其他刑事犯罪；
 - (c) 收集刑事犯罪的电子形式的证据。

第 15 条. 提交令

各缔约国均应采取必要的立法和其他措施，授权其主管机关命令本国境内某人提供该人持有或控制的、存储在计算机系统或计算机数据存储介质上的指定计算机数据。

第 16 条. 搜查和扣押已存储的计算机数据

各缔约国均应采取必要的立法和其他措施，授权其主管机关搜查、扣押和扣留任何此类证据，主管机关应有权获取存储在任何计算机中的任何程序或数据，或有权访问主管机关有合理理由怀疑目前或已经涉及用于本公约所规定任何犯罪的任何计算机和任何相关设备或材料，检查或查验其操作情况。

第 17 条. 管辖权

1. 各缔约国在下列情况下应采取必要措施，确立对本公约规定的犯罪的管辖权：
 - (a) 犯罪发生在该缔约国境内；或者

(b) 犯罪发生在罪行实施时悬挂该缔约国国旗的船只上或已根据该缔约国的法律注册的航空器内。

2. 根据本公约的主权条款，缔约国在下列条件下还可以确立对任何此类犯罪的管辖权：

(a) 犯罪系针对该缔约国的国民；或者

(b) 犯罪人系该缔约国的国民；或者

(c) 犯罪系针对该缔约国。

3. 为本公约的引渡条款之目的，各缔约国应采取必要措施，在被指控犯罪人位于其境内且其仅因该人是其本国国民而不予引渡时，确立其对本公约所规定犯罪的管辖权。

4. 各缔约国还可采取必要措施，在被指控犯罪人位于其境内且其不予以引渡时，确立其对本公约所规定犯罪的管辖权。

5. 若根据本条第 1 或 2 款行使管辖权的缔约国被告知或通过其他途径获悉，任何其他缔约国正在对同一行为进行侦查、起诉或审判程序，这些缔约国的主管机关应酌情相互磋商，以便协调行动。

6. 在不影响一般国际法准则的情况下，本公约不排除缔约国行使其依据本国法律确立的任何刑事管辖权。

第 18 条. 受害者权利

1. 各缔约国应制定适当程序，为本公约所涵盖犯罪的被害人提供获得补偿的机会。

2. 各缔约国应在不违背国内法的情况下，在对犯罪人提起的刑事诉讼程序的适当阶段，以不损害被告方权利的方式使被害人的观点和关切得到表达和考虑。

新加坡

[原件：英文]

[2022 年 4 月 28 日]

总则

术语和定义

2. 应当从一开始就明确本公约所使用术语的定义，特别是已提出的用来表述本公约主题事项的两个关键术语，即“网络犯罪”和“为犯罪目的使用信息和通信技术行为”。“网络犯罪”一词被广泛接受，它包括依托网络实施的犯罪和借助网络实施的犯罪。第二个术语“为犯罪目的使用信息和通信技术行为”包含超出“网络犯罪”范围的一系列通信技术相关问题。

3. 新加坡认为，本公约应以“网络犯罪”为基础，因为这是一个被广泛接受的术语，涵盖了会员国正在面临的当前和新出现的网络犯罪威胁。这将让本公约更加侧重于网络空间特有的或借助网络空间实施的犯罪，并能够以更加务实的方式应对这些威胁。

4. 第一届会议上也审议了公约中应使用“预防和打击”还是“打击”的字眼。新加坡倾向于使用“预防和打击”，此前的文书、包括《联合国打击跨国组织犯罪公约》中也使用了“预防和打击”。

数据隐私

5. 数据隐私考量应兼顾确保公共安全的需要，包括为确保网络安全打击网络犯罪，以及允许执法机构采取必要措施，迅速有效地打击网络犯罪。

刑事定罪和执法

6. 本公约还应包括网络诈骗（依托网络实施的和借助网络实施的诈骗），因为当今世界绝大多数诈骗案件均为网络诈骗。仅在新加坡，2021年诈骗受害者损失就达到至少6.333亿新加坡元，诈骗案件数量比上一年增加52.9%，占有犯罪案件的一半以上。诈骗团伙资源充足，它们利用技术跨国行骗并掩盖其踪迹。

7. 新加坡草拟的建议如下文所示。我们相信，这些建议是如何在本公约中专门针对关键网络诈骗的现实而可靠的起点。

非法访问

1. 各缔约国应采取必要的立法和其他措施，将无权而故意实施的访问整个或部分计算机系统的行为定为刑事犯罪。

2. 缔约国可规定该犯罪是通过违反安全措施实施的，目的是获取计算机数据或有其他不诚实的意图，例如，冒充他人身份，或者涉及接入另一个计算机系统的计算机系统。

网络诈骗

各缔约国应采取必要的立法和其他措施，将通过下列方式无权而故意实施的、造成他人或实体财产损失的行为定为刑事犯罪：

(a) 任何输入、篡改、删除或抑制数据的行为；

(b) 任何干扰计算机系统正常运行的行为；

(c) 利用计算机系统欺骗或诱导他人或实体从事或不从事其本不会从事或不从事的某一行为，心怀欺诈或不诚实的意图，为本人或其他人获得无权获得的：

(一) 经济利益；和（或）

- (二) 实施者本来无法获得的计算机数据或个人信息。

非法获取密码和证书

各缔约国应采取必要的立法和其他措施，在国内法中规定，无权而故意实施的采购、获取、接受或分发计算机系统或计算机数据的密码或访问证书，均属刑事犯罪。

程序措施和执法

保全、收集、获取和共享电子证据和数据

8. 关于保全、收集、获取和共享电子证据和数据，我们想说明三点：

(a) 由于越来越多的数据被存储在云端，并且越来越多的交易以数字形式开展，特别是针对网络犯罪的犯罪侦查主要涉及数字证据。若不及时保全、收集和获取数字证据，将会阻碍侦查和起诉；

(b) 通过现有渠道，例如司法协助条约等渠道请求数字证据，过程漫长。若不及时保全、收集和获取数字证据，等到各国决定同意司法协助条约请求时，此类证据很有可能已被覆盖。因此，我们支持必须对加快保全数据的合法请求采取措施；

(c) 网络犯罪具有跨国性质。技术进步使得犯罪分子能够跨国远程实施犯罪活动。关于跨境共享电子证据和数据的条款将使执法机构能够获得可采取行动的侦查线索，方便成功逮捕和随后起诉犯罪分子并追回资产。如执行请求可能会损害被请求方的主权、安全、公共秩序或其他重要利益，本公约应允许缔约方选择拒绝这类请求。

9. 此外，我们注意到会员国的法律制度和情况各异，最终会影响其落实程序措施的能力，特别是有关实时收集和拦截数据的能力。我们注意到对于大多数网络犯罪案件，如能特别是在一项获得各国广泛支持的多边条约中载入保全、收集、获取和共享电子证据和数据的措施，就已经能够大大有助于侦查程序。因此，我们应当避免在行动过程中限制过严，以便使本条约的条款适用于大多数国家，从而获得更广泛的加入/批准。这样能让我们以协调一致的方式更加有效地在全球解决网络犯罪。

资产追回

10. 新加坡听到许多会员国提出必须建立资产追回机制。我们对此表示支持。网络犯罪集团开展的跨国行动十分复杂，不易发现或者粉碎。这些集团资源充足，善于利用技术来掩盖踪迹。如果犯罪所得已经从一国转移出境，通常很难追回。

11. 因此，本公约提供了执行具体、及时、有效和协调一致的资产追回全球措施的机会，因为任何国家追回已被转移出其管辖区的犯罪所得的能力取决于外

国执法机构的合作。各国必须在资产追回方面开展合作，让犯罪组织无法从犯罪所得中获益，使其无法变得更加壮大、能力更强、更加严密。

乌拉圭

[原件：英文]

[2022年5月6日]

1. 本公约应根据大会第 74/247 号决议，考虑到国家、区域和国际层面在预防和打击为犯罪目的使用信息和通信技术方面现有的国际文书和努力。

因此，本公约还应就本公约与其他既有文书之间的联系，包括优先适用和非排他性等事宜，制定一项条款。

乌拉圭认为，案文中应包括呼吁将联合国系统内协调一致地预防和打击非法使用信息和通信技术作为一项总则。

2. 应为本公约配置一个灵活的后续和修订机制，同时考虑到在该事项上的进展和永久性变化。

本公约应以中立技术语言为基础，避免使用与具体操作系统或软件相关的语言，目的是提供一种更广泛的方法，能够联系迅速变化的环境加以解释。

乌拉圭认为，除了包含灵活的修订程序以方便更新并建立争端解决机制之外，本公约还必须允许提出解释性声明。

应定期举行缔约方会议，研究该主题的重大变化，并将其反映在本公约的内容当中。《联合国反腐败公约》第六十九条第一款可提供指导：

缔约国会议应当尽力就每项修正案达成一致。如果已经为达成一致作出一切努力而仍未达成一致意见，作为最后手段，该修正案须有出席缔约国会议并参加表决的缔约国的三分之二多数票方可通过。

3. 应当考虑提供私营部门、民间社会和学术界的参与和意见的实例。

4. 关于国际管辖权，乌拉圭认为应当在考虑到调查的时间优先和申诉日期的前提下，解决两个或两个以上国家管辖权重叠的问题。

尽管如此，缔约国在针对本公约规定的任何在其领土上，或在悬挂本国国旗的船只上，或在依据本国法律注册的航空器内实施的犯罪行使管辖权时，如果被告知或通过其他途径获悉，任何其他缔约国正在对同一行为进行侦查、起诉或审判程序，这些缔约国的主管机关应酌情相互磋商，以便协调行动。

如犯罪人在一国领土内且因国籍问题无法引渡，缔约方也应采取本公约规定的措施。如本公约所规定犯罪的实施者身在某国境内，则该国应毫不延迟地向其主管部门提交案件，以便根据该国法律提起法律诉讼。

5. 打击网络犯罪是一项及时而迫切的挑战，应当在充分考虑到保护、尊重和实现人权和基本自由的前提下加以应对。

应当根据人权领域各自的国际义务理解和使用本公约的所有条款。因此，应当有一个序言部分段落重申《世界人权宣言》、《公民及政治权利国际公约》和其他人权相关文书。
